SYBASE®

# Guide d'administration système
# Volume 1

**Adaptive Server Enterprise**

**12.5**

Réf. du document : 37929-01-1250-01

Dernière mise à jour : Mai 2001



Sybase, Inc., 6475 Christie Avenue, Emeryville, CA 94608, Etats-Unis d'Amérique.

# Table des matières

# Préface

Ce manuel, *Sybase Adaptive Server - Guide d'administration système*, traite de l'administration et du contrôle des bases de données Sybase Adaptive Server Enterprise, quelles que soient les applications de bases de données utilisées.

## A qui s'adresse ce manuel ?

Ce manuel s'adresse aux administrateurs système (SA) Sybase et aux propriétaires de bases de données (DBO).

## Comment utiliser ce manuel ?

Ce manuel contient les chapitres et annexes suivants :

- Le chapitre 1, "Présentation de l'administration du système", décrit la structure du système Sybase.
- Le chapitre 2, "Bases de données système et facultatives", traite du contenu et du rôle des bases de données système d'Adaptive Server.
- Le chapitre 3, "Administration système présentée aux débutants", récapitule les tâches importantes que doivent exécuter les administrateurs système débutants.
- Le chapitre 4, "Diagnostic des problèmes système", traite de la gestion des erreurs d'Adaptive Server et de Backup Server™. Il décrit également des procédures pour arrêter les serveurs et supprimer les processus utilisateur.

- Le chapitre 5, "Définition des paramètres de configuration", résume les paramètres de configuration définis à l'aide de sp_configure, qui permettent de contrôler la plupart des aspects du fonctionnement d'Adaptive Server.
- Le chapitre 6, "Restriction de l'accès aux ressources du serveur", explique comment créer et gérer des limites d'utilisation des ressources avec Adaptive Server.
- Le chapitre 7, "Configuration des jeux de caractères, des ordres de tri et des langues", traite des questions de localisation, comme les fichiers fournis dans les modules de langue et la configuration de la langue, l'ordre de tri et le jeu de caractères d'Adaptive Server.
- Le chapitre 8, "Configuration des conversions de jeux de caractères entre clients et serveur", présente la conversion de jeux de caractères entre Adaptive Server et les clients en environnement hétérogène.
- Le chapitre 9, "Administration de la sécurité", contient une présentation générale des fonctions de sécurité disponibles dans Adaptive Server.
- Le chapitre 10, "Gestion des connexions et des utilisateurs de bases de données Adaptive Server", décrit les méthodes de gestion des connexions à Adaptive Server et des utilisateurs de bases de données.
- Le chapitre 11, "Gestion des autorisations utilisateur", décrit l'utilisation et la mise en oeuvre des autorisations utilisateur.
- Le chapitre 12, "Audit", décrit comment définir l'audit de votre installation.
- Le chapitre 13, "Gestion des serveurs distants", décrit les différentes opérations devant être exécutées par l'administrateur système et le responsable de la sécurité du système de chaque Adaptive Server pour permettre les appels RPC.
- Le chapitre 14, "Utilisation de Kerberos, DCE et Windows NT LAN Manager", décrit les services de sécurité basés sur le réseau vous permettant d'authentifier les utilisateurs et de protéger les données transmises d'une machine à l'autre sur un réseau.
- Le chapitre 15, "Présentation des sujets relatifs aux ressources disque", contient une présentation des sujets relatifs aux ressources disque d'Adaptive Server.
- Le chapitre 16, "Initialisation des devices de base de données", décrit le mode d'initialisation et d'utilisation des devices de base de données.

- Le chapitre 17, "Mise en miroir des devices de base de données", décrit la mise en miroir des devices de base de données pour une reprise instantanée suite à des pannes de disque.
- Le chapitre 18, "Configuration de la mémoire", explique comment configurer Adaptive Server pour une utilisation de la mémoire disponible sur votre système.
- Le chapitre 19, "Configuration des caches de données", décrit comment créer des caches nommés en mémoire et comment lier des objets à ces caches.
- Le chapitre 20, "Gestion des serveurs multiprocesseur", explique comment utiliser plusieurs processeurs CPU avec Adaptive Server et traite des questions liées à l'administration du système et qui sont caractéristiques des environnements SMP.
- Le chapitre 21, "Création et gestion des bases de données utilisateur", traite de l'emplacement physique des bases de données, des tables et des index ainsi que de l'espace qui leur est alloué.
- Le chapitre 22, "Définition des options de base de données", décrit le mode de configuration des options de base de données.
- Le chapitre 23, "Création et utilisation de segments", traite de l'utilisation des segments (ensembles nommés de devices) dans les bases de données.
- Le chapitre 24, "Utilisation de la commande reorg", décrit le mode d'utilisation de la commande reorg.
- Le chapitre 25, "Contrôle de la cohérence des bases de données", décrit l'utilitaire de vérification de la cohérence des bases de données, dbcc, qui permet de détecter et de résoudre les incidents sur les bases de données.
- Le chapitre 26, "Elaboration d'un plan de sauvegarde et de reprise", traite des fonctionnalités du Backup Server et explique comment mettre au point votre stratégie de sauvegarde.
- Le chapitre 27, "Sauvegarde et restauration de bases de données utilisateur", présente la restauration des bases de données utilisateur.
- Le chapitre 28, "Restauration des bases de données système", présente la restauration des bases de données système.
- Le chapitre 29, "Gestion de l'espace libre avec des seuils", explique comment gérer l'espace en utilisant des seuils.

**Documentations**

La documentation Sybase Adaptive Server Enterprise comprend les manuels suivants :

- Les Notes de mise à jour pour votre plate-forme contiennent les informations de dernière minute qui ne figurent pas dans les manuels. Une version plus récente des Notes de mise à jour est disponible sur le Web. Pour rechercher des informations ultérieures à la commercialisation du CD-ROM du produit, consultez le site Sybase Technical Library.
- Le *Guide d'installation* d'Adaptive Server pour votre plate-forme décrit les procédures d'installation, de mise à niveau et de configuration pour tous les produits Adaptive Server et Sybase associés.
- Le *Manuel de configuration d'Adaptive Server Enterprise* pour votre plate-forme fournit des instructions sur les tâches de configuration particulières pour Adaptive Server.
- *Adaptive Server Enterprise - Nouvelles fonctionnalités* décrit les nouvelles fonctionnalités de la version 12.5 d'Adaptive Server, les modifications apportées au système pour leur prise en charge et les modifications susceptibles d'avoir des conséquences sur vos applications existantes.
- Le *Guide de l'utilisateur Transact-SQL* présente Transact-SQL, version enrichie du langage de base de données relationnelle de Sybase. Ce manuel sert de référence pour les utilisateurs qui découvrent le système de gestion de bases de données. Il décrit également les bases de données exemple pubs2 et pubs3.
- Le *Guide d'administration système* fournit des informations détaillées sur l'administration des serveurs et des bases de données. Ce manuel contient des instructions relatives à la gestion des ressources physiques, de la sécurité et des bases de données système et utilisateur, ainsi qu'au paramétrage de la conversion de caractères, la langue et l'ordre de tri.
- Le *Manuel de référence* contient des informations détaillées sur toutes les commandes, fonctions, procédures et types de données Transact-SQL. Ce manuel fournit également la liste des mots réservés Transact-SQL et les définitions des tables système.
- Le document *Performances et optimisation* explique comment optimiser les performances d'Adaptive Server. Il contient des informations sur les aspects de la conception des bases de données qui conditionnent les performances, sur l'optimisation des requêtes, sur le paramétrage d'Adaptive Server pour des bases de données volumineuses, sur la configuration des caches et des disques et sur l'impact du verrouillage et des curseurs sur les performances.

- Le manuel *Utilitaires* décrit les utilitaires d'Adaptive Server tels qu'isql et bcp, qui sont exécutés au niveau du système d'exploitation.
- Le *Guide de référence rapide* est un petit fascicule qui répertorie les noms et syntaxes des commandes, fonctions, procédures système, procédures système étendues, types de données et utilitaires-. Il est uniquement disponible sur papier.
- Le *Diagramme des tables système* est un poster qui illustre les tables système selon le modèle entités-relations. Il est uniquement disponible sur papier.
- Les documents *Error Messages et Troubleshooting Guide* expliquent comment résoudre les conditions d'erreur les plus courantes et donnent les solutions aux problèmes système souvent rencontrés par les utilisateurs.
- Le *Guide de l'utilisateur de Component Integration Services* explique comment utiliser la fonctionnalité Component Integration Services d'Adaptive Server pour se connecter à des bases de données distantes Sybase et non Sybase.
- Le document *Java dans Adaptive Server Enterprise* explique comment installer et utiliser les classes Java en tant que types de données, fonctions et procédures stockées dans la base de données Adaptive Server.
- Le document *Utilisation de Sybase Failover en environnement haute disponibilité* traite de l'utilisation de Sybase Failover pour configurer Adaptive Server comme serveur compagnon dans un environnement haute disponibilité.
- Le document *Utilisation des fonctionnalités DTM* traite de la configuration et de l'utilisation des fonctionnalités DTM d'Adaptive Server ainsi que de la résolution des éventuels problèmes dans les environnements de traitement des transactions distribuées.
- Le *Guide de l'utilisateur d'EJB Server* explique comment utiliser EJB Server pour déployer et exécuter Enterprise JavaBeans dans Adaptive Server.
- Le document *XA Interface Integration Guide for CICS, Encina, and TUXEDO* fournit des instructions sur l'utilisation de l'interface DTM XA de Sybase avec les gestionnaires de transactions X/Open XA.
- Le *Glossaire* définit les termes techniques utilisés dans la documentation Adaptive Server.

- Le document *Sybase jConnect for JDBC Programmer's Reference* décrit le produit jConnect for JDBC et explique comment l'utiliser pour accéder aux données stockées dans des systèmes de gestion de bases de données relationnelles.
- Le document *Full-Text Search Specialty Data Store - Guide de l'utilisateur* explique comment utiliser la fonction Full-Text Search avec Verity afin d'effectuer des recherches dans les données d'Adaptive Server Enterprise.
- Le *Guide de l'utilisateur de Monitor Historical Server* explique comment utiliser Historical Server afin d'obtenir des statistiques de performances de SQL Server et Adaptive Server.
- Le *Guide de l'utilisateur de Monitor Server* explique comment utiliser Monitor Server afin d'obtenir des statistiques de performances de SQL Server et Adaptive Server.
- Le document *Monitor Client Library Programmer's Guide* explique comment écrire des applications Monitor Client Library accédant aux données de performances d'Adaptive Server.

**Autres sources d'information**

Utilisez le CD Sybase Technical Library ainsi que le site Web Technical Library Product Manuals pour obtenir davantage d'informations sur les produits :

- Le CD-ROM Technical Library, qui contient des manuels sur les produits et des documents techniques, est livré avec le logiciel. L'explorateur DynaText (téléchargeable à partir du site Product Manuals (http://www.sybase.com/detail/1,3693,1010661,00.html) vous permet d'accéder aux informations techniques sur les produits dans un format facile à utiliser.

  Pour plus d'informations sur l'installation et le démarrage de la Technical Library, reportez-vous au *Technical Library Installation Guide*.
- Le site Web Technical Library Product Manuals est une version HTML du CD Technical Library, à laquelle vous pouvez accéder à l'aide d'un navigateur Web standard. Outre les manuels sur les produits, vous trouverez également des liens vers le site Web Technical Documents (anciennement Tech Info Library), la page Solved Cases et des forums Sybase/Powersoft.

  Pour accéder à Technical Library Product Manuals, rendez-vous sur le site Product Manuals (http://www.sybase.com/support/manuals/).

**Certifications Sybase sur le Web**

La documentation technique disponible sur le site Web de Sybase est fréquemment mise à jour.

❖ **Pour accéder aux informations les plus récentes sur les certifications de produit :**

1 Cliquez sur Technical Documents (http://www.sybase.com/support/techdocs/).

2 Sélectionnez des produits dans la barre de navigation située à gauche.

3 Sélectionnez un nom de produit dans la liste des produits.

4 Sélectionnez le filtre Certification Report, choisissez une période de temps dans la liste Time Frame, puis cliquez sur Go.

5 Cliquez sur le titre du rapport de certification que vous voulez consulter.

❖ **Pour accéder aux informations les plus récentes sur les recueils de correctifs de bugs et les mises à jour**

1 Cliquez sur Technical Documents (http://www.sybase.com/support/techdocs/).

2 Sélectionnez EBFs/Updates. Saisissez vos nom d'utilisateur et mot de passe si vous y êtes invité (pour les comptes Web existants) ou créez un compte (service gratuit).

3 Sélectionnez une période de temps dans la liste Time Frame, puis cliquez sur Go.

4 Sélectionnez un produit.

5 Cliquez sur l'EBF ou la mise à jour souhaité.

❖ **Pour créer une vue personnalisée du site Web de Sybase (y compris des pages de support technique)**

Créez un profil MySybase. MySybase est un service gratuit qui vous permet de créer une vue personnalisée des pages Web de Sybase.

1 Cliquez sur Technical Documents (http://www.sybase.com/support/techdocs/).

2 Cliquez sur MySybase, puis créez un profil MySybase.

# Conventions

Les conventions typographiques utilisées dans ce manuel sont les suivantes :

## Format des instructions SQL

SQL est un langage à structure non imposée. Il n'existe aucune règle quant au nombre de mots qui peuvent être placés sur une ligne ou quant à l'emplacement des fins de ligne. Cependant, pour une meilleure lisibilité, toutes les instructions et tous les exemples de ce manuel sont présentés de telle sorte que chaque clause d'une instruction commence sur une nouvelle ligne. Les clauses composées de plusieurs parties s'étendent sur les lignes suivantes, qui apparaissent alors en retrait.

## Conventions syntaxiques pour les instructions SQL

Le tableau 1 répertorie les conventions syntaxiques utilisées pour les instructions dans le présent manuel :

***Tableau 1 : Conventions syntaxiques des instructions***

| Clé | Définition |
|---|---|
| `commande` | Les noms de commande, d'option de commande, d'utilitaire, de drapeau d'utilitaire et autres mots-clés apparaissent en<br>`Courier gras`<br>dans la syntaxe des instructions et en Helvetica gras dans le corps du texte. |
| *`variable`* | Les variables (termes se substituant aux valeurs à insérer) apparaissent en italiques. |
| `{ }` | Les accolades indiquent que vous devez choisir au moins une des options énumérées. N'insérez pas les accolades dans l'option. |
| `[ ]` | Les crochets indiquent que les options citées sont facultatives. N'incluez pas les crochets à votre option. |
| `( )` | Les parenthèses font partie intégrante de la commande. |
| `\|` | La barre verticale indique que vous ne pouvez choisir qu'une seule des options énumérées. |
| `,` | La virgule vous permet de choisir autant d'options que vous le souhaitez, à condition de les séparer par une virgule dans la commande. |

- Les instructions syntaxiques (qui affichent la syntaxe et les options d'une commande) apparaissent comme suit :

  ```
  sp_dropdevice [nom_device]
  ```

  ou, pour une commande comportant plusieurs options :

  ```
  select nom_colonne
      from nom_table
      where conditions_de_recherche
  ```

  Dans les instructions à syntaxe, les mots-clés (commandes) sont dans une police normale et les identificateurs sont en minuscules : police normale pour les mots-clés, italique pour les mots tapés par l'utilisateur.

- Les exemples de commandes Transact-SQL sont présentés comme suit :

  ```
  select * from publishers
  ```

- Les exemples de résultats apparaissent de la façon suivante :

```
pub_id  pub_name                city        state
------- ------------------      ----------- -----
0736    New Age Books           Boston      MA
0877    Binnet & Hardley        Washington  DC
1389    Algodata Infosystems    Berkeley    CA

(3 rows affected)
```

## Casse

Vous pouvez ignorer la casse lorsque vous tapez des mots-clés :

SELECT est identique à Select et à select.

## Options obligatoires {vous devez en choisir au moins une}

- *Accolades et barres verticales :* choisissez *une seule* option.

```
{mourir_debout | vivre_à_genoux | vivre_debout}
```

- *Accolades et virgules :* choisissez *une ou plusieurs* options. Dans le second cas, séparez-les par des virgules.

  ```
  {comptant, chèque, carte}
  ```

## Options facultatives

- *Un seul élément entre crochets :* Pas de sélection nécessaire.

  ```
  [anchovies]
  ```

- *Crochets et barres verticales :* Choisissez *aucune ou une seule* option.

  ```
  [beans | rice | sweet_potatoes]
  ```

- *Crochets et virgules :* Choisissez *aucune, une ou plusieurs* options. Si vous choisissez plusieurs options, séparez-les par des virgules.

  ```
  [extra_cheese, avocados, sour_cream]
  ```

## Ellipse

Une ellipse (. . .) signifie que vous pouvez *répéter* le dernier élément autant de fois que nécessaire. Dans cette instruction de syntaxe, buy représente un mot-clé requis :

```
buy thing = price [cash | check | credit]
    [, thing = price [cash | check | credit]]...
```

Vous devez acheter au moins un article et indiquer son prix. Vous pouvez choisir un mode de paiement parmi les éléments entre crochets. Vous pouvez également choisir d'acheter d'autres articles dans la quantité de votre choix. Pour chaque article acheté, indiquez son nom, son prix et un mode de paiement (facultatif).

Une ellipse peut également être utilisée dans une ligne pour désigner des portions d'une commande issues d'un exemple de texte. L'instruction de syntaxe ci-dessous représente la commande create database complète, même s'il manque des mots-clés requis, ainsi que d'autres options :

```
create database...for load
```

## Expressions

Plusieurs types d'**expressions** sont utilisés dans les instructions de syntaxe Adaptive Server.

***Tableau 2 : Types d'expressions utilisées dans les instructions syntaxiques***

| Utilisation | Définition |
|---|---|
| *expression* | Peut inclure des constantes, des littéraux, des fonctions, des identificateurs de colonne, des variables ou des paramètres. |
| *expression_logique* | Expression renvoyant TRUE, FALSE ou UNKNOWN |

| Utilisation | Définition |
|---|---|
| *expression_constante* | Expression renvoyant toujours la même valeur, telle que "5+3" ou "ABCDE". |
| *expression_virg_flot* | Toute expression en virgule flottante ou expression convertie implicitement en un nombre en virgule flottante. |
| *expression_entier* | Toute expression entière ou se convertissant de façon implicite en une valeur entière |
| *expression_numérique* | Toute expression numérique renvoyant une valeur unique. |
| *expression_car* | Expression renvoyant une valeur unique de type caractère. |
| *expression_binaire* | Toute expression renvoyant une valeur unique de type binary ou varbinary |

**Si vous avez besoin d'aide**

Pour chaque installation Sybase faisant l'objet d'un contrat de support, une ou plusieurs personnes désignées sont autorisées à contacter le Support Technique de Sybase. Si vous avez des questions ou besoin d'aide pendant l'installation, demandez à la personne désignée de contacter le Support Technique de Sybase ou la filiale Sybase la plus proche.

CHAPITRE 1

# Présentation de l'administration du système

Ce chapitre présente les principales rubriques de l'administration système d'Adaptive Server. Il aborde les sujets suivants :



## Adaptive Server tâches d'administration

L'administration d'Adaptive Server comprend les tâches suivantes :

- Installation d'Adaptive Server et de Backup Server
- Création et gestion des comptes login Adaptive Server
- Octroi des rôles et autorisations aux utilisateurs d'Adaptive Server
- Gestion et contrôle de l'utilisation de l'espace disque, de la mémoire et des connexions
- Sauvegarde et restauration de bases de données
- Diagnostic des problèmes système
- Configuration d'Adaptive Server pour optimiser les performances

Par ailleurs, les administrateurs système peuvent également assurer certaines tâches de conception de base de données, comme l'application des normes de cohérence. Il peut arriver que cette fonction empiète en partie sur le travail des concepteurs d'applications.

Bien que l'administrateur système se concentre sur des tâches indépendantes des applications exécutées sur Adaptive Server, il ou elle est néanmoins la personne qui possède la meilleure vue d'ensemble de toutes les applications. De ce fait, il est en mesure d'indiquer aux concepteurs d'applications les données qui existent déjà sur Adaptive Server, de formuler des recommandations concernant la normalisation des données sur l'ensemble des applications, etc.

Toutefois, il n'est pas toujours aisé de faire la distinction entre ce qui est spécifique d'une application. Les propriétaires de bases de données utilisateur seront ainsi amenés à consulter certaines sections du présent ouvrage. De même, les administrateurs système et les propriétaires de bases de données se reporteront au *Guide de l'utilisateur Transact-SQL* (plus particulièrement aux chapitres sur la définition de données, les procédures stockées et les triggers). Pour leur part, les administrateurs système et concepteurs d'applications pourront consulter le manuel *Performances et optimisation*.

## Rôles requis pour les tâches d'administration système

Nombre de commandes et procédures abordées dans ce manuel ne peuvent être exécutées qu'avec le rôle SA ou SSO. D'autres sections de ce manuel concernent également les propriétaires de bases de données. Dans une base de données, le nom d'utilisateur du propriétaire de la base est "dbo". Celui-ci ne peut toutefois pas se connecter en tant que "dbo" : en effet, un propriétaire se connecte sous son nom de login Adaptive Server et il n'est reconnu "dbo" par Adaptive Server que lorsqu'il utilise la base de données.

Un certain nombre de tâches opérationnelles, administratives et liées à la sécurité sont regroupées dans les rôles système suivants :

- L'**administrateur système**, dont les tâches comprennent :
  - la gestion de la mémoire à disques,
  - le contrôle de la procédure de reprise automatique d'Adaptive Server,
  - l'optimisation de l'exploitation d'Adaptive Server via la modification des paramètres système configurables,
  - le diagnostic et la génération d'états sur les problèmes système,
  - la sauvegarde et le chargement des bases de données,
  - l'octroi et la révocation du rôle d'administrateur système,

  - la modification et la suppression des logins du serveur,
  - l'octroi des autorisations aux utilisateurs d'Adaptive Server,
  - la création de bases de données utilisateur et l'octroi de leur appartenance,
  - la définition de groupes pouvant être utilisés pour l'octroi et la révocation des autorisations.
- Le **responsable de la sécurité du système**, qui exécute des tâches liées à la sécurité telles que :
  - la création des logins du serveur, y compris l'attribution des mots de passe initiaux,
  - la modification du mot de passe des comptes,
  - l'octroi et la révocation des rôles d'opérateur et de responsable de la sécurité du système,
  - la création, l'octroi et la révocation des rôles définis par l'utilisateur,
  - l'octroi de la fonctionnalité d'emprunter l'identité d'un autre utilisateur sur le serveur,
  - la définition du délai d'expiration du mot de passe,
  - la configuration d'Adaptive Server pour une utilisation des services de sécurité basés sur le serveur,
  - la gestion du système d'audit.
- L'**opérateur**, qui est un utilisateur ayant la capacité de sauvegarder et de charger les bases de données à l'échelle du serveur. Le rôle d'opérateur permet à un seul utilisateur d'utiliser les commandes dump database, dump transaction, load database et load transaction pour sauvegarder et restaurer l'ensemble des bases de données sur un serveur sans pour autant être le propriétaire de chacune de ces bases de données. Ces opérations peuvent être exécutées dans une base de données unique par le propriétaire de la base de données ou par l'administrateur système.

Ces rôles renforcent la responsabilisation des utilisateurs qui exécutent des tâches opérationnelles et administratives. Vous pouvez ainsi contrôler leurs activités et remonter si nécessaire jusqu'à l'auteur de telle ou telle tâche. Un administrateur système opère en dehors du système de protection des contrôles d'accès discrétionnaires (DAC), c'est-à-dire lorsqu'un administrateur système accède à des objets et qu'Adaptive Server ne vérifie pas les autorisations DAC.

De plus, deux catégories de propriétaires d'objets jouissent d'un statut spécial à cause des objets qu'ils possèdent. Ces types d'appartenance sont les suivants :

- Propriétaire des objets de la base de données
- Propriétaire de la base de données

## Propriétaire de la base de données

Le **propriétaire de la base de données** est le créateur d'une base de données ou bien la personne vers laquelle l'appartenance de la base de données a été transférée. Un administrateur système octroie aux utilisateurs le droit de créer des bases de données à l'aide de la commande grant.

Le propriétaire de la base de données se connecte à Adaptive Server à l'aide du nom et du mot de passe qui lui ont été attribués. Dans d'autres bases de données, ce propriétaire est identifié par son nom d'utilisateur usuel. Dans la base de données, Adaptive Server reconnaît l'utilisateur comme détenant le compte "dbo".

Un propriétaire de la base de données peut :

- exécuter la procédure système sp_adduser pour permettre à d'autres utilisateurs d'Adaptive Server d'accéder à la base de données ;
- utiliser la commande grant pour octroyer à d'autres utilisateurs l'autorisation de créer des objets et d'exécuter des commandes à l'intérieur de la base de données.

Pour plus d'informations sur l'ajout d'utilisateurs à une base de données, reportez-vous au chapitre 10, "Gestion des connexions et des utilisateurs de bases de données Adaptive Server". Pour plus d'informations sur l'octroi d'autorisations à des utilisateurs, reportez-vous au chapitre 11, "Gestion des autorisations utilisateur".

Le propriétaire de la base de données ne dispose pas automatiquement des autorisations liées aux objets détenus par d'autres utilisateurs. Toutefois, un propriétaire de bases de données peut disposer temporairement et à tout moment des autorisations détenues par d'autres utilisateurs dans la base de données, en utilisant la commande setuser. Grâce à une utilisation combinée des commandes setuser et grant, le propriétaire de la base de données peut acquérir les autorisations pour n'importe quel objet de la base de données.

---

**Remarque** Etant donné le rôle extrêmement puissant du propriétaire de la base de données, l'administrateur système doit décider avec le plus grand soin qui sera le propriétaire des bases de données sur le serveur. Le responsable de la sécurité du système doit envisager l'audit de l'activité liée aux bases de données exercée par l'ensemble des propriétaires de bases de données.

---

## Propriétaire des objets de la base de données

Le **propriétaire des objets de la base de données** est un utilisateur qui crée un objet d'une base de données. Les **objets** d'une base de données sont des tables, des index, des vues, des valeurs par défaut, des triggers, des règles, des contraintes et des procédures. La création d'un objet de la base de données par un utilisateur est soumise à l'octroi d'une autorisation par le propriétaire de la base de données, pour la création d'objets de type particulier. Aucun nom de login ou mot de passe particulier n'est requis pour un propriétaire d'objets de la base de données.

Pour créer un objet, le propriétaire d'un objet de la base de données utilise l'instruction appropriée create, puis octroie l'autorisation aux autres utilisateurs.

Le créateur d'un objet de la base de données dispose automatiquement de toutes les autorisations requises pour cet objet. L'administrateur système dispose également de toutes les autorisations requises pour l'objet en question. Le propriétaire d'un objet doit explicitement octroyer les autorisations aux autres utilisateurs pour que ces derniers puissent accéder à l'objet. Même le propriétaire de la base de données ne peut pas utiliser un objet directement, sauf dans le cas où il s'est vu octroyer les autorisations correspondantes par le propriétaire de l'objet. Toutefois, le propriétaire de la base de données peut toujours utiliser la commande setuser pour emprunter l'identité de n'importe quel autre utilisateur dans la base de données, y compris celle du propriétaire de l'objet.

**Remarque** Lorsqu'un objet d'une base de données appartient à une autre personne que le propriétaire de la base de données, l'utilisateur (y compris l'administrateur système) doit qualifier le nom de cet objet avec le nom du propriétaire de l'objet – *nom_propriétaire.nom_objet* – pour accéder à l'objet. Si de nombreux utilisateurs doivent accéder à un objet ou à une procédure, en particulier dans le cas d'une requête ad hoc, le fait que ces objets appartiennent au "dbo" simplifie énormément l'accès.

## Utilisation d'*isql* pour l'exécution de tâches d'administration système

Les tâches d'administration système décrites dans ce manuel impliquent que vous recouriez à l'utilitaire de ligne de commande isql. Cette section fournit quelques informations élémentaires sur l'utilisation d'isql. Pour plus d'informations sur isql, reportez-vous au document *Guide Utilitaires*.

Vous pouvez également faire appel à l'utilitaire graphique Sybase Central™ pour exécuter la plupart des tâches décrites dans ce manuel, comme expliqué dans "Utilisation de Sybase Central pour les tâches d'administration système", page 8.

### Lancement d'*isql*

Sur la plupart des plates-formes, pour lancer isql, entrez la commande suivante à l'invite du système d'exploitation :

```
isql -Uusername
```

où *nom_utilisateur* indique le nom d'utilisateur de l'administrateur système. Adaptive Server vous demande votre mot de passe.

**Remarque** N'utilisez pas l'option -P d'isql pour spécifier votre mot de passe car celui-ci serait alors visible par les autres utilisateurs.

Vous pouvez utiliser isql en mode ligne de commande pour entrer la plupart des exemples Transact-SQL qui apparaissent dans ce manuel.

## Saisie des instructions

Les instructions que vous entrez dans isql peuvent s'étendre sur plusieurs lignes. isql ne procède pas à leur exécution tant que vous n'avez pas entré "go" sur une ligne distincte. Exemple :

```
1> select *
2> from sysobjects
3> where type = "TR"
4> go
```

Les exemples de ce manuel n'incluent pas de commande go entre les instructions. Cependant si vous utilisez ces commandes, vous devez entrer la commande go pour qu'elles s'exécutent.

## Sauvegarde et réutilisation d'instructions

Dans ce manuel, il est fréquemment suggéré de sauvegarder les requêtes Transact-SQL utilisées pour créer ou modifier des bases de données utilisateur et des objets de base de données. Pour ce faire, la méthode la plus simple consiste à créer ou copier les instructions dans un fichier au format ASCII. Par la suite, vous pouvez fournir des instructions à isql à partir de ce fichier, par exemple pour recréer des bases de données ou des objets de base de données.

Pour utiliser isql avec un fichier au format ASCII, la syntaxe est la suivante :

```
isql -Uusername -ifilename
```

où *nom_fichier* est le chemin d'accès complet du fichier contenant les requêtes Transact-SQL. Sous UNIX et d'autres plates-formes, vous pouvez utiliser le symbole inférieur à (<) pour rediriger le fichier.

Les requêtes Transact-SQL contenues dans le fichier ASCII doivent utiliser une syntaxe correcte, ainsi que la commande go.

## Utilisation de Sybase Central pour les tâches d'administration système

Vous pouvez exécuter la plupart des tâches d'administration système décrites dans ce manuel à l'aide de Sybase Central, utilitaire graphique fourni avec Adaptive Server.

Vous pouvez notamment exécuter les tâches suivantes avec Sybase Central :

- initialisation des devices de base de données (serveurs Windows NT uniquement),
- définition des paramètres de configuration,
- visualisation de l'espace de journalisation disponible dans une base de données,
- génération d'un langage de définition de données (DDL),
- création de logins,
- ajout de serveurs distants,
- création de bases de données,
- création de procédures stockées,
- définition de rôles,
- ajout de caches de données,
- définition d'options de base de données,
- sauvegarde et restauration de bases de données.

Vous pouvez également utiliser la fonction Monitor Viewer de Sybase Central pour accéder à Adaptive Server Monitor™. Une aide en ligne étendue est également disponible dans Sybase Central.

Vous pouvez utiliser la fonction de génération de DDL pour enregistrer votre travail dans des scripts Transact-SQL. Cette fonction vous permet de sauvegarder dans un script les actions que vous avez exécutées sur l'ensemble d'un serveur ou dans une base de données spécifique.

# Tables système

La base de données master contient des **tables système** qui gardent trace des informations concernant Adaptive Server dans son ensemble. En outre, toute base de données (y compris la base de données master) contient d'autres tables système qui, elles, gardent trace des informations propres à cette base de données.

Dans la base de données master (base contrôlant Adaptive Server), toutes les tables fournies par Adaptive Server sont considérées comme des tables système. De plus, chaque base de données utilisateur est créée avec un sous-groupe de ces tables système. Les tables système sont également appelées **dictionnaires de données** ou catalogues système.

Une base de données master et ses tables sont créées à l'installation d'Adaptive Server. Dans une base de données utilisateur, les tables système sont automatiquement créées lorsque la commande create database est émise. Tous les noms de tables système commencent par "sys". Vous ne pouvez pas créer de tables dans des bases de données utilisateur portant les mêmes noms que des tables système. Le document *Manuel de référence d'Adaptive Server* fournit une explication des tables système et de leurs colonnes.

## Interrogation des tables système

Vous pouvez interroger les tables système de la même manière que les autres tables. Par exemple, l'instruction suivante renvoie le nom de tous les triggers de la base de données :

```
select name
from sysobjects
where type = "TR"
```

En outre, Adaptive Server fournit des **procédures stockées** (appelées **procédures système**), dont bon nombre d'entre-elles constituent un raccourci pour l'interrogation des tables système.

Les procédures système suivantes donnent des informations sur les tables système :

| | |
|---|---|
| • sp_commonkey | • sp_helpremotelogin |
| • sp_configure | • sp_help_resource_limit |
| • sp_countmedatada | • sp_helprotect |
| • sp_dboption | • sp_helpsegment |

| | |
|---|---|
| • sp_estspace | • sp_helpserver |
| • sp_help | • sp_helpsort |
| • sp_helpartition | • sp_helptext |
| • sp_helpcache | • sp_helpthreshold |
| • sp_helpconfig | • sp_helpuser |
| • sp_helpconstraint | • sp_lock |
| • sp_helpdb | • sp_monitor |
| • sp_helpdevice | • sp_monitorconfig |
| • sp_helpgroup | • sp_procqmode |
| • sp_helpindex | • sp_showcontrolinfo |
| • sp_helpjava | • sp_showexeclass |
| • sp_helpjoins | • sp_showplan |
| • sp_helpkey | • sp_spaceused |
| • sp_helplanguage | • sp_who |
| • sp_helplog | • sp_help_resource_limit |

Pour obtenir des informations plus complètes sur les procédures système, reportez-vous au *Manuel de référence d'Adaptive Server*.

## Clés des tables système

Les clés primaires, étrangères et communes des tables système sont définies dans les bases de données master et model. Pour obtenir un rapport sur les clés définies, exécutez sp_helpkey. Pour un rapport sur les colonnes de deux tables système qui peuvent potentiellement être jointes, exécutez sp_helpjoins.

Le *Diagramme des tables système d'Adaptive Server* livré avec Adaptive Server illustre les relations entre les colonnes dans les tables système.

## Mise à jour des tables système

Les tables système Adaptive Server contiennent des informations essentielles au bon fonctionnement des bases de données. En temps normal, vous n'avez pas besoin de modifier directement les données des tables système.

Mettez à jour les tables système uniquement sur instruction du Support Technique de Sybase ou suite à la lecture du manuel *Guide de dépannage* ou du présent manuel.

Pour modifier des tables système, vous devez d'abord exécuter la commande sp_configure afin d'autoriser les mises à jour sur les tables système. Ensuite, tout utilisateur ayant l'autorisation nécessaire peut modifier une table système. De plus, pour toute modification directe des tables système, suivez ces directives :

- Modifiez les tables système uniquement à l'intérieur d'une transaction. Exécutez une commande begin transaction avant la commande de modification des données.
- Vérifiez que seules les lignes voulues ont été altérées par la commande et que les données ont été correctement modifiées.
- Si tel n'est pas le cas, exécutez une commande rollback transaction. Si la modification est correcte, exécutez une commande commit transaction.

**Avertissement !** Certaines tables système ne doivent être modifiées par aucun utilisateur. En effet, certaines tables système sont constituées dynamiquement par des traitements système, contiennent des informations codées ou n'affichent qu'une partie de leurs données à l'interrogation. Des mises à jour imprudentes sur certaines tables système peuvent bloquer l'exécution d'Adaptive Server, rendre inaccessibles certains objets de base de données, intervertir les autorisations sur les objets ou encore mettre fin à une session utilisateur.
Par ailleurs, vous ne devez jamais tenter de modifier la définition des tables système d'aucune manière, pour inclure des contraintes, par exemple. Les triggers, les valeurs par défaut et les règles ne sont pas autorisés dans les tables système. Si vous tentez de créer un trigger ou de lier une règle ou une valeur par défaut à une table système, vous verrez apparaître un message d'erreur.

# Procédures système

Le nom de toutes les procédures système commence par "sp_". Elles sont stockées dans la base de données sybsystemprocs mais vous pouvez exécuter nombre d'entre elles dans n'importe quelle base de données en émettant la procédure stockée à partir de la base de données ou en qualifiant le nom de la procédure avec celui de la base de données.

Si vous exécutez une procédure système dans une base de données autre que sybsystemprocs, elle agit sur les tables système de la base de données depuis laquelle elle est exécutée. Par exemple, si le propriétaire de la base de données pubs2 exécute sp_adduser à partir de pubs2 ou exécute la commande pubs2..sp_adduser, le nouvel utilisateur est ajouté à pubs2..sysusers. Toutefois, cela ne s'applique pas aux procédures système qui ne mettent à jour que des tables dans la base de données master.

Les autorisations sur les procédures système sont abordées dans le *Manuel de référence d'Adaptive Server*.

## Utilisation des procédures système

Un **paramètre** est un argument transmis à une procédure stockée ou à une procédure système. Si une valeur de paramètre d'une procédure système contient des mots réservés, des signes de ponctuation ou des espaces imbriqués, elle doit être placée entre guillemets ou apostrophes. Si le paramètre est un nom d'objet qualifié d'un nom de base de données ou de propriétaire, le nom entier doit figurer entre guillemets ou apostrophes.

Les procédures système peuvent être exécutées dans des sessions qui utilisent les transactions en mode chaîné ou non chaîné. Toutefois, les procédures système qui modifient les données dans les tables système de la base de données master ne peuvent pas être exécutées dans une transaction, puisqu'une telle opération pourrait compromettre la reprise. De même, les procédures système qui créent des tables de travail temporaires ne peuvent pas être exécutées dans des transactions.

Si aucune transaction n'est active lorsque vous exécutez une procédure système, Adaptive Server désactive le mode chaîné et définit transaction isolation level 1 pour toute la durée de la procédure. Avant de rendre la main, il rétablit le mode et le niveau d'isolement à leur état initial. Pour plus d'informations sur les modes de transaction et les niveaux d'isolement, reportez-vous au *Manuel de référence d'Adaptive Server*.

Toutes les procédures système renvoient un état. Exemple :

```
return status = 0
```

indique que la procédure a abouti.

## Tables de procédures système

Les procédures système utilisent plusieurs *tables de procédures système* dans les bases de données master et sybsystemdb pour convertir les valeurs système internes (par exemple, les bits d'état) en un format compréhensible par l'utilisateur. L'une d'elles, spt_values, est utilisée par plusieurs procédures système :

| | |
|---|---|
| • sp_configure | • sp_helpdevice |
| • sp_dboption | • sp_helpindex |
| • sp_depends | • sp_helpkey |
| • sp_help | • sp_helprotect |
| • sp_helpdb | • sp_lock |

La mise à jour de la table spt_values ne peut se faire que lors d'une mise à niveau ; cette table ne peut pas être modifiée autrement. Pour savoir de quelle manière l'utiliser, exécutez sp_helptext et consultez le texte de l'une des procédures système qui la référence.

Les autres tables de procédures système sont spt_monitor et spt_committab, ainsi que les tables requises par les procédures du catalogue. La table spt_committab se trouve dans la base de données sybsystemdb.

Par ailleurs, plusieurs procédures système créent des tables temporaires, puis les suppriment après utilisation. Par exemple, sp_helpdb crée #spdbdesc, sp_helpdevice crée #spdevtab et sp_helpindex crée #spindtab.

## Création de procédures système

Un grand nombre de procédures système sont expliquées dans ce manuel, dans les sections auxquelles elles se rapportent. Pour obtenir des informations détaillées sur les procédures système, reportez-vous au *Manuel de référence d'Adaptive Server*.

Les administrateurs système peuvent écrire des procédures système, qui sont ensuite exécutables dans n'importe quelle base de données. Il suffit de créer une procédure stockée dans sybsystemprocs et de lui donner un nom commençant par "sp_". L'uid de la procédure stockée doit être 1, celui du propriétaire de la base de données.

La plupart des procédures système que vous créez interrogent les tables système. Vous pouvez également créer des procédures stockées qui modifient les tables système, mais cela n'est pas conseillé.

Pour créer une procédure stockée qui modifie les tables système, un SSO doit d'abord activer le paramètre de configuration allow updates to system tables. Toute procédure stockée créée pendant que ce paramètre est activé pourra *toujours* mettre à jour les tables système, même une fois allow updates to system tables désactivé. Pour créer une procédure stockée qui mette à jour les tables système, procédez comme suit :

1 Activez allow updates to system tables à l'aide de sp_configure.

2 Créez la procédure stockée à l'aide de la commande create procedure.

3 Désactivez allow updates to system tables à l'aide de sp_configure.

**Avertissement !** Soyez extrêmement prudent lorsque vous modifiez des tables système. Pour tester les procédures qui modifient les tables système, utilisez toujours des bases de données de développement ou de test, et non des bases de données de production.

# Procédures stockées étendues système

Une procédure stockée étendue (ESP) permet d'appeler des fonctions de langage externes depuis Adaptive Server. Adaptive Server contient un ensemble d'ESP, mais les utilisateurs peuvent également créer des ESP personnalisées. Les noms des procédures stockées étendues système commencent tous par "xp_" et résident dans la base de données sybsystemprocs.

xp_cmdshell est une ESP système très utile, qui exécute une commande du système d'exploitation sur le système où est installé Adaptive Server.

Vous pouvez appeler une ESP système exactement comme s'il s'agissait d'une procédure stockée. La seule différence réside dans le fait qu'une ESP système exécute un code de langage procédural et non des requêtes Transact-SQL. Toutes les ESP sont mises en oeuvre par une application Open Server appelée Serveur XP, qui est exécutée sur la même machine qu'Adaptive Server. Serveur XP démarre automatiquement au premier appel d'ESP.

Pour plus d'informations sur les ESP système fournies avec Adaptive Server, reportez-vous au *Manuel de référence d'Adaptive Server.*

### Création d'ESP système

Créez une ESP système dans la base de données sybsystemprocs à l'aide de la commande create procedure. Les procédures système sont automatiquement incluses dans la base de données sybsystemprocs. Le nom de l'ESP et de la fonction de langage procédural qui lui est associée doit commencer par "xp_". L'uid de la procédure stockée doit être 1, celui du propriétaire de la base de données.

Pour obtenir des informations générales sur la création d'ESP, reportez-vous au chapitre 15, "Utilisation des procédures stockées étendues" du *Guide de l'utilisateur Transact-SQL.*

## Journalisation des messages d'erreur

Adaptive Server écrit les informations de démarrage dans un journal d'erreurs local à chaque initialisation. Le programme d'installation définit automatiquement l'emplacement du journal d'erreurs lorsque vous configurez un nouvel Adaptive Server. Pour connaître le nom de fichier et l'emplacement par défaut du journal d'erreurs, reportez-vous au Manuel de configuration pour votre plate-forme.

La plupart des messages d'erreur d'Adaptive Server apparaissent uniquement sur le terminal de l'utilisateur. Toutefois, les messages d'erreur fatale (degrés de sévérité de 19 et plus), les messages d'erreur du noyau et les messages d'informations d'Adaptive Server sont enregistrés dans le journal d'erreurs.

Adaptive Server laisse le journal d'erreurs ouvert jusqu'à la fin du processus serveur. Si vous voulez réduire la taille du journal d'erreurs en supprimant les messages anciens, arrêtez le processus Adaptive Server avant d'effectuer cette opération.

**Remarque** Sur certaines plates-formes telles que Windows NT, Adaptive Server enregistre également des messages d'erreur dans le journal des événements du système d'exploitation. Pour plus d'informations sur les journaux d'erreurs, reportez-vous au manuel d'installation et de configuration d'Adaptive Server.

# Connexion à un Adaptive Server

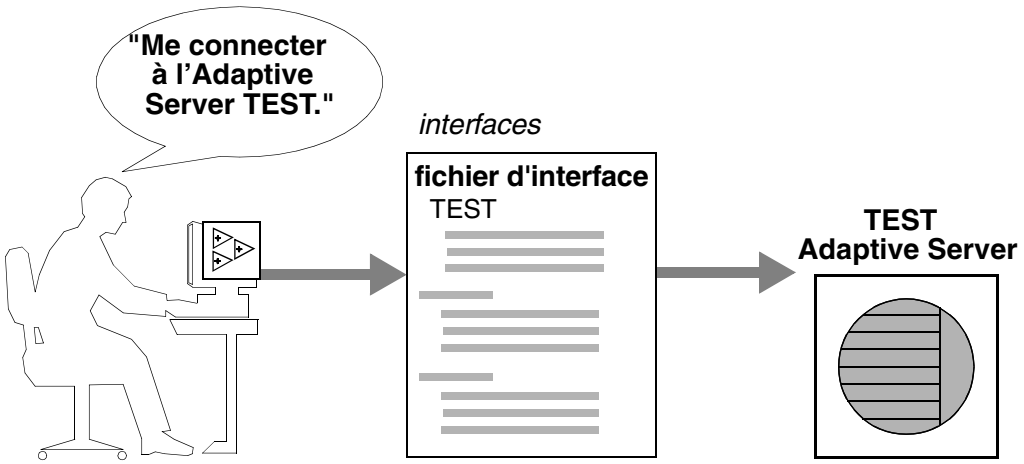
Adaptive Server peut communiquer avec d'autres Adaptive Server, avec les applications Open Server et les logiciels clients du réseau. Les clients peuvent communiquer avec un ou plusieurs serveurs et les serveurs peuvent communiquer avec d'autres serveurs en effectuant des appels de procédure à distance (RPC). Pour que les produits entrent en interaction, chacun d'eux doit savoir où les autres résident sur le réseau. Cette information est stockée dans un fichier d'interface.

## Fichier d'interface

Le fichier d'interface est généralement nommé *interfaces*, *interfac* ou *sql.ini*, selon le système d'exploitation.

Le fichier d'interface s'apparente à un carnet d'adresses. Il répertorie le nom et l'adresse de tous les serveurs connus. Lorsque vous voulez vous connecter à un serveur spécifique, le programme client cherche le nom du serveur dans le fichier d'interface, puis se connecte à ce serveur en utilisant l'adresse indiquée (voir figure 1-1).

***Figure 1-1 : Connexion à un Adaptive Server***




Le nom, l'emplacement et le contenu du fichier d'interface varient selon les systèmes d'exploitation. En outre, le format des adresses Adaptive Server dans le fichier d'interface varie selon les protocoles réseau.

A l'installation d'Adaptive Server, le programme d'installation crée un fichier d'interface simple que vous pouvez utiliser pour les connexions locales à Adaptive Server par l'intermédiaire d'un ou de plusieurs protocoles réseau. En tant qu'administrateur système, il vous appartient de modifier le fichier d'interface et de le distribuer aux utilisateurs pour leur permettre de se connecter à Adaptive Server via le réseau. Pour plus d'informations sur le fichier d'interface de votre plate-forme, reportez-vous au Manuel de configuration pour votre plate-forme.

## Services de répertoire

Le service de répertoire assure la gestion de la création, de la modification et de la recherche d'informations relatives aux services d'accès au réseau. Les services de répertoire sont fournis par la plate-forme ou par des sociétés tierces et doivent être achetés et installés indépendamment d'Adaptive Server. Voici deux exemples de services de répertoire : Registre NT et DCE (Distributed Computing Environment).

Le fichier *$SYBASE/config/libtcl.cfg* est un fichier de configuration fourni par Sybase utilisé par les serveurs et les clients pour déterminer :

- le service de répertoire à utiliser et
- l'emplacement du gestionnaire de services de répertoire indiqué.

Si aucun service de répertoire n'est installé ou répertorié dans le fichier *libtcl.cfg*, Adaptive Server s'adresse par défaut au fichier d'interface pour obtenir les informations relatives au service d'accès au réseau.

L'administrateur système doit modifier le fichier *libtcl.cfg* afin que ce dernier soit adapté à l'environnement d'exploitation.

Certains services de répertoire sont attachés à une plate-forme donnée ; d'autres peuvent être utilisés sur plusieurs plates-formes différentes. Etant donné la nature spécifiquement liée à la plate-forme des services de répertoire, reportez-vous au Manuel de configuration pour votre plate-forme pour de plus amples informations sur la configuration des services de répertoire.

## LDAP comme service de répertoire

Le protocole Lightweight Directory Access Protocol (LDAP) est un standard du secteur pour l'accès aux services de répertoire. Les services de répertoire permettent aux composants de consulter des informations en utilisant un nom distinctif (DN) sur un serveur LDAP qui stocke et gère les informations relatives au serveur, aux utilisateurs et aux logiciels utilisés au sein de l'entreprise ou via un réseau.

Le serveur LDAP peut se trouver sur une autre plate-forme que celle sur laquelle les clients Adaptive Server s'exécutent. Le protocole LDAP définit le protocole de communication et le contenu des messages échangés entre les clients et les serveurs. Les messages sont des opérateurs, comme les demandes du client de lecture, écriture et requête, ainsi que les réponses des serveurs, qui incluent des informations sur le format des données.

Le serveur LDAP stocke et extrait des informations sur :

- Adaptive Server (adresse IP, numéro de port et protocole réseau),
- les mécanismes de sécurité et filtres,
- le nom de serveur compagnon à haute disponibilité.

Le serveur LDAP peut être configuré avec ces restrictions d'accès :

- Authentification anonyme – toutes les données sont visibles pour tous les utilisateurs.
- Authentification avec nom et mot de passe – Adaptive Server utilise le nom d'utilisateur et le mot de passe par défaut du fichier :

  UNIX, 32 bits – *$SYBASE/$SYBASE_OCS/config/libtcl.cfg*

  UNIX, 64 bits – *$SYBASE/$SYBASE_OCS/config/libtcl64.cfg*

  NT – *%SYBASE%\%SYBASE_OCS%\ini\libtcl.cfg*

Les propriétés de l'authentification avec le nom d'utilisateur et le mot de passe établissent et interrompent une connexion de session à un serveur LDAP.

---

**Remarque** Le nom d'utilisateur et le mot de passe transmis au serveur LDAP pour l'authentification de l'utilisateur sont différents de ceux utilisés pour accéder à Adaptive Server.

---

Lorsqu'un serveur LDAP est spécifié dans le fichier *libtcl.cfg* ou *libtcl64.cfg* (fichier *libtcl*.cfg* collectivement), les informations du serveur sont accessibles uniquement depuis le serveur LDAP. Adaptive Server ne tient pas compte du fichier d'interface.

Si plusieurs services de répertoire sont supportés sur un serveur, l'ordre dans lequel la recherche est effectuée est spécifié dans le fichier *libtcl*.cfg*. Vous ne pouvez pas spécifier l'ordre de la recherche avec l'option de commande de ligne dataserver.

## Services de répertoire multiples

Tout type de service LDAP, qu'il s'agisse d'un serveur réel ou d'une passerelle vers d'autres services LDAP, est appelé serveur LDAP.

Vous pouvez spécifier plusieurs services de répertoire si vous souhaitez une protection de reprise sur le serveur secondaire à haute disponibilité dans le fichier *libtcl*.cfg*. Tous les services de répertoire figurant dans la liste ne sont pas tenus d'être des serveurs LDAP.

Exemple :

```
[DIRECTORY]
   ldap=libdldap.so ldap://test:389/dc=sybase,dc=com
   dce=libddce.so ditbase=/.:/subsys/sybase/dataservers
   ldap=libdldap.so ldap://huey:11389/dc=sybase,dc=com
```

Dans cet exemple, en cas d'échec de la connexion à *test:389*, la connexion échoue sur le pilote DCE avec la base DIT spécifiée. Là encore, en cas d'échec, le système tente de se connecter au serveur LDAP sur *huey:11389*. Les différents fournisseurs font appel à différents formats de base DIT.

**Remarque** Pour plus d'informations, reportez-vous au *Open Client Client-Library/C Programmer's Guide* et au *Open Client Client-Library/C Reference Manual*.

## Services de répertoire LDAP et fichier d'interface Sybase

Le pilote LDAP implémente les services de répertoire à utiliser avec un serveur LDAP. Les répertoires LDAP sont des infrastructures qui mettent à votre disposition :

- une alternative réseau au fichier d'interface Sybase classique,
- une vue simple et arborescente des informations relatives notamment aux utilisateurs, aux logiciels, aux ressources, aux réseaux, aux fichiers, etc.

Le tableau 1-1 met en évidence les différences entre le fichier d'interface Sybase et un serveur LDAP.

***Tableau 1-1 : Fichier d'interface et services de répertoire LDAP***

| Fichier d'interface | Services de répertoire |
|---|---|
| Spécifique à la plate-forme | Indépendant de la plate-forme |
| Spécifique à chaque installation Sybase | Centralisés et hiérarchiques |
| Contient différentes entrées master et de requête | Une seule entrée pour chaque serveur auquel accèdent les clients et les serveurs |
| Ne peut pas stocker des métadonnées relatives au serveur | Stocke des métadonnées relatives au serveur |

### Performances

Les performances peuvent être ralenties si vous utilisez un serveur LDAP et non un fichier d'interface car le serveur LDAP a besoin de temps pour établir une connexion réseau et extraire les données. Dans la mesure où cette connexion est effectuée au démarrage d'Adaptive Server, les variations éventuelles des performances seront visibles à la connexion. En cas de charge système normale, le délai n'est pas perceptible. En cas de charge système élevée avec un grand nombre de connexions, en particulier en cas de connexions répétées de courte durée, la différence en termes de performances globales que vous observez si vous utilisez un serveur LDAP et non le fichier d'interface classique peut être perceptible.

## Fonctions de sécurité disponibles dans Adaptive Server

SQL Server version 11.0.6 a été jugé conforme par l'organisme National Security Agency (NSA) aux critères de la Classe C2. Ces critères sont exposés dans un document établi par le DOD (Department of Defense) et appelé "Orange Book" : DOD 52.00.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria* [TCSEC].

La configuration de SQL Server version 11.0.6, qui a fait l'objet d'une évaluation au niveau de sécurité C2 par la NSA en 1996 sur la plate-forme HP 9000 HP-UX BLS, 9.09+, est désignée par l'expression **configuration évaluée**. Certaines fonctions de SQL Server, comme les procédures distantes et les mises à jour directes des tables système, ont été exclues de la configuration évaluée. Elles sont signalées par des notes insérées dans la documentation d'Adaptive Server. Pour obtenir une liste complètes des fonctions exclues de la configuration évaluée, reportez-vous à l'Annexe A du document *SQL Server Installation and Configuration Guide for HP 9000 HP-UX BLS, 9.09+*.

Cette version d'Adaptive Server contient toutes les fonctions de sécurité figurant dans SQL Server version 11.0.6 ainsi que d'autres fonctions nouvelles. Le tableau 1-2 résume les fonctions principales.

***Tableau 1-2 : Principales fonctions de sécurité***

| Fonction de sécurité | Description |
|---|---|
| DAC (Discretionary Access Controls, contrôles d'accès discrétionnaires) | Des contrôles d'accès permettent aux propriétaires d'objets de limiter l'accès à certains objets, en général avec des commandes d'octroi et de révocation des autorisations grant et revoke. Ce type de contrôle est laissé à la discrétion des propriétaires d'objets. |
| Contrôle d'identification et d'authentification | Seuls des utilisateurs autorisés peuvent se connecter au système. |
| Division des rôles | Cette fonction permet d'octroyer des rôles privilégiés à des utilisateurs afin que seuls ceux qui sont désignés puissent exécuter certaines tâches. Adaptive Server propose des rôles prédéfinis, appelés "rôles système", par exemple Administrateur système (SA) ou Responsable de la sécurité du système (SSO). De plus, Adaptive Server permet aux responsables de la sécurité du système de définir des rôles supplémentaires appelés "rôles utilisateur". |
| Sécurité réseau | Des services de sécurité permettent d'authentifier les utilisateurs et de protéger les données transmises d'une machine à l'autre sur le réseau. |
| Audit | Cette fonction permet d'effectuer un audit des événements, comme les connexions, les déconnexions, les initialisations du serveur, les appels de procédures distantes, les accès aux objets de base de données et toutes les actions exécutées par un utilisateur spécifique ou possédant un rôle particulier. De plus, Adaptive Server offre une option unique pour auditer tout un ensemble d'événements liés à la sécurité au niveau serveur. |

CHAPITRE 2

# Bases de données système et facultatives

Ce chapitre décrit les bases de données système qui résident sur tous les systèmes Adaptive Server. Il décrit également les bases de données facultatives fournies par Sybase que vous pouvez installer, ainsi qu'une base de données susceptible d'être installée par le support technique de Sybase à des fins de diagnostic.

Les sujets traités dans ce chapitre sont les suivants :



## Présentation des bases de données système

Au moment de l'installation, Adaptive Server contient les bases de données système suivantes :

- la base de données master
- la base de données model
- la base de données des procédures système, sybsystemprocs
- la base de données temporaire, tempdb

De manière facultative, vous pouvez installer :

- la base de données d'audit, sybsecurity
- la base de données des transactions avec commit à deux phases, sybsystemdb
- les bases de données exemples, pubs2 et pubs3
- la base de données dbcc, dbccdb

Pour plus d'informations sur l'installation des bases de données master, model, sybsystemprocs et tempdb, reportez-vous au Guide d'installation pour votre plate-forme. Pour plus d'informations sur l'installation de dbccdb, reportez-vous au chapitre 25, "Contrôle de la cohérence des bases de données".

Les bases de données master, model et les bases de données temporaires se trouvent sur le device désigné lors de l'installation, appelé device master. La base de données master réside entièrement sur le device master et ne peut pas être répartie sur d'autres devices. Toutes les autres bases de données et objets utilisateur doivent être créés sur d'autres devices.

---

**Avertissement !** Ne placez pas les bases de données utilisateur sur le device master. Des bases de données utilisateur sur le device master rendent plus difficile la restauration des bases de données système endommagées. Vous pourriez également être dans l'impossibilité de restaurer les bases de données utilisateur stockées sur le device master.

---

Vous devez installer les bases de données sybsecurity et sybsystemdb sur un device et un segment indépendants. Pour plus d'informations, reportez-vous au Guide d'installation pour votre plate-forme.

Vous pouvez installer la base de données sybsystemprocs sur un device de votre choix. Il peut être nécessaire de modifier les scripts d'installation de pubs2 et pubs3 pour partager le device créé pour sybsystemprocs.

Les scripts *installpubs2* et *installpubs3* ne spécifiant pas de device dans l'instruction create database, ces bases de données sont créées sur le device par défaut. A l'installation, le device master est le device par défaut. Pour modifier ce comportement, vous pouvez modifier les scripts ou consulter les instructions du chapitre 16, "Initialisation des devices de base de données" pour plus d'informations sur l'ajout de devices de bases de données et la désignation de device par défaut.

# Base de données *master*

La base de données master gère le fonctionnement d'Adaptive Server et stocke les informations sur toutes les bases de données utilisateur et devices associés. Le tableau 2-1 répertorie les informations conservées par la base de données master.

***Tableau 2-1 : Informations de la base de données master***

| Informations | Table système |
|---|---|
| Comptes utilisateur | syslogins |
| Comptes utilisateur distants | sysremotelogins |
| Serveurs distants avec lesquels ce serveur peut communiquer | sysservers |
| Processus en cours | sysprocesses |
| Variables d'environnement configurables | sysconfigures |
| Messages d'erreur système | sysmessages |
| Bases de données résidant sur Adaptive Server | sysdatabases |
| Espace de stockage alloué à chaque base de données | sysusages |
| Disques et bandes montés sur le système | sysdevices |
| Verrous actifs | syslocks |
| Jeux de caractères | syscharsets |
| Langues | syslanguages |
| Utilisateurs détenant un rôle au niveau du serveur | sysloginroles |
| Rôles disponibles au niveau du serveur | syssrvroles |
| Moteurs Adaptive Server en ligne | sysengines |

Comme la base de données master stocke des informations sur les bases de données et devices utilisateur, vous ne pouvez exécuter les commandes pour exécuter les commandes create database, alter database, disk init, disk refit, disk reinit et les commandes de mise en miroir de disques qu'à partir de la base de données master.

## Contrôle de la création d'objets dans la base de données *master*

Lors de la première installation d'Adaptive Server, seuls les administrateurs système peuvent créer des objets dans la base de données master, parce que l'administrateur système devient implicitement "dbo" (propriétaire de la base de données) de toutes les bases de données qu'il utilise. Tous les objets créés sur la base de données master seront utilisés pour l'administration globale du système. Les autorisations d'accès à la base master doivent être définies de sorte que tous les utilisateurs ne puissent pas y créer des objets.

---

**Avertissement !** Ne placez jamais d'objets utilisateur dans la base master, car cela risquerait de saturer le journal des transactions. Dans ce cas, vous ne pourrez plus utiliser les commandes dump transaction pour libérer de l'espace dans la base master.

---

Pour empêcher les utilisateurs de créer des objets dans la base master, vous pouvez également changer leur base de données par défaut (la base de données à laquelle l'utilisateur est connecté par défaut) par sp_modifylogin. Pour plus d'informations, reportez-vous au chapitre 10, à la section "Ajout d'utilisateurs aux bases de données".

Si vous créez vos propres procédures système, créez-les dans la base de données sybsystemprocs plutôt que dans la base master.

## Sauvegarde de *master* et conservation de copies des tables système

Pour parer à toute défaillance matérielle ou logicielle, deux tâches de maintenance sont essentielles :

- Effectuer des sauvegardes fréquentes de la base de données master et de toutes les bases de données utilisateur. Pour plus d'informations, reportez-vous à la section "Mise à jour des sauvegardes de la base de données master", page 43. Reportez-vous également au chapitre 28, "Restauration des bases de données système" pour une présentation de la procédure de restauration de la base de données master.

- Conserver une copie (de préférence hors ligne) de ces tables système : sysusages, sysdatabases, sysdevices, sysloginroles et syslogins. Pour plus d'informations, reportez-vous à la section "Conservation des tables système", page 44. Avec des copies de ces scripts, si une panne de disque dur ou un autre incident grave rendait la base de données inutilisable, vous pouvez utiliser les procédures de restauration décrites au chapitre 28, "Restauration des bases de données système". Si vous ne disposez pas de copies à jour de vos scripts, il sera beaucoup plus difficile d'assurer la reprise d'Adaptive Server si la base de données master est endommagée.

# Base de données *model*

Adaptive Server inclut la base de données model, qui fournit un modèle ou prototype pour la création de nouvelles bases de données utilisateur. Chaque fois qu'un utilisateur entre la commande create database, Adaptive Server effectue une copie de la base de données model et donne à cette nouvelle base de données la taille spécifiée dans la commande create database.

---

**Remarque** Une nouvelle base de données ne doit pas être plus petite que la base de données model.

---

La base de données model contient les tables système nécessaires pour chaque base de données utilisateur. Vous pouvez modifier model pour personnaliser la structure de vos futures bases de données ; toute modification effectuée sur la base model se reflètera dans chacune des nouvelles bases de données. Les modifications les plus courantes effectuées par les administrateurs système sur la base model sont :

- Ajout de types de données définis par l'utilisateur, de règles ou de valeurs par défaut.
- Ajout d'utilisateurs pouvant accéder à toutes les bases de données sur Adaptive Server.
- Attribution d'autorisations par défaut, en particulier pour les comptes "guest".

- Définition d'options de base de données comme select into/bulkcopy/pllsort. Les valeurs de ces paramètres se retrouveront dans toutes les nouvelles bases de données. Leur valeur d'origine dans model est off. Pour plus d'informations sur les options de base de données, reportez-vous au chapitre 22, "Définition des options de base de données".

Généralement, la plupart des utilisateurs n'ont pas l'autorisation de modifier la base de données model. Il n'y a pas beaucoup de raisons de leur octroyer une autorisation en écriture, puisque Adaptive Server copie la totalité du contenu de cette base dans chaque nouvelle base utilisateur.

La taille de model ne peut pas être supérieure à la taille de tempdb. Adaptive Server affiche un message d'erreur si vous tentez d'augmenter la taille de model sans avoir auparavant attribué à tempdb une taille au moins aussi grande.

**Remarque** Conservez une copie de sauvegarde de la base de données model et sauvegardez model par la commande dump database à chaque modification. En cas de défaillance du support, restaurez model comme une base de données utilisateur.

## Base de données *sybsystemprocs*

Les procédures système Sybase sont stockées dans la base de données sybsystemprocs. Quand un utilisateur exécute une procédure stockée à partir d'une base de données quelconque, Adaptive Server commence par rechercher cette procédure dans la base de données en cours pour l'utilisateur. Si cette base de données ne contient pas de procédure portant ce nom, Adaptive Server la recherche dans sybsystemprocs. S'il n'y a pas de procédure de ce nom dans sybsystemprocs, Adaptive Server poursuit la recherche dans la table master.

Si la procédure modifie les tables système (par exemple sp_adduser modifie la table sysusers), les modifications sont effectuées dans la base de données depuis laquelle la procédure est exécutée.

Pour modifier les autorisations par défaut sur les procédures système, vous devez les modifier dans la base sybsystemprocs.

**Remarque** A chaque modification de sybsystemprocs, vous devez sauvegarder la base de données.

# Base de données *tempdb*

Adaptive Server utilise une **base de données temporaire**, tempdb. Elle fournit une zone de stockage pour les tables temporaires et répond à d'autres besoins de stockage temporaire. L'espace disponible dans tempdb est partagé entre tous les utilisateurs de toutes les bases de données du serveur.

La taille par défaut de tempdb dépend de la taille de page logique de votre serveur, soit 2, 4, 8 ou 16 Ko. Certaines activités peuvent nécessiter une augmentation de la taille de tempdb. Les plus courantes sont les suivantes :

- Opérations sur des tables temporaires volumineuses.
- Activités nombreuses sur des tables temporaires, ce qui remplit les journaux de tempdb.
- Tris volumineux ou nombreux tris simultanés. Les sous-requêtes et agrégats par group by font également appel à tempdb.

Vous pouvez augmenter la taille de tempdb avec la commande alter database. La base tempdb est créée au départ sur le device master. Il est possible de lui ajouter de l'espace à partir du device master ou de tout autre device de base de données.

## Création de tables temporaires

Aucune autorisation spéciale n'est nécessaire pour utiliser tempdb, c'est-à-dire pour créer des tables temporaires ou exécuter des commandes qui peuvent nécessiter de l'espace de stockage dans la base de données temporaire.

Pour créer des tables temporaires, vous pouvez soit faire précéder le nom de table d'un signe dièse (#) dans une instruction create table, soit spécifier le préfixe de nom "tempdb..".

Les tables temporaires créées avec un signe dièse ne sont accessibles que par la session Adaptive Server en cours : les utilisateurs des autres sessions ne peuvent pas y accéder. Ces tables temporaires non partageables sont supprimées à la fin de chaque session. Les 13 premiers octets du nom de la table, incluant le signe dièse (#), doivent être uniques. Adaptive Server attribue aux noms de ces tables un suffixe sous forme d'un nombre sur 17 octets. (Vous pouvez voir le suffixe lors d'une requête sur tempdb..sysobjects.)

Les tables temporaires créées avec le préfixe "tempdb." sont stockées dans tempdb et peuvent être partagées par plusieurs sessions Adaptive Server. Adaptive Server ne modifie pas les noms des tables temporaires créées de cette façon. La table existe jusqu'au redémarrage d'Adaptive Server ou jusqu'à la suppression de la table par son propriétaire avec la commande drop table.

Les procédures système s'appliquent aux tables temporaires seulement si vous les exécutez depuis tempdb.

Si une procédure stockée crée des tables temporaires, ces tables sont supprimées à l'issue de la procédure. Les tables temporaires peuvent aussi être supprimées explicitement avant la fin d'une session.

---

**Avertissement !** Ne créez pas de tables temporaires avec le préfixe "tempdb.." à partir d'une procédure stockée sauf si vous souhaitez partager ces tables avec d'autres utilisateurs ou sessions.

---

A chaque redémarrage d'Adaptive Server, celui-ci copie la base model dans la base tempdb, ce qui efface la base de données. Les tables temporaires ne sont pas récupérables.

# Base de données *sybsecurity*

La base de données sybsecurity contient le système d'audit d'Adaptive Server. Elle inclut :

- Les tables système, sysaudits_01, sysaudits_02, ... sysaudits_08, qui contiennent la trace d'audit
- La table sysauditoptions, qui contient les lignes décrivant les options d'audit global
- Toutes les autres tables système par défaut dérivées de model

Le système d'audit est traité plus en détail dans le chapitre 12, "Audit".

# Base de données *sybsystemdb*

La base de données sybsystemdb contient des informations sur les transactions distribuées. Les versions 12.0 et ultérieures d'Adaptive Server peuvent fournir des services de coordination de transactions pour les transactions propagées sur des serveurs distants via des appels de procédure distante (RPC) ou le système CIS (Component Integration System). Les informations sur les serveurs distants participant aux transactions distribuées sont stockées dans la table syscoordinations.

---

**Remarque** Les services de gestion de transactions distribuées d'Adaptive Server version 12.0 et ultérieures font l'objet d'une licence séparée. Vous devez acheter et installer une licence valide pour les utiliser. Reportez-vous au document *Utilisation des fonctionnalités DTM* et au guide d'installation pour plus d'informations.

---

La base de données sybsystemdb stocke aussi des informations sur les transactions SYB2PC qui utilisent le protocole avec commit à deux phases de Sybase. La table spt_committab, qui contient des informations sur l'état d'achèvement des transactions avec commit à deux phases, est stockée dans la base de données sybsystemdb.

Les transactions avec commit à deux phases ainsi que la création de la base de données sybsystemdb sont traitées en détail dans le Manuel de configuration pour votre plate-forme.

# Bases de données exemple *pubs2* et *pubs3*

L'installation des bases de données exemple pubs2 et pubs3 est facultative. Ces bases de données sont fournies comme outil d'apprentissage d'Adaptive Server. La base de données exemple pubs2 est utilisée pour la plupart des exemples de la documentation Adaptive Server, sauf spécification contraire pour les exemples qui utilisent la base de données pubs3. Pour plus d'informations sur l'installation de pubs2 et pubs3, reportez-vous au Guide d'installation pour votre plate-forme. Pour plus d'informations sur le contenu des bases de données exemples, reportez-vous au *Guide de l'utilisateur Transact-SQL.*

## Maintenance des bases de données exemple

Les bases de données exemples contiennent un utilisateur "guest" qui permet à tout utilisateur autorisé d'Adaptive Server d'accéder à ces bases. L'utilisateur "guest" possède de nombreuses autorisations dans pubs2 et pubs3, y compris celles de sélectionner, d'insérer, de mettre à jour et de supprimer des tables utilisateur. Pour plus d'informations sur l'utilisateur "guest" et la liste des autorisations correspondantes dans pubs2 et pubs3, reportez-vous au chapitre 10, "Gestion des connexions et des utilisateurs de bases de données Adaptive Server".

La taille des bases de données pubs2 et pubs3 est déterminée par la taille de page logique de votre serveur, 2, 4, 8 et 16 Ko. Si possible, il est préférable de fournir à chaque nouvel utilisateur une copie nettoyée de pubs2 et pubs3 pour éviter toute confusion avec les modifications apportées par d'autres utilisateurs. Si vous souhaitez placer pubs2 ou pubs3 sur un device de base de données spécifique, modifiez le script d'installation avant d'installer la base de données.

Si l'espace disque est limité, vous pouvez demander aux utilisateurs d'exécuter la commande begin transaction avant de mettre à jour l'une des bases de données exemple. Quand l'utilisateur a terminé la mise à jour d'une des bases de données exemples, il peut alors exécuter la commande rollback transaction pour annuler les modifications.

## Données *image* dans *pubs2*

Adaptive Server inclut un script pour l'installation de données image dans la base de données pubs2 (pubs3 n'utilise pas de données image). Les données image sont constituées de six images, deux dans chacun des trois formats PICT, TIF et Sun raster. Sybase ne fournit aucun outil pour l'affichage des données image. Vous devez utiliser les outils graphiques appropriés pour afficher les images après leur extraction de la base de données.

Reportez-vous au Guide d'installation pour votre plate-forme pour plus d'informations sur l'installation des données image dans pubs2.

## Base de données *dbccdb*

dbcc checkstorage enregistre les informations de configuration pour la **base de données cible**, les activités de fonctionnement et les résultats du fonctionnement dans la base de données dbccdb. Cette base de données contient les procédures stockées dbcc de création et de maintenance de dbccdb et de génération de rapports sur les résultats des opérations dbcc checkstorage. Pour plus d'informations, reportez-vous au chapitre 25, "Contrôle de la cohérence des bases de données".

## Base de données *sybdiag*

Le Support Technique de Sybase peut créer une base de données sybdiag sur votre système à des fins de débogage. Cette base de données contient des données de configuration de diagnostic, elle ne doit pas être utilisée par les clients.

CHAPITRE 3

# Administration système présentée aux débutants

Ce chapitre :

- présente aux administrateurs système débutants les points essentiels ;
- aide les administrateurs système à trouver des informations dans la documentation Sybase.

Il aborde les sujets suivants :



Ce chapitre peut également constituer, pour les administrateurs avertis, une référence en matière d'organisation des opérations de maintenance courantes.

## Utilisation de serveurs "test"

Il est toujours recommandé d'installer et d'utiliser un Adaptive Server "test" et/ou de “développement” que vous supprimerez avant de créer le serveur de "production". L'utilisation d'un serveur test facilite la programmation et l'essai des différentes configurations, ainsi que la correction des erreurs. Il est beaucoup plus simple d'apprendre à installer et à exploiter de nouvelles fonctionnalités sans pour autant risquer d'avoir à redémarrer un serveur de production ou de recréer une base de données de production.

Si vous choisissez d'utiliser un serveur test, nous vous suggérons de le faire au moment de l'installation ou de la mise à niveau d'Adaptive Server, lorsque vous configurez le serveur. C'est à ce stade que sont prises les décisions les plus importantes concernant le système de production final. Les sections suivantes décrivent comment l'utilisation d'un serveur test peut aider les administrateurs système.

## Présentation des nouvelles procédures et fonctionnalités

L'utilisation d'un serveur test permet de tester les principales procédures d'administration avant de les appliquer en production. Si vous êtes un administrateur Adaptive Server néophyte, de nombreuses procédures présentées dans cet ouvrage vous seront inconnues et vous devrez peut-être faire plusieurs tentatives avant de parvenir à vous acquitter d'une tâche. Les administrateurs avertis gagneront à expérimenter les techniques introduites par les nouvelles fonctionnalités d'Adaptive Server.

## Planification des ressources

Le serveur test permet de planifier les ressources finales requises par votre système et aide à déceler une insuffisance de ressources que vous n'auriez pas anticipée.

Les ressources disque, principalement, peuvent avoir de graves conséquences sur la conception finale du système de production. Par exemple, vous pouvez décider qu'une certaine base de données nécessite une reprise instantanée en cas de panne de disque. Il faudrait, à cette fin, configurer un ou plusieurs devices de base de données supplémentaires, afin de mettre en miroir la base de données concernée. Si vous prenez conscience de ce besoin avec un serveur test, vous pouvez modifier la structure physique des bases de données et des tables sans déranger les utilisateurs des bases.

Vous pouvez également utiliser un serveur test pour évaluer les performances d'Adaptive Server et de vos applications en testant différentes configurations matérielles. Cette méthode permet de déterminer la configuration optimale des ressources physiques au niveau d'Adaptive Server et du système d'exploitation, avant d'utiliser votre système en production.

### Atteinte des objectifs en matière de performances

La plupart des objectifs de performances passent principalement par une planification rigoureuse de la conception et de la configuration des bases de données. Par exemple, vous pouvez vous apercevoir que les performances d'insertion et d'E/S entraînent sur certaines tables des goulets d'étranglement. Dans ce cas, il est conseillé de recréer la table sur un segment dédié, en la partitionnant. Ce type de modification perturbe le système de production ; même le simple changement d'un paramètre de configuration peut vous obliger à redémarrer Adaptive Server.

## Installation des produits Sybase

La responsabilité de l'installation d'Adaptive Server et d'autres produits Sybase revient parfois à l'administrateur système. Si c'est votre cas, les indications suivantes vous seront utiles.

### Vérification de la compatibilité entre produits

Avant d'installer de nouveaux produits ou de mettre à niveau des produits existants, lisez les notes de mise à jour fournies avec les produits afin de vous renseigner sur les questions de compatibilité pouvant avoir une incidence sur votre système. Des problèmes de compatibilité peuvent se présenter entre le matériel et les logiciels, ainsi qu'entre les différentes versions d'un même logiciel. La lecture préalable des notes de mise à jour peut vous faire gagner du temps en ce qui concerne la détection et la résolution des problèmes de compatibilité.

Reportez-vous également aux listes de problèmes connus installées avec Adaptive Server. Pour plus d'informations, reportez-vous aux notes de mise à jour.

## Installation ou mise à niveau d'Adaptive Server

Avant de commencer une installation ou une mise à niveau, parcourez le Guide d'installation pour votre plate-forme. Vous devez planifier certaines opérations d'installation et configurer le système d'exploitation *avant* d'installer Adaptive Server. Vous pouvez également vous adresser à l'administrateur de votre système d'exploitation qui vous aidera à définir la configuration requise du système d'exploitation pour Adaptive Server. Selon la plate-forme que vous utilisez, il peut s'agir de configuration de la mémoire, de partitions de disque, d'E/S asynchrones ou d'autres fonctionnalités. Nombre de ces tâches doivent être finies avant de commencer avec l'installation.

Avant de commencer la mise à niveau d'un serveur, sauvegardez toutes les données en mode autonome (y compris la base de données master, les bases de données utilisateur, les triggers et les procédures système). Après la mise à niveau, effectuez immédiatement une autre sauvegarde complète des données, surtout s'il existe des incompatibilités entre les anciens fichiers de sauvegarde et les nouvelles versions.

## Installation de logiciels tiers supplémentaires

### Protocoles réseau

Adaptive Server prend généralement en charge le ou les protocole(s) réseau propres à votre plate-forme matérielle. Si votre réseau accepte d'autres protocoles, installez les supports correspondants.

### Services de répertoire

Il existe une alternative à l'utilisation du fichier d'interface Sybase. Vous pouvez en effet utiliser un service de répertoire pour obtenir une adresse de serveur ou toute autre information relative au réseau. Les services de répertoire sont fournis par la plate-forme ou par des sociétés tierces et doivent être achetés et installés indépendamment d'Adaptive Server. Pour plus d'informations sur les services de répertoire supportés actuellement par Adaptive Server, reportez-vous au Manuel de configuration pour votre plate-forme. Consultez également la section "Services de répertoire", page 17.

### Configuration et test des connexions clientes

L'établissement d'une connexion cliente est le résultat de la coordination entre Adaptive Server, le logiciel client et les produits réseau. Si vous utilisez l'un des protocoles réseau installés avec Adaptive Server, vous trouverez dans le Manuel de configuration pour votre plate-forme des informations sur les essais de connexion réseau. Si vous utilisez un autre protocole, suivez les instructions fournies avec le produit réseau. Pour tester les connexions clientes avec Adaptive Server, vous pouvez également faire appel aux utilitaires "ping" livrés avec les produits de connexion Sybase. Pour obtenir une description générale du mode de connexion des clients à Adaptive Server, reportez-vous à la section "Connexion à un Adaptive Server", page 16. Pour plus de détails sur le nom et le contenu du fichier d'interface, consultez également le Manuel de configuration pour votre plate-forme.

## Allocation des ressources physiques

L'allocation de ressources physiques consiste à fournir à Adaptive Server la mémoire, l'espace disque et la puissance CPU nécessaires pour atteindre vos objectifs de performances et de reprise. Un administrateur système doit décider de l'utilisation des ressources lors de l'installation d'un nouveau serveur. Vous devez également revoir l'allocation des ressources d'Adaptive Server lorsque vous mettez votre plate-forme à niveau en ajoutant de la mémoire, des contrôleurs de disque ou des processeurs, ou lorsque la conception de votre système de bases de données est modifiée. Or, l'évaluation préalable des performances d'Adaptive Server et de vos applications peut vous aider à déceler, au niveau des ressources matérielles, des défaillances pouvant bloquer les performances.

Pour en savoir plus sur les types de ressources disque requis par Adaptive Server, reportez-vous au chapitre 15, "Présentation des sujets relatifs aux ressources disque". Pour plus d'informations sur la mémoire et les ressources CPU, consultez également le chapitre 18, "Configuration de la mémoire" et le chapitre 20, "Gestion des serveurs multiprocesseur".

Vous trouverez dans les sections suivantes des conseils utiles pour déterminer vos besoins en ressources physiques.

## Serveurs dédiés et serveurs partagés

Pour planifier les ressources d'Adaptive Server, vous devez tout d'abord connaître les ressources requises par les *autres* applications exécutées sur la même machine. Dans la plupart des cas, les administrateurs système utilisent Adaptive Server sur une machine dédiée. Cela signifie que seuls le système d'exploitation et le logiciel réseau utilisent des ressources qui pourraient être réservées à Adaptive Server. Dans un système partagé, d'autres applications fonctionnent sur la même machine qu'Adaptive Server, par exemple des programmes clients et des serveurs d'impression d'Adaptive Server. L'évaluation des ressources disponibles pour Adaptive Server peut s'avérer délicate avec les systèmes partagés, car les types de programmes et les structures correspondantes peuvent changer.

Dans les deux cas, c'est à l'administrateur système que revient la responsabilité d'évaluer, lors de la configuration des ressources d'Adaptive Server, celles qui sont destinées aux systèmes d'exploitation, aux programmes clients, aux environnements de multifenêtrage, etc. Configurez Adaptive Server de façon qu'il n'utilise que les ressources qui lui sont attribuées. Sinon, le serveur ne démarrera pas ou fonctionnera avec de faibles performances.

## Aide à la décision et applications OLTP

Adaptive Server propose de nombreuses fonctionnalités permettant d'optimiser les performances des applications OLTP, du système d'aide à la décision et des environnements prévoyant une charge de travail mixte. Vous devez néanmoins déterminer à l'avance les besoins des applications de votre système pour tirer le meilleur parti de ces fonctionnalités.

Pour les systèmes à charge de travail mixte, établissez à l'avance une liste détaillée des tables qui seront le plus utilisées par type d'application. Cela peut vous aider à atteindre des performances maximales pour les applications.

## Planification avancée des ressources

Il est essentiel de connaître et de planifier l'utilisation des ressources. Par exemple, pour les ressources disque, une fois que vous avez initialisé un device et que vous l'avez attribué à Adaptive Server, il ne peut plus être destiné à une autre utilisation (même si les données d'Adaptive Server ne remplissent jamais le device). De même, Adaptive Server s'attribue automatiquement l'espace mémoire qui lui a été alloué, empêchant qu'il soit utilisé par d'autres applications.

Les suggestions suivantes peuvent vous aider à planifier l'utilisation des ressources :

- Pour restaurer une base de données, il est *toujours* vivement conseillé de placer le journal de transactions sur un device distinct de celui des données. Reportez-vous au chapitre 21, "Création et gestion des bases de données utilisateur".
- Pensez à mettre en miroir les devices stockant les données importantes pour votre travail. Reportez-vous au chapitre 17, "Mise en miroir des devices de base de données". Pensez également à utiliser les disk arrays et la mise en miroir de disques pour les données d'Adaptive Server si votre système d'exploitation prend en charge ces fonctionnalités.
- Si vous travaillez avec un Adaptive Server test, il peut être plus pratique d'initialiser les devices de base de données comme des fichiers du système d'exploitation et non comme des partitions de disque. Adaptive Server prend en charge les partitions de disque et les fichiers du système d'exploitation.
- N'oubliez pas que la modification des options de configuration peut avoir une influence sur l'utilisation des ressources physiques, notamment la mémoire, par Adaptive Server. Ceci vaut en particulier pour les ressources de mémoire. Pour plus d'informations sur la quantité de mémoire utilisée par chacun des paramètres, reportez-vous au chapitre 5, "Définition des paramètres de configuration".

## Configuration du système d'exploitation

Une fois déterminé les ressources disponibles pour Adaptive Server et les ressources requises, configurez ces ressources physiques au niveau du système d'exploitation.

- Si vous utilisez les partitions de disque, initialisez les device blocs (raw devices) à la taille requise par Adaptive Server. Sachez que si vous initialisez une partition de disque pour Adaptive Server, elle ne peut plus être destinée à une autre utilisation (par exemple, le stockage des fichiers du système d'exploitation). Adressez-vous à l'administrateur de votre système d'exploitation qui vous aidera à initialiser et à configurer les partitions de disque à la bonne taille.
- Configurez le nombre de connexions réseau. Vérifiez cependant que la machine sur laquelle Adaptive Server fonctionne est effectivement capable de gérer toutes ces connexions. Reportez-vous à la documentation de votre système d'exploitation.
- D'autres configurations, concernant votre système d'exploitation et les applications que vous utilisez, peuvent s'avérer nécessaires. Pour plus d'informations sur les exigences du système d'exploitation d'Adaptive Server, consultez le Guide d'installation pour votre plate-forme. Reportez-vous également à votre documentation logiciel client ou adressez-vous aux ingénieurs de votre site pour connaître les exigences du système d'exploitation liées à vos applications.

# Sauvegarde et reprise

Il est essentiel de sauvegarder régulièrement vos bases pour préserver la cohérence de votre système de base de données. Bien qu'Adaptive Server procède à une reprise automatique après les pannes système (par exemple, les coupures de courant), vous pouvez *seul* restaurer les données perdues au cours d'une panne de disque. Pour sauvegarder votre système, suivez les instructions ci-dessous.

Les chapitres suivants expliquent comment élaborer et appliquer un plan de sauvegarde et de restauration :

- chapitre 26, "Elaboration d'un plan de sauvegarde et de reprise"
- chapitre 27, "Sauvegarde et restauration de bases de données utilisateur"

- chapitre 28, "Restauration des bases de données système"
- chapitre 29, "Gestion de l'espace libre avec des seuils"

## Mise à jour des sauvegardes de la base de données master

Il est impératif, pour tous les plans de sauvegarde et de restauration, de sauvegarder la base de données master. Elle contient en effet des informations sur la structure complète de votre système de bases de données. Elle répertorie les bases de données, devices et fragments de devices d'Adaptive Server qui composent votre système. Comme Adaptive Server a besoin de ces informations pour la restauration, il est essentiel de conserver une copie de sauvegarde de la base de données master constamment mise à jour.

Pour ce faire, sauvegardez la base de données après chaque commande ayant une incidence sur les disques, le stockage, les bases de données ou les segments. Cela implique une sauvegarde de la base de données master après les procédures suivantes :

- création ou suppression de bases de données ;
- initialisation de nouveaux devices de bases de données ;
- ajout de devices de sauvegarde ;
- utilisation des commandes de mise en miroir des devices ;
- création ou suppression de procédures système stockées dans la base master ;
- création, suppression ou modification d'un segment ;
- ajout de nouveaux logins Adaptive Server.

Pour sauvegarder la base master sur un device de type bande, démarrez isql et entrez la commande suivante :

```
dump database master to "device_bande"
```

où *device_bande* correspond au nom du device de type bande (par exemple */dev/rmt0*).

### Conservation des tables système

Outre la sauvegarde régulière de la base master, conservez des copies des tables système suivantes : sysdatabases, sysdevices, sysusages, sysloginroles et syslogins. Pour ce faire, exécutez l'utilitaire bcp décrit dans le manuel *Utilitaires* et stockez une version papier du contenu de chaque table. Pour créer une copie papier, imprimez le résultat des requêtes suivantes :

```
select * from sysusages order by vstart
select * from sysdatabases
select * from sysdevices
select * from sysloginroles
select * from syslogins
```

Si vous possédez des copies de ces tables et qu'une panne de disque ou tout autre événement rendant inutilisable votre base de données survient, vous pourrez avoir recours aux procédures de restauration décrites au chapitre 28, "Restauration des bases de données système".

Il est également conseillé de conserver des copies de tous les scripts DDL (langage de définition de données) concernant les objets utilisateur, en se conformant aux explications de la section "Stockage des enregistrements", page 47.

## Automatisation des procédures de sauvegarde

La création d'une procédure de sauvegarde automatique facilite et accélère la préparation des sauvegardes. Cette automatisation peut s'avérer aussi simple que l'utilisation d'un script du système d'exploitation ou d'un utilitaire (par exemple, l'utilitaire cron pour UNIX) pour exécuter les commandes de sauvegarde nécessaires. Vous pouvez également automatiser la procédure en utilisant des seuils (reportez-vous au chapitre 29, "Gestion de l'espace libre avec des seuils".)

Même si les commandes requises pour un script d'automatisation dépendent du système d'exploitation utilisé, tous les scripts devraient effectuer les mêmes opérations de base, à savoir :

1 Démarrage d'isql et sauvegarde du journal de transactions dans une zone de stockage (par exemple, un fichier temporaire).

2 Changement du nom du fichier de sauvegarde de manière à ce qu'il contienne la date et l'heure de sauvegarde, ainsi que le nom de la base de données.

3 Consignation des caractéristiques de la nouvelle sauvegarde dans un fichier d'archives.

4 Enregistrement, dans un fichier d'erreurs séparé, de toutes les erreurs survenues pendant la sauvegarde.

5 Envoi automatique d'un courrier électronique à l'administrateur système en cas d'erreur.

## Vérification de la cohérence des données avant la sauvegarde d'une base

Parfois, la sauvegarde d'une base de données n'est pas suffisante, il faut aussi que les sauvegardes soient cohérentes et *fiables* (surtout pour la base master). Si vous sauvegardez une base de données contenant des erreurs internes, elle contiendra les mêmes erreurs une fois restaurée.

Les commandes de dbcc permettent de vérifier, avant sauvegarde, si une base de données contient des erreurs. Utilisez toujours les commandes de dbcc pour vérifier la cohérence d'une base de données avant de la sauvegarder. Si dbcc décèle des erreurs, procédez aux corrections nécessaires avant de sauvegarder la base de données.

A terme, vous pouvez envisager d'exécuter dbcc pour garantir l'exactitude de vos bases de données. Si vous n'avez pas détecté beaucoup d'erreurs au cours de ses exécutions successives, vous pouvez estimer que le risque d'altération de la base de données est négligeable et décider de n'exécuter dbcc qu'occasionnellement. Mais si les risques de perte de données sont trop importants, continuez d'exécuter les commandes de dbcc à chaque sauvegarde de la base.

---

**Remarque** Afin de maintenir les performances, de nombreux sites effectuent les contrôles avec dbcc en dehors des heures de pointe ou sur des serveurs séparés.

---

Pour plus d'informations sur la commande dbcc, reportez-vous au chapitre 25, "Contrôle de la cohérence des bases de données".

## Contrôle de la taille du journal

Lorsque le journal de transactions arrive presque à saturation, il peut s'avérer impossible d'utiliser les procédures courantes pour sauvegarder les transactions et libérer de l'espace. L'administrateur système doit contrôler la taille du journal et effectuer des sauvegardes régulières du journal de transactions (en plus des sauvegardes de base de données) afin d'éviter cette situation. Il est conseillé de définir une procédure stockée associée au seuil qui vous avertit (ou qui sauvegarde le journal) dès que le journal a atteint une capacité donnée. Pour plus d'informations sur l'utilisation des procédures associées aux seuils, reportez-vous au chapitre 29, "Gestion de l'espace libre avec des seuils". Il est également préférable de sauvegarder le journal de transactions juste avant d'effectuer une sauvegarde complète de la base de données, afin de réduire le temps nécessaire à la sauvegarde et à la restauration de la base.

Vous pouvez aussi contrôler manuellement l'espace occupé par le segment de journal, en utilisant la procédure stockée sp_helpsegment conformément aux indications de la section "Obtention d'informations relatives aux segments", page 749.

# Maintenance courante, détection et résolution des problèmes

Outre les sauvegardes régulières, l'administrateur système effectue également, tout au long de la vie du serveur, les opérations de maintenance suivantes.

## Démarrage et arrêt d'Adaptive Server

La plupart des administrateurs système automatisent le démarrage d'Adaptive Server de façon qu'il coïncide avec celui du serveur. Il faut, pour cela, modifier les scripts de démarrage du système d'exploitation ou faire appel aux autres procédures du système d'exploitation. Pour plus d'informations sur le démarrage et l'arrêt d'Adaptive Server, reportez-vous au Manuel de configuration pour votre plate-forme.

### Affichage et troncature du journal d'erreurs

Vous devez examiner régulièrement le contenu du journal d'erreurs afin de déterminer si des erreurs graves sont survenues. Vous pouvez aussi utiliser les scripts du système d'exploitation pour balayer le journal d'erreurs et rechercher des messages spécifiques et pour avertir l'administrateur système de certaines erreurs. La surveillance du journal d'erreurs permet généralement de déceler des problèmes récurrents et de même nature ou de déterminer si un device de base de données présente des défaillances. Pour plus d'informations sur les messages d'erreur et leur sévérité, reportez-vous au chapitre 4, "Diagnostic des problèmes système".

Comme, à chaque démarrage, Adaptive Server ajoute des messages d'état et d'informations au journal d'erreurs, ce dernier peut devenir extrêmement volumineux. Vous pouvez régulièrement "tronquer" le journal en l'ouvrant et en supprimant des enregistrements obsolètes. En veillant à ce que le journal conserve une taille raisonnable, vous économisez de l'espace disque, tout en facilitant la localisation des erreurs courantes.

## Stockage des enregistrements

En tant qu'administrateur système, le stockage des enregistrements relatifs à votre système Adaptive Server représente une part importante de vos attributions. Un enregistrement précis des modifications et des problèmes rencontrés peut constituer une bonne référence lorsque vous contactez le Support Technique de Sybase ou que vous restaurez des bases de données. Surtout, il peut fournir des informations essentielles aux administrateurs qui gèrent le système Adaptive Server en votre absence. Les sections suivantes présentent les types d'enregistrement les plus utiles.

### Contacts

Conservez une liste des personnes à contacter pour vous-même, pour le responsable de la sécurité du système (SSO), pour l'opérateur et pour les propriétaires de bases de données. Notez, pour chaque rôle, un deuxième contact. Mettez ces informations à la disposition de tous les utilisateurs Adaptive Server afin qu'ils transmettent aux personnes concernées des demandes d'amélioration et qu'ils fassent part des problèmes rencontrés.

## Informations de configuration

En principe, vous devriez créer des bases de données et des objets de base de données et configurer Adaptive Server en utilisant les fichiers scripts que vous stockerez ensuite en lieu sûr. En cas d'incident, vous pouvez ainsi recréer la totalité de votre système. Cela vous permet également de recréer rapidement les systèmes de bases de données sur de nouvelles plates-formes matérielles, à des fins d'évaluation. Si vous utilisez un outil externe pour l'administration système, n'oubliez pas de générer des scripts équivalents après avoir effectué des tâches d'administration.

Pensez à noter les informations suivantes :

- commandes utilisées pour créer les bases de données et les objets de base de données (scripts DDL) ;
- commandes ajoutant de nouveaux logins Adaptive Server et de nouveaux utilisateurs de base de données ;
- fichier de configuration courant d'Adaptive Server, conformément aux indications de la section "Utilisation de sp_configure avec un fichier de configuration", page 91 ;
- nom, emplacement et taille de tous les fichiers et partitions de disque initialisés comme devices de base de données.

Il est également utile de consigner dans un journal, avec leur date, toutes les modifications apportées à la configuration d'Adaptive Server. Notez tous les changements avec un bref commentaire indiquant quand et pourquoi vous les avez effectués, ainsi qu'avec un résumé du résultat final.

## Planification de la maintenance

Notez sur un calendrier les opérations de maintenance programmées. Ce calendrier doit répertorier toutes les procédures exécutées sur votre site, à savoir :

- utilisation de dbcc pour vérifier la cohérence des bases de données ;
- sauvegarde des bases de données système et utilisateur ;
- contrôle de l'espace laissé dans les journaux de transactions (quand la vérification n'est pas automatique) ;
- sauvegarde du journal de transactions ;
- examen du journal d'erreurs d'Adaptive Server, de Backup Server™ et d'Adaptive Server Monitor™ ;

- exécution de la commande update statistics (reportez-vous au chapitre 34, "Utilisation des commandes set statistics" du manuel *Performances et optimisation*) ;
- examen des informations d'audit, si le système d'audit est installé ;
- nouvelle compilation des procédures stockées ;
- contrôle de l'utilisation des ressources du serveur.

## Informations sur le système

Enregistrez les informations concernant le matériel et le système d'exploitation sur lesquels fonctionne Adaptive Server. Il peut s'agir des éléments suivants :

- copies des fichiers de configuration ou des fichiers de démarrage du système d'exploitation ;
- copies des fichiers de configuration du réseau (par exemple les *hosts* et *services*) ;
- noms des fichiers exécutables et des devices de base de données d'Adaptive Server avec les autorisations d'exécution correspondantes ;
- nom et emplacement des devices de type bande utilisés pour les sauvegardes ;
- copies des scripts du système d'exploitation ou des programmes de sauvegarde automatique permettant de démarrer Adaptive Server ou d'effectuer d'autres opérations d'administration.

## Plan de reprise en cas d'incident

A partir des principales procédures de sauvegarde et de restauration, des conseils de la section "Sauvegarde et reprise", page 42 et de votre expérience personnelle de restauration des données, faites un résumé des opérations de restauration adaptées à votre système. Cette précaution peut s'avérer utile aussi bien pour vous que pour les autres administrateurs système qui peuvent avoir besoin de restaurer le système de production en cas d'urgence.

# Obtention d'une aide complémentaire

La quantité d'informations nouvelles que les administrateurs système doivent assimiler peut être décourageante. Il existe quelques outils logiciels qui peuvent vous aider à étudier et à simplifier les principales tâches d'administration. Il s'agit entre autres d'Adaptive Server Monitor, utilisé pour contrôler les performances et les activités du serveur, ainsi que de Sybase Central, qui simplifie un grand nombre de tâches d'administration. Sont également disponibles de nombreux logiciels tiers conçus pour aider les administrateurs système à gérer les opérations de maintenance quotidiennes.

CHAPITRE 4

# Diagnostic des problèmes système

Ce chapitre traite du diagnostic et de la résolution des problèmes.

Les sujets traités dans ce chapitre sont les suivants :



## Messages d'erreur et réponse d'Adaptive Server aux problèmes système

Lorsqu'Adaptive Server rencontre un problème, que celui-ci ait été provoqué par l'utilisateur ou le système, il affiche des informations sur la nature du problème, sa sévérité et les différentes solutions. Ces messages comprennent les éléments suivants :

- un **numéro de message** qui identifie, de manière unique, le message d'erreur ;
- un **degré de sévérité** compris entre 10 et 24, qui indique le type et le niveau de sévérité du problème ;
- un **numéro d'état d'erreur** qui permet d'identifier, de manière unique, la ligne de code d'Adaptive Server où l'erreur s'est produite ;
- un **message d'erreur** qui décrit la nature du problème et propose éventuellement des solutions.

Par exemple, le message suivant s'affiche si vous faites une faute de frappe et tentez d'accéder à une table qui n'existe pas :

```
select * from publisher
Msg 208, Level 16, State 1:
publisher not found. Specify owner.objectname or use
sp_help to check whether the object exists (sp_help
may produce lots of output).
```

Parfois, une même requête peut donner lieu à plusieurs messages d'erreur. Généralement, lorsqu'il y a plusieurs erreurs dans un batch ou une requête, Adaptive Server ne donne des informations que sur la première. Les autres erreurs ne sont signalées qu'à l'exécution suivante du batch ou de la requête.

Les messages d'erreur sont stockés dans master..sysmessages qui est mise à jour à chaque nouvelle version d'Adaptive Server. Les premières lignes sont les suivantes (pour un Adaptive Server dont la langue par défaut est l'américain) :

```
select error, severity, description
from sysmessages
where error >=101 and error <=106
and langid is null
error severity description
----- -------- ----------------------------------------------------
  101       15 Line %d: SQL syntax error.
  102       15 Incorrect syntax near '%.*s'.
  103       15 The %S_MSG that starts with '%.*s' is too long.
               Maximum length is %d.
  104       15 Order-by items must appear in the select-list if
               the statement contains set operators.
  105       15 Unclosed quote before the character string '%.*s'.
  106       16 Too many table names in the query. The maximum
               allowable is %d.

(6 rows affected)
```

Vous pouvez obtenir votre propre liste en interrogeant sysmessages. Vous trouverez ci-dessous quelques informations complémentaires pour écrire votre requête :

- Si votre serveur supporte plusieurs langues, sysmessages stocke chaque message dans chaque langue. La colonne langid indique NULL pour l'américain et donne l'ID de langue syslanguages.langid correspondant pour les autres langues installées sur le serveur. Pour toute information sur les langues de votre serveur, utilisez sp_helplanguage.
- La colonne dlevel dans sysmessages n'est actuellement pas utilisée.
- La colonne sqlstate stocke la valeur SQLSTATE pour les conditions d'erreur et les exceptions définies dans ANSI SQL92.
- Les numéros de message à partir de 17000 correspondent à des messages d'erreur de procédure système et à des chaînes de message.

## Messages d'erreur et numéros de message

La combinaison du numéro de message (*error*) et de l'ID de langue (*langid*) identifie, de manière unique, chaque message d'erreur. Ainsi, les messages dont les numéros sont identiques, mais dont les ID sont différents, sont des traductions.

```
select error, description, langid
from sysmessages
where error = 101
error description                                langid
----- ---------------------------------------- ------
  101 Line %d: SQL syntax error.                   NULL
  101 Ligne %1!: erreur de syntaxe SQL.               1
  101 Zeile %1!: SQL Syntaxfehler.                    2

(3 rows affected)
```

Le message d'erreur décrit le problème. Ces descriptions comprennent souvent un numéro de ligne, une référence à un type d'objet de base de données (une table, une colonne, une procédure stockée, etc.) ou le nom d'un objet de base de données spécifique.

Dans le champ description de sysmessages, le signe pour cent (%) suivi d'un caractère ou d'une chaîne de caractères sert de marque de réservation pour les données que fournit ensuite Adaptive Server lorsqu'il rencontre le problème et génère le message d'erreur. "%d" est une marque de réservation pour un nombre ; "%S_MSG" est une marque de réservation pour un type d'objet de base de données ; "%.*s" (tous entre guillemets) est une marque de réservation pour le nom d'un objet de base de données spécifique. Le tableau 4-1 répertorie les marques de réservation et ce qu'elles représentent.

Par exemple, le champ description pour le numéro de message 103 est le suivant :

```
The %S_MSG that starts with '%.*s' is too long.
Maximum length is %d.
```

Selon le cas, vous pouvez obtenir le message d'erreur suivant :

```
The column that starts with 'title' is too long.
Maximum length is 80.
```

Lorsque vous signalez des erreurs, veillez tout particulièrement à préciser le numéro, le type des objets et leur nom. (Reportez-vous à la section "Rapport d'erreurs", page 64).

## Variables dans le texte des messages d'erreur

Le tableau 4-1 détaille les symboles qui apparaissent dans le texte des messages d'erreur (explication des messages d'erreur) :

***Tableau 4-1 : Symboles utilisés dans le texte des messages d'erreur***

| Le symbole | désigne |
|---|---|
| %d, %D | un nombre décimal. |
| %x,%X,%.*x,%lx, %04x, %08lx | un nombre hexadécimal. |
| %s | une chaîne se terminant par une valeur NULL. |
| %.*s, %*s, %*.s | une chaîne, généralement le nom d'un objet de base de données spécifique. |
| %S_*type* | une structure définie par Adaptive Server. |
| %c | un caractère unique. |
| %f | un nombre en virgule flottante. |
| %ld | un décimal long. |
| %lf | un nombre en virgule flottante double. |

# Journalisation des erreurs d'Adaptive Server

La plupart des messages d'erreur Adaptive Server apparaissent uniquement à l'écran de l'utilisateur.

La trace des messages d'erreur fatale (degrés de sévérité 19 et au-delà) et des messages d'erreur du noyau est envoyée dans un journal d'erreurs. Le nom de ce fichier varie ; reportez-vous au Manuel de configuration pour votre plate-forme ou au *Guide Utilitaires*.

---

**Remarque** Le journal d'erreurs appartient à l'utilisateur qui a installé Adaptive Server (ou à la personne qui a démarré Adaptive Server après la suppression d'un journal d'erreurs). Si un problème d'autorisation ou de propriété du journal d'erreurs se pose au niveau du système d'exploitation, cela peut bloquer le démarrage d'Adaptive Server.

---

Adaptive Server crée un journal d'erreurs s'il n'existe pas déjà. Vous spécifiez l'emplacement du journal d'erreurs au démarrage, en définissant le paramètre *journal_erreurs* dans le fichier runserver ou sur la ligne de commande. L'utilitaire d'installation Sybase configure le fichier runserver avec *$SYBASE/install* comme emplacement du journal d'erreurs si vous ne spécifiez pas d'autre emplacement lors de l'installation. Si vous ne spécifiez aucun emplacement dans le fichier runserver ou sur la ligne de commande, le journal d'erreurs est créé dans le répertoire dans lequel vous démarrez Adaptive Server. Pour plus d'informations sur la manière de spécifier l'emplacement du journal d'erreurs, reportez-vous à la commande dataserver du *Guide Utilitaires*.

---

**Remarque** Démarrez toujours Adaptive Server à partir du même répertoire, ou encore à l'aide du fichier runserver ou du drapeau du journal d'erreurs, de façon à pouvoir retrouver votre journal d'erreurs.

---

Chaque fois que vous démarrez un serveur, des messages contenant des informations sur la réussite (ou l'échec) du démarrage et de la restauration de chaque base de données du serveur sont insérés dans le journal d'erreurs. Ensuite, tous les messages d'erreur fatale et d'erreur noyau sont ajoutés au journal d'erreurs. Si vous devez réduire la taille du journal d'erreurs en supprimant les messages périmés ou inutiles, tronquez le journal lorsqu'Adaptive Server est arrêté.

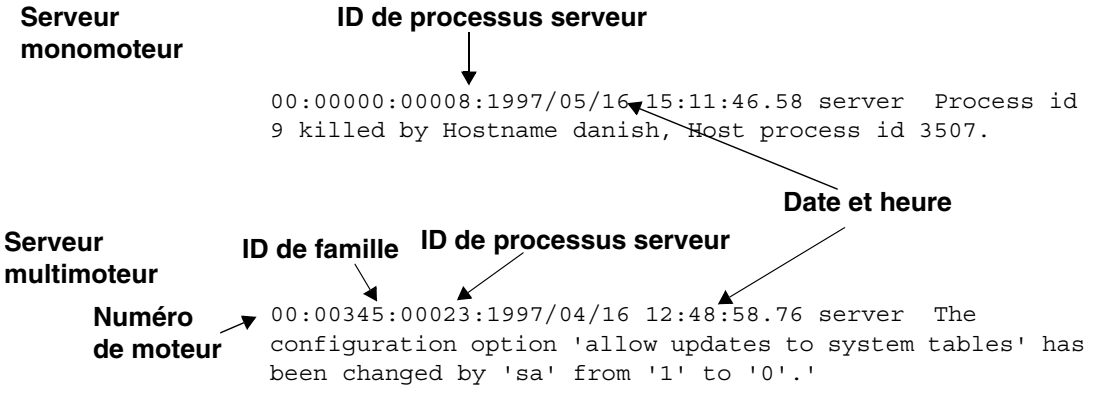
## Format du journal d'erreurs

Les entrées du journal d'erreurs contiennent les informations suivantes :

- Le moteur concerné, à chaque entrée de journal. Le numéro de moteur apparaît sous la forme d'un numéro à deux chiffres. Si seul un moteur est en ligne, "00." s'affiche.
- L'ID de famille du thread d'origine :
  - Dans un traitement en série, "00000." s'affiche.
  - Dans une **page suspecte**, l'ID de processus serveur du parent du thread d'origine s'affiche.
- L'ID de processus serveur du thread d'origine :
  - Dans un traitement en série, il s'agit de l'ID de processus serveur du thread qui a généré le message. S'il s'agit d'un thread système, "00000." s'affiche.
  - Dans un traitement parallèle, il s'agit de l'ID de processus serveur du thread d'origine.
- La date, au format *aaaa/mm/jj*, qui permet de trier les messages d'erreur par date.
- L'heure, affichée au format 24 heures. Le format de l'heure comprend également les secondes et centièmes de seconde.
- Le mot "server" ou "kernel". Cette entrée est uniquement destinée au Support Technique de Sybase.
- Le message d'erreur à proprement parler.

La figure 4-1 représente deux exemples de ligne d'un journal d'erreurs :

***Figure 4-1 : Format du journal d'erreurs***



## Degrés de sévérité

Le degré de sévérité d'un message indique le type de problème rencontré par Adaptive Server. Pour une cohérence maximale, lorsqu'Adaptive Server répond à des conditions d'erreur, les messages qu'il affiche proviennent de sysmessages ; en revanche, les actions qu'il déclenche reposent sur une table interne. Certains messages correspondants n'ayant pas les mêmes degrés de sévérité, vous constaterez peut-être une différence entre le comportement attendu et celui obtenu si, par exemple, vous développez des applications ou des procédures qui font référence aux messages et aux degrés de sévérité d'Adaptive Server.

---

**Avertissement !** Vous pouvez créer vos propres messages et numéros d'erreur à partir des numéros d'erreur Adaptive Server (par exemple, en ajoutant 20 000 à la valeur d'Adaptive Server). Cependant, vous ne devez pas modifier les messages système fournis avec Adaptive Server dans la table système sysmessages.

---

Vous pouvez ajouter les messages d'erreur définis par l'utilisateur à sysusermessages à l'aide de la procédure système sp_addmessage. Consultez le *Adaptive Server - Manuel de référence*.

Les utilisateurs doivent aviser l'administrateur système de tout problème de degré de sévérité 17 et plus. Celui-ci doit alors résoudre ces problèmes et analyser leur fréquence d'apparition.

Si le problème concerne la base de données dans son intégralité, l'administrateur système sera peut-être amené à recourir au Database Consistency Checker (dbcc) pour déterminer l'étendue des dommages. Le dbcc peut identifier des objets qu'il faudra supprimer. S'il peut réparer certains dommages, il est possible qu'il faille néanmoins recharger la base de données.

Pour plus d'informations, reportez-vous aux chapitres suivants :

- dbcc est traité au chapitre 25, "Contrôle de la cohérence des bases de données".
- Le chargement de bases de données utilisateur est traité au chapitre 27, "Sauvegarde et restauration de bases de données utilisateur".
- Le chargement de bases de données système est traité au chapitre 28, "Restauration des bases de données système".

Les sections suivantes indiquent la signification de chaque degré de sévérité.

## Degrés 10 à 18

Les messages d'erreur des degrés de sévérité 10 à 16 sont générés par des problèmes provenant d'erreurs utilisateur. Ces problèmes peuvent être résolus par l'utilisateur. Les degrés de sévérité 17 et 18 ne mettent pas fin à la session de l'utilisateur.

Au-delà du degré de sévérité 17, les erreurs doivent être signalées à l'administrateur système ou au propriétaire de la base de données.

### Degré 10 : informations d'état

Les messages de degré de sévérité 10 ne désignent pas du tout des erreurs. Ils fournissent des informations supplémentaires après l'exécution de certaines commandes et n'indiquent généralement pas de numéro de message ou de degré de sévérité. Par exemple, après exécution d'une commande create database, Adaptive Server affiche un message indiquant à l'utilisateur l'espace effectivement alloué à la nouvelle base de données.

### Degré 11 : objet de base de données spécifié introuvable

Les messages de degré de sévérité 11 indiquent qu'Adaptive Server ne trouve pas un objet référencé dans la commande.

Cela se produit souvent lorsque l'utilisateur fait une erreur lors de la saisie du nom d'un objet de base de données, ne spécifie pas le nom du propriétaire d'un objet ou confond la base de données courante avec une autre. Contrôlez bien l'orthographe des noms, indiquez le nom du propriétaire si l'objet n'appartient ni à vous-même ni au "dbo", et assurez-vous que vous êtes bien dans la base de données voulue.

### Degré 12 : type de données erroné

Les messages de degré de sévérité 12 indiquent qu'il y a un problème au niveau des types de données. Par exemple, l'utilisateur a peut-être tenté d'entrer, dans une colonne, une valeur dont le type de données est incorrect ou a essayé de comparer des colonnes ayant des types de données différents (donc incompatibles).

Pour résoudre les problèmes de comparaison, utilisez la fonction convert avec select. Pour plus d'informations sur la fonction convert, reportez-vous au *Adaptive Server - Manuel de référence* ou au *Guide de l'utilisateur Transact-SQL.*

### Degré 13 : erreur de syntaxe de la transaction utilisateur

Les messages de degré de sévérité 13 indiquent qu'il y a un problème dans la transaction en cours définie par l'utilisateur. Par exemple, cela survient si vous lancez la commande commit transaction sans avoir au préalable exécuté begin transaction ou que vous tentez d'annuler une transaction jusqu'à un point de sauvegarde qui n'a pas été défini (il peut s'agir d'une simple faute de frappe au niveau du nom du point de sauvegarde).

Le degré de sévérité 13 peut également indiquer un interblocage, auquel cas le processus est bloqué. L'utilisateur doit, par conséquent, relancer sa commande.

### Degré 14 : autorisation insuffisante pour exécuter la commande

Les messages de degré de sévérité 14 indiquent que vous n'avez pas l'autorisation requise pour exécuter la commande ou accéder à l'objet de base de données. Vous pouvez alors demander au propriétaire de l'objet de base de données, au propriétaire de la base ou à l'administrateur système de vous octroyer la permission d'utiliser la commande ou l'objet en question.

### Degré 15 : erreur de syntaxe dans les instructions SQL

Les messages de degré de sévérité 15 indiquent que l'utilisateur a fait une erreur dans la syntaxe de la commande. Le texte de ces messages d'erreur indique le numéro des lignes sur lesquelles l'erreur s'est produite ainsi que le terme le plus proche.

### Degré 16 : erreurs utilisateur diverses

La plupart des messages de degré de sévérité 16 indiquent que l'utilisateur a commis une erreur non fatale qui n'entre dans aucune autre catégorie. Les messages de degré de sévérité 16 et au-delà peuvent également indiquer des erreurs logicielles ou matérielles.

Par exemple, l'utilisateur peut avoir tenté de mettre à jour une vue sans tenir compte des restrictions. Il existe un autre type d'erreur, généré lorsqu'un nom de colonne non qualifié est utilisé par différentes tables au sein d'une commande. En effet, Adaptive Server n'a aucun moyen de déterminer les intentions de l'utilisateur. Vérifiez la syntaxe de la commande et le contexte de la base de données courante.

Les messages qui comportent habituellement un degré de sévérité supérieur à 16 indiquent le degré de sévérité 16 lorsqu'ils sont générés par dbcc checktable ou dbcc checkalloc, pour que la vérification puisse se poursuivre sur l'objet suivant. Lorsque vous exécutez l'utilitaire dbcc, consultez le manuel *Messages d'erreur* pour obtenir des informations sur les messages d'erreur compris entre 2500 et 2599 et portant le degré de sévérité 16.

---

**Remarque** Généralement, les erreurs de degré de sévérité 17 et 18 ne sont pas signalées dans le journal d'erreurs. Il faut donc que les utilisateurs avertissent l'administrateur système de ce type d'erreur.

---

## Degré 17 : ressources insuffisantes

Les messages d'erreur de degré de sévérité 17 indiquent que la commande a amené Adaptive Server à consommer toutes ses ressources (généralement l'espace réservé à la base sur le disque) ou à dépasser une limite définie par l'administrateur système. Vous pouvez continuer votre travail en cours, mais il est possible que vous ne puissiez plus exécuter de commande spécifique.

Les limites système sont, d'une part, le nombre de bases pouvant être ouvertes simultanément et, d'autre part, le nombre de connexions à Adaptive Server autorisées. Elles sont stockées dans des tables système et peuvent être consultées au moyen de la commande sp_configure. Pour plus d'informations sur la modification des variables de configuration, reportez-vous au chapitre 5, "Définition des paramètres de configuration".

Le propriétaire de la base de données peut corriger les messages d'erreur de degré de sévérité 17 indiquant que votre espace mémoire est insuffisant. Les autres messages d'erreur de degré de sévérité 17 sont corrigés par l'administrateur système.

### Degré 18 : erreur interne non fatale détectée

Les messages de degré de sévérité 18 signalent un bug logiciel interne. Toutefois, la commande est exécutée jusqu'à son terme et la connexion à Adaptive Server est maintenue. Vous pouvez continuer votre travail en cours, mais il est possible que vous ne puissiez plus exécuter de commande spécifique. Par exemple, Adaptive Server peut détecter qu'une décision concernant le chemin d'accès à une requête particulière a été prise sans raison valable.

Les utilisateurs ont tendance à ne pas faire état des problèmes générant de tels messages car ceux-ci ne les empêchent pas de travailler normalement. Il convient donc de bien spécifier aux utilisateurs d'aviser l'administrateur système à chaque occurrence d'un message de ce degré (ou d'un degré supérieur), pour que l'administrateur système puisse établir un rapport.

## Degrés de sévérité 19 à 26

Les erreurs fatales génèrent des messages d'erreur d'un degré de sévérité de 19 et supérieur. Elles interrompent la connexion de l'utilisateur à Adaptive Server (certaines ayant des degrés de sévérité supérieurs arrêtent Adaptive Server). Pour poursuivre son travail, l'utilisateur doit relancer le programme client.

L'état du processus est bloqué avant qu'il ne s'arrête et des informations concernant ce qui s'est produit sont enregistrées. Le processus est ensuite supprimé.

Une fois la connexion de l'utilisateur interrompue, celui-ci risque de ne pas pouvoir se reconnecter et reprendre son travail. Certains des problèmes compris dans cet intervalle de degrés de sévérité concernent un seul utilisateur et un seul processus. D'autres s'appliquent, au contraire, à l'ensemble des processus de la base de données. Dans certains cas, il peut s'avérer nécessaire de redémarrer Adaptive Server. Si ces problèmes n'endommagent pas nécessairement une base de données ou les objets qui lui sont associés, cela est néanmoins une conséquence possible. Ils peuvent également résulter d'une altération antérieure de la base de données ou de ses objets. D'autres problèmes peuvent être dus à des dysfonctionnements matériels.

Une trace des messages d'erreur fatale du noyau est dirigée vers le journal d'erreurs pour pouvoir être analysée par l'administrateur système.

### Degré 19 : erreur fatale Adaptive Server au niveau des ressources

Les messages de degré de sévérité 19 indiquent qu'une limite interne non configurable a été dépassée et qu'Adaptive Server ne peut pas effectuer de reprise. Vous devez vous reconnecter à Adaptive Server.

### Degré 20 : erreur fatale Adaptive Server dans le processus en cours

Les messages de degré de sévérité 20 indiquent qu'Adaptive Server a rencontré un bug dans une commande. Ce dernier n'a affecté que le processus courant et il est peu probable que la base de données ait été endommagée. Exécutez le programme de diagnostic dbcc. Vous devez vous reconnecter à Adaptive Server.

### Degré 21 : erreur fatale Adaptive Server dans les processus de base de données

Les messages de degré de sévérité 21 indiquent qu'Adaptive Server a rencontré un bug qui concerne tous les processus de la base de données courante. Il est toutefois peu probable que la base de données proprement dite ait été endommagée. Redémarrez Adaptive Server et exécutez le programme de diagnostic dbcc. Vous devez vous reconnecter à Adaptive Server.

### Degré 22 : erreur fatale Adaptive Server : Cohérence de la table suspecte

Les messages de degré de sévérité 22 indiquent que la table ou l'index spécifiés dans le message ont été précédemment endommagés par un problème matériel ou logiciel.

La première chose à faire est de redémarrer Adaptive Server et d'exécuter dbcc pour déterminer si d'autres objets de la base sont également endommagés. Quel que soit le résultat de dbcc, il n'est pas exclu que le problème soit limité au cache et ne concerne pas le disque. Dans ce cas, le redémarrage d'Adaptive Server permet de résoudre le problème.

Si le redémarrage ne suffit pas, cela signifie que le problème s'étend au disque. Il peut parfois être résolu par la suppression de l'objet spécifié dans le message d'erreur. Par exemple, si le message indique qu'Adaptive Server a trouvé une ligne de longueur 0 dans un index non clusterisé, le propriétaire de la table peut supprimer l'index et le recréer.

Adaptive Server désactive toute page ou index qu'il trouve suspect pendant la reprise. Utilisez sp_setsuspect_granularity pour déterminer si la reprise marque comme suspectes une base de données complète ou des pages individuelles uniquement. Pour plus d'informations, reportez-vous à la commande sp_setsuspect_granularity dans le Adaptive Server - Manuel de référence.

Vous devez vous reconnecter à Adaptive Server.

### Degré 24 : erreur matérielle ou table système altérée

Ces messages d'erreur reflètent un certain type de panne de disque ou (dans de rares cas) l'altération de sysusages. L'administrateur système devra peut-être recharger la base de données. Vous pouvez également être contraint de contacter votre distributeur.

### Degré 23 : erreur fatale : cohérence de la table suspecte

Les messages de degré de sévérité 23 indiquent que la cohérence de la base de données est suspecte en raison de dommages précédemment causés par un problème matériel ou logiciel. Redémarrez Adaptive Server et exécutez le programme de diagnostic dbcc.

Même lorsqu'une erreur de degré 23 indique que toute la base de données est suspecte, il n'est pas exclu que les dommages soient limités au cache et que le disque soit intact. Dans ce cas, le redémarrage d'Adaptive Server à l'aide de startserver permet de résoudre le problème.

### Degré 25 : erreur interne Adaptive Server

Le erreurs de degré 25 ne sont pas visibles par l'utilisateur ; ce sont des erreurs Adaptive Server internes.

### Degré 26 : erreur de règle

Ces messages d'erreur indiquent qu'une règle de verrouillage ou de synchronisation interne a été enfreinte. Arrêtez et redémarrez Adaptive Server.

## Rapport d'erreurs

Lorsque vous signalez une erreur, veillez à préciser les informations suivantes :

- le numéro du message, son degré et le numéro d'état ;
- tout numéro, type ou nom d'objet de base de données inclus dans le message d'erreur ;
- le contexte dans lequel le message a été généré, c'est-à-dire le nom de la commande qui était en cours d'exécution. Une sortie imprimée de la trace du journal d'erreurs peut également être utile.

# Journalisation des erreurs Backup Server

A l'instar d'Adaptive Server, Backup Server crée un journal d'erreurs, si celui-ci n'existe pas déjà. Vous spécifiez l'emplacement du journal d'erreurs au démarrage, en définissant le paramètre *journal_erreurs* dans le fichier runserver ou sur la ligne de commande. L'utilitaire d'installation Sybase configure le fichier runserver avec *$SYBASE/install* comme emplacement du journal d'erreurs si vous ne spécifiez pas d'autre emplacement lors de l'installation. Si vous ne spécifiez aucun emplacement dans le fichier runserver ou sur la ligne de commande, le journal d'erreurs est créé dans le répertoire dans lequel vous démarrez Backup Server. Utilisez l'option backupserver -V (bcksvr -V sous Windows NT) pour limiter les messages imprimés au journal d'erreurs. Pour plus d'informations sur la manière de spécifier l'emplacement du journal d'erreurs, reportez-vous aux sections décrivant Backup Server dans le manuel *Guide Utilitaires*.

Les messages d'erreur Backup Server ont la forme suivante :

```
MMM DD YYY: Backup Server:N.N.N.N: Texte du message
```

Les numéros des messages Backup Server se composent de 4 nombres entiers séparés par des points (N.N.N.N). Les messages sous la forme N.N.N proviennent d'Open Server™.

Les quatre éléments d'un message d'erreur Backup Server sont *major.minor.severity.state* :

- L'élément *major* désigne généralement la zone fonctionnelle du code de Backup Server où l'erreur s'est produite :
  - 1 – erreurs système
  - 2 – erreurs d'événement Open Server
  - 3 – erreurs d'appel de procédure à distance Backup Server
  - 4 – erreurs des E/S de la couche service
  - 5 – erreurs de transfert de données sur le réseau
  - 6 – erreurs de gestion de volume
  - 7 – erreurs d'analyse d'option

  La plupart des erreurs des catégories 1 à 6 peuvent être des erreurs internes à Backup Server ou résulter d'un ensemble de problèmes système. Les principales erreurs de la catégorie 7 découlent presque toujours de problèmes dans les options que vous spécifiez pour une commande de sauvegarde ou de chargement.
- Les éléments *minor* sont numérotés séquentiellement au sein d'une catégorie principale.
- L'élément *severity* peut prendre l'une des valeurs suivantes :
  - 1 – informations, aucune action utilisateur n'est requise.
  - 2, 3 – une condition inattendue, potentiellement fatale pour la session, s'est produite L'erreur peut porter sur tous les points suivants (ou un seul d'entre eux) : utilisation, environnement ou logique interne.
  - 4 – une condition inattendue, fatale pour l'exécution de Backup Server, s'est produite Quittez immédiatement Backup Server.
- Les codes *state* établissent une correspondance un-pour-un avec les entrées du rapport d'erreurs dans le code. Si vous contactez le Support Technique pour des erreurs Backup Server, le code d'état détermine la cause exacte de l'erreur.

# Suppression des processus

Un processus désigne une tâche exécutée par Adaptive Server. Un numéro unique d'identification (spid) est affecté à chaque processus lorsqu'il est lancé. Ces numéros d'identification, ainsi que d'autres informations sur les processus, sont stockés dans master..sysprocesses. Les processus qui s'exécutent dans un environnement de processus parallèles créent des processus fils dont chacun possède son spid. Plusieurs processus créent et affectent des spids : démarrage d'Adaptive Server, tâches de connexion, points de reprise, tâche de gestion, etc. Vous pouvez consulter la plupart de ces informations à l'aide de la procédure système sp_who.

Lorsqu'elle est exécutée sur un serveur monomoteur, la procédure système sp_who signale le processus sp_who comme en cours d'exécution et tous les autres processus comme exécutables ou en état de veille. Sur un serveur multimoteur, il peut y avoir un processus en cours d'exécution par moteur.

La commande kill supprime un processus en cours. Le plus souvent, un processus est supprimé car il interfère avec d'autres utilisateurs et la personne responsable de son exécution n'est pas joignable. Il peut arriver qu'un processus pose des verrous bloquant l'accès aux objets de la base, mais aussi que de nombreux processus en veille occupent les connexions utilisateur. Un administrateur système peut supprimer des processus :

- en attente d'une alarme, telle qu'une commande waitfor,
- en attente d'envois ou de réceptions du réseau,
- en attente de verrou,
- en attente de messages de synchronisation d'un autre processus appartenant à une famille donnée,
- ainsi que la plupart des processus exécutables ou en cours d'exécution.

Adaptive Server permet de supprimer un processus uniquement s'il peut interrompre correctement toutes les transactions non terminées et libérer toutes les ressources système utilisées par le processus. Pour les processus appartenant à une même famille, la suppression de tout processus fils entraînera la suppression de tous les autres processus de la famille. Il est toutefois plus facile de supprimer le processus parent. Pour une famille de processus, la commande kill est détectée plus rapidement si l'état du processus fils est :

```
sync sleep
```

Le tableau 4-2 indique les valeurs rapportées par sp_who lorsque la commande kill prend effet.

***Tableau 4-2 : Valeurs d'état rapportées par sp_who***

| Etat | Indique | Effets de la commande kill |
|---|---|---|
| recv sleep | En attente de lecture réseau | Immédiat. |
| send sleep | En attente d'envoi réseau | Immédiat. |
| alarm sleep | En attente d'une alarme telle que<br>`waitfor delay "10:00"` | Immédiat. |
| lock sleep | En attente d'acquisition de verrou | Immédiat. |
| sync sleep | En attente d'un message de synchronisation d'un autre processus de la famille | Immédiat. Les autres processus de la famille doivent également être placés en état d'interruption. |
| sleeping | En attente d'E/S disque ou de toute autre ressource Indique très probablement un processus en cours d'exécution qui recourt massivement aux E/S disque | Supprimé à la reprise, effet généralement immédiat ; certains processus en veille ne reprennent pas ; il est alors nécessaire de réinitialiser le serveur pour les supprimer. |
| runnable | Dans la file d'attente des processus exécutables | Immédiat. |
| running | En cours d'exécution sur l'un des moteurs du serveur | Immédiat. |
| infected | Le serveur a détecté une condition d'erreur grave ; extrêmement rare | La commande kill n'est pas recommandée. Pour supprimer le processus, il est probablement nécessaire de redémarrer le serveur. |
| background | Processus, tel qu'une procédure associée au seuil, exécuté par Adaptive Server et non par un processus utilisateur | Immédiat ; utilisez kill avec la plus grande prudence. Il est conseillé de contrôler attentivement sysprocesses avant de supprimer un processus en arrière-plan. |
| log suspend | Processus suspendus lorsque le seuil ultime du journal a été atteint | Immédiat. |

Seul un administrateur système peut lancer la commande kill ; l'autorisation de l'exécuter ne peut pas être transférée.

La syntaxe est la suivante :

```
kill spid
```

Vous ne pouvez supprimer qu'un seul processus à la fois, mais vous pouvez exécuter une série de commandes de suppression dans un batch. Par exemple :

```
1> kill 7
2> kill 8
3> kill 9
4> go
```

Il n'est pas possible d'annuler la commande kill et elle ne peut pas être incluse dans une transaction définie par l'utilisateur. spid doit être une valeur numérique constante ; vous ne pouvez pas utiliser de variable. Voici quelques exemples de résultats générés par sp_who :

```
fid    spid       status        loginame           origname       hostname
blk          dbname
    cmd
----     -----        --------- --------                    ---------        -
------         ----         -------             -    ----------------
0    1        recv sleep       howard           howard        svr30eng    0
master
    AWAITING COMMAND
0     2        sleeping       NULL           NULL              0        master
    NETWORK HANDLER
0    3        sleeping       NULL           NULL              0        master
    DEADLOCK TUNE
0    4        sleeping       NULL           NULL              0        master
    MIRROR HANDLER
0    5        sleeping       NULL           NULL               0         master
    CHECKPOINT SLEEP
0    6        sleeping       NULL           NULL              0        master
    HOUSEKEEPER
0    7      recv sleep      bill          bill      bigblue      0      master
    AWAITING COMMAND
0    8    recv sleep        wilbur         wilbur      hazel      0      master
    AWAITING COMMAND
0    9    recv sleep        joan          joan      luv2work      0      master
    AWAITING COMMAND
0    10    running         foote          foote       svr47hum    0      master
    SELECT
(10 rows affected, return status = 0)
```

Dans l'exemple ci-dessus, les processus 2 à 6 ne peuvent pas être supprimés : il s'agit de processus système. Le nom de login NULL et l'absence de nom d'hôte les identifient clairement comme processus système. Ils sont toujours accompagnés des indications NETWORK HANDLER, MIRROR HANDLER, HOUSEKEEPER et CHECKPOINT SLEEP (plus rarement, CHECKPOINT). AUDIT PROCESS est activé si vous activez le système d'audit.

Les processus 1, 8, 9 et 10 peuvent être supprimés puisqu'ils ont les valeurs d'état suivantes : "recv sleep", "send sleep", "alarm sleep" et "lock sleep".

Dans les résultats générés par sp_who , il est impossible de savoir si un processus à l'état "recv sleep" appartient à un utilisateur d'Adaptive Server et s'est interrompu momentanément pour examiner les résultats d'une commande ou s'il indique qu'un utilisateur a redémarré un PC ou tout autre terminal et a laissé un processus en attente. Pour obtenir plus d'informations sur la signification de l'état d'un processus, vous devez interroger la table sysprocesses. Par exemple, la requête suivante indique l'ID du processus hôte et le logiciel client utilisé par le processus 8 :

```
select hostprocess, program_name
    from sysprocesses
where spid = 8
hostprocess program_name
 ----------- ----------------
 3993        isql
```

Associée aux informations sur l'utilisateur et l'hôte renvoyées par sp_who, cette requête fournit des informations supplémentaires pour rechercher le processus au niveau du système d'exploitation.

## Utilisation de *sp_lock* pour l'examen des processus bloquants

En complément à sp_who, la procédure système sp_lock permet d'identifier les processus qui bloquent d'autres processus. Si la colonne blk dans le rapport sp_who indique qu'un autre processus est bloqué en attente d'acquisition de verrous, sp_lock donne des informations sur le processus bloquant. Par exemple, dans le résultat sp_who ci-dessus, le processus 10 est bloqué par le processus 7. Pour afficher des informations sur ce dernier, lancez :

```
sp_lock 7
```

Pour plus d'informations sur le verrouillage dans Adaptive Server, reportez-vous au document *Performances et optimisation*.

# Configuration d'Adaptive Server pour la sauvegarde du texte des batchs SQL

Il arrive qu'une requête ou une procédure provoque la suspension d'Adaptive Server Monitor. Les utilisateurs qui disposent du rôle d'administrateur système peuvent configurer Adaptive Server pour qu'il permette à Adaptive Server Monitor d'accéder au texte de l'instruction SQL en batch qui est en cours d'exécution. Dans le cas de batchs à exécution longue, l'affichage du texte SQL peut vous aider à déboguer les processus suspendus ou à optimiser les instructions longues, particulièrement consommatrices de ressources.

Adaptive Server doit être configuré pour collecter le texte des instructions SQL en batch et pour l'enregistrer dans la mémoire partagée, où il peut être lu par Adaptive Server Monitor Server (le composant serveur d'Adaptive Server Monitor). La demande cliente peut émaner de Monitor Viewer, module de connexion de Sybase Central, ou d'autres applications Adaptive Server Monitor Server.

La configuration d'Adaptive Server pour qu'il sauvegarde le texte des instructions SQL en batch permet, en outre, de visualiser le plan d'exécution de requête en cours au format showplan (comme si vous activiez l'option showplan). Pour visualiser le plan d'exécution de requête en cours à partir d'Adaptive Server, reportez-vous à la section "Affichage du plan d'exécution de requête d'une instruction SQL", page 75. Les batchs SQL peuvent uniquement être affichés via Adaptive Server Monitor Server. Pour plus d'informations sur l'affichage du texte des instructions en batch, reportez-vous à la documentation Adaptive Server Monitor Server.

Comme la requête ou la procédure affichée peut être imbriquée dans un batch d'instructions SQL, la table sysprocesses inclut désormais des colonnes correspondant au numéro de ligne, au numéro d'instruction et au spid de l'instruction suspendue, pour vous permettre de visualiser le plan d'exécution de requête.

Adaptive Server n'étant pas configuré par défaut pour sauvegarder le texte des instructions SQL en batch, vous devez le configurer pour qu'il alloue de la mémoire à cette fonction. L'accès d'Adaptive Server Monitor à SQL n'a aucun impact sur les performances si vous n'avez pas alloué une partie de la mémoire à la sauvegarde des instructions SQL en batch.

## Allocation de mémoire au texte des batchs

Vous pouvez définir la quantité de texte SQL en batch que vous voulez sauvegarder. Une fois que la sauvegarde du texte est activée, Adaptive Server copie tous les nouveaux batchs de texte SQL dans la mémoire qu'il partage avec SQL Server Monitor. Comme tout nouveau batch libère la mémoire pour la connexion et remplace le batch précédent, vous ne pouvez visualiser que les instructions SQL en cours d'exécution. Pour sauvegarder le texte SQL, conformez-vous aux étapes suivantes :

1 Configurez la quantité de texte SQL pouvant être stocké en mémoire (reportez-vous à la section "Configurez la quantité de texte SQL pouvant être stocké en mémoire.", page 71).

2 Activez SQL Server pour qu'il sauvegarde le texte SQL (reportez-vous à la section "Activation d'Adaptive Server pour démarrer la sauvegarde du texte SQL", page 73).

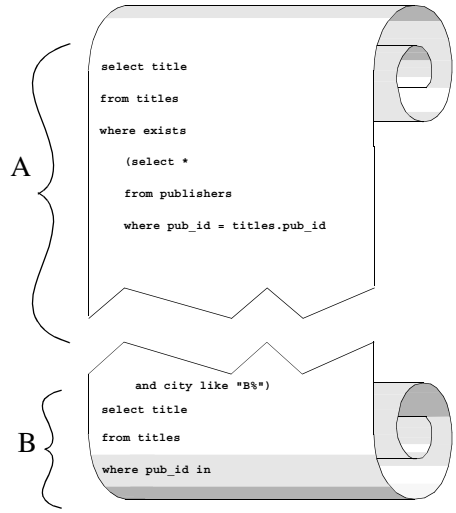
**Remarque** Vous devez disposer des autorisations d'administrateur système (SA) pour configurer et sauvegarder le texte des instructions SQL en batch.

### Configurez la quantité de texte SQL pouvant être stocké en mémoire.

Après l'installation, vous devez déterminer la quantité maximale de texte SQL pouvant être copié dans la mémoire partagée. Lorsque vous déterminez la quantité de mémoire à réserver par utilisateur, tenez compte des remarques suivantes :

- Les batchs SQL qui dépassent la quantité de mémoire allouée sont tronqués sans préavis. Cela signifie que si vous n'avez pas alloué suffisamment de mémoire aux instructions en batch, le texte qui vous intéresse peut se trouver dans la partie du batch qui a été tronquée, comme l'illustre la figure 4-2.

***Figure 4-2 : Troncature du texte SQL si la mémoire réservée est insuffisante***




Par exemple, si vous configurez Adaptive Server pour qu'il sauvegarde la quantité de texte désignée par l'accolade A dans l'illustration, mais que l'instruction en cours d'exécution se trouve dans le texte désigné par l'accolade B, Adaptive Server n'affichera pas cette instruction.

- Plus l'espace réservé au texte SQL dans la mémoire partagée est important, moins il y a de risques que l'instruction qui vous intéresse soit tronquée dans le batch copié en mémoire partagée. Toutefois, Adaptive Server rejette immédiatement les valeurs très élevées car elles ne laissent pas suffisamment de place aux caches de données et de procédures.

Il est recommandé d'utiliser une valeur initiale de 1024 octets par connexion utilisateur.

Utilisez sp_configure avec le paramètre de configuration max SQL text monitored pour allouer une partie de la mémoire partagée :

```
sp_configure "max SQL text monitored", octets_par_connexion
```

où *octets_par_connexion* (nombre maximal d'octets sauvegardés pour chaque connexion cliente) est compris entre 0 (valeur par défaut) et 2 147 483 647 (limite théorique).

Comme il alloue de la mémoire au texte SQL lors du démarrage, Adaptive Server doit être redémarré pour que ce paramètre prenne effet.

L'espace total alloué au texte SQL en mémoire partagée est le produit du nombre d'*octets_par_connexion* par le nombre de connexions utilisateur actuellement configurées.

### Activation d'Adaptive Server pour démarrer la sauvegarde du texte SQL

Une fois que vous avez alloué une partie de la mémoire partagée au texte SQL, Adaptive Server sauvegarde une copie de chaque batch SQL chaque fois que vous activez un résumé des événements Adaptive Server Monitor qui comporte des batchs SQL.

Vous pouvez en outre être appelé à reconfigurer l'intervalle entre deux balayages du buffer d'événements d'Adaptive Server Monitor pour le texte SQL. Pour plus d'informations, reportez-vous à la documentation Adaptive Server Monitor.

## Commandes SQL non représentées par du texte

Si vous utilisez des fonctions Client-Library™ non représentées par du texte, telles que ct_cursor ou ct_dynamic pour lancer des commandes SQL, Client-Library code les informations pour augmenter les performances et Adaptive Server décode et affiche généralement les informations élémentaires sur les commandes. Par exemple, si vous ouvrez un curseur avec ct_cursor alors que la commande est en cours d'exécution, le résumé des événements Adaptive Server Monitor affiche le nom de ce curseur et l'instruction de déclaration qui lui est associée.

Le tableau 4-3 répertorie toutes les fonctions Client-Library non représentées par du texte.

***Tableau 4-3 : Commandes SQL non représentées par du texte***

| Routine Client-Library | Routine DB-Library | Nom de présentation | Données de présentation |
|---|---|---|---|
| ct_cursor | N/A | CLOSE_CURSOR | Nom du curseur, instruction |
| ct_cursor | N/A | DECLARE_CURSOR | Nom du curseur, instruction |
| ct_cursor | N/A | DELETE_AT_CURSOR | Nom du curseur, instruction |
| ct_cursor | N/A | FETCH_CURSOR | Nom du curseur, instruction |
| ct_fetch (lors du traitement du résultat de ct_cursor) | N/A | FETCH_CURSOR | Nom du curseur, instruction |
| ct_cursor CURSOR_ROWS ou ct_cancel lorsque la connexion comporte des curseurs Client-Library | N/A | CURSOR_INFO | Nom du curseur, instruction |
| ct_cursor | N/A | OPEN_CURSOR | Nom du curseur, instruction |
| ct_cursor | N/A | UPDATE_AT_CURSOR | Nom du curseur, instruction |
| ct_command(CS_RPC_CMD) (comportement par défaut) | dbrpcinit (uniquement dans la version 10.0.1 ou ultérieure) | DBLIB_RPC | Nom de l'appel de procédure à distance (RPC) |
| ct_dynamic | N/A | DYNAMIC_SQL | Nom de l'instruction dynamique, instruction |
| ct_command(CS_MSG_CMD) | N/A | MESSAGE | Aucun |
| ct_param | dbrpcparam | PARAM_FORMAT | Aucun |
| ct_param | dbrpcparam | PARAMS | Aucun |
| ct_command(CS_RPC_CMD) (uniquement lorsqu'une version de TDS inférieure à la version 5.0 est utilisée) | dbrpcparam (dans les versions de DB-Library inférieures à la 10.0.1) | RPC | Nom de l'appel de procédure à distance (RPC) |

Pour plus d'informations sur les commandes SQL non représentées par du texte, reportez-vous à votre documentation Open Client.

## Affichage du plan d'exécution de requête d'une instruction SQL

Utilisez la procédure système sp_showplan et le *spid* de la connexion utilisateur concernée pour rechercher le plan d'exécution de requête associé à l'instruction actuellement exécutée sur cette connexion. Vous pouvez également utiliser sp_showplan pour visualiser le plan d'exécution de requête associé à une instruction précédente du même batch.

La syntaxe est la suivante :

```
declare @batch int
declare @context int
declare @statement int
execute sp_showplan <spid_value>, @batch_id= @batch output,
@context_id= @context output, @stmt_num=@statement output
```

où *id_batch* désigne le numéro unique d'un batch, *id_contexte* le numéro unique de chaque procédure (ou trigger) exécutée dans le batch et *num_inst*, le numéro de l'instruction en cours dans le batch. Adaptive Server utilise l'ID de batch pour synchroniser le plan d'exécution de requête avec le texte du batch et les autres données récupérées par Adaptive Server Monitor.

---

**Remarque** Vous devez être administrateur système pour pouvoir exécuter sp_showplan.

---

Par exemple, si vous souhaitez visualiser le plan de requête associé à l'instruction en cours pour spid 99 :

```
declare @batch int
declare @context int
declare @statement int
exec sp_showplan 99, @batch output, @context output, @statement output
```

Vous pouvez exécuter la procédure du plan d'exécution de requête indépendamment d'Adaptive Server Monitor et ce, qu'Adaptive Server ait alloué ou non une partie de la mémoire partagée au texte SQL.

### Affichage des instructions précédentes

Pour afficher le plan d'exécution de requête de l'instruction précédente du même batch, lancez sp_showplan avec les mêmes valeurs que pour la requête initiale, mais avec un numéro d'instruction inférieur d'une unité. Cette méthode permet de visualiser toutes les instructions du batch, jusqu'à la requête numéro un.

## Affichage d'une procédure imbriquée

Bien que sp_showplan permette d'afficher le plan d'exécution de requête associé à l'instruction en cours, l'instruction effectivement exécutée peut se trouver dans une procédure (ou une chaîne de procédures imbriquées) appelée à partir du batch SQL initial. Le tableau 4-4 montre les colonnes de sysprocesses contenant des informations sur ces instructions imbriquées.

***Tableau 4-4 : Colonnes ajoutées à sysprocesses***

| Colonne | Type de données | Spécifie |
|---|---|---|
| *id* | Nombre entier | l'ID d'objet de la procédure en cours d'exécution (ou 0 si aucune procédure n'est active) |
| *stmtnum* | Nombre entier | le numéro de l'instruction en cours au sein de la procédure active (ou le numéro de l'instruction SQL en batch si aucune procédure n'est active) |
| *linenum* | Nombre entier | le numéro de ligne de l'instruction en cours au sein de la procédure stockée active (ou le numéro de ligne de l'instruction SQL en batch en cours si aucune procédure n'est active) |

Ces informations sont sauvegardées dans sysprocesses, que le texte SQL soit activé ou que de la mémoire lui ait été allouée ou non.

Pour afficher les colonnes id, stmtnum et linenum, entrez :

```
select id, stmtnum, linenum
from sysprocesses
where spid = spid_of_hung_session
```

**Remarque** Vous n'avez pas besoin de disposer du rôle sa_role pour exécuter cette instruction select.

# Arrêt des serveurs

Un administrateur système peut arrêter Adaptive Server ou Backup Server à l'aide de la commande shutdown. La syntaxe est la suivante :

shutdown [*nom_backup_server*] [with {wait|nowait}]

La valeur par défaut de la commande shutdown est with wait. Autrement dit, les commandes shutdown et shutdown with wait sont équivalentes.

## Arrêt Adaptive Server

Si vous n'indiquez pas de nom de serveur, shutdown arrête l'Adaptive Server en cours d'utilisation. Lorsque vous lancez une commande shutdown, Adaptive Server :

1 désactive tous les logins, sauf celui des administrateurs système ;

2 exécute un point de reprise dans chaque base de données et transfère toutes les pages modifiées de la mémoire sur le disque ;

3 attend la fin de l'exécution des procédures et instructions SQL en cours.

Ainsi, shutdown limite la durée de la reprise automatique au redémarrage d'Adaptive Server.

L'option with nowait arrête Adaptive Server immédiatement. Les processus utilisateur sont annulés et la reprise peut s'avérer plus longue après une commande shutdown with nowait. Pour réduire le temps nécessaire à la reprise, exécutez une commande checkpoint avant toute commande shutdown with nowait.

## Arrêt d'un Backup Server

Pour arrêter un Backup Server, indiquez son nom :

```
shutdown SYB_BACKUP
```

Par défaut, cette commande a l'option with wait. Ainsi, toutes les sauvegardes et restaurations en cours sont menées à bien avant l'arrêt de Backup Server. En revanche, dès lors que vous exécutez une commande shutdown, aucune nouvelle session de sauvegarde ou de restauration ne peut être lancée sur Backup Server.

Pour consulter le nom des Backup Server accessibles à partir de votre Adaptive Server, lancez sp_helpserver. Utilisez la valeur figurant dans la colonne name de la commande shutdown. Vous pouvez arrêter uniquement un Backup Server qui figure :

- dans sysservers sur votre Adaptive Server et
- dans votre fichier d'interface local.

Pour ajouter un Backup Server à sysservers, utilisez la commande sp_addserver.

## Recherche des sauvegardes et restaurations actives

Pour contrôler l'activité de votre Backup Server avant d'exécuter la commande shutdown, lancez sp_who sur Backup Server :

```
                        SYB_BACKUP...sp_who
spid   status   loginame hostname   blk cmd
------ -------- -------- ---------- --- ----------------
     1 sleeping NULL     NULL       0   CONNECT HANDLER
     2 sleeping NULL     NULL       0   DEFERRED HANDLER
     3 runnable NULL     NULL       0   SCHEDULER
     4 runnable NULL     NULL       0   SITE HANDLER
     5 running  sa       heliotrope 0   NULL
```

## Utilisation de *nowait* sur Backup Server

La commande shutdown *backup_server* with nowait arrête Backup Server et ce, quelle que soit l'activité en cours. Utilisez cette commande uniquement en cas de problème grave. En effet, vos sauvegardes et restaurations risqueraient d'être incomplètes ou incohérentes.

Si vous utilisez shutdown with nowait pendant la sauvegarde d'un journal ou d'une base de données, assurez-vous que le message indiquant que la sauvegarde a abouti s'affiche effectivement. Si ce message ne s'affiche pas, ou si vous avez un doute, vous devez exécuter la commande dump database avant de procéder à toute sauvegarde de transactions. Ainsi, vous aurez la certitude de ne pas utiliser de sauvegardes incohérentes.

Si vous utilisez shutdown with nowait pendant une restauration et que vous ne recevez aucun message confirmant l'exécution complète de cette restauration, vous risquez de ne pas pouvoir émettre d'autres commandes load transaction sur la base de données. Exécutez un contrôle complet de la cohérence de la base (dbcc) avant de l'utiliser. Le cas échéant, vous devez émettre l'ensemble des commandes de restauration, en commençant par load database.

# Informations sur les problèmes connus

Les Notes de mise à jour sont une source précieuse d'informations sur les problèmes connus ou les incompatibilités avec Adaptive Server et Backup Server. Il est conseillé de les consulter à l'avance, afin de réduire la perte de temps et le travail de recherche liés à la résolution de problèmes déjà connus.

Le programme d'installation d'Adaptive Server installe également des fichiers qui répertorient tous les rapports relatifs aux problèmes système (SPR) et aux problèmes résolus (CPR) pour Adaptive Server. Les rapports relatifs aux problèmes sont organisés par zones fonctionnelles du produit. Par exemple, il existe deux fichiers relatifs à Backup Server : l'un, *cpr_bus*, contient une liste de rapports relatifs aux problèmes résolus et l'autre, *spr_bus*, une liste de rapports relatifs aux problèmes non résolus.

Reportez-vous aux Notes de mise à jour pour connaître l'emplacement des fichiers CPR et SPR.

CHAPITRE 5

# Définition des paramètres de configuration

Ce chapitre décrit les paramètres de configuration d'Adaptive Server. Un paramètre de configuration est un paramètre que vous définissez avec la procédure système sp_configure. Les paramètres de configuration sont utilisés pour de nombreux services, depuis les opérations de base jusqu'aux opérations spécifiques du serveur, et pour optimiser les performances.

## Paramètres de configuration d'Adaptive Server

Le tableau suivant contient une liste alphabétique des paramètres de configuration d'Adaptive Server.

| Paramètres de configuration |
|---|
| "abstract plan cache", page 192 |
| "abstract plan dump", page 192 |
| "abstract plan load", page 193 |
| "abstract plan replace", page 193 |
| "additional network memory", page 184 |
| "allow backward scans", page 193 |
| "allow nested triggers", page 194 |
| "allow procedure grouping", page 233 |
| "allow remote access", page 164 |
| "allow resource limits", page 195 |
| "allow sendmsg", page 164 |
| "allow sql server async i/o", page 120 |
| "allow resource limits", page 195 |
| "allow updates to system tables", page 195 |
| "auditing", page 234 |
| "audit queue size", page 234 |

| Paramètres de configuration |
|---|
| "cis bulk insert array size", page 115 |
| "cis bulk insert batch size", page 115 |
| "cis connect timeout", page 116 |
| "cis cursor rows", page 116 |
| "cis packet size", page 117 |
| "cis rpc handling", page 118 |
| "configuration file", page 140 |
| "cpu accounting flush interval", page 197 |
| "cpu grace time", page 198 |
| "current audit table", page 236 |
| "deadlock checking period", page 148 |
| "deadlock retries", page 149 |
| "default character set id", page 144 |
| "default database size", page 199 |
| "default exp_row_size percent", page 201 |
| "default fill factor percent", page 200 |
| "default language id", page 144 |
| "default network packet size", page 165 |
| "default sortorder id", page 145 |
| "default unicode sortorder", page 243 |
| "disable character set conversions", page 145 |
| "disk i/o structures", page 121 |
| "dtm detach timeout period", page 125 |
| "dtm lock timeout period", page 125 |
| "dump on conditions", page 202 |
| "enable full-text search", page 119 |
| "enable cis", page 118 |
| "enable DTM", page 127 |
| "enable housekeeper GC", page 208 |
| "enable HA", page 207 |
| "enable java", page 141 |
| "enable enterprise java beans", page 142 |
| "enable file access", page 119 |
| "enable full-text search", page 119 |
| "enable rep agent threads", page 191 |
| "enable ssl", page 237 |
| "enable sort-merge joins and JTC", page 202 |

| Paramètres de configuration |
| --- |
| "enable surrogate processing", page 243 |
| "enable unicode conversion", page 244 |
| "enable unicode normalization", page 244 |
| "enable xact coordination", page 127 |
| "esp execution priority", page 137 |
| "esp execution stacksize", page 137 |
| "esp unload dll", page 138 |
| "event buffers per engine", page 204 |
| "event log computer name (Windows NT seulement)", page 134 |
| "event logging (Windows NT seulement)", page 135 |
| "executable codesize + overhead", page 155 |
| "global async prefetch limit", page 109 |
| "global cache partition number", page 110 |
| "housekeeper free write percent", page 205 |
| "i/o accounting flush interval", page 211 |
| "i/o polling process count", page 212 |
| "identity burning set factor", page 209 |
| "identity grab size", page 210 |
| "license information", page 232 |
| "lock address spinlock ratio", page 146 |
| "lock hashtable size", page 151 |
| "lock shared memory", page 186 |
| "lock scheme", page 152 |
| "lock spinlock ratio", page 150 |
| "lock table spinlock ratio", page 154 |
| "lock wait period", page 153 |
| "log audit logon failure", page 136 |
| "log audit logon success", page 136 |
| "max async i/os per engine", page 173 |
| "max async i/os per server", page 174 |
| "max cis remote connections", page 119 |
| "max network packet size", page 166 |
| "max number network listeners", page 169 |
| "max online engines", page 189 |
| "max parallel degree", page 178 |
| "max scan parallel degree", page 179 |
| "max SQL text monitored", page 187 |

| Paramètres de configuration |
| --- |
| "maximum dump conditions", page 216 |
| "memory alignment boundary", page 110 |
| "memory per worker process", page 180 |
| "msg confidentiality reqd", page 237 |
| "msg integrity reqd", page 238 |
| "number of alarms", page 216 |
| "number of aux scan descriptors", page 217 |
| "number of devices", page 122 |
| "number of dtx participants", page 128 |
| "number of index trips", page 111 |
| "number of large i/o buffers", page 104 |
| "number of locks", page 147 |
| "number of mailboxes", page 220 |
| "number of messages", page 220 |
| "number of oam trips", page 112 |
| "number of open databases", page 155 |
| "number of open indexes", page 158 |
| "number of open objects", page 159 |
| "number of pre-allocated extents", page 221 |
| "number of remote connections", page 169 |
| "number of remote logins", page 170 |
| "number of remote sites", page 170 |
| "number of sort buffers", page 222 |
| "number of user connections", page 245 |
| "number of worker processes", page 178 |
| "open index hash spinlock ratio", page 161 |
| "open index spinlock ratio", page 162 |
| "open object spinlock ratio", page 163 |
| "o/s file descriptors", page 176 |
| "page lock promotion HWM", page 213 |
| "page lock promotion LWM", page 214 |
| "page lock promotion PCT", page 215 |
| "page utilization percent", page 123 |
| "partition groups", page 222 |
| "partition spinlock ratio", page 223 |
| "permission cache entries", page 248 |
| "print deadlock information", page 224 |

| Paramètres de configuration |
| --- |
| "print recovery information", page 105 |
| "procedure cache size", page 113 |
| "read committed with lock", page 153 |
| "recovery interval in minutes", page 106 |
| "remote server pre-read packets", page 171 |
| "row lock promotion HWM", page 230 |
| "row lock promotion LWM", page 231 |
| "row lock promotion PCT", page 232 |
| "runnable process search count", page 224 |
| "secure default login", page 238 |
| "select on syscomments.text column", page 239 |
| "shared memory starting address", page 176 |
| "size of auto identity column", page 225 |
| "size of global fixed heap", page 142 |
| "size of process object heap", page 143 |
| "size of shared class heap", page 143 |
| "size of unilib cache", page 245 |
| "SQL Perfmon Integration (Windows NT uniquement)", page 226 |
| "sql server clock tick length", page 227 |
| "stack guard size", page 249 |
| "stack size", page 251 |
| "start mail session (Windows NT seulement)", page 138 |
| "strict dtm enforcement", page 130 |
| "suspend audit when device full", page 240 |
| "syb_sendmsg port number", page 171 |
| "systemwide password expiration", page 241 |
| "lock table spinlock ratio", page 154 |
| "tape retention in days", page 108 |
| "tcp no delay", page 172 |
| "text prefetch size", page 228 |
| "time slice", page 228 |
| "total data cache size", page 114 |
| "total logical memory", page 188 |
| "txn to pss ratio", page 131 |
| "unified login required (Windows NT uniquement)", page 242 |
| "upgrade version", page 229 |
| "user log cache size", page 252 |

| Paramètres de configuration |
| --- |
| "user log cache spinlock ratio", page 254 |
| "use security services (Windows NT uniquement)", page 242 |
| "xact coordination interval", page 132 |
| "xp_cmdshell context", page 139 |

# Présentation des paramètres de configuration

Les paramètres de configuration sont des paramètres définis par l'utilisateur qui contrôlent les différents aspects du fonctionnement d'Adaptive Server. Adaptive Server affecte une valeur par défaut à chaque paramètre de configuration. Vous pouvez utiliser les paramètres de configuration pour adapter Adaptive Server aux besoins particuliers d'une installation.

Lisez attentivement ce chapitre pour déterminer les paramètres de configuration que vous allez devoir modifier pour optimiser les performances du serveur. Reportez-vous également au document *Performances et optimisation* pour plus d'informations sur l'utilisation de sp_configure pour optimiser Adaptive Server.

**Avertissement !** Soyez prudent lorsque vous modifiez les paramètres de configuration. Des changements arbitraires des valeurs des paramètres peuvent affecter les performances d'Adaptive Server et d'autres aspects de son fonctionnement.

## Fichier de configuration d'Adaptive Server

Adaptive Server conserve les valeurs des paramètres de configuration dans un fichier de configuration au format texte ASCII. Lorsque vous installez un nouvel Adaptive Server, les paramètres prennent leurs valeurs par défaut, le nom par défaut du fichier est *server_name.cfg* et celui-ci se trouve dans le répertoire d'installation de Sybase ($SYBASE). Lorsque vous modifiez un paramètre de configuration, Adaptive Server enregistre une copie de l'ancien fichier de configuration sous le nom *server_name.001*, *server_name.002* etc. Adaptive Server écrit les nouvelles valeurs dans le fichier *server_name.cfg* ou dans un fichier dont vous avez précisé le nom au démarrage.

## Comment modifier les paramètres de configuration

Les méthodes suivantes permettent de définir ou de modifier les paramètres de configuration :

- Exécution de la procédure système sp_configure avec les paramètres et les valeurs appropriés,
- Edition du fichier de configuration puis appel de sp_configure avec l'option configuration file ou
- Spécification du nom d'un fichier de configuration au démarrage.

Les paramètres de configuration sont *dynamiques* ou *statiques*. Les paramètres dynamiques sont appliqués dès que vous exécutez sp_configure. Les paramètres statiques ne prennent effet qu'après avoir redémarré Adaptive Server, car il doit leur réallouer de la mémoire. La description de chaque paramètre indique s'il est statique ou dynamique. Adaptive Server écrit la nouvelle valeur dans la table système sysconfigures et dans le fichier de configuration lorsque vous modifiez la valeur, pas quand vous redémarrez Adaptive Server. Le fichier de configuration courant et sysconfigures reflètent les valeurs configurées et non pas les valeurs d'exécution. La table système syscurconfigs reflète les valeurs d'exécution courantes des paramètres de configuration.

## Qui a le droit de modifier les paramètres de configuration

Les rôles nécessaires pour pouvoir utiliser sp_configure sont les suivants :

- Tout utilisateur peut exécuter sp_configure pour afficher des informations sur les paramètres et leur valeur courante.
- Seul l'administrateur système et le responsable de la sécurité du système peuvent exécuter sp_configure pour modifier des paramètres de configuration.
- Seul un responsable de la sécurité du système peut exécuter sp_configure pour modifier des valeurs de :

| | |
|---|---|
| • allow procedure grouping | • secure default login |
| • allow updates to system tables | • select on syscomments.text column |
| • auditing | • suspend audit when device full |
| • audit queue size | • systemwide password expiration |
| • current audit table | • unified login required (Windows NT uniquement) |

| | |
|---|---|
| • msg confidentiality reqd | • use security services (Windows NT uniquement) |
| • msg confidentiality reqd | • secure default login |
| • msg integrity reqd | • select on syscomments.text column |
| • allow procedure grouping | • suspend audit when device full |
| • allow updates to system tables | • systemwide password expiration |
| • auditing | • unified login required (Windows NT uniquement) |
| • audit queue size | • use security services (Windows NT uniquement) |
| • current audit table | • pour activer la sécurité basée sur une session SSL |
| • msg confidentiality reqd | |
| • allow remote access | |
| • allow remote access | |

## Spécification de l'unité avec sp_configure

sp_configure vous permet d'indiquer la valeur des paramètres de configuration dans les spécificateurs d'unité. Les spécificateurs d'unité sont p ou P pour les pages, m ou M pour les mégaoctets et g ou G pour les gigaoctets. Si vous n'indiquez aucune unité lorsque vous configurez un paramètre qui contrôle la mémoire, Adaptive Server utilise la taille de la page logique comme unité de base.

La syntaxe utilisée pour indiquer une unité particulière est la suivante :

```
sp_configure "parameter name", 0, "p|P|k|K|m|M|g|G"
```

Vous devez inclure le "0" comme marque de réservation.

Lorsque vous configurez à 100 Mo max memory pour un serveur qui utilise des pages de 2 Ko, la syntaxe est :

```
sp_configure "max memory", 51200
```

Cependant, vous pouvez également définir max memory pour ce serveur à 100 Mo à l'aide de la spécification d'unité "m" en tapant :

```
sp_configure "max memory", 0, "100m"
```

Vous pouvez utiliser cette spécification d'unité pour configurer n'importe quel paramètre. Pour définir number of locks à 1024, par exemple, vous pouvez saisir :

```
sp_configure "number of locks", 1024
```

ou :

```
sp_configure "number of locks", 0, 1K
```

Cette fonctionnalité ne modifiera pas la manière dont Adaptive Server affiche le résultat de sp_configure.

## Obtention d'aide sur les paramètres de configuration

Vous pouvez utiliser sp_helpconfig ou sp_configure pour obtenir des informations sur un paramètre de configuration donné. Exemple :

```
sp_helpconfig "number of open"
Configuration option is not unique.
option_name                    config_value run_value
------------------------------ ------------ -----------
number of open databases                12          12
number of open indexes                 500         500
number of open objects                 500         500

sp_helpconfig "number of open indexes"
number of open indexes sets the maximum number of indexes that can be open at
one time on SQL Server. The default value is 500.
Minimum Value Maximum Value Default Value Current Value Memory Used
------------- ------------- ------------- ------------- -----------
          100    2147483647           500           500         208

sp_configure "number of open indexes"
Parameter Name           Default  Memory Used  Config Value  Run Value
-----------------------  -------  -----------  ------------  ---------
number of open indexes       500          208           500        500
```

Pour plus d'informations, reportez-vous à la section "Utilisation de sp_helpconfig pour obtenir de l'aide sur les paramètres de configuration", page 624.

# Utilisation de *sp_configure*

sp_configure affiche et réinitialise les paramètres de configuration. Vous pouvez limiter le nombre de paramètres affichés par sp_configure en utilisant sp_displaylevel pour définir le niveau d'affichage à l'une des trois valeurs :

- Basic
- Intermediate
- Comprehensive

Pour plus d'informations sur les niveaux d'affichage, reportez-vous à la section "Sous-ensembles définis par l'utilisateur de la hiérarchie des paramètres : Niveaux d'affichage", page 99. Pour plus d'informations sur sp_displaylevel, reportez-vous au document *Manuel de référence d'Adaptive Server*.

Le tableau 5-1 décrit la syntaxe de sp_configure. Les informations dans la colonne "Effet" supposent que votre niveau d'affichage est "comprehensive".

***Tableau 5-1 : syntaxe de sp_configure***

| Commande | Effet |
|---|---|
| sp_configure | Affiche les paramètres de configuration par groupe, leurs valeurs courantes et par défaut, la dernière valeur à laquelle ils ont été définis et la quantité de mémoire utilisée par cette définition. |
| sp_configure "*paramètre*" | Affiche la valeur courante, la valeur par défaut, la dernière valeur modifiée et la quantité de mémoire utilisée par la définition de tous les paramètres correspondant à paramètre. |
| sp_configure "*paramètre*", *valeur* | Réaffecte *valeur* à *paramètre*. |
| sp_configure "*paramètre*", 0, "default" | Rétablit la valeur par défaut d'un paramètre. |
| sp_configure "*nom_groupe*" | Affiche tous les paramètres de configuration de *nom_groupe*, leurs valeurs courantes et par défaut, la dernière valeur à laquelle ils ont été définis ainsi que la quantité de mémoire utilisée par chaque définition. |
| sp_configure "configuration file", 0, "*sous_commande*", "*nom_fichier*" | Définit les paramètres de configuration à partir du fichier de configuration. Voir "Utilisation de sp_configure avec un fichier de configuration", page 91 pour les descriptions des paramètres. |

## Eléments de syntaxe

Les variables suivantes sont utilisées dans le tableau 5-1 :

- *paramètre* – désigne tout paramètre ou sous-chaîne de configuration Adaptive Server correct(e).
- *valeur* – désigne tous nombre entier dans la plage des valeurs autorisées pour ce paramètre (reportez-vous aux descriptions de chacun des paramètres pour connaître les valeurs autorisées). Les paramètres de type logique ne peuvent prendre que deux valeurs : 1 (activé) et 0 (désactivé).
- *nom_groupe* – indique le nom de tout groupe dans la hiérarchie des paramètres.

### Analyse des paramètres

sp_configure interprète chaque paramètre (et fragment de nom de paramètre) comme un "*%paramètre%*". Une chaîne qui n'identifie pas un paramètre donné de manière unique renvoie des valeurs pour tous les paramètres qui correspondent à la chaîne. Exemple :

```
sp_configure "lock"
```

renvoie les valeurs de tous les paramètres de configuration qui contiennent "verrou", comme lock shared memory, number of locks, lock promotion HWM, server clock tick length, print deadlock information et deadlock retries.

---

**Remarque** Si vous essayez de définir une valeur en utilisant un fragment de nom de paramètre qui n'est pas unique, sp_configure renvoie les valeurs courantes de tous les paramètres qui correspondent au fragment et vous demande un nom de paramètre unique.

---

## Utilisation de *sp_configure* avec un fichier de configuration

Vous pouvez configurer Adaptive Server de manière interactive en utilisant sp_configure comme décrit ci-dessus, ou alors de manière non interactive en demandant à Adaptive Server de lire les valeurs d'une version modifiée ou restaurée du fichier de configuration.

L'utilisation des fichiers de configuration présente les avantages suivants :

- Vous pouvez dupliquer une configuration spécifique sur plusieurs serveurs en utilisant le même fichier de configuration.
- Vous pouvez utiliser un fichier de configuration comme référence pour tester différentes valeurs de configuration sur votre serveur.
- Vous pouvez utiliser un fichier de configuration pour effectuer un contrôle de validation des valeurs des paramètres avant de les attribuer pour de bon.
- Vous pouvez créer plusieurs fichiers de configuration et passer de l'un à l'autre en fonction des ressources nécessaires.

Vous pouvez créer une copie du fichier de configuration en utilisant sp_configure avec le paramètre "configuration file" puis modifier le fichier au niveau du système d'exploitation. Vous pouvez ensuite utiliser sp_configure avec le paramètre "configuration file" pour ordonner à Adaptive Server de lire les valeurs dans le fichier modifié. Vous pouvez également spécifier le nom du fichier de configuration au démarrage.

Pour plus d'informations sur la modification du fichier, reportez-vous à la section "Edition du fichier de configuration", page 95. Pour plus d'informations sur la spécification du nom du fichier de configuration au démarrage, reportez-vous à la section "Lancement d'Adaptive Server avec un fichier de configuration", page 96.

## Conseils pour nommer le fichier de configuration

A chaque fois que vous modifiez un paramètre de configuration avec sp_configure, Adaptive Server crée une copie du fichier de configuration périmé en utilisant la convention d'appellation *server_name.001*, *server_name.002*, *server_name.003...server_name.999*.

Si vous souhaitez utiliser un fichier de configuration autre que le fichier par défaut et que vous conservez la partie *nom_serveur* du nom du fichier, vous devez inclure au moins un caractère alphabétique dans l'extension. En variante, vous pouvez modifier la partie *nom_serveur* du nom du fichier. Cette procédure évite les confusions avec les fichiers de configuration de secours générés par Adaptive Server lorsque vous modifiez un paramètre.

## Utilisation de *sp_configure* pour lire ou écrire le fichier de configuration

La syntaxe d'utilisation de l'option configuration file avec sp_configure est la suivante :

```
sp_configure "configuration file", 0, "sous-commande", "nom_fichier"
```

où :

- "configuration file" (guillemets compris) désigne le paramètre du fichier de configuration.
- Il faut indiquer 0 comme deuxième paramètre de sp_configure afin d'assurer la compatibilité descendante.
- "*sous-commande*" est l'une des commandes décrites ci-dessous.
- *nom_fichier* spécifie le fichier de configuration que vous voulez utiliser en combinaison avec une quelconque *sous-commande*. Si vous ne précisez pas un répertoire dans le nom du fichier, Adaptive Server utilise alors le répertoire à partir duquel il a été lancé.

## Paramètres pour utiliser les fichiers de configuration

Les quatre paramètres décrits ci-dessous peuvent être utilisés avec les fichiers de configuration.

### *write*

write crée *file_name* à partir de la configuration courante. Si *file_name* existe déjà, un message est écrit dans le journal d'erreurs et le fichier existant est renommé selon la convention *file_name.001*, *file_name.002*, etc. Si vous avez modifié un paramètre statique mais que vous n'avez pas redémarré le serveur, write donne la *valeur d'exécution courante* de ce paramètre. Si vous ne précisez aucun répertoire avec *nom_fichier*, le fichier est enregistré dans le répertoire à partir duquel Adaptive Server a été lancé.

### *read*

read effectue un contrôle de validation sur les valeurs se trouvant dans *nom_fichier* et lit celles qui ont été validées dans le serveur. S'il manque des paramètres dans *file_name*, les valeurs courantes de ces paramètres sont utilisées.

Si la valeur d'un paramètre statique dans *file_name* est différente de sa valeur d'exécution courante, read échoue et un message est imprimé. La validation est cependant toujours effectuée sur les valeurs se trouvant dans *file_name*.

***verify***

verify effectue un contrôle de validation sur les valeurs se trouvant dans *file_name*. Ce paramètre est utile si vous avez modifié le fichier de configuration, car il vous évite de risquer de configurer votre serveur avec des valeurs incorrectes.

***restore***

restore crée *file_name* avec les valeurs de configuration les plus récentes. Si vous avez configuré des paramètres statiques avec de nouvelles valeurs, cette sous-commande écrira dans le fichier les valeurs configurée et non pas les valeurs d'exécution courantes. Ceci est très utile si vous avez perdu tous les exemplaires du fichier de configuration et que vous avez besoin d'en créer un nouveau. Si vous ne précisez aucun répertoire avec *nom_fichier*, le fichier est enregistré dans le répertoire à partir duquel Adaptive Server a été lancé.

**Exemples**

Cet exemple effectue un contrôle de validation sur les valeurs se trouvant dans le fichier *srv.config* et lit les paramètres qui ont été validés dans le serveur. Les valeurs d'exécution courantes remplacent les valeurs qui échouent au contrôle de validation.

```
sp_configure "configuration file", 0, "read",
"srv.config"
```

Cet exemple crée le fichier *my_server.config* et y écrit les valeurs de configuration actuellement utilisées par le serveur.

```
sp_configure "configuration file", 0, "write",
"my_server.config"
```

Cet exemple effectue un contrôle de validation sur les valeurs se trouvant dans le fichier *generic.config*.

```
sp_configure "configuration file", 0, "verify",
"generic.config"
```

Cet exemple écrit les valeurs configurées dans le fichier *restore.config*.

```
sp_configure "configuration file", 0, "restore",
"restore.config"
```

## Edition du fichier de configuration

Le fichier de configuration est un fichier au format ASCII que vous pouvez éditer avec tout éditeur de texte capable d'enregistrer les fichiers au format ASCII. La syntaxe de chaque paramètre est la suivante :

```
nom_paramètre={valeur | DEFAULT}
```

où *nom_paramètre* est le nom du paramètre que vous voulez spécifier, *valeur* est la valeur numérique à attribuer à *nom_paramètre* et "DEFAULT" précise que vous voulez utiliser la valeur par défaut de *nom_paramètre*.

**Exemples :**

```
deadlock retries = 1
```

indique que la transaction peut faire une nouvelle tentative pour acquérir un verrou lorsque l'interblocage se produit pendant un rétrécissement ou une **page d'allocation** d'index.

```
cpu accounting flush interval=DEFAULT
```

précise qu'il faut utiliser la valeur par défaut du paramètre cpu accounting flush interval.

Lorsque vous éditez un fichier de configuration, vos modifications ne sont pas validées avant d'avoir contrôlé le fichier avec l'option verify, lu le fichier avec l'option read ou relancé Adaptive Server avec ce fichier de configuration.

Si tous vos fichiers de configuration sont perdus ou endommagés, vous pouvez en créer un nouveau depuis un serveur en cours d'exécution à l'aide de la sous-commande restore en précisant un nom pour le nouveau fichier. Les paramètres dans le nouveau fichier prendront les valeurs d'exécution courantes du serveur.

#### Autorisations des fichiers de configuration

Les fichiers de configuration sont des fichiers texte au format ASCII non cryptés. Par défaut, ils sont créés avec une autorisation de lecture et d'écriture accordée au propriétaire du fichier et avec une autorisation de lecture pour tous les utilisateurs. Si vous avez créé le fichier de configuration au niveau du système d'exploitation, vous êtes le propriétaire du fichier ; si vous avez créé le fichier de configuration depuis Adaptive Server à l'aide du paramètre write ou restore, le propriétaire du fichier est alors l'utilisateur qui a lancé Adaptive Server. Il s'agit généralement de l'utilisateur "sybase". Pour restreindre l'accès aux fichiers de configuration, utilisez la commande d'autorisation de votre système d'exploitation pour attribuer les droits appropriés d'écriture, de lecture et d'exécution.

**Remarque** Vous devez définir les autorisations de la même manière pour *chaque* fichier de configuration créé.

#### Sauvegarde des fichiers de configuration

Les fichiers de configuration sont sauvegardés automatiquement lorsque vous effectuez une sauvegarde de la base de données master. Ce sont des fichiers du système d'exploitation et vous devez les sauvegarder de la même manière que les autres fichiers système.

#### Contrôle du nom du fichier de configuration en cours d'utilisation

Le résultat de sp_configure tronque le nom du fichier de configuration en raison des limitations d'espace. Pour afficher le nom entier du fichier de configuration, utilisez :

```
select s1.value2
from syscurconfigs s1, sysconfigures s2
where s1.config = s2.config
and s2.name = "configuration file"
```

## Lancement d'Adaptive Server avec un fichier de configuration

Au démarrage, Adaptive Server lit par défaut le fichier de configuration *server_name.cfg* qui se trouve dans le répertoire de démarrage. Si ce fichier n'existe pas, un nouveau fichier est créé et Adaptive Server utilise les valeurs par défaut pour tous les paramètres.

Vous pouvez lancer Adaptive Server avec un fichier de configuration que vous spécifiez. Pour plus d'informations, reportez-vous au *Guide Utilitaires*.

Si le fichier de configuration que vous avez indiqué n'existe pas, Adaptive Server imprime un message d'erreur et ne démarre pas.

Si la commande réussit, le fichier *server_name.bak* est créé. Ce fichier contient les valeurs de configuration enregistrées dans sysconfigures avant la mise à jour de sysconfigures avec les valeurs lues dans le fichier de configuration que vous avez indiqué. Ce fichier est remplacé à chaque nouveau démarrage.

#### Erreurs du fichier de configuration

Si le fichier de configuration contient des erreurs, Adaptive Server risque de ne pas démarrer ou démarre en utilisant les valeurs par défaut.

Adaptive Server utilise les valeurs par défaut dans les cas suivants :

- Il existe des valeurs incorrectes. Si un paramètre exige une valeur numérique, par exemple, et que le fichier de configuration contient une chaîne de caractères, Adaptive Server utilise la valeur par défaut.
- Des valeurs sont inférieures au minimum autorisé.

## Hiérarchie des paramètres

Les paramètres de configuration sont groupés en fonction du domaine de fonctionnement d'Adaptive Server qu'ils affectent. Il est ainsi plus facile d'identifier tous les paramètres éventuellement requis pour optimiser un domaine de fonctionnement particulier d'Adaptive Server.

Les groupes sont les suivants :

- Sauvegarde et restauration
- Gestionnaire de cache
- Administration des Component Integration Services
- E/S disque
- Administration DTM
- Journal d'erreurs
- Procédures stockées étendues

- Informations générales
- Services Java
- Langues
- Gestionnaire de verrous
- Utilisation de la mémoire
- Caches de métadonnées
- Communication en réseau
- Ressources du système d'exploitation
- Requêtes parallèles
- Mémoire physique
- Processeurs
- Administration du thread RepAgent
- Administration du serveur SQL
- Aspect sécurité
- Environnement utilisateur

Bien que chaque paramètre possède un groupe primaire auquel il appartient, de nombreux paramètres possèdent des groupes secondaires auxquels ils appartiennent également. number of remote connections, par exemple, appartient sur un plan primaire au groupe Communication en réseau, mais appartient également sur un plan secondaire au groupe Administration d'Adaptive Server et au groupe Utilisation de la mémoire. Cela reflète le fait que certains paramètres ont des répercussions sur plusieurs domaines du fonctionnement d'Adaptive Server. sp_configure affiche les paramètres dans tous les groupes auxquels ils appartiennent.

La syntaxe pour afficher tous les groupes et leurs paramètres associés ainsi que les valeurs courantes de ces paramètres est la suivante :

```
sp_configure
```

---

**Remarque** Le nombre de paramètres renvoyés par sp_configure dépend de la valeur du niveau d'affichage. Reportez-vous à la section "Sous-ensembles définis par l'utilisateur de la hiérarchie des paramètres : Niveaux d'affichage", page 99 pour plus d'informations sur les niveaux d'affichage.

---

La syntaxe permettant d'afficher un groupe particulier avec ses paramètres associés est la suivante :

```
sp_configure "nom_groupe"
```

où *nom_groupe* est le nom du groupe qui vous intéresse. Pour afficher le groupe E/S disque, par exemple, tapez :

```
sp_configure "Disk I/O"
Group: Disk I/O

Parameter Name           Default Memory Used Config Value Run Value
--------------           ------- ----------- ------------  ---------
allow sql server async i/o     1           0             1         1
disk i/o structures          256           0           256       256
number of devices             10           0            10        10
page utilization percent      95           0            95        95
```

**Remarque** Si le serveur utilise un ordre de tri ne faisant pas la distinction entre les majuscules et les minuscules, sp_configure sans paramètre renvoie une liste de tous les paramètres et groupes de configuration dans l'ordre alphabétique, sans afficher de regroupement.

## Sous-ensembles définis par l'utilisateur de la hiérarchie des paramètres : Niveaux d'affichage

Vous devrez peut-être ajuster certains paramètres plus souvent que d'autres, suivant votre utilisation d'Adaptive Server. Vous trouverez peut-être plus facile de travailler avec un sous-ensemble de paramètres plutôt que de visualiser le groupe complet alors que vous n'en utilisez que quelques-uns. Vous pouvez affecter l'une des trois valeurs à votre niveau d'affichage afin de disposer du sous-ensemble de paramètres qui correspond le mieux à votre façon de travailler.

Le niveau d'affichage par défaut est "comprehensive". Le niveau d'affichage que vous choisissez reste le même pour les autres sessions. Vous pouvez cependant le modifier à tout moment pour afficher plus ou moins de paramètres de configuration.

- "Basic" (élémentaire) : affiche uniquement les paramètres de configuration les plus élémentaires. Il convient à une optimisation très générale du serveur.

- "Intermediate" (intermédiaire) : affiche des paramètres un peu plus complexes, en plus des paramètres "basic". Ce niveau est adapté aux opérations d'optimisation du serveur moyennement complexes.
- "Comprehensive" (expert) : affiche tous les paramètres de configuration, y compris les plus complexes. Ce niveau est destiné aux utilisateurs qui souhaitent effectuer une optimisation très détaillée du serveur.

La syntaxe à utiliser pour afficher le niveau d'affichage courant est la suivante :

sp_displaylevel

La syntaxe à utiliser pour définir le niveau d'affichage est la suivante :

sp_displaylevel *nom_utilisateur* [, basic | intermediate | comprehensive]

où *nom_utilisateur* est votre nom de login à Adaptive Server.

## Effet du niveau d'affichage sur le résultat de *sp_configure*

Si vous avez défini un niveau d'affichage "basic" ou "intermediate", sp_configure ne renvoie qu'un sous-ensemble des paramètres que vous obtiendriez avec un niveau d'affichage "comprehensive". Avec un niveau d'affichage "intermediate", par exemple, pour afficher les paramètres dans le groupe Langues, tapez :

```
sp_configure "Languages"
```

Le résultat pourrait ressembler à ce qui suit :

```
Group: Languages
Parameter Name            Default  Memory Used  Config Value  Run Value
--------------------------- ------- ----------- ------------ ---------
default character set id           1           0            1         1
default language id                0           0            0         0
number of languages in cache       3           4            3         3
```

Il ne s'agit cependant que d'un sous-ensemble des paramètres du groupe Langues, car certains paramètres de ce groupe ne sont affichés qu'au niveau "comprehensive".

## Commande *reconfigure*

Les versions SQL Server antérieures à 11.0 imposaient l'exécution de reconfigure après sp_configure. Cela n'est plus nécessaire depuis la version 11.0 de SQL Server. La commande reconfigure existe toujours, mais elle est sans effet. Elle est incluse dans cette version d'Adaptive Server afin que vous puissiez exécuter vos scripts SQL antérieurs à 11.0 sans modification.

Les scripts qui emploient reconfigure fonctionnent toujours dans la version actuelle, mais nous vous recommandons de les modifier dès que possible car les futures versions d'Adaptive Server ne supporteront plus reconfigure.

## Optimisation des performances avec *sp_configure* et *sp_sysmon*

sp_sysmon contrôle les performances d'Adaptive Server et renvoie des statistiques qui décrivent le fonctionnement du système. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

Vous pouvez exécuter sp_sysmon avant et après l'utilisation de sp_configure pour ajuster les paramètres de configuration. Le résultat constitue une base pour l'optimisation des performances et permet d'observer les résultats des modifications de la configuration.

Ce chapitre contient des références croisées au document *Performances et optimisation* pour les paramètres sp_configure qui peuvent affecter les performances d'Adaptive Server.

# Résultat de *sp_configure*

L'exemple de résultat ci-dessous montre le type d'informations imprimées par sp_configure si votre niveau d'affichage est "comprehensive" et si vous l'exécutez sans paramètres. Les valeurs imprimées varient en fonction de votre plate-forme et des valeurs déjà modifiées.

```
                    sp_configure
Group: General Information
Parameter Name           Default Memory Used Config Value Run Value
--------------       ------- ----------- ------------ ---------
configuration file         0           0            0 /remote/pub
```

```
Group: Backup/Recovery

Parameter Name           Default Memory Used Config Value Run Value
--------------           ------- ----------- ------------ ---------
recovery interval in minutes   5           0            5         5
tape retention in days         0           0            0         0
recovery flags                 0           0            0         0
...
```

**Remarque** Tous les groupes et paramètres de configuration apparaissent dans le résultat si votre niveau d'affichage est "comprehensive".

La colonne "Default" contient les valeurs d'origine d'Adaptive Server. Si vous ne configurez pas explicitement un paramètre, il conserve sa valeur par défaut.

La colonne "Memory Used" (mémoire utilisée) affiche la quantité de mémoire utilisée (en kilo-octets) par le paramètre avec sa valeur courante. Certains paramètres liés sont tirés de la même zone de mémoire. La mémoire utilisée pour stack size et stack guard size, par exemple, est déjà comprise dans la mémoire utilisée pour number of user connections. Si vous totalisiez la mémoire utilisée par chacun de ces paramètres séparément, vous obtiendriez une quantité supérieure à celle effectivement utilisée. Dans la colonne "Memory Used" (mémoire utilisée), les paramètres qui "partagent" la mémoire avec d'autres paramètres sont signalés par un dièse ("#").

La colonne "Config Value" (valeur configurée) affiche la dernière valeur affectée au paramètre de configuration. Lorsque vous exécutez sp_configure pour modifier un paramètre dynamique :

- Les valeurs de configuration et d'exécution sont mises à jour.
- Le fichier de configuration est mis à jour.
- La modification est immédiatement prise en compte.

Lorsque vous modifiez un paramètre statique :

- La valeur de configuration est mise à jour.
- Le fichier de configuration est mis à jour.
- La modification ne prend effet qu'au redémarrage d'Adaptive Server.

La colonne "Run Value" (valeur d'exécution) affiche la valeur actuellement utilisée par Adaptive Server. Elle change lorsque vous modifiez la valeur d'un paramètre dynamique avec sp_configure et, pour les paramètres statiques, lorsque vous redémarrez Adaptive Server.

# Tables *sysconfigures* et *syscurconfigs*

L'état affiché par sp_configure se compose essentiellement des tables système master..sysconfigures et master..syscurconfigs et contient des informations supplémentaires provenant des tables sysattributes, sysdevices et d'autres tables système.

La colonne value (valeur) dans la table sysconfigures contient le dernier jeu de valeurs de sp_configure ou du fichier de configuration ; la colonne value dans syscurconfigs contient la valeur en cours d'utilisation. Les deux valeurs sont identiques dans le cas des paramètres dynamiques. Pour les paramètres statiques, qui nécessitent un redémarrage du serveur, les deux valeurs sont différentes si elles ont été modifiées depuis le dernier lancement d'Adaptive Server. Les valeurs peuvent également être différentes si vous utilisez les valeurs par défaut. Dans ce cas, sysconfigures contient 0 et syscurconfigs contient la valeur calculée et utilisée par Adaptive Server.

sp_configure effectue une jointure sur sysconfigures et syscurconfigs pour afficher les valeurs retournées par sp_configure.

## Interrogation de *syscurconfigs* et *sysconfigures* : exemple

Vous pouvez vouloir interroger sysconfigures et syscurconfigs pour obtenir des informations présentées selon vos convenances. sp_configure sans arguments, par exemple, affiche la mémoire utilisée pour les paramètres de configuration, mais n'indique par les valeurs minimale et maximale. Vous pouvez interroger ces tables système pour obtenir une liste complète d'utilisation de la mémoire ainsi que les valeurs minimales, maximales, par défaut à l'aide de la requête suivante :

```
select b.name, memory_used, minimum_value,
maximum_value, defvalue
from master.dbo.sysconfigures b,
master.dbo.syscurconfigs c
where b.config *= c.config and parent != 19
and b.config > 100
```

# Détails sur les paramètres de configuration

La section suivante contient des informations succinctes et détaillées sur chaque paramètre de configuration. Les paramètres sont énumérés par groupe et par ordre alphabétique au sein de chaque groupe.

Dans de nombreux cas, la valeur maximale autorisée du paramètre de configuration est extrêmement élevée. La valeur maximale pour votre serveur est généralement limitée par la mémoire disponible et non par les restrictions de sp_configure.

## Paramètres de configuration renommés

Les paramètres de configuration suivants ont été renommés :

| Ancien nom | Nouveau nom | Voir |
|---|---|---|
| lock promotion HWM | page lock promotion HWM | "page lock promotion HWM", page 213 |
| lock promotion LWM | page lock promotion LWM | "page lock promotion LWM", page 214 |
| lock promotion PCT | page lock promotion PCT | "page lock promotion PCT", page 215 |

## Paramètres de configuration remplacés

Le nouveau paramètre lock spinlock ratio remplace le paramètre de configuration page lock spinlock ratio.

## Sauvegarde et restauration

Les paramètres suivants permettent de configurer Adaptive Server pour la sauvegarde et la restauration des données :

### *number of large i/o buffers*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 6 |
| Valeurs correctes | 1–32 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre number of large i/o buffers définit le nombre de buffers de 16 Ko réservés à la réalisation d'opérations d'E/S importantes pour certains utilitaires d'Adaptive Server. Ces buffers pour grandes E/S sont initialement utilisés par la commande load database. load database utilise un buffer pour charger la base de données, indépendamment du nombre de devices de sauvegarde spécifiés. load database peut ensuite utiliser jusqu'à huit buffers pour initialiser les pages pour la base de données en cours de chargement. Ces buffers ne sont pas utilisés par load transaction. Si vous voulez exécuter plus de six commandes load database simultanément, configurez un buffer de grande E/S pour chaque commande load database.

create database et alter database utilisent ces buffers pour des grandes E/S lorsqu'elles effacent des pages de la base de données. Chaque instance de create database ou de load database peut utiliser jusqu'à 8 buffers de grande E/S.

Ces buffers sont également utilisés par la mise en miroir des disques et par certaines commandes dbcc.

### *print recovery information*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | recovery flags |
| Valeur par défaut | 0 (désactivé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Le paramètre print recovery information détermine les informations affichées par Adaptive Server sur la console pendant la restauration (la restauration est effectuée sur chaque base de données au démarrage d'Adaptive Server lorsqu'une sauvegarde de la base de données est chargée). La valeur par défaut est 0, ce qui veut dire qu'Adaptive Server n'affiche que le nom de la base de données et un message indiquant que la restauration est en cours. L'autre valeur est 1, ce qui veut dire qu'Adaptive Server affiche des informations sur chaque transaction individuelle traitée pendant la restauration ainsi qu'une indication précisant si elle a été annulée ou validée.

### *recovery interval in minutes*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | recovery interval |
| Valeur par défaut | 5 |
| Plage de valeurs | 1–32767 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

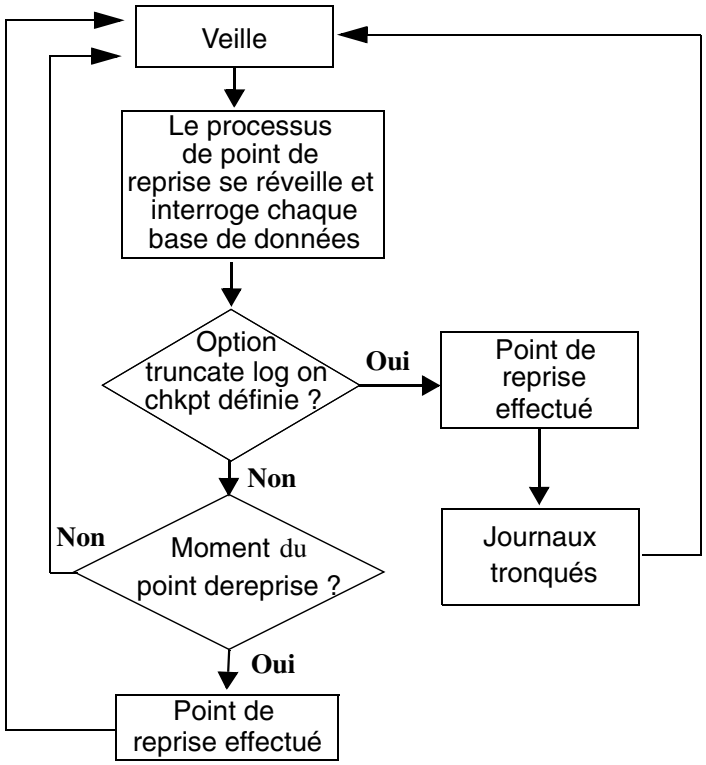
Le paramètre recovery interval in minutes définit le nombre maximum de minutes par base de données utilisées par Adaptive Server pour terminer sa procédure de restauration en cas de défaillance du système. La procédure de restauration annule les transactions en avant ou en arrière en commençant par la transaction qui est indiquée par le processus du point de reprise comme étant la transaction active la plus ancienne. La charge de travail du processus de restauration dépend de la valeur de recovery interval in minutes.

Adaptive Server estime qu'une minute est nécessaire pour restaurer 6 000 lignes du journal des transactions. Le temps de restauration varie cependant en fonction du type d'enregistrement du journal. Si vous définissez recovery interval in minutes sur 3, le processus du point de reprise écrit les pages modifiées sur le disque seulement si syslogs contient plus de 18 000 lignes depuis le dernier point de reprise.

**Remarque** L'intervalle de restauration n'a aucune incidence sur les transactions longues et peu journalisées (telles que create index) qui sont actives lorsque l'incident survient. En effet, l'annulation de ces transactions peut prendre autant de temps que leur exécution. Pour éviter des retards importants, sauvegardez chaque base de données après des opérations de maintenance sur les index.

Adaptive Server utilise le paramètre recovery interval in minutes et le niveau d'activité de chaque base de données pour déterminer le point de reprise de chaque base de données. Lorsque Adaptive Server fixe le point de reprise d'une base de données, il écrit toutes les **pages modifiées** (pages de données qui ont été modifiées dans le cache) sur le disque. Cela peut créer une brève période d'opérations d'E/S intenses également appelée *pointe de point de reprise*. Le point de reprise consiste également à effectuer certaines autres opérations de maintenance comme la troncature du journal des transactions pour chaque base de données pour laquelle l'option truncate log on chkpt est définie. A peu près une fois par minute, le processus de point de reprise en veille "se réveille", vérifie le paramètre truncate log on chkpt et contrôle l'intervalle de restauration pour déterminer si un point de reprise est nécessaire. La figure 5-1 illustre la logique appliquée par Adaptive Server pendant ce processus.

***Figure 5-1 : Processus de point de reprise***



Vous pouvez modifier l'intervalle de restauration suite à un changement de l'application et de son utilisation. Vous pouvez, par exemple, raccourcir l'intervalle de restauration en cas d'augmentation de l'activité de mise à jour sur Adaptive Server. Le fait de raccourcir l'intervalle de restauration donne lieu à des points de reprise plus fréquents avec des pointes de point de reprise plus fréquentes, ce qui ralentit légèrement le système. D'un autre côté, un intervalle de restauration trop élevé peut donner lieu à un temps de restauration excessivement long. Les pointes provoquées par la production des points de reprise peuvent être réduites en modifiant le paramètre housekeeper free write percent. Pour plus d'informations, reportez-vous à la section "housekeeper free write percent", page 205. Pour plus d'informations sur les effets du paramètre recovery interval in minutes sur les performances, reportez-vous à la section "Dimensionnement du cache des procédures", page 323 dans le document *Performances et optimisation*.

Utilisez sp_sysmon pour déterminer comment un intervalle de restauration particulier affecte le système. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### *tape retention in days*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | tape retention |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–365 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Le paramètre tape retention in days spécifie le nombre de jours pendant lesquels vous prévoyez de conserver chaque bande après son utilisation pour la sauvegarde d'une base de données ou d'un journal de transactions. Son rôle est d'éviter l'effacement accidentel d'une bande de sauvegarde.

Si vous avez fixé tape retention in days à 7 jours, par exemple, et que vous essayez d'utiliser la bande avant que 7 jours se soient écoulés depuis la dernière sauvegarde sur cette bande, Backup Server émet un message d'avertissement.

Vous pouvez ignorer l'avertissement en utilisant l'option with init lorsque vous exécutez la commande de sauvegarde. La bande sera alors ré-enregistrée et toutes les données qu'elle contenait seront perdues.

Les commandes dump database et dump transaction disposent toutes deux d'une option retaindays qui a priorité sur la valeur de tape retention in days pour une sauvegarde particulière. Pour plus d'informations, reportez-vous à la section "Protection des fichiers de sauvegarde contre l'écrasement", page 922.

## Gestionnaire de cache

Les paramètres de ce groupe configurent les caches des données et des procédures.

### *global async prefetch limit*

| **Récapitulatif** | |
|---|---|
| Valeur par défaut | 10 |
| Plage de valeurs | 0–100 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Le paramètre global async prefetch limit indique le pourcentage d'une zone de buffers qui peut contenir les pages qui y sont amenées par prélecture asynchrone et qui n'ont pas encore été lues. Ce paramètre définit la limite de toutes les zones dans tous les caches pour lesquels la limite n'a pas été définie explicitement avec sp_poolconfig.

Si la limite d'une zone est dépassée, la prélecture asynchrone est provisoirement interrompue jusqu'à ce que le pourcentage de pages non lues redevienne inférieur à la limite. Pour plus d'informations, reportez-vous au chapitre 25, "Optimisation de la prélecture asynchrone", dans le document *Performances et optimisation*.

### global cache partition number

| Récapitulatif | |
|---|---|
| Valeur par défaut | 1 |
| Plage de valeurs | 1–64, puissances de 2 |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

global cache partition number définit le nombre par défaut de partitions pour tous les caches de données. Le nombre de partitions pour un cache donné peut être défini avec sp_cacheconfig ; la valeur locale a priorité sur la valeur globale.

Utilisez le partitionnement des caches pour diminuer les conflits de verrou d'attente dans le cache. Le partitionnement du cache améliore généralement les performances lorsque le conflit de verrou d'attente dépasse 100 %. En doublant le nombre de partitions, vous divisez par deux les conflits de verrou d'attente.

Pour plus d'informations sur la configuration des partitions de cache, reportez-vous à la section "Ajout de partitions de cache", page 670. Reportez-vous au chapitre 25, "Optimisation de la prélecture asynchrone" dans le document *Performances et optimisation* pour plus d'informations.

### memory alignment boundary

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | calignment |
| Valeur par défaut | Taille de page logique |
| Plage de valeurs | 2048[a]–16384<br>a. Minimum déterminé par la taille de page logique du serveur |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre memory alignment boundary détermine la limite d'adresse mémoire sur laquelle sont alignés les caches de données.

Certaines machines effectuent les E/S avec plus d'efficacité lorsque les structures sont alignées sur une limite donnée d'adresse mémoire. Pour conserver cet alignement, les valeurs de memory alignment boundary doivent toujours être des puissances de 2 entre la taille de page logique et 2048 Ko.

**Remarque** Le paramètre memory alignment boundary est inclus pour le support de certaines plates-formes physiques. Ne le modifiez pas sauf si vous y êtes invité par le Support Technique de Sybase.

### *number of index trips*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cindextrips |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–65535 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre number of index trips précise le nombre de fois qu'une page d'index ancienne traverse la chaîne MRU/LRU (utilisé plus récemment/ utilisé moins récemment) avant que son échange ne soit envisagé. Lorsque vous augmentez la valeur de number of index trips, les pages d'index restent dans le cache pendant plus longtemps.

Un cache de données est mis en œuvre sous la forme d'une chaîne MRU/ LRU. Lorsque les threads de l'utilisateur accèdent aux pages de données et d'index, ces pages sont placées à l'extrémité MRU de la chaîne MRU/LRU du cache. Dans certaines environnements à transactions intenses (et dans certains tests de performances), il est souhaitable de conserver les pages d'index dans le cache car elles seront probablement requises prochainement. En donnant à number of index trips une valeur plus élevée, les pages d'index sont conservées plus longtemps dans le cache ; une valeur plus faible donne lieu à un échange plus fréquent des pages d'index dans le cache.

Il est inutile de définir le nombre de pages d'index pour les pages LRU de type "relaxed". Pour plus d'informations, reportez-vous au chapitre 19, "Configuration des caches de données".

**Remarque** Si le cache utilisé par un index est relativement petit (notamment s'il partage de l'espace avec d'autres objets) et que le volume des transactions est élevé, ne définissez pas une valeur trop élevée pour number of index trips. Le cache peut être saturé de pages non périmées, ce qui peut retarder les processus qui attendent de l'espace dans le cache.

### *number of oam trips*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | coamtrips |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–65535 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre number of oam trips précise le nombre de fois qu'une page de *table d'allocation d'objets* (*OAM*) traverse la chaîne MRU/LRU avant que son échange ne soit envisagé. Plus la valeur de number of oam trips est élevée, plus les pages OAM anciennes restent longtemps dans le cache.

Chaque table et index d'une table possède une page de table d'allocation d'objets (OAM). La page OAM contient des informations sur les pages allouées à la table ou à l'index et est contrôlée lorsqu'une nouvelle page est nécessaire à l'index ou à la table. (Pour plus d'informations, reportez-vous à la section "page utilization percent", page 123.) Chaque page de l'OAM peut contenir la configuration d'allocation de 2 000 à 63 750 pages d'index ou de données.

Les pages de l'OAM pointent vers la page d'allocation de chaque unité d'allocation dans laquelle l'objet occupe de l'espace. De leur côté, les pages d'allocation consignent les informations sur l'utilisation des extents et des pages à l'intérieur de l'unité d'allocation.

Dans certains environnement et tests de performances qui font appel à des allocations d'espace importantes (c'est-à-dire des opérations de copie volumineuses), les performances sont améliorées si les pages OAM sont conservées plus longtemps dans le cache. En fixant une valeur plus élevée pour number of oam trips, les pages OAM restent dans le cache.

**Remarque** Ne donnez pas une valeur trop élevée à number of oam trips si le cache est relativement petit et s'il est utilisé par un grand nombre d'objets. Le cache risquerait alors d'être encombré par des pages OAM non périmées et les threads de l'utilisateur seraient retardés.

### *procedure cache size*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 12.5 | procédure cache percent |
| Valeur par défaut | 3271 |
| Plage de valeurs | 3271–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

Indique la taille du cache de procédure en pages de 2 Ko. Adaptive Server utilise le cache de procédure pendant l'exécution des procédures stockées. Si le serveur constate que le cache contient déjà une copie d'une procédure, il n'aura pas besoin de la lire sur le disque. Adaptive Server utilise également l'espace du cache de procédure pour compiler les requêtes pendant la création des procédures stockées.

La valeur optimale pour procedure cache size pouvant varier d'une application à l'autre, le fait de réinitialiser ce paramètre peut améliorer les performances d'Adaptive Server. Si vous exécutez de nombreuses procédures ou requêtes spécifiques différentes, par exemple, votre application fera un usage plus intensif du cache de procédure et il est donc recommandé d'augmenter sa valeur.

**Avertissement !** Si procedure cache size est trop faible, les performances d'Adaptive Server seront fortement affectées.

#### Si vous effectuez une mise à niveau

Si vous effectuez une mise à niveau, procedure cache size est fixé à la taille du cache de procédure original au moment de la mise à niveau. procedure cache size peut être configuré de manière dynamique et dépend de la valeur max memory actuellement configurée.

### *total data cache size*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–2147483647 |
| Etat | Calculé |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

Le paramètre total data cache size indique la taille mémoire, en kilo-octets, actuellement disponible pour les pages de données, d'index et de journal. Il s'agit d'une valeur calculée que l'utilisateur ne peut pas modifier directement.

La taille mémoire disponible pour le cache des données peut être affectée par différents facteurs dont :

- La taille de la mémoire physique disponible sur la machine
- Les valeurs des paramètres suivants :
  - total logical memory
  - number of user connections
  - total procedure cache percent
  - number of open databases
  - number of open objects
  - number of open indexes
  - number of devices

Plusieurs autres paramètres affectent également l'espace mémoire disponible, mais à un niveau moindre.

Reportez-vous à la section "Détails sur les paramètres de configuration", page 104 pour plus d'informations sur la manière dont Adaptive Server alloue la mémoire et sur les caches de données.

## Administration des Component Integration Services

Les paramètres suivants configurent Adaptive Server pour les Component Integration Services.

### *cis bulk insert array size*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 50 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Lorsque vous effectuez un transfert en masse des données d'Adaptive Server Enterprise vers un autre Adaptive Server Enterprise, CIS place en interne les lignes dans un tampon et demande à la bibliothèque de masse Open Client de les transférer d'un seul bloc. La taille du tableau est commandée par cis bulk insert array size. La valeur par défaut est de 50 lignes et la propriété est dynamique, ce qui permet de la modifier sans redémarrer le serveur.

### *cis bulk insert batch size*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre cis bulk insert batch size détermine le nombre de lignes de la ou des tables sources qui doivent être copiées en masse dans la table cible sous la forme d'un batch unique en utilisant select into.

Si la valeur par défaut (zéro) est conservée, toutes les lignes sont copiées en tant que batch unique. Dans le cas contraire, le serveur exécute une validation globale (bulk commit) sur le serveur cible après que le nombre de lignes spécifié par ce paramètre a été copié dans la table cible ; le batch est ainsi validé.

Lorsqu'une opération de copie de masse générée normalement par un client (telle que celle produite par l'utilitaire bcp) est reçue, le client est alors supposé contrôler la taille du batch et le serveur ignore la valeur de ce paramètre.

### *cis connect timeout*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–32767 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre cis connect timeout détermine le temps d'attente, en secondes, pour une connexion Client-Library réussie. Par défaut, aucune temporisation n'est prévue.

### *cis cursor rows*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 50 |
| Plage de valeurs | 1–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre cis cursor rows permet aux utilisateurs de spécifier le décompte de lignes de curseur pour les opérations cursor open et cursor fetch. Si vous augmentez cette valeur, un plus grand nombre de lignes sera extrait en une seule opération. La vitesse de l'opération est ainsi accrue mais une quantité de mémoire plus importante est requise. La valeur par défaut est 50.

### *cis packet size*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 512 |
| Plage de valeurs | 512–32768 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre cis packet size spécifie la taille des paquets TDS (Tabular Data Stream™) qui sont échangés entre le serveur et un serveur distant lors de l'établissement de la connexion.

Sur la plupart des systèmes, la taille de paquet par défaut est 512 octets, ce qui convient pour la majorité des applications. Des tailles supérieures peuvent toutefois améliorer de façon significative les performances des requêtes, notamment lorsqu'elles traitent des données de type text et image ou des données de masse.

Si vous indiquez une taille de paquet supérieure à la valeur par défaut et que la version d'Adaptive Server interrogée est 10 ou supérieure, le serveur cible doit être configuré de façon à autoriser les paquets de longueur variable. Dans ce cas, les paramètres de configuration d'Adaptive Server concernés sont les suivants :

- additional netmem
- maximum network packet size

### *cis rpc handling*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre cis rpc handling spécifie la méthode par défaut pour la gestion d'un appel de procédure distante (RPC). Si cis rpc handling est à 0, le gestionnaire du site Adaptive Server est le mécanisme de gestion RPC par défaut. Si le paramètre est à 1, la gestion RPC utilise alors obligatoirement les méthodes d'accès des Component Integration Services. Pour plus d'informations, reportez-vous à la section traitant de set cis rpc handling dans le document *Component Integration Services - Guide de l'utilisateur*.

### *enable cis*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre enable cis permet d'activer ou de désactiver les Component Integration Services.

### enable file access

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Permet d'accéder au système de fichier externe par le biais de tables proxy. Nécessite une licence pour ASE_XFS.

### enable full-text search

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Permet d'utiliser les services de recherche Full-Text. Nécessite une licence pour ASE_EFTS.

### max cis remote connections

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

Le paramètre max cis remote connections spécifie le nombre maximum de connexions Client-Library simultanées qui peuvent être établies avec des serveurs distants par les Component Integration Services.

Par défaut, Component Integration Services autorise jusqu'à 4 connexions simultanées par utilisateur vers des serveurs distants. Si vous définissez le nombre maximal d'utilisateurs sur 25, Component Integration Services autorise jusqu'à 100 connexions Client-Library simultanées.

Si ce nombre ne satisfait pas les besoins de votre installation, vous pouvez redéfinir le paramètre en spécifiant le nombre de connexions Client-Library sortantes simultanées que le serveur peut établir.

## E/S disque

Les paramètres de ce groupe configurent les E/S disque d'Adaptive Server.

### *allow sql server async i/o*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | T1603 (indicateur de trace) |
| Valeur par défaut | 1 |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre allow sql server async i/o permet à Adaptive Server de fonctionner avec des E/S disque asynchrones. Pour pouvoir utiliser des E/S disque asynchrones, vous devez activer cette fonctionnalité *à la fois* sur Adaptive Server *et* sur votre système d'exploitation. Reportez-vous à la documentation de votre système d'exploitation pour plus d'informations sur l'activation des E/S asynchrones au niveau du système d'exploitation.

Dans tous les cas, les E/S disque asynchrones sont plus rapides que les synchrones. Ceci est lié au fait que lorsque Adaptive Server émet une E/S asynchrone, il n'est pas obligé d'attendre une réponse avant d'émettre d'autres E/S.

### *disable disk mirroring*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Valeurs correctes | 1, 0 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

disable disk mirroring active ou désactive la mise en miroir des disques pour Adaptive Server. Il s'agit d'une variable globale ; Adaptive Server n'effectue aucune mise en miroir de disque si ce paramètre de configuration est défini sur 1 et Adaptive Server est relancé. Définissez disable disk mirroring sur 0 pour activer la mise en miroir des disques.

**Remarque** La mise en miroir des disques doit être activée si vous configurez Adaptive Server pour une reprise sur le serveur secondaire dans un système à haut niveau de disponibilité.

### *disk i/o structures*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cnblkio |
| Valeur par défaut | 256 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre disk i/o structures définit le nombre initial de blocs de contrôle d'E/S disque qu'Adaptive Server alloue au démarrage.

Les processus utilisateur ont besoin d'un bloc de contrôle d'E/S disque avant qu'Adaptive Server puisse initier une demande d'E/S pour le processus. La mémoire pour les blocs de contrôle d'E/S disque est préallouée au démarrage d'Adaptive Server. Il est recommandé de donner à disk i/o structures la valeur la plus élevée autorisée par votre système afin de réduire le risque de manquer de structures d'E/S disque. Reportez-vous à la documentation de votre système d'exploitation pour plus d'informations sur les E/S disque simultanées.

Utilisez sp_sysmon pour déterminer si vous devez allouer plus de structures d'E/S disque. Reportez-vous au document *Performances et optimisation*. Vous pouvez donner au paramètre de configuration max asynch i/os per server la même valeur que disk i/o structures. Pour plus d'informations, reportez-vous à la section "max async i/os per server", page 174.

### *number of devices*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | devices |
| Valeur par défaut | 10 |
| Plage de valeurs | 1–256 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

Le paramètre number of devices détermine le nombre de devices de base de données que peut utiliser Adaptive Server. Il ne comprend pas les devices utilisés pour les sauvegardes de la base de données et du journal des transactions.

Vous pouvez également assigner le nombre de devices (vdevno) lorsque vous exécutez disk init, bien que cette valeur soit facultative. Si vous n'affectez aucune valeur vdevno, Adaptive Server affecte le prochain numéro de device virtuel disponible.

Si vous affectez un numéro de device virtuel, chaque numéro de device doit être unique parmi les numéros de device utilisés par Adaptive Server. Le numéro 0 est réservé au device master. Les numéros admis sont compris entre 1 et 256 ; le numéro le plus élevé doit cependant être inférieur de 1 au nombre de devices de base de données que vous avez configuré pour Adaptive Server. Si vous avez configuré votre serveur pour 10 devices, par exemple, les numéros de device corrects sont compris entre 1 et 9.

Pour déterminer les numéros en cours d'utilisation, exécutez sp_helpdevice et consultez la colonne *device_number* du résultat.

Si vous voulez diminuer la valeur de number of devices après avoir ajouté des devices de base de données, vous devez tout d'abord vérifier les numéros déjà utilisés par les devices de base de données. La commande suivante imprime la valeur la plus élevée utilisée :

```
select max(low/power(2,24))+1
    from master..sysdevices
```

**Avertissement !** Si vous définissez une valeur trop faible pour number of devices dans votre fichier de configuration, Adaptive Server ne pourra pas démarrer. Vous pouvez connaître les devices utilisés en consultant la table système sysdevices.

### *page utilization percent*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 95 |
| Plage de valeurs | 1–100 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre page utilization percent est utilisé pendant les allocations de page pour contrôler si Adaptive Server balaie l'OAM (*table d'allocation d'objets*) d'une table pour rechercher les pages inutilisées ou alloue tout simplement un nouvel extent à la table. (Reportez-vous à la section "number of oam trips", page 112 pour plus d'informations sur l'OAM.) Le paramètre page utilization percent permet d'optimiser les performances des serveurs dotés de tables de très grande taille ; il réduit la durée nécessaire pour ajouter de l'espace supplémentaire.

Si page utilization percent est fixé à 100, Adaptive Server balaie toutes les pages OAM pour rechercher les pages inutilisées allouées à l'objet avant d'allouer un nouvel extent. Si ce paramètre a une valeur inférieure à 100, Adaptive Server compare de la manière suivante le paramètre page utilization percent avec le rapport entre les pages utilisées et non utilisées allouées à la table :

```
100 * used pages/(used pages + unused pages)
```

Si le paramètre page utilization percent est inférieur au rapport, Adaptive Server alloue un nouvel extent au lieu de rechercher les pages inutilisées.

Lorsque vous insérez des données dans une table de 10 Go, par exemple, qui possède 120 pages OAM et une seule page de données inutilisée :

- Une valeur de page utilization percent de 100 a pour effet qu'Adaptive Server balaie les 120 pages OAM pour localiser une page de données inutilisée.
- Une valeur de page utilization percent de 95 permet à Adaptive Server d'allouer un nouvel extent à l'objet, car 95 est inférieur au rapport entre les pages utilisées et inutilisées.

Une valeur de page utilization percent faible entraîne un nombre plus élevé de pages inutilisées. Une valeur de page utilization percent élevée ralentit les allocations de page dans les très grandes tables, car Adaptive Server effectue un balayage OAM pour rechercher toutes les pages inutilisées avant d'allouer un nouvel extent, ce qui augmente les E/S logiques et physiques.

Si les allocations de page (notamment dans le cas d'insertions importantes) semblent lentes, vous pouvez diminuer la valeur de page utilization percent, mais n'oubliez pas de la rétablir après avoir inséré les données. Une valeur inférieure affecte toutes les tables du serveur et donne lieu à des pages inutilisées dans toutes les tables.

La copie de masse rapide ignore le paramètre page utilization percent et alloue toujours de nouveaux extents jusqu'à ce que la base de données ne contienne plus d'extents disponibles.

## Administration DTM

Les paramètres suivants permettent de configurer les fonctionnalités de gestion des transactions distribuées (DTM) :

### *dtm detach timeout period*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (minutes) |
| Valeurs correctes | 0 à 2 147 483 647 (minutes) |
| Etat | Dynamique |
| Niveau d'affichage | 10 |
| Rôle requis | Administrateur système |

dtm detach timeout period définit la durée, en minutes, pendant laquelle une transaction distribuée peut rester en situation détachée. Dans certains environnements X/Open XA, une transaction peut devenir détachée de son thread de commande (généralement pour être attachée à un autre thread de commande). Adaptive Server permet de maintenir les transactions en situation détachée pendant la durée spécifiée par le paramètre dtm detach timeout period. Une fois cette période écoulée, Adaptive Server annule la transaction détachée.

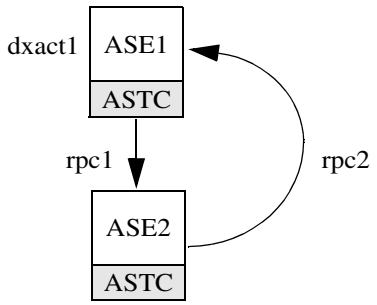
### *dtm lock timeout period*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 300 (secondes) |
| Valeurs correctes | 1 à 2 147 483 647 (secondes) |
| Etat | Dynamique |
| Niveau d'affichage | 10 |
| Rôle requis | Administrateur système |

dtm lock timeout period définit la durée, en minutes, pendant laquelle une branche de transaction distribuée attendra que les ressources de verrouillage deviennent disponibles. Lorsque cette période s'est écoulée, Adaptive Server considère que la transaction se trouve dans une situation d'interblocage et annule la branche de transaction qui a déclenché l'interblocage. Cela annule finalement toute la transaction distribuée.

Les transactions distribuées peuvent potentiellement s'interbloquer elles-mêmes si une transaction se propage vers un serveur distant et que le serveur distant, à son tour, répercute à nouveau une transaction vers le serveur qui l'a initiée. Cette situation est illustrée à la figure 5-2. A la figure 5-2, la tâche de la transaction distribuée "dxact1" est propagée vers l'Adaptive Server 2 via "rpc1". L'Adaptive Server 2 répercute ensuite la transaction vers le serveur de coordination via "rpc2". "rpc2" et "dxact1" partagent le même gtrid, mais ont des qualificatifs de branche différents, ce qui les empêche de partager les mêmes ressources de transaction. Si "rpc2" attend un verrou détenu par "dxact1", il se produit alors uns situation d'interblocage.

***Figure 5-2 : Interblocage de transactions distribuées***




Adaptive Server n'essaie pas de détecter les interblocages internes au serveur. Pour ce faire, il s'en remet à dtm lock timeout period. A la figure 5-2, lorsque la durée fixée par dtm lock timeout period s'est écoulée, la transaction créée pour "rpc2" est annulée. Adaptive Server 2 signale alors une erreur dans sa tâche et, pour terminer, "dxact1" est également annulée.

La valeur de dtm lock timeout period s'applique uniquement aux transactions distribuées. Les transactions locales peuvent utiliser une temporisation de verrouillage avec le paramètre lock wait period qui s'applique à l'ensemble du serveur.

---

**Remarque** Adaptive Server n'utilise pas dtm lock timeout period pour détecter les interblocages sur les tables système.

---

### enable DTM

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | 10 |
| Rôle requis | Administrateur système |

enable DTM active ou désactive la fonctionnalité DTM (gestion des transactions distribuées) d'Adaptive Server. Lorsque la fonctionnalité DTM est activée, vous pouvez utiliser Adaptive Server en tant que gestionnaire de ressources dans les systèmes X/Open XA et MSDTC. Vous devez redémarrer le serveur pour que ce paramètre prenne effet. Reportez-vous au document *XA Interface Integration Guide for CICS, Encina, and TUXEDO* pour plus d'informations sur l'utilisation d'Adaptive Server dans un environnement X/Open XA. Reportez-vous à Utilisation des fonctionnalités DTM pour plus d'informations sur les transactions dans les environnements MSDTC et pour des informations sur les services natifs de coordination des transactions d'Adaptive Server.

**Remarque** L'information de licence et la valeur d'exécution de enable DTM sont indépendantes l'une de l'autre. Que vous possédiez ou non une licence DTM, la valeur d'exécution et la valeur configurée sont définies sur 1 après le redémarrage d'Adaptive Server. Vous ne pouvez pas exécuter DTM tant que vous ne possédez pas de licence. Si vous n'avez pas installé de licence valide, Adaptive Server enregistre un message d'erreur et n'active pas la fonctionnalité. Reportez-vous au Guide d'installation pour plus d'informations sur l'installation des clés de licence.

L'information de licence et la valeur de configuration sont indépendantes l'une de l'autre.

### enable xact coordination

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 (activé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |

| Récapitulatif | |
|---|---|
| Etat | Statique |
| Niveau d'affichage | 10 |
| Rôle requis | Administrateur système |

Le paramètre enable xact coordination permet d'activer ou de désactiver les services de coordination des transactions d'Adaptive Server. Lorsque ce paramètre est défini sur 1 (activé), les services de coordination sont activés et le serveur peut propager les transactions à d'autres Adaptive Server. Cela peut se produire lorsqu'une transaction exécute un appel de procédure distante (RPC) pour mettre à jour les données dans un autre serveur ou met à jour les données dans un autre serveur en utilisant les services d'intégration des composants (CIS). Les services de coordination des transactions vérifient que les mises à jour apportées à des données situées sur l'Adaptive Server distant sont validées ou annulées avec la transaction d'origine.

Si ce paramètre est défini sur 0 (désactivé), Adaptive Server ne coordonne par le travail sur les serveurs distants. Les transactions peuvent toujours exécuter des RPC et mettre à jour des données en utilisant les CIS, mais Adaptive Server ne peut pas vérifier si les transactions distantes sont annulées avec la transaction d'origine ou si le travail distant est validé avec une transaction d'origine au cas où les serveurs distants rencontrent une défaillance. Cela correspond au mode de fonctionnement d'Adaptive Server avant la version 12.x.

### *number of dtx participants*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 500 |
| Valeurs correctes | 100 à 2 147 483 647 |
| Etat | Dynamique |
| Niveau d'affichage | 10 |
| Rôle requis | Administrateur système |

number of dtx participants définit le nombre total de transactions distantes que le service de coordination des transactions d'Adaptive Server peut propager et coordonner en même temps. Un participant DTX est une mémoire structurée interne utilisée par le service de coordination pour gérer une branche de transaction distante. Lorsque les transactions sont propagées vers les serveurs distants, le service de coordination doit obtenir de nouveaux participants DTX pour gérer ces branches.

Par défaut, Adaptive Server peut coordonner 500 transactions distantes. Le fait de réduire la valeur du paramètre number of dtx participants réduit le nombre de transactions distantes que le serveur peut gérer. Si aucun participant DTX n'est disponible, il est impossible de commencer de nouvelles transactions. Les transactions distribuées en cours risquent d'être annulées si aucun participant DTX n'est disponible pour propager une nouvelle transaction distante.

Le fait d'augmenter la valeur du paramètre number of dtx participants augmente le nombre de transactions distantes qu'Adaptive Server peut gérer, mais accroît également la mémoire utilisée.

#### Optimisation du paramètre number of dtx participants pour votre système

Au cours d'une période de pointe, utilisez la commande sp_monitorconfig pour examiner l'utilisation des participants DTX :

```
                    sp_monitorconfig "number of dtx participants"
Usage information at date and time: Jun 18 1999 9:00AM.
Name            # Free   # Active   % Active  # Max Ever Used   Re-used
--------------  --------  --------   --------   -------------  ---------
number of dtx   480          20         4.00             210         NA
participants
```

Si la valeur #Free est nulle ou très basse, les nouvelles transactions distribuées risquent de ne pas pouvoir commencer en raison d'un manque de participants DTX. Dans ce cas, vous devrez peut-être augmenter la valeur du paramètre number of dtx participants.

Si la valeur #Max Ever Used est trop basse, les participants DTX non utilisés risquent d'occuper de la mémoire qui pourrait servir à d'autres fonctions du serveur. Dans ce cas, pensez à réduire la valeur du paramètre number of dtx participants.

### *strict dtm enforcement*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | 10 |
| Rôle requis | Administrateur système |

strict dtm enforcement détermine si les services de coordination des transactions d'Adaptive Server appliquent strictement ou non les propriétés ACID des transactions distribuées.

Dans les environnements où Adaptive Server doit propager et coordonner les transactions uniquement vers d'autres Adaptive Server qui supportent la coordination des transactions, définissez strict dtm enforcement sur 1 (activé). Les transactions ne seront ainsi propagées que vers les serveurs qui peuvent participer aux transactions coordonnées d'Adaptive Server et les transactions seront achevées de manière cohérente. Si une transaction tente de mettre à jour des données sur un serveur qui ne supportent pas les services de coordination des transactions, Adaptive Server annule la transaction.

Dans les environnements hétérogènes, vous pouvez vouloir utiliser des serveurs qui ne supportent pas la coordination des transactions. Il s'agit notamment des anciennes versions d'Adaptive Server et des environnements de stockage de bases de données non-Sybase configurés avec CIS. Dans ce cas, vous pouvez définir strict dtm enforcement sur 0 (désactivé). Adaptive Server pourra ainsi distribuer les transactions à des Adaptive Server existants et à d'autres environnements de stockage de données sans toutefois pouvoir garantir que le travail distant de ces serveurs est bien annulé ou validé avec la transaction d'origine.

### *txn to pss ratio*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 16 |
| Valeurs correctes | 1 à 2 147 483 647 |
| Etat | Statique |
| Niveau d'affichage | 1 |
| Rôle requis | Administrateur système |

Adaptive Server gère les transactions sous la forme de ressources de serveur configurables. A chaque fois qu'une nouvelle transaction commence, Adaptive Server doit obtenir un **descripteur de transaction** libre d'une zone globale créée au moment du démarrage. Les descripteurs de transaction sont des mémoires structurées internes utilisées par Adaptive Server pour représenter les transactions actives.

Adaptive Server a besoin d'un descripteur de transaction libre pour :

- Le bloc externe de chaque transaction du serveur. Le bloc externe d'une transaction peut être créé explicitement lorsqu'un client exécute une nouvelle commande begin transaction. Adaptive Server peut également créer implicitement un bloc de transaction externe lorsque des clients utilisent Transact-SQL pour modifier des données sans utiliser begin transaction pour définir la transaction.

  **Remarque** Les blocs de transaction imbriqués suivants, créés avec des commandes begin transaction supplémentaires, ne requièrent pas de descripteurs de transaction supplémentaires.

- Chaque base de données à laquelle vous accédez dans une **transaction portant sur plusieurs bases de données**. Adaptive Server doit obtenir un nouveau descripteur de transaction à chaque fois qu'une transaction utilise ou modifie des données dans une nouvelle base de données.

txn to pss ratio détermine le nombre total de descripteurs de transaction disponibles pour le serveur. Au démarrage, ce nombre est multiplié par le paramètre number of user connections pour créer le groupe de descripteurs de transaction :

```
# of transaction descriptors = number of user connections * txn to pss ratio
```

La valeur par défaut qui est 16 assure la compatibilité avec les versions antérieures d'Adaptive Server. Dans les versions antérieures à la version 12.x, Adaptive Server allouait 16 descripteurs de transaction pour chaque connexion utilisateur. Dans la version 12.x, le nombre de transactions simultanées n'est limité que par le nombre de descripteurs disponibles sur le serveur.

**Remarque** Le nombre de bases de données auxquelles vous pouvez accéder dans une transaction portant sur plusieurs bases de données reste limité à 16.

#### Optimisation du paramètre txn to pss ratio pour votre système

Au cours d'une période de pointe, utilisez la commande sp_monitorconfig pour examiner l'utilisation des descripteurs de transaction :

```
                    sp_monitorconfig "txn to pss ratio"
Usage information at date and time: Jun 18 1999 8:54AM.
Name            # Free   # Active   % Active  # Max Ever Used   Re-used
--------------  --------  --------   --------   --------------  --------
txn to pss       784          80       10.20         523           NA
ratio
```

Si la valeur #Free est égale à zéro ou est très faible, les transactions peuvent prendre du retard car Adaptive Server attend la libération de descripteurs de transaction sur le serveur. Dans ce cas, vous devrez peut-être augmenter la valeur du paramètre txn to pss ratio.

Si la valeur #Max Ever Used est trop basse, les descripteurs de transaction non utilisés risquent d'occuper de la mémoire qui pourrait servir à d'autres fonctions du serveur. Dans ce cas, pensez à réduire la valeur du paramètre txn to pss ratio.

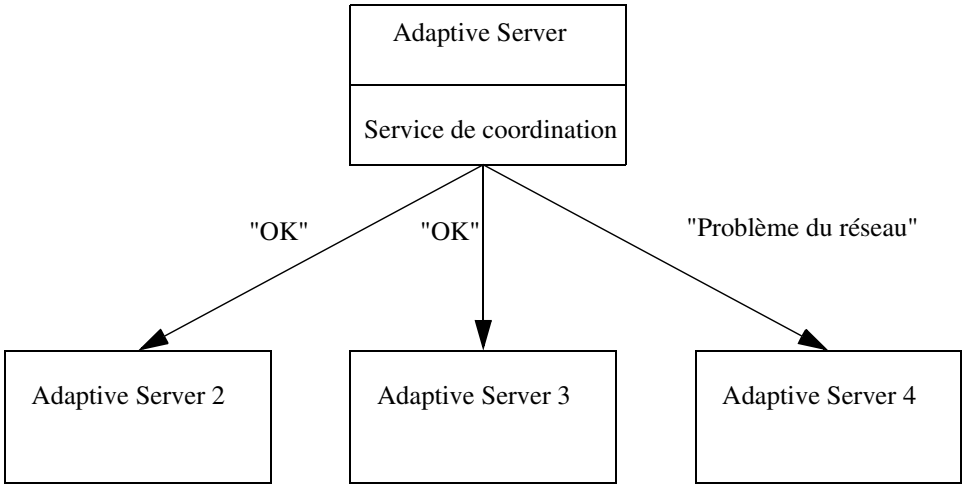
### *xact coordination interval*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 60 (secondes) |
| Valeurs correctes | 1 à 2 147 483 647 (secondes) |
| Etat | Dynamique |
| Niveau d'affichage | 10 |
| Rôle requis | Administrateur système |

xact coordination interval définit la durée entre deux tentatives de résolution des branches de transaction qui ont été propagées vers des serveurs distants.

L'Adaptive Server qui assure la coordination tente régulièrement de résoudre le travail des serveurs distants qui participent à une transaction distribuée. Comme illustré à la figure 5-3, le serveur chargé de la coordination contacte en série chaque serveur distant participant à la transaction distribuée. Le fait que le service de coordination soit dans l'incapacité de résoudre une branche de transaction peut avoir différentes raisons. Si le serveur distant est impossible à joindre en raison de problèmes du réseau, par exemple, le serveur chargé de la coordination essaie une nouvelle fois d'établir une connexion après la durée spécifiée par xact coordination level.

***Figure 5-3 : Résolution des branches de transaction distantes***




Si le paramètre xact coordination interval conserve sa valeur par défaut de 60, Adaptive Server essaie de résoudre les transactions distantes une fois par minute. Une diminution de cette valeur peut accélérer la réalisation des transactions distribuées, mais seulement si les transactions elles-mêmes sont résolues en moins d'une minute. Dans des circonstances normales, la diminution de la valeur du paramètre xact coordination interval n'affecte en rien les performances.

Le fait d'augmenter la valeur du paramètre xact coordination interval peut ralentir la réalisation des transactions distribuées et peut avoir pour effet que les branches de transaction mobilisent des ressources plus longtemps qu'elles ne le feraient normalement. Dans des circonstances normales, il est déconseillé de donner au paramètre xact coordination interval une valeur supérieure à sa valeur par défaut.

## Journal d'erreurs

Les paramètres de ce groupe configurent le journal d'erreurs d'Adaptive Server et la journalisation des événements Adaptive Server dans le journal d'événements Windows NT.

### *event log computer name* (Windows NT seulement)

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 'LocalSystem' |
| Valeurs correctes | • Nom d'une machine NT sur le réseau configurée pour enregistrer les messages d'Adaptive Server<br>• 'LocalSystem'<br>• 'NULL' |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre event log computer name indique le nom du PC Windows NT qui enregistre les messages Adaptive Server dans son journal d'événements Windows NT. Vous pouvez utiliser ce paramètre pour enregistrer les messages Adaptive Server sur une machine distante. Cette fonctionnalité est seulement disponible sur les serveurs Windows NT.

Si le paramètre a pour valeur 'LocalSystem' ou 'NULL', l'enregistrement sera effectué par défaut sur le système local.

Vous pouvez également faire appel à l'utilitaire Server Config pour définir le paramètre event log computer name en précisant le nom de l'ordinateur d'enregistrement des événements sous Event Logging.

En définissant le paramètre event log computer name avec sp_configure ou en indiquant le nom de l'ordinateur d'enregistrement des événements sous Event Logging, vous annulez les effets de l'option de ligne de commande -G, si elle a été spécifiée. Si Adaptive Server a été démarré avec l'option -G, vous pouvez modifier la machine distante de destination en définissant le paramètre event log computer name.

Pour plus d'informations sur la journalisation des messages Adaptive Server sur un site distant, reportez-vous au document *Adaptive Server - Manuel de configuration pour Windows NT*.

## *event logging* (Windows NT seulement)

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre event logging active et désactive la journalisation des messages Adaptive Server dans le journal d'événements Windows NT. Cette fonctionnalité est seulement disponible sur les serveurs Windows NT.

La valeur par défaut de 1 active la journalisation des messages Adaptive Server dans le journal d'événements Windows NT ; 0 la désactive.

Le paramètre event logging est défini avec l'utilitaire Server Config en sélectionnant l'option "Utiliser l'Observateur d'événements de Windows NT" sous Event Logging.

Le fait de définir le paramètre event logging ou de sélectionner l'option "Use Windows NT Event Logging" (utiliser journalisation d'événements Windows NT) sous Event Logging annule les effets de l'option de ligne de commande -g, si elle a été spécifiée.

### log audit logon failure

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Plage de valeurs | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre log audit logon failure spécifie s'il faut enregistrer les échecs de connexion à Adaptive Server dans le journal d'erreurs d'Adaptive Server et, sur les serveurs Windows NT, dans le journal d'événements Windows NT si la journalisation d'événements est activée.

Une valeur de 1 entraîne l'enregistrement des connexions qui ont échoué, une valeur de 0 ne les enregistre pas.

### log audit logon success

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Plage de valeurs | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre log audit logon success spécifie s'il faut enregistrer les connexions réussies à Adaptive Server dans le journal d'erreurs d'Adaptive Server et, sur les serveurs Windows NT, dans le journal d'événements Windows NT si la journalisation d'événements est activée.

Une valeur de 1 entraîne l'enregistrement des connexions réussies, une valeur de 0 ne les enregistre pas.

## Procédures stockées étendues

Les paramètres de ce groupe affectent le comportement des procédures stockées étendues (ESP).

### *esp execution priority*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 8 |
| Plage de valeurs | 0–15 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre esp execution priority définit la priorité du thread Serveur XP pour l'exécution des ESP. Les ESP peuvent fortement solliciter le processeur pendant de longues périodes. De même, du fait que Serveur XP réside sur la même machine que Adaptive Server, Serveur XP peut influer sur les performances d'Adaptive Server.

Utilisez le paramètre esp execution priority pour définir la priorité du thread Serveur XP pour l'exécution des ESP. Reportez-vous au manuel *Open Server Server-Library/C Reference Manual* pour plus d'informations sur la planification des threads Open Server.

### *esp execution stacksize*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 34816 |
| Plage de valeurs | 34816–$2^{14}$ |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre esp execution stacksize définit la taille en octets des piles allouées pour l'exécution des ESP.

Utilisez ce paramètre si vos propres fonctions ESP nécessitent une pile de taille supérieure à la taille par défaut qui est 34 816.

### *esp unload dll*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Plage de valeurs | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre esp unload dll spécifie si les DLL qui supportent les ESP doivent être déchargées automatiquement de la mémoire de Serveur XP lorsque l'appel des ESP est terminé.

Si esp unload dll est défini sur 0, les DLL ne sont pas déchargées automatiquement. Si le paramètre est défini sur 1, les DLL sont déchargées automatiquement.

Si esp unload dll est défini sur 0, vous pouvez toujours décharger explicitement des DLL individuelles lors de l'exécution à l'aide de sp_freedll.

### *start mail session* (Windows NT seulement)

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre start mail session active et désactive l'ouverture automatique d'une session de messagerie Adaptive Server lorsque vous démarrez Adaptive Server. Cette fonctionnalité est seulement disponible sur les serveurs Windows NT.

Si ce paramètre est défini sur 1, Adaptive Server ouvre une session de messagerie au prochain démarrage d'Adaptive Server. Si ce paramètre est défini sur 0, Adaptive Server n'ouvre pas de session de messagerie au prochain démarrage.

Si start mail session est défini sur 0, vous pouvez ouvrir explicitement une session de messagerie Adaptive Server à l'aide de l'ESP système xp_startmail.

Avant de définir le paramètre start mail session, vous devez préparer votre système Windows NT en créant une boîte aux lettres et un profil de messagerie pour Adaptive Server. Vous devez ensuite créer un compte Adaptive Server pour Sybmail. Pour plus d'informations sur la préparation de votre système pour Sybmail, reportez-vous au document *Adaptive Server - Manuel de configuration pour Windows NT*.

### *xp_cmdshell context*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Valeurs correctes | 0, 1 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre xp_cmdshell context définit le contexte de sécurité dans lequel les commandes du système d'exploitation seront exécutées en utilisant l'ESP système xp_cmdshell.

En définissant xp_cmdshell context sur 1, vous limitez le contexte de sécurité de xp_cmdshell aux utilisateurs qui possèdent un compte au niveau du système d'exploitation. Son fonctionnement est spécifique à chaque plate-forme. Si xp_cmdshell context est défini sur 1, pour pouvoir utiliser une ESP xp_cmdshell, un compte utilisateur doit exister au niveau du système d'exploitation pour le nom d'utilisateur Adaptive Server. Un utilisateur Adaptive Server ayant pour nom "sa", par exemple, ne pourra pas utiliser xp_cmdshell sauf s'il ou elle possède un compte utilisateur "sa" au niveau du système d'exploitation.

Sous Windows NT, lorsque xp_cmdshell context est défini sur 1, xp_cmdshell n'aboutit que si le nom employé par l'utilisateur pour se connecter à Adaptive Server est un nom d'utilisateur Windows NT correct avec des privilèges d'administrateur système Windows NT pour le système sur lequel est exécuté Adaptive Server.

Sur les autres plates-formes, lorsque xp_cmdshell context est défini sur 1, xp_cmdshell n'aboutit que si Adaptive Server a été démarré par un utilisateur possédant des privilèges de "superutilisateur" au niveau du système d'exploitation. Lorsque Adaptive Server reçoit une demande d'exécution de xp_cmdshell, il vérifie l'*uid* du nom de l'utilisateur du demandeur ESP et exécute la commande du système d'exploitation avec les autorisations de cet *uid*.

Si xp_cmdshell context est défini sur 0, les autorisations du compte du système d'exploitation sous lesquelles est exécuté Adaptive Server sont les autorisations utilisées pour exécuter une commande du système d'exploitation depuis xp_cmdshell. Les utilisateurs ont ainsi la possibilité d'exécuter des commandes du système d'exploitation qu'ils ne pourraient normalement pas exécuter dans le contexte de sécurité de leurs propres comptes de système d'exploitation.

## Informations générales

Le paramètre de ce groupe ne concerne aucun domaine particulier du fonctionnement d'Adaptive Server.

### *configuration file*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | N/A |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre configuration file spécifie l'emplacement du fichier de configuration en cours d'utilisation. Reportez-vous à la section "Utilisation de sp_configure avec un fichier de configuration", page 91 pour une description complète des fichiers de configuration.

Dans le résultat de sp_configure, la colonne "Run Value" n'affiche que 10 caractères. Le chemin d'accès et le nom complets de votre fichier de configuration n'apparaissent ainsi pas forcément dans le résultat.

## Services Java

Les paramètres de ce groupe activent et configurent la mémoire pour Java dans Adaptive Server. Reportez-vous au manuel *Java in Adaptive Server Enterprise* pour plus d'informations sur Java dans la base de données.

Si vous utilisez les appels de méthode à JDBC, vous aurez peut-être besoin d'augmenter la taille de la pile d'exécution disponible pour l'utilisateur. Pour plus d'informations sur le paramètre stack size, reportez-vous à la section "stack size", page 251.

### *enable java*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Plage de valeurs | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre enable java active et désactive Java dans la base de données Adaptive Server. Vous ne pouvez pas installer de classes Java ni exécuter des opérations Java si Java n'a pas été activé sur le serveur.

**Remarque** L'information de licence et la valeur d'exécution de enable java sont indépendantes l'une de l'autre. Que vous possédiez ou non une licence java, la valeur d'exécution et la valeur configurée sont définies sur 1 après le redémarrage d'Adaptive Server. Vous ne pouvez pas exécuter Java tant que vous ne possédez pas de licence. Si vous n'avez pas installé de licence valide, Adaptive Server enregistre un message d'erreur et n'active pas la fonctionnalité. Reportez-vous au Guide d'installation pour plus d'informations sur l'installation des clés de licence.

### *enable enterprise java beans*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Plage de valeurs | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre enable enterprise java beans active et désactive EJB Server dans la base de données Adaptive Server. Vous ne pouvez pas utiliser EJB Server si Adaptive Server n'est pas activé pour EJB Server.

**Remarque** L'information de licence et la valeur d'exécution de enable java beans sont indépendantes l'une de l'autre. Que vous possédiez ou non une licence java, la valeur d'exécution et la valeur configurée sont définies sur 1 après le redémarrage d'Adaptive Server. Vous ne pouvez pas exécuter EJB Server tant que vous ne possédez pas de licence. Si vous n'avez pas installé de licence valide, Adaptive Server enregistre un message d'erreur et n'active pas la fonctionnalité. Reportez-vous au Guide d'installation pour plus d'informations sur l'installation des clés de licence.

### *size of global fixed heap*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeurs par défaut | 150 pages (version 32 bits)<br>300 pages (version 64 bits) |
| Valeurs minimales | 10 pages (version 32 bits)<br>20 pages (version 64 bits) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre size of global fixed heap spécifie l'espace mémoire pour les structures de données internes et les autres besoins.

Si vous modifiez la taille du segment de mémoire fixe global, vous devez également modifier la mémoire logique totale de la même valeur.

### size of process object heap

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeurs par défaut | 1500 pages (version 32 bits)<br>3000 pages (version 64 bits) |
| Valeurs minimales | 45 pages (version 32 bits)<br>90 pages (version 64 bits) |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

Le paramètre size of process object fixed heap spécifie l'espace mémoire total pour tous les processus qui utilisent la machine virtuelle Java.

Si vous modifiez la taille du segment de mémoire fixe du processus objet, vous devez également modifier la mémoire logique totale de la même valeur.

### size of shared class heap

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeurs par défaut | 1536 pages (version 32 bits)<br>3072 pages (version 64 bits) |
| Valeurs minimales | 650 pages (version 32 bits)<br>1300 pages (version 64 bits) |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

Le paramètre size of shared class heap spécifie l'espace mémoire partagé pour toutes les classes Java appelées dans la machine virtuelle Java. Adaptive Server maintient le segment de mémoire de classe partagée sur tout le serveur pour les classes Java définies par l'utilisateur et fournies par le système.

Si vous modifiez la taille du segment de mémoire de classe partagée, vous devez également modifier la mémoire logique totale de la même valeur.

## Langues

Les paramètres de ce groupe permettent de configurer les langues, les jeux de caractères et les ordres de tri.

### *default character set id*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | default character set id |
| Valeur par défaut | 1 |
| Plage de valeurs | 0–255 |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Le paramètre default character set id spécifie le numéro du jeu de caractères par défaut utilisé par le serveur. Le jeu par défaut est défini au moment de l'installation et peut être modifié ultérieurement avec les utilitaires d'installation Sybase. Reportez-vous au chapitre 7, "Configuration des jeux de caractères, des ordres de tri et des langues", pour une description de la manière de changer les jeux de caractères et les ordres de tri.

### *default language id*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | langue par défaut |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–32767 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Le paramètre default language id est le numéro d'identification de la langue utilisée pour afficher les messages système, sauf si un utilisateur a choisi une autre langue parmi celles disponibles sur le serveur. La langue us_english (anglais américain) a toujours un ID NULL. Un numéro unique est affecté à chaque langue supplémentaire ajoutée.

### *default sortorder id*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | default sortorder id |
| Valeur par défaut | 50 |
| Plage de valeurs | 0–255 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre default sortorder id est le numéro d'ordre de tri qui est installé par défaut sur le serveur. Reportez-vous au chapitre 7, "Configuration des jeux de caractères, des ordres de tri et des langues". pour modifier l'ordre de tri par défaut.

### *disable character set conversions*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (activé) |
| Valeurs correctes | 0 (activé), 1 (désactivé) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

En donnant au paramètre disable character set conversions la valeur 1, vous désactivez la conversion du jeu de caractères pour les données échangées entre les clients et Adaptive Server. Par défaut, Adaptive Server effectue une conversion des données en provenance et à destination des clients qui emploient des jeux de caractères différents de ceux du serveur. Si certains clients utilisent le jeu de caractères Latin-1 (iso_1), par exemple, et qu'Adaptive Server utilise Roman-8 (roman8) comme jeu de caractères par défaut, les données en provenance des clients sont converties en Roman-8 lors de leur chargement dans Adaptive Server. Pour les clients qui utilisent Latin-1, les données sont de nouveau converties lorsqu'elles sont envoyées au client et ne sont pas converties pour les clients qui utilisent le même jeu de caractères qu'Adaptive Server.

Vous pouvez empêcher toute conversion en activant le paramètre disable character set conversions. Si tous les clients utilisent un jeu de caractères donné, par exemple, et que vous voulez qu'Adaptive Server stocke toutes les données dans ce jeu de caractères, vous pouvez définir disable character set conversions sur 1 pour qu'aucune conversion n'ait lieu.

## Gestionnaire de verrous

Les paramètres de ce groupe configurent les verrous.

### *lock address spinlock ratio*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 100 |
| Plage de valeurs | 1–2147483647 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Si Adaptive Server est exécuté avec plusieurs moteurs, le paramètre address lock spinlock ratio définit le nombre de lignes de la table de hachage des verrous d'adresse internes qui sont protégées par un verrou d'attente.

Adaptive Server gère l'acquisition et la libération des verrous d'adresse en utilisant une table de hachage interne composée de 1031 lignes (également appelées compartiments de hachage). Cette table peut utiliser un ou plusieurs verrous d'attente pour traiter en série l'accès entre des processus exécutés sur différents moteurs.

La valeur par défaut de address lock spinlock ratio pour Adaptive Server est 100, ce qui définit 11 verrous d'attente pour la table de hachage des verrous d'adresse. Les 10 premiers verrous d'attente protègent chacun 100 lignes et le onzième verrou d'attente protège les 31 lignes restantes. Si vous indiquez une valeur égale ou supérieure à 1031 pour address lock spinlock ratio, Adaptive Server utilise alors un seul verrou d'attente pour toute la table.

### *number of locks*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | locks |
| Valeur par défaut | 5000 |
| Plage de valeurs | 1000–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

Le paramètre number of locks définit le nombre total de verrous disponibles pour tous les utilisateurs sur Adaptive Server.

Le nombre total de verrous requis par Adaptive Server dépend du nombre et de la nature des requêtes en cours d'exécution. Le nombre de verrous requis par une requête peut varier considérablement en fonction du nombre de traitements parallèles simultanés et du type d'action exécutée par les transactions. Utilisez sp_lock pour connaître le nombre de verrous utilisés à un moment particulier.

Pour les opérations de traitement en série, il est recommandé de commencer par un nombre arbitraire de 20 verrous pour chaque connexion active simultanément.

L'exécution en parallèle requiert davantage de verrous que l'exécution en série. Si vous constatez, par exemple, qu'une requête emploie en moyenne cinq processus de travail, essayez d'augmenter d'un tiers la valeur number of locks configurée pour un traitement en série.

Lorsque tous les verrous du système sont épuisés, Adaptive Server affiche un message d'erreur de niveau serveur. Si les utilisateurs signalent des erreurs de verrou, celles-ci sont généralement résolues en augmentant la valeur de number of locks ; mais n'oubliez pas que les verrous occupent de la mémoire. Pour plus d'informations, reportez-vous à la section "Nombre de verrous", page 633.

**Remarque** Le verrouillage des lignes de données vous imposera peut-être de modifier la valeur de number of locks. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### *deadlock checking period*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 500 |
| Plage de valeurs | 0–2147483 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre deadlock checking period spécifie la durée minimale (en millisecondes) avant qu'Adaptive Server n'amorce une recherche des interblocages pour un processus en attente de libération d'un verrou. La recherche des interblocages est une perte de temps inutile pour les applications qui ne rencontrent aucun ou très peu d'interblocages et le surcoût augmente à mesure que le pourcentage de demandes de verrou en attente d'un verrou augmente également.

Si vous définissez ce paramètre sur une valeur différente de zéro (*n)*, Adaptive Server lance une recherche des interblocages lorsqu'un processus aura attendu pendant au moins *n* millisecondes.Vous pouvez, par exemple, demander à un processus d'attendre un verrou pendant au moins 700 millisecondes avant chaque recherche des interblocages de la manière suivante :

```
sp_configure "deadlock checking period", 700
```

Si vous définissez ce paramètre sur 0, Adaptive Server lance la recherche des interblocages dès que le processus commence à attendre un verrou. Toute valeur inférieure au nombre de millisecondes dans une impulsion d'horloge est considérée égale à 0. Reportez-vous à la section "sql server clock tick length", page 227 pour plus d'informations.

Plus la valeur de deadlock checking period est élevée, plus le processus attendra avant que les interblocages ne soient détectés. Cependant, comme Adaptive Server accorde la plupart des verrous demandés avant que le temps d'attente imparti ne se soit écoulé, les processus concernés ne subissent pas le surplus de travail généré par la recherche des interblocages. Si l'interblocage est peut fréquent dans vos applications, définissez une valeur plus élevée pour deadlock checking period afin d'éviter le surplus de travail lié à la recherche des interblocages sur tous les processus. Dans le cas contraire, la valeur par défaut de 500 devrait faire l'affaire.

Utilisez sp_sysmon pour déterminer la fréquence des interblocages dans votre système et la meilleure valeur pour deadlock checking period. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### *deadlock retries*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 5 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

deadlock retries indique le nombre de fois où la transaction peut faire une nouvelle tentative pour acquérir un verrou lorsque l'interblocage se produit pendant un rétrécissement ou une **page suspecte** d'index.

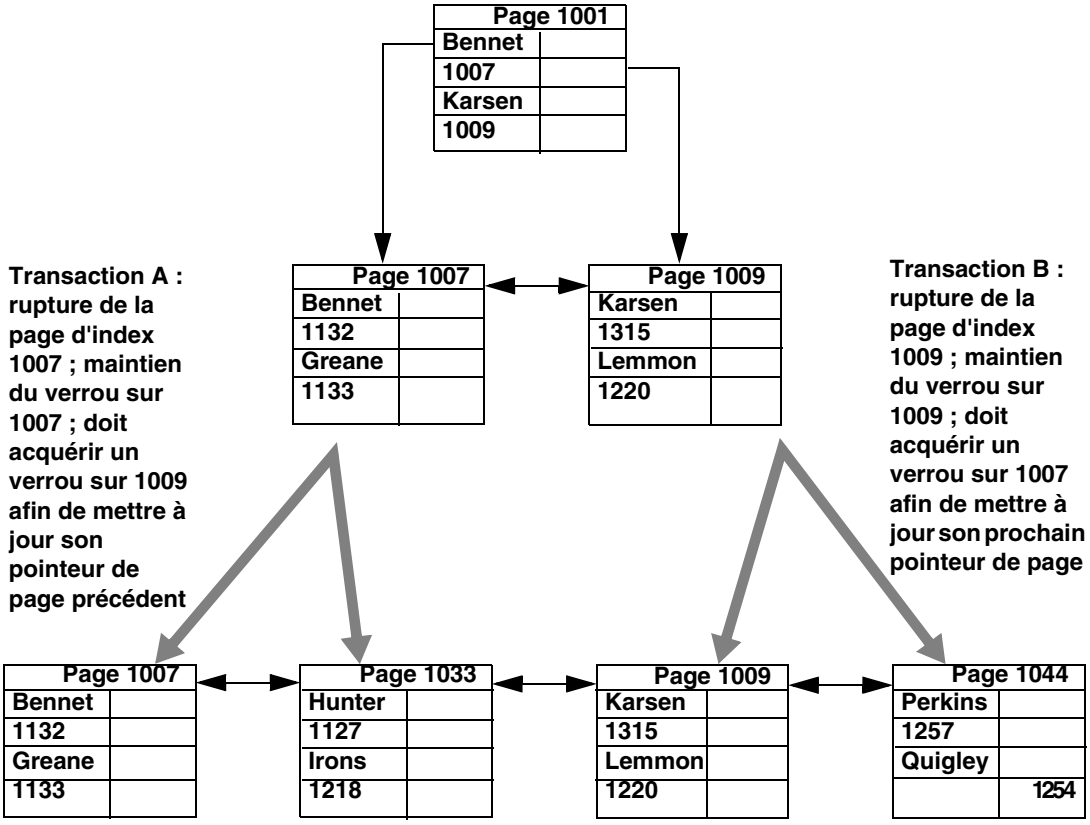
La figure 5-4, par exemple, illustre le scénario suivant :

- La transaction A verrouille la page 1007 et doit acquérir un verrou sur la page 1009 pour mettre à jour les pointeurs de page pour une rupture de page.
- La transaction B insère également une ligne d'index qui provoque une rupture de page, maintient un verrou sur la page 1009 et doit acquérir un verrou sur la page 1007.

Dans cette situation, plutôt que de choisir immédiatement un processus comme victime de l'interblocage, Adaptive Server renonce aux verrous d'index pour l'une des transactions. Cela permet souvent à l'autre transaction de se terminer et de libérer ses verrous.

Pour la transaction qui a abandonné sa tentative de verrouillage, l'index est une nouvelle fois balayé depuis la page d'origine et l'opération de rupture de page est de nouveau tentée le nombre de fois indiqué par deadlock retries.

***Figure 5-4 : Interblocages pendant une rupture de page dans un index clusterisé***




sp_sysmon signale les interblocages et les tentatives. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

## *lock spinlock ratio*

| **Récapitulatif** | |
|---|---|
| Valeur par défaut | 85 |
| Plage de valeurs | 1–2147483647 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Adaptive Server gère l'acquisition et la libération des verrous en utilisant une table de hachage interne composée d'un nombre paramétrable de compartiments de hachage. Sur les systèmes SMP, cette table de hachage peut utiliser un ou plusieurs verrous d'attente pour traiter en série l'accès entre des processus exécutés sur différents moteurs. Pour définir le nombre de compartiments de hachage, utilisez lock hashtable size.

Si Adaptive Server est exécuté avec plusieurs moteurs, le paramètre lock spinlock ratio définit le nombre de compartiments de hachage de verrou qui sont protégés par un verrou d'attente. Si vous augmentez lock hashtable size, le nombre de verrous d'attente augmente et le nombre de compartiments de hachage protégés par un verrou d'attente reste ainsi le même.

La valeur par défaut d'Adaptive Server pour lock spinlock ratio est 85. Si lock hashtable size est à sa valeur par défaut de 2048, le rapport par défaut des verrous d'attente définit 26 verrous d'attente pour la table de hachage de verrou. Pour plus d'informations sur la configuration des rapports de verrou d'attente, reportez-vous à la section "Configuration des paramètres de taux de verrous d'attente", page 691 du *Guide d'administration système*.

sp_sysmon indique la longueur moyenne des chaînes de hachage dans la table de hachage de verrou. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### *lock hashtable size*

| **Récapitulatif** | |
|---|---|
| Valeur par défaut | 2048 |
| Plage de valeurs | 1–2147483647 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre de configuration lock hashtable size configure le nombre de *compartiments de hachage* contenus dans la table de hachage de verrou. Cette table gère tous les verrous de ligne, de page et de table et toutes les demandes de verrou. A chaque fois qu'une tâche acquiert un verrou, celui-ci est assigné à un compartiment de hachage et chaque demande de verrou pour ce verrou contrôle le même compartiment de hachage. Si cette valeur est trop faible, le nombre de verrous dans chaque compartiment de hachage sera élevé, ce qui ralentira les recherches. Sur les Adaptive Server dotés de plusieurs moteurs, une valeur trop faible peut également donner lieu à un nombre accru de conflits de verrou d'attente. Ne définissez pas cette valeur en dessous de la valeur par défaut qui est 2048.

lock hashtable size doit être une puissance de 2. Si la valeur que vous indiquez n'est pas une puissance de 2, sp_configure arrondit la valeur à la puissance de 2 immédiatement supérieure et imprime un message d'information.

La taille optimale de la table de hachage est une fonction du nombre d'objets distincts (pages, tables et lignes) qui seront verrouillés simultanément. La taille optimale de la table de hachage est au moins égale à 20 % du nombre d'objets distincts qui doivent être verrouillés simultanément. Reportez-vous au document *Performances et optimisation* pour plus d'informations sur la configuration de la taille des tables de hachage de verrou.

### *lock scheme*

| **Récapitulatif** | |
|---|---|
| Valeur par défaut | allpages (toutes les pages) |
| Plage de valeurs | allpages, datapages, datarows (toutes les pages, pages de données, lignes de données) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

lock scheme détermine le plan de verrouillage par défaut qui sera utilisé par les commandes create table et select into lorsqu'un plan de verrouillage n'est pas précisé dans la commande.

Les valeurs du paramètre lock scheme sont des chaînes de caractères, vous devez donc placer un 0 comme marque de réservation du deuxième paramètre qui doit être numérique et spécifier allpages, datapages ou datarows comme troisième paramètre :

```
sp_configure "lock scheme", 0, datapages
```

### lock wait period

| Récapitulatif | |
|---|---|
| Valeur par défaut | 2147483647 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

lock wait period limite la durée en secondes pendant laquelle une tâche attend d'acquérir un verrou sur une table, une page de données ou une ligne de données. Si la tâche n'acquiert pas le verrou pendant la période indiquée, Adaptive Server renvoie le message d'erreur 12205 à l'utilisateur et annule la transaction.

L'option lock wait de la commande set définit une durée en secondes applicable à toute la session pendant laquelle une tâche attendra un verrou. Elle remplace le paramètre au niveau serveur pour la session.

Avec la valeur par défaut, tous les processus attendent indéfiniment des verrous. Pour rétablir la valeur par défaut, redéfinissez la valeur sur 2147483647 ou utilisez :

```
sp_configure "lock wait period", 0, "default"
```

### read committed with lock

| Récapitulatif | |
|---|---|
| Valeur par défaut | 0 (désactivé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

read committed with lock détermine si un Adaptive Server qui emploie le niveau d'isolation 1 pour les transactions (lecture validée) maintient des verrous partagés sur les lignes ou les pages des tables en mode verrouillage des données seules pendant les requêtes select. Pour les curseurs, cette option ne s'applique qu'aux curseurs déclarés en lecture seule. Ce paramètre est désactivé par défaut pour réduire les conflits de verrouillage et les blocages. Ce paramètre n'affecte que les requêtes sur les tables en mode verrouillage des données seules.

Pour un isolement de transactions de niveau 1, les requêtes select sur les tables en mode verrouillage de toutes les pages continuent à maintenir les verrous sur la page dans la position courante. Tout curseur pouvant être mis à jour sur une table en mode verrouillage des données seules maintient également les verrous sur la page ou la ligne courante. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### *lock table spinlock ratio*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 20 |
| Plage de valeurs | 1–2147483647 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Si Adaptive Server est exécuté avec plusieurs moteurs, le paramètre de configuration table lock spinlock ratio définit le nombre de lignes de la table de hachage des verrous de tables internes qui sont protégées par un **spinlock**.

Adaptive Server gère l'acquisition et la libération des verrous de table en utilisant une table de hachage interne composée de 101 lignes (également appelées compartiments de hachage). Cette table peut utiliser un ou plusieurs verrous d'attente pour traiter en série l'accès entre des processus exécutés sur différents moteurs.

La valeur par défaut de table lock spinlock ratio pour Adaptive Server est 20, ce qui définit 6 verrous d'attente pour la table de hachage des verrous de table. Les 5 premiers verrous d'attente protègent chacun 20 lignes et le sixième verrou d'attente protège la dernière ligne. Si vous indiquez une valeur égale ou supérieure à 101 pour table lock spinlock ratio, Adaptive Server utilise alors un seul verrou d'attente pour toute la table.

## Utilisation de la mémoire

Le paramètre suivant optimise l'utilisation de la mémoire par Adaptive Server :

### *executable codesize + overhead*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | sql server code size |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–2147483647 |
| Etat | Calculé |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

executable codesize + overhead indique la taille combinée (en kilo-octets) de la mémoire pour Adaptive Server exécutable et le surplus. Il s'agit d'une valeur calculée que l'utilisateur ne peut pas modifier.

## Caches de métadonnées

Les paramètres suivants déterminent la taille du cache de métadonnées pour les informations fréquemment utilisées du catalogue système. Le *cache de métadonnées* est une zone réservée de la mémoire utilisée pour analyser les informations sur les bases de données, les index ou les objets. Plus le nombre de bases de données, d'index ou d'objets ouverts est grand, plus la taille du cache de métadonnées est élevée. La section "Bases de données, index et objets ouverts", page 632 traite des caches de métadonnées dans un contexte d'utilisation de la mémoire.

### *number of open databases*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | open databases |
| Valeur par défaut | 12 |
| Plage de valeurs | 5–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

number of open databases définit le nombre maximum de bases de données pouvant être ouvertes simultanément sur Adaptive Server.

Lorsque vous calculez une valeur, incluez les bases de données système master, model, sybsystemprocs et tempdb. Si vous avez installé le système d'audit, incluez la base de données sybsecurity. Comptabilisez également les bases de données d'exemples pubs2 et pubs3, la base de données de syntaxe sybsyntax et la base de données dbcc dbccdb si elles sont installées.

Si vous prévoyez d'apporter des modifications substantielles comme le chargement d'une base de données de grande taille depuis un autre serveur, vous pouvez calculer une taille estimée du cache de métadonnées en utilisant sp_helpconfig. sp_helpconfig affiche l'espace mémoire requis pour un nombre donné de descripteurs de métadonnées ainsi que le nombre de descripteurs qui peuvent être logés dans un espace mémoire donné. Un descripteur de métadonnées de base de données représente l'état de la base de données pendant qu'elle est utilisée ou mise en cache entre les utilisations.

### Optimisation du paramètre *number of open databases* pour votre système

Si Adaptive Server affiche un message vous indiquant que vous avez dépassé le nombre total autorisé de bases de données ouvertes, vous devrez corriger la valeur.

Procédez comme suit pour optimiser le paramètre de configuration number of open databases :

- Etape 1 : Déterminez le nombre total de bases de données (descripteurs de métadonnées de base de données).
- Etape 2 : Affectez ce nombre à number of open databases.
- Etape 3 : Recherchez le nombre de bases de données actives (descripteurs de métadonnées de base de données) pendant une période de pointe.
- Etape 4 : Affectez ce nombre plus 10 % à number of open databases.

La section suivante détaille les étapes de base mentionnées ci-dessus.

1 Utilisez la procédure système sp_countmetadata pour rechercher le nombre total de descripteurs de métadonnées de base de données. Exemple :

```
sp_countmetadata "open databases"
```

Le meilleur moment pour exécuter sp_countmetadata est une période de faible activité du serveur. L'exécution de sp_countmetadata pendant une période de pointe peut provoquer des conflits avec d'autres processus.

Supposons qu'Adaptive Server renvoie les informations suivantes :

```
There are 50 databases, requiring 1719 Kbytes of
memory. The 'open databases' configuration
parameter is currently set to 500.
```

2 Affectez la valeur 50 à number of open databases :

```
sp_configure "number of open databases", 50
```

Cette nouvelle configuration est seulement un point de départ. La taille idéale doit se baser sur le nombre de descripteurs de cache de métadonnées de base de données *actifs*, et non pas sur le nombre *total* de bases de données.

3 Recherchez le nombre de descripteurs de métadonnées actifs pendant une période de pointe. Exemple :

```
sp_monitorconfig "open databases"
Usage information at date and time: Jan 14 1997  8:54AM.
Name            # Free   # Active   % Active  # Max Ever Used   Re-used
--------------  --------  --------   --------  ---------------   -------
number of open  50        20       40.00      26                No
databases
```

20 descripteurs de métadonnées de base de données sont actifs pendant cette période de pointe, le nombre maximum de descripteurs qui ont été actifs depuis le dernier démarrage du serveur est 26.

Pour plus d'informations, reportez-vous à la section sp_monitorconfig dans le document *Manuel de référence d'Adaptive Server*.

4 Affectez au paramètre number of open databases la valeur 26, plus un espace supplémentaire de 10 % (environ 3), soit un total de 29 :

```
sp_configure "number of open databases", 29
```

Exécutez régulièrement sp_monitorconfig s'il y a beaucoup d'activité sur le serveur, par exemple si des bases de données ont été ajoutées ou supprimées. Vous devrez corriger la taille du cache lorsque le nombre de descripteurs actifs change.

### *number of open indexes*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 500 |
| Plage de valeurs | 100–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

number of open indexes définit le nombre maximum d'index pouvant être ouverts simultanément sur Adaptive Server.

Si vous prévoyez d'apporter des modifications substantielles comme le chargement d'une base de données possédant un grand nombre d'index depuis un autre serveur, vous pouvez calculer une taille estimée du cache de métadonnées en utilisant sp_helpconfig. sp_helpconfig affiche l'espace mémoire requis pour un nombre donné de descripteurs de métadonnées ainsi que le nombre de descripteurs qui peuvent être logés dans un espace mémoire donné. Un descripteur de métadonnées d'index représente l'état d'un index pendant qu'il est utilisé ou mis en cache entre les utilisations.

Optimisation du paramètre *number of open indexes* pour votre système

La valeur d'exécution par défaut est 500. Si ce nombre est insuffisant, Adaptive Server affiche un message après avoir essayé de réutiliser des descripteurs d'index actifs et vous devrez corriger cette valeur.

Procédez comme suit pour optimiser le paramètre de configuration number of open indexes :

1 Utilisez la procédure système sp_countmetadata pour rechercher le nombre total de descripteurs de métadonnées d'index. Exemple :

```
sp_countmetadata "open indexes"
```

Le meilleur moment pour exécuter sp_countmetadata est une période de faible activité du serveur. L'exécution de sp_countmetadata pendant une période de pointe peut provoquer des conflits avec d'autres processus.

Supposons qu'Adaptive Server renvoie les informations suivantes :

```
Il y a 698 index d'utilisateur dans toutes les
bases de données et ceux-ci nécessitent 286 289
Ko de mémoire. Le paramètre de configuration
'open indexes' est actuellement défini sur 500.
```

2 Affectez la valeur 698 à number of open indexes de la manière suivante :

```
sp_configure "number of open indexes", 698
```

Cette nouvelle configuration est seulement un point de départ. La taille idéale doit se baser sur le nombre de descripteurs de cache de métadonnées d'index *actifs*, et non pas sur le nombre total d'index.

3 Recherchez le nombre de descripteurs de métadonnées d'index actifs pendant une période de pointe. Exemple :

```
sp_monitorconfig "open indexes"
Usage information at date and time: Jan 14 1997  8:54AM.
Name            # Free   # Active   % Active  # Max Ever Used   Re-used
--------------  --------  --------   --------  ---------------   -------
number of open  182        516       73,92      590                No
indexes
```

Dans cet exemple, 590 est le nombre maximum de descripteurs de métadonnées d'index qui ont été utilisés depuis le dernier démarrage du serveur.

Pour plus d'informations, reportez-vous à la section sp_monitorconfig dans le document *Manuel de référence d'Adaptive Server*.

4 Affectez au paramètre number of open indexes la valeur 590, plus un espace supplémentaire de 10 % (59), soit un total de 649 :

```
sp_configure "number of open indexes", 649
```

Exécutez régulièrement sp_monitorconfig s'il y a beaucoup d'activité sur le serveur, par exemple si des tables ont été ajoutées ou supprimées. Vous devrez corriger la taille du cache lorsque le nombre de descripteurs actifs change.

### *number of open objects*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | open objects |
| Valeur par défaut | 500 |
| Plage de valeurs | 100–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

number of open objects définit le nombre maximum d'objets pouvant être ouverts simultanément sur Adaptive Server.

Si vous prévoyez d'apporter des modifications substantielles comme le chargement d'une base de données possédant un grand nombre d'objets depuis un autre serveur, vous pouvez calculer une taille estimée du cache de métadonnées en utilisant sp_helpconfig. sp_helpconfig affiche l'espace mémoire requis pour un nombre donné de descripteurs de métadonnées ainsi que le nombre de descripteurs qui peuvent être logés dans un espace mémoire donné. Un descripteur de métadonnées d'objet représente l'état d'un objet pendant qu'il est utilisé ou mis en cache entre les utilisations.

### Optimisation du paramètre *number of open objects* pour votre système

La valeur d'exécution par défaut est 500. Si ce nombre est insuffisant, Adaptive Server affiche un message après avoir essayé de réutiliser des descripteurs d'objet actifs. Vous devrez corriger cette valeur.

Procédez comme suit pour optimiser le paramètre de configuration number of open objects :

1. Utilisez la procédure système sp_countmetadata pour rechercher le nombre total de descripteurs de métadonnées d'objet. Exemple :

   ```
   sp_countmetadata "open objects"
   ```

   Le meilleur moment pour exécuter sp_countmetadata est une période de faible activité du serveur. L'exécution de sp_countmetadata pendant une période de pointe peut provoquer des conflits avec d'autres processus.

   Supposons qu'Adaptive Server renvoie les informations suivantes :

   ```
   Il y a 340 objets d'utilisateur dans toutes les
   bases de données et ceux-ci nécessitent 140 781
   Ko de mémoire. Le paramètre de configuration
   'open objects' est actuellement défini sur 500.
   ```

2. Affectez cette valeur au paramètre number of open objects de la manière suivante :

   ```
   sp_configure "number of open objects", 357
   ```

   357 couvre les 340 objets d'utilisateur plus 5 % pour supporter les tables temporaires.

   Cette nouvelle configuration est seulement un point de départ. La taille idéale doit se baser sur le nombre de descripteurs de cache de métadonnées d'objet *actifs*, et non pas sur le nombre *total* d'objets.

3 Recherchez le nombre de descripteurs de cache de métadonnées actifs pendant une période de pointe, par exemple :

```
                sp_monitorconfig "open objects"
Usage information at date and time: Jan 14 1997  8:54AM.
Name            # Free   # Active   % Active  # Max Ever Used   Re-used
--------------  --------  --------   --------   ---------------   -------
number of open  160        357       71,40      397                No
objects
```

Dans cet exemple, 397 est le nombre maximum de descripteurs d'objet qui ont été utilisés depuis le dernier démarrage du serveur.

4 Affectez au paramètre number of open objects la valeur 397, plus 10 % (40), soit un total de 437 :

```
sp_configure "number of open objects", 437
```

Exécutez régulièrement sp_monitorconfig s'il y a beaucoup d'activité sur le serveur, par exemple si des tables ont été ajoutées ou supprimées. Vous devrez corriger la taille du cache lorsque le nombre de descripteurs actifs change. Pour plus d'informations, reportez-vous à la section sp_monitorconfig dans le *Manuel de référence d'Adaptive Server*.

### *open index hash spinlock ratio*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 100 |
| Plage de valeurs | 1–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

open index hash spinlock ratio définit le nombre de tables de hachage de descripteur de métadonnées d'index qui sont protégées par un **spinlock**. Ce paramètre est uniquement utilisé pour les systèmes multitraitement.

Tous les descripteurs d'index qui font partie de la table sont accessibles par le biais d'une table de hachage. Lorsqu'une requête est exécutée sur la table, Adaptive Server utilise des tables de hachage pour rechercher les informations d'index nécessaires dans ses lignes sysindexes. Une table de hachage est un mécanisme interne utilisé par Adaptive Server pour rechercher rapidement des informations.

Vous n'avez normalement pas besoin de modifier ce paramètre. Dans quelques rares cas, toutefois, vous devrez le réinitialiser si Adaptive Server présente des conflits provoqués par les verrous d'attente de hachage. Vous pouvez obtenir des informations sur les conflits de verrous d'attente en utilisant sp_sysmon. Pour plus d'informations sur sp_sysmon, reportez-vous au document *Performances et optimisation*.

Pour plus d'informations sur la configuration des rapports des verrous d'attente, reportez-vous à la section "Configuration des paramètres de taux de verrous d'attente", page 691.

### *open index spinlock ratio*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 100 |
| Plage de valeurs | 1–214748364 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

open index spinlock ratio définit le nombre de descripteurs de métadonnées d'index qui sont protégés par un **spinlock**.

Adaptive Server utilise un verrou d'attente pour protéger un descripteur d'index, car plusieurs processus peuvent accéder au contenu du descripteur d'index. Ce paramètre est uniquement utilisé pour les systèmes multitraitement.

La valeur de ce paramètre définit la proportion de descripteurs d'index par verrou d'attente.

Si un verrou d'attente est partagé par un nombre excessif de descripteurs d'index, il peut provoquer un conflit de verrous d'attente. Utilisez sp_sysmon pour obtenir un rapport sur les conflits entre verrous d'attente. Reportez-vous au document *Performances et optimisation* pour plus d'informations Si le résultat de sp_sysmon indique un conflit de verrou d'attente de descripteur d'index de plus de 3 %, essayez de réduire la valeur du paramètre open index spinlock ratio.

Pour plus d'informations sur la configuration des rapports des verrous d'attente, reportez-vous à la section "Configuration des paramètres de taux de verrous d'attente", page 691.

### *open object spinlock ratio*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 100 |
| Plage de valeurs | 1–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

open object spinlock ratio définit le nombre de descripteurs d'objet qui sont protégés par un **spinlock**. Adaptive Server utilise un verrou d'attente pour protéger un descripteur d'objet, car plusieurs processus peuvent accéder au contenu du descripteur d'objet. Ce paramètre est uniquement utilisé pour les systèmes multitraitement.

La valeur par défaut de ce paramètre est 100 ; 1 verrou d'attente pour 100 descripteurs d'objet configurés sur votre système. Si votre serveur est configuré avec un seul moteur, Adaptive Server définit un seul verrou d'attente de descripteur d'objet, indépendamment du nombre de descripteurs d'objet.

Si un verrou d'attente est partagé par un nombre excessif de descripteurs d'objet, il provoque un conflit de verrous d'attente. Utilisez sp_sysmon pour obtenir un rapport sur les conflits entre verrous d'attente. Pour plus d'informations sur les conflits entre verrous d'attente, reportez-vous au document *Performances et optimisation*. Si le résultat de sp_sysmon indique un conflit de verrou d'attente de descripteur d'objet de plus de 3 %, essayez de réduire la valeur du paramètre open object spinlock ratio.

Pour plus d'informations sur la configuration des rapports des verrous d'attente, reportez-vous à la section "Configuration des paramètres de taux de verrous d'attente", page 691.

## Communication en réseau

Les paramètres de ce groupe permettent de configurer les communications entre Adaptive Server et des serveurs distants et entre Adaptive Server et les programmes clients.

### allow remote access

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | remote access |
| Valeur par défaut | 1 (activé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Responsable de la sécurité du système (SSO) |

allow remote access contrôle les connexions depuis des Adaptive Server distants. La valeur par défaut de 1 permet à Adaptive Server de communiquer avec Backup Server. Seul un responsable de la sécurité du système (SSO) peut définir le paramètre allow remote access.

Une valeur 0 désactive les RPC de serveur à serveur. Comme Adaptive Server communique avec Backup Server via les RPC, le fait de définir ce paramètre sur 0 rend impossible la sauvegarde d'une base de données.

Le fait de laisser cette option sur 1 ne constitue par un risque pour la sécurité, car d'autres actions d'administration sont nécessaires pour permettre aux serveurs distants autres que Backup Server d'exécuter des RPC.

### allow sendmsg

| Récapitulatif | |
|---|---|
| Valeur par défaut | 0 (désactivé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Responsable de la sécurité du système (SSO) |

Le paramètre allow sendmsg active ou désactive l'envoi de messages depuis Adaptive Server vers un port UDP (User Datagram Protocol - protocole de datagramme utilisateur). Lorsque allow sendmsg est défini sur 1, n'importe quel utilisateur peut envoyer des messages à l'aide de sp_sendmsg ou de syb_sendmsg. Pour définir le numéro du port utilisé par Adaptive Server, reportez-vous à la section "syb_sendmsg port number", page 171.

**Remarque** L'envoi de messages vers des ports UDP n'est pas supporté sous Windows NT.

### *default network packet size*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | default network packet size |
| Valeur par défaut | 512 |
| Plage de valeurs | 512–524288 |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

default network packet size détermine la taille de paquet par défaut pour tous les utilisateurs d'Adaptive Server. Vous pouvez définir default network packet size sur tout multiple de 512 octets ; les valeurs qui ne sont pas des multiples pairs de 512 sont arrondies vers le bas.

La mémoire pour tous les utilisateurs qui se connectent avec la taille de paquet par défaut est allouée depuis la zone de mémoire d'Adaptive Server telle qu'elle a été définie avec le paramètre total logical memory. Cette mémoire est allouée aux paquets du réseau au démarrage d'Adaptive Server.

Chaque connexion d'utilisateur d'Adaptive Server utilise :

- Un buffer de lecture
- Un buffer pour les messages
- Un buffer d'écriture

Chacun de ces buffers a besoin de default network packet size octets. L'espace mémoire total alloué pour les paquets du réseau est :

```
(number of user connections + number of worker processes) * 3 * default network
packet size
```

Si vous définissez le paramètre default network packet size sur 1024 octets, par exemple, et que vous avez 50 connexions utilisateur et 20 processus de travail, l'espace mémoire de réseau requis est :

(50 + 20) * 3 * 1024 = 215 040 octets

Si vous augmentez la valeur de default network packet size, vous devez également augmenter la valeur de max network packet size pour qu'elle soit au moins égale à celle du premier paramètre. Si la valeur de max network packet size est supérieure à la valeur de default network packet size, augmentez la valeur de additional network memory. Pour plus d'informations, reportez-vous à la section "additional network memory", page 184.

Utilisez sp_sysmon pour observer comment les modifications de la valeur de default network packet size affectent la gestion des E/S réseau et le basculement entre les tâches. Essayez, par exemple, d'augmenter default network packet size et vérifiez ensuite le résultat de sp_sysmon pour voir comment cela affecte bcp pour de grands batch. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

#### Demander une taille de paquet supérieure lors de la connexion

La taille de paquet par défaut pour la majorité des programmes clients comme bcp et isql est définie sur 512 octets. Si vous modifiez la taille de paquet par défaut, les clients doivent demander une taille de paquet plus grande lorsqu'ils se connectent. Utilisez l'argument -A avec les programmes clients d'Adaptive Server pour demander une taille de paquet supérieure. Exemple :

```
isql -A2048
```

### *max network packet size*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | maximum network packet size |
| Valeur par défaut | 512 |
| Plage de valeurs | 512–524288 |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

max network packet size spécifie la taille maximale d'un paquet de réseau qui peut être demandée par les clients qui communiquent avec Adaptive Server.

Si certaines de vos applications envoient ou reçoivent de grands volumes de données par le biais du réseau, vous pouvez nettement améliorer les performances de ces applications en augmentant la taille des paquets de réseau. C'est le cas des opérations de copie de masse et des applications qui lisent ou écrivent des valeurs de type text ou image importantes.

Vous voulez généralement :

- Que la valeur de default network packet size soit suffisamment faible pour les utilisateurs qui exécutent des requêtes courtes
- Que la valeur de max network packet size soit suffisamment grande pour permettre aux utilisateurs qui envoient ou reçoivent des grands volumes de données de demander des tailles de paquet plus grandes

max network packet size doit toujours être égal ou supérieur à default network packet size. Les valeurs qui ne sont pas des multiples pairs de 512 sont arrondies vers le bas.

Pour les applications clientes qui demandent explicitement une taille de paquet de réseau plus grande pour la recevoir, vous devez également configurer de la mémoire réseau supplémentaire. Pour plus d'informations, reportez-vous à la section "additional network memory", page 184.

Reportez-vous aux sections bcp et isql dans le *Guide Utilitaires* pour plus d'informations sur l'utilisation de tailles de paquet supérieures pour ces programmes. La documentation Open Client Client-Library contient des informations sur l'utilisation de tailles de paquet variables.

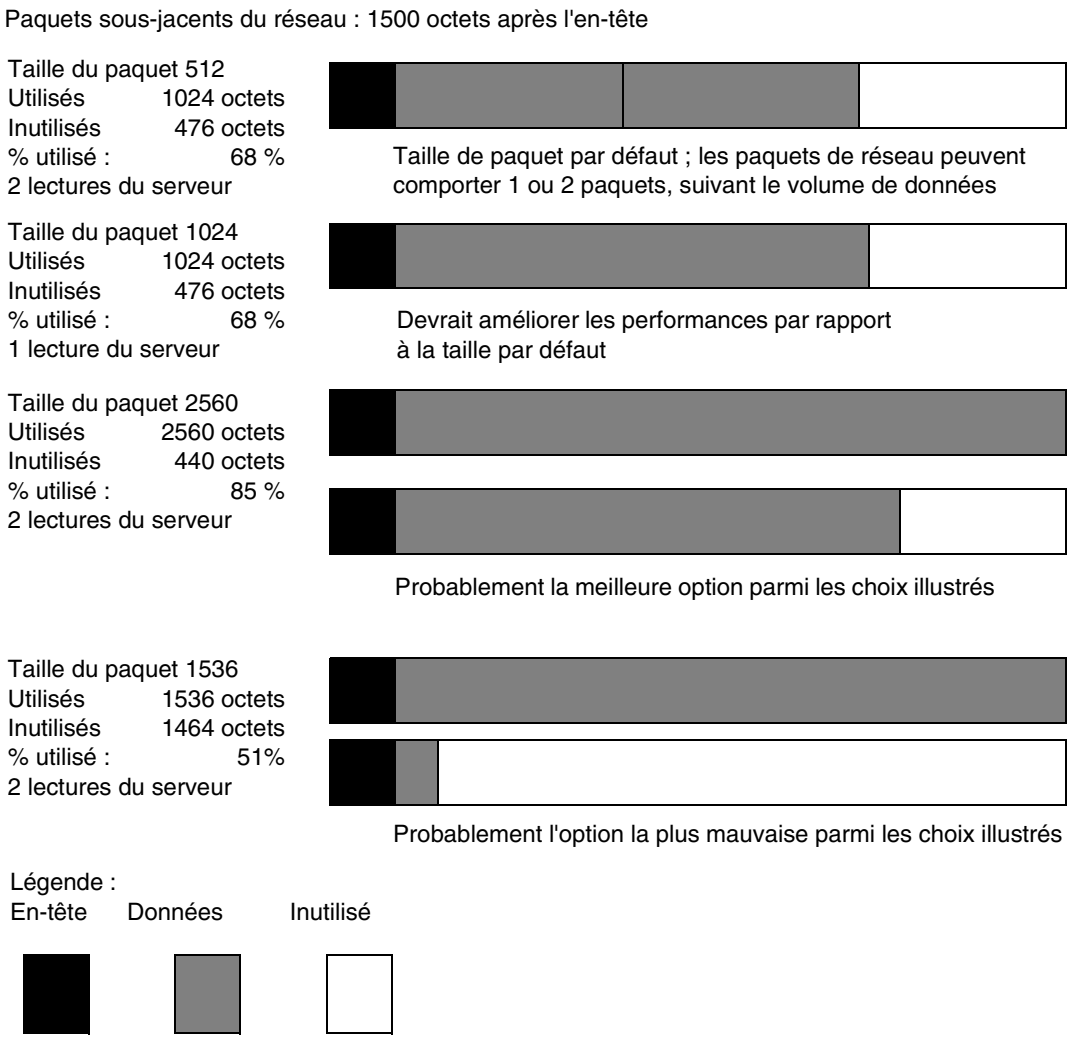
#### Choix de la taille des paquets

Pour optimiser les performances, choisissez une taille de paquet de serveur qui fonctionne efficacement avec la taille de paquet sous-jacente de votre réseau. Les objectifs sont les suivants :

- Diminution du nombre d'opérations de lecture et d'écriture du serveur sur le réseau
- Diminution de l'espace inutilisé dans les paquets de réseau (augmentation du débit sur le réseau)

Si les paquets de votre réseau transportent 1500 octets de données, par exemple, en définissant la taille du paquet Adaptive Server sur 1024 (512*2), vous obtiendrez certainement de meilleures performances qu'en la définissant sur 1536 (512*3). La figure 5-5 illustre les performances de quatre tailles de paquet différentes dans un tel scénario.

***Figure 5-5 : Facteurs permettant de déterminer la taille des paquets***



Après avoir déterminé l'espace disponible des paquets sous-jacents sur votre réseau, effectuez votre propre test de performances afin de déterminer la taille optimale pour votre configuration.

Utilisez sp_sysmon pour observer comment les modifications de la valeur de max network packet size affectent la gestion des E/S réseau et le basculement entre les tâches. Essayez, par exemple, d'augmenter max network packet size et vérifiez ensuite le résultat de sp_sysmon pour voir comment cela affecte bcp pour de grands batch. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### *max number network listeners*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cmaxnetworks |
| Valeur par défaut | 5 |
| Plage de valeurs | 0–2147483647 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

max number network listeners spécifie le nombre maximum de récepteurs de réseau admis en même temps par Adaptive Server.

Chaque port master possède un récepteur de réseau. Il n'est généralement pas nécessaire de disposer de plusieurs ports master, sauf si votre Adaptive Server doit communiquer par plus d'un type de réseau. Certaines plates-formes supportent les interfaces de réseau aussi bien de type socket que de type TLI (Transport Layer Interface). Reportez-vous au Manuel de configuration pour votre plate-forme pour plus d'informations sur les types de réseau supporté.

### *number of remote connections*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | remote connections |
| Valeur par défaut | 20 |
| Plage de valeurs | 5–32767 |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

number of remote connections spécifie le nombre de connexions logiques qui peuvent être ouvertes simultanément en direction et en provenance d'un Adaptive Server. Chacune des connexions simultanées vers XP Server pour l'exécution des ESP utilise au maximum une connexion distante (remote connection). Pour plus d'informations, reportez-vous au chapitre 13, "Gestion des serveurs distants".

### *number of remote logins*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | remote logins |
| Valeur par défaut | 20 |
| Plage de valeurs | 0–32767 |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

number of remote logins détermine le nombre de connexions utilisateur actives entre Adaptive Server et les serveurs distants. Chacune des connexions simultanées vers XP Server pour l'exécution des ESP utilise au maximum un login distant (remote login). Définissez ce paramètre sur une valeur égale ou inférieure à celle de number of remote connections. Pour plus d'informations, reportez-vous au chapitre 13, "Gestion des serveurs distants".

### *number of remote sites*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | remote sites |
| Valeur par défaut | 10 |
| Plage de valeurs | 0–32767 |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

number of remote sites détermine le nombre maximum de sites distants auxquels Adaptive Server peut accéder simultanément. Chaque connexion entre Adaptive Server et un XP Server utilise une connexion de site distant.

En interne, number of remote sites détermine le nombre de gestionnaires de site qui peuvent être actifs en même temps. Tous les accès serveur depuis un même site sont gérés avec un gestionnaire de site unique. Pour plus d'informations, reportez-vous au chapitre 13, "Gestion des serveurs distants".

### *remote server pre-read packets*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | pre-read packets |
| Valeur par défaut | 3 |
| Plage de valeurs | 3–32767 |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

remote server pre-read packets détermine le nombre de paquets qui seront "prélus" par un gestionnaire de site pendant les connexions avec les serveurs distants.

Toutes les communications entre deux serveurs sont gérées par un seul gestionnaire de site afin de réduire le nombre de connexions requises. Ce gestionnaire de site peut effectuer une lecture anticipée des paquets de données et en assurer le suivi pour chaque processus utilisateur avant que le processus auquel ils sont destinés soit prêt.

La valeur par défaut de remote server pre-read packets convient pour la majorité des serveurs. Une augmentation de la valeur consomme plus de mémoire, une diminution de la valeur peut ralentir le trafic du réseau entre les serveurs. Pour plus d'informations, reportez-vous au chapitre 13, "Gestion des serveurs distants".

### *syb_sendmsg port number*

| Récapitulatif | |
|---|---|
| Valeur par défaut | 0 |
| Valeurs correctes | 0 ou 1024–65 535, ou limite du système |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre syb_sendmsg port number spécifie le numéro de port qui sera utilisé par Adaptive Server pour envoyer des messages à un port UDP (User Datagram Protocol) avec sp_sendmsg ou syb_sendmsg.

Un port est utilisé pour chaque moteur configuré et ces ports sont numérotés consécutivement à partir du numéro de port indiqué. Si le numéro de port est défini sur la valeur par défaut 0, Adaptive Server affecte les numéros de port.

**Remarque** L'envoi de messages vers des ports UDP n'est pas supporté sous Windows NT.

Le paramètre de configuration allow sendmsg doit être défini sur 1 par un Responsable de la sécurité du système pour permettre l'envoi de messages vers des ports UDP. Un Administrateur système doit définir le paramètre allow sendmsg sur 1 pour activer la messagerie UDP. Reportez-vous à "allow sendmsg", page 164. Pour plus d'informations sur la messagerie UDP, reportez-vous à la section sp_sendmsg dans le *Manuel de référence d'Adaptive Server*.

### *tcp no delay*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | T1610 (indicateur de trace) |
| Valeur par défaut | 0 (désactivé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre tcp no delay contrôle le regroupement des paquets TCP (Transmission Control Protocol). La valeur par défaut est 0, ce qui veut dire que les paquets TCP sont regroupés.

Normalement, le TCP regroupe les petits paquets logiques en paquets physiques plus grands (en retardant légèrement les paquets) afin de remplir les trames du réseau physique avec autant de données que possible. Cette procédure est destinée à améliorer le débit du réseau dans les environnements à émulation de terminal où ce sont généralement des entrées clavier qui sont envoyées sur le réseau.

Il est toutefois préférable de désactiver le regroupement des paquets TCP pour les applications qui utilisent des petits paquets TDS (Tabular Data Stream™). Pour désactiver le regroupement des paquets TCP, définissez tcp no delay sur 1.

**Remarque** Lorsque le regroupement des paquets TCP est désactivé, les paquets seront envoyés indépendamment de leur taille, ce qui augmentera le volume de trafic sur le réseau.

## Ressources du système d'exploitation

Les paramètres de ce groupe concernent l'utilisation des ressources du système d'exploitation par Adaptive Server.

### *max async i/os per engine*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cnmaxaio_engine |
| Valeur par défaut | 2147483647 |
| Plage de valeurs | 1–2147483647 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

max async i/os per engine spécifie le nombre maximum de requêtes d'E/S disque asynchrones en attente à la fois pour un moteur unique. Pour plus d'informations, reportez-vous à la section "max async i/os per server", page 174.

### *max async i/os per server*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cnmaxaio_server |
| Valeur par défaut | 2147483647 |
| Plage de valeurs | 1–2147483647 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre max async i/os per server spécifie le nombre maximum de requêtes d'E/S disque asynchrones qui peuvent être en attente à la fois pour Adaptive Server. Cette limite n'est pas affectée par le nombre de moteurs en ligne par Adaptive Server ; max async i/os per server limite le nombre total d'E/S asynchrones qu'un serveur peut émettre à la fois, indépendamment du nombre de moteurs en ligne qu'il possède. max async i/os per engine limite le nombre d'E/S en attente par moteur.

La majorité des systèmes d'exploitation limitent le nombre d'E/S disque asynchrones qui peuvent être traitées simultanément. Certains fixent cette limite par un processus du système d'exploitation, certains limitent le nombre par système et d'autres utilisent les deux méthodes. Si une application dépasse ces limites, le système d'exploitation renvoie un message d'erreur. Comme les appels au système d'exploitation sont relativement coûteux, il est inutile qu'Adaptive Server tente d'effectuer des E/S asynchrones qui sont rejetées par le système d'exploitation.

Pour éviter cela, Adaptive Server tient une comptabilité des E/S asynchrones en attente par moteur et par serveur ; si un moteur émet une E/S asynchrone qui risque de dépasser la valeur de max async i/os per engine ou de max async i/os per server, Adaptive Server retarde l'E/S jusqu'à ce que suffisamment d'E/S en attente soient terminées pour que la limite ne soit pas dépassée.

Supposons, par exemple, un système d'exploitation qui limite le nombre d'E/S asynchrones à 200 par système et à 75 par processus et un Adaptive Server avec trois moteurs en ligne. Les moteurs ont actuellement un total de 200 E/S asynchrones en attente, distribuées d'après le tableau suivant.

| Moteur | Nombre d'E/S en attente | Résultat |
|---|---|---|
| 0 | 60 | Le moteur 0 retarde toute nouvelle E/S asynchrone jusqu'à ce que le total pour le serveur soit devenu inférieur à la limite *par système* fixée par le système d'exploitation et continue ensuite l'émission d'E/S asynchrones. |
| 1 | 75 | Le moteur 1 retarde toute nouvelle E/S asynchrone jusqu'à ce que le total par moteur soit devenu inférieur à la limite *par processus* fixée par le système d'exploitation et continue ensuite l'émission d'E/S asynchrones. |
| 2 | 65 | Le moteur 2 retarde toute nouvelle E/S asynchrone jusqu'à ce que le total pour le serveur soit devenu inférieur à la limite *par système* fixée par le système d'exploitation et continue ensuite l'émission d'E/S asynchrones. |

Toutes les E/S (aussi bien asynchrones que synchrones) ont besoin d'une structure d'E/S disque, ce qui implique que le nombre total d'E/S disque en attente est limité par la valeur du paramètre disk i/o structures. Il est légèrement plus efficace pour Adaptive Server de retarder les E/S car il ne peut pas obtenir une structure d'E/S disque que de laisser le nombre de requêtes d'E/S dépasser max i/os per server. Il est recommandé de donner au paramètre de configuration max async i/os per server la même valeur que disk i/o structures. Reportez-vous à la section "disk i/o structures", page 121.

Si votre système d'exploitation permet de modifier les limites d'E/S asynchrones, assurez-vous qu'elles soient suffisamment élevées pour Adaptive Server. Il n'y a aucun inconvénient à les définir au niveau requis.

Utilisez sp_sysmon pour vérifier si les limites par serveur ou par moteur retardent les E/S sur votre système. Si sp_sysmon montre qu'Adaptive Server dépasse la limite des requêtes en attente par moteur ou par serveur, augmentez la valeur du paramètre correspondant. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### o/s file descriptors

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | Spécifique au site |
| Etat | Lecture seule |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

o/s file descriptors indique le nombre maximum de descripteurs de fichier par processus configurés pour votre système d'exploitation. Ce paramètre est en lecture seule et ne peut pas être modifié par le biais d'Adaptive Server.

De nombreux systèmes d'exploitation vous permettent de configurer le nombre de descripteurs de fichier disponibles par processus. Reportez-vous à la documentation de votre système d'exploitation pour plus d'informations à ce sujet.

Le nombre de descripteurs de fichier disponibles pour les connexions Adaptive Server, qui sera inférieur à la valeur de o/s file descriptors, est stocké dans la variable *@@max_connections*. Reportez-vous à la section "Limite supérieure du paramètre maximum number of user connections", page 246 pour plus d'informations sur le nombre de descripteurs de fichier disponibles pour les connexions.

### shared memory starting address

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | mrstart |
| Valeur par défaut | 0 |
| Plage de valeurs | Spécifique à la plate-forme |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

shared memory starting address détermine l'adresse virtuelle où commence la région de la mémoire partagée d'Adaptive Server.

Il est peu probable que vous soyez obligé de modifier le paramètre shared memory starting address. Le cas échéant, contactez préalablement le Support Technique Sybase.

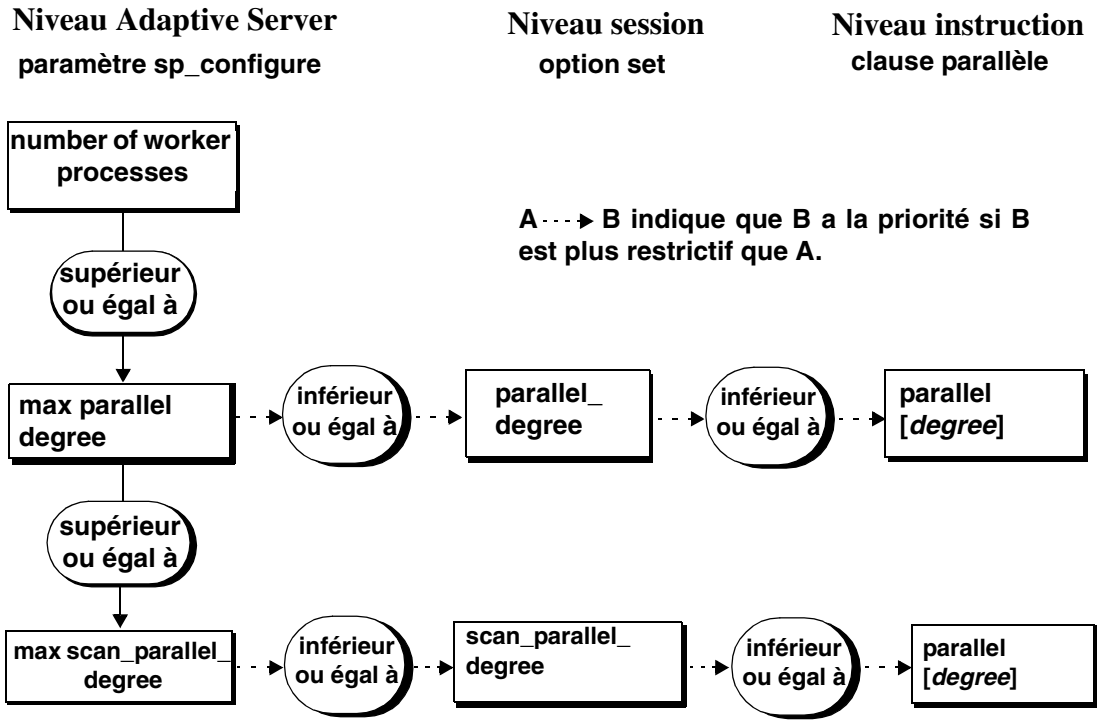
## Requêtes parallèles

Les paramètres suivants configurent Adaptive Server pour le traitement parallèle des requêtes – dans quel cas l'optimiseur évalue chaque requête pour déterminer si elle est adaptée à une exécution en parallèle.

Reportez-vous au chapitre 17, "Optimiseur Adaptive Server", et au chapitre 23, "Optimisation des requêtes parallèles", dans le document *Performances et optimisation* pour déterminer les meilleures valeurs à utiliser pour les paramètres de configuration et pour comprendre comment ces valeurs affectent l'optimiseur.

Les paramètres number of worker processes, max parallel degree et max scan parallel degree contrôlent le traitement des requêtes en parallèle au niveau du serveur. L'utilisation des options parallel_degree, process_limit_action et scan_parallel_degree de la commande set peut limiter l'optimisation parallèle au niveau de la session et l'utilisation du mot-clé parallel de la commande select peut limiter l'optimisation parallèle de requêtes spécifiques. La figure 5-6 illustre la priorité des paramètres de configuration et des paramètres de session.

***Figure 5-6 : Priorité des options parallèles***



### number of worker processes

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

number of worker processes spécifie le nombre maximum de processus de travail qu'Adaptive Server peut utiliser en une fois pour toutes les requêtes combinées exécutées simultanément en parallèle.

Adaptive Server émet un message d'avertissement au démarrage si la mémoire est insuffisante pour créer le nombre spécifié de processus de travail. memory per worker process contrôle la mémoire allouée à chaque processus de travail.

### max parallel degree

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Plage de valeurs | 1–255 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

max parallel degree spécifie le nombre maximum de processus de travail autorisés par requête au niveau du serveur. Ceci est appelé le *degré maximum de parallélisme*.

Si ce nombre est trop faible, l'amélioration des performances d'une requête donnée peut s'avérer insuffisante. Si ce nombre est trop élevé, le serveur risque de compiler des plans qui requièrent plus de processus qu'il n'y en a de disponibles au moment de l'exécution ou alors le système peut devenir saturé, ce qui entraîne une baisse de rendement. Pour permettre le balayage en parallèle des partitions, définissez ce paramètre à une valeur égale ou supérieure au nombre de partitions dans la table que vous interrogez.

La valeur de ce paramètre doit être inférieure ou égale à la valeur courante du paramètre number of worker processes.

Si vous définissez max parallel degree sur 1, Adaptive Server balaie toutes les tables ou tous les index en série.

La modification de max parallel degree a pour effet que tous les plans de requête dans le cache de procédure deviennent caducs et de nouveaux plans sont compilés la prochaine fois que vous exécutez une procédure stockée ou un trigger.

Reportez-vous au chapitre 24, "Tri parallèle", dans le document *Performances et optimisation* pour plus d'informations sur le tri en parallèle.

### *max scan parallel degree*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Plage de valeurs | 1–255 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

max scan parallel degree spécifie le degré de parallélisme maximum au niveau du serveur pour les balayages avec hachage. Les balayages avec hachage peuvent être utilisés pour les méthodes d'accès suivantes :

- Balayages d'index en parallèle pour les tables partitionnées et non partitionnées
- Balayages de tables en parallèle pour les tables non partitionnées

max scan parallel degree s'applique par table ou par index, ce qui veut dire que si max scan parallel degree est égal à 3 et qu'une table dans une requête en jointure est balayée en utilisant un balayage de table en hachage et que l'accès à la deuxième table s'effectue de préférence par un balayage d'index en hachage, la requête peut utiliser 9 processus de travail (sous réserve que max scan parallel degree soit fixé à 9 ou plus).

L'optimiseur utilise ce paramètre comme indication lorsqu'il sélectionne le nombre de processus à utiliser pour les opérations de balayage en parallèle sans partition. Il ne s'applique pas au tri en parallèle. Les processus parallèles peuvent accéder au même device pendant le balayage, car il n'y a pas de partitionnement pour diffuser les données entre les devices. Cette situation peut donner lieu à des conflits de disque et à des mouvements de tête supplémentaires, ce qui dégrade les performances. Pour éviter que ces accès disque multiples ne deviennent un problème, utilisez ce paramètre pour réduire le nombre maximum de processus qui peuvent accéder en parallèle à la table.

Si ce nombre est trop faible, l'amélioration des performances d'une requête donnée peut s'avérer insuffisante. Si ce nombre est trop élevé, le serveur risque de compiler des plans qui utilisent suffisamment de processus pour rendre l'accès disque moins efficace. En règle générale, la valeur de ce paramètre doit être comprise entre 2 et 3, car il ne faut pas plus de 2 à 3 processus de travail pour utiliser pleinement les E/S d'un device physique donné.

Définissez ce paramètre à une valeur inférieure ou égale à la valeur courante de max parallel degree. Adaptive Server renvoie une erreur si vous spécifiez un nombre supérieur à la valeur de max parallel degree.

Si max scan parallel degree est défini sur 1, Adaptive Server n'effectue pas de balayages par hachage.

En modifiant max scan parallel degree, tous les plans de requête dans le cache de procédure deviennent caducs et de nouveaux plans sont compilés la prochaine fois que vous exécutez une procédure stockée ou un trigger.

### *memory per worker process*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1024 |
| Plage de valeurs | 1024–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

memory per worker process spécifie l'espace mémoire (en octets) utilisé par les processus de travail. Chaque processus de travail a besoin de mémoire pour l'échange de messages pendant la coordination des requêtes. Cette mémoire est allouée depuis une zone de mémoire partagée dont la taille est égale à la valeur de memory per worker process multipliée par la valeur de number of worker processes. La taille par défaut convient parfaitement pour le traitement de la majorité des requêtes. Si vous utilisez dbcc checkstorage et si number of worker processes est défini sur 1, il peut s'avérer nécessaire d'augmenter memory per worker process à 1792 octets. Reportez-vous à la section "Autres paramètres de configuration pour le traitement en parallèle", page 568 du document *Performances et optimisation* pour plus d'informations sur la définition de ce paramètre.

Pour plus d'informations sur l'allocation de mémoire par Adaptive Server, reportez-vous au chapitre 18, "Configuration de la mémoire"..

## Mémoire physique

Les paramètres de ce groupe configurent les ressources de la mémoire physique de votre machine.

### *allocate max shared memory*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 12.5 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0,1 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

allocate max shared memory détermine si Adaptive Server alloue toute la mémoire spécifiée par max memory au démarrage ou seulement l'espace mémoire requis par le paramètre de configuration.

En définissant allocate max shared memory sur 0, vous avez la certitude qu'Adaptive Server n'utilisera que le volume de mémoire partagée requis pour la configuration courante et n'allouera que l'espace mémoire requis par les paramètres de configuration au démarrage, ce qui est inférieur à la valeur de max memory.

Si vous définissez allocate max shared memory sur 1, Adaptive Server alloue au démarrage toute la mémoire spécifiée par max memory. Si allocate max shared memory est défini sur 1 et si vous augmentez la valeur de max memory, Adaptive Server utilise immédiatement des segments de mémoire partagée supplémentaires. Cela veut dire qu'Adaptive Server dispose toujours de la mémoire nécessaire pour tout changement de configuration de la mémoire et qu'il n'y a pas de dégradation des performances pendant que le serveur fait des corrections pour de la mémoire supplémentaire. Mais si vos prévisions de croissance de la mémoire sont imprécises et que la valeur de max memory est trop importante, vous risquez de gâcher de la mémoire physique.

### *dynamic allocation on demand*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 12.5 | N/A |
| Valeur par défaut | 1 |
| Plage de valeurs | 0, 1 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

Détermine à quel moment la mémoire est allouée pour les modifications des paramètres de configuration de la mémoire dynamique.

Si vous définissez dynamic allocation on demand sur 1, la mémoire est seulement allouée en fonction du besoin. Cela veut dire que si vous faites passer la valeur du paramètre number of user connections de 100 à 200, la mémoire pour chaque utilisateur n'est ajoutée que lorsque l'utilisateur se connecte au serveur. Adaptive Server continue d'ajouter de la mémoire jusqu'à atteindre le nouveau maximum pour les connexions utilisateur.

Si dynamic allocation on demand est défini sur 0, toute la mémoire requise pour d'éventuelles modifications dynamiques de la configuration est allouée immédiatement. Cela veut dire que si vous faites passer le nombre de connexions utilisateur de 100 à 200, la mémoire requise pour les 100 connexions utilisateur supplémentaires est allouée immédiatement.

### *max memory*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 12.5 | N/A |
| Valeur par défaut | Dépendant de la plate-forme |
| Plage de valeurs | Minimum dépendant de la plate-forme –2 147 483 647 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

Spécifie le volume maximum de mémoire physique totale qu'Adaptive Server pourra allouer. max memory doit être supérieur à la mémoire logique totale consommée par la configuration courante d'Adaptive Server.

Les performances ne sont pas diminuées lorsque vous configurez Adaptive Server pour qu'il utilise le maximum de mémoire disponible sur votre ordinateur. Il vous faudra cependant évaluer les autres besoins en mémoire de votre système, sinon Adaptive Server risque de ne pas avoir suffisamment de mémoire pour démarrer.

Le chapitre 18, "Configuration de la mémoire", du *Guide d'administration du système* contient des instructions sur l'optimisation du paramètre max memory pour Adaptive Server.

#### Si le démarrage d'Adaptive Server est impossible

Si vous définissez allocate max shared memory sur 1, Adaptive Server doit pouvoir disposer de l'espace mémoire spécifié par max memory. Si cette mémoire n'est pas disponible, Adaptive Server ne démarre pas. Le cas échéant, réduisez la mémoire occupée par Adaptive Server en modifiant manuellement la valeur de max memory dans le fichier de configuration du serveur. Vous pouvez également faire passer la valeur de allocate max shared memory à 0 afin que toute la mémoire spécifiée par max memory ne soit pas occupée au démarrage.

Vous pouvez aussi réduire la valeur d'autres paramètres de configuration qui occupent un espace mémoire important. Redémarrez ensuite Adaptive Server pour qu'il utilise la mémoire spécifiée par ces nouvelles valeurs. Si Adaptive Server ne démarre pas parce que le total des valeurs des autres paramètres de configuration est supérieur à la valeur de max memory, reportez-vous au chapitre 18, "Configuration de la mémoire", du *Guide d'administration du système* pour plus d'informations sur les paramètres de configuration qui occupent de la mémoire.

### *additional network memory*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | additional network memory |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

additional network memory définit la taille maximale de la mémoire supplémentaire qui peut être utilisée pour les paquets du réseau dont la taille est supérieure à la taille par défaut. Adaptive Server arrondit la valeur saisie au multiple de 2 Ko immédiatement inférieur. La valeur par défaut indique qu'aucun espace supplémentaire n'est alloué pour les paquets de grande taille.

Si vous augmentez max network packet size sans augmenter additional network memory, les clients ne pourront pas utiliser des paquets plus grands que la taille par défaut, car toute la mémoire réseau allouée est réservée aux utilisateurs à la taille par défaut. Adaptive Server garantit que chaque utilisateur peut se connecter avec la taille de paquet par défaut. Dans cette situation, les utilisateurs qui demandent une taille de paquet supplémentaire à la connexion reçoivent un message d'avertissement leur indiquant que leur application va utiliser la taille par défaut.

Une augmentation de la valeur de additional network memory peut améliorer les performances pour les applications qui transfèrent de grands volumes de données. Procédez comme suit pour déterminer la valeur de additional network memory lorsque vos applications utilisent des paquets de grande taille :

- Estimez le nombre d'utilisateurs qui demanderont simultanément des paquets de grande taille et les tailles qui seront demandées par leurs applications.

- Multipliez cette somme par trois, car chaque connexion a besoin de trois buffers.
- Ajoutez 2 % pour l'en-tête et
- Arrondissez la valeur au multiple de 2048 immédiatement supérieur.

Exemple d'estimation de ces besoins simultanés de paquets de grande taille :

| Application | Taille du paquet | En-tête |
|---|---|---|
| bcp | 8192 | |
| Client-Library | 8192 | |
| Client-Library | 4096 | |
| Client-Library | 4096 | |
| Total | 24576 | |
| Multipliez par 3 buffers/utilisateur | *3 | |
| | 73728 | |
| Calculez 2 % pour l'en-tête | | * 0,02=1474 |
| Ajoutez l'en-tête | + 1474 | |
| Additional network memory | 75202 | |
| Arrondissez à un multiple de 2048 | 75776 | |

additional network memory doit être défini sur 75 776 octets.

### *heap memory per user*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 4 Ko |
| Valeurs correctes | 0–2 147 483 647 octets |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

heap memory per user détermine le nombre de segments de mémoire par utilisateur. Une zone de segments de mémoire est une mémoire interne créée au démarrage et utilisée par les tâches pour allouer de manière dynamique de la mémoire en fonction des besoins. Cette zone de mémoire est importante si vous exécutez des tâches qui utilisent des colonnes larges, ce qui nécessite beaucoup de mémoire de la pile. Le segment de mémoire alloue un buffer temporaire qui permet à ces tâches à colonne large de se terminer. Le segment de mémoire utilisé par la tâche est rendu à la zone de segments de mémoire lorsque la tâche est terminée.

La taille de la zone de mémoire dépend du nombre de connexions utilisateur. Sybase recommande de définir heap memory per user sur une valeur triple de la taille de votre page logique.

### *lock shared memory*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | T1611 (indicateur de trace) |
| Valeur par défaut | 0 (désactivé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

lock shared memory empêche l'échange de pages Adaptive Server sur le disque et permet au noyau du système d'exploitation d'éviter le code de verrouillage de page interne du serveur. Cette configuration peut diminuer les coûteuses lectures du disque.

Toutes les plates-formes ne supportent pas le verrouillage de la mémoire partagée. Même si votre plate-forme le permet, le paramètre lock shared memory peut échouer en raison d'autorisations mal déclarées, d'une insuffisance de mémoire physique ou pour d'autres raisons. Reportez-vous au Manuel de configuration pour votre plate-forme pour plus d'informations sur le verrouillage de la mémoire partagée.

### max SQL text monitored

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–2147483647 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

max SQL text monitored spécifie l'espace mémoire alloué par connexion d'utilisateur pour enregistrer le texte SQL dans la mémoire partagée par Adaptive Server Monitor.

L'espace mémoire initialement alloué pour l'enregistrement de texte est nul. Ce paramètre étant statique, vous devez redémarrer Adaptive Server avant de pouvoir commencer à enregistrer du texte SQL.

Si vous n'allouez pas suffisamment de mémoire pour les instructions en batch, le texte qui vous intéresse peut se trouver dans la partie du batch qui a été tronquée. Sybase recommande d'utiliser une valeur initiale de 1024 octets par connexion utilisateur.

Le volume total de mémoire partagée alloué au texte SQL est le produit de max SQL text monitored par le nombre de connexions utilisateur actuellement configurées.

Reportez-vous à la section "Configuration d'Adaptive Server pour la sauvegarde du texte des batchs SQL", page 70 pour plus d'informations sur max SQL text monitored.

### total physical memory

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 12.5 | total memory |
| Valeur par défaut | N/A |
| Plage de valeurs | N/A |
| Etat | Lecture seule |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

total physical memory est un paramètre de configuration en lecture seule qui affiche la mémoire physique totale disponible pour la configuration actuelle d'Adaptive Server. La mémoire physique totale est l'espace mémoire qu'utilise Adaptive Server à un moment donné. Il faut configurer Adaptive Server de manière à ce que la valeur de max memory soit supérieure à la valeur de total logical memory et que la valeur de total logical memory soit supérieure à la valeur de total physical memory.

### *total logical memory*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 12.5 | total memory |
| Valeur par défaut | N/A |
| Plage de valeurs | N/A |
| Etat | Lecture seule |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

total logical memory affiche la mémoire logique totale disponible pour la configuration actuelle d'Adaptive Server. La mémoire logique totale est l'espace mémoire qu'utilise la configuration actuelle d'Adaptive Server. total logical memory affiche la mémoire qui doit être disponible sans qu'elle soit nécessairement utilisée à un moment donné. Reportez-vous au paramètre de configuration total physical memory pour plus d'informations sur l'espace mémoire utilisé à un moment donné. Vous ne pouvez pas utiliser total logical memory pour définir l'un des paramètres de configuration de la mémoire.

## Processeurs

Les paramètres de ce groupe configurent les processeurs dans un environnement SMP.

### *number of engines at startup*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 12.5 | N/A |
| Valeur par défaut | 1 |
| Plage de valeurs | 1–nombre de processeurs sur la machine |
| Etat | Statique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

Adaptive Server permet à l'utilisateur de déconnecter tous les moteurs, sauf le moteur zéro.

Le paramètre number of engines at startup est uniquement utilisé pendant le démarrage pour définir le nombre de moteurs placés en ligne. Il est conçu pour offrir aux utilisateurs le plus de souplesse possible dans leur choix du nombre de moteurs mis en ligne, avec pour restriction que vous ne pouvez pas définir number of engines at startup sur une valeur supérieure au nombre de processeurs présents sur votre machine ou à une valeur supérieure à celle du paramètre max online engines. Les utilisateurs qui souhaitent mettre des moteurs en ligne après le démarrage doivent attribuer la même valeur à max online engines et à number of engines at startup. Une différence entre number of engines at startup et max online engines utilise environ 1,8 Mo de mémoire par moteur.

### *max online engines*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | max online engines |
| Valeur par défaut | 1 |
| Plage de valeurs | 1–128 |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Le rôle de max online engines est de définir un nombre élevé de moteurs mis en ligne à tout moment dans un environnement SMP. Ce paramètre ne tient pas compte du nombre de processeurs disponibles au moment du démarrage et permet aux utilisateurs d'ajouter des processeurs ultérieurement.

max engines online spécifie le nombre maximum de moteurs Adaptive Server qui peuvent être en ligne à tout moment dans un environnement SMP. Le chapitre 20, "Gestion des serveurs multiprocesseur", traite en détail la manière de définir ce paramètre pour votre environnement SMP.

Au démarrage, Adaptive Server démarre avec un seul moteur et termine son initialisation qui comprend la restauration de toutes les bases de données. Sa tâche finale est d'allouer des moteurs de serveur supplémentaires. Chaque moteur accède à des structures de données communes dans la mémoire partagée.

Lorsque vous définissez le paramètre de configuration max engines online :

- Le nombre de moteurs ne doit jamais dépasser celui des processeurs.
- Suivant la charge globale du système (y compris les applications autres que Adaptive Server), vous pouvez obtenir un rendement optimal en laissant certains processeurs libres pour l'exécution de processus autres que ceux d'Adaptive Server.
- Vous pouvez obtenir un meilleur rendement en exécutant moins de moteurs avec un usage accru du processeur plutôt que d'utiliser plus de moteurs en utilisant moins le processeur.
- L'évolutivité dépend de l'application. Vous devez effectuer des tests de performances complets de votre application pour déterminer la meilleure configuration des moteurs en ligne.
- Vous pouvez utiliser la commande dbcc engine pour mettre les moteurs hors ligne et pour les remettre en ligne. Vous pouvez mettre hors ligne tous les moteurs sauf le moteur zéro.

Reportez-vous à la section "Désactivation d'un moteur à l'aide de la commande dbcc engine", page 686 pour plus d'informations sur l'utilisation de dbcc engine. Reportez-vous au chapitre 3, "Utilisation des moteurs et des CPU", dans le document *Performances et optimisation* pour plus d'informations sur l'optimisation des performances et des moteurs.

## Administration du thread RepAgent

Les paramètres de ce groupe configurent la réplication par le biais de Replication Server®.

### *enable rep agent threads*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–1 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

Le paramètre de configuration enable rep agent threads active le thread RepAgent dans Adaptive Server.

Jusqu'à la version 11.0.3 de Replication Server, Log Transfer Manager (LTM), un composant du système de réplication, transférait les données de réplication à Replication Server. Dans les versions de Replication Server ultérieures à 11.0.3, le transfert des données de réplication est traité par RepAgent, qui est exécuté comme un thread sous Adaptive Server. Le paramètre de configuration enable rep agent threads active cette fonctionnalité.

D'autres étapes sont également requises pour permettre la réplication. Reportez-vous à la documentation sur Replication Server pour plus d'informations.

## Administration du serveur SQL

Les paramètres de ce groupe se rapportent à l'administration générale d'Adaptive Server.

### *abstract plan cache*

| Récapitulatif | |
|---|---|
| Valeur par défaut | 0 |
| Plage de valeurs | 0–1 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

abstract plan cache permet de mettre en mémoire cache les clés de hachage de plan abstrait. Par défaut, la mise en mémoire cache n'est pas activée. Pour plus d'informations, reportez-vous au chapitre 30, "Création et utilisation des plans abstraits", dans le document *Performances et optimisation*. abstract plan load doit être activé pour que la mise en mémoire cache des plans ait lieu.

### *abstract plan dump*

| Récapitulatif | |
|---|---|
| Valeur par défaut | 0 |
| Plage de valeurs | 0–1 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

abstract plan dump active l'enregistrement des plans abstraits dans le groupe de plans abstraits ap_stdout. Pour plus d'informations, reportez-vous au chapitre 30, "Création et utilisation des plans abstraits", dans le document *Performances et optimisation*.

### *abstract plan load*

| Récapitulatif | |
|---|---|
| Valeur par défaut | 0 |
| Plage de valeurs | 0–1 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

abstract plan load active l'association de requête avec des plans abstraits dans le groupe de plans abstraits ap_stdin. Pour plus d'informations, reportez-vous au chapitre 30, "Création et utilisation des plans abstraits", dans le document *Performances et optimisation*.

### *abstract plan replace*

| Récapitulatif | |
|---|---|
| Valeur par défaut | 0 |
| Plage de valeurs | 0–1 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

abstract plan replace active le remplacement de plan pour les plans abstraits dans le groupe de plans abstraits ap_stdout. Pour plus d'informations, reportez-vous au chapitre 30, "Création et utilisation des plans abstraits", dans le document *Performances et optimisation*. abstract plan load doit être activé pour que le mode remplacement prenne effet.

### *allow backward scans*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 (activé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

allow backward scans contrôle la manière dont l'optimiseur exécute les requêtes select qui contiennent la commande order by...desc :

- Lorsque la valeur est définie sur 1, l'optimiseur peut accéder à l'index ou aux lignes de la table en suivant la chaîne des pages dans l'ordre d'index décroissant.
- Lorsque la valeur est définie sur 0, l'optimiseur sélectionne les lignes dans une table de travail en suivant les pointeurs de page d'index dans l'ordre croissant et trie ensuite la table de travail dans l'ordre décroissant.

La première méthode, qui effectue un balayage décroissant, peut accélérer l'accès aux tables dont les résultats doivent être triés par ordre décroissant de la valeur des colonnes. Certaines applications peuvent cependant rencontrer des interblocages liés au balayage décroissant. Les interblocages peuvent être plus nombreux, notamment si des requêtes delete ou update effectuent un balayage croissant en utilisant le même index. Les ruptures de page dans l'index peuvent également donner lieu à des interblocages.

Vous pouvez utiliser print deadlock information pour envoyer des messages sur les interblocages au journal d'erreur. Reportez-vous à la section "print deadlock information", page 224. En variante, vous pouvez utiliser sp_sysmon pour rechercher les interblocages. Reportez-vous au document *Performances et optimisation* pour plus d'informations sur les interblocages.

### *allow nested triggers*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | nested trigger |
| Valeur par défaut | 1 (activé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

allow nested triggers contrôle l'utilisation des triggers imbriqués. Lorsque la valeur est définie sur 1, les modifications de données effectuées par des triggers peuvent déclencher d'autres triggers. Définissez allow nested triggers sur 0 pour désactiver les triggers imbriqués. Une option set, self_recursion, contrôle si les modifications effectuées par un trigger peuvent provoquer un nouveau déclenchement de ce trigger.

### *allow resource limits*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

allow resource limits contrôle l'utilisation des limites de ressources. Lorsque la valeur est définie sur 1, le serveur alloue de la mémoire interne pour les plages de temps, les limites de ressources et les alarmes internes du serveur. Le serveur attribue également en interne les plages et les limites applicables aux sessions utilisateur. Le résultat de sp_configure affiche le coût d'une requête estimé par l'optimiseur. Définissez allow resource limits sur 0 pour désactiver les limites de ressources.

### *allow updates to system tables*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | allow updates |
| Valeur par défaut | 0 (désactivé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

allow updates to system tables permet aux utilisateurs ayant un rôle d'Administrateur système d'apporter des modifications aux tables système et de créer des procédures stockées qui peuvent modifier les tables système. Un administrateur de bases de données peut mettre à jour les tables système qu'il ou elle possède si allow updates to system tables est activé.

Les tables système comprennent :

- Toutes les tables fournies par Sybase dans la base de données master
- Toutes les tables dans les bases de données utilisateur qui commencent par "sys" et dont la valeur ID dans la table sysobjects est inférieure ou égale à 100.

**Avertissement !** Une modification incorrecte apportée à une table système peut endommager la base de données et provoquer une perte de données. Utilisez toujours begin transaction lorsque vous modifiez une table système pour la protéger contre les erreurs qui risqueraient d'endommager vos bases de données. Désactivez immédiatement allow updates to system tables lorsque vous avez terminé vos modifications.

Les procédures stockées et les triggers que vous avez créés pendant que allow updates to system tables est activé pourront toujours mettre à jour les tables système, même après avoir désactivé ce paramètre. Lorsque vous activez allow updates to system tables, vous créez un "créneau de vulnérabilité", c'est-à-dire une période pendant laquelle les utilisateurs peuvent modifier les tables système ou créer une procédure stockée avec laquelle les tables système pourront être modifiées à l'avenir.

Les tables système étant très importantes, il est préférable de n'activer ce paramètre que dans des situations parfaitement maîtrisées. Redémarrez Adaptive Server en mode utilisateur unique pour garantir qu'aucun autre utilisateur ne puisse accéder à Adaptive Server pendant la mise à jour directe des tables système. Pour plus d'informations, reportez-vous à startserver et dataserver dans le document *Utilitaires*.

### *cpu accounting flush interval*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cpu flush |
| Valeur par défaut | 200 |
| Plage de valeurs | 1–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

cpu accounting flush interval spécifie la durée, en impulsions d'horloge *machine*, pendant laquelle Adaptive Server attend avant de vider les statistiques d'utilisation du processeur pour chaque utilisateur de sysprocesses vers syslogins, une procédure utilisée en comptabilisation du taux de charge du processeur. (Notez que cette durée est mesurée en impulsions d'horloge *machine* et non en impulsions d'horloge Adaptive Server.)

Lorsqu'un utilisateur se connecte à Adaptive Server, le serveur commence à totaliser les chiffres relatifs à l'utilisation du processeur pendant ce processus utilisateur dans sysprocesses. Lorsqu'un utilisateur se déconnecte d'Adaptive Server ou lorsque la valeur de cpu accounting flush interval est dépassée, les statistiques cumulées d'utilisation du processeur sont vidées de sysprocesses vers syslogins. Ces statistiques continuent d'être totalisées dans syslogins jusqu'à ce que vous remettiez les totaux à zéro à l'aide de sp_clearstats. Vous pouvez afficher les totaux courants dans syslogins à l'aide de sp_reportstats.

La valeur que vous avez définie pour cpu accounting flush interval dépend du type d'état que vous prévoyez de générer. Si vous voulez générer un état mensuel, affectez une valeur relativement élevée à cpu accounting flush interval. Avec des états plus espacés, il est moins important d'effectuer une mise à jour fréquente des données dans syslogins.

D'un autre côté, si vous essayez d'effectuer des sélections spécifiques périodiques sur la colonne totcpu dans syslogins pour déterminer le taux d'utilisation du processeur par processus, affectez à cpu accounting flush interval une valeur inférieure. Vous augmenterez ainsi la probabilité de présence de données à jour dans syslogins lorsque vous exécutez vos sélections.

En affectant à cpu accounting flush interval une valeur faible, les processus risquent d'être identifiés par erreur par le gestionnaire de verrous comme des victimes potentielles d'un interblocage. Lorsque le gestionnaire de verrous détecte un interblocage, il vérifie le temps processeur cumulé par chaque processus en cours. Le processus dont la valeur est la plus faible est choisi comme victime de l'interblocage et le gestionnaire de verrous y met fin. De plus, lorsque la valeur de cpu accounting flush interval est faible, les gestionnaires de tâches qui stockent les informations d'utilisation du processeur pour les processus sont initialisés plus fréquemment. Résultat, les processus semblent avoir totalisé plus de temps processeur qu'ils ne l'ont fait en réalité. En conséquence, le gestionnaire de verrous choisit un processus comme victime de l'interblocage alors qu'en réalité, ce processus a plus de temps processeur cumulé que le processus concurrent.

Si vous ne prévoyez pas de générer des états sur l'utilisation du processeur, affectez à cpu accounting flush interval sa valeur maximale. Vous réduirez ainsi le nombre de mises à jour de syslogins et le nombre de fois que ses pages doivent être écrites sur le disque.

### *cpu grace time*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | ctimemax |
| Valeur par défaut | 500 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

cpu grace time, combiné avec time slice, spécifie la durée maximale pendant laquelle un processus utilisateur peut être exécuté sans arrêter le processeur avant qu'Adaptive Server ne prenne la main et y mette fin avec une erreur time-slice. Les unités de cpu grace time sont les impulsions de temps définies par sql server clock tick length. Pour plus d'informations, reportez-vous à la section "sql server clock tick length", page 227.

Lorsqu'un processus dépasse le temps cpu grace time Adaptive Server "l'infecte" en supprimant le processus des files d'attente internes. Le processus est supprimé, mais Adaptive Server n'est pas affecté. Cela évite aux processus ininterrompus de monopoliser le processeur. Si l'un de vos processus utilisateur est infecté, vous pouvez remédier provisoirement au problème en augmentant la valeur de cpu grace time. Vous devez cependant être sûr que le problème réside réellement dans un processus qui prend plus de temps que la valeur de cpu grace time pour se terminer et non pas dans un processus ininterrompu.

Le fait d'augmenter provisoirement la valeur de cpu grace time est une solution de secours et non pas un remède définitif, car cela peut donner lieu à d'autres complications. Voir "time slice", page 228. Reportez-vous également au chapitre 3, "Utilisation des moteurs et des CPU", et à la section "Planification de la tâche en exécution", page 32 du document *Performances et optimisation* pour plus d'informations sur la planification des tâches.

### *default database size*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | database size |
| Valeur par défaut | Taille de page logique |
| Plage de valeurs | $2^a$ –10000<br>a. Minimum déterminé par la taille de page logique du serveur. |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

default database size définit le nombre de mégaoctets par défaut alloués à une nouvelle base de données utilisateur si l'instruction create database est émise sans paramètres de taille. Une taille de base de données indiquée dans une instruction create database a priorité sur la valeur définie par ce paramètre de configuration.

Si la majorité des nouvelles bases de données de votre application Adaptive Server ont besoin d'une taille supérieure à celle d'une page logique, vous pouvez augmenter la valeur par défaut.

**Remarque** Si vous modifiez la base de données model, vous devez également augmenter la valeur de default database size, car la commande create database copie model pour créer une nouvelle base de données utilisateur.

### *default fill factor percent*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | fillfactor |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–100 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

default fill factor percent détermine le niveau de remplissage de chaque page d'index par Adaptive Server lorsqu'il crée un nouvel index sur des données existantes, sauf si le facteur de remplissage est précisé dans l'instruction create index. Le pourcentage fillfactor n'a d'utilité que lors de la création de l'index. En cas de modification des données, le niveau de remplissage des pages change.

default fill factor percent affecte :

- Le volume d'espace de stockage utilisé par vos données – Adaptive Server redistribue les données lorsqu'il crée l'index clusterisé.
- Les performances – le fractionnement des pages consomme des ressources d'Adaptive Server.

Il est rarement nécessaire de modifier default fill factor percent, notamment parce que vous pouvez remplacer sa valeur dans la commande create index. Reportez-vous à la section create index dans le *Manuel de référence d'Adaptive Server* pour plus d'informations sur le pourcentage du facteur de remplissage.

### *default exp_row_size percent*

| Récapitulatif | |
|---|---|
| Valeur par défaut | 5 |
| Plage de valeurs | 0–100 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

default exp_row_size percent réserve de l'espace pour les mises à jour d'extension dans les tables en mode verrouillages des données seules afin de réduire la redirection de ligne. Une *mise à jour d'extension* est toute mise à jour d'une ligne de données qui augmente la longueur de la ligne. Les lignes de données qui autorisent des valeurs nulles ou qui contiennent des colonnes de longueur variable peuvent faire l'objet de mises à jour d'extension. Dans les tables en mode verrouillage des données seules, les mises à jour d'extension peuvent nécessiter une redirection de ligne si la taille de la ligne de données augmente au point que celle-ci ne tient plus sur la page.

La valeur par défaut est définie sur 5 % de la taille de page disponible pour les mises à jour d'extension. Compte tenu des 2002 octets disponibles pour le stockage des données sur les pages d'une table en mode verrouillage de données seules, la valeur par défaut réserve 100 octets pour une éventuelle extension. Cette valeur est uniquement appliquée aux pages des tables qui contiennent des colonnes de longueur variable.

Les valeurs correctes sont comprises entre 0 et 99. En définissant default exp_row_size percent sur 0, toutes les pages sont complètement remplies et il n'existe aucun espace pour les mises à jour d'extension.

default exp_row_size percent est appliqué aux tables en mode verrouillage de données seules contenant des colonnes de longueur variable lorsque exp_row_size n'est pas explicitement fourni avec create table ou défini avec sp_chgattribute. Si une valeur est fournie avec create table, cette valeur est prioritaire sur la valeur du paramètre de configuration. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### dump on conditions

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–1 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

dump on conditions détermine si Adaptive Server génère une sauvegarde des données dans la mémoire partagée lorsqu'il rencontre les conditions indiquées dans maximum dump conditions.

**Remarque** L'usage du paramètre dump on conditions est réservé au Support Technique de Sybase. Ne le modifiez pas sauf si vous y êtes invité par le Support Technique de Sybase.

### enable sort-merge joins and JTC

| Récapitulatif | |
|---|---|
| Valeur par défaut | 0 |
| Plage de valeurs | 0–1 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre de configuration enable sort-merge joins and JTC détermine quelles jointures par fusion et quelles fermetures transitives par jointure sont prises en compte par l'optimiseur de requête. Par défaut, les jointures par fusion et les fermetures transitives par jointure ne sont pas activées. Pour activer les jointures par fusion, définissez ce paramètre sur 1.

Les jointures par fusion et les fermetures transitives par jointure peuvent améliorer les performances des requêtes qui accèdent à de grands volumes de données, mais augmentent la durée de l'optimisation. Les options de session set sort-merge on et set jtc on ont priorité sur le paramétrage au niveau du serveur. Pour plus d'informations, reportez-vous aux sections "Activation et désactivation des jointures par fusion", page 458 et "Activation et désactivation de la fermeture transitive de jointures", page 459 dans le document *Performances et optimisation*.

### *enable row level access control*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 12.5 | N/A |
| Valeur par défaut | 0 |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Responsable de la sécurité du système (SSO) |

Permet le contrôle d'accès au niveau de la ligne. Vous devez activer la clé de licence des services de sécurité avant de pouvoir configurer enable row level access control.

### *enable ssl*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 12.5 | N/A |
| Valeur par défaut | 0 |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Responsable de la sécurité du système (SSO) |

Le paramètre enable ssl permet d'activer ou de désactiver la sécurité SSL de la session (Secure Sockets Layer).

### *event buffers per engine*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 100 |
| Plage de valeurs | 1–2147483647 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre event buffers per engine spécifie le nombre d'événements par moteur Adaptive Server qui peuvent être surveillés simultanément par Adaptive Server Monitor. Les événements sont utilisés par le moniteur d'Adaptive Server pour observer les performances d'Adaptive Server ; si vous n'utilisez pas Adaptive Server Monitor, définissez ce paramètre sur 1.

La valeur que vous affectez à event buffers per engine dépend du nombre de moteurs de votre configuration, du niveau d'activité sur votre Adaptive Server et des types d'applications que vous exécutez.

Une valeur faible pour event buffers per engine peut donner lieu à des pertes d'informations d'événement. La valeur par défaut est certainement trop faible pour la majorité des sites. Des valeurs de 2000 et plus devraient mieux convenir pour la surveillance générale. Vous devrez cependant procéder à des essais pour déterminer la valeur appropriée pour votre site.

Une valeur trop élevée pour event buffers per engine permet généralement de réduire la dégradation des performances d'Adaptive Server entraînée par Adaptive Server Monitor.

Chaque buffer d'événement occupe 100 octets de mémoire. Pour déterminer l'espace mémoire total utilisé par une valeur donnée de event buffers per engine, multipliez la valeur par le nombre de moteurs Adaptive Server dans votre configuration.

### housekeeper free write percent

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Plage de valeurs | 0–100 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

housekeeper free write percent spécifie le pourcentage maximum d'augmentation d'écritures de bases de données résultant de la tâche housekeeper.

Pour interrompre l'exécution de la tâche housekeeper lorsque la fréquence des écritures de base de données devient supérieure de 5 % à la normale, par exemple, définissez la valeur de housekeeper free write percent sur 5 :

```
sp_configure "housekeeper free write percent", 5
```

Lorsqu'Adaptive Server n'a pas de tâche utilisateur à traiter, la tâche housekeeper commence automatiquement à écrire les pages modifiées du cache vers le disque. Ces écritures se traduisent par une meilleure utilisation du processeur, par une réduction du nombre de vidages du buffer pendant le traitement des transactions et par des points de reprise moins espacés.

Dans des applications qui effectuent régulièrement une mise à jour de la même page de la base de données, la tâche housekeeper peut être à l'origine de certaines écritures inutiles dans la base de données. Bien que ces écritures n'aient lieu que pendant les cycles d'inactivité du serveur, elles peuvent être inacceptables sur des systèmes dont les disques sont surchargés.

Les statistiques des tables et des index qui sont utilisées pour optimiser les requêtes sont maintenues dans les structures de la mémoire pendant le traitement des requêtes. Lorsque ces statistiques changent, les modifications ne sont pas écrites immédiatement dans la table systabstats afin de réduire les conflits d'E/S et pour améliorer les performances. A la place, la tâche housekeeper vide régulièrement les statistiques vers le disque.

**Avertissement !** En définissant housekeeper free write percent sur 0, vous désactivez le vidage des statistiques vers la table systabstats. Les performances peuvent être sérieusement affectées en cas de changement important des statistiques.

La valeur par défaut permet à la tâche housekeeper d'augmenter les E/S disque d'un maximum de 1 %, ce qui améliore les performances et la vitesse de restauration sur la majorité des systèmes.

Pour désactiver la tâche housekeeper, définissez la valeur du paramètre housekeeper free write percent sur 0 (zéro) :

```
sp_configure "housekeeper free write percent", 0
```

Vous ne devez définir cette valeur sur 0 que si les conflits de disque sont élevés sur votre système et que celui-ci ne peut pas tolérer les E/S supplémentaires générées par la tâche housekeeper.

Si vous désactivez la tâche housekeeper, assurez-vous que les statistiques soient tenues à jour. Ci-après les commandes qui écrivent les statistiques sur le disque :

- update statistics
- dbcc checkdb (pour toutes les tables dans une base de données) ou dbcc checktable (pour une seule table)
- sp_flushstats

Vous devez exécuter l'une de ces commandes sur toutes les tables qui ont été mises à jour depuis la dernière écriture des statistiques sur le disque aux moments suivants :

- Avant de sauvegarder une base de données
- Avant un arrêt normal
- Après un redémarrage suite à une défaillance ou à un arrêt normal. Dans ce cas, vous ne pouvez pas utiliser sp_flushstats, vous devez utiliser les commandes update statistics ou dbcc.
- Après toute modification importante à une table, comme une opération de copie de masse importante, une modification du plan de verrouillage, la suppression ou l'insertion d'un grand nombre de lignes ou une commande truncate table.

Pour que la tâche housekeeper puisse fonctionner en continu, indépendamment du pourcentage d'écritures supplémentaires dans la base de données, définissez la valeur de housekeeper free write percent sur 100 :

```
sp_configure "housekeeper free write percent", 100
```

Utilisez sp_sysmon pour surveiller les performances de la tâche housekeeper. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

Il peut également être utile de vérifier le nombre de points de reprise libres amorcés par la tâche housekeeper. Le document *Performances et optimisation* décrit ce résultat.

### *enable HA*

| **Récapitulatif** | |
|---|---|
| Valeur par défaut | 0 |
| Plage de valeurs | 0–1 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

En définissant enable HA sur 1, vous configurez Adaptive Server comme un serveur compagnon dans un sous-système à haut niveau de disponibilité. Adaptive Server utilise le mode reprise sur le serveur secondaire de Sybase pour interagir avec le sous-système à haut niveau de disponibilité. Vous devez définir enable HA sur 1 avant d'exécuter le script *installhasvss* (*insthasv* sous Windows NT), lequel installe les procédures système pour le mode reprise sur le serveur secondaire de Sybase.

**Remarque** L'information de licence et la valeur d'exécution de enable HA sont indépendantes l'une de l'autre. Que vous possédiez ou non une licence pour le mode reprise sur le serveur secondaire de Sybase, la valeur d'exécution et la valeur configurée sont définies sur 1 après le redémarrage d'Adaptive Server. Vous ne pouvez pas exécuter le mode reprise sur le serveur secondaire de Sybase tant que vous ne possédez pas de licence. Si vous n'avez pas installé de licence valide, Adaptive Server enregistre un message d'erreur et n'active pas la fonctionnalité. Reportez-vous au Guide d'installation pour plus d'informations sur l'installation des clés de licence.

Notez que le fait de définir enable HA sur 1 ne veut pas dire qu'Adaptive Server est configuré pour fonctionner comme un système à haut niveau de disponibilité. Vous devez effectuer les étapes décrites dans le document *Utilisation de Sybase Failover en environnement haute disponibilité* pour configurer Adaptive Server en tant que serveur compagnon dans un système à haut niveau de disponibilité.

Lorsque enable HA est défini sur 0, vous ne pouvez pas configurer le mode reprise sur le serveur secondaire de Sybase et vous ne pouvez pas exécuter *installhasvss* (*insthasv* sous Windows NT).

### *enable housekeeper GC*

| **Récapitulatif** | |
|---|---|
| Valeur par défaut | 1 |
| Plage de valeurs | 0–1 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Lorsque enable housekeeper GC est défini sur 1, la tâche housekeeper effectue une récupération d'espace sur les tables en mode verrouillage des données seules. Le paramètre housekeeper free write percent doit lui aussi être supérieur à 0, sinon la tâche housekeeper est désactivée. Lorsqu'un utilisateur supprime une ligne d'une table en mode verrouillage des données seules, une tâche est mise en file d'attente pour rechercher les suppressions validées dans les pages de données et d'index.

Lorsque enable housekeeper GC est défini sur 0, la tâche housekeeper n'effectue pas de réclamation d'espace. Si toutes les tables de votre serveur utilisent le plan de verrouillage allpages ou si le nombre de mises à jour par suppressions ou par rétrécissement est très faible sur les tables en mode verrouillage des données seules, le fait de définir enable housekeeper GC sur 0 améliore les performances en réduisant légèrement la charge supplémentaire de la tâche housekeeper. Utilisez ce paramètre :

- Si vous utilisez uniquement le verrouillage allpages
- Si peu de suppressions sont effectuées sur vos tables en mode verrouillage des données seules
- Si votre charge de travail ne laisse que peu de temps d'inactivité au processeur

sp_sysmon indique la fréquence des récupérations d'espace effectuées par la tâche housekeeper et le nombre de pages récupérées. Reportez-vous au document *Performances et optimisation*.

### *identity burning set factor*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | identity burning set factor |
| Valeur par défaut | 5000 |
| Plage de valeurs | 1–9999999 |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Les colonnes IDENTITY sont de type numeric et d'échelle zéro dont les valeurs sont générées par Adaptive Server. Les valeurs des colonnes peuvent être comprises entre un minimum de 1 et un maximum déterminé par la précision de la colonne.

Pour chaque table comprenant une colonne IDENTITY, Adaptive Server divise l'ensemble des valeurs possibles de la colonne en blocs de chiffres consécutifs et rend disponible un bloc à la fois dans la mémoire. A chaque insertion d'une ligne dans une table, Adaptive Server attribue à la colonne IDENTITY la prochaine valeur disponible du bloc. Le bloc suivant devient disponible lorsque tous les numéros d'un bloc ont été utilisés.

Cette méthode de choix des valeurs de la colonne IDENTITY améliore les performances du serveur. Lorsque Adaptive Server affecte une nouvelle valeur à la colonne, il lit la valeur maximale courante dans la mémoire et ajoute 1. Les accès disque ne deviennent nécessaires que lorsque toutes les valeurs du bloc ont été utilisées. Tous les numéros restants dans un bloc étant supprimés lors d'une défaillance du serveur (ou shutdown with nowait), cette méthode peut donner lieu à des valeurs manquantes dans la colonne IDENTITY.

Utilisez identity burning set factor pour modifier le pourcentage de valeurs potentielles de la colonne qui sont mises à disposition dans chaque bloc. Ce chiffre doit être suffisamment élevé pour garantir de bonnes performances, mais pas trop élevé pour éviter que les valeurs manquantes dans la colonne soient trop nombreuses. La valeur par défaut qui est 5000 libère en une seule fois 0,05 % des valeurs potentielles de la colonne IDENTITY.

Pour obtenir la valeur correcte de sp_configure, exprimez le pourcentage sous forme décimale et multipliez-le par $10^7$ (10 000 000). Pour libérer 15 % (0,15) des valeurs potentielles de la colonne IDENTITY en une seule fois, par exemple, définissez une valeur de 0,15 fois $10^7$ (ou 1 500 000) pour sp_configure :

```
sp_configure "identity burning set factor", 1500000
```

### *identity grab size*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Plage de valeurs | 1–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Le paramètre identity grab size permet à chaque processus Adaptive Server de réserver un bloc de valeurs de la colonne IDENTITY pour les insertions dans des tables contenant une colonne IDENTITY.

Cette option est utile si vous effectuez des insertions et que vous voulez que les données insérées possèdent des numéros IDENTITY consécutifs. Si vous saisissez des données de bulletin de salaire, par exemple, et que vous voulez que tous les enregistrements associés à un service particulier se trouvent dans le même bloc de lignes, attribuez à identity grab size la valeur correspondant au nombre d'enregistrements pour ce service.

identity grab size s'applique à tous les utilisateurs d'Adaptive Server. Une valeur élevée de identity grab size donne lieu à des espaces importants entre les valeurs de la colonne IDENTITY si de nombreux utilisateurs insèrent des données dans les tables comprenant des colonnes IDENTITY.

Sybase recommande d'attribuer à identity grab size une valeur suffisamment élevée pour recevoir le groupe d'enregistrements le plus grand que vous voulez insérer dans des lignes contiguës.

### *i/o accounting flush interval*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | i/o flush |
| Valeur par défaut | 1000 |
| Plage de valeurs | 1–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

i/o accounting flush interval spécifie la durée, en impulsions d'horloge *machine*, pendant laquelle Adaptive Server attend avant de vider les statistiques d'E/S pour chaque utilisateur de sysprocesses vers syslogins. Ce paramètre est utilisé pour la comptabilisation du taux de charge du processeur.

Lorsqu'un utilisateur se connecte à Adaptive Server, le serveur commence à totaliser les statistiques d'E/S pendant ce processus utilisateur dans sysprocesses. Lorsque la valeur de i/o accounting flush interval est dépassée ou qu'un utilisateur se déconnecte d'Adaptive Server, les statistiques d'E/S cumulées pour cet utilisateur sont vidées de sysprocesses vers syslogins. Ces statistiques continuent d'être totalisées dans syslogins jusqu'à ce que vous remettiez les totaux à zéro à l'aide de sp_clearstats. Vous pouvez afficher les totaux actuels dans syslogins à l'aide de sp_reportstats.

La valeur que vous avez fixée pour i/o accounting flush interval dépend du type d'état que vous prévoyez de générer. Si vous voulez générer un état mensuel, affectez une valeur relativement élevée à i/o accounting flush interval. Ceci est lié au fait qu'avec des états plus espacés, il est moins important d'effectuer une mise à jour fréquente des données dans syslogins.

Si vous prévoyez d'effectuer des sélections spécifiques périodiques sur la colonne totio dans syslogins pour déterminer le volume d'E/S par processus, affectez à i/o accounting flush interval une valeur inférieure. Vous augmenterez ainsi la probabilité de présence de données à jour dans syslogins lorsque vous exécutez vos sélections.

Si vous ne prévoyez pas de générer d'états sur les statistiques d'E/S, affectez à cpu accounting flush interval sa valeur maximale.Vous réduirez ainsi le nombre de mises à jour de syslogins et le nombre de fois que ses pages doivent être écrites sur le disque.

### *i/o polling process count*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cmaxscheds |
| Valeur par défaut | 10 |
| Plage de valeurs | 1–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre i/o polling process count spécifie le nombre maximum de processus qu'Adaptive Server peut exécuter avant que l'ordonnanceur ne contrôle l'achèvement des E/S disque et/ou réseau. L'optimisation de i/o polling process count affecte à la fois le temps de réponse et le rendement d'Adaptive Server.

Adaptive Server vérifie l'achèvement des E/S disque ou réseau :

- Si le nombre de tâches exécutées depuis la dernière fois qu'Adaptive Server a vérifié l'achèvement des E/S est égal à la valeur de i/o polling process count et
- A chaque impulsion d'horloge d'Adaptive Server.

En règle générale, une augmentation de la valeur de i/o polling process count peut augmenter le débit pour les applications qui génèrent de nombreuses E/S disque et réseau. A l'inverse, une diminution de la valeur peut améliorer le temps de réponse des processus dans ces applications, vraisemblablement avec le risque de réduire le débit.

Si vos applications créent à la fois des E/S et des tâches qui sollicitent fortement le processeur, l'optimisation de i/o polling process count à une valeur faible (1–2) garantit que les tâches à fort taux d'E/S peuvent accéder aux cycles du processeur.

Pour les applications OLTP (ou toute application à fort taux d'E/S avec des connexions utilisateur et des transactions courtes), l'optimisation de i/o polling process count à une valeur comprise entre 20 et 30 peut augmenter le débit, mais peut également augmenter le temps de réponse.

Tenez compte de trois autres paramètres lorsque vous optimisez i/o polling process count :

- sql server clock tick length, qui spécifie la durée d'une impulsion d'horloge d'Adaptive Server en microsecondes. Reportez-vous à la section "sql server clock tick length", page 227.

- time slice, qui spécifie la durée, en nombre d'impulsions d'horloge d'Adaptive Server, pendant laquelle l'ordonnanceur autorise l'exécution d'un processus utilisateur. Reportez-vous à la section "time slice", page 228.
- cpu grace time, qui spécifie la durée maximale (en impulsions d'horloge) pendant laquelle un processus utilisateur peut être exécuté sans arrêter le processeur avant qu'Adaptive Server ne prenne la main et y mette fin avec une erreur time-slice. Reportez-vous à la section "cpu grace time", page 198.

Utilisez sp_sysmon pour déterminer les effets d'une modification du paramètre i/o polling process count. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### *page lock promotion HWM*

| **Récapitulatif** | |
|---|---|
| Valeur par défaut | 200 |
| Plage de valeurs | 2–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Le paramètre page lock promotion HWM (repère de niveau haut), combiné avec les paramètres page lock promotion LWM (repère de niveau bas) et page lock promotion PCT (pourcentage), spécifie le nombre de verrous de page autorisés pendant une session de balayage unique d'une table en mode verrouillage de page ou d'un index avant qu'Adaptive Server essaie de passer des verrous de page à un verrou de table.

page lock promotion HWM définit un nombre maximum de verrous de page autorisés sur une table avant qu'Adaptive Server essaie de passer à un verrou de table. Lorsque le nombre de verrous de page acquis pendant une session de balayage dépasse page lock promotion HWM, Adaptive Server essaie d'acquérir un verrou de table. La valeur de page lock promotion HWM ne peut pas être supérieure à la valeur de number of locks.

Reportez-vous à la section "Configuration des verrous et des seuils de conversion des verrous", page 241 dans le document *Performances et optimisation* pour plus d'informations sur les sessions de balayage et sur la configuration des limites de conversion des verrous de page.

La valeur par défaut de page lock promotion HWM convient à la majorité des applications. Vous pouvez augmenter la valeur pour éviter le verrouillage des tables. Si vous savez, par exemple, qu'une mise à jour régulière de 500 pages est effectuée sur des tables en mode verrouillage allpages ou datapages qui contiennent des milliers de pages, vous pouvez augmenter la concurrence d'accès aux tables en fixant le paramètre page lock promotion HWM à 500 afin que la conversion de verrou n'ait pas lieu avec la valeur par défaut qui est 200.

Vous pouvez également configurer la conversion de verrou pour les tables en mode verrouillage de page et les visualiser au niveau de l'objet. Reportez-vous à la section sp_setrowlockpromote dans le document *Manuel de référence d'Adaptive Server*.

Utilisez sp_sysmon pour vérifier comment une modification de page lock promotion HWM affecte le nombre de conversions de verrou. sp_sysmon indique le rapport entre les conversions de verrou concernant exclusivement des pages et celles concernant exclusivement des tables et le rapport entre les conversions de verrou de pages partagées et de tables partagées. Reportez-vous à la section "Conversions de verrou", page 1044 dans le document *Performances et optimisation*.

### *page lock promotion LWM*

| **Récapitulatif** | |
|---|---|
| Valeur par défaut | 200 |
| Plage de valeurs | 2–valeur de page lock promotion HWM |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Le paramètre page lock promotion LWM (repère de niveau bas), combiné avec les paramètres page lock promotion HWM (repère de niveau haut) et page lock promotion PCT (pourcentage), spécifie le nombre de verrous de page autorisés pendant une session de balayage unique d'une table en mode verrouillage de page ou d'un index avant qu'Adaptive Server essaie de passer des verrous de page à un verrou de table.

Le paramètre page lock promotion LWM définit le nombre de verrous de page en-dessous duquel Adaptive Server n'essaie pas d'exécuter un verrou de table sur un objet. La valeur de page lock promotion LWM doit être inférieure ou égale à la valeur de page lock promotion HWM.

Reportez-vous à la section "Configuration des verrous et des seuils de conversion des verrous", page 241 dans le document *Performances et optimisation* pour plus d'informations sur les sessions de balayage et sur la configuration des limites de conversion des verrous.

La valeur par défaut de page lock promotion LWM est suffisante pour la majorité des applications. Si Adaptive Server a épuisé tous les verrous (sauf pour une instruction isolée), vous devez augmenter la valeur de number of locks. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

Vous pouvez également configurer la conversion de verrou de page au niveau de l'objet. Reportez-vous à la section sp_setrowlockpromote dans le document *Manuel de référence d'Adaptive Server*.

### *page lock promotion PCT*

| **Récapitulatif** | |
|---|---|
| Valeur par défaut | 100 |
| Plage de valeurs | 1–100 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Si le nombre de verrous maintenus sur un objet est compris entre page lock promotion LWM (repère de niveau bas) et page lock promotion HWM (repère de niveau haut), page lock promotion PCT définit le pourcentage de verrous de page (en fonction de la taille de la table) au-dessus duquel Adaptive Server essaie d'acquérir un verrou de table.

Reportez-vous à la section "Configuration des verrous et des seuils de conversion des verrous", page 241 dans le document *Performances et optimisation* pour plus d'informations sur la configuration des limites de conversion des verrous de page.

La valeur par défaut de page lock promotion PCT convient à la majorité des applications.

Vous pouvez également configurer la conversion de verrou au niveau de l'objet pour les objets en mode verrouillage de page. Reportez-vous à la section sp_setrowlockpromote dans le document *Manuel de référence d'Adaptive Server*.

### maximum dump conditions

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 10 |
| Plage de valeurs | 10–100 |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Le paramètre maximum dump conditions définit le nombre maximum de conditions que vous pouvez spécifier et pour lesquelles Adaptive Server génère une sauvegarde des données dans la mémoire partagée.

**Remarque** Ce paramètre est réservé au Support Technique de Sybase. Ne le modifiez pas sauf si vous y êtes invité par le Support Technique de Sybase.

### number of alarms

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cnalarm |
| Valeur par défaut | 40 |
| Plage de valeurs | 40–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

number of alarms spécifie le nombre de structures d'alarme allouées par Adaptive Server.

La commande Transact-SQL waitfor définit un moment, un intervalle de temps ou un événement spécifique pour l'exécution d'un bloc d'instructions, d'une procédure stockée ou d'une transaction. Adaptive Server utilise les alarmes pour exécuter correctement les commandes waitfor. D'autres processus internes nécessitent des alarmes.

Lorsque Adaptive Server a besoin de plus d'alarmes que celles qui sont actuellement allouées, le message suivant est écrit dans le journal d'erreurs :

```
uasetalarm: no more alarms available
```

Le nombre d'octets de mémoire pour chacune est faible. Si vous augmentez de manière importante la valeur de number of alarms, vous devez corriger max memory en conséquence.

### *number of aux scan descriptors*

| Récapitulatif | |
|---|---|
| Valeur par défaut | 200 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

number of aux scan descriptors définit le nombre de descripteurs de balayage auxiliaires disponibles dans une zone partagée par tous les utilisateurs sur un serveur.

Chaque connexion utilisateur et chaque processus de travail possède 48 descripteurs de balayage qui lui sont alloués de manière exclusive. Parmi eux, 16 sont réservés pour les tables utilisateur, 12 pour les tables de travail et 20 pour les tables système (dont 4 mis de côté pour les conditions d'annulation). Un descripteur est nécessaire pour chaque table référencée directement ou indirectement par une requête. Une référence de table utilisateur contient les éléments suivants :

- Toutes les tables référencées dans la clause from de la requête
- Toutes les tables référencées dans une vue nommée dans la requête (la vue elle-même n'est pas comptée)
- Toutes les tables référencées dans une sous-requête
- Toutes les tables dont l'intégrité référentielle doit être contrôlée (celles-ci sont seulement utilisées pour les insertions, les mises à jour et les suppressions)
- Une table créée avec select...into
- Toutes les tables de travail créées pour la requête

Si une table est référencée plus d'une fois (par exemple dans une autojointure, dans plus d'une vue ou dans plus d'une sous-requête), la table est comptée à chaque fois. Si la requête contient une union, chaque instruction select dans la requête union est un balayage séparé. Si une requête est exécutée en parallèle, le processus de coordination et chaque processus de travail nécessitent un descripteur de balayage pour chaque référence à une table.

Lorsque le nombre de tables utilisateur référencées par une requête de balayage dépasse 16 ou lorsque le nombre de tables de travail dépasse 12, des descripteurs de balayage sont alloués depuis la zone partagée. Les tables en mode verrouillage de données seules ont également besoin d'un descripteur de table système pour chaque table en mode verrouillage de données seules à laquelle on accède par le biais d'un balayage de table (mais non celles auxquelles on accède par le biais d'un balayage d'index). Si on accède à plus de 16 tables en mode verrouillage des données seules à l'aide des balayages de table dans une requête, des descripteurs de balayage auxiliaires leur sont alors alloués.

Si un balayage a besoin de descripteurs de balayage auxiliaires après avoir consommé la quantité allouée et qu'il n'y a plus de descripteurs disponibles dans la zone partagée, Adaptive Server affiche un message d'erreur et annule la transaction utilisateur.

Si aucune de vos requêtes n'a besoin de descripteurs de balayage supplémentaires, vous pouvez laisser le paramètre number of aux scan descriptors à sa valeur par défaut lorsque les exigences de votre système augmentent. Ne définissez ce paramètre sur 0 que si vous êtes sûr que les utilisateurs du système n'exécuteront pas de requêtes sur plus de 16 tables et que vos tables ne présentent que peu ou aucune contrainte d'intégrité. Pour plus d'informations, reportez-vous à la section "Surveillance de l'utilisation des descripteurs de balayage", page 219.

Utilisez l'une des méthodes suivantes si vos requêtes ont besoin de plus de descripteurs de balayage :

- Ré-écrivez la requête ou fractionnez-la en plusieurs étapes en utilisant des tables temporaires. Pour les tables en mode verrouillage des données seules, envisagez d'ajouter des index si les balayages de la table sont nombreux.
- Revoyez la conception du plan de la table afin qu'elle utilise moins de descripteurs de balayage si elle emploie un grand nombre de contraintes d'intégrité référentielle. Vous pouvez vérifier le nombre de descripteurs qui seront utilisés par une requête en activant set showplan, noexec on avant d'exécuter la requête.

- Augmentez la valeur de number of aux scan descriptors.

Les sections suivantes expliquent comment surveiller l'utilisation courante et le repère de niveau haut avec sp_monitorconfig pour éviter d'être à court de descripteurs et comment estimer le nombre de descripteurs de balayage dont vous avez besoin.

#### Surveillance de l'utilisation des descripteurs de balayage

sp_monitorconfig indique le nombre de descripteurs de balayage inutilisés (libres), le nombre de descripteurs de balayage auxiliaires en cours d'utilisation, le pourcentage de ceux qui sont actifs et le nombre maximum de descripteurs de balayage utilisés depuis le dernier démarrage du serveur. Exécutez régulièrement cette instruction pendant les périodes de pointe pour surveiller l'utilisation des descripteurs de balayage.

Cet exemple de résultat montre l'utilisation des 500 descripteurs de balayage configurés :

```
sp_monitorconfig "aux scan descriptors"
Usage information at date and time: Jan 24 1997 9:54AM.
Name            # Free   # Active   % Active  # Max Ever Used   Re-used
--------------  --------  -------   ---------   --------------  -------
number of aux   260       240      48,00      427               NA
scan
descriptors
```

240 descripteurs de balayage auxiliaires seulement sont utilisés, ce qui en laisse 260 de libres. Le nombre maximum de descripteurs de balayage utilisés à tout moment depuis le dernier démarrage d'Adaptive Server est toutefois de 427, ce qui laisse une marge d'environ 20 pour-cent pour une augmentation de l'utilisation et pour les périodes exceptionnellement chargées. "Re-used" ne concerne pas les descripteurs de balayage.

#### Estimation et configuration des descripteurs de balayage auxiliaires

Procédez comme suit pour obtenir une estimation de l'utilisation des descripteurs de balayage :

1 Déterminez le nombre de références de table pour chaque requête qui fait référence à plus de 16 tables utilisateur ou pour celles qui contiennent un grand nombre de contraintes référentielles en exécutant la requête avec set showplan et set noexec activés. Si des descripteurs de balayage auxiliaires sont requis, showplan indique le nombre nécessaire :

```
Auxiliary scan descriptors required: 17
```

Le nombre indiqué comprend tous les descripteurs de balayage auxiliaires nécessaires pour la requête, y compris ceux pour tous les processus de travail. Si vos requêtes font seulement appel à des contraintes référentielles, vous pouvez également utiliser sp_helpconstraint, qui affiche le nombre de contraintes référentielles par table.

2 Pour chaque requête qui emploie des descripteurs de balayage auxiliaires, estimez le nombre d'utilisateurs qui exécuteront la requête simultanément et multipliez. Si vous supposez que 10 utilisateurs exécuteront une requête qui a besoin de 8 descripteurs auxiliaires, vous en aurez besoin de 80 à tout moment.

3 Additionnez les résultats de chaque requête pour calculer le nombre total de descripteurs de balayage auxiliaires requis.

### *number of mailboxes*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cnmbox |
| Valeur par défaut | 30 |
| Plage de valeurs | 30–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

number of mailboxes spécifie le nombre de structures de boîte aux lettres allouées par Adaptive Server. Les boîtes aux lettres, qui sont utilisées en combinaison avec les messages, sont utilisées en interne par Adaptive Server pour la communication et la synchronisation entre les processus du service de noyau. Les boîtes aux lettres ne sont pas utilisées par les processus utilisateur. Ne modifiez pas ce paramètre sauf si vous y êtes invité par le Support Technique de Sybase.

### *number of messages*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cnmsg |
| Valeur par défaut | 64 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

number of messages spécifie le nombre de structures de message allouées par Adaptive Server. Les messages, qui sont utilisés en combinaison avec les boîtes aux lettres, sont utilisés en interne par Adaptive Server pour la communication et la synchronisation entre les processus du service de noyau. Les messages sont également utilisés pour la coordination entre une famille de processus dans le traitement en parallèle. Ne modifiez pas ce paramètre sauf si vous y êtes invité par le Support Technique de Sybase.

### *number of pre-allocated extents*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cpreallocext |
| Valeur par défaut | 2 |
| Plage de valeurs | 0–31 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

number of pre-allocated extents spécifie le nombre d'extents (huit pages) alloués dans un pas unique au gestionnaire de pages. Ce paramètre est actuellement utilisé seulement par bcp pour améliorer les performances lors de la copie de grands volumes de données. Par défaut, bcp alloue deux extents à la fois et écrit à chaque fois un enregistrement d'allocation dans le journal.

En affectant une valeur à number of pre-allocated extents, bcp allouera le nombre spécifié d'extents à chaque fois qu'elle aura besoin d'espace et écrira un enregistrement unique dans le journal pour l'événement. La valeur 0 désactive l'allocation d'extent, ce qui veut dire qu'une page unique est allouée à chaque fois que la commande bulk copy a besoin d'une page. Comme chaque allocation de page est journalisée, cela peut nettement augmenter le volume d'espace requis pour la journalisation des transactions.

Un objet peut se voir allouer plus de pages qu'il n'en a vraiment besoin, il est donc conseillé d'affecter une valeur faible à number of pre-allocated extents si vous utilisez bcp pour de petits batches. Si vous utilisez bcp pour de grands batches, augmentez la valeur de number of pre-allocated extents afin de réduire le nombre d'en-têtes nécessaires pour allouer des pages et pour réduire le nombre d'enregistrements dans le journal.

### number of sort buffers

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | csortbufsize |
| Valeur par défaut | 500 |
| Plage de valeurs | 0–32767 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

number of sort buffers spécifie le nombre de buffers de 2 Ko utilisés pour conserver les pages lues des tables d'entrée et pour effectuer des fusions d'index pendant les tris.

Sybase recommande de laisser ce paramètre à sa valeur par défaut sauf lorsque vous créez des index en parallèle. Une valeur trop élevée peut empêcher les processus autres que les tris d'accéder à la zone des buffers de 2 Ko dans les caches qui sont utilisés pour effectuer les tris.

Reportez-vous à la section "Caches, buffers de tri et tris en parallèle", page 639 dans le document *Performances et optimisation* pour plus d'informations sur la configuration de cette valeur pour les instructions create index en parallèle.

### partition groups

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1024 |
| Plage de valeurs | 1–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

partition groups spécifie le nombre maximum de groupes de partition qui peuvent être alloués par Adaptive Server. Les groupes de partition sont des structures internes utilisées par Adaptive Server pour contrôler l'accès aux partitions individuelles d'une table.

Un groupe de partitions se compose de 16 caches de partition qui stockent chacun des informations sur une partition unique. Tous les caches d'un groupe de partitions sont utilisés pour stocker des informations sur la même table partitionnée. Si une table comprend moins de 16 partitions, les caches de partition non utilisés dans ce groupe restent inutilisés et ne peuvent pas être utilisés par une autre table. Une table qui compte plus de 16 partitions nécessite plusieurs groupes de partitions.

La valeur par défaut permet un maximum de 1024 groupes de partitions ouverts et un maximum de 16 384 (1024 fois 16) partitions ouvertes. Le nombre réel de partitions peut être légèrement inférieur en raison du groupage des partitions.

Adaptive Server alloue des groupes de partitions à une table lorsque vous partitionnez la table ou lorsque vous y accédez pour la première fois après avoir redémarré Adaptive Server. Vous ne pourrez pas accéder à la table ou la partitionner s'il n'y a pas assez de groupes de partitions pour celle-ci.

### *partition spinlock ratio*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 10 |
| Plage de valeurs | 1–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Si Adaptive Server est exécuté avec plusieurs moteurs, le paramètre partition spinlock ratio définit le nombre de lignes dans les caches de partition internes qui sont protégées par un **spinlock**.

Adaptive Server gère l'accès aux partitions de table en utilisant des *groupes de partitions* internes qui contiennent chacun des caches de partition. Chaque cache de partition stocke des informations sur une partition (par exemple la dernière page de la partition) que les processus doivent utiliser lorsqu'ils accèdent à cette partition.

Par défaut, les systèmes Adaptive Server sont configurés avec le paramètre partition spinlock ratio à 10, soit 1 verrou d'attente pour 10 caches de partition. Une diminution de la valeur de partition spinlock ratio peut avoir un léger impact sur les performances d'Adaptive Server. La valeur par défaut convient pour la majorité des serveurs.

Pour plus d'informations sur la configuration des rapports des verrous d'attente, reportez-vous à la section "Configuration des paramètres de taux de verrous d'attente", page 691.

### *print deadlock information*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | T1204 (indicateur de trace) |
| Valeur par défaut | 0 (désactivé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

print deadlock information active l'impression des informations d'interblocage vers le journal d'erreur.

Si vous rencontrez des interblocages répétitifs, définissez print deadlock information sur 1 pour obtenir des informations utiles pour rechercher la cause des interblocages. Mais si vous attribuez la valeur 1 à print deadlock information, vous risquez de constater une nette détérioration des performances d'Adaptive Server. N'utilisez cette configuration que lorsque vous recherchez les causes d'interblocage.

Utilisez le résultat de sp_sysmon pour déterminer si des interblocages se produisent dans votre application. Le cas échéant, définissez print deadlock information sur 1 pour connaître leur origine. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### *runnable process search count*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cschedspins |
| Valeur par défaut | 2000 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

runnable process search count spécifie le nombre de fois qu'un moteur tourne en boucle à la recherche d'une tâche exécutable avant d'abandonner le processeur au système d'exploitation.

Les moteurs d'Adaptive Server vérifient la file d'attente des tâches exécutables dès qu'une tâche se termine ou dépasse son temps alloué pour le moteur. A un moment donné, les files d'attente ne contiendront plus aucune tâche. Un moteur peut soit abandonner le processeur au système d'exploitation, soit continuer de rechercher une tâche à exécuter. Une valeur plus élevée de runnable process search count a pour effet que le moteur tourne en boucle un plus grand nombre de fois et sollicite ainsi le processeur pendant plus longtemps. Une valeur plus faible de runnable process search count entraîne la libération du processeur par le moteur plus tôt.

Si votre machine est un monoprocesseur qui dépend des threads auxiliaires pour effectuer des E/S, vous pourrez constater une certaine amélioration des performances en affectant à runnable process search une valeur permettant d'effectuer des E/S réseau, des E/S disque ou d'autres tâches du système d'exploitation. Si un client, tel qu'une opération de copie de masse, est exécuté sur la même machine qu'un serveur monoprocesseur qui utilise des threads auxiliaires, il peut s'avérer particulièrement important de permettre à la fois au serveur et au client d'accéder au processeur.

La valeur par défaut offre de bonnes performances pour les Adaptive Server exécutés sur des machines monoprocesseur qui n'utilisent pas de threads auxiliaires et pour les machines multiprocesseur.

Utilisez sp_sysmon pour déterminer la manière dont le paramètre runnable process search count affecte l'utilisation des cycles processeur d'Adaptive Server, les arrêts du moteur pour le système d'exploitation et les contrôles réseau bloquants. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### *size of auto identity column*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 10 |
| Plage de valeurs | 1–38 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

size of auto identity column définit la précision des colonnes IDENTITY qui sont automatiquement créées avec les options sp_dboption auto identity et unique auto_identity index.

La valeur maximale pouvant être insérée dans une colonne IDENTITY est $10^{precision} - 1$. Lorsqu'une colonne IDENTITY atteint cette valeur maximale, toutes les instructions insert ultérieures renvoient une erreur qui annule la transaction courante.

Lorsque cela se produit, utilisez l'instruction create table pour créer une table identique à l'ancienne, mais ayant une précision supérieure pour la colonne IDENTITY. Une fois que vous avez créé la nouvelle table, copiez les données de l'ancienne table vers la nouvelle à l'aide de l'instruction insert ou de l'utilitaire bcp.

## *SQL Perfmon Integration* (Windows NT uniquement)

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 (activé) |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

SQL Perfmon Integration active et désactive l'aptitude à surveiller les statistiques d'Adaptive Server depuis l'analyseur de performances Windows NT.

Adaptive Server doit être enregistré comme service NT pour être intégré dans l'analyse des performances. Cet enregistrement est automatique si :

- Vous démarrez Adaptive Server à l'aide du Services Manager dans le groupe de programmes Sybase for Windows NT.
- Vous utilisez l'option "Services" du Panneau de configuration.
- Vous avez configuré Windows NT pour qu'Adaptive Server démarre comme un service automatique.

Le document *Adaptive Server - Manuel de configuration pour Windows NT* contient une liste des compteurs d'Adaptive Server que vous pouvez surveiller.

### *sql server clock tick length*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cclkrate |
| Valeur par défaut | Spécifique à la plate-forme |
| Plage de valeurs | Minimum spécifique à la plate-forme–1 000 000, par multiples de la valeur par défaut |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

sql server clock tick length spécifie la durée d'une impulsion d'horloge du serveur en microsecondes. La valeur par défaut et la valeur minimale sont toutes deux spécifiques à la plate-forme. Adaptive Server arrondit les valeurs à un multiple pair de *n*, où *n* est la valeur par défaut spécifique à la plate-forme de l'impulsion d'horloge. Vous pouvez connaître les valeurs courantes de sql server clock tick length à l'aide de sp_helpconfig ou de sp_configure.

Dans les applications à usage mixte avec certaines tâches liées au processeur, le fait de réduire la valeur de sql server clock tick length facilite les tâches relatives aux E/S. 20 000 est ici une valeur raisonnable. En raccourcissant la durée de l'impulsion d'horloge, les tâches liées au processeur dépasseront le temps alloué au moteur plus fréquemment par unité de temps, ce qui offre plus d'accès au processeur pour d'autres tâches. Cela peut également augmenter les temps de réponse de manière arbitraire, car Adaptive Server exécute ses tâches de service une fois par impulsion d'horloge. En diminuant la durée d'une impulsion d'horloge, les tâches de service seront exécutées plus fréquemment par unité de temps.

En augmentant sql server clock tick length, vous favorisez les tâches liées au processeur car elles sont exécutées plus longtemps entre les options contextuelles. La valeur maximale de 1 000 000 devrait convenir pour les applications essentiellement liées au processeur, mais les tâches liées aux E/S risquent d'en être affectées. Un compromis peut être obtenu en optimisant cpu grace time (voir "cpu grace time", page 198) et time slice (voir "time slice", page 228).

**Remarque** Une modification de la valeur de sql server clock tick length peut avoir de sérieuses répercussions sur les performances d'Adaptive Server. Prenez contact avec le Support Technique Sybase avant de modifier cette valeur.

### *text prefetch size*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 16 |
| Valeurs correctes | 0 à 65 535 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre text prefetch size limite le nombre de pages de données de type text et image qui peuvent être lues par anticipation dans une zone de buffer existante. Adaptive Server ne lit par anticipation que les données de type text et image qui ont été créées avec Adaptive Server 12.x ou qui ont été mises à niveau à l'aide de dbcc rebuild_text.

### *time slice*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | time slice |
| Valeur par défaut | 100 |
| Plage de valeurs | 50–1000 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

time slice spécifie la durée en millisecondes pendant laquelle l'ordonnanceur d'Adaptive Server autorise l'exécution d'une tâche. Si la valeur définie pour time slice est trop faible, Adaptive Server risque de prendre trop de temps pour passer d'une tâche à l'autre, ce qui augmente le temps de réponse. Si elle est trop élevée, les tâches qui consomment beaucoup de temps processeur risquent de monopoliser les moteurs, ce qui augmente également le temps de réponse. La valeur par défaut de 100 millisecondes permet à chaque tâche d'être exécutée pendant 1/10 de seconde avant de libérer le processeur pour une autre tâche.

Reportez-vous à la section "cpu grace time", page 198. Reportez-vous également au chapitre 3, "Utilisation des moteurs et des CPU", et à la section "Planification de la tâche en exécution", page 32 du document *Performances et optimisation* pour plus d'informations sur la planification des tâches.

Utilisez sp_sysmon pour déterminer comment time slice affecte les arrêts volontaires par les moteurs d'Adaptive Server. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### *upgrade version*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | upgrade version |
| Valeur par défaut | 1100 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

upgrade version indique la version de l'utilitaire de mise à niveau avec lequel vous avez effectué la mise à niveau de votre device master. L'utilitaire de mise à niveau vérifie et modifie ce paramètre pendant une mise à niveau.

**Avertissement !** Il est déconseillé de modifier ce paramètre malgré que cela soit possible. Vous pourriez rencontrer de sérieux problèmes avec Adaptive Server.

Vous pouvez déterminer si une mise à niveau a été effectuée sur votre device master en utilisant upgrade version sans préciser de valeur :

```
sp_configure "upgrade version"
```

### row lock promotion HWM

| Récapitulatif | |
|---|---|
| Valeur par défaut | 200 |
| Plage de valeurs | 2–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Le paramètre row lock promotion HWM (repère de niveau haut), combiné avec les paramètres row lock promotion LWM (repère de niveau bas) et row lock promotion PCT (pourcentage), spécifie le nombre de verrous de ligne autorisés pendant une session de balayage unique d'une table ou d'un index avant qu'Adaptive Server essaie de passer des verrous de ligne à un verrou de table.

row lock promotion HWM définit un nombre maximum de verrous de ligne autorisés sur une table avant qu'Adaptive Server essaie de passer à un verrou de table. Lorsque le nombre de verrous de ligne acquis pendant une session de balayage dépasse row lock promotion HWM, Adaptive Server essaie d'acquérir un verrou de table. La valeur de row lock promotion HWM ne peut pas être supérieure à la valeur de number of locks.

Reportez-vous à la section "Configuration des verrous et des seuils de conversion des verrous", page 241 dans le document *Performances et optimisation* pour plus d'informations sur les sessions de balayage et sur la configuration des limites de conversion des verrous.

La valeur par défaut de row lock promotion HWM convient à la majorité des applications. Vous pouvez augmenter la valeur pour éviter le verrouillage des tables. Si vous savez, par exemple, que des mises à jour sont effectuées régulièrement sur 500 lignes d'une table qui compte des milliers de lignes, vous pouvez augmenter la concurrence d'accès des tables en définissant row lock promotion HWM sur 500.

Vous pouvez également configurer la conversion de verrou de ligne au niveau de l'objet. Reportez-vous à la section sp_setrowlockpromote dans le document Manuel de référence d'Adaptive Server.

### *row lock promotion LWM*

| Récapitulatif | |
|---|---|
| Valeur par défaut | 200 |
| Plage de valeurs | 2–valeur de row lock promotion HWM |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Le paramètre row lock promotion LWM (repère de niveau bas), combiné avec les paramètres row lock promotion HWM (repère de niveau haut) et row lock promotion PCT (pourcentage), spécifie le nombre de verrous de ligne autorisés pendant une session de balayage unique d'une table ou d'un index avant qu'Adaptive Server essaie de passer des verrous de ligne à un verrou de table.

Le paramètre row lock promotion LWM définit le nombre de verrous de ligne en-dessous duquel Adaptive Server n'essaie pas d'acquérir un verrou de table sur un objet. La valeur de row lock promotion LWM doit être inférieure ou égale à la valeur de row lock promotion HWM.

Reportez-vous à la section "Configuration des verrous et des seuils de conversion des verrous", page 241 dans le document *Performances et optimisation* pour plus d'informations sur les sessions de balayage et sur la configuration des limites de conversion des verrous.

La valeur par défaut de row lock promotion LWM est suffisante pour la majorité des applications. Si Adaptive Server a épuisé tous les verrous (sauf pour une instruction isolée), vous devez augmenter la valeur de number of locks. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

Vous pouvez également configurer la conversion de verrou de ligne au niveau de l'objet. Reportez-vous à la section sp_setrowlockpromote dans le document *Manuel de référence d'Adaptive Server*.

### row lock promotion PCT

| Récapitulatif | |
|---|---|
| Valeur par défaut | 100 |
| Plage de valeurs | 1–100 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Si le nombre de verrous maintenus sur un objet est compris entre row lock promotion LWM (repère de niveau bas) et row lock promotion HWM (repère de niveau haut), row lock promotion PCT définit le pourcentage de verrous de ligne (en fonction du nombre de lignes dans la table) au-dessus duquel Adaptive Server essaie d'acquérir un verrou de table.

Reportez-vous à la section "Configuration des verrous et des seuils de conversion des verrous", page 241 dans le document *Performances et optimisation* pour plus d'informations sur la configuration des limites de conversion des verrous de ligne.

La valeur par défaut de row lock promotion PCT convient à la majorité des applications.

Vous pouvez également configurer la conversion de verrou de ligne au niveau de l'objet. Reportez-vous à la section sp_setrowlockpromote dans le document *Manuel de référence d'Adaptive Server*.

### license information

| Récapitulatif | |
|---|---|
| Valeur par défaut | 0 |
| Valeurs correctes | $0–2^{31}$ |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

license information permet aux administrateurs système Sybase de contrôler le nombre de licences utilisateur utilisées dans Adaptive Server. Ce paramètre permet seulement de contrôler le nombre de licences octroyées, il n'applique pas l'accord de licence.

Si license information est défini sur 0, Adaptive Server ne contrôle pas l'utilisation des licences. Si license information est supérieur à 0, la tâche housekeeper contrôle le nombre de licences utilisées pendant les cycles d'inactivité dans Adaptive Server. Définissez license information sur le nombre spécifié de licences dans votre accord de licence.

Si le nombre de licences utilisées est supérieur à la valeur affectée à license information, Adaptive Server écrit le message suivant dans le journal d'erreurs :

```
WARNING: Exceeded configured number of user licenses
```

A la fin de chaque période de 24 heures, le nombre maximum de licences utilisées pendant cette période est ajouté à la table syblicenseslog. La période de 24 heures recommence au début à chaque redémarrage d'Adaptive Server.

Pour plus d'informations, reportez-vous à la section "Contrôle de l'utilisation des licences", page 412.

## Aspect sécurité

Les paramètres de ce groupe configurent les fonctionnalités relatives à la sécurité.

### *allow procedure grouping*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 (activé) |
| Plage de valeurs | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Responsable de la sécurité du système (SSO) |

allow procedure grouping contrôle l'aptitude à regrouper les procédures stockées de même nom afin qu'elles puissent être supprimées avec une seule instruction drop procedure. Pour exécuter Adaptive Server dans la *configuration évaluée*, vous devez interdire le regroupement des procédures stockées en définissant cette option sur 0. Reportez-vous à la section **configuration évaluée** dans le *Adaptive Server - Glossaire* pour plus d'informations.

### *auditing*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Plage de valeurs | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Responsable de la sécurité du système (SSO) |

auditing active ou désactive l'audit pour Adaptive Server.

### *audit queue size*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | audit queue size |
| Valeur par défaut | 100 |
| Plage de valeurs | 1–65535 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Responsable de la sécurité du système (SSO) |

La file d'attente d'audit en mémoire contient les enregistrements d'audit générés pour chaque processus utilisateur jusqu'à ce que les enregistrements puissent être traités et écrits vers la trace d'audit. Un Responsable de la sécurité du système peut modifier la taille de la file d'attente d'audit à l'aide du paramètre audit queue size. Il faut trouver le compromis entre les performances et le risque lorsque vous définissez la taille de la file d'attente. Si la file d'attente est trop grande, les enregistrements peuvent y rester pendant un certain temps. Tant qu'un enregistrement se trouve dans la file d'attente, il risque d'être perdu en cas de panne du système. D'un autre côté, si la file d'attente est trop petite, elle peut régulièrement être pleine, ce qui affecte les performances générales du système et les processus utilisateur qui génèrent des enregistrements d'audit sont en veille si la file d'attente d'audit est pleine.

Voici quelques règles permettant de déterminer la taille recommandée de la file d'attente d'audit. Vous devez également tenir compte du nombre d'audits effectués sur votre site.

- Chaque enregistrement d'audit occupe 424 octets, un enregistrement peut cependant se limiter à 22 octets seulement s'il est écrit dans une page de données.
- Le nombre maximum d'enregistrements d'audit pouvant être perdus en cas de panne du système est égal à la taille de la file d'attente d'audit (enregistrements qui s'y trouvent), plus 20. Lorsque les enregistrements quittent la file d'attente d'audit, ils demeurent sur une page de buffer jusqu'à ce qu'ils soient écrits dans la table d'audit courante sur le disque. Les pages sont vidées vers le disque au maximum tous les 20 enregistrements (moins si le processus d'audit n'est pas occupé en permanence).
- Le champ extrainfo et les champs contenant des noms dans les tables d'audit du système sont de longueur variable, ce qui implique que les enregistrements d'audit qui contiennent des noms complets sont généralement plus importants.

Le nombre d'enregistrements d'audit qui peuvent tenir sur une page varie entre 4 et 80 ou plus. La mémoire requise pour la taille par défaut (100) de la file d'attente d'audit est d'environ 42 Ko.

### *current audit table*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Plage de valeurs | 0–8 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Responsable de la sécurité du système (SSO) |

Le paramètre de configuration current audit table définit la table dans laquelle Adaptive Server écrit des lignes d'audit. Un Responsable de la sécurité du système peut modifier la table d'audit courante en utilisant :

```
sp_configure "current audit table", n
  [, "with truncate"]
```

où n est un nombre entier qui détermine la nouvelle table d'audit courante de la manière suivante :

- 1 représente sysaudits_01, 2 représente sysaudits_02, etc. jusqu'à 8.
- 0 indique à Adaptive Server de définir la table suivante comme table d'audit courante. Si votre installation comporte trois tables d'audit, par exemple, (*sysaudits_01*, *sysaudits_02* et *sysaudits_03*), Adaptive Server définit la table d'audit courante sur :
  - 2 si la table d'audit courante est *sysaudits_01*
  - 3 si la table courante est *sysaudits_02*
  - 1 si la table d'audit courante est *sysaudits_03*

"with truncate" précise qu'Adaptive Server doit tronquer la nouvelle table si elle n'est pas déjà vide. sp_configure échoue si cette option n'est pas précisée et que la table n'est pas vide.

**Remarque** Si Adaptive Server tronque la table d'audit courante alors que ses données n'ont pas été archivées, tous les enregistrements d'audit qu'elle contenait sont perdus. Archivez les données d'audit avant d'employer l'option with truncate.

Pour pouvoir exécuter sp_configure afin de modifier la table d'audit courante, votre rôle actif doit être sso_role. Vous pouvez écrire une procédure relative aux seuils pour changer automatiquement la table d'audit courante.

### *enable ssl*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 12.5 | N/A |
| Valeur par défaut | 0 |
| Valeurs correctes | 0 (désactivé), 1 (activé) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre enable ssl permet d'activer ou de désactiver la sécurité SSL de la session (Secure Sockets Layer).

### *msg confidentiality reqd*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Plage de valeurs | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Responsable de la sécurité du système (SSO) |

Le paramètre msg confidentiality reqd impose que tous les messages en provenance et à destination d'Adaptive Server soient cryptés. Le paramètre use security services doit être défini sur 1 pour que les messages soient cryptés.

### *msg integrity reqd*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 (désactivé) |
| Plage de valeurs | 0 (désactivé), 1 (activé) |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Responsable de la sécurité du système (SSO) |

msg integrity reqd impose que l'intégrité des données de tous les messages soit vérifiée. use security services doit être défini sur 1 pour que cette opération ait lieu. Si msg integrity reqd est défini sur 1, Adaptive Server autorise l'établissement de la connexion client sauf si le client utilise l'un des services de sécurité suivants : message integrity, replay detection, origin checks ou out-of-seq checks.

### *secure default login*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0 (suivi d'un autre paramètre nommant le nom de login par défaut) |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Responsable de la sécurité du système (SSO) |

Le paramètre secure default login spécifie un nom de login par défaut pour tous les utilisateurs préauthentifiés mais ne disposant pas de nom de login dans la table master..syslogins.

Etablissez la connexion sécurisée par défaut avec :

```
sp_configure "secure default login", 0,
    default_login_name
```

où :

- secure default login est le nom du paramètre.

- 0 est un paramètre nécessaire car le deuxième paramètre de sp_configure doit être une valeur numérique.
- *nom_de_connexion_par_défaut* représente le nom de login par défaut pour un utilisateur non identifié par Adaptive Server, mais qui a déjà été authentifié par un mécanisme de sécurité. Ce nom doit être un nom de login correct dans master..syslogins.

Pour définir "dlogin" comme nom de login sécurisé par défaut, par exemple, tapez :

```
sp_configure "secure default login", 0, dlogin
```

### *select on syscomments.text column*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Plage de valeurs | 0–1 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Responsable de la sécurité du système (SSO) |

Ce paramètre permet de protéger le texte des objets de la base de données en limitant l'autorisation select sur la colonne text de la table syscomments. La valeur par défaut de 1 déclare "public" l'autorisation select. Définissez l'option sur 0 pour limiter l'autorisation select au propriétaire de l'objet et à l'administrateur système.

Pour exécuter Adaptive Server dans la *configuration évaluée*, vous devez protéger le texte source des objets de base de données en définissant cette option sur 0.

Pour plus d'informations, reportez-vous à la section **configuration évaluée** dans le document *Adaptive Server - Glossaire*.

### *suspend audit when device full*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Plage de valeurs | 0–1 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Responsable de la sécurité du système (SSO) |

suspend audit when device full détermine le comportement d'Adaptive Server lorsqu'un device d'audit devient complètement saturé.

**Remarque** Si vous utilisez plusieurs tables d'audit, chacune sur un device différent, et que vous avez créé une procédure relative aux seuils pour chaque segment de la table d'audit, les devices d'audit ne devraient jamais être saturés. La condition "full" (saturation) ne se produit que si votre procédure ne fonctionne pas correctement.

Choisissez l'une de ces valeurs :

- 0 – tronque la table d'audit suivante et l'active dès que la table d'audit courante arrive à saturation. En définissant ce paramètre sur 0, vous garantissez que le processus d'audit ne sera jamais interrompu. Vous courez cependant le risque que des enregistrements d'audit plus anciens soient perdus s'ils n'ont pas été archivés.
- 1 – suspend le processus d'audit et tous les processus utilisateur susceptibles de générer un événement auditable. Pour reprendre le fonctionnement normal, le Responsable de la sécurité du système doit se connecter et activer une table vide comme table d'audit courante. Au cours de cette période, les actions du Responsable de la sécurité du système sont exemptées d'audit. Si elles devaient générer des enregistrements d'audit en fonctionnement normal, Adaptive Server enverrait un message d'erreur et des informations sur l'événement au journal d'erreurs.

Définissez ce paramètre sur 1 pour une exécution dans la configuration évaluée. Reportez-vous à la section **configuration évaluée** dans le document *Adaptive Server - Glossaire* pour plus d'informations.

### *systemwide password expiration*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | password expiration interval |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–32767 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Responsable de la sécurité du système (SSO) |

systemwide password expiration, qui peut seulement être défini par un Responsable de la sécurité du système, définit le nombre de jours pendant lesquels les mots de passe restent corrects après avoir été changés. Les mots de passe n'expirent jamais si systemwide password expiration est défini sur 0. Si sa valeur est supérieure à 0, tous les mots de passe expirent après le nombre de jours spécifié. Le mot de passe d'un compte est considéré avoir expiré si une période supérieure à *nombre_de_jours* s'est écoulée depuis la dernière modification du mot de passe de ce compte.

Lorsque le nombre de jours restant avant l'expiration est inférieur à 25 % de la valeur de systemwide password expiration ou 7 jours, la valeur la plus grande étant prise en compte, un message indiquant le nombre de jours restant avant l'expiration s'affiche à chaque connexion de l'utilisateur. Les utilisateurs peuvent modifier leurs mots de passe à tout moment avant l'expiration.

Lorsque le mot de passe d'un compte a expiré, l'utilisateur peut toujours se connecter à Adaptive Server mais il ne peut plus exécuter de commande avant d'avoir utilisé sp_password pour modifier son mot de passe. Si le Responsable de la sécurité du système modifie le mot de passe de l'utilisateur pendant que le compte est en mode sp_password seulement, le compte revient à la situation normale après l'attribution du nouveau mot de passe.

Cette restriction s'applique uniquement aux sessions de connexion établies après l'expiration du mot de passe. Les utilisateurs qui sont connectés au moment où leur mot de passe vient à expiration ne sont pas affectés avant leur prochaine connexion.

### *unified login required* (Windows NT uniquement)

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0, 1 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Responsable de la sécurité du système (SSO) |

unified login required impose que tous les utilisateurs qui se connectent à Adaptive Server soient authentifiés par Windows NT LAN Manager. Le paramètre use security services doit avoir la valeur 1 pour pouvoir utiliser le service de sécurité de connexion unifié.

### *use security services* (Windows NT uniquement)

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0, 1 |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Responsable de la sécurité du système (SSO) |

use security services précise qu'Adaptive Server utilisera les services de sécurité fournis par Windows NT LAN Manager. Les services de connexion unifiés fournis avec LAN Manager ne pourront pas être utilisés si ce paramètre est défini sur 0.

## Unicode

Les paramètres de ce groupe configurent les fonctionnalités relatives à Unicode.

### *default unicode sortorder*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | (non utilisé actuellement) |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Le paramètre default unicode sortorder est une chaîne de caractères qui définit l'ordre de tri Unicode par défaut installé sur le serveur. La valeur utilisée est une chaîne plutôt qu'une valeur numérique afin de garantir un identificateur unique. Reportez-vous au chapitre 7, "Configuration des jeux de caractères, des ordres de tri et des langues". pour modifier l'ordre de tri Unicode par défaut.

### *enable surrogate processing*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Plage de valeurs | 0–1 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Active le traitement et maintient l'intégrité des paires de substitution dans les données Unicode. Définissez enable surrogate processing sur 1 pour activer le traitement de substitution. S'il est désactivé, le serveur ignore la présence des paires de substitution dans les données unicode et tous les codes qui maintiennent l'intégrité des paires de substitution sont ignorés. Les performances sont ainsi améliorées, mais la gamme des caractères Unicode qui apparaissent dans les données est limitée.

### enable unicode conversion

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–2 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Active la conversion des caractères en utilisant Unilib pour les données de type char, varchar et text. Définissez enable unicode conversion sur 1 pour utiliser la conversion intégrée. Si Adaptive Server ne trouve pas la conversion intégrée, il utilise la conversion de caractères Unilib. Définissez enable unicode conversion sur 2 pour utiliser la conversion Unilib appropriée. Définissez le paramètre sur 0 pour utiliser uniquement la conversion intégrée du jeu de caractères.

### enable unicode normalization

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 1 |
| Plage de valeurs | 0–1 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Active la normalisation de caractères Unilib. Le processus de normalisation modifie les données de manière à ce qu'il n'y ait qu'une seule représentation de la base de données pour une séquence donnée de caractères abstraits. Les caractères suivis de diacritiques combinés sont souvent remplacés par des formes précombinées.

Définissez enable unicode normalization sur 1 pour utiliser le processus intégré qui applique la normalisation à toutes les données Unicode entrantes. Si ce paramètre est désactivé (défini sur 0), l'étape de normalisation n'a pas lieu et c'est le code client qui est responsable de la normalisation à la place du serveur. Les performances sont améliorées si la normalisation est désactivée, mais seulement si *tous* les clients présentent des données Unicode au serveur en utilisant la même représentation.

**Remarque** La normalisation ne peut plus être activée une fois qu'elle a été désactivée. Cette modification unilatérale évite que des données non normalisées pénètrent dans la base de données.

### *size of unilib cache*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 0 |
| Plage de valeurs | 0–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

Détermine la taille du cache Unilib. Le paramètre size of unilib cache indique la taille en octets. Le cache nécessaire peut être plus important si vous utilisez plusieurs conversions.

## Environnement utilisateur

Les paramètres de ce groupe configurent les environnements utilisateur.

### *number of user connections*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | user connections |
| Valeur par défaut | 25 |
| Plage de valeurs | 5–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

number of user connections définit le nombre maximum d'utilisateurs qui peuvent se connecter simultanément à Adaptive Server. Il ne se réfère pas au nombre maximum de processus, ce nombre ne dépend pas seulement de la valeur de ce paramètre mais également des autres activités du système.

Limite supérieure du paramètre *maximum number of user connections*

Le nombre maximum autorisé de descripteurs de fichier par processus dépend du système d'exploitation. Reportez-vous à la Manuel de configuration pour votre plate-forme.

Le nombre de descripteurs de fichier disponibles pour les connexions Adaptive Server est stocké dans la variable globale @@*max_connections*. Vous pouvez indiquer le nombre maximum de descripteurs de fichier utilisables par votre système avec :

```
select @@max_connections
```

La valeur renvoyée représente le nombre maximum de descripteurs de fichier autorisés par le système pour vos processus, moins l'en-tête. L'en-tête augmente avec le nombre de moteurs. Reportez-vous à la section "Gestion des connexions utilisateur", page 689 pour plus d'informations sur la manière dont le multitraitement affecte le nombre de descripteurs de fichier disponibles pour les connexions Adaptive Server.

Vous devez également réserver un certain nombre de connexions pour les éléments suivants, que vous définissez également avec des paramètres de configuration :

- Les devices de la base de données, y compris les devices miroirs
- Routines de gestion du site
- Récepteurs de réseau

La formule suivante détermine la valeur maximale que vous pouvez attribuer à number of user connections, number of devices, max online engines, number of remote sites et max number network listeners :

number of user connections + (number of devices * max online engines * 2) + number of remote sites + max number network listeners ne peut pas être supérieur à la valeur de @@*max_connections*.

Optimisation de la valeur du paramètre *max number of user connections*

Il n'existe pas de formule permettant de déterminer le nombre de connexions autorisées pour chaque utilisateur. Vous devez estimer ce nombre en vous basant sur les contraintes système et utilisateur décrites ici. Vous devez également tenir compte du fait que la probabilité d'un partage occasionnel ou temporaire des connexions entre les utilisateurs est plus élevée sur un système qui compte de nombreux utilisateurs. Les processus suivants ont besoin de connexions utilisateur :

- Une connexion est nécessaire pour chaque utilisateur qui exécute isql.
- Les développeurs d'application utilisent une connexion pour chaque session d'édition.

- Le nombre de connexions requises par les utilisateurs qui exécutent une application dépend de la manière dont l'application a été programmée. Les utilisateurs qui exécutent des programmes Open Client ont besoin d'une connexion par DB-Lib dbprocess ou Client-Library cs_connection ouverte.

---

**Remarque** Il est conseillé d'estimer le nombre maximum de connexions qui seront utilisées par Adaptive Server et de mettre à jour number of user connections lorsque vous ajoutez des devices physiques ou des utilisateurs au système. Utilisez régulièrement sp_who pour déterminer le nombre d'utilisateurs actifs sur votre Adaptive Server.

---

Certains autres paramètres de configuration, dont stack size et default network packet size, affectent l'espace mémoire requis pour chaque connexion utilisateur.

### Connexions utilisateur pour la mémoire partagée

Adaptive Server utilise la valeur du paramètre number of user connections afin d'établir le nombre de connexions de mémoire partagée pour EJB Server. Par conséquent, si number of user connections est 30, Adaptive Server établit 10 connexions de mémoire partagée pour EJB Server. Les connexions de mémoire partagée ne représentent pas un sous-ensemble de connexions utilisateur et ne sont pas soustraites du nombre de connexions utilisateur.

Pour augmenter le nombre de connexions utilisateur pour la mémoire partagée, vous devez :

1 Augmenter la valeur de number of user connections à un chiffre dont le tiers est égal au nombre souhaité de connexions de mémoire partagée.

2 Redémarrer Adaptive Server.

Bien que number of user connections soit un paramètre dynamique, vous devez redémarrer le serveur pour modifier le nombre de connexions utilisateur pour la mémoire partagée. Reportez-vous au document *Guide de l'utilisateur EJB Server* pour plus d'informations.

### *permission cache entries*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cfgcprot |
| Valeur par défaut | 15 |
| Plage de valeurs | 1–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

permission cache entries détermine le nombre de protecteurs de cache par tâche. Ce paramètre augmente l'espace mémoire pour chaque connexion utilisateur et processus de travail.

Les informations sur les autorisations utilisateur sont conservées dans le cache des autorisations. Lorsqu'Adaptive Server contrôle les autorisations, il consulte tout d'abord le cache des autorisations. S'il ne trouve pas ce dont il a besoin, il cherche dans la table sysprotects. Cette opération est nettement plus rapide si Adaptive Server trouve les informations dont il a besoin dans le cache des autorisations et n'est pas obligé de consulter la table sysprotects.

Adaptive Server ne consulte cependant le cache des autorisations que lorsqu'il contrôle des autorisations utilisateur, pas lors de l'octroi ou de l'annulation des autorisations. Tout le cache des autorisations est vidé lorsqu'une autorisation est accordée ou annulée. Cela est lié au fait que les autorisations existantes possèdent des estampilles qui deviennent périmées lorsque de nouvelles autorisations sont accordées ou annulées.

Si les utilisateurs d'Adaptive Server effectuent fréquemment des opérations qui demandent un contrôle de leurs autorisations, vous pourrez constater un léger gain de performances en augmentant la valeur de permission cache entries. Cet effet ne devrait pas être suffisamment significatif pour garantir une optimisation notable.

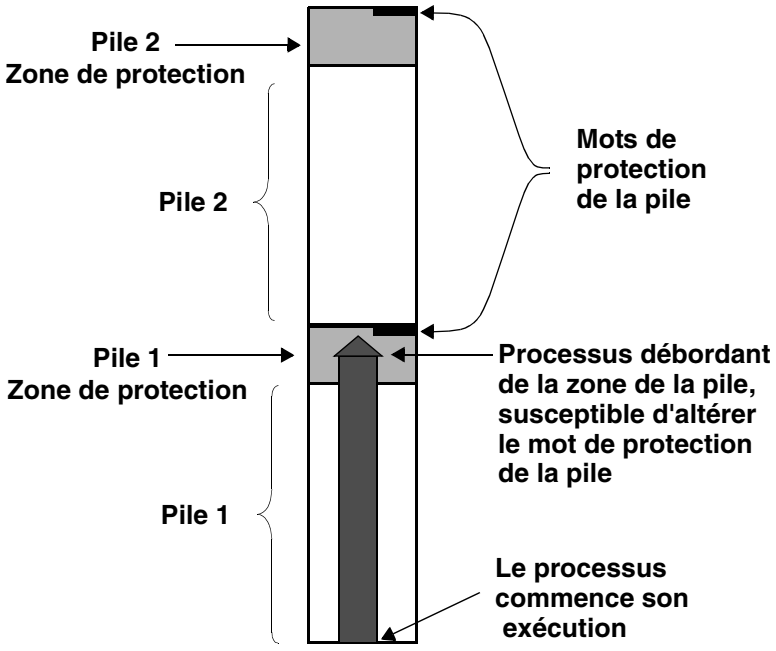
Si les utilisateurs d'Adaptive Server accordent ou annulent fréquemment des autorisations, n'attribuez pas une valeur trop élevée à permission cache entries. L'espace utilisé pour le cache des autorisations serait occupé inutilement, car celui-ci est vidé à chaque commande grant et revoke.

### *stack guard size*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | cguardsz |
| Valeur par défaut | 4096 |
| Plage de valeurs | 0–2147483647 |
| Etat | Statique |
| Niveau d'affichage | Comprehensive |
| Rôle requis | Administrateur système |

stack guard size définit la taille (en octets) de la zone de protection de la pile. La *zone de protection de la pile* est une pile de débordement de taille configurable qui se trouve à la fin de chaque pile. Adaptive Server alloue une pile pour chaque connexion utilisateur et processus de travail lors du démarrage. Ces piles sont contiguës dans la même zone de la mémoire et une zone de protection se trouve à la fin de chaque pile. La fin de chaque zone de protection de pile comporte un *mot de protection*, lequel est une structure de 4 octets ayant un modèle connu. La figure 5-7 illustre comment un processus peut altérer un mot de protection d'une pile.

***Figure 5-7 : Processus susceptibles d'altérer le mot de protection de la pile***



Adaptive Server vérifie périodiquement si le pointeur de pile d'une connexion utilisateur a pénétré dans la zone de protection de pile associée à la pile de cette connexion utilisateur. Si c'est le cas, Adaptive Server annule la transaction, renvoie la commande à l'application qui a généré la transaction et produit une erreur 3626 :

```
The transaction was aborted because it used too much
stack space.  Either use sp_configure to increase the
stack size, or break the query into smaller pieces.
spid: %d, suid: %d, hostname: %.*s, application
name: %.*s
```

Adaptive Server vérifie aussi régulièrement si le modèle du mot de protection a changé, ce qui indiquerait qu'un processus a débordé la limite de la pile. Si cela se produit, Adaptive Server imprime ces messages sur le journal d'erreurs et s'arrête :

```
kernel: *** Stack overflow detected: limit: 0x%lx sp: 0x%lx
kernel: *** Stack Guardword corrupted
kernel: *** Stack corrupted, server aborting
```

Dans le premier message, "limit" est l'adresse de la fin de la zone de protection de la pile et "sp" est la valeur courante du pointeur de pile.

De plus, Adaptive Server vérifie régulièrement si le pointeur de pile est complètement en-dehors à la fois de la pile et de la zone de protection de la pile pendant le processus du pointeur. Le cas échéant, Adaptive Server s'arrête même si le mot de protection n'est pas altéré. Si cela se produit, Adaptive Server imprime les messages suivants sur le journal d'erreurs :

```
kernel: *** Stack overflow detected: limit: 0x%lx sp: 0x%lx
kernel: *** Stack corrupted, server aborting
```

La valeur par défaut de stack guard size convient à la majorité des applications. Toutefois, si vous rencontrez des arrêts du serveur en raison d'une altération du mot de protection ou d'un débordement de la pile, augmentez stack guard size par incréments de 2 Ko. *Chaque* connexion utilisateur et processus utilisateur configuré(e) possède une zone de protection de la pile. Lorsque vous augmentez la valeur de stack guard size, vous utilisez l'espace mémoire correspondant multiplié par le nombre de connexions utilisateur et de processus de travail que vous avez configurés.

Plutôt que d'augmenter stack guard size dans le but d'éviter des problèmes de débordement de la pile, essayez d'augmenter stack size (voir "stack size", page 251). La zone de protection de la pile est conçue comme une zone de débordement et non pas comme une extension de la pile normale.

Adaptive Server alloue de l'espace de pile pour chaque tâche en additionnant les valeurs des paramètres stack size et stack guard size. La valeur de stack guard size doit être un multiple de 2 Ko. Si la valeur indiquée n'est pas un multiple de 2 Ko, les routines de vérification de sp_configure arrondissent la valeur au multiple immédiatement supérieur.

### *stack size*

| Récapitulatif | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | stack size |
| Valeur par défaut | Spécifique à la plate-forme |
| Plage de valeurs | Minimum spécifique à la plate-forme –2 147 483 647 |
| Etat | Statique |
| Niveau d'affichage | Basic |
| Rôle requis | Administrateur système |

stack size spécifie la taille (en octets) des piles d'exécution utilisées par chaque processus utilisateur sur Adaptive Server. Pour trouver les valeurs du paramètre stack size pour votre plate-forme, utilisez sp_helpconfig ou sp_configure. La valeur de stack size doit être un multiple de 2 Ko. Si la valeur indiquée n'est pas un multiple de 2 Ko, les routines de vérification de sp_configure arrondissent la valeur au multiple immédiatement supérieur.

Une *pile d'exécution* est une zone de la mémoire Adaptive Server dans laquelle les processus utilisateur gardent un suivi de leur contexte et stockent les données locales.

Certaines requêtes peuvent augmenter la probabilité de débordement de la pile. Il s'agit, par exemple, de requêtes contenant des clauses where extrêmement longues, des listes de sélection longues, de procédures stockées profondément imbriquées ainsi que de sélections et de mises à jour multiples à l'aide de holdlock. Lorsqu'un débordement de la pile se produit, Adaptive Server imprime un message d'erreur et annule la transaction. Reportez-vous à la section "stack guard size", page 249 pour plus d'informations sur les débordements de la pile. Reportez-vous au *Guide de dépannage et des messages d'erreur* pour plus d'informations sur les messages d'erreur spécifiques.

Pour résoudre le problème du débordement de la pile, il faut diviser les requêtes importantes en requêtes plus petites ou augmenter la valeur de stack size. Le fait de modifier stack size affecte l'espace mémoire requis pour *chaque* connexion utilisateur et processus de travail configuré(e). Pour plus d'informations, reportez-vous à la section "total logical memory", page 188.

Si certaines de vos requêtes dépassent la taille de la pile d'exécution, vous pouvez les ré-écrire sous la forme de séries de requêtes plus courtes. C'est notamment le cas si vous n'avez que peu de requêtes de ce type ou si vous les exécutez peu fréquemment.

Il n'existe aucun moyen de déterminer l'espace de la pile qui sera occupé par une requête avant d'exécuter celle-ci réellement. L'espace de pile pour chaque connexion utilisateur et processus de travail est alloué au démarrage.

La détermination de la valeur appropriée pour stack size est donc une opération empirique. Il est recommandé de tester vos requêtes les plus longues et les plus complexes en utilisant la valeur par défaut de stack size. Celle-ci est certainement suffisante si elles sont exécutées sans générer de messages d'erreur. Si des messages sont produits, commencez par augmenter stack size d'une valeur faible (2 Ko). Exécutez de nouveau vos requêtes et vérifiez si la valeur ajoutée est suffisante. Dans le cas contraire, continuez à augmenter stack size jusqu'à ce que vos requêtes soient exécutées sans produire de messages d'erreur.

Si vous utilisez CIS ou si Java est activé dans la base de données et que vous voulez utiliser des méthodes qui appellent JDBC, Sybase vous recommande d'augmenter la valeur par défaut de 50 %. La valeur par défaut devrait être suffisante si vous n'utilisez pas JDBC ou CIS.

### *user log cache size*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | Taille de page logique |
| Plage de valeurs | 2048[a]–2 147 483 647<br>a. Minimum déterminé par la taille de page logique du serveur |
| Etat | Statique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

user log cache size spécifie la taille (en octets) de chaque cache de journaux utilisateur. Cette taille est déterminée par la taille de la page logique du serveur. Il y a un cache de journaux utilisateur pour chaque connexion utilisateur et processus de travail configuré. Adaptive Server utilise ces caches pour mettre en buffer les enregistrement dans le journal des transactions utilisateur afin de réduire les conflits à la fin du journal des transactions.

Lorsqu'un cache utilisateur est plein ou qu'un autre événement se produit (par exemple lorsque la transaction est terminée), Adaptive Server "vide" tous les enregistrements de journal du cache des journaux utilisateur vers le journal des transactions de la base de données. En commençant par consolider les enregistrement de journal dans chaque cache des journaux utilisateur plutôt que d'ajouter immédiatement chaque enregistrement au journal des transaction de la base de données, Adaptive Server réduit les conflits entre les processus qui écrivent dans le journal, notamment pour les systèmes SMP configurés avec plusieurs moteurs.

---

**Remarque** Pour les transactions qui utilisent une base de données contenant à la fois des segments de données et de journal, le cache des journaux utilisateur est vidé vers le journal des transactions après chaque enregistrement de journal. Aucune mise en buffer n'est effectuée. Il est recommandé d'augmenter la taille du cache des journaux utilisateur si vos bases de données ne possèdent pas de segments de journal dédiés.

---

N'attribuez pas à user log cache size une valeur supérieure au volume maximum d'informations de journal écrites par la transaction d'une application. Comme Adaptive Server vide le cache des journaux utilisateur lorsque la transaction se termine, la mémoire supplémentaire allouée au cache des journaux utilisateur est occupée inutilement. Si aucune transaction sur votre serveur ne génère plus de 4000 octets d'enregistrements du journal des transactions, ne donnez pas à user log cache size une valeur supérieure à celle-ci. Exemple :

```
sp_configure "user log cache size", 4000
```

Une valeur excessive de user log cache size occupe inutilement de la mémoire. Si cette valeur est trop faible, le cache des journaux utilisateur risque de se remplir et de se vider plusieurs fois par transaction, ce qui augmente le risque de conflits pour le journal des transactions. Si le volume des transactions est faible, le taux de conflits pour le journal des transactions peut être négligeable.

Utilisez sp_sysmon pour comprendre comment ce paramètre affecte le fonctionnement du cache. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

### *user log cache spinlock ratio*

| **Récapitulatif** | |
|---|---|
| Nom dans les versions antérieures à la version 11.0 | N/A |
| Valeur par défaut | 20 |
| Plage de valeurs | 1–2147483647 |
| Etat | Dynamique |
| Niveau d'affichage | Intermediate |
| Rôle requis | Administrateur système |

Si Adaptive Server est exécuté avec plusieurs moteurs, le paramètre user log cache spinlock ratio définit la proportion de caches de journaux utilisateur par **spinlock** de cache de journaux utilisateur. Il y a un cache de journaux utilisateur pour chaque connexion utilisateur configurée.

La valeur par défaut de ce paramètre est 20, soit 1 verrou d'attente pour 20 connexions utilisateur configurées sur votre serveur.

Utilisez sp_sysmon pour comprendre comment ce paramètre affecte le fonctionnement du cache. Reportez-vous au document *Performances et optimisation* pour plus d'informations.

Reportez-vous à la section "Configuration des paramètres de taux de verrous d'attente", page 691 pour plus d'informations sur la configuration des rapports des verrous d'attente.

CHAPITRE 6

# Restriction de l'accès aux ressources du serveur

Ce chapitre décrit comment utiliser les limites d'utilisation des ressources pour restreindre le coût des E/S, le nombre de lignes ou le temps de traitement utilisé par un login ou une application dans des moments critiques. Il décrit également la création d'intervalles de temps nommés permettant de spécifier des blocs de temps contigus pour les limites d'utilisation des ressources.

Les sujets traités dans ce chapitre sont les suivants :



## Présentation des limites d'utilisation des ressources

Adaptive Server fournit les limites d'utilisation des ressources pour permettre aux administrateurs système d'empêcher les requêtes et les transactions de monopoliser les ressources du serveur. Une *limite d'utilisation des ressources* est un ensemble de paramètres spécifiés par un administrateur système pour empêcher une application ou un login de :

- dépasser les coûts d'E/S estimés ou réels, déterminés par l'optimiseur ;
- renvoyer plus d'un certain nombre de lignes ;
- dépasser un temps écoulé donné.

L'ensemble de paramètres pour une limite d'utilisation des ressources inclut l'heure d'application de la limite et le type d'action à effectuer. Par exemple, vous pouvez empêcher l'exécution de rapports très volumineux aux heures de pointe ou fermer une session dont la requête génère des **produits cartésiens** non voulus.

# Planification des limites d'utilisation des ressources

Pour planifier une limite d'utilisation des ressources, tenez compte des éléments suivants :

- le moment d'application de la limite (heure et jour) ;
- les utilisateurs et applications à contrôler ;
- le type de limite à imposer ;
    - le coût d'E/S (estimé ou réel) pour des requêtes pouvant nécessiter de nombreuses lectures physiques et logiques ;
    - le nombre de lignes pour des requêtes susceptibles de renvoyer des jeux de résultats volumineux ;
    - le temps écoulé pour des requêtes dont l'exécution peut s'avérer longue en raison de leur complexité ou de facteurs externes tels que la charge du serveur.
- l'application d'une limite à des requêtes individuelles ou la définition d'une portée plus large (transaction ou batch de requête) ;
- l'application des limites de coûts d'E/S avant ou pendant l'exécution ;
- l'action à effectuer en cas de dépassement de limite (émission d'un avertissement, annulation de la transaction ou du batch de requête ou suppression de la session).

Une fois la planification effectuée, utilisez les procédures système pour effectuer les actions suivantes :

- spécifier l'heure et le jour d'application de la limite, créez un intervalle de temps nommé à l'aide de la procédure sp_add_time_range ;
- créer des limites d'utilisation des ressources à l'aide de la procédure sp_add_resource_limit ;

- obtenir des informations sur les limites d'utilisation des ressources existantes, utilisez la procédure sp_help_resource_limit ;
- modifier les intervalles de temps et les limites d'utilisation des ressources, utilisez respectivement les procédures sp_modify_time_range et sp_modify_resource_limit ;
- supprimer les intervalles de temps et les limites d'utilisation des ressources, utilisez respectivement les procédures sp_drop_time_range et sp_drop_resource_limit.

# Activation des limites d'utilisation des ressources

Configurez Adaptive Server pour activer les limites d'utilisation des ressources. Utilisez le paramètre de configuration allow resource limits, comme suit :

```
sp_configure "allow resource limits", 1
```

La valeur 1 active les limites d'utilisation des ressources, tandis que la valeur 0 les désactive. allow resource limits étant statique, vous devez donc redémarrer le serveur pour que les modifications soient prises en compte.

Le paramètre allow resource limits indique au serveur d'allouer de la mémoire interne pour les intervalles de temps, les limites d'utilisation des ressources et les alarmes de serveur internes, et affecte en interne des intervalles applicables et des limites aux sessions de login.

L'activation du paramètre allow resource limits modifie également le résultat de showplan et statistics i/o, comme suit :

- showplan affiche les informations sur le coût des E/S estimé pour les instructions DML. Les informations affichées représentent l'évaluation des coûts par l'optimiseur de la requête sous la forme d'un nombre sans unité. Le coût total des E/S estimé est affiché pour l'intégralité de la requête. Cette évaluation des coûts dépend des statistiques de la table (nombre de valeurs et répartition) et de la taille des zones de buffer appropriées. Elle dépend de facteurs comme l'état des zones de buffer et le nombre d'utilisateurs actifs. Pour plus d'informations, reportez-vous à la section "Messages décrivant les méthodes d'accès, la mise en mémoire cache et le coût des E/S", page 854 dans le document *Performances et optimisation*.

- statistics io inclut le coût total réel des E/S d'une instruction selon la formule d'évaluation des coûts de l'optimiseur. Cette valeur est un nombre représentant la somme du nombre d'E/S logiques multiplié par le coût d'une E/S logique et le nombre d'E/S physiques multiplié par le coût d'une E/S physique. Pour plus d'informations, reportez-vous au chapitre 34, "Utilisation des commandes set statistics" dans le manuel *Performances et optimisation*.

# Définition des intervalles de temps

Un *intervalle de temps* est un bloc de temps contigu au sein d'un seul jour sur un ou plusieurs jours contigus. Il est défini par ses périodes de début et de fin.

Adaptive Server inclut un intervalle de temps prédéfini, l'intervalle "at all times", qui couvre la période de minuit à minuit, du lundi au dimanche. Vous pouvez créer, modifier et supprimer les intervalles de temps, comme requis par les limites d'utilisation des ressources.

Les intervalles de temps nommés peuvent se chevaucher. Toutefois, les limites d'une combinaison utilisateur/application particulière ne peuvent pas être associées à des intervalles de temps nommés qui se chevauchent. Vous pouvez créer différentes limites qui partagent le même intervalle de temps.

Par exemple, supposons que vous limitiez le login "joe_user" pour qu'il renvoie 100 lignes lorsqu'il exécute l'application de calcul de la paie pendant les heures de travail. Ultérieurement, vous tentez de limiter l'extraction de lignes pour ce même utilisateur pendant les heures de pointe qui chevauchent les heures de travail. Vous recevrez un message indiquant l'échec de la nouvelle limite, parce qu'elle aurait chevauché une limite existante.

Bien que vous ne puissiez pas limiter l'extraction de lignes pour "joe_user" dans l'application de calcul de la paie pendant des intervalles de temps qui se chevauchent, rien ne vous empêche de placer une seconde limite sur "joe_user" pendant le même intervalle de temps que la limite d'extraction de lignes. Par exemple, vous pouvez limiter la durée d'exécution d'une de ses requêtes au même intervalle de temps que vous avez utilisé pour limiter l'extraction de lignes.

Lorsque vous créez un intervalle de temps nommé, Adaptive Server le stocke dans la table système systimeranges pour contrôler si une limite d'utilisation des ressources est active. Chaque intervalle de temps a un ID d'intervalle. L'intervalle "at all times" a l'ID d'intervalle 1. Les messages d'Adaptive Server utilisent l'ID d'intervalle pour se référer à des intervalles de temps particuliers.

## Détermination des intervalles de temps requis

Utilisez un graphique semblable à celui présenté ci-après pour déterminer les intervalles de temps à créer pour chaque serveur. Contrôlez l'utilisation du serveur sur la semaine ; puis, indiquez les périodes pendant lesquelles le serveur est très sollicité ou exécute des tâches cruciales qui ne doivent pas être interrompues.

| Day / Time | 00:00 | 01:00 | 02:00 | 03:00 | 04:00 | 05:00 | 06:00 | 07:00 | 08:00 | 09:00 | 10:00 | 11:00 | 12:00 | 13:00 | 14:00 | 15:00 | 16:00 | 17:00 | 18:00 | 19:00 | 20:00 | 21:00 | 22:00 | 23:00 | 00:00 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mon | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tues | | | | | | | | | | | | | | | | | | | | | | | | | |
| Wed | | | | | | | | | | | | | | | | | | | | | | | | | |
| Thurs | | | | | | | | | | | | | | | | | | | | | | | | | |
| Fri | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sat | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sun | | | | | | | | | | | | | | | | | | | | | | | | | |

## Création d'intervalles de temps nommés

Créez des intervalles de temps nommés à l'aide de sp_add_time_range, pour :

- nommer l'intervalle de temps ;
- spécifier les jours de début et de fin de l'intervalle de temps ;
- spécifier les heures de début et de fin de l'intervalle de temps.

Pour la syntaxe et plus d'informations, reportez-vous à sp_add_time_range dans le *Manuel de référence d'Adaptive Server*.

### Exemple d'intervalle de temps

Supposons que l'exécution de deux tâches cruciales soit planifiée chaque semaine aux heures suivantes :

- La tâche 1 s'exécute de 07 h 00 à 10 h 00 le mardi et le mercredi.
- La tâche 2 s'exécute du samedi 08 h 00 au dimanche 13 h 00.

Le tableau suivant utilise "1" pour indiquer l'exécution de la tâche 1 et "2" pour la tâche 2 :

| Day / Time | 00:00 | 01:00 | 02:00 | 03:00 | 04:00 | 05:00 | 06:00 | 07:00 | 08:00 | 09:00 | 10:00 | 11:00 | 12:00 | 13:00 | 14:00 | 15:00 | 16:00 | 17:00 | 18:00 | 19:00 | 20:00 | 21:00 | 22:00 | 23:00 | 00:00 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mon | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tues | | | | | | | | 1 | 1 | 1 | 1 | | | | | | | | | | | | | | |
| Wed | | | | | | | | 1 | 1 | 1 | 1 | | | | | | | | | | | | | | |
| Thurs | | | | | | | | | | | | | | | | | | | | | | | | | |
| Fri | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sat | | | | | | | | | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| Sun | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | | | | | | | | | | | |

La tâche 1 peut être couverte par un seul intervalle de temps, tu_wed_7_10 :

```
sp_add_time_range tu_wed_7_10, tuesday, wednesday, "7:00", "10:00"
```

La tâche 2 nécessite deux intervalles de temps distincts, pour samedi et dimanche :

```
sp_add_time_range saturday_night, saturday, saturday, "08:00", "23:59"
sp_add_time_range sunday_morning, sunday, sunday, "00:00", "13:00"
```

## Modification d'un intervalle de temps nommé

Utilisez sp_modify_time_range pour :

- spécifier l'intervalle de temps à modifier ;
- modifier les dates de début et de fin ;
- modifier les heures de début et de fin.

Pour la syntaxe et plus d'informations, reportez-vous à sp_modify_time_range dans le *Manuel de référence d'Adaptive Server*.

Par exemple, pour remplacer le jour de fin de l'intervalle de temps *heures_travail* par samedi, tout en conservant le jour de début et les heures de début et de fin existantes, entrez :

```
sp_modify_time_range business_hours, NULL, Saturday, NULL, NULL
```

Pour spécifier un nouveau jour et une nouvelle heure de fin pour l'intervalle de temps *avant_heures*, entrez :

```
sp_modify_time_range before_hours, NULL, Saturday, NULL, "08:00"
```

**Remarque** Vous ne pouvez pas modifier l'intervalle de temps "at all times".

## Suppression d'un intervalle de temps nommé

Utilisez sp_drop_time_range pour supprimer un intervalle de temps défini par l'utilisateur.

Pour la syntaxe et plus d'informations, reportez-vous à sp_modify_time_range dans le *Manuel de référence d'Adaptive Server*.

Par exemple, pour supprimer l'intervalle de temps *soirées* de la table système systimeranges dans la base de données master, entrez :

```
sp_drop_time_range evenings
```

**Remarque** Vous ne pouvez pas supprimer l'intervalle de temps "at all times" ni aucun intervalle de temps pour lequel des limites d'utilisation des ressources sont définies.

## Application des modifications des intervalles de temps

Les intervalles de temps actifs sont liés à une session de login au début de chaque batch de requête. Une modification des intervalles de temps actifs du serveur liée à un changement de temps réel n'a aucun impact sur une session durant le traitement d'un batch de requêtes. En d'autres termes, si une limite d'utilisation des ressources restreint les batchs de requête pendant un intervalle de temps donné, mais que le batch a commencé avant que l'intervalle de temps ne soit actif, le batch de requête en cours d'exécution n'est pas concerné par la limite d'utilisation des ressources. Toutefois, si vous exécutez un second batch de requête lors de la même session de login, ce batch sera modifié par le changement apporté à l'heure.

L'ajout, la modification et la suppression d'intervalles de temps n'ont pas d'incidence sur les intervalles de temps actifs pour les sessions de login en cours.

Si une limite d'utilisation des ressources a comme portée une transaction, et qu'un changement des intervalles actifs du serveur se produit alors qu'une transaction est en cours, le nouvel intervalle actif ne s'applique pas à la transaction courante.

# Identification des utilisateurs et des limites

Pour chaque limite d'utilisation des ressources, vous devez indiquer l'objet auquel elle s'applique.

Vous pouvez appliquer une limite d'utilisation des ressources à n'importe lequel des éléments suivants :

- toutes les applications utilisées par un login particulier,
- tous les logins qui utilisent une application spécifique,
- une application spécifique utilisée par un login donné.

L'*application* est définie comme un programme client qui s'exécute en haut de l'architecture d'Adaptive Server et dont l'accès se fait par le biais d'un login spécifique. Pour exécuter une application sur Adaptive Server, vous devez indiquer son nom à l'aide de la propriété de connexion CS_APPNAME en utilisant cs_config (application Open Client Client-Library) ou la fonction DBSETLAPP d'Open Client DB-Library. Pour afficher le nom des applications qui s'exécutent sur votre serveur, sélectionnez la colonne program_name dans la table master..sysprocesses.

Pour plus d'informations sur la propriété de connexion CS_APPNAME, reportez-vous au manuel *Open Client Client-Library/C Reference Manual*. Pour plus d'informations sur la fonction DBSETLAPP, reportez-vous au manuel *Open Client DB-Library/C Reference Manual*.

## Identification des utilisateurs consommant beaucoup de ressources

Avant de mettre en oeuvre les limites d'utilisation des ressources, exécutez sp_reportstats. Le résultat de cette procédure vous aidera à identifier les utilisateurs qui consomment beaucoup de ressources système. Exemple :

```
                    sp_reportstats
Name    Since         CPU     Percent CPU  I/O     Percent I/O
------  -----------   -----   ------------ -----   -------------
probe   jun 19 1993   0       0%           0       0%
julie   jun 19 1993   10000   24.9962%     5000    24.325%
jason   jun 19 1993   10002   25.0013%     5321    25.8866%
ken     jun 19 1993   10001   24.9987%     5123    24.9234%
kathy   jun 19 1993   10003   25.0038%     5111    24.865%
                         Total CPU   Total I/O
                         ---------   ---------
                         40006       20555
```

Le résultat ci-dessus indique que l'utilisation est équilibrée entre les utilisateurs. Pour plus d'informations sur le taux de charge du processeur, reportez-vous aux sections "cpu accounting flush interval", page 197 et "i/o accounting flush interval", page 211.

## Identification des applications consommant beaucoup de ressources

Pour identifier les applications qui s'exécutent sur votre système et les utilisateurs qui les lancent, exécutez une requête sur la table système sysprocesses dans la base de données master.

La requête suivante détermine que isql, payroll, perl et acctng sont les seuls programmes clients dont les noms ont été transmis à Adaptive Server :

```
select spid, cpu, physical_io,
  substring(user_name(uid),1,10) user_name,
  hostname, program_name, cmd
from sysprocesses
```

```
spid  cpu    physical_io  user_name hostname program_name cmd
----  ---    -----------  --------- -------- ------------ ------
  17    4          12748  dbo       sabrina  isql         SELECT
 424    5              0  dbo       HOWELL   isql         UPDATE
 526    0            365  joe       scotty   payroll      UPDATE
 568    1           8160  dbo       smokey   perl         SELECT
 595   10              1  dbo       froth    isql         DELETE
 646    1              0  guest     walker   isql         SELECT
 775    4          48723  joe_user  mohindra acctng       SELECT

(7 rows affected)
```

Comme la table système sysprocesses est construite de façon dynamique pour faire état des processus en cours, les requêtes répétées sur cette table produisent des résultats différents. Répétez cette requête plusieurs fois par jour pendant un certain temps pour déterminer les applications qui s'exécutent sur votre système.

Les valeurs des E/S physiques et de la CPU sont régulièrement transférées dans la table système syslogins où elles incrémentent les valeurs fournies par sp_reportstats.

Une fois que vous avez identifié les applications s'exécutant sur votre système, utilisez showplan et statistics io pour évaluer l'utilisation des ressources des requêtes dans les applications.

Si vous avez configuré Adaptive Server pour qu'il active les limites d'utilisation des ressources, vous pouvez utiliser showplan pour évaluer les ressources utilisées avant l'exécution et statistics io pour évaluer les ressources utilisées lors de l'exécution. Pour plus d'informations sur la configuration d'Adaptive Server pour activer les limites d'utilisation des ressources, reportez-vous à la section "Activation des limites d'utilisation des ressources", page 257.

Outre statistics io, statistics time s'avère également utile pour évaluer les ressources consommées par une requête. Utilisez statistics time pour afficher le temps nécessaire à l'exécution de chaque phase de la requête. Pour plus d'informations, reportez-vous au chapitre 19, "Outils d'optimisation de la requête" du manuel *Performances et optimisation*.

## Choix d'un type de limite

Une fois que vous avez déterminé les utilisateurs et les applications à limiter, vous pouvez choisir trois types de limite d'utilisation des ressources.

Le tableau 6-1 décrit la fonction et la portée de chaque type de limite et indique les outils permettant de déterminer si une requête particulière peut bénéficier de ce type de limite. Dans certains cas, il peut être approprié de créer plusieurs types de limite pour un utilisateur et une application donnés. Pour plus d'informations sur les types de limite, reportez-vous à la section "Présentation des types de limite", page 268.

***Tableau 6-1 : Types de limite d'utilisation des ressources***

| Type de limite | Utilisation pour des requêtes | Evaluation de l'utilisation des ressources | Portée | Application pendant |
|---|---|---|---|---|
| io_cost | Nécessitant de nombreuses lectures logiques et physiques | Utilisez set showplan on avant d'exécuter la requête afin d'afficher le coût estimé des E/S ; utilisez set statistics io on pour connaître le coût réel des E/S. | Requête | Pré-exécution ou exécution |
| row_count | Renvoyant des jeux de résultats volumineux | Utilisez la variable globale *@@rowcount* pour déterminer les limites appropriées au nombre de lignes. | Requête | Exécution |
| elapsed_time | Dont le temps d'exécution est élevé en raison de leur complexité ou de facteurs externes tels que la charge du serveur ou l'attente d'un verrou | Utilisez set statistics time on avant d'exécuter la requête afin d'afficher le temps écoulé en millisecondes. | Batch de requête ou transaction | Exécution |

La table système spt_limit_types stocke les informations sur chaque type de limite.

## Détermination du moment d'application de la limite

Le **moment d'application** est la phase de traitement de la requête pendant laquelle Adaptive Server applique une limite d'utilisation des ressources donnée. Les limites d'utilisation des ressources sont appliquées pendant les phases suivantes :

- Pré-exécution : Adaptive Server applique les limites d'utilisation des ressources avant l'exécution, en fonction de l'évaluation des coûts des E/S par l'optimiseur. Cette limite empêche l'exécution de requêtes potentiellement longues. Le coût des E/S est le seul type de ressource pouvant être limité à ce moment.

Lors de l'évaluation du coût des E/S des instructions DML (langage de manipulation de données) au sein des clauses d'une instruction conditionnelle, Adaptive Server considère chaque instruction DML individuellement. Il évalue toutes les instructions, même en cas d'exécution d'une seule clause.

Une limite d'utilisation des ressources au moment de la pré-exécution ne peut porter que sur une requête ; c'est-à-dire que les valeurs des ressources limitées au moment de la compilation sont calculées et contrôlées requête par requête uniquement.

Adaptive Server n'applique pas les limites d'utilisation des ressources au moment de la pré-exécution aux instructions d'un trigger.

- Exécution : Adaptive Server applique les limites d'utilisation des ressources au moment de l'exécution pour empêcher une requête de monopoliser les ressources du serveur (et du système d'exploitation). Il est possible que les limites appliquées au moment de l'exécution utilisent plus de ressources (temps CPU et E/S supplémentaires) que celles appliquées au moment de la pré-exécution.

## Détermination de la portée des limites d'utilisation des ressources

Le paramètre *portée* spécifie la durée d'une limite dans des instructions Transact-SQL. Les portées possibles sont la requête, le batch de requête et la transaction.

- Requête : Adaptive Server applique les limites d'utilisation des ressources à toute instruction Transact-SQL qui accède au serveur ; par exemple, select, insert et update. Lorsque vous exécutez ces instructions au sein d'un batch de requête, Adaptive Server les évalue individuellement.

  Adaptive Server considère qu'une procédure stockée est une série d'instructions DML. Il évalue la limite d'utilisation des ressources de chaque instruction au sein de la procédure stockée. Si une procédure stockée exécute une autre procédure stockée, Adaptive Server évalue chaque instruction DML au sein de la procédure stockée imbriquée au niveau de l'imbrication interne.

Adaptive Server vérifie les limites d'utilisation des ressources au moment de la pré-exécution avec la portée d'une requête, un niveau d'imbrication à la fois. Au fur et à mesure qu'Adaptive Server entre dans chaque niveau d'imbrication, il vérifie les limites d'utilisation des ressources actives par rapport à l'utilisation des ressources estimée de chaque instruction DML avant d'exécuter les instructions de ce niveau d'imbrication. Une limite d'utilisation des ressources est transgressée si l'utilisation des ressources estimée de toute requête DML à ce niveau d'imbrication dépasse la valeur d'une limite d'utilisation des ressources active. Adaptive Server effectue l'action liée à la limite d'utilisation des ressources transgressée.

Adaptive Server vérifie les limites d'utilisation des ressources au moment de l'exécution avec la portée d'une requête par rapport à l'utilisation des ressources cumulée de chaque requête DML. Une violation des limites se produit lorsque l'utilisation des ressources d'une requête dépasse la valeur d'une limite d'utilisation des ressources d'exécution. Là encore, Adaptive Server effectue l'opération liée à cette limite d'utilisation des ressources.

- Batch de requête : un batch de requête est composé d'une ou de plusieurs instructions Transact-SQL ; par exemple, dans isql, un groupe de requêtes devient un batch de requête s'il est exécuté par un seul délimiteur de fin de commande go.

  Le batch de requête commence au niveau d'imbrication 0 ; chaque appel à une procédure stockée incrémente le niveau d'imbrication de 1 (jusqu'au niveau d'imbrication maximal). Chaque renvoi d'une procédure stockée décrémente le niveau d'imbrication de 1.

  Seules les limites d'utilisation des ressources appliquées au moment de l'exécution peuvent porter sur un batch de requête.

  Adaptive Server vérifie les limites d'utilisation des ressources au moment de l'exécution avec la portée d'un batch de requête par rapport à l'utilisation des ressources cumulée des instructions de chaque batch de requête. Une limite est transgressée si l'utilisation des ressources d'un batch de requête dépasse la valeur d'une limite d'utilisation des ressources active au moment de l'exécution. Adaptive Server effectue l'action liée à cette limite d'utilisation des ressources.

- Transaction : Adaptive Server applique les limites avec une portée de transaction à tous les niveaux d'imbrication lors de la transaction par rapport à l'utilisation des ressources cumulée pour la transaction.

Une limite est transgressée si l'utilisation des ressources de la transaction dépasse la valeur d'une limite d'utilisation des ressources active au moment de l'exécution. Adaptive Server effectue l'action liée à cette limite d'utilisation des ressources.

Seules les limites d'utilisation des ressources appliquées au moment de l'exécution peuvent porter sur une transaction.

Adaptive Server ne reconnaît pas les transactions imbriquées lors de l'application des limites d'utilisation des ressources. Une limite d'utilisation des ressources portant sur une transaction commence lorsque la variable globale @@*trancount* prend la valeur 1 et finit quand @@*trancount* prend la valeur 0.

# Présentation des types de limite

Il existe trois types de limite d'utilisation des ressources qui permettent de restreindre l'utilisation des ressources de différentes façons.

## Restriction du coût des E/S

Le coût des E/S est fondé sur le nombre d'accès logiques et physiques ("lectures") utilisés pendant le traitement des requêtes. Pour déterminer le plan de traitement le plus efficace avant l'exécution, l'optimiseur d'Adaptive Server utilise les ressources physiques et logiques pour évaluer le coût des E/S.

Adaptive Server utilise le résultat de la formule d'évaluation des coûts de l'optimiseur comme un nombre "sans unité" ; c'est-à-dire qu'une valeur ne repose pas nécessairement sur une seule unité de mesure (telle que les secondes ou les millisecondes).

Pour définir les limites d'utilisation des ressources, vous devez comprendre comment ces limites se traduisent en overhead système au moment de l'exécution. Par exemple, vous devez savoir quelle est l'incidence d'une requête ayant un coût de *x* E/S logiques et de *y* E/S physiques sur un serveur de production.

La restriction de io_cost peut contrôler les requêtes qui consomment beaucoup d'E/S, notamment les requêtes qui renvoient un jeu de résultats volumineux. Toutefois, si vous exécutez une requête simple qui renvoie toutes les lignes d'une table volumineuse et que vous ne disposez pas de statistiques courantes sur la taille de la table, il est possible que l'optimiseur ne puisse pas estimer que la requête dépassera la limite d'utilisation des ressources io_cost. Pour empêcher les requêtes de renvoyer des jeux de résultats volumineux, créez une limite d'utilisation des ressources portant sur row_count.

Il est probable que le suivi des limites de coût des E/S soit moins précis pour les tables partitionnées que pour les tables non partitionnées si Adaptive Server est configuré pour le traitement des requêtes parallèles. Pour plus d'informations sur l'utilisation des limites d'utilisation des ressources dans les requêtes parallèles, reportez-vous au manuel *Performances et optimisation*.

## Identification des coûts des E/S

Pour définir les limites appropriées pour le coût des E/S, déterminez le nombre de lectures logiques et physiques requises par certaines requêtes types. Utilisez les commandes set suivantes :

- set showplan on affiche l'évaluation des coûts par l'optimiseur. Utilisez ces informations pour définir les limites d'utilisation des ressources au moment de la pré-exécution. Ces limites sont transgressées lorsque l'évaluation des coûts par l'optimiseur pour une requête dépasse la valeur limite. De telles limites empêchent l'exécution de requêtes potentiellement longues.
- set statistics io on affiche le nombre réel de lectures logiques et physiques requises. Utilisez ces informations pour définir les limites d'utilisation des ressources au moment de l'exécution. Ces limites sont transgressées lorsque le coût réel des E/S pour une requête dépasse la valeur limite.

Les statistiques de coût réel des E/S incluent uniquement le coût des accès pour les tables de travail et les tables utilisateur concernées par la requête. Il est possible qu'Adaptive Server utilise d'autres tables en interne ; par exemple, il accède à la table sysmessages pour afficher les statistiques. Par conséquent, il peut exister des cas dans lesquels une requête dépasse ses limites de coût réel des E/S, même si les statistiques indiquent le contraire.

Lors de l'évaluation du coût d'une requête, l'optimiseur suppose que chaque page qu'il considère comme requise nécessitera une E/S physique pour le premier accès et se trouvera dans le cache pour des accès répétés. Il est possible que le coût réel des E/S soit différent du coût estimé par l'optimiseur, pour plusieurs raisons.

Le coût estimé sera supérieur au coût réel si certaines pages se trouvent déjà dans le cache ou si les statistiques sont incorrectes. Le coût estimé peut être inférieur au coût réel si l'optimiseur choisit des E/S de 16 Ko et si certaines pages se trouvent dans des zones de cache de 2 Ko qui nécessitent de nombreuses E/S de 2 Ko. En outre, si une jointure large force le cache à vider ses pages sur le disque, les accès répétés peuvent nécessiter des E/S physiques répétées.

L'évaluation de l'optimiseur ne sera pas précise si les statistiques de répartition ou de densité sont obsolètes ou inutilisables.

## Calcul du coût des E/S d'un curseur

Le coût estimé pour le traitement d'un curseur est calculé au moment de declare cursor pour tous les curseurs à l'exception du curseur d'exécution. Le coût estimé d'un curseur d'exécution est calculé à l'ouverture du curseur.

Les limites d'utilisation des ressources au moment de la pré-exécution portant sur le coût des E/S sont appliquées au moment de l'exécution de l'instruction open *nom_curseur* pour tous les types de curseur. L'optimiseur recalcule la valeur limite chaque fois que l'utilisateur tente d'ouvrir le curseur.

Une limite d'utilisation des ressources au moment de l'exécution s'applique au coût cumulé des E/S d'un curseur, de l'ouverture du curseur à sa fermeture. L'optimiseur recalcule la limite des E/S à chaque fois que le curseur est ouvert.

Pour plus d'informations sur les curseurs, reportez-vous au chapitre 17, "Curseurs : Accès aux données ligne par ligne", dans le *Guide de l'utilisateur Transact-SQL*.

### Portée du type de limite *io_cost*

Une limite d'utilisation des ressources qui restreint le coût des E/S porte uniquement sur les requêtes simples. Si vous lancez plusieurs instructions dans un batch de requête, Adaptive Server évalue l'utilisation des E/S pour chaque requête. Pour plus d'informations, reportez-vous à la section "Détermination de la portée des limites d'utilisation des ressources", page 266.

## Restriction du temps écoulé

Le temps écoulé correspond au nombre de secondes requises pour exécuter un batch de requête ou une transaction. Il est déterminé par des facteurs tels que la complexité de la requête, la charge du serveur et l'attente de verrous.

Utilisez les informations collectées à l'aide de set statistics time pour définir les limites appropriées au temps écoulé. Vous ne pouvez limiter la ressource de temps écoulé qu'au moment de l'exécution.

A l'aide de set statistics time activé, exécutez des requêtes types pour déterminer le temps de traitement en millisecondes. N'oubliez pas de convertir les millisecondes en secondes lorsque vous créez la limite d'utilisation des ressources.

Les limites d'utilisation des ressources portant sur le temps écoulé sont appliquées à toutes les instructions SQL dans la portée de la limite (batch de requête ou transaction), et pas seulement aux instructions DML. Une limite d'utilisation des ressources est transgressée si le temps écoulé pour la portée donnée dépasse la valeur limite.

Comme le temps écoulé ne peut être limité qu'au moment de l'exécution, une requête individuelle poursuivra son exécution, même si son temps écoulé dépasse la limite. Si plusieurs instructions figurent dans un batch, une limite de temps écoulé prend effet après qu'une instruction transgresse la limite et avant que l'instruction suivante ne soit exécutée. S'il n'existe qu'une seule instruction dans un batch, la définition d'une limite de temps écoulé n'a pas d'incidence.

Les limites de temps écoulé séparées ne sont pas appliquées aux procédures stockées ni aux transactions imbriquées. Autrement dit, si une transaction est imbriquée dans une autre, la limite de temps écoulé s'applique à la transaction externe, qui englobe le temps écoulé de la transaction interne. Par conséquent, si vous comptez le temps d'exécution d'une transaction, ce temps comprend l'ensemble des transactions imbriquées.

### Portée du type de limite *elapsed_time*

La portée d'une limite d'utilisation des ressources qui restreint le temps écoulé est un batch de requête ou une transaction. Vous ne pouvez pas limiter le temps écoulé d'une requête simple. Pour plus d'informations, reportez-vous à la section "Détermination de la portée des limites d'utilisation des ressources", page 266.

## Restriction de la taille du jeu de résultats

Le type de limite row_count restreint le nombre de lignes renvoyées à l'utilisateur. Une transgression se produit si le nombre de lignes renvoyées par une instruction select dépasse la valeur limite.

Si la limite d'utilisation des ressources émet un avertissement et qu'une requête dépasse la limite de ligne, la totalité des lignes est renvoyée, suivie d'un message d'avertissement indiquant la valeur limite ; par exemple :

```
Row count exceeded limit of 50.
```

Si la limite d'utilisation des ressources supprime le batch de requête ou la transaction ou supprime la session et qu'une requête dépasse la limite de ligne, seul le nombre de lignes limitées est renvoyé et le batch de requête, la transaction ou la session est abandonné(e). Adaptive Server affiche un message du type suivant :

```
Row count exceeded limit of 50.
Transaction has been aborted.
```

Le type de limite row_count s'applique à l'ensemble des instructions select au moment de l'exécution. Vous ne pouvez pas limiter un nombre estimé de lignes renvoyées au moment de la pré-exécution.

### Détermination des limites de nombre de lignes

Utilisez la variable globale @@*rowcount* pour déterminer les limites appropriées au nombre de lignes. La sélection de cette variable après l'exécution d'une requête type peut vous indiquer le nombre de lignes renvoyées par la requête.

### Application des limites de nombre de lignes à un curseur

Une limite de nombre de lignes s'applique au nombre cumulé de lignes renvoyées par le biais d'un curseur, de l'ouverture du curseur à sa fermeture. L'optimiseur recalcule la limite row_count à chaque fois qu'un curseur est ouvert.

### Portée du type de limite *row_count*

Une limite d'utilisation des ressources restreignant le nombre de lignes s'applique uniquement aux requêtes simples, et non aux lignes cumulées renvoyées par un batch de requête ou une transaction. Pour plus d'informations, reportez-vous à la section "Détermination de la portée des limites d'utilisation des ressources", page 266.

## Création d'une limite d'utilisation des ressources

Créez une limite d'utilisation des ressources à l'aide de sp_add_resource_limit. Respectez la syntaxe suivante :

```
sp_add_resource_limit nom, nom_app, nom_intervalle,
valeur_limite, application, action, portée
```

Utilisez les paramètres de cette procédure système pour :

- Spécifier le nom de l'utilisateur ou de l'application à laquelle s'applique la limite d'utilisation des ressources.

  Vous devez indiquer un *nom* ou un *nom_app* ou les deux. Si vous spécifiez un utilisateur, son nom doit exister dans la table syslogins. Spécifiez "null" pour créer une limite qui s'applique à l'ensemble des utilisateurs ou des applications.

- Indiquer l'intervalle de temps.

L'intervalle de temps doit déjà exister lorsque vous créez la limite. Pour plus d'informations, reportez-vous à la section "Définition des intervalles de temps", page 258.

- Spécifier le type de limite (io_cost, row_count ou elapsed_time) et définir une valeur appropriée au type de limite.

  Pour plus d'informations, reportez-vous à la section "Choix d'un type de limite", page 265.

- Indiquer si la limite d'utilisation des ressources doit être appliquée avant ou pendant l'exécution de la requête.

  Spécifiez des valeurs numériques pour ce paramètre. Les limites d'utilisation des ressources au moment de la pré-exécution, qui sont définies comme 1, ne sont correctes que pour la limite io_cost. Les limites d'utilisation des ressources au moment de l'exécution, qui sont définies comme 2, sont correctes pour les trois types de limite. Pour plus d'informations, reportez-vous à la section "Détermination du moment d'application de la limite", page 266.

- Spécifier l'action à entreprendre (émission d'un avertissement, abandon du batch de requête ou de la transaction ou suppression de la session).

  Spécifiez des valeurs numériques pour ce paramètre.

- Spécifier la portée (requête, batch de requête ou transaction).

  Spécifiez des valeurs numériques pour ce paramètre. Pour plus d'informations, reportez-vous à la section "Détermination de la portée des limites d'utilisation des ressources", page 266.

Pour plus d'informations, reportez-vous à sp_add_resource_limit dans le *Manuel de référence d'Adaptive Server*.

## Exemples de limites d'utilisation des ressources

Cette section fournit trois exemples de définition de limite d'utilisation des ressources.

### Exemple 1

```
sp_add_resource_limit NULL, payroll, tu_wed_7_10,
elapsed_time, 120, 2, 1, 2
```

Cet exemple crée une limite d'utilisation des ressources qui s'applique à tous les utilisateurs de l'application payroll car la valeur du paramètre nom est NULL. La limite est correcte pendant l'intervalle de temps tu_wed_7_10. Le type de limite, elapsed_time, a la valeur de 120 secondes. Comme elapsed_time n'est appliqué qu'au moment de l'exécution, le paramètre *application* prend la valeur 2. Le paramètre *action* prend la valeur 1, qui émet un avertissement. La *portée* de la limite prend la valeur 2, batch de requête, par le dernier paramètre. Par conséquent, si le temps écoulé du batch de requête dépasse 120 secondes d'exécution, Adaptive Server émet un avertissement.

### Exemple 2

```
sp_add_resource_limit joe_user, NULL,
saturday_night, row_count, 5000, 2, 3, 1
```

Cet exemple crée une limite d'utilisation des ressources qui s'applique à toutes les requêtes et applications exécutées par "joe_user" lors de l'intervalle de temps saturday_night. Si une requête (*portée* = 1) renvoie plus de 5000 lignes, Adaptive Server supprime la transaction (*action* = 3). Cette limite d'utilisation des ressources est appliquée au moment de l'exécution (*application* = 2).

### Exemple 3

```
sp_add_resource_limit joe_user, NULL, "at all
times", io_cost, 650, 1, 3, 1
```

Cet exemple crée aussi une limite d'utilisation des ressources qui s'applique à toutes les requêtes et applications exécutées par "joe_user". Toutefois, cette limite spécifie l'intervalle de temps par défaut, "at all times". Quand l'optimiseur estime que la valeur io_cost de la requête (*portée* = 1) dépasserait la valeur spécifiée de 650, Adaptive Server supprime la transaction (*action* = 3). Cette limite d'utilisation des ressources est appliquée au moment de la pré-exécution (*application* = 1).

## Informations sur les limites existantes

Utilisez la procédure système sp_help_resource_limit pour obtenir des informations sur les limites d'utilisation des ressources existantes.

Les utilisateurs qui ne disposent pas d'un rôle d'administrateur système peuvent utiliser la procédure sp_help_resource_limit pour afficher leurs propres limites d'utilisation des ressources (uniquement).

Les utilisateurs spécifient leurs propres noms de login comme paramètre ou définissent le paramètre nom sur la valeur "null". Les deux procédures suivantes renvoient toutes les limites d'utilisation des ressources pour l'utilisateur "joe_user" lorsqu'elles sont exécutées par joe_user :

```
sp_help_resource_limit
```

ou

```
sp_help_resource_limit joe_user
```

Les administrateurs système peuvent utiliser la procédure sp_help_resource_limit pour obtenir les informations suivantes :

- Toutes les limites telles qu'elles sont stockées dans sysresourcelimits (tous les paramètres sont NULL). Exemple :

  ```
  sp_help_resource_limit
  ```

- Toutes les limites pour un login donné (*nom* n'est pas NULL, tous les autres paramètres sont NULL). Exemple :

  ```
  sp_help_resource_limit joe_user
  ```

- Toutes les limites pour une application donnée (app_name ne prend pas la valeur NULL ; tous les autres paramètres sont NULL). Exemple :

  ```
  sp_help_resource_limit NULL, payroll
  ```

- Toutes les limites effectives à une heure ou un jour donn(é) (*heure_limite* ou *jour_limite* ne prend pas la valeur NULL ; tous les autres paramètres prennent la valeur NULL). Exemple :

  ```
  sp_help_resource_limit @limitday = wednesday
  ```

- La limite, le cas échéant, effective à une heure donnée pour un login donné (*nom* ne prend pas la valeur NULL, *heure_limite* ou *jour_limite* ne prend pas la valeur NULL). Exemple :

  ```
  sp_help_resource_limit joe_user, NULL, NULL,
  wednesday
  ```

Pour plus d'informations, reportez-vous à sp_help_resource_limit dans le *Manuel de référence d'Adaptive Server*.

## Affichage de toutes les limites d'utilisation des ressources existantes

Si vous utilisez la procédure sp_help_resource_limit sans spécifier de paramètre, Adaptive Server répertorie toutes les limites d'utilisation des ressources du serveur. Exemple :

```
                    sp_help_resource_limit
name     appname rangename rangeid limitid limitvalue enforced  action scope
----     ------- --------- ------- ------- ---------- --------  ------ -----
NULL     acctng  evenings        4       2        120         2       1     2
stein    NULL    weekends        1       3       5000         2       1     1
joe_user acctng  bus_hours       5       3       2500         2       2     1
joe_user finance bus_hours       5       2        160         2       1     6
wong     NULL    mornings        2       3       2000         2       1     1
wong     acctng  bus_hours       5       1         75         1       3     1
```

Dans le résultat, la colonne rangeid affiche la valeur provenant de systimeranges.id correspondant au nom figurant dans la colonne rangename. La colonne limitvalue indique la valeur définie par la procédure sp_add_resource_limit ou sp_modify_resource_limit. Le tableau 6-2 indique la signification des valeurs figurant dans les colonnes limitid, enforced, action et scope.

***Tableau 6-2 : Valeurs de résultats de sp_help_resource_limit***

| Colonne | Signification | Valeur |
|---|---|---|
| limitid | Quel est le type de limite ? | 1 Coût des E/S<br>2 Temps écoulé<br>3 Nombre de lignes |
| application | Quand la limite est-elle appliquée ? | 1 Avant l'exécution<br>2 Pendant l'exécution<br>3 Les deux |
| action | Quelle action est prise quand la limite est atteinte ? | 1 Emission d'un avertissement<br>2 Abandon du batch de requête<br>3 Abandon de la transaction<br>4 Suppression de la session (kill) |
| scope | Quelle est la portée de la limite ? | 1 Requête<br>2 Batch de requête<br>4 Transaction<br>6 Batch de requête + transaction |

Si un administrateur système spécifie un nom de login lors de l'exécution de la procédure sp_help_resource_limit, Adaptive Server répertorie toutes les limites d'utilisation des ressources pour ce login. Non seulement le résultat affiche les limites d'utilisation des ressources spécifiques de l'utilisateur nommé, mais aussi toutes les limites appartenant à tous les utilisateurs des applications spécifiées, parce que l'utilisateur nommé est inclus dans tous les utilisateurs.

Par exemple, le résultat suivant indique toutes les limites d'utilisation des ressources s'appliquant à un utilisateur nommé "joe_user". Comme une limite est définie pour l'ensemble des utilisateurs de l'application acctng, cette limite est comprise dans le résultat.

```
                    sp_help_resource_limit joe_user
name      appname rangename rangeid limitid limitvalue enforced  action scope
----      ------- --------- ------- ------- ---------- --------  ------ -----
NULL      acctng  evenings        4       2        120         2       1     2
joe_user acctng  bus_hours       5       3       2500         2       2     1
joe_user finance bus_hours       5       2        160         2       1     6
```

# Modification des limites d'utilisation des ressources

Utilisez sp_modify_resource_limit pour spécifier une nouvelle valeur de limite ou une nouvelle action à prendre, ou les deux, en cas de dépassement de la limite. Vous ne pouvez pas modifier le login ni l'application auxquels s'applique une limite, ni spécifier un nouvel intervalle de temps, type de limite, moment d'application ou portée.

La syntaxe de la procédure sp_modify_resource_limit est la suivante :

> sp_modify_resource_limit *nom*, *nom_app*, *nom_intervalle*, *type_limite*, *valeur_limite*, *application*, *action*, *portée*

Pour modifier une limite d'utilisation des ressources, spécifiez les valeurs suivantes :

- Vous devez spécifier une valeur non NULL pour *nom* ou *nom_app*.
  - Pour modifier une limite qui s'applique à tous les utilisateurs d'une application particulière, spécifiez une valeur NULL pour *nom*.
  - Pour modifier une limite s'appliquant à toutes les applications utilisées par *nom*, donnez la valeur "null" à *nom_app*.

    - Pour modifier une limite sur une application particulière, spécifiez le nom de l'application que le programme client transmet à Adaptive Server dans le paquet de connexion.
- Vous devez indiquer des valeurs autres que null pour *nom_intervalle* et *type_limite*. S'il est nécessaire d'identifier de manière unique la limite, indiquez des valeurs autres que null *action* et *portée*.
- Si vous donnez à *valeur_limite* ou à *action* la valeur "null", vous indiquez que cette valeur ne varie pas.

Pour plus d'informations, reportez-vous à sp_modify_resource_limit dans le *Manuel de référence d'Adaptive Server*.

## Exemples de modification d'une limite d'utilisation des ressources

```
sp_modify_resource_limit NULL, payroll,
tu_wed_7_10, elapsed_time, 90, null, null, 2
```

Cet exemple change la valeur de la limite d'utilisation des ressources qui restreint le temps écoulé pour tous les utilisateurs de l'application *paie* pendant l'intervalle de temps tu_wed_7_10. La valeur limite pour le temps écoulé passe à 90 secondes (au lieu de 120 secondes). Les valeurs relatives au moment de l'exécution, à l'action et à la portée demeurent inchangées.

```
sp_modify_resource_limit joe_user, NULL,
saturday_night, row_count, NULL, NULL, 2, NULL
```

Cet exemple modifie l'action prise par la limite d'utilisation des ressources qui restreint le nombre de lignes de toutes les requêtes et applications ad hoc exécutées par "joe_user" pendant l'intervalle de temps saturday_night. La précédente valeur pour l'action était 3, qui supprime la transaction si une requête dépasse le nombre de lignes spécifié. La nouvelle valeur, définie à 2, supprime le batch de requête. Les valeurs relatives au type de limite, au moment de l'exécution et à la portée demeurent inchangées.

# Suppression des limites d'utilisation des ressources

Utilisez sp_drop_resource_limit pour supprimer une limite d'utilisation des ressources d'un Adaptive Server.

Respectez la syntaxe suivante :

sp_drop_resource_limit {*nom* , *nom_app* } [, *nom_intervalle*, *type_limite*, *application*, *action*, *portée*]

Pour supprimer une limite d'utilisation des ressources, spécifiez suffisamment d'informations pour identifier la limite de façon unique. Vous devez spécifier une valeur autre que null pour *nom* ou *nom_app*. En outre, spécifiez les valeurs en fonction de celles figurant dans le tableau 6-3.

***Tableau 6-3 : Identification des limites d'utilisation des ressources à supprimer***

| Paramètre | Valeur spécifiée | Conséquence |
|---|---|---|
| *nom* | • Login spécifié<br>• NULL | Supprime les limites s'appliquant à un login particulier.<br>Supprime les limites s'appliquant à tous les utilisateurs d'une application particulière. |
| *nom_app* | • Application spécifiée<br>• NULL | Supprime les limites s'appliquant à une application particulière.<br>Supprime les limites s'appliquant à toutes les applications utilisées par le login spécifié. |
| *intervalle_temps* | • Un intervalle de temps existant stocké dans la table système systimeranges<br>• NULL | Supprime les limites s'appliquant à un intervalle de temps particulier.<br>Supprime toutes les limites d'utilisation des ressources pour le paramètre *nom*, *nom_app*, *type* spécifié, le moment d'application, le paramètre *action* et *portée*, sans considération du paramètre *nom_intervalle*. |
| *type_limite* | • Un des trois types de limite suivants : row_count, elapsed_time, io_cost<br>• NULL | Supprime les limites s'appliquant à un type de limite particulier.<br>Supprime toutes les limites d'utilisation des ressources pour le paramètre *nom*, *nom_app*, *intervalle*, *action* spécifié, et scope, sans considération de *type_limite*. |
| *application* | • Un des moments d'application suivants : pré-exécution ou exécution<br>• NULL | Supprime les limites s'appliquant au moment d'application spécifiée.<br>Supprime toutes les limites d'utilisation des ressources pour le paramètre *nom*, *nom_app*, *type_limite*, *intervalle_temps*, *action* spécifié et scope, sans considération du moment d'application. |

| Paramètre | Valeur spécifiée | Conséquence |
|---|---|---|
| *action* | • Un des quatre types de limite suivants : avertissement en cas de problème, abandon de batch de requête, suppression de session<br>• NULL | Supprime les limites s'appliquant à un type d'action particulier.<br>Supprime toutes les limites d'utilisation des ressources pour le paramètre *nom*, *nom_app*, *intervalle*, *type_limite* spécifié, le moment d'application, et le paramètre *portée*, sans considération du paramètre *action*. |
| *portée* | • Un des types de portée suivants : requête, batch de requête, transaction<br>• NULL | Supprime les limites s'appliquant à une portée particulière.<br>Supprime toutes les limites d'utilisation des ressources pour le paramètre *nom*, *nom_app*, *intervalle_temps*, *type_limite* spécifié, le moment d'application, et le paramètre *action*, sans considération du paramètre *portée*. |

Quand vous utilisez sp_droplogin pour supprimer un login Adaptive Server, toutes les limites associées à ce login sont également supprimées.

Pour plus d'informations, reportez-vous à sp_drop_resource_limit dans le *Manuel de référence d'Adaptive Server*.

## Exemples de suppression d'une limite d'utilisation des ressources

```
sp_drop_resource_limit NULL, payroll, tu_wed_7_10
```

Cet exemple supprime toutes les limites d'utilisation des ressources pour tous les utilisateurs de l'application de paie pendant l'intervalle de temps tu_wed_7_10.

```
sp_drop_resource_limit NULL, payroll, tu_wed_7_10, elapsed_time
```

Cet exemple est similaire au précédent, mais ne supprime que la limite d'utilisation des ressources contrôlant le temps écoulé pour tous les utilisateurs de l'application de calcul de la paie (payroll) pendant l'intervalle de temps tu_wed_7_10.

```
sp_drop_resource_limit joe_user, payroll
```

Cet exemple supprime toutes les limites d'utilisation des ressources pour "joe_user" dans l'application de paie.

# Priorité des limites d'utilisation des ressources

Adaptive Server fournit des règles de priorité pour les intervalles de temps et les limites d'utilisation des ressources.

## Intervalles de temps

Pour chaque session de login pendant les intervalles de temps actifs, seule une limite peut être active pour chaque combinaison distincte de type de limite, moment d'application et portée. Les règles de priorité pour déterminer la limite active sont les suivantes :

- Si aucune limite n'est définie pour l'ID de login pour l'intervalle "at all times" ou les intervalles de temps actifs, il n'existe pas de limite active.
- Si des limites sont définies pour le login pour l'intervalle "at all times" et les intervalles de temps actifs, alors la limite des intervalles de temps actifs devient prioritaire.

## Limites d'utilisation des ressources

Comme le nom de login utilisateur ou le nom de l'application, ou les deux, sont utilisés pour identifier une limite d'utilisation des ressources, Adaptive Server observe une priorité de recherche prédéfinie tout en balayant la table sysresourcelimits à la recherche des limites applicables à une session de login. Le tableau ci-après décrit la priorité de correspondance entre les combinaisons de nom de login et de nom d'application :

| Niveau | Nom de login | Nom d'application |
|---|---|---|
| 1 | joe_user | payroll |
| 2 | NULL | payroll |
| 3 | joe_user | NULL |

Si une ou plusieurs correspondances sont trouvées pour un niveau de priorité donné, les niveaux supérieurs ne font pas l'objet de recherche. Cela empêche les conflits relatifs aux limites similaires pour des combinaisons login/application différentes.

Si aucune correspondance n'est trouvée à aucun niveau, aucune limite n'est appliquée à la session.

CHAPITRE 7

# Configuration des jeux de caractères, des ordres de tri et des langues

Ce chapitre présente les sujets liés à la supportée de la localisation et de l'internationalisation d'Adaptive Server Enterprise.

Les sujets traités dans ce chapitre sont les suivants :



## Compréhension de l'internationalisation et de la localisation

L'**internationalisation** est le processus qui permet à une application de supporter plusieurs langues et conventions culturelles.

Une application internationalisée utilise des fichiers externes pour fournir des informations propres à une langue au moment de l'exécution. Dépourvue de code propre à la langue, une application internationalisée peut être déployée dans n'importe quel environnement en langue native sans nécessiter de changement de code. Il est possible d'adapter à plusieurs langues ou régions une version unique d'un produit logiciel, conforme aux besoins et aux habitudes locales, sans avoir à effectuer de modifications techniques. Cette approche du développement logiciel permet des économies de temps et d'argent substantielles sur toute la durée de vie d'une application.

La **localisation** est le processus d'adaptation d'un produit internationalisé aux besoins d'une langue ou d'une région, tel l'espagnol. Ce processus comprend notamment la fourniture de traductions pour les messages système et l'interface utilisateur, ainsi que les formats corrects de date, d'heure et de devise. Une version d'un produit logiciel peut comporter plusieurs versions localisées.

Sybase assure la supportée de l'internationalisation et de la localisation. Adaptive Server comprend des fichiers de définition des jeux de caractères et de l'ordre de tri, nécessaires pour assurer la supportée du traitement des données dans les principales langues d'Europe de l'Ouest, d'Europe de l'Est, du Moyen-Orient, d'Amérique latine et d'Asie.

Les modules de langue Sybase proposent des messages système traduits et des formats pour le chinois (simplifié), le français, l'allemand, le japonais, le coréen, le brésilien et l'espagnol. Par défaut, Adaptive Server est livré avec des messages système en anglais américain.

Ce chapitre décrit les jeux de caractères et les modules de langue disponibles. De plus, il récapitule les étapes nécessaires au changement des jeux de caractères, de l'ordre de tri ou de la langue des messages par défaut pour Adaptive Server.

# Avantages des systèmes internationalisés

Concevoir une application pour la faire fonctionner en dehors de son pays d'origine est une tâche qui peut sembler titanesque. Pour les programmeurs, internationalisation rime souvent avec dépendances du code en dur fondées sur les conventions culturelles et linguistiques d'un seul pays.

Une meilleure approche consiste à écrire une application internationalisée : autrement dit, une méthode qui étudie l'environnement informatique local pour déterminer le langage à utiliser et qui charge les fichiers contenant les informations propres à une langue au moment de l'exécution.

Une application internationalisée peut être déployée dans tous les pays, ce qui présente plusieurs avantages :

- Vous écrivez et maintenez une application et non une douzaine (voire davantage).
- L'application peut être déployée, sans modification, dans de nouveaux pays au fil des besoins. Il suffit de fournir les fichiers de localisation corrects.
- Tous les sites peuvent s'attendre à des fonctionnalités et un comportement standard.

## Exemple de système internationalisé

Un système internationalisé peut inclure des applications clientes, des passerelles et des serveurs internationalisés s'exécutant sur plusieurs plates-formes dans différents environnements en langue native.

Par exemple, un système international peut contenir les composants suivants :

- des applications de traitement des commandes à New York, Mexico et Paris (applications Client-Library) ;
- un serveur de gestion de stock en Allemagne (Adaptive Server) ;
- un serveur de passation des commandes en France (Adaptive Server) ;
- une application de comptabilité centralisée au Japon (application Open Server fonctionnant avec Adaptive Server).

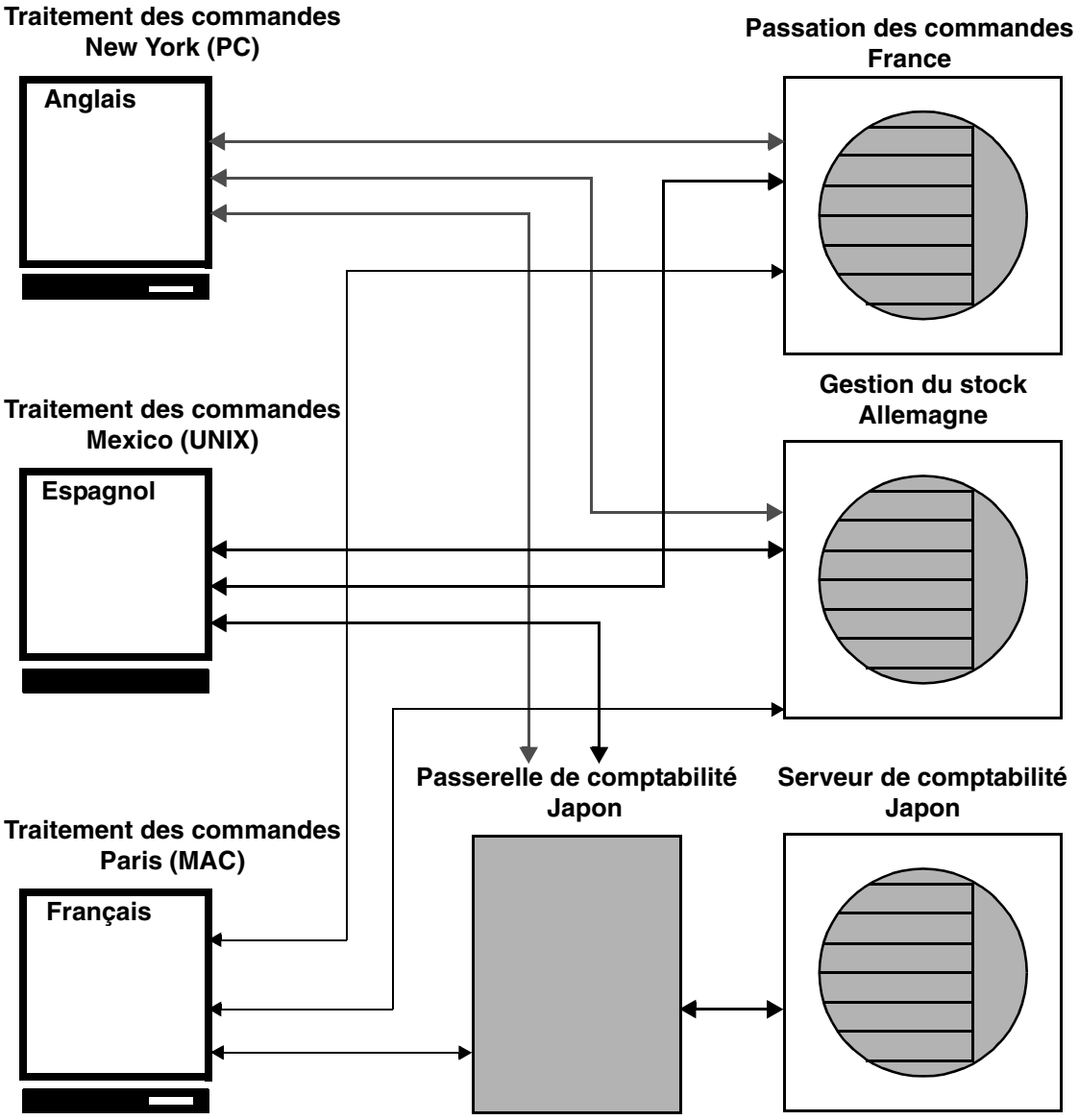
Dans ce système, les applications de traitement des commandes :

- demandent au serveur de gestion du stock de déterminer si les articles demandés sont en stock ;
- passent les commandes avec le serveur de passation des commandes ;
- envoient les informations financières à l'application comptable.

Le serveur de gestion de stock et le serveur de passation des commandes répondent aux demandes, tandis que l'application comptable collecte les informations financières et génère des rapports.

L'aspect du système est le suivant :

***Figure 7-1 : Exemple d'un système international***



Dans cet exemple, toutes les applications et les serveurs utilisent des langues et des jeux de caractères locaux pour accepter les messages d'entrée et de sortie.

## Eléments d'un système internationalisé

Pour configurer la langue de votre serveur dans un environnement internationalisé, vous pouvez manipuler trois éléments. Sybase vous suggère de les examiner et de planifier soigneusement le réseau client/serveur que vous souhaitez créer.

- Jeu de caractères – langue dans laquelle le serveur envoie et reçoit des données à destination ou en provenance des serveurs clients. Sélectionnez-le après avoir planifié et analysé attentivement les besoins linguistiques de tous les serveurs clients.
- Ordre de tri – les options d'ordre de tri sont fonction de la langue et du jeu de caractères sélectionnés.
- Messages système – les messages s'affichent dans l'une des langues fournies par Sybase. Si la langue de votre serveur ne figure pas parmi les langues proposées, les messages système s'affichent en anglais, la valeur par défaut.

Les sections suivantes décrivent chacun de ces éléments en détail.

# Sélection du jeu de caractères de votre serveur

Toutes les données codées dans votre serveur possèdent un code spécial. Par exemple, la lettre "a" porte le code "97" en numérotation décimale. Un **jeu de caractères** est une collection spécifique de caractères (alphabétiques, numériques, symboles, caractères de contrôle non imprimables etc.) assortis des valeurs numériques ou des codes qui leur sont affectés. En général, un jeu de caractères contient les caractères d'un alphabet, par exemple, l'alphabet latin utilisé pour l'anglais ou bien un script comme le cyrillique utilisé avec des langues telles que le russe, le serbe ou le bulgare. Les jeux de caractères propres à une plate-forme et qui supportent un sous-ensemble de langues, par exemple, les langues d'Europe de l'Ouest, sont dits **natifs** ou **nationaux**. Tous les jeux de caractères fournis avec Adaptive Server sont natifs, à l'exception de Unicode UTF-8.

Un **script** est un système d'écriture, soit une collection de tous les éléments caractérisant la forme écrite d'une langue. Par exemple, le latin, le japonais ou l'arabe. Selon les langues supportées par un alphabet ou un script, un jeu de caractères peut supporter une ou plusieurs langues. Ainsi, l'alphabet latin supporte les langues d'Europe de l'Ouest (voir le Groupe 1 dans le tableau 7-1) tandis que le script japonais ne supporte qu'une seule langue, le japonais. Le jeu de caractères du Groupe 1 accepte donc plusieurs langues, contrairement à de nombreux autres jeux, tels que ceux du Groupe 101, qui n'en acceptent qu'une seule.

La ou les langues supportées par un jeu de caractères s'appellent un **groupe de langues**. Un groupe de langues contient une ou plusieurs langues ; un jeu de caractères natifs est le codage, propre à une plate-forme, des caractères d'une ou de plusieurs langues d'un groupe de langues donné.

Dans un réseau client/serveur, vous pouvez supporter le traitement des données dans plusieurs langues *si toutes les langues appartiennent au même groupe* (voir le tableau 7-1). Si, par exemple, les données du serveur sont codées dans un jeu de caractères du Groupe 1, vous pouvez avoir dans la même base de données des données en français, en allemand, en italien et dans n'importe quelle autre langue du Groupe 1. En revanche, vous ne pouvez pas stocker dans la même base de données des données provenant d'un autre groupe de langues. Il est donc impossible de stocker des données en japonais avec des données en français ou en allemand.

Contrairement aux jeux de caractères natifs décrits précédemment, **Unicode** est un jeu de caractères international supportant plus de 650 langues dans le monde, telles que le japonais, le chinois, le russe, le français et l'allemand. Unicode permet d'associer sur le même serveur plusieurs langues issues de différents groupes de langues, quelle que soit la plate-forme choisie.

Etant donné que tous les jeux de caractères supportent le script latin et donc l'anglais, un jeu de caractères accepte toujours au moins deux langues, l'anglais et une autre langue.

De nombreuses langues sont supportées par plusieurs jeux de caractères. Celui que vous installez pour une langue dépend de la plate-forme et du système d'exploitation du client.

Adaptive Server supporte les langues et les jeux de caractères ci-après :

***Tableau 7-1 : Langues et jeux de caractères supportés***

| Groupe de langues | Langues | Jeux de caractères |
|---|---|---|
| Groupe 1 | *Europe de l'Ouest :*<br>albanais, catalan, danois, hollandais, anglais, féroïen, finnois, français, galicien, allemand, islandais, irlandais, italien, norvégien, portugais, espagnol, suédois | ASCII 8, CP 437, CP 850, CP 860, CP 863, CP 1252[a], ISO 8859-1, ISO 8859-15, Macintosh Roman, ROMAN8 |
| Groupe 2 | *Europe de l'Est :*<br>croate, tchèque, estonien, hongrois, letton, lituanien, polonais, roumain, slovaque, slovène (et anglais) | CP 852, CP 1250, ISO 8859-2, Macintosh Central European |
| Groupe 4 | Balte (et anglais) | CP 1257 |
| Groupe 5 | *Cyrillique :*<br>bulgare, biélorusse, macédonien, russe, serbe, ukrainien (et anglais) | CP 855, CP 866, CP 1251, ISO 8859-5, Koi8, Macintosh Cyrillic |
| Groupe 6 | Arabe (et anglais) | CP 864, CP 1256, ISO 8859-6 |
| Groupe 7 | Grec (et anglais) | CP 869, CP 1253, GREEK8, ISO 8859-7, Macintosh Greek |
| Groupe 8 | Hébreu (et anglais) | CP 1255, ISO 8859-8 |
| Groupe 9 | Turc (et anglais) | CP 857, CP 1254, ISO 8859-9, Macintosh Turkish, TURKISH8 |
| Groupe 101 | Japonais (et anglais) | CP 932 DEC Kanji, EUC-JIS, Shift-JIS |
| Groupe 102 | Chinois simplifié (PRC) (et anglais) | CP 936, EUC-GB |
| Groupe 103 | Chinois traditionnel (ROC) (et anglais) | Big 5, CP 950[b], EUC-CNS |
| Groupe 104 | Coréen (et anglais) | EUC-KSC |
| Groupe 105 | Thaï (et anglais) | CP 874, TIS 620 |

| Groupe de langues | Langues | Jeux de caractères |
|---|---|---|
| Groupe 106 | Vietnamien (et anglais) | CP 1258 |
| Unicode | Plus de 650 langues | UTF-8 |

a. CP 1252 est identique à ISO 8859-1, sauf pour les points de code 0x80–0x9F qui sont mappés aux caractères dans CP 1252.
b. CP 950 est identique à Big 5.

**Remarque** L'anglais est supporté par tous les jeux de caractères car les 128 premiers caractères décimaux comprennent l'alphabet latin (défini en tant que "ASCll-7). Les caractères situés au-delà présentent des différences selon les jeux de caractères. Ils servent à supporter les caractères dans différentes langues natives. Ainsi, les points de code allant de 0 à 127 de CP 932 et de CP 874 supportent l'alphabet anglais et latin. Toutefois, les points de code compris entre 128 et 255 supportent les caractères japonais dans CP 932 et les points de code de 128 à 255 les caractères thaïs dans CP 874.

Les jeux de caractères suivants supportent l'"euro", le symbole monétaire européen : CP 1252 (Europe de l'Ouest) ; CP 1250 (Europe de l'Est) ; CP 1251 (cyrillique) ; CP 1256 (arabe) ; CP 1253 (grec) ; CP 1255 (hébreu) ; CP 1254 (turc) ; CP 874 (thaï) et Unicode UTF-8.

Pour associer des langues issues de plusieurs groupes de langues, vous *devez* utiliser Unicode. Si Unicode est le jeu de caractères installé sur votre serveur, vous pouvez supporter plus de 650 langues sur un serveur unique et combiner des langues provenant de n'importe quel groupe de langues.

## Sélection du jeu de caractères par défaut sur le serveur

Lors de la configuration de votre serveur, vous êtes invité à spécifier un jeu de caractères par défaut. C'est celui dans lequel le serveur stocke et manipule les données. Chaque serveur ne peut avoir qu'un seul jeu de caractères par défaut.

Par défaut, l'outil d'installation considère qu'il s'agit du jeu de caractères natifs du système d'exploitation de la plate-forme. Tout jeu de caractères supporté par Adaptive Server peut toutefois jouer ce rôle (voir le tableau 7-1).

Ainsi, si vous installez le serveur sur un IBM RS/6000 exécutant AIX et que vous sélectionnez l'une des langues d'Europe de l'Ouest à installer, l'outil d'installation considère que le jeu de caractères par défaut est ISO 8859-1.

Si vous installez un serveur Unicode, sélectionnez UTF–8 comme jeu de caractères par défaut.

Pour les serveurs non-Unicode, déterminez la plate-forme utilisée par la majeure partie de vos systèmes clients et utilisez le jeu de caractères défini pour cette plate-forme comme jeu de caractères par défaut du serveur.

Cette méthode présente deux avantages :

- Le nombre de caractères non mappables entre les jeux de caractères est réduit.

  En général, comme le mappage un-à-un total n'existe pas entre les caractères de deux jeux, il existe un risque potentiel de perte de données. Ce risque est mineur car la plupart des caractères non convertis sont des symboles spéciaux rarement utilisés ou propres à une plate-forme.

- Cela réduit la conversion des jeux de caractères requise.

  Lorsque le jeu de caractères du système client diffère du jeu de caractères par défaut du serveur, il faut convertir les données afin d'en assurer la cohérence. Bien que la diminution des performances résultant de la conversion soit peu significative, il est judicieux de sélectionner le jeu de caractères par défaut, ce qui se traduit par des conversions moins nombreuses.

Par exemple, si la plupart de vos clients utilisent CP850, spécifiez CP850 sur votre serveur. Procédez ainsi même si votre serveur se trouve sur un système HP-UX (dont le jeu de caractères natifs pour les langues du Groupe 1 est ROMAN8).

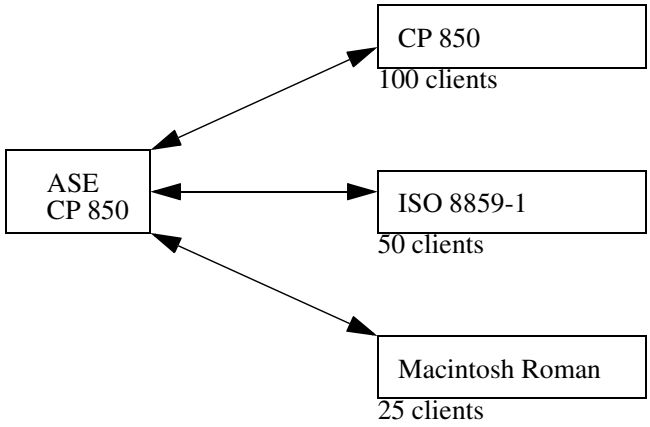
---

**Remarque** Sybase vous recommande vivement de choisir le jeu de caractères par défaut avant de créer des bases de données et de modifier les bases de données fournies par Sybase.

---

Dans l'exemple ci-dessous, 175 clients accèdent au même Adaptive Server. Ils sont tous situés sur des plates-formes différentes et utilisent plusieurs jeux de caractères. Le principal lien qui unit ces clients est que *tous* les jeux de caractères du système client/serveur appartiennent au même groupe de langues (reportez-vous au tableau 7-1). Notez que la langue par défaut de Adaptive Server est CP 850, le jeu de caractères utilisé par la majeure partie des clients. Le fonctionnement du serveur est plus efficace et la conversion des jeux de caractères moins importante.

***Figure 7-2 : Clients utilisant différents jeux de caractères dans le même groupe de langues***




Pour choisir le jeu de caractères par défaut de votre serveur, aidez-vous des tableaux ci-après illustrant les jeux de caractères les plus courants par plate-forme et par langue.

***Tableau 7-2 : Plate-formes clientes courantes en Europe de l'Ouest***

| Plate-forme | Langue | Jeu de caractères |
|---|---|---|
| Win 95, 98 | Anglais américain (U.S. English), Europe de l'Ouest | CP 1252 |
| Win NT 4.0 | U.S. English, Europe de l'Ouest | CP 1252 |
| Win 2000 | U.S. English, Europe de l'Ouest | CP 1252 |
| Sun Solaris | U.S. English, Europe de l'Ouest | ISO 8859-1 |
| HP-UX 10,11 | U.S. English, Europe de l'Ouest | ISO 8859-1 |
| IBM AIX 4.x | U.S. English, Europe de l'Ouest | ISO 8859-1 |

***Tableau 7-3 : Plate-formes clientes courantes au Japon***

| Plate-forme | Langue | Jeu de caractères |
|---|---|---|
| Win 95, 98 | Japonais | CP 932 pour Windows |
| Win NT 4.0 | Japonais | CP 932 pour Windows |
| Win 2000 | Japonais | CP 932 pour Windows |
| Sun Solaris | Japonais | EUC-JIS |
| HP-UX 10,11 | Japonais | EUC-JIS |
| IBM AIX 4.x | Japonais | EUC-JIS |

***Tableau 7-4 : Plate-formes clientes courantes en Chine***

| Plate-forme | Langue | Jeu de caractères |
|---|---|---|
| Win 95, 98 | Chinois (simplifié) | CP 936 pour Windows |
| Win NT 4.0 | Chinois (simplifié) | CP 936 pour Windows |
| Win 2000 | Chinois (simplifié) | CP 936 pour Windows |
| Sun Solaris | Chinois (simplifié) | EUC-GB |
| HP-UX 10,11 | Chinois (simplifié) | EUC-GBS |
| IBM AIX 4.x | Chinois (simplifié) | EUC-GB |

# Sélection de l'ordre de tri

Le tri des caractères varie selon les langues. Ainsi en anglais, *Cho* sera trié avant *Co*, tandis qu'en espagnol, l'inverse est appliqué. En allemand, la lettre ß correspond à un seul caractère ; cependant, dans les dictionnaires, elle est considérée comme le double caractère *ss* et triée en conséquence. Le tri des caractères accentués suit un ordre particulier de sorte que *aménité* précède *amène*, alors que l'inverse serait vrai, si ces mots étaient écrits sans accent. Par conséquent, pour que les caractères soient classés correctement, il est indispensable que leur tri s'effectue en fonction de la langue.

Chaque jeu de caractères est assorti d'un ou plusieurs ordres de tri qu'Adaptive Server utilise pour assembler les données. Tout ordre de tri se rattache à une langue ou à un jeu de langues donnés et à un jeu de caractères spécifique. L'anglais, le français et l'allemand peuvent suivre le même ordre puisqu'ils trient de la même façon les mêmes caractères ; par exemple, *A*, *a*, *B*, *b* et ainsi de suite. Quant aux caractères spécifiques à l'une des langues, comme les caractères accentués *é*, *è* et *à*, qui s'emploient en français et pas en anglais ni en allemand, leur ordre de tri ne soulève en conséquence aucune difficulté. Toutefois, il n'en va pas de même avec l'espagnol qui trie différemment les doubles lettres *ch* et *ll*. C'est pourquoi, bien que les mêmes jeux de caractères supportent les quatre langues, il existe une série d'ordres de tri pour l'anglais, le français et l'allemand et une série différente pour l'espagnol.

Par ailleurs, tout jeu de caractères donné est rattaché à un ordre de tri. Par conséquent, il existe une série d'ordres de tri pour l'anglais, le français et l'allemand dans le jeu de caractères ISO 8859-1, une autre série dans le jeu de caractères CP 850 et ainsi de suite. Les ordres de tri disponibles pour un jeu de caractères donné se trouvent dans les fichiers de définition des ordres de tri (fichiers **.srt*) contenus dans le répertoire des jeux de caractères. Pour plus d'informations sur les jeux de caractères et leurs ordres de tri possibles, reportez-vous à la section "Ordres de tri disponibles", page 296.

## Utilisation des ordres de tri

Les ordres de tri servent à :

- créer des index,
- stocker des données dans les tables indexées,
- spécifier une clause order by.

## Autres types d'ordres de tri

Tous les jeux de caractères comportent au minimum un ordre de tri binaire qui classe toutes les données à l'aveuglette en ne tenant compte que de la valeur arithmétique du code attribué pour représenter chacune des lettres (le code "binaire") du jeu de caractères. Ce type d'ordre fonctionne correctement pour les premiers 128 caractères de chaque jeu (ASCll English) et pour les langues asiatiques. Lorsqu'un jeu de caractères supporte plusieurs langues (Groupe 1 ou Unicode, par exemple), l'ordre de tri binaire peut donner des résultats incorrects et il faut en sélectionner un autre.

Le tri des jeux de caractères peut également s'effectuer d'après un ou plusieurs ordres alphabétiques recensés ci-dessous :

- *Ordre alphabétique, distinction majuscules/minuscules et distinction d'accents*, trie séparément les lettres en majuscules et en minuscules. L'ordre alphabétique reconnaît les différentes formes accentuées d'une lettre et les classe après la forme non accentuée associée.

- *Ordre alphabétique, sans distinction majuscules/minuscules, distinction d'accents*, trie les données dans l'ordre alphabétique sans différencier les majuscules des minuscules. Les majuscules sont équivalentes aux minuscules correspondantes et sont mélangées dans les résultats. Cette solution est commode pour éviter les entrées en double dans les tables de noms.
- *Ordre alphabétique, distinction majuscules/minuscules, distinction d'accents, ordre avec préférence*, ne différencie pas les majuscules des minuscules au moment de déterminer les éléments équivalents. Un mot en majuscules équivaut au même mot en minuscules. Si toutes les autres conditions sont égales, les majuscules ont la préférence (elles figurent en premier).

  L'utilisation de "sans distinction majuscules/minuscules avec préférences" peut aboutir à des performances médiocres en présence de vastes tables, lorsque les colonnes désignées dans une clause *order by* correspondent à la clé de l'index clusterisé de la table. Ne sélectionnez pas cette option, sauf s'il est indispensable pour votre installation que les majuscules soient triées avant les minuscules dans des chaînes qui autrement seraient équivalentes dans le cadre de clauses *order by*.
- *Ordre alphabétique, sans distinction majuscules/minuscules et des accents*, traite les lettres accentuées comme leur équivalent sans accent. Toutes ces lettres sont donc mélangées dans les résultats.

## Sélection de l'ordre de tri par défaut

Les serveurs Sybase n'acceptent qu'un seul ordre de tri par défaut à la fois. Si vos utilisateurs emploient la même langue ou que leurs langues utilisent le même ordre de tri, sélectionnez celui souhaité. Si, par exemple, ils utilisent des données en français et s'attendent à ce qu'elles soient triées selon cette langue, vous pouvez choisir l'un des ordres de tri alphabétiques correspondant au français. De même, s'ils travaillent sur des données en plusieurs langues et que celles-ci utilisent le même ordre de tri, par exemple, l'anglais, le français et l'allemand, vous pouvez choisir un ordre de tri ; il s'appliquera à tous les utilisateurs indépendamment de la langue traitée.

Toutefois, si certains utilisateurs emploient d'autres langues qui nécessitent des ordres de tri différents, par exemple, le français et l'espagnol, vous devez alors sélectionner l'un des ordres de tri comme valeur par défaut. Si vous retenez, par exemple, un tri français, les utilisateurs espagnols ne trouveront pas les doubles caractères *ch* et *ll* là où ils sont habituellement classés. La procédure d'installation configure le serveur avec l'ordre de tri binaire, celui appliqué par défaut.

La fonction sortkey peut servir à paramétrer d'autres ordres de tri personnalisés pour vos données, soit un pour chaque langue. Il est possible de les sélectionner de façon dynamique pour répondre aux besoins des différents utilisateurs. Bien que la fonction sortkey soit indépendante de l'ordre de tri par défaut, elle peut coexister sur le même serveur. La portée et la profondeur des ordres de tri fournis par cette fonction sont supérieures à celles obtenues avec le système de tri par défaut. Pour plus d'informations, reportez-vous à sortkey et compare dans le *Manuel de référence d'Adaptive Server*.

***Tableau 7-5 : Ordres de tri disponibles***

| Langue ou script | Jeux de caractères | Ordres de tri |
|---|---|---|
| Toutes les langues | UTF-8 | Binaire |
| Cyrillique :<br>bulgare, biélorusse, macédonien, russe, serbe, ukrainien | CP 855, CP 866, CP 1251, ISO 8859-5, Koi8, Macintosh Cyrillic | Ordre alphabétique, distinction majuscules/minuscules et distinction d'accents |
| Anglais, français, allemand | ASCII 8, CP 437, CP850, CP 860, CP 863, CP 1252a, ISO 8859–1, ISO 8859–15, Macintosh Roman, ROMAN8 | Ordre alphabétique, distinction majuscules/minuscules et distinction d'accents<br>Ordre alphabétique, sans distinction majuscules/minuscules, distinction d'accents<br>Ordre alphabétique, distinction majuscules/minuscules et distinction d'accents avec préférences<br>Ordre alphabétique, sans distinction majuscules/minuscules ni distinction d'accents |
| Anglais, français, allemand | CP 850 | Autre ordre alphabétique, distinction majuscules/minuscules<br>Autre ordre alphabétique, distinction majuscules/minuscules, sans distinction d'accents<br>Autre ordre alphabétique, distinction majuscules/minuscules avec préférences |
| Grec | ISO 8859–7 | Ordre alphabétique, distinction majuscules/minuscules et distinction d'accents |

| Langue ou script | Jeux de caractères | Ordres de tri |
|---|---|---|
| Hongrois | ISO 8859–2 | Ordre alphabétique, distinction majuscules/minuscules et distinction d'accents<br>Ordre alphabétique, sans distinction majuscules/minuscules, distinction d'accents<br>Ordre alphabétique, sans distinction majuscules/minuscules ni distinction d'accents |
| Russe | CP 866, CP 1251, ISO 8859–5, Koi8, Macintosh Cyrillic | Ordre alphabétique, distinction majuscules/minuscules et distinction d'accents<br>Ordre alphabétique, sans distinction majuscules/minuscules, distinction d'accents |
| Scandinave | CP 850 | Ordre alphabétique, distinction majuscules/minuscules et distinction d'accents<br>Ordre alphabétique, sans distinction majuscules/minuscules avec préférences |
| Espagnol | ASCII 8, CP 437, CP850, CP 860, CP 863, CP 1252, ISO 8859–1, ISO 8859–15, Macintosh Roman, ROMAN8 | Ordre alphabétique, distinction majuscules/minuscules et distinction d'accents<br>Ordre alphabétique, sans distinction majuscules/minuscules, distinction d'accents<br>Ordre alphabétique, sans distinction majuscules/minuscules ni distinction d'accents |
| Thaï | CP 874, TIS 620 | Ordre alphabétique |
| Turc | ISO 8859–9 | Ordre alphabétique, distinction majuscules/minuscules et distinction d'accents<br>Ordre alphabétique, sans distinction majuscules/minuscules ni distinction d'accents<br>Ordre alphabétique, sans distinction majuscules/minuscules, distinction d'accents |

Si votre langue n'apparaît pas dans cette liste, il n'existe aucun ordre de tri propre à votre langue. Sélectionnez un ordre de tri binaire, puis faites des recherches pour savoir si la fonction sortkey correspond à vos besoins. Comme l'illustre ce tableau, de nombreuses langues possèdent plusieurs ordres de tri.

## Sélection de l'ordre de tri Unicode par défaut

L'ordre de tri Unicode par défaut se distingue de celui du jeu de caractères par défaut du serveur. Ce paramètre de configuration distinct est statique. Il demande le redémarrage de votre serveur et la réindexation des données unichar en cas de modification de ces dernières. Cet ordre de tri est identifié à l'aide d'un paramètre de chaîne, de préférence à un paramètre numérique, ce qui garantit son unicité.

Les ordres de tri Unicode disponibles par défaut sont les suivants :

***Tableau 7-6 : Ordres de tri Unicode par défaut***

| Nom | Description |
|---|---|
| options par défaut | ordre ML Unicode par défaut |
| binaire | ordre binaire par défaut |
| thaidict | Thaï, ordre alphabétique |
| scandict | Scandinave, ordre alphabétique |
| scannocp | Scandinave, sans distinction majuscules/minuscules |
| dict | Anglais, ordre alphabétique |
| nocase | Anglais, sans distinction majuscules/minuscules |
| noaccent | Anglais, sans distinction d'accents |
| espdict | Espagnol, ordre alphabétique |
| espnocs | Espagnol, sans distinction majuscules/minuscules |
| espnoac | Espagnol, sans distinction d'accents |
| rusdict | Russe, ordre alphabétique |
| rusnocs | Russe, sans distinction majuscules/minuscules |
| cyrdict | Cyrillique, ordre alphabétique |
| cyrnocs | Cyrillique, sans distinction majuscules/minuscules |
| elldict | Grec, ordre alphabétique |
| hundict | Hongrois, ordre alphabétique |
| hunnoac | Hongrois, sans distinction d'accents |
| hunnocs | Hongrois, sans distinction majuscules/minuscules |
| turkdict | Turc, ordre alphabétique |
| turknoac | Turc, sans distinction d'accents |
| turknocs | Turc, sans distinction majuscules/minuscules |
| sjisbin | Japonais, sjis binaire |
| iso14651 | Ordre standard ISO 14651 |
| eucjisbin | eucjis japonais |
| gb2312bin | gb2312 chinois |
| cp932msbin | cp932 japonais |

| Nom | Description |
|---|---|
| b165bin | b165 chinois |
| euckcsbin | euckcs coréen |
| utf8bin | correspond à l'ordre de tri binaire Unicode UTF-8 |

Vous pouvez ajouter des ordres de tri à l'aide des fichiers externes dans le répertoire *$SYBASE/collate/Unicode*. Les noms et les ID de classement sont stockés dans SYSCHARSETS. Avant de définir l'ordre de tri Unicode par défaut, il n'est pas nécessaire que les noms des ordres de tri Unicode externes soient en SYSCHARSETS.

**Remarque** Sybase fournit les ordres de tri Unicode externes. N'essayez pas de les créer.

## Choix de la langue des messages système

Toute installation d'Adaptive Server peut exploiter les modules de langue qui renferment les fichiers de messages en plusieurs langues. Les messages existent dans les langues suivantes : anglais, chinois (simplifié), français, allemand, japonais, coréen, brésilien, portugais et espagnol. Si la langue de votre client n'en fait *pas* partie, les messages système s'afficheront en anglais, la langue par défaut.

Chaque client peut décider d'afficher les messages dans sa propre langue en même temps que dans d'autres et ce, à partir du même serveur ; un client lira ainsi les messages système en français, un autre en espagnol et un troisième en allemand. Cependant, pour y parvenir, toutes les langues sélectionnées *doivent* appartenir au même groupe de langues. Par exemple, le français, l'espagnol et l'allemand font partie du groupe de langues 1. En revanche, le japonais fait partie du groupe de langues 101 qui ne contient aucune autre langue. Par conséquent, si la langue utilisée sur un serveur est le japonais, les messages système apparaîtront uniquement en japonais ou en anglais. N'oubliez pas en effet que *tous* les groupes de langues peuvent afficher les messages en anglais. Il existe également une langue par défaut pour l'ensemble du serveur ; elle s'applique lorsque l'utilisateur n'en a défini aucune. Si vous utilisez Unicode, vous pouvez lire les messages système dans n'importe quelle langue supportée.

Pour sélectionner la langue de vos messages système, choisissez l'une ou l'autre de ces possibilités :

- Sélectionnez une langue faisant partie de votre profil utilisateur.
- Indiquez une langue dans le fichier *locales.dat*.

Le tableau suivant présente les langues des messages système supportées ainsi que leurs groupes de langues. Chaque utilisateur peut sélectionner uniquement une langue par session.

***Tableau 7-7 : Messages système supporté***

| Groupe de langues | Langues des messages système | Jeux de caractères |
|---|---|---|
| Groupe 1 | Français, allemand, espagnol, brésilien | ASCII 8, CP 437, CP 850, CP 860, CP 863, CP 1252, ISO 8859-1, ISO 8859-15, Macintosh Roman, ROMAN8 |
| Groupe 101 | Japonais | CP 932, DEC Kanji, EUC-JIS, Shift-JIS |
| Groupe 102 | Chinois simplifié (PRC) | CP 936, EUC-GB |
| Groupe 104 | Coréen | EUC-KSC |
| Unicode | Français, allemand, espagnol, brésilien, japonais, chinois simplifié, coréen | UTF-8 |
| Tous les autres groupes de langues | Anglais | |

Vous devez installer des modules de langue pour toutes les langues dans lesquelles les clients recevront des messages. Ces modules, présents dans le sous-répertoire *locales* du répertoire d'installation d'Adaptive Server, font partie du groupe de fichiers appelé *fichiers de localisation*. Pour plus d'informations sur les fichiers de localisation et la structure des répertoires de messages logiciels, reportez-vous à la section "Types des fichiers de localisation", page 315.

# Configuration du serveur : exemples

Cette section aborde les options de configuration et les étapes à suivre pour les mettre en application. Il s'agit en fait d'un d'exemple qui présente des idées et des méthodes applicables à votre propre processus de configuration.

## Serveur version espagnole

Les indications fournies ci-après expliquent comment configurer un nouveau serveur dont tous les clients utilisent la même langue. Procédure :

1 Sélectionnez la langue du serveur, l'espagnol en l'occurrence. En observant le tableau 7-1, page 289, vous notez que l'espagnol fait partie du groupe de langues 1. Sélectionnez un jeu de caractères à partir de ce groupe en tenant compte de votre plate-forme. Sybase recommande de sélectionner celui qu'utilise la majeure partie des clients. Cependant, si vous estimez que votre entreprise est appelée à se développer en direction d'autres pays et d'autres langues, vous pouvez envisager d'installer Unicode (reportez-vous à la section "Sélection du jeu de caractères de votre serveur", page 288).

2 Installez sur le serveur le module de langue prévu pour l'espagnol. Il permet aux clients d'afficher les messages système en espagnol.

3 Sélectionnez l'ordre de tri par défaut. En vous reportant au tableau 7-5, page 296, vous constatez que l'espagnol comporte trois ordres de tri possibles, en plus de l'ordre de tri binaire. Sélectionnez-en un.

4 Redémarrez le serveur.

## Entreprise américaine au Japon

Ce cas de figure sous-entend qu'il existe au Japon des clients qui souhaiteront entrer des données, les trier et recevoir des messages système en japonais, tout en soumettant les données à un serveur auquel seuls des utilisateurs de langue anglaise auront accès. Procédure :

1 Sélectionnez le jeu de caractères par défaut destiné au serveur. Si celui que vous installez provient du groupe de langues 101 (japonais), vous pourrez disposer du japonais et de l'anglais sur le même serveur.

2 Installez le module de langue correspondant au japonais pour que les messages système soient disponibles dans cette langue.

3 Sélectionnez l'ordre de tri. En vous reportant au tableau 7-5, page 296, vous remarquez que l'ordre de tri binaire est le seul disponible pour le japonais. Les clients anglais et japonais auront donc tous deux cet ordre de tri par défaut. Pensez à utiliser la fonction sortkey pour fournir des solutions aux deux groupes d'utilisateurs.

4 Assurez-vous que chaque utilisateur japonais demande des messages en japonais par défaut. Puisque vous utilisez un jeu de caractères issu du groupe de langues 101 et que vous avez déjà installé le module de langue en japonais, votre client au Japon obtiendra les messages en japonais, tandis qu'aux Etats-Unis vos clients pourront décider de les afficher en anglais.

## Entreprise japonaise aux clients multinationaux

L'entreprise est implantée au Japon et a des clients en France, en Allemagne et en Espagne.

Ce cas de figure laisse entendre qu'il vous faudra mélanger des langues européennes et asiatiques sur le même serveur.

1 Sélectionnez la langue et le jeu de caractères par défaut du serveur. Puisque votre entreprise est installée au Japon et que la plupart de vos clients se trouvent au Japon, la langue par défaut du serveur devrait être le japonais. Cependant, vous voulez que vos clients de France, d'Allemagne et d'Espagne puissent envoyer et recevoir des données dans leur langue maternelle. En consultant le tableau 7-1, page 289, vous notez que le japonais fait partie du groupe de langues 101, tandis que le français, l'allemand et l'espagnol appartiennent au groupe de langues 1. Puisque les langues qui vous sont nécessaires ne font pas partie du même groupe de langues, la seule façon de les avoir toutes sur le même serveur est de sélectionner Unicode comme jeu de caractères par défaut.

2 Installez les modules de langue correspondant au japonais, au français, à l'allemand et à l'espagnol.

3 Sélectionnez l'ordre de tri binaire, puisqu'il constitue le seul ordre de tri disponible pour le jeu de caractères Unicode. (Vous pouvez néanmoins envisager d'utiliser la fonction sortkey dans votre application pour fournir des données triées dans l'ordre de prédilection de chaque utilisateur.)

4 Sélectionnez le japonais comme langue par défaut des messages système. Les clients des autres pays peuvent sélectionner leur propre langue native pour les messages.

# Changement du jeu de caractères, de l'ordre de tri ou de la langue des messages

L'administrateur système peut changer le jeu de caractères, l'ordre de tri ou la langue par défaut qu'Adaptive Server utilise pour les messages, même après avoir configuré le serveur. Etant donné que tout ordre de tri est tributaire d'un jeu de caractères particulier, tout changement de jeu implique un autre ordre de tri. Vous pouvez toutefois changer l'ordre de tri sans changer de jeux de caractères, puisqu'un même jeu peut présenter plusieurs ordres de tri possibles.

Pour afficher l'ordre de tri, le jeu de caractères d'Adaptive Server par défaut ainsi qu'un tableau de ses ordres de tri principaux, tapez :

```
sp_helpsort
```

## Changement du jeu de caractères par défaut

Adaptive Server ne peut avoir qu'un seul *jeu de caractères par défaut*, celui dans lequel les données sont stockées dans sa base de données. Lorsque vous installez Adaptive Server, vous spécifiez un jeu de caractères par défaut.

---

**Avertissement !** Lisez attentivement les instructions ci-dessous et soyez prudent en changeant le jeu de caractères par défaut défini dans Adaptive Server. Sybase vous recommande de réaliser d'abord des sauvegardes avant de changer un jeu de caractères par défaut.

---

Lorsque vous changez le jeu de caractères par défaut défini dans Adaptive Server, vous devez convertir les données existantes dans le nouveau jeu de caractères par défaut. La conversion n'est pas nécessaire dans les cas suivants *uniquement* :

- Le serveur ne contient pas de données utilisateur.
- Il est possible de détruire des données utilisateur sur le serveur.
- Vous êtes *absolument certain* que les données du serveur se servent uniquement du code ASCll-7. Vous pouvez alors changer la valeur par défaut sans copier les données en dehors du serveur.

Dans tous les autres cas, vous devez convertir les données existantes comme suit :

1 Copiez les données à l'extérieur du serveur à l'aide de bcp.

2 Changez le jeu de caractères par défaut.

3 Utilisez bcp avec les drapeaux appropriés à la conversion des données pour rapatrier les données sur le serveur.

Pour plus d'informations sur l'utilisation de bcp pour copier les données, reportez-vous au guide *Utilitaires*.

---

**Avertissement !** Une fois les données converties dans un autre jeu de caractères (UTF-8 notamment), il se peut que les données soient trop volumineuses pour la taille de colonne allouée. Recréez les colonnes affectées avec une taille plus grande. Pour plus d'informations, reportez-vous à l'outil Unidb dans le produit Sybase UDK.

---

En principe, la conversion du code entre le jeu de caractères des données existantes et le nouveau jeu par défaut est supportée. Dans le cas contraire, des erreurs de conversion se produisent et les données ne sont pas converties correctement. Pour plus d'informations sur la conversion des jeux de caractères supporté, reportez-vous au chapitre 8, "Configuration des conversions de jeux de caractères entre clients et serveur",.

Bien qu'il soit possible de convertir entre eux les jeux de caractères, l'opération risque d'engendrer des erreurs en raison des petites caractéristiques qui les différencient ou parce que certains caractères n'ont pas d'équivalent dans d'autres jeux. Il arrive que les lignes contenant les données problématiques ne soient pas recopiées dans la base de données ou que celles-ci contiennent des caractères incomplets ou incorrects.

## Changement de l'ordre de tri par défaut

Adaptive Server peut ne disposer que d'un seul *ordre de tri par défaut*, à savoir la séquence de tri qu'il utilise pour classer les données. Lorsque vous prévoyez de changer l'ordre de tri des caractères sur un Adaptive Server donné, il ne faut pas oublier que : tous les Adaptive Server de votre structure doivent avoir le même ordre de tri. Le fait de s'en tenir à un seul ordre engendre la cohérence et facilite la gestion du traitement distribué.

Après avoir changé l'ordre de tri par défaut, il faut parfois recréer les index. Pour plus d'informations, reportez-vous à la section "Reconfiguration du jeu de caractères, de l'ordre de tri ou de la langue des messages", page 305.

## Reconfiguration du jeu de caractères, de l'ordre de tri ou de la langue des messages

Cette section décrit les étapes à suivre avant et après changement du jeu de caractères, de l'ordre de tri ou de la langue des messages d'Adaptive Server. Pour connaître les procédures à suivre afin de configurer le jeu de caractères, l'ordre de tri et la langue des messages d'un nouveau serveur, reportez-vous au Manuel de configuration pour votre plate-forme.

S'il n'y a pas lieu de convertir les données dans un nouveau jeu de caractères et que l'ancien et le nouveau jeu utilisent l'ordre de tri binaire, vous pouvez faire une sauvegarde de la base de données. Vous la restaurerez à partir des sauvegardes effectuées avant la reconfiguration du jeu de caractères.

---

**Remarque** Sauvegardez toutes les bases de données d'Adaptive Server avant et après changement des jeux de caractères ou des ordres de tri.

---

En règle générale, il n'est pas possible de recharger les données à partir de la sauvegarde d'une base de données une fois le jeu de caractères et l'ordre de tri par défaut reconfigurés.

Si ce qui suit est vrai, utilisez bcp pour copier les données dans vos bases de données et en dehors de celles-ci.

- Si une base de données contient des caractères alphanumériques et que vous voulez convertir les données dans un nouveau jeu de caractères. Ne chargez pas de sauvegarde des données de la base dans un Adaptive Server doté du nouveau jeu de caractères par défaut. Adaptive Server interprète les données chargées comme si elles présentaient le nouveau jeu de caractères et elles seront endommagées.
- Si vous ne changez que l'ordre de tri par défaut et non le jeu de caractères par défaut. Vous ne pouvez pas charger une base de données à partir d'une sauvegarde effectuée avant changement de l'ordre de tri. Si vous tentez de le faire, un message d'erreur apparaît et le chargement est interrompu.

- Vous changez le jeu de caractères par défaut et soit le nouvel ordre de tri, soit l'ancien n'est pas binaire. Vous ne pouvez pas charger une sauvegarde de base de données effectuée avant changement du jeu de caractères.

## Etapes préliminaires

Avant d'exécuter le programme d'installation pour reconfigurer Adaptive Server :

1 Sauvegardez toutes les bases de données utilisateur ainsi que la base de données master. Si vous avez apporté des modifications à la base de données model ou sybsystemprocs, sauvegardez-la également.

2 Chargez le module de langue si ce n'est déjà fait (pour connaître la procédure à suivre, reportez-vous au Manuel de configuration pour votre plate-forme).

3 Si vous changez le jeu de caractères par défaut d'Adaptive Server alors que vos bases courantes contiennent des données qui ne sont pas en ASCII-7, utilisez bcp pour copier les données présentes dans vos bases.

Une fois le module de langue chargé, vous pouvez lancer le programme d'installation d'Adaptive Server qui permet de :

- installer ou supprimer les langues des messages et les jeux de caractères compris dans Adaptive Server ;
- changer la langue des messages ou le jeu de caractères par défaut ;
- sélectionner un autre ordre de tri.

Pour en savoir plus sur l'utilisation du programme d'installation, reportez-vous au Manuel de configuration pour votre plate-forme.

Vous reconfigurez la langue, le jeu de caractères ou l'ordre de tri à l'aide de l'utilitaire sqlloc décrit à la section Utilitaires pour UNIX. Si vous travaillez sous Windows NT, choisissez l'utilitaire Server Config décrit dans le manuel de configuration Adaptive Server pour Windows NT. Si vous ajoutez un nouveau jeu de caractères qui n'existe pas dans Adaptive Server, reportez-vous au manuel *Sybase Character Sets* pour connaître la procédure à suivre.

Lorsque vous avez installé les langues supplémentaires sans changer le jeu de caractères, ni l'ordre de tri d'Adaptive Server, vous avez terminé le processus de reconfiguration.

Si vous avez changé le jeu de caractères par défaut d'Adaptive Server et que vos bases courantes contiennent des données qui ne sont pas en ASCII-7, recopiez les données dans les bases à l'aide de la procédure bcp avec les indicateurs appropriés pour activer la conversion.

Si vous avez changé l'ordre de tri et le jeu de caractères par défaut d'Adaptive Server, reportez-vous à la section "Reconfiguration du jeu de caractères, de l'ordre de tri ou de la langue des messages", page 305.

## Configuration de la langue par défaut de l'utilisateur

Si vous installez une langue supplémentaire, les utilisateurs qui gèrent les programmes clients peuvent lancer la procédure sp_modifylogin pour définir cette langue comme leur langue par défaut ou définir la variable LANG sur la machine cliente avec les entrées appropriées dans le fichier locales.dat.

## Restauration après reconfiguration

Chaque fois qu'Adaptive Server est arrêté puis redémarré, chacune des bases de données fait systématiquement l'objet d'une récupération. La restauration automatique est décrite en détail au chapitre 26, "Elaboration d'un plan de sauvegarde et de reprise".

Une fois la restauration terminée, les nouvelles définitions de l'ordre de tri et du jeu de caractères sont chargées.

Lorsque l'ordre de tri a été changé, Adaptive Server passe en mode mono-utilisateur pour permettre d'apporter les mises à jour nécessaires aux tables du système et empêcher les autres utilisateurs d'utiliser le serveur. Chacune des tables du système dont l'index est constitué de caractères est automatiquement contrôlée pour vérifier que le changement de l'ordre de tri n'a pas corrompu d'index. Les index de ce type compris dans les tables du système sont automatiquement reconstruits si nécessaire, en utilisant la définition du nouvel ordre de tri.

Une fois les index du système reconstruits, ceux des utilisateurs, orientés index, sont marqués comme étant "suspects" dans la table sysindexes du système, sans qu'ils soient vérifiés. Les tables des utilisateurs dont les index sont suspects sont marquées comme étant "en lecture seule" dans la table sysobjects pour empêcher leur mise à jour et l'utilisation des index "suspects" jusqu'à leur vérification et, si nécessaire, leur reconstruction.

Ensuite, les nouvelles informations relatives à l'ordre de tri remplacent les anciennes sur le disque, à l'endroit où les informations de configuration sont enregistrées. Puis, Adaptive Server s'arrête pour pouvoir démarrer la session suivante avec un ensemble d'informations système complètes et justes.

## Utilisation de la procédure *sp_indsuspect* pour rechercher les index altérés

Lorsqu'Adaptive Server s'est arrêté, redémarrez-le et utilisez sp_indsuspect pour rechercher les tables dont l'index est à recréer. La syntaxe est la suivante :

```
sp_indsuspect [nom_table]
```

où *nom_table* est le nom facultatif d'une table particulière. Si *nom_table* n'est pas indiqué, sp_indsuspect crée, lors du changement de l'ordre de tri, une liste de toutes les tables de la base de données courante dont les index sont marqués comme "suspects".

Dans cet exemple, l'exécution de sp_indsuspect dans la base de données mydb génère un index suspect :

```
sp_indsuspect
Suspect indexes in database mydb
Own.Tab.Ind (Obj_ID, Ind_ID) =
dbo.holdings.h_name_ix(160048003, 2)
```

## Reconstruction des index après changement de l'ordre de tri

dbcc reindex vérifie la cohérence des index sur les tables utilisateur en exécutant une version "rapide" de dbcc checktable. Pour plus d'informations, reportez-vous à la section "dbcc checktable", page 784. dbcc reindex supprime et reconstruit les index lorsque l'ordre de tri utilisé n'est pas cohérent avec le nouvel ordre de tri. Lorsque la commande dbcc reindex trouve la première erreur liée à l'index, un message s'affiche et les index incohérents sont recréés. L'administrateur système ou le propriétaire de la table doit exécuter dbcc reindex après avoir changé l'ordre de tri sur Adaptive Server.

La syntaxe est la suivante :

dbcc reindex ({*nom_table* | *id_table*})

Exécutez cette commande sur toutes les tables signalées par sp_indsuspect comme contenant des index suspects. Par exemple :

```
dbcc reindex(titles)
One or more indexes are corrupt. They will be
rebuilt.
```

Dans l'exemple précédent, la commande dbcc reindex trouve un ou plusieurs index suspects dans la table titles ; les index appropriés sont supprimés, puis reconstruits.

Si une table contient des index corrects ou n'en contient aucun, dbcc reindex ne recrée pas d'index mais affiche un message d'information. Si une table est suspectée de contenir des données altérées, la commande est interrompue. Dans ce cas, un message d'erreur demande à l'utilisateur d'exécuter dbcc checktable.

Lorsque dbcc reindex se termine correctement, toutes les marques "suspect" figurant dans les index de la table sont supprimées. La marque "lecture seule" est également supprimée et la table peut être mise à jour. Ces marques sont supprimées, que les index aient ou non besoin d'une reconstruction.

dbcc reindex ne réindexe pas les tables système. En cas de redémarrage d'Adaptive Server à la suite d'un changement de l'ordre de tri, les index système sont automatiquement contrôlés puis reconstruits, si nécessaire, lors du processus de restauration.

## Mise à niveau des données *text* après changement des jeux de caractères

Si vous avez changé un jeu de caractères d'Adaptive Server en **jeu de caractères codé sur plusieurs octets**, utilisez dbcc fix_text pour mettre à niveau les valeurs text.

La syntaxe est la suivante :

dbcc fix_text ({*nom_table* | *id_table*})

Le passage à un jeu de caractères codé sur plusieurs octets complique la gestion des données text. Une valeur text pouvant couvrir plusieurs pages, Adaptive Server doit pouvoir gérer des caractères qui s'étendent sur plusieurs pages. Pour ce faire, Adaptive Server a besoin d'informations supplémentaires sur chaque page text. L'administrateur système ou le propriétaire de la table doit exécuter dbcc fix_text sur chaque table qui possède des données text afin de calculer les nouvelles valeurs nécessaires.

Pour afficher les noms de toutes les tables contenant des données text, utilisez la commande suivante :

```
select sysobjects.name
from sysobjects, syscolumns
where syscolumns.type = 35
and sysobjects.id = syscolumns.id
```

L'administrateur système ou le propriétaire de la table doit exécuter dbcc fix_text pour calculer les nouvelles valeurs nécessaires.

La syntaxe de dbcc fix_text est la suivante :

dbcc fix_text (*nom_table* | *id_table*)

Cette table nommée doit résider dans la base de données courante.

dbcc fix_text ouvre la table spécifiée, calcule les statistiques de caractères nécessaires à chaque valeur text, puis ajoute les statistiques aux champs d'en-tête de pages appropriés. Ce processus peut être long car il dépend du nombre et de la taille des valeurs text contenues dans une table. dbcc fix_text peut générer un nombre important d'enregistrements susceptibles de saturer le journal des transactions. dbcc fix_text effectue des mises à jour en séquences de petites transactions de sorte qu'en cas de saturation, seule une petite partie du travail est perdue.

Si vous manquez d'espace de journalisation, purgez le journal (reportez-vous au chapitre 27, "Sauvegarde et restauration de bases de données utilisateur"). Ensuite, relancez dbcc fix_text en utilisant la table qui était en cours de mise à niveau lors de l'interruption de la première commande dbcc fix_text. Chaque valeur de texte codée sur plusieurs octets contient des informations indiquant si elle a déjà été mise à niveau ; ainsi, dbcc fix_text met à jour uniquement les valeurs text non encore traitées.

Si votre base de données stocke son journal sur un segment distinct, vous pouvez utiliser les seuils pour gérer la purge du fichier journal. Pour plus d'informations, reportez-vous au chapitre 29, "Gestion de l'espace libre avec des seuils".

Si dbcc fix_text ne peut pas acquérir un verrou dont il a besoin sur une page de texte, le problème est signalé et le travail se poursuit de la façon suivante :

```
Unable to acquire an exclusive lock on text page 408.
This text value has not been recalculated. In order
to recalculate those TEXT pages you must release the
lock and reissue the dbcc fix_text command.
```

### Récupération des valeurs *text* après changement des jeux de caractères

Si vous tentez de récupérer des valeurs text après avoir adopté un jeu de caractères codé sur plusieurs octets et que vous n'avez pas exécuté dbcc fix_text, la commande échoue et le message d'erreur suivant s'affiche :

```
Adaptive Server is now running a multi-byte
character set, and this TEXT column's character
counts have not been recalculated using this
character set. Use dbcc fix_text before running this
query again.
```

**Remarque** Si vous avez modifié l'ordre de tri ou le jeu de caractères et que des erreurs se sont produites, consultez la section "How to Manually Change Sort Order or Default Character Set" du *Adaptive Server Enterprise Troubleshooting and Error Messages Guide*.

## Installation des chaînes de date pour les langues non supportées

Vous pouvez recourir à sp_addlanguage pour installer les noms des jours de la semaine et des mois de l'année pour les langues qui ne disposent pas de modules de langue. Avec sp_addlanguage, vous définissez :

- le nom de la langue et (en option) un alias pour le nom,
- la liste des noms complets des mois et la liste des abréviations des noms de mois,
- la liste des noms complets des jours de la semaine,
- le format de date pour la saisie des dates (tel que mois/jour/année),
- le numéro du premier jour de la semaine.

Cet exemple ajoute des informations pour l'italien :

```
sp_addlanguage italian, italiano,
"gennaio,febbraio,marzo,aprile,maggio,giugno,luglio,agosto,settembre,ottobre,
novembre,dicembre",
"genn,feb,mar,apr,mag,giu,lug,ago,sett,ott,nov,dic",
"lunedi,martedi,mercoledi,giovedi,venerdi,sabato,domenica",
dmy, 1
```

sp_addlanguage applique des règles strictes de saisie des données. Les listes de noms de mois, d'abréviations de mois et de jours de la semaine doivent être séparées par des virgules, sans espaces ni retours chariot. De plus, elles doivent contenir le nombre d'éléments correct (12 pour les mois, 7 pour les jours de la semaine.)

Les valeurs correctes des formats de date sont les suivantes : mdy, dmy, ymd, ydm, myd et dym. La valeur dmy indique que les dates sont au format jour/mois/année. Ce format affecte uniquement la saisie des données ; pour modifier le format du résultat, vous devez utiliser la fonction convert.

## Interprétation de la date sur le client et le serveur

En général, les valeurs de date sont résolues sur le client. Lorsqu'un utilisateur sélectionne des valeurs de date, Adaptive Server les envoie au client au format interne. Le client utilise le fichier *common.loc* ainsi que d'autres fichiers de localisation situés dans le sous-répertoire de langues par défaut du répertoire *locales* pour convertir le format interne en caractères. Si, par exemple, la langue par défaut de l'utilisateur est l'espagnol, Adaptive Server recherche le fichier *common.loc* dans */locales/spanish/char_set*. Il utilise les informations du fichier pour afficher, par exemple, 12 febrero 1997.

Imaginons que la langue par défaut de l'utilisateur est l'italien, langue pour laquelle Adaptive Server ne fournit pas de module de langue et que des valeurs de date en italien aient été ajoutées. Lorsque le client se connecte au serveur et recherche le fichier *common.loc* pour l'italien, il ne le trouve pas. Le client imprime un message d'erreur et se connecte au serveur. Si l'utilisateur sélectionne ensuite des valeurs de date, celles-ci s'affichent au format anglais. Pour afficher les valeurs de date ajoutées avec sp_addlanguage, utilisez la fonction convert pour forcer la conversion des dates en caractères sur le serveur.

La demande suivante génère un jeu de résultats avec des dates au format anglais américain (U.S. English) :

```
select pubdate from titles
```

la demande ci-dessous renvoyant la date avec les noms de mois en italien :

```
select convert(char(19),pubdate) from titles
```

# Fichiers d'internationalisation et de localisation

## Types de fichiers d'internationalisation

Les fichiers supportant le traitement des données dans une langue particulière s'appellent des *fichiers d'internationalisation*. Plusieurs types de fichiers d'internationalisation sont livrés avec Adaptive Server. Ils sont décrits dans le tableau 7-8.

***Tableau 7-8 : Fichiers d'internationalisation***

| Fichier | Emplacement | Objectif et contenu |
|---|---|---|
| *charset.loc* | Dans chaque sous-répertoire de jeux de caractères du répertoire *charsets* | Fichiers de définition des jeux de caractères qui déterminent les propriétés lexicales de chaque caractère, telles que les caractères alphanumériques, la ponctuation, l'opérande et les caractères majuscules et minuscules. Utilisés par Adaptive Server pour traiter correctement les données. |
| **.srt* | Dans chaque sous-répertoire de jeux de caractères du répertoire *charsets* | Définit l'ordre de tri des caractères alphanumériques et des caractères spéciaux, y compris les ligatures, les caractères diacritiques et autres aspects linguistiques. |
| **.xlt* | Dans chaque sous-répertoire de jeux de caractères du répertoire *charsets* | Fichiers de conversion de caractères propres aux terminaux à utiliser avec des utilitaires tels que bcp et isql. Pour plus d'informations sur le mode d'utilisation des fichiers *xlt*, reportez-vous au chapitre 8, "Configuration des conversions de jeux de caractères entre clients et serveur", et au guide *Utilitaires*. |

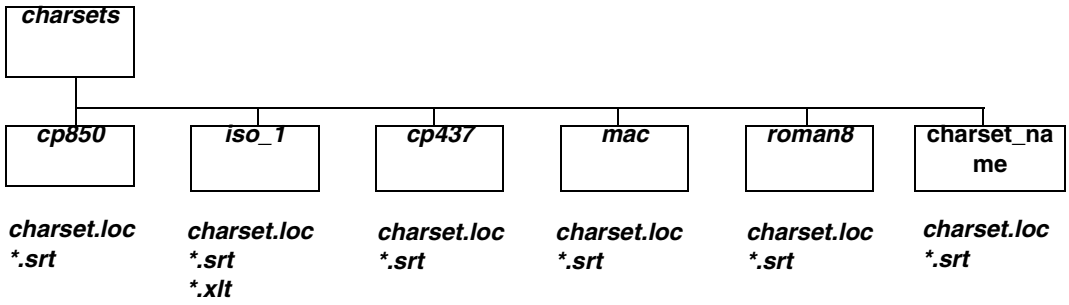
**Avertissement !** Ne modifiez pas les fichiers d'internationalisation. Si vous devez installer une nouvelle définition de terminal ou un nouvel ordre de tri, contactez votre revendeur Sybase ou votre distributeur le plus proche.

## Structure des répertoires de jeux de caractères

La figure 7-3 affiche la structure des répertoires pour les jeux de caractères d'Europe de l'Ouest accompagnant Adaptive Server. Il existe un sous-répertoire distinct pour chaque jeu de caractères dans le répertoire *charsets*. Le sous-répertoire de chaque jeu de caractères (par exemple, *cp850*) contient les fichiers de définition de l'ordre de tri et des jeux de caractères, ainsi que les fichiers propres aux terminaux.

Si vous chargez des jeux de caractères supplémentaires, ceux-ci apparaissent également dans le répertoire *charsets* :

***Figure 7-3 : Structure du répertoire charsets***




Les variables globales suivantes contiennent des informations sur les jeux de caractères.

| | |
|---|---|
| @@*char_convert* | Contient 0 si la conversion des jeux de caractères est désactivée. Contient 1 si elle est activée. |
| @@*client_csname* | Contient le nom du jeu de caractères client. Possède la valeur NULL si ce jeu n'a jamais été initialisé ; sinon, contient le nom du jeu de caractères utilisé pour la connexion. |
| @@*client_csid* | ID du jeu de caractères du client. Possède la valeur -1 si ce jeu n'a jamais été initialisé ; sinon, contient l'ID du dernier jeu du client issu de syscharsets pour la connexion. |
| @@*maxcharlen* | Contient la longueur maximale, en octets, d'un caractère du jeu de caractères par défaut d'Adaptive Server. |
| @@*ncharsize* ou @@*charsize ?* | Longueur maximale, en octets, d'un jeu de caractères du jeu de caractères par défaut du serveur actif. |
| @@*unicharsize* | Egal à 2. |

## Types des fichiers de localisation

Adaptive Server comprend plusieurs fichiers de localisation pour chaque module de langue, comme illustré dans le tableau 7-9.

***Tableau 7-9 : Fichiers de localisation***

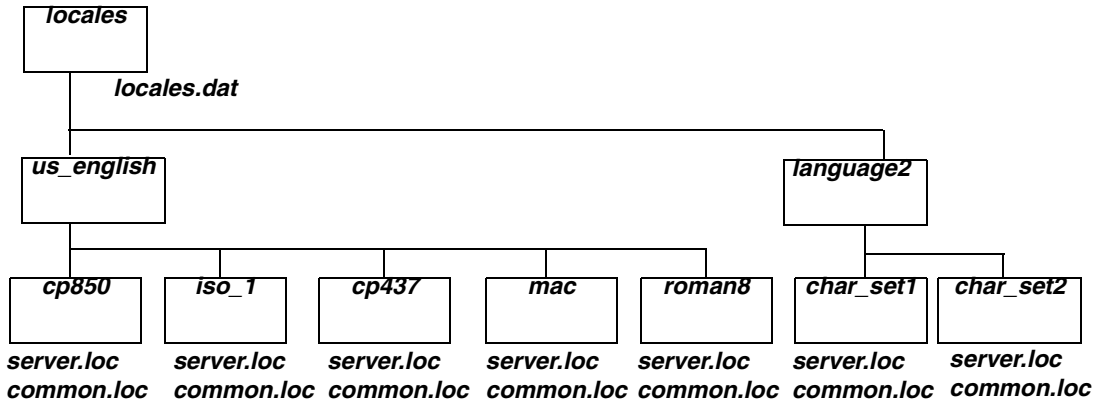
| Fichier | Emplacement | Objectif et contenu |
|---|---|---|
| *locales.dat* | Dans le répertoire *locales* | Utilisé par les applications du client pour identifier la langue des messages et le jeu de caractères par défaut. |
| *server.loc* | Dans les sous-répertoires des jeux de caractères sous chaque sous-répertoire de langues dans le répertoire *locales* | Messages logiciels traduits dans la langue locale. Les produits Sybase possèdent des fichiers **.loc* propres aux produits. Si une entrée n'est pas traduite, ce message ou cette chaîne du logiciel apparaît en anglais américain et non dans la langue locale. |
| *common.loc* | Dans chaque répertoire de jeux de caractères et de langues du répertoire *locales* | Contient les noms locaux des mois de l'année et leurs abréviations ainsi que des informations sur les formats de date, d'heure et de devise locaux. |

**Avertissement !** Ne modifiez pas les fichiers de localisation. Si vous devez modifier des informations dans ces fichiers, contactez votre revendeur Sybase ou votre distributeur le plus proche.

## Structure des répertoires de messages logiciels

La figure 7-4 montre le mode d'organisation des fichiers de localisation. Le répertoire *locales* contient un sous-répertoire pour chaque langue installée. Il existe toujours un sous-répertoire *us_english*. (Sur les plates-formes PC, ce répertoire s'appelle *english*.) Lorsque, pendant l'installation, vous êtes invité à sélectionner les langues à installer sur Adaptive Server, le programme d'installation répertorie les langues de messages logiciels supportées. Si vous installez les modules de langue concernant des langues supplémentaires, des sous-répertoires s'affichent pour ces langues. Chaque langue contient des sous-répertoires pour les jeux de caractères supportée, par exemple, *cp850* est un jeu de caractères supporté pour *us_english*. Les fichiers de messages logiciels de chaque produit Sybase résident dans les sous-répertoires des jeux de caractères.

***Figure 7-4 : structure des répertoires de messages***




## Langues des messages et variables globales

Les variables globales suivantes contiennent des informations sur les langues :

| | |
|---|---|
| @@*langid* | Contient l'ID de la langue locale utilisée (spécifié dans syslanguages.langid). |
| @@*language* | Contient le nom de la langue utilisée, tel qu'il est spécifié dans syslanguages.name. |

CHAPITRE 8

# Configuration des conversions de jeux de caractères entre clients et serveur

Ce chapitre décrit la procédure de configuration de la conversion des jeux de caractères pour les clients utilisant un jeu de caractères différent de celui d'Adaptive Server.

Les sujets abordés dans ce chapitre sont les suivants :



## Conversion de jeux de caractères dans Adaptive Server

En environnement hétérogène, Adaptive Server peut devoir communiquer avec des clients s'exécutant sur des plates-formes qui font appel à des jeux de caractères différents. Deux jeux de caractères peuvent supporter la même langue (par exemple, ISO 8858-1 et CP 850 supportent les langues du groupe 1), mais coder différemment les caractères. Par exemple, avec ISO 8859-1, le caractère *à* est codé *0xE0* en hexadécimal, mais codé *0x85* en hexadécimal avec CP 850.

Pour assurer l'intégrité des données entre les clients et les serveurs, il faut convertir les jeux de caractères. Le but est qu'un "a" demeure un "a", même si l'on change de machine et de jeu de caractères. Ce processus s'appelle la *conversion des jeux de caractères*.

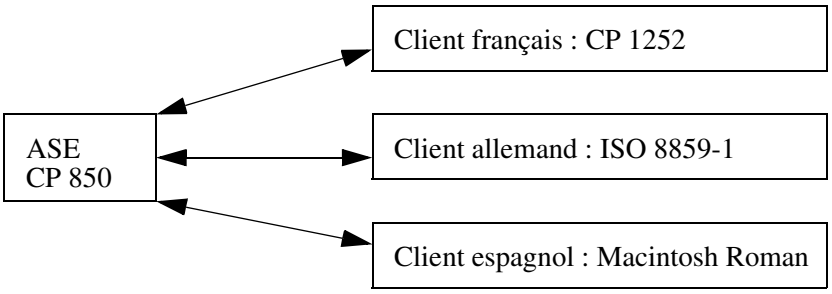
# Conversions de jeux de caractères supportés

La conversion s'effectue entre deux jeux de caractères. Les conversions supportées par un système client/serveur donné dépendent du jeu de caractères utilisé par le serveur et ses clients. Le type de conversion diffère selon que le serveur utilise un jeu de caractères par défaut natif ou Unicode UTF-8.

## Conversion de jeux de caractères natifs

Adaptive Server supporte la conversion entre jeux de caractères natifs relevant du même groupe de langues. Si le serveur dispose d'un jeu de caractères natif par défaut, les jeux de caractères du client doivent appartenir au même groupe de langues. La figure 8-1 donne un exemple d'un système client/serveur pour l'Europe occidentale. Dans cet exemple, les jeux de caractères du client et le jeu de caractères par défaut d'Adaptive Server appartiennent tous deux au Groupe 1. Les données sont correctement converties entre les jeux de caractères du client et celui du serveur. Appartenant tous au même groupe de langues, les clients peuvent afficher toutes les données sur le serveur, quel qu'en soit l'expéditeur.

***Figure 8-1 : Conversion de jeux de caractères client/serveur appartenant au même groupe de langues***

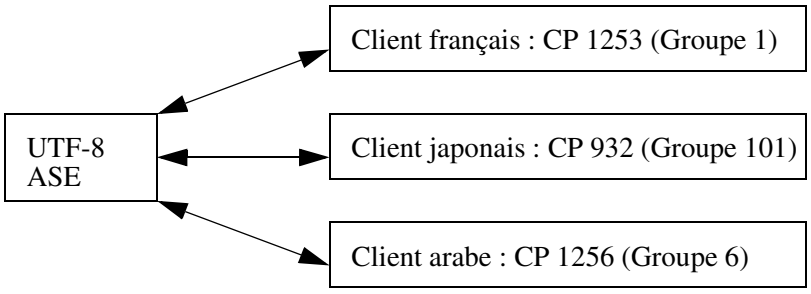



Pour obtenir la liste des groupes de langues et des jeux de caractères supportés, reportez-vous à "Langues et jeux de caractères supportés", page 289.

## Conversion dans un système Unicode

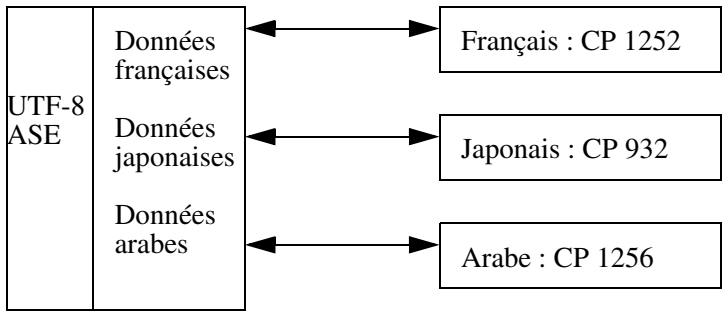
Adaptive Server supporte également la conversion de jeux de caractères entre UTF-8 et n'importe quel jeu de caractères natif supporté par Sybase. Le jeu de caractères par défaut du serveur en système Unicode étant UTF-8, le jeu de caractères du client peut être un jeu natif de n'importe quel groupe de langues. De ce fait, des clients japonais (groupe 101), français (groupe 1) et arabe (groupe 6) peuvent tous envoyer et recevoir des données du même serveur. Les données de chaque client sont correctement converties lors du passage du client au serveur.

***Figure 8-2 : Conversion des jeux de caractères en système Unicode***




A noter toutefois que le client ne peut afficher les données que dans la langue supportée par son jeu de caractères. Par conséquent, le client japonais peut voir n'importe quelles données en japonais sur le serveur, mais pas celles en arabe ou en français. De la même manière, le client français peut voir du français ou n'importe quelle langue européenne supportée par son jeu de caractères, mais ni le japonais, ni l'arabe.

***Figure 8-3 : Affichage des données Unicode***



ASCII 7 est un sous-ensemble de *tous* les jeux de caractères, y compris Unicode. De ce fait, il est compatible avec tous les jeux de caractères de tous les groupes de langues. Si le jeu de caractères d'Adaptive Server ou du client est en ASCII 7, tous les caractères ASCII codés sur 7 bits passent du client au serveur sans qu'une conversion soit nécessaire.

Sybase déconseille de configurer un serveur pour ASCII-7, mais vous pouvez obtenir les mêmes avantages de compatibilité en contraignant chaque client à n'utiliser que les 128 premiers caractères de chaque jeu de caractères natif.

# Types de conversions de jeux de caractères

Sur Adaptive Server, la conversion de jeux de caractères s'implémente de deux manières :

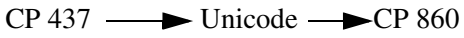
- conversions directes par Adaptive Server,
- conversions Unicode.

## Conversions directes par Adaptive Server

Les conversions directes d'Adaptive Server supportent les conversions entre deux jeux de caractères natifs du *même* groupe de langues. Par exemple, Adaptive Server supporte la conversion entre CP 437 et CP 850, car tous deux appartiennent au groupe de langue 1. Les conversions directes d'Adaptive Server sont possibles entre de nombreux jeux de caractères natifs d'un groupe de langues, mais pas tous (voir le tableau 8-1, page 322).

## Conversions Unicode

Les conversions Unicode sont possibles pour tous les jeux de caractères natifs. Lors de la conversion d'un jeu de caractères natif à un autre, Unicode sert de jeu de caractères intermédiaire. Par exemple, pour passer du jeu de caractères par défaut du serveur (CP 437) au jeu de caractères du client (CP 860), CP 437 est d'abord converti en Unicode, qui est à son tour converti en CP 860.




Comme l'illustre cet exemple, les conversions Unicode s'utilisent lorsque le jeu de caractères par défaut du serveur est, soit UTF-8, soit natif. Vous devez configurer votre serveur à l'utilisation des conversions Unicode (à moins que le jeu de caractères par défaut du serveur ne soit UTF-8).

Les versions antérieures d'Adaptive Server ont recours aux conversions directes, qui constituent la méthode par défaut des conversions de jeux de caractères. Néanmoins, les conversions Unicode implémentées dans les versions récentes d'Adaptive Server facilitent et simplifient l'opération. Sybase continue de supporter les conversions directes existantes d'Adaptive Server, mais il fait également appel aux conversions Unicode pour supporter entièrement la conversion de tous les jeux de caractères. Sybase n'envisage pas d'ajouter de nouvelles conversions directes.

# Choix du type de conversion

Pour connaître les options de conversion de votre système client/serveur, reportez-vous au tableau 8-1, page 322.

## Systèmes client/serveur non-Unicode

Dans un système non-Unicode, les jeux de caractères du serveur et des clients étant natifs, vous pouvez utiliser les conversions directes d'Adaptive Server.

Néanmoins, en l'absence d'une conversion directe Adaptive Server, vous devez utiliser les conversions Unicode.

- Si tous les jeux de caractères de votre système client/serveur relèvent de la colonne 1 du tableau 8-1, utilisez les conversions directes d'Adaptive Server. Les jeux de caractères doivent tous appartenir au même groupe de langues.
- Si les jeux de caractères de votre système client/serveur relèvent de la colonne 2 du tableau 8-1 ou d'une combinaison des colonnes 1 et 2, vous *devez* configurer votre serveur pour qu'il fasse appel à des conversions Unicode. Là encore, les jeux de caractères doivent tous appartenir au même groupe de langues.

Par exemple, si le jeu de caractères par défaut du serveur est CP 850 et celui du client, soit ISO 8859-1, soit ROMAN 8, le tableau 8-1 indique que la conversion directe est possible. En revanche, si vous ajoutez un client utilisant le jeu CP 1252 à cette configuration, comme il n'existe pas de conversion directe entre CP 1252 et CP 850 (le jeu de caractères par défaut du serveur), vous *devez* utiliser les conversions Unicode pour passer de CP 1252 à CP 850. Lorsque vous disposez d'une combinaison de jeux de caractères – certains pour lesquels vous pouvez utiliser les conversions Adaptive Server directes et d'autres pour lesquels vous devez utiliser les conversions Unicode – vous pouvez spécifier l'utilisation d'une combinaison de conversions Adaptive Server directes et de conversions Unicode.

## Systèmes client/serveur Unicode

Si le jeu par défaut de votre serveur est Unicode UTF-8, toutes les conversions se font entre UTF-8 et le jeu de caractères natif utilisé sur les systèmes clients. Par conséquent, un système Unicode utilise *exclusivement* les conversions Unicode.

***Tableauau 8-1 : Méthodes de conversion des jeux de caractères***

| | **Colonne 1** | **Colonne 2** |
|---|---|---|
| **Groupe de langues** | **Conversions Adaptive Server directes et conversions Unicode** | **Conversions Unicode seulement** |
| Groupe 1 | CP 437, CP 850, ISO 8859-1, Macintosh Roman, ROMAN8 | CP 860, CP 1252, ISO 8859-15, CP 863 |
| Groupe 2 | CP 852, CP 1250, CP 8859-1, Macintosh Central European | ISO 8859-2 |
| Groupe 4 | Conversions non nécessaires (un seul jeu de caractères supporté) | |
| Groupe 5 | CP 855, CP 866, CP 1251, ISO 8859-5, Koi8, Macintosh Cyrillic | |

| | Colonne 1 | Colonne 2 |
|---|---|---|
| **Groupe de langues** | **Conversions Adaptive Server directes et conversions Unicode** | **Conversions Unicode seulement** |
| Groupe 6 | | CP 864, CP 1256, ISO 8859-6 |
| Groupe 7 | CP 869, CP 1253, GREEK8, ISO 8859-7, Macintosh Greek | |
| Groupe 8 | | CP 1255, ISO 8859-8 |
| Groupe 9 | CP 857, CP 1254, ISO 8859-9, Macintosh Turkish, TURKISH8 | |
| Groupe 101 | DEC Kanjii, EUC-JIS, Shift-JIS | CP 932 |
| Groupe 102 | | CP 936, EUG-GB |
| Groupe 103 | | Big 5, CP 950, EUC-CNS |
| Groupe 104 | Conversions non nécessaires (un seul jeu de caractères supporté) | |
| Groupe 105 | | CP 874, TIS 620 |
| Groupe 106 | Conversions non nécessaires (un seul jeu de caractères supporté) | |
| Unicode | Conversions non nécessaires (un seul jeu de caractères supporté) | |

## Configuration du serveur

Par défaut, Adaptive Server utilise les conversions directes pour passer les données d'un jeu de caractères à un autre. Pour utiliser les conversions Unicode, vous devez configurer le serveur à l'aide de la commande sp_configure. Définissez l'option enable unicode conversions sur 1 ou 2.

- Si vous définissez sp_configure "enable unicode conversions" sur 1 :

  Cette valeur active les conversions Adaptive Server directes ou les conversions Unicode. Adaptive Server vérifier d'abord s'il existe une conversion directe pour le jeu de caractères du serveur et du client. Si c'est le cas, il s'en sert ; sinon, il utilise la conversion Unicode.

  Choisissez cette valeur si les jeux de caractères de votre système client/serveur entrent dans les colonnes 1 et 2 du tableau 8-1.

- Si vous définissez sp_configure "enable unicode conversions" sur 2 :

  Cette valeur active les conversions Unicode. Adaptive Server se sert des conversions Unicode sans rechercher la conversion directe d'Adaptive Server.

  Choisissez cette valeur si les conversions client/serveur modifient la longueur des données (pour plus d'informations, reportez-vous à la section "Conversions et modification de la longueur des données", page 327).

Si tous les jeux de caractères relèvent de la colonne 2 du tableau 8-1, vous devez définir enable unicode conversions sur 2 pour vous servir en permanence des conversions Unicode.

Si le jeu par défaut du serveur est UTF-8, il n'utilise automatiquement que les conversions Unicode.

# Activation et désactivation de la conversion des jeux de caractères

Lors de la requête de connexion, le client indique à Adaptive Server le jeu de caractères qu'il emploie. Adaptive Server le compare à son propre jeu de caractères par défaut ; si les deux noms sont identiques, aucune conversion n'intervient. Sinon, Adaptive Server vérifie s'il supporte la conversion entre son propre jeu de caractères par défaut et celui du client. Si ce n'est pas le cas, il envoie un message d'erreur au client, poursuit le processus de connexion et la conversion du jeu de caractères est activée automatiquement. Si le jeu de caractères par défaut du serveur est UTF-8, il fait automatiquement appel aux conversions Unicode. Si le jeu par défaut est un jeu de caractères natif, le serveur fait appel aux conversions directes ASE, sauf si l'utilisateur spécifie d'utiliser les conversions Unicode.

Vous pouvez désactiver la conversion des jeux de caractères au niveau du serveur. Cela peut s'avérer utile dans les cas suivants :

- tous vos clients utilisent un jeu de caractères identique au jeu de caractères par défaut du serveur ; aucune conversion n'est nécessaire ;
- la conversion entre le jeu de caractères du client et le jeu de caractères par défaut du serveur n'est pas supportée ;

- vous souhaitez stocker des données dans le serveur sans les convertir, autrement dit, sans en modifier le codage.

Pour désactiver la conversion des jeux de caractères au niveau du serveur, définissez le paramètre disable character set conversion sur 1. La connexion des clients au serveur n'activera aucune conversion. Ce paramètre est défini par défaut sur 0 (conversion activée).

Vous pouvez également contrôler la conversion des jeux de caractères au niveau de la connexion à l'aide de la commande set char_convert depuis une session client. set char_convert off désactive la conversion entre un client donné et le serveur. Si le client et le serveur utilisent le même jeu de caractères, ce qui rend la conversion inutile, vous pouvez utiliser la commande set char_convert off. set char_convert on réactive la conversion.

## Caractères impossibles à convertir

Au cours de la conversion, certains caractères ne peuvent pas être convertis. Deux causes sont possibles :

- Le caractère existe (est codé) dans le jeu de caractères source mais pas dans le jeu cible. Par exemple, la ligature OE fait partie du jeu de caractères Macintosh (code point 0xCE). Ce caractère n'existe pas dans le jeu de caractères ISO 8859-1. La présence d'une ligature OE dans des données converties du jeu de caractères Macintosh vers le jeu ISO 8859-1 génère une erreur de conversion.
- Le caractère existe dans les jeux source et cible, mais dans ce dernier il est représenté par un nombre d'octets différent.

  Par exemple, les caractères accentués codés sur 1 octet (tels que á et è) sont codés sur 2 octets dans UTF-8, les caractères thaïs codés sur 2 octets sont codés sur trois octets dans UTF-8. Pour éviter ces contraintes, configurez l'option enable unicode conversion sur 1 ou 2.

# Traitement des erreurs de conversion de jeux de caractères

Les filtres de conversion de jeux de caractères d'Adaptive Server signalent des erreurs de conversion lorsqu'un caractère existe dans le jeu de caractères du client mais pas dans celui du serveur ou réciproquement. Adaptive Server doit garantir que les données converties en entrée sur le serveur peuvent de nouveau être converties dans le jeu de caractères du client lorsque celui-ci les extrait. Pour que cette opération soit réalisable, Adaptive Server doit éviter de placer des données "suspectes" dans la base de données.

Lorsqu'Adaptive Server rencontre une erreur de conversion dans les données entrées, il génère le message d'erreur suivant :

```
Msg 2402, Severity 16 (EX_USER):
Erreur lors de la conversion du jeu de caractères
client en jeu de caractères serveur. Certains
caractères risquent de ne pas être convertis.
```

Une erreur de conversion empêche l'exécution de la requête sur les déclarations insert et update. Si cela se produit, repérez et supprimez les caractères posant problème.

Lorsqu'Adaptive Server rencontre une erreur de conversion lors de l'envoi de données au client, il remplace les octets des caractères suspects par des points d'interrogation ASCII (?). Cela n'empêche pas le batch de la requête de se poursuivre jusqu'à achèvement. A l'issue de l'instruction, Adaptive Server envoie le message suivant :

```
Msg 2403, Severity 16 (EX_INFO):
AVIS! Certains caractères n’ont pu être convertis
dans le jeu de caractères client. Les octets non
convertis ont été transformés en points
d’interrogation ('?').
```

# Conversions et modification de la longueur des données

Dans certains cas, la conversion des données entre le jeu de caractères du serveur et celui du client modifie la longueur des données. Cela se produit, par exemple, lorsque le jeu de caractères d'un système utilise un octet pour représenter chaque caractère et celui de l'autre système en utilise deux.

Lorsque la conversion des jeux de caractères modifie la longueur des données, deux cas de figure sont possibles :

- La longueur des données diminue, comme dans les exemples suivants :
  - grec ou russe en UTF-8 codé sur plusieurs octets vers grec ou russe codé sur un seul octet
  - caractères japonais Hankaku Katakana codés sur deux octets en EUC-JIS vers caractères codés sur un octet en Shift-JIS
- La longueur des données augmente, comme dans les exemples suivants :
  - thaï codé sur un seul octet vers Thaï codé sur plusieurs octets en UTF-8
  - Caractères japonais codés sur un octet en Shift-JIS vers Hankaku Katakana codé sur deux octets en EUC-JIS

## Configuration de votre système et de l'application

Si vous utilisez UTF-8 à un endroit quelconque de votre système client/serveur ou si vous utilisez un jeu de caractères japonais, il est probable que la conversion des jeux de caractères modifiera la longueur des données. Si c'est le cas, vous devez configurer votre serveur pour qu'il traite ces modifications. Cela peut nécessiter la reconfiguration de votre client pour qu'il traite les changements de longueur des données.

1 Configurez le serveur pour qu'il utilise les conversions Unicode. Pour plus d'informations, reportez-vous à la section "Configuration du serveur", page 323. Si la longueur des données augmente entre le serveur et le client, il faut également effectuer les étapes 2 et 3.

2 Le client doit exécuter Open Client 11.1 ou une version ultérieure. Lors de la connexion, il doit informer le serveur qu'il est capable de traiter les données CS_LONGCHAR à l'aide de la fonction Open Client ct_capability.

   Il faut définir le paramètre *capability* sur CS_DATA_LCHAR et le paramètre *value* sur CS_TRUE :

```
CS_INT capval = CS_TRUE
ct_capability(connexion,CS_SET,CS_CAP_RESPONS,
     CS_DATA_LCHAR,&capval)
```

   où *connexion* joue le rôle de pointeur vers une structure CS_CONNECTION.

3 Lorsque les conversions allongent les données, les données char et varchar sont converties au jeu de caractères du client et envoyées au client sous forme de données CS_LONGCHAR. L'application cliente doit être codée pour extraire les données reçues sous cette forme.

# Spécification du jeu de caractères des utilitaires

Les utilitaires Sybase supposent que le jeu de caractères par défaut de la plate-forme du client est identique à celui qu'utilise le client, ce qui n'est pas toujours le cas. C'est pourquoi il se peut que vous deviez spécifier le jeu de caractères du client dans la ligne de commande. La conversion des jeux de caractères peut être contrôlée dans les utilitaires autonomes. Une option de ligne de commande des utilitaires isql, bcp et defncopy spécifie le jeu de caractères du client et se substitue temporairement aux paramètres de la variable LANG ou à ceux de *locales.dat*.

-J *nom_jeu_car* (UNIX et PC) définit le jeu de caractères du client sur *nom_jeu_car*.

En cas d'omission de la balise de la ligne de commande du jeu de caractères du client, le jeu de caractères par défaut de la plate-forme est utilisé. Reportez-vous au manuel *Utilitaires* pour en savoir plus.

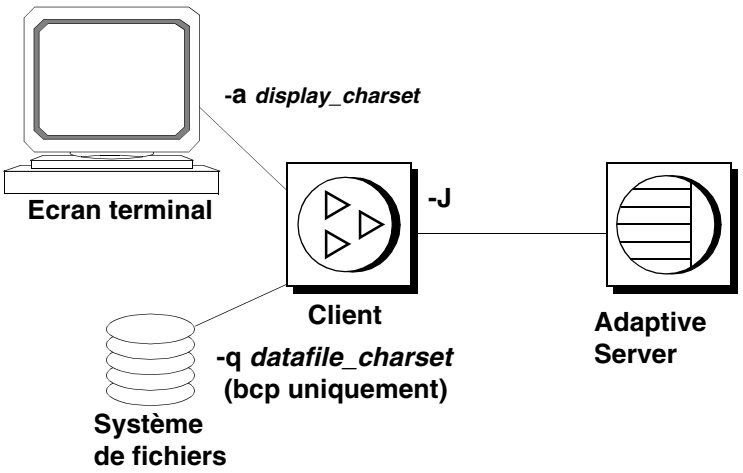
# Options d'affichage et de jeu de caractères de fichiers des lignes de commande

Bien que ce chapitre traite avant tout de la conversion des jeux de caractères entre les clients et Adaptive Server, celle-ci peut s'avérer nécessaire à deux autres endroits :

- entre le client et le terminal,
- entre le client et un système de fichiers.

La figure 8-4 illustre les chemins d'accès et les options de ligne de commande disponibles dans les utilitaires autonomes isql, bcp et defncopy.

***Figure 8-4 : Cas de conversion de jeu de caractères***




Comme décrit plus haut, l'option de ligne de commande -J ou /clientcharset spécifie le jeu de caractères utilisé par le client lorsque celui-ci échange des données de type caractères avec Adaptive Server.

## Configuration du jeu de caractères de l'écran

Utilisez l'option de ligne de commande -a si vous exécutez le client à partir d'un terminal dont le jeu de caractères diffère de celui du client. Dans la figure 8-4, les options -a et -J sont utilisées conjointement pour identifier le fichier de conversion de jeux de caractères (fichier *.xlt*).

N'utilisez -a sans -J que si le jeu de caractères du client est identique au jeu de caractères par défaut.

## Configuration du jeu de caractères des fichiers

Utilisez l'option de ligne de commande -q si vous exécutez bcp pour copier des données de caractères depuis ou vers un système de fichiers dont le jeu de caractères diffère de celui du client. Dans la figure 8-4, exécutez l'option -q ou /filecharset et l'option -J ou /clientcharset conjointement pour identifier le fichier de conversion des jeux de caractères (*.xlt*) requis.

CHAPITRE 9

# Administration de la sécurité

Ce chapitre présente les fonctions de sécurité disponibles dans Adaptive Server.

Les sujets traités dans ce chapitre sont les suivants :



## Fonctions de sécurité disponibles dans Adaptive Server

SQL Server version 11.0.6 a été jugé conforme par l'organisme National Security Agency (NSA) aux critères de la Classe C2. Ces critères sont exposés dans un document établi par le DOD (Department of Defense) et appelé "Orange Book" : DOD 52.00.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria* [TCSEC].

La configuration de SQL Server version 11.0.6, qui a fait l'objet d'une évaluation au niveau de sécurité C2 par la NSA en 1996 sur la plate-forme HP 9000 HP-UX BLS, 9.09+, est désignée par l'expression configuration évaluée. Certaines fonctions de SQL Server, comme les procédures distantes et les mises à jour directes des tables système, ont été exclues de la configuration évaluée. Elles sont signalées par des notes insérées dans la documentation d'Adaptive Server. Pour obtenir une liste complète des fonctions exclues de la configuration évaluée, reportez-vous à l'annexe A du document *SQL Server Installation and Configuration Guide for HP 9000 HP-UX BLS, 9.09+*.

Adaptive Server version 11.5 contient toutes les fonctions de sécurité figurant dans SQL Server version 11.0.6 ainsi que d'autres fonctions nouvelles. Le tableau 9-1 résume les principales fonctions.

***Tableau 9-1 : Principales fonctions de sécurité***

| Fonction de sécurité | Description |
|---|---|
| DAC (Discretionary Access Controls, contrôles d'accès discrétionnaires) | Des contrôles d'accès permettent aux propriétaires d'objets de limiter l'accès à certains objets, en général avec des commandes d'octroi et de révocation des autorisations grant et revoke. Ce type de contrôle est laissé à la discrétion des propriétaires d'objets. |
| Contrôle d'identification et d'authentification | Seuls des utilisateurs autorisés peuvent se connecter au système. |
| Division des rôles | Cette fonction permet d'octroyer des rôles privilégiés à des utilisateurs afin que seuls ceux qui sont désignés puissent exécuter certaines tâches. Adaptive Server propose des rôles prédéfinis, appelés "rôles système", par exemple Administrateur système (SA) ou Responsable de la sécurité du système (SSO). De plus, Adaptive Server permet aux responsables de la sécurité du système de définir des rôles supplémentaires appelés "rôles utilisateur". |
| Sécurité réseau | Des services de sécurité permettent d'authentifier les utilisateurs et de protéger les données transmises d'une machine à l'autre sur le réseau. |
| Audit | Cette fonction permet d'effectuer un audit des événements, comme les connexions, les déconnexions, les initialisations du serveur, les appels de procédures distantes, les accès aux objets de base de données et toutes les actions exécutées par un utilisateur spécifique ou possédant un rôle particulier. De plus, Adaptive Server offre une option unique pour auditer tout un ensemble d'événements liés à la sécurité au niveau serveur. |

# Procédure générale d'administration de la sécurité

Le tableau 9-2 décrit les principales tâches requises pour administrer la sécurité d'accès dans Adaptive Server et vous renvoie à la documentation qui explique comment réaliser ces tâches.

***Tableau 9-2 : Procédure générale d'administration du système***

| Tâche | Description | Voir |
|---|---|---|
| 1. Installer Adaptive Server, y compris la fonction d'audit. | Cette tâche inclut l'installation, le chargement des fichiers à partir de leur support, l'installation proprement dite et la gestion des ressources physiques nécessaires. | Le Guide d'installation pour votre plate-forme |
| 2. Configurer un environnement administratif sécurisé. | Cette tâche inclut l'activation de la fonction d'audit, l'octroi de rôles aux utilisateurs pour permettre un suivi individuel et l'attribution de noms de login aux administrateurs système et aux responsables de la sécurité du système. | Chapitre 10, "Gestion des connexions et des utilisateurs de bases de données Adaptive Server" |
| 3. Ajouter des logins utilisateur dans le serveur, ajouter des utilisateurs dans la base de données, établir des groupes et des rôles, définir des procurations. | Cette tâche inclut l'ajout de logins, la création de groupes, l'ajout d'utilisateurs dans les bases de données, la suppression et le verrouillage des logins et l'attribution de mots de passe initiaux. Elle inclut également l'attribution des rôles aux utilisateurs, la création des rôles utilisateur et la définition de la hiérarchie des rôles ainsi que les règles d'exclusion mutuelle. | Chapitre 10, "Gestion des connexions et des utilisateurs de bases de données Adaptive Server" |
| 4. Administrer les autorisations relatives aux utilisateurs, aux groupes et aux rôles. | Cette tâche inclut l'octroi et la révocation des autorisations pour certaines commandes SQL, l'exécution de certaines procédures système et l'accès aux bases de données, aux tables, aux colonnes de table spécifiques et aux vues. | Chapitre 11, "Gestion des autorisations utilisateur" |
| 5. Administrer l'utilisation des serveurs distants. | Cette tâche inclut la mise en place et l'administration des accès autorisés entre les serveurs, l'ajout et la suppression d'accès aux serveurs distants et le mappage des noms de login distants sur les noms de login locaux. | Chapitre 13, "Gestion des serveurs distants" et la documentation relative à l'installation et à la configuration d'Adaptive Server de votre plate-forme |
| 6. Configurer et gérer la fonction d'audit. | Cette tâche consiste à déterminer les éléments à auditer, contrôler l'utilisation faite d'Adaptive Server et utiliser la trace d'audit pour détecter les accès frauduleux au système et la mauvaise utilisation des ressources. | Chapitre 12, "Audit" et la documentation relative à l'installation et à la configuration d'Adaptive Server pour votre plate-forme |
| 7. Configurer votre installation pour des services de sécurité réseau. | Cette tâche inclut la configuration du serveur afin qu'il utilise certains services (comme l'unification des logins, le cryptage des données pour en assurer la confidentialité, l'intégrité des données) et l'évaluation des besoins en sécurité pour les procédures distantes. | Chapitre 14, "Utilisation de Kerberos, DCE et Windows NT LAN Manager" |

# Recommandations pour la configuration de la sécurité

Pour configurer la sécurité dans Adaptive Server, reportez-vous aux recommandations formulées dans les sections suivantes.

## Utilisation du login "sa"

Lorsqu'Adaptive Server est installé, un login unique, "sa", est défini avec les rôles d'administrateur système (SA) et de responsable de la sécurité du système (SSO). Ceci signifie que le login "sa" dispose de tous les pouvoirs.

N'utilisez le login "sa" que durant la configuration initiale. Par la suite, au lieu d'autoriser plusieurs utilisateurs à se servir du compte "sa", mettez en place une stratégie de traçabilité des utilisateurs en attribuant des rôles spécifiques à chacun des administrateurs.

---

**Avertissement !** Lors de la connexion à Adaptive Server, n'utilisez pas l'option `-P` d'`isql` pour spécifier votre mot de passe car un autre utilisateur pourrait le voir.

---

## Modification du mot de passe du login "sa"

Le login "sa" est configuré au départ avec un mot de passe "NULL". Utilisez la procédure `sp_password` pour le modifier, immédiatement après l'installation.

## Cas d'activation de la fonction d'audit

Activez l'audit au tout début du processus d'administration afin de disposer d'un enregistrement des commandes privilégiées qui sont exécutées par les responsables de la sécurité du système et par les administrateurs système. Vous pouvez également auditer les commandes qui sont exécutées par les utilisateurs possédant certains rôles spéciaux, comme les opérateurs lorsqu'ils sauvegardent et chargent des bases de données.

## Attribution de noms de login

Attribuez des noms de login Adaptive Server identiques aux noms de login du système d'exploitation correspondant. Ceci facilite la connexion à Adaptive Server, simplifie la gestion des comptes ou logins du serveur et du système d'exploitation et permet une meilleure corrélation entre les données d'audit générées par Adaptive Server et celles du système d'exploitation.

# Exemple de configuration de la sécurité

Supposons que vous ayez décidé d'attribuer des rôles spéciaux aux utilisateurs ci-dessous (tableau 9-3).

***Tableau 9-3 : Utilisateurs auxquels vous attribuez des rôles***

| Nom | Rôle | Nom de login du système d'exploitation |
|---|---|---|
| Rajnish Smith | sso_role | rsmith |
| Catharine Macar-Swan | sa_role | cmacar |
| Soshi Ikedo | sa_role | sikedo |
| Julio Rozanski | oper_role | jrozan |

Le tableau 9-4 répertorie l'ensemble des commandes à utiliser pour configurer un environnement d'exploitation sécurisé pour Adaptive Server, en attribuant des rôles comme indiqué dans le Tableau 5-3. Après vous être connecté au système d'exploitation, exécutez les commandes en utilisant le compte "sa" initial.

***Tableau 9-4 : Exemples de commandes utilisées pour configurer la sécurité***

| Commandes | Résultat |
|---|---|
| isql -Usa | Vous connecte à Adaptive Server en tant que "sa". Les rôles sa_role et sso_role sont tous les deux actifs. |
| sp_audit "security", "all", "all", "on"<br><br>sp_audit "all", "sa_role", "all", "on"<br><br>sp_audit "all", "sso_role", "all", "on"' | Définit les options d'audit pour les événements liés à la sécurité au niveau serveur, ainsi que l'audit de toutes les actions pour lesquelles les rôles sa_role ou sso_role sont actifs. |

| Commandes | Résultat |
|---|---|
| sp_configure "auditing", 1 | Active l'audit.<br><br>Remarque : Avant d'activer l'audit, définissez une procédure de seuil pour la trace d'audit et déterminez le mode de gestion du journal de transactions dans sybsecurity. Pour plus d'informations, reportez-vous au chapitre 12, "Audit". |
| sp_addlogin rsmith, js&2P3d,<br>@fullname = "Rajnish Smith"<br><br>sp_addlogin cmacar, Fr3ds#1,<br>@fullname = "Catharine Macar-Swan"<br><br>sp_addlogin sikedo, mi5pd1s,<br>@fullname = "Soshi Ikedo"<br><br>sp_addlogin jrozan, w1seCrkr,<br>@fullname = "Julio Rozanski" | Ajoute des logins et des mots de passe pour Rajnish, Catharine, Soshi et Julio.<br><br>Aucune base de données par défaut n'étant spécifiée pour ces utilisateurs, leur base par défaut sera master. |
| grant role sso_role to rsmith<br><br>grant role sa_role to sikedo<br><br>grant role sa_role to cmacar<br><br>grant role oper_role to jrozan | Octroie le rôle sso_role à Rajnish, le rôle sa_role à Soshi et Catharine et le rôle oper_role à Julio. |
| use sybsecurity<br><br>sp_changedbowner rsmith | Accorde un accès à la base de données d'audit, sybsecurity, en désignant Rajnish, qui est responsable de la sécurité du système, comme le propriétaire de la base de données. |
| sp_locklogin sa,"lock" | Verrouille le login "sa" afin que personne ne puisse se connecter en tant que "sa". Les utilisateurs ne peuvent prendre que les rôles qui ont été configurés pour eux.<br><br>Remarque : Ne verrouillez pas le login "sa" tant que vous n'avez pas octroyé aux utilisateurs les rôles sa_role et sso_role et vérifié qu'ils fonctionnent correctement. |

## Contrôles d'accès discrétionnaires

Les propriétaires d'objets peuvent autoriser certains utilisateurs à accéder à ces objets. Ils peuvent aussi leur accorder le droit de transmettre l'autorisation d'accès à d'autres. Grâce aux contrôles d'accès discrétionnaires d'Adaptive Server, vous pouvez accorder divers types d'autorisations aux utilisateurs, aux groupes et aux rôles en vous servant de la commande grant. Utilisez la commande revoke pour annuler ces autorisations. Les commandes grant et revoke autorisent les utilisateurs à exécuter les commandes spécifiées et à accéder aux tables, aux vues et aux colonnes désignées.

Certaines commandes sont utilisables à tout moment par les utilisateurs, sans autorisation. D'autres ne le sont que par des utilisateurs disposant d'un statut particulier, comme celui d'administrateur système et elles ne sont pas transférables.

La possibilité d'associer à des commandes des autorisations qui peuvent être octroyées et révoquées est fonction du statut de chaque utilisateur (par exemple administrateur système, propriétaire de base de données, propriétaire d'un objet de base de données) ; elle varie aussi selon qu'un utilisateur a le droit ou non de transférer ses autorisations à d'autres personnes.

Les contrôles d'accès discrétionnaires sont présentés au chapitre 11, "Gestion des autorisations utilisateur".

## Contrôle d'identification et d'authentification

A chaque utilisateur d'Adaptive Server est attribué un login de connexion avec un ID unique. Toutes les activités de l'utilisateur sur le serveur peuvent être associées à un ID utilisateur sur le serveur et faire l'objet d'un audit.

Les mots de passe Adaptive Server sont enregistrés dans la table master..syslogins sous une forme cryptée. Lorsque vous vous connectez à Adaptive Server depuis un client, vous pouvez choisir de crypter le mot de passe au niveau client avant de l'envoyer sur le réseau.

Un SSO peut accorder à un utilisateur le droit d'emprunter l'identité d'un autre utilisateur. Cette possibilité appelée **procuration** permet aux administrateurs de vérifier les autorisations d'un utilisateur spécifique ou d'effectuer une opération de maintenance sur les objets de base de données d'un utilisateur. Les serveurs d'applications peuvent se connecter au serveur et exécuter des procédures et des commandes au nom de plusieurs utilisateurs.

## Contrôles d'identification et d'authentification avec la sécurité réseau

Grâce à un mécanisme de sécurité, Adaptive Server permet une authentification préalable des utilisateurs avant qu'ils se connectent au serveur. Il s'agit d'un dispositif appelé **unification des logins** qui permet à un utilisateur de se connecter à plusieurs serveurs sans avoir à fournir chaque fois un nom de login et un mot de passe.

Les contrôles d'identification et d'authentification sont présentés au chapitre 10, "Gestion des connexions et des utilisateurs de bases de données Adaptive Server". Pour plus d'informations, reportez-vous également à la section "Utilisation de la procuration" et au chapitre 13, "Gestion des serveurs distants".

## Division des rôles

Une fonction importante d'Adaptive Server est la division des *rôles*. Les rôles supportés par Adaptive Server vous permettent de mettre en place le principe de traçabilité des utilisateurs. Adaptive Server propose des rôles système (administrateur système et responsable de la sécurité du système) et des rôles utilisateur créés par un responsable de la sécurité du système.

Les rôles permettent de responsabiliser les utilisateurs effectuant des tâches fonctionnelles et administratives. Vous pouvez ainsi contrôler leurs activités et remonter si nécessaire jusqu'à l'auteur de telle ou telle tâche.

### Hiérarchie des rôles

Un responsable de la sécurité du système (SSO) peut hiérarchiser les rôles de sorte que, si un utilisateur possède un rôle, il possède automatiquement ceux qui en dépendent dans la hiérarchie. Par exemple, le rôle "chief_financial_officer" peut contenir deux rôles, "financial_analyst" et "salary_administrator". Ainsi, l'analyste financier principal pourra effectuer toutes les tâches et voir toutes les données des analystes et des gestionnaires de salaire qui lui sont subordonnés.

### Exclusion mutuelle

Il est possible de définir deux rôles qui s'excluent mutuellement au niveau de :

- Affectation : un utilisateur ne peut pas se voir affecter les deux rôles. Par exemple, les rôles "payment_requestor" et "payment_approver" ne pourront pas être accordés tous les deux à un même utilisateur.
- Activation : un utilisateur ne peut pas activer les deux rôles. Par exemple, un utilisateur peut posséder les rôles "senior_auditor" et "equipment_buyer", mais il n'aura pas le droit de les activer en même temps.

Les rôles système, ainsi que les rôles utilisateur, peuvent être définis dans une hiérarchie ou être mutuellement exclusifs. Ainsi, vous définirez un rôle "super_user" qui contiendra les rôles Administrateur système, Opérateur et Support Technique. Par ailleurs, vous indiquerez que les rôles Administrateur système et Responsable de la sécurité du système s'excluent mutuellement au niveau de l'appartenance, de sorte qu'un utilisateur ne pourra pas se voir attribuer les deux rôles.

Pour plus d'informations sur l'administration et l'utilisation des rôles, reportez-vous à la section "Création et attribution de rôles aux utilisateurs", page 382.

## SSL (Secure Sockets Layer) dans Adaptive Server

Dorénavant, les services de sécurité d'Adaptive Server Enterprise supportent la sécurité SSL au niveau de la session. **SSL** est la norme de sécurisation pour la transmission d'informations confidentielles comme les numéros de cartes de crédit, les ventes d'actions et les transactions bancaires via Internet.

Même si le cryptage des clés publiques n'entre pas dans le cadre de ce document, il est utile d'en décrire les bases afin de présenter la manière dont SSL sécurise les voies de communication Internet. Ce document ne constitue pas un guide exhaustif sur le cryptage par clé publique.

L'implémentation des fonctions SSL d'Adaptive Server considèrent qu'il existe un responsable de la sécurité du système ayant des connaissances approfondies des stratégies de sécurité de votre site, de SSL et du cryptage par clé publique.

## Présentation des communications via Internet

Le protocole **TCP/IP** est le protocole de transfert principal utilisé dans les relations client/serveur et il régit la transmission des données via Internet. Le protocole TCP/IP utilise des ordinateurs intermédiaires pour transférer des données de l'expéditeur au destinataire. Les ordinateurs intermédiaires introduisent des faiblesses dans le système de communication par lesquels les données peuvent subir des altérations, des vols, des écoutes électroniques et des usurpations d'identité.

### Cryptage par clé publique

Plusieurs mécanismes, regroupés sous la notion de **cryptage par clé publique**, ont été développés et implémentés pour protéger les données sensibles lors de la transmission via Internet. Le cryptage par clé publique comprend le cryptage, l'échange de clés, les signatures et les certificats électroniques.

#### Cryptage

Le **cryptage** est un processus dans lequel un algorithme de cryptage est utilisé pour encoder des informations pour les préserver de quiconque à l'exception du destinataire prévu. Il existe deux types de clés utilisées pour le cryptage :

- Le **cryptage par clé symétrique** consiste en un algorithme (clé) utilisé à la fois pour le cryptage et le décryptage du message. Cette forme de cryptage offre une sécurité minimale car la clé est simple et, par conséquent, facile à déchiffrer. Cependant, le transfert des données cryptées avec une clé symétrique est rapide car le calcul nécessaire au cryptage et au décryptage du message est réduit.

- Le **cryptage par clé publique/privée**, également appelé clé asymétrique, consiste en une paire de clés créée à partir de composants publics et privés pour crypter et décrypter les messages. En général, le message est crypté par l'expéditeur avec une clé privée et décrypté par le destinataire avec la clé publique de l'expéditeur, mais cela peut varier. Vous pouvez utiliser la clé publique d'un destinataire pour crypter un message et le destinataire utilise alors la clé privée pour décrypter le message.

  L'algorithme utilisé pour créer les clés publiques et privées est plus complexe et, par conséquent, plus difficile à déchiffrer. Cependant, le cryptage par clé publique/privée implique davantage de calcul et envoie plus d'informations, ce qui ralentit considérablement les transferts de données.

### Echange de clés

La solution pour réduire le surcoût en calcul et pour accélérer les transactions sans nuire à la sécurité est d'utiliser une combinaison de clé symétrique et de cryptage par clé publique/privée, ce qui porte le nom d'échange de clés.

Pour les grandes quantités de données, une clé symétrique est utilisée pour crypter le message initial. L'expéditeur envoie soit sa clé privée, soit la clé publique du destinataire pour crypter la clé symétrique. Le message crypté et la clé symétrique cryptée sont envoyés au destinataire. En fonction de la clé utilisée pour crypter le message (publique ou privée), le destinataire utilise le contraire pour décrypter la clé symétrique. Une fois que la clé a été échangée, le destinataire utilise la clé symétrique pour décrypter le message.

### Signatures électroniques

Les **signatures électroniques** sont utilisées pour la détection des altérations et la non-répudiation. Les signatures électroniques sont créées avec un algorithme mathématique qui génère une chaîne de nombres unique et à longueur fixe à partir d'un message sous forme de texte. Le résultat est appelé hachage ou condensé de messages.

Pour assurer l'intégrité des messages, le condensé de messages est crypté avec la clé privée de l'auteur de la signature, puis est envoyé au destinataire avec les informations relatives à l'algorithme de hachage. Le destinataire décrypte le message avec la clé publique de l'auteur de la signature. Ce processus re-génère également le condensé de messages initial. Si le condensé correspond, le message est intact et n'est pas altéré. S'il ne correspond pas, les données ont soit été modifiées pendant le transfert, soit signées par un imposteur.

Par ailleurs, la signature électronique permet la **non-répudiation** : les expéditeurs ne peuvent pas nier (ou répudier) qu'ils ont envoyé un message car c'est leur clé privée qui a crypté le message. Évidemment, si la clé privée a été volée ou déchiffrée, la signature électronique n'a aucune valeur vis-à-vis de la non-répudiation.

### Certificats

Les **certificats** s'apparentent à des passeports : une fois qu'un certificat vous a été affecté, les autorités possèdent toutes les informations d'identification dans le système. Le contrôle d'immigration peut accéder à vos informations lorsque vous vous déplacez d'un pays à l'autre. Tout comme un passeport, le certificat sert à vérifier l'identité d'une entité (serveur, routeur, sites Web etc.) vers une autre.

Adaptive Server utilise deux types de certificats :

- Les **certificats de serveur** : un certificat de serveur authentifie le serveur qui le contient. Les certificats sont émis par une autorité de certification (CA) tierce habilitée. La CA valide l'identité du détenteur et intègre la clé publique de celui-ci et les autres informations d'identification dans le certificat électronique. Les certificats contiennent également la signature électronique de la CA émettrice, en vérifiant l'intégrité des données contenues et en validant leur utilisation.
- Les **certificats de CA** (également appelés **certificats d'origine sécurisés**) constituent une liste de CA habilitées chargée par le serveur au démarrage. Les certificats de CA sont utilisés par les serveurs lorsqu'ils fonctionnent comme client, en cas d'appels de procédures à distance (RPC) par exemple. Adaptive Server charge son certificat d'origine sécurisé au démarrage. Lors de la connexion à un serveur distant pour les RPC, Adaptive Server vérifie que la CA qui a signé le certificat du serveur distant est une CA "habilitée" figurant dans son propre fichier d'origine sécurisé par la CA. Si ce n'est pas le cas, la connexion échoue.

Les certificats sont valides pendant une période donnée et peuvent être révoqués par la CA pour différents motifs (en cas de violation du système de sécurité, par exemple). Si un certificat est révoqué pendant une session, la connexion de la session continue. Les autres tentatives de connexion échouent. De même, lorsqu'un certificat arrive à expiration, les tentatives de connexion échouent.

La combinaison de ces mécanismes protège les données transmises via Internet des écoutes électroniques et de l'altération. Ces mécanismes protègent également les utilisateurs de l'usurpation d'identité dans laquelle une entité prétend en être une autre (mystification) ou bien une personne ou une organisation affirme être configurée pour un but précis alors que l'intention réelle est de se procurer des informations confidentielles (informations trompeuses).

## Présentation de SSL

SSL est un standard permettant d'envoyer des données cryptées via un réseau WAM ou via un socket grâce à des connexions réseau sécurisées.

Avant que la connexion SSL soit établie, le serveur et le client échangent une série de boucles E/S pour négocier une session sécurisée cryptée et s'accorder sur celle-ci. Ce processus porte le nom de négociation SSL.

### Négociation SSL

Lorsqu'un client demande une connexion, le serveur utilisant SSL présente son certificat pour prouver son identité avant la transmission des données. En substance, la négociation comprend les étapes suivantes :

- Le client envoie une demande de connexion au serveur. La demande comprend les options SSL ou TLS (Transport Layer Security) supportées par le client.
- Le serveur renvoie son certificat et la liste des versions de CipherSuites supportées, ce qui inclut les options SSL/TLS, les algorithmes utilisés pour l'échange des clés et les signatures électroniques.
- Une session sécurisée cryptée est établie lorsque le client et le serveur se sont accordés sur une version de CipherSuite.

Pour plus d'informations sur la **négociation SSL** et le protocole SSL/TLS, accédez au site Web d'Internet Engineering Task Force : (http://www.ietf.org).

Pour obtenir une liste des versions de CipherSuites supportées par Adaptive Server, reportez-vous à la section "CipherSuites", page 354.

## SSL dans Adaptive Server

L'implémentation de SSL dans Adaptive Server propose plusieurs niveaux de sécurité.

- Le serveur s'authentifie lui-même (il prouve qu'il est le serveur que vous souhaitez contacter) et une session SSL cryptée est ouverte avant l'envoi des données.
- Une fois la connexion SSL établie, le client qui demande la connexion peut envoyer son nom d'utilisateur et son mot de passe via la connexion sécurisée cryptée.
- La comparaison de la signature électronique du certificat du serveur peut déterminer si les données reçues par le client ont été modifiées avant d'atteindre le destinataire prévu.

Adaptive Server utilise l'API SSL Plus™ Library de Certicom Corp.

### Filtre SSL

Le service de répertoire d'Adaptive Server (fichier d'interface, registre NT ou service LDAP, par exemple) définit l'adresse du serveur et les numéros de ports et détermine les protocoles de sécurité appliqués pour les connexions du client. Adaptive Server implémente le protocole SSL sous forme de filtre concaténé aux lignes master et query des services.

Vous pouvez configurer les adresses et les numéros de ports sur lesquels Adaptive Server accepte les connexions afin que plusieurs protocoles réseau et de sécurité puissent être activés pour un seul serveur. Les attributs des connexions du serveur sont spécifiés avec les services de répertoire (LDAP ou DCE) ou avec le fichier d'interface Sybase classique. Pour plus d'informations, reportez-vous à la section "Création d'entrées de répertoire de serveur", page 350.

Toutes les tentatives de connexions à une entrée master ou query dans le fichier d'interface avec un **filtre SSL** doivent supporter le protocole SSL. Il est possible de configurer un serveur de sorte que celui-ci accepte les connexions SSL et dispose d'autres connexions qui acceptent du texte en clair (données non cryptées) ou utilisent d'autres mécanismes de sécurité.

Par exemple, le fichier d'interface sur UNIX qui supporte les connexions SSL et de texte non crypté se présente ainsi :

```
SYBSRV1
    master tli tcp /dev/tcp \x00020abc123456780000000000000000 ssl
    query tli tcp /dev/tcp \x00020abc123456780000000000000000 ssl
    master tli tcp /dev/tcp \x00020abd12345678000000000000000
```

Le filtre SSL est différent des autres mécanismes (DCE et Kerberos, par exemple) qui sont définis au moyen de lignes SECMECH (mécanisme de sécurité) dans le fichier d'interface (*sql.ini* sous Windows).

## Authentification via le certificat

Le protocole SSL nécessite l'authentification du serveur par le biais d'un certificat de serveur pour activer la session cryptée. De même, quand Adaptive Server fonctionne comme client pendant des RPC, un référentiel de CA habilitées doit être disponible pour qu'une connexion client puisse y accéder pour valider le certificat de serveur.

### Le certificat de serveur

Chaque Adaptive Server doit posséder son propre fichier de certificat de serveur chargé au démarrage. L'emplacement par défaut du fichier de certificats est :

UNIX : *$SYBASE/$SYBASE_ASE/certificates/servername.crt*

NT : *%SYBASE%\%SYBASE_ASE%\certificates\servername.crt*

où *nom_serveur* correspond au nom de l'Adaptive Server spécifié dans la ligne de commande au démarrage avec l'indicateur -s ou dans la variable d'environnement $DSLISTEN.

Le fichier du certificat de serveur se compose de données encodées, dont le certificat du serveur et la clé privée cryptée du certificat du serveur.

Vous pouvez également spécifier l'emplacement du fichier du certificat de serveur lorsque vous utilisez sp_ssladmin.

---

**Remarque** Pour réussir à établir une connexion client, le nom commun dans le certificat doit correspondre au nom Adaptive Server dans le fichier d'interface.

---

### Les certificats d'origine sécurisés CA

La liste des CA habilitées est chargée par Adaptive Server au démarrage à partir du fichier de certificats d'origine sécurisés. Le fichier de certificats d'origine sécurisés est identique par la forme au fichier de certificat, à ceci près qu'il contient des certificats pour les CA connues d'Adaptive Server. L'Adaptive Server local peut accéder au fichier de certificats d'origine sécurisés à l'emplacement suivant :

UNIX : *$SYBASE/$SYBASE_ASE/certificates/servername.txt*

NT : *%SYBASE%\%SYBASE_ASE\certificates\servername.txt*

où *servername* correspond au nom du serveur. Le fichier de certificats d'origine sécurisés est utilisé par Adaptive Server uniquement lorsqu'il fonctionne comme client (pour l'exécution de RPC ou de connexions CIS, par exemple).

Le responsable de la sécurité du système ajoute et supprime les CA acceptées par Adaptive Server à l'aide d'un éditeur de texte ASCII classique.

---

**Avertissement !** Utilisez le rôle de responsable de la sécurité du système (sso_role) dans Adaptive Server pour restreindre l'accès et l'exécution sur les objets sensibles en termes de sécurité.

---

Adaptive Server met à votre disposition des outils permettant de générer une demande de certificat et d'autoriser des certificats. Pour plus d'informations, reportez-vous à la section "Utilisation d'outils Adaptive Server pour demander et autoriser des certificats", page 349.

## Types de connexion

Cette section décrit les différentes connexions client-serveur et serveur-serveur.

### Connexion des clients à Adaptive Server

Les applications Open Client établissent une connexion par socket à Adaptive Server de la même manière que les connexions de clients existantes sont établies. Avant la transmission des données de l'utilisateur, une négociation SSL est effectuée au niveau du socket lorsque l'appel de transfert réseau aboutit côté client et que l'appel d'acceptation aboutit côté serveur.

### Appels de procédures à distance serveur-serveur

Adaptive Server établit une connexion par socket à un autre serveur pour un RPC de la même manière que des connexions RPC existantes sont établies. Avant la transmission des données de l'utilisateur, une négociation SSL est effectuée au niveau du socket lorsque l'appel de connexion de transfert réseau aboutit. Si la connexion par socket serveur-serveur a déjà été établie, la connexion par socket et le contexte de sécurité existants sont réutilisés.

Lorsqu'Adaptive Server fonctionne comme client lors de RPC, il demande le certificat du serveur distant au cours de la connexion. Adaptive Server vérifie alors que la CA qui a signé le certificat du serveur distant est habilitée, c'est-à-dire, qu'elle figure sur sa propre liste de CA habilitées dans le fichier de certificats d'origine sécurisés. Il vérifie également que le nom commun du certificat du serveur correspond au nom commun utilisé lors de l'établissement de la connexion.

Serveur compagnon et SSL

Vous pouvez utiliser un serveur compagnon pour configurer Adaptive Server en mode reprise sur le serveur secondaire. Vous devez configurer les serveurs principal et secondaire avec les mêmes paramètres SSL et RPC. En cas de reprise sur le serveur secondaire (fail over) ou de retour vers le serveur primaire (fail back), les sessions de sécurité sont ré-établies avec les connexions.

Connexions Open Client

Component Integration Services, RepAgent, Distributed Transaction Management, ainsi que d'autres modules d'Adaptive Server utilisent Client-Library pour établir les connexions aux serveurs autres qu'Adaptive Server. Le serveur distant est authentifié par son certificat. Le serveur distant authentifie la connexion client Adaptive Server pour les RPC à l'aide du nom d'utilisateur et du mot de passe.

## Activation de SSL

Adaptive Server détermine le service de sécurité à utiliser en fonction du fichier d'interface (*sql.ini* sous Windows).

Pour activer SSL :

1 Générez un certificat pour le serveur.

2 Créez un fichier de certificats d'origine sécurisés.

3 Activez SSL à l'aide de sp_configure. Dans une invite de commande, tapez la commande suivante :

```
sp_configure "enable ssl", 1
```

1 active le sous-système SSL au démarrage, alloue de la mémoire et SSL réalise le cryptage des données au niveau câble sur le réseau.

0 désactive SSL (valeur par défaut).

4 Ajoutez le filtre SSL dans le fichier d'interface. Pour plus d'informations, reportez-vous à la section "Création d'entrées de répertoire de serveur", page 350.

5 Ajoutez un certificat au fichier de certificats à l'aide de sp_ssladmin. Pour plus d'informations, reportez-vous à la section "Administration des certificats", page 351.

6 Arrêtez Adaptive Server, puis redémarrez-le.

---

**Remarque** Pour plus d'informations sur les outils certauth, certreq et certpk12 servant à demander, autoriser et convertir des certificats tiers, reportez-vous au guide *Utilitaires*.

---

Contrairement aux autres services de sécurité (DCE, Kerberos et NTLAN, par exemple), SSL ne s'appuie ni sur la section "Security" du fichier de configuration d'Open Client/Open Server, *libtcl.cfg* ni sur les objets qui se trouvent dans *objectid.dat*.

L'administrateur système doit prendre en compte l'utilisation de la mémoire par SSL lors de l'évaluation de la mémoire physique totale. Pour les connexions SSL dans Adaptive Server, vous devez disposer d'approximativement 40 ko par connexion (les connexions comprennent les connexions utilisateur, les serveurs distants et les récepteurs réseau). La mémoire est réservée et préallouée dans une zone de mémoire et utilisée en interne par les bibliothèques Adaptive Serve et SSL Plus, à la demande.

## Obtention d'un certificat

Le responsable de la sécurité du système installe les certificats de serveur et les clés privées pour Adaptive Server :

- en utilisant des outils tiers disponibles dans l'infrastructure de clés publiques déjà déployée dans l'environnement du client ;
- en utilisant l'outil de demande de certificat d'Adaptive Server conjointement à la CA tiers habilitée.

Pour obtenir un certificat, vous devez demander un certificat auprès d'une CA. Si vous demandez un certificat auprès d'un tiers et que ce certificat est au format PKCS #12, convertissez le certificat en un format compris par Adaptive Server à l'aide de certpk12.

Pour tester l'outil de demande de certificat d'Adaptive Server et pour vérifier que les méthodes d'authentification fonctionnent sur votre serveur, Adaptive Server fournit un outil de test qui permet d'agir en tant que CA et d'émettre soi-même un certificat signé par une CA.

Les principales étapes de la création d'un certificat à utiliser avec Adaptive Server sont les suivantes :

1 Générez la paire de clés publique et privée.

2 Stockez la clé privée dans un emplacement sûr.

3 Générez la demande de certificat.

4 Envoyez la demande de certificat à la CA.

5 Après signature et envoi du certificat par la CA, stockez-le dans un fichier et ajoutez la clé privée au certificat.

6 Stockez le certificat dans le répertoire d'installation d'Adaptive Server.

#### Outils tiers pour la demande de certificats

La plupart des fournisseurs de PKI tiers et certains navigateurs possèdent des utilitaires permettant de générer des certificats et des clés privées. Ces utilitaires sont généralement des Assistants qui vous invitent à définir, par le biais d'une série de questions, un nom distinctif et un nom commun pour le certificat.

Suivez les instructions fournies par l'Assistant pour créer des demandes de certificat. Une fois que vous avez reçu le certificat au format PKCS #12, générez un fichier de certificat et un fichier de clé privée à l'aide de certpk12. Concaténez les deux fichiers en un fichier *servername.crt* où *servername* correspond au nom du serveur et placez-le dans le répertoire *certificates* sous *$SYBASE/$SYBASE_ASE.* Pour plus d'informations, reportez-vous au guide *Utilitaires* de votre plate-forme.

#### Utilisation d'outils Adaptive Server pour demander et autoriser des certificats

Adaptive Server propose des outils permettant de demander et d'autoriser des certificats. certreq génère des paires de clés publiques et privées et des demandes de certificats. certauth convertit une demande de certificat de serveur en certificat signé par la CA.

---

**Avertissement !** N'utilisez certauth qu'à des fins de test. Sybase vous recommande d'utiliser les services d'une CA commerciale qui garantit la protection de l'intégrité du certificat d'origine sécurisé et parce qu'un certificat signé par une CA reconnue facilite la migration vers l'utilisation de certificats clients pour l'authentification.

---

La préparation du certificat d'origine sécurisé du serveur est une procédure qui se déroule en cinq étapes. Les deux premières étapes permettent de créer un certificat d'origine sécurisé test, afin de pouvoir vérifier si vous êtes en mesure de créer des certificats de serveur. Une fois que vous disposez d'un certificat de CA (certificat d'origine sécurisé), répétez les étapes 3 à 5 pour signer les certificats de serveur.

1 Demandez un certificat à l'aide de certreq.

2 Convertissez la demande de certificat en certificat auto-signé par la CA (certificat d'origine sécurisé) à l'aide de certauth.

3 Demandez un certificat de serveur et une clé privée à l'aide de certreq.

4 Convertissez la demande de certificat en certificat de serveur signé par la CA à l'aide de certauth.

5 Concaténez le texte de la clé privée au certificat de serveur et stockez le certificat dans le répertoire d'installation du serveur.

Pour plus d'informations sur les utilitaires Sybase, certauth, certreq et certpk12 qui permettent de demander, d'autoriser et de convertir des certificats tiers, reportez-vous au guide *Utilitaires* de votre plate-forme.

---

**Remarque** certauth et certreq dépendent des algorithmes RSA et DSA. Ces outils ne fonctionnent qu'avec des modules de cryptage utilisant des algorithmes RSA et DSA pour créer la demande de certificat.

Adaptive Server supporte le moteur de cryptage de Certicom Corp., Security Builder™, qui supporte les algorithmes RSA et DSA pour créer les demandes de certificat.

---

## Création d'entrées de répertoire de serveur

Adaptive Server accepte les connexions des clients et les RPC serveur-serveur. Vous pouvez configurer l'adresse et les numéros de port pour lesquels Adaptive Server accepte les connexions afin de pouvoir spécifier plusieurs réseaux, protocoles et ports de substitution.

Dans le fichier d'interface, SSL est spécifié comme filtre dans les lignes master et query, alors que les mécanismes de sécurité (DCE ou Kerberos, par exemple) sont identifiés dans une ligne SECMECH. L'exemple suivant présente une entrée TLI pour un Adaptive Server utilisant SSL dans un environnement UNIX.

Une entrée pour un Adaptive Server avec SSL et les mécanismes de sécurité DCE sous UNIX peut prendre cette forme :

```
SYBSRV1
    master tli tcp /dev/tcp \x00020abc12345678000000000000000 ssl
    query tli tcp /dev/tcp \x00020abc12345678000000000000000 ssl
    master tli tcp /dev/tcp \x00020abd12345678000000000000000
    SECMECH 1.3.6.1.4.897.4.6.1
```

Une entrée pour le serveur avec SSL et les mécanismes de sécurité Kerberos sous NT peut prendre cette forme :

```
[SYBSRV2]
    query=nlwnsck, 18.52.86.120,2748,ssl
    master=nlwnsck 18.52.86.120,2748,ssl
    master=nlwnsck 18.52.86.120,2749
    secmech=1.3.6.1.4.897.4.6.6
```

Les lignes SECMECH pour SYBSRV1 et SYBSRV2 dans les exemples contiennent un identificateur d'objet (OID) qui fait référence, respectivement, aux mécanismes de sécurité DCE et Kerberos. Les valeurs de l'OID sont définies dans :

UNIX : *$SYBASE/$SYBASE_OCS/config/objectid.dat*

NT : *%SYBASE%\%SYBASE_OCS\ini\objectid.dat*

Dans ces exemples, le service de sécurité SSL est spécifié sur le port numéro 2748(0x0abc).

---

**Remarque** Le recours à SSL conjointement à un mécanisme de sécurité SECMECH est censé faciliter la migration de la sécurité SECMECHs vers la sécurité SSL.

---

## Administration des certificats

Pour administrer SSL et les certificats dans Adaptive Server, utilisez sp_ssladmin. sso_role est nécessaire à l'exécution de la procédure stockée.

sp_ssladmin est utilisé pour :

- ajouter des certificats de serveur local. Vous pouvez ajouter des certificats et spécifier le mot de passe utilisé pour crypter les clés privées ou demander la saisie du mot de passe dans la ligne de commande au démarrage.
- supprimer des certificats de serveur local ;
- répertorier des certificats de serveur.

La syntaxe de sp_ssladmin est la suivante :

```
sp_ssladmin {[addcert, chemin_certificat [, password|NULL]]
       [dropcert, chemin_certificat]
       [lscert]
       [help]}
```

Exemple :

```
sp_ssladmin addcert, "/sybase/ASE-12_5/certificates/Server1.crt",
      "mon_mot_de_passe"
```

Une entrée est ajoutée pour le serveur local, *Server1.crt*, dans le fichier de certificat au chemin absolu */sybase/ASE-12_5/certificates* (*x:\sybase\ASE-12_5\certificates* sous Windows). La clé privée est cryptée avec le mot de passe "*mon_mot_de_passe*". Le mot de passe doit être celui que vous avez spécifié lors de la création de la clé privée.

Avant d'accepter le certificat, sp_ssladmin vérifie que :

- la clé privée peut être décryptée à l'aide du mot de passe fourni (sauf lorsque NULL est spécifié) ;
- la clé privée et la clé publique présentes dans le certificat correspondent l'une à l'autre ;
- la chaîne du certificat, de la CA principale au certificat de serveur, est correcte ;
- le nom commun du certificat correspond au nom commun du fichier d'interface.

Si les noms communs ne correspondent pas l'un à l'autre, sp_ssladmin affiche un avertissement. En cas d'échec des autres critères, le certificat n'est pas ajouté au fichier de certificat.

---

**Avertissement !** Adaptive Server limite les mots de passe à 64 caractères. Par ailleurs, certaines plates-formes limitent la longueur des mots de passe corrects lors de la création de certificats de serveur. Sélectionnez un mot de passe respectant ces limites :

- Sun Solaris : plates-formes 32 et 64 bits, 256 caractères maximum ;
- Linux : 128 caractères ;
- IBM : plates-formes 32 et 64 bits, 32 caractères ;
- HP : plates-formes 32 et 64 bits, 8 caractères ;
- Digital UNIX : 80 caractères ;
- Windows NT : 256 caractères.

---

L'utilisation de la valeur NULL comme mot de passe est censée protéger les mots de passe lors de la configuration initiale de SSL, avant le début de la session SSL cryptée. Puisque vous n'avez pas encore configuré SSL, le mot de passe transite sous forme non cryptée via la connexion. Vous pouvez éviter cette situation en spécifiant la valeur NULL pour le mot de passe à la première connexion.

Lorsque NULL constitue le mot de passe, vous devez lancer dataserver avec un indicateur qui invite l'administrateur à indiquer le mot de passe de la clé privée dans la ligne de commande.

Après avoir relancé Adaptive Server avec la connexion SSL établie, utilisez de nouveau sp_ssladmin mais cette fois en utilisant le vrai mot de passe. Le mot de passe est alors crypté et stocké par Adaptive Server. Tout autre lancement d'Adaptive Server à partir de la ligne de commande utilise le mot de passe crypté. Vous n'avez pas besoin de spécifier le mot de passe dans la ligne de commande au démarrage.

Il existe une alternative au mot de passe NULL à la première connexion, qui consiste à éviter une connexion à distance à Adaptive Server via isql. Vous pouvez spécifier "localhost" comme *nom_hôte* dans le fichier *interfaces* (*sql.ini* pour Windows) afin d'empêcher les clients de se connecter à distance. Il n'est possible d'établir qu'une connexion locale et le mot de passe n'est jamais transmis via la connexion réseau.

## Performances

L'établissement d'une session sécurisée entraîne un surcoût en traitement car la taille des données augmente après le cryptage, ce qui demande de traiter des informations de cryptage et de décryptage supplémentaires. Généralement, l'E/S supplémentaire cumulée lors de la négociation SSL ralentit de 10 à 20 fois la connexion des utilisateurs. Par ailleurs, les connexions SSL requièrent davantage de mémoire. Vous devez approximativement disposer de 40 ko de mémoire supplémentaire pour chaque connexion utilisateur.

## CipherSuites

Lors de la négociation SSL, le client et le serveur négocient un protocole de sécurité commun via CipherSuite. **CipherSuites** constitue une liste préférentielle d'algorithmes d'échange de clés, de méthodes de hachage et de cryptage utilisés par les applications SSL. Pour obtenir une description complète de CipherSuites, visitez le site de l'organisation Internet Engineering Task Force (IETF) : (http://www.ietf.org/rfc/rfc2246.txt).

Par défaut, la version la plus robuste de CipherSuites supportées par le client et le serveur est la version utilisée pour la session SSL.

Adaptive Server supporte la version de CipherSuites accompagnant l'API SSL Plus Library et le moteur de cryptage, Security Builder™, tous deux développés par Certicom Corp.

Vous trouverez ci-dessous la liste des versions de CipherSuites, triées dans l'ordre décroissant de puissance, supportées par Adaptive Server 12.5.

```
TLS_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_RC4_128_MD5,
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,
TLS_DHE_DSS_WITH_RC4_128_SHA,
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_RSA_WITH_DES_CBC_SHA,
TLS_DHE_DSS_WITH_DES_CBC_SHA,
TLS_DHE_RSA_WITH_DES_CBC_SHA,
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA,
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA,
TLS_DHE_DSS_EXPORT1024_WITH_RC4_56_SHA,
TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA,
TLS_RSA_EXPORT_WITH_RC4_40_MD5,
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA,
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
```

**Remarque** Les versions de CipherSuites répertoriées ci-dessous respectent la spécification de couche de transfert (TLS). TLS est une version améliorée de SSL 3.0 et un alias de SSL version 3.0 CipherSuites.

# Sécurité réseau

Adaptive Server propose des services de sécurité réseau qui permettent d'authentifier des utilisateurs et de protéger les données transmises d'une machine à une autre sur un réseau.

Dans un environnement informatique client/serveur distribué, les accès frauduleux à des données confidentielles sont possibles. Avec Adaptive Server, vous pouvez utiliser des services de sécurité de fournisseurs tiers pour authentifier les utilisateurs, crypter les informations et éviter la falsification des données.

Selon le mécanisme de sécurité que vous choisissez, Adaptive Server vous permet d'utiliser un ou plusieurs des services de sécurité suivants :

- Unification des logins : utilise le mécanisme de sécurité visant à authentifier les utilisateurs *une fois* sans qu'ils aient à fournir un nom et un mot de passe chaque fois qu'ils se connectent à un Adaptive Server.
- Confidentialité des messages : crypte les données qui transitent sur le réseau.
- Authentification réciproque : utilise le mécanisme de sécurité pour vérifier l'identité du client et du serveur. (Cette procédure doit être demandée par le client et ne peut pas être imposée par Adaptive Server.)
- Intégrité des messages : vérifie que les données transmises n'ont pas été modifiées.
- Détection par ré-exécution : vérifie que les données n'ont pas été interceptées par un intrus.
- Vérification de l'ordre : vérifie l'ordre des données transmises.
- Contrôles de l'origine des messages : vérifie l'origine du message.
- Sécurité des procédures distantes : établit l'authentification réciproque, la confidentialité des messages et l'intégrité des messages pour les transmissions de procédures distantes.

**Remarque** Il se peut que le mécanisme de sécurité que vous utilisez ne supporte pas tous ces services.

# Audit

Adaptive Server inclut un système d'audit complet. Celui-ci comprend une base de données système appelée sybsecurity, des paramètres de configuration pour gérer l'audit, une procédure système, sp_audit, pour définir toutes les options d'audit et une autre, sp_addauditrecord, pour ajouter dans la trace d'audit des enregistrements définis par l'utilisateur. Lorsque vous installez la fonction d'audit, vous pouvez spécifier le nombre de tables d'audit qu'Adaptive Server utilisera pour la trace d'audit. Si vous utilisez deux tables ou plus pour stocker la trace d'audit, vous pouvez configurer un système d'audit qui s'exécute normalement, sans intervention manuelle ni perte d'enregistrements.

Un responsable de la sécurité du système gère le système d'audit et il est le seul à pouvoir démarrer et arrêter l'audit, définir des options d'audit et traiter les données qui en résultent. En tant que SSO, vous pouvez établir un audit pour des événements tels que :

- des événements liés à la sécurité au niveau serveur,
- la création, la suppression et la modification d'objets de base de données,
- toutes les actions réalisées par un utilisateur spécifique ou par des utilisateurs détenant un rôle particulier,
- l'octroi ou la révocation des accès aux bases de données,
- l'importation ou l'exportation de données,
- les connexions et les déconnexions.

La fonction d'audit est présentée au chapitre 12, "Audit".

# Sécurité des logins définie par les utilisateurs

Les options de sécurité des logins définies par l'utilisateur permettent un contrôle plus précis des fonctions de sécurité d'Adaptive Server.

Dans la version 12.0 et ultérieure d'Adaptive Server, le responsable de la sécurité du système peut :

- ajouter plus de logins et de rôles utilisateur que dans les versions antérieures ;

- spécifier le nombre maximal autorisé de saisie d'un mot de passe incorrect pour un login ou un rôle avant que celui-ci soit automatiquement verrouillé ;
- verrouiller et déverrouiller des rôles manuellement ;
- s'assurer que tous les mots de passe utilisateur comprennent au moins un chiffre ;
- spécifier la longueur minimale du mot de passe au niveau du serveur ou pour un rôle ou un login spécifique ;
- afficher toutes les informations relatives à la sécurité pour des logins et des rôles ;
- associer un délai de validité du mot de passe à un login ou un rôle spécifique.

Il est possible d'utiliser des valeurs négatives pour les ID utilisateur (*uid*).

L'ID utilisateur du serveur (*suid*) associé à un groupe ou à un rôle dans sysusers n'est pas égal à son correspondant négatif de l'ID utilisateur (*uid*). Chaque *suid* associé à un groupe ou à un rôle dans sysusers est défini à – 2 (INVALID_SUID).

## Définition et modification du nombre de tentatives de connexion

La définition du nombre maximal de tentatives de connexion autorisées offre une protection contre les intrus qui essaient de deviner les mots de passe par la force ou en se basant sur le dictionnaire. Un responsable de la sécurité du système peut spécifier un nombre maximal de tentatives consécutives de connexion, au-delà duquel le login ou le rôle est automatiquement verrouillé. Le nombre autorisé de tentatives de connexion infructueuses peut être défini au niveau du serveur ou pour des logins et des rôles particuliers. Les paramètres définis individuellement ont la priorité sur le paramétrage au niveau du serveur.

Le nombre de connexions qui ont échoué est enregistré dans la colonne logincount de la table master..syslogins. Une connexion réussie ramène ce nombre à 0.

### Définition au niveau serveur du nombre maximal de tentatives de connexion autorisées

Pour définir au niveau serveur le nombre maximal de tentatives de connexion autorisées pour des logins et des rôles, utilisez le paramètre de configuration maximum failed logins.

Par exemple :

```
sp_configure "maximum failed logins", 5
```

Définit à 5 le nombre maximal de tentatives infructueuses de connexion, au niveau du serveur.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de maximum failed logins, reportez-vous à la commande sp_configure.

### Définition du nombre maximal de tentatives de connexion autorisées pour des logins spécifiques

Pour définir le nombre maximal de tentatives de connexion autorisées pour un login spécifique au moment de la création, utilisez sp_addlogin.

Par exemple :

```
sp_addlogin joe, "Djdiek3", pubs2, null, null, null, null, 2
```

Crée le nouveau login joe avec le mot de passe "Djdiek3" et fixe à 2 le nombre maximal de tentatives de connexion infructueuses pour joe.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de maxfailedlogins, reportez-vous à la commande sp_addlogin.

### Définition du nombre maximal de tentatives de connexion autorisées pour des rôles spécifiques

Pour définir le nombre maximal de tentatives de connexion autorisées pour un rôle spécifique au moment de la création, utilisez create role.

Par exemple :

```
create role intern_role with passwd "temp244", max failed_logins 20
```

Crée le rôle intern_role avec le mot de passe "temp244" et fixe à 20 le nombre maximal de tentatives de connexion infructueuses pour intern_role.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de max failed_logins, reportez-vous à la commande create role.

## Modification du nombre maximal de tentatives de connexion autorisées pour des logins spécifiques

Utilisez sp_modifylogin pour définir ou modifier le nombre maximal de tentatives de connexion infructueuses autorisées pour un login existant.

Par exemple :

```
sp_modifylogin "joe", @option="max failed_logins", @value="40"
```

Modifie le nombre maximal de tentatives de connexion infructueuses autorisées pour le login "joe" et le fixe à 40.

**Remarque** Le paramètre *value* est du type de données character ; par conséquent, vous devez mettre les valeurs numériques entre guillemets.

```
sp_modifylogin "all overrides", "max failed_logins", "3"
```

Modifie pour tous les logins le nombre maximal de tentatives de connexion infructueuses autorisées et le fixe à 3.

```
sp_modifylogin "all overrides", @option="max failed_logins", @value="-1"
```

Supprime pour tous les logins le nombre maximal de tentatives de connexion infructueuses autorisées.

sp_modifylogin n'affecte que les rôles utilisateur et non les rôles système. Pour plus d'informations sur la syntaxe et les règles d'utilisation de max failed_logins, reportez-vous à la commande sp_modifylogin.

## Modification du nombre maximal de tentatives de connexion autorisées pour des rôles spécifiques

Utilisez la commande alter role pour définir ou modifier le nombre maximal de tentatives de connexion infructueuses autorisées pour un rôle.

Par exemple :

```
alter role physician_role set max failed_logins 5
```

Remplace par 5 le nombre maximal de tentatives de connexion infructueuses autorisées pour physician_role.

```
alter role "all overrides" set max failed_logins -1
```

Supprime pour tous les rôles le nombre maximal de tentatives de connexion infructueuses autorisées.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de max failed_logins, reportez-vous à la commande alter role.

## Verrouillage et déverrouillage des logins et des rôles

Un login ou un rôle peut être verrouillé lorsque :

- son mot de passe arrive à expiration,
- le nombre maximal de tentatives de connexion infructueuses autorisées est atteint ou
- le responsable de la sécurité du système verrouille manuellement le rôle ou le login.

### Verrouillage et déverrouillage des logins

Le responsable de la sécurité du système peut utiliser la procédure sp_locklogin pour verrouiller ou déverrouiller manuellement un login. (Cette fonctionnalité n'est pas nouvelle, mais elle est mentionnée ici à des fins de comparaison avec les nouvelles méthodes disponibles pour verrouiller ou déverrouiller des rôles.)

Par exemple :

```
sp_locklogin "joe", "lock"
sp_locklogin "joe", "unlock"
```

Les informations sur l'état de verrouillage d'un login sont stockées dans la colonne status de syslogins.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de sp_locklogin, reportez-vous à la commande sp_locklogin.

### Verrouillage et déverrouillage des rôles

Le responsable de la sécurité du système peut utiliser la procédure alter role pour verrouiller ou déverrouiller manuellement un rôle.

Par exemple :

```
alter role physician_role lock
alter role physician_role unlock
```

Les informations sur l'état de verrouillage d'un rôle sont stockées dans la colonne status de syssrvroles.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de lock et unlock, reportez-vous à la commande alter role.

### Déverrouillage des logins et des rôles au démarrage du serveur

Le déverrouillage automatique d'un login peut entraîner sur un site le verrouillage des comptes autorisant à déverrouiller des logins (comptes des administrateurs système et des SSO). Dans ces situations, utilisez l'argument -u avec l'utilitaire dataserver afin de déverrouiller un login ou un rôle spécifique au démarrage d'Adaptive Server.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de l'indicateur -u, reportez-vous au guide *Utilitaires*.

## Affichage des informations relatives au mot de passe

Cette section traite de l'affichage des informations relatives au mot de passe pour les logins et les rôles.

### Affichage des informations relatives au mot de passe pour des logins spécifiques

Utilisez sp_displaylogin pour afficher les paramètres des mots de passe pour un login.

Par exemple, l'instruction suivante affiche des informations sur le login joe :

```
sp_displaylogin joe
Suid: 2
Loginame: joe
Fullname: Joseph Resu
Default Database: master
Default Language:
Configured Authorization: intern_role (default OFF)
Locked: NO
Date of Last Password Change: Nov 24 1997  3:35PM
Password expiration interval : 5
Password expired : NO
Minimum password length:4
Maximum failed logins : 10
Current failed logins : 3
```

Pour plus d'informations sur la syntaxe et les règles d'utilisation, reportez-vous à la commande sp_displaylogin.

### Affichage des informations relatives au mot de passe pour des rôles spécifiques

Utilisez sp_displayroles pour afficher les paramètres des mots de passe pour un rôle.

Par exemple :

```
sp_displayroles physician_role, "display_info"
Role name = physician_role
Locked : NO
Date of Last Password Change : Nov 24 1997  3:35PM
Password expiration interval = 5
Password expired : NO
Minimum password length = 4
Maximum failed logins = 10
Current failed logins = 3
```

Affiche des informations sur le rôle physician_role.

Pour plus d'informations sur la syntaxe et les règles d'utilisation, reportez-vous à la commande sp_displayroles.

## Recherche d'au moins un chiffre dans les mots de passe

Le responsable de la sécurité du système peut vérifier si le mot de passe contient au moins un chiffre, en utilisant le paramètre de configuration check password for digit. Si ce dernier est défini, il ne s'applique pas aux mots de passe existants. Par défaut, cette fonction de vérification est désactivée.

Par exemple :

```
sp_configure "check password for digit", 1
```

Active la fonction de vérification du mot de passe.

```
sp_configure "check password for digit", 0
```

Désactive la fonction de vérification du mot de passe.

Pour plus d'informations sur la syntaxe et les règles d'utilisation du nouveau paramètre, reportez-vous à la commande sp_configure.

## Définition et modification de la longueur minimale du mot de passe

Dans les précédentes versions, la longueur minimale du mot de passe était une valeur de six caractères, codée en dur et non configurable. Désormais, les mots de passe sont configurables et vous pouvez les personnaliser en fonction de vos besoins, par exemple utiliser les numéros d'identification personnels (PIN) à quatre chiffres ou des logins anonymes avec des mots de passe NULL.

Le responsable de la sécurité du système peut spécifier :

- une longueur minimale qui s'applique globalement aux mots de passe,
- une longueur minimale du mot de passe établie par login ou par rôle.

La valeur établie par login ou par rôle remplace le paramétrage au niveau serveur. La définition d'une longueur minimale s'applique aux mots de passe nouvellement créés, non à ceux déjà existants.

### Définition de la longueur minimale du mot de passe au niveau du serveur

Utilisez le paramètre de configuration minimum password length pour spécifier au niveau du serveur la longueur minimale du mot de passe des logins et des rôles.

Par exemple :

```
sp_configure "minimum password length", 4
```

Définit la longueur minimale du mot de passe pour tous les logins et tous les rôles à 4 caractères.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de minimum password length, reportez-vous à la commande sp_configure.

### Définition de la longueur minimale du mot de passe pour un login spécifique

Pour définir la longueur minimale du mot de passe pour un login spécifique au moment de la création, utilisez sp_addlogin.

Par exemple :

```
sp_addlogin joe, "Djdiek3", @minpwdlen=4
```

Crée le nouveau login joe avec le mot de passe "Djdiek3" et définit sur 4 la longueur minimale du mot de passe pour joe.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de minpwdlen, reportez-vous à la commande sp_addlogin.

### Définition de la longueur minimale du mot de passe pour un rôle spécifique

Pour définir la longueur minimale du mot de passe pour un rôle spécifique au moment de la création, utilisez create role.

Par exemple :

```
create role intern_role with passwd "temp244", min passwd length 0
```

Crée le nouveau rôle intern_role avec le mot de passe "temp244" et définit sur 0 la longueur minimale du mot de passe pour intern_role. Le mot de passe initial est de sept caractères, mais il peut être modifié et prendre une longueur quelconque puisque la longueur minimale est fixée à 0.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de min passwd length, reportez-vous à la commande create role.

### Modification de la longueur minimale du mot de passe pour un login spécifique

Définissez ou modifiez la longueur minimale d'un login existant à l'aide de sp_modifylogin. sp_modifylogin n'affecte que les rôles utilisateur et non les rôles système.

Par exemple :

```
sp_modifylogin "joe", @option="min passwd length", @value="8"
```

Modifie la longueur minimale du mot de passe pour le login "joe" et la fixe à 8 caractères.

**Remarque** Le paramètre *value* est du type de données character ; par conséquent, vous devez mettre les valeurs numériques entre guillemets.

```
sp_modifylogin "all overrides", "min passwd length", @value="2"
```

Modifie pour tous les logins la longueur minimale du mot de passe et la fixe à 2 caractères.

```
sp_modifylogin "all overrides", @option="min passwd length", @value="-1"
```

Supprime toutes les longueurs minimales de mot de passe spécifiques des logins.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de min passwd length, reportez-vous à la commande sp_modifylogin.

### Modification de la longueur minimale du mot de passe pour un rôle spécifique

Utilisez alter role pour définir ou modifier la longueur minimale du mot de passe pour un rôle existant.

Par exemple :

```
alter role physician_role set min passwd length 5
```

Définit la longueur minimale du mot de passe pour le rôle existant physician_role à 5 caractères.

```
alter role "all overrides" set min passwd length -1
```

Supprime toutes les longueurs minimales de mot de passe spécifiques des rôles.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de set min passwd length, reportez-vous à la commande alter role.

## Définition de l'intervalle d'expiration du mot de passe

Les administrateurs système et les responsables de la sécurité du système peuvent :

| Utiliser | Pour |
|---|---|
| sp_addlogin | Spécifier l'intervalle d'expiration du mot de passe d'un login au moment de la création. |
| sp_modifylogin | Modifier l'intervalle d'expiration d'un mot de passe de login. sp_modifylogin n'affecte que les rôles utilisateur et non les rôles système. |
| create role | Spécifier le délai d'expiration du mot de passe d'un rôle au moment de la création. |
| alter role | Modifier le délai d'expiration du mot de passe d'un rôle. |

Les règles suivantes s'appliquent au délai d'expiration des mots de passe de logins et de rôles :

- Un intervalle d'expiration du mot de passe attribué à des comptes de connexion ou à des rôles individuels remplace la valeur définie au niveau global. Ceci vous permet de spécifier des délais plus courts pour les comptes ou les rôles stratégiques, par exemple pour les mots de passe du responsable de la sécurité système et des intervalles d'expiration plus longs pour les comptes moins critiques (par exemple pour un login anonyme).

- Un login ou un rôle dont le délai de validité du mot de passe a expiré n'est pas directement activé.

Pour plus d'informations sur la syntaxe et les règles d'utilisation des commandes et procédures système, reportez-vous au *Manuel de référence d'Adaptive Server*.

### Expiration des mots de passe désactivée pour les mots de passe des versions inférieures à 12.x

L'expiration du mot de passe n'affectait pas les rôles dans les versions antérieures à Adaptive Server 12.x. Par conséquent, dans Adaptive Server 12.x et plus, cette option est désactivée pour tous les mots de passe de rôles existants définis par l'utilisateur. Durant la mise à niveau, tous les mots de passe de rôles définis par l'utilisateur ont un intervalle d'expiration égal à 0.

### Message relatif à un mot de passe en cours d'expiration

Lorsque le mot de passe d'un login ou d'un rôle est sur le point d'expirer, un avertissement invite l'utilisateur à contacter le responsable de la sécurité du système.

### Comment contourner la protection par mot de passe

Il peut s'avérer nécessaire de contourner le mécanisme de protection par mot de passe dans le cas de systèmes de connexion automatisés. Vous pouvez créer un rôle qui donne accès à tous les autres rôles sans mot de passe.

Si un responsable de la sécurité du système souhaite désactiver la protection par mot de passe pour certains utilisateurs, il peut octroyer le rôle protégé par mot de passe à un autre rôle et accorder ce dernier aux utilisateurs de son choix. L'activation de ce dernier rôle active automatiquement le rôle protégé par mot de passe sans qu'il soit nécessaire de saisir un mot de passe.

Exemple :

Jane est la responsable SSO d'une société ABC Inc. qui utilise des systèmes de connexion automatisés. Jane crée les rôles suivants :

- financial_assistant

```
create role financial_assistant with passwd
"L54K3j"
```

- accounts_officer

```
create role accounts_officer with passwd "9sF6ae"
```

- chief_financial_officer

```
create role chief_financial_officer
```

Elle accorde les rôles financial_assistant et accounts_officer au rôle chief_financial_officer :

```
grant role financial_assistant, accounts_officer to
chief_financial_officer
```

Puis elle accorde le rôle chief_financial_officer à Bob :

```
grant role chief_financial_officer to bob
```

Bob se connecte à Adaptive Server et active le rôle chief_financial_officer :

```
set role chief_financial_officer on
```

Les rôles financial_assistant et accounts_officer sont alors automatiquement activés sans que Bob ait à fournir un mot de passe. Bob peut désormais accéder à toutes les fonctions ou données qui dépendent des rôles financial_assistant et accounts_officer sans taper les mots de passe qui leur sont spécifiques.

## Création d'un intervalle d'expiration du mot de passe pour un nouveau login

Utilisez sp_addlogin pour définir l'intervalle d'expiration du mot de passe pour un nouveau login.

Par exemple :

```
sp_addlogin joe, "Djdiek3", null, null, null, 2
```

Crée le nouveau login joe avec le mot de passe "Djdiek3" et définit l'intervalle d'expiration de son mot de passe à 2 jours.

Pour plus d'informations sur la syntaxe et les règles d'utilisation du nouveau paramètre, reportez-vous à la commande sp_addlogin.

## Création d'un intervalle d'expiration du mot de passe pour un nouveau rôle

Utilisez create role pour définir l'intervalle d'expiration du mot de passe pour un nouveau rôle.

Par exemple :

```
create role intern_role with passwd "temp244", passwd expiration 7
```

Crée le nouveau rôle intern_role avec le mot de passe "temp244" et définit l'intervalle d'expiration de celui-ci à 7 jours.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de passwd expiration, reportez-vous à la commande create role.

## Ajout d'une date de création pour les mots de passe

Les mots de passe ont une "date de création" égale à la date de mise à niveau du serveur. La date de création pour les mots de passe de login est stockée dans la colonne pwdate de syslogins. La date de création pour les mots de passe de rôle est stockée dans la colonne pwdate de syssrvroles.

## Modification ou suppression de l'intervalle d'expiration du mot de passe pour un login ou un rôle

Utilisez sp_modifylogin pour modifier ou supprimer l'intervalle d'expiration du mot de passe pour un login existant, ainsi que pour en ajouter un à un login qui n'en a pas. sp_modifylogin n'affecte que les rôles utilisateur et non les rôles système.

Par exemple :

```
sp_modifylogin "joe", @option="passwd expiration", @value="5"
```

Modifie l'intervalle d'expiration du mot de passe pour le login "joe" et le fixe à 5 jours.

**Remarque** Le paramètre *value* est du type de données character ; par conséquent, vous devez mettre les valeurs numériques entre guillemets.

```
sp_modifylogin "all overrides", @option="passwd expiration", @value="3"
```

Modifie pour tous les logins le délai de validité du mot de passe avant expiration et le fixe à 3 jours.

```
sp_modifylogin "all overrides", @option="passwd expiration", @value="-1"
```

Supprime pour tous les logins le délai de validité du mot de passe avant expiration.

Pour plus d'informations sur la syntaxe et les règles d'utilisation de passwd expiration, reportez-vous à la commande sp_modifylogin.

CHAPITRE 10

# Gestion des connexions et des utilisateurs de bases de données Adaptive Server

Ce chapitre décrit les méthodes de gestion des connexions à Adaptive Server et des utilisateurs de bases de données.

Les sujets traités dans ce chapitre sont les suivants :

# Ajout d'utilisateurs : Présentation

Les procédures d'ajout de connexions à Adaptive Server, d'ajout d'utilisateurs aux bases de données et d'octroi d'**autorisations** d'utilisation de commandes et d'objets de base de données se répartissent entre le responsable de la sécurité du système (SSO), l'administrateur système (SA) et le propriétaire de la base de données (DBO).

L'ajout d'utilisateurs s'effectue par les étapes suivantes :

1 Un responsable de la sécurité du système utilise sp_addlogin pour créer un compte de connexion sur le serveur pour un nouvel utilisateur.

2 Un administrateur système ou propriétaire de base de données utilise sp_adduser pour ajouter un utilisateur à une base de données. Cette commande peut aussi attribuer à l'utilisateur un alias ou affecter cet utilisateur à un groupe. Pour plus d'informations, reportez-vous à la section "Création de groupes", page 374.

3 Un responsable de la sécurité du système octroie des rôles spécifiques à l'utilisateur.

4 Un administrateur système, propriétaire de base de données ou propriétaire d'objets octroie à l'utilisateur ou au groupe des autorisations spécifiques sur certaines commandes et objets de base de données. Les utilisateurs ou les groupes peuvent aussi se voir déléguer l'octroi de certaines autorisations sur des objets à d'autres utilisateurs ou groupes. Pour plus d'informations sur les autorisations, reportez-vous au chapitre 11, "Gestion des autorisations utilisateur".

Le tableau 10-1 récapitule les procédures système et commandes utilisées pour ces tâches.

***Tableau 10-1 : Ajout d'utilisateurs à Adaptive Server et aux bases de données***

| Tâche | Rôle requis | Commande ou procédure | Base de données |
|---|---|---|---|
| Création de logins, attribution de mots de passe, de bases de données par défaut, de langue par défaut et de nom complet | Responsable de la sécurité du système (SSO) | sp_addlogin | Toute base de données |
| Création de groupes | Propriétaire de la base de données ou administrateur système | sp_addgroup | Utilisateur de base de données |
| Création et attribution de rôles | Responsable de la sécurité du système (SSO) | create role | |

| Tâche | Rôle requis | Commande ou procédure | Base de données |
|---|---|---|---|
| Ajout d'utilisateurs à une base de données, attribution d'alias et affectation à des groupes | Propriétaire de la base de données ou administrateur système | sp_adduser | Utilisateur de base de données |
| Octroi à des groupes, des utilisateurs ou des rôles de l'autorisation de création ou d'accès à des objets de base de données | Propriétaire de base de données, administrateur système ou propriétaire d'objet | grant | Base de données utilisateur |

# Choix et création d'un mot de passe

Votre mot de passe permet d'éviter tout accès intempestif par des personnes non autorisées. Pour la création de votre mot de passe, observez les règles suivantes :

- N'utilisez pas d'informations telles que votre date de naissance, adresse ou tout autre mot ou numéro ayant un rapport avec votre vie privée.
- N'utilisez pas le nom de vos animaux ou de vos proches.
- N'utilisez pas de mots figurant dans le dictionnaire ou épelés à l'envers.

Les mots de passe les plus difficiles à deviner sont ceux qui associent des lettres majuscules et minuscules et des nombres. Ne le donnez jamais à personne et ne l'écrivez jamais à un endroit où il risque d'être vu.

Suivez les règles suivantes pour créer un mot de passe :

- La longueur minimale des mots de passe est de 6 octets.
- Toutes les lettres, les chiffres ou les symboles imprimables peuvent être utilisés dans les mots de passe.
- Un mot de passe doit être entre guillemets dans la commande sp_addlogin :
  - S'il contient d'autres caractères que A–Z, a–z, 0–9, _, #, des caractères alphabétiques codés corrects sur un ou plusieurs octets ou des caractères alphabétiques accentués,
  - s'il commence par un chiffre de 0 à 9.

# Ajout de logins à Adaptive Server

Utilisez sp_addlogin pour ajouter un nom de **login** à Adaptive Server. Vous n'avez pas à l'utiliser pour donner à l'utilisateur l'autorisation d'accéder aux bases de données utilisateur. Utilisez sp_adduser pour cela. Seul le responsable de la sécurité du système peut exécuter sp_addlogin. Respectez la syntaxe suivante :

```
sp_addlogin nom_login, mot_de_passe
[, base_de_données_par_défaut]
    [, langue_par_défaut [, nom_complet]]]
```

où :

- *nom_login* est le nom de login du nouvel utilisateur. Le nom de login doit être conforme aux règles concernant les identificateurs et doit être unique sur Adaptive Server. Pour simplifier la procédure de login comme l'administration du serveur, vous pouvez utiliser le même nom de login que pour le système d'exploitation. Ceci facilite la connexion à Adaptive Server parce que beaucoup de programmes client utilisent le nom de login du système d'exploitation comme valeur par défaut. Ceci simplifie aussi l'administration des comptes de connexion du serveur et du système d'exploitation et facilite la corrélation des données d'utilisation et d'audit générées par Adaptive Server et par le système d'exploitation.
- *mot_de_passe* est le mot de passe du nouvel utilisateur. Pour des règles de choix et de création de mots de passe sécurisés, reportez-vous à la section "Choix et création d'un mot de passe", page 371. Pour plus d'informations sur la modification d'un mot de passe, reportez-vous à la section "Changement des mots de passe", page 397.
- *base_de_données_par_défaut* est la **base de données par défaut** – où l'utilisateur commencera chaque session Adaptive Server.

---

**Remarque** La base de données par défaut est master. Pour éviter la création par les utilisateurs d'objets de base de données dans la base master, attribuez une base de données par défaut autre que master à la plupart des utilisateurs.

---

Un administrateur système peut changer la base par défaut de tout utilisateur à l'aide de sp_modifylogin. Les autres utilisateurs ne peuvent modifier que leur base de données par défaut.

Après spécification de la base de données par défaut, ajoutez l'utilisateur à cette base par défaut avec sp_adduser pour qu'il puisse se connecter directement à cette base.

- *langue_par_défaut* est la **langue par défaut** pour l'affichage des messages et invites à l'utilisateur. Si vous n'indiquez pas ce paramètre, c'est la langue par défaut d'Adaptive Server qui est utilisée. Un administrateur système peut changer la langue par défaut de tout utilisateur à l'aide de sp_modifylogin. Les autres utilisateurs ne peuvent modifier que leur langue par défaut.
- *nom_complet* est le nom complet de l'utilisateur. Il est utile à des fins d'identification et de documentation. Si vous ne l'indiquez pas, aucun nom complet n'est ajouté. Un administrateur système peut changer le nom complet de tout utilisateur à l'aide de sp_modifylogin. Les autres utilisateurs ne peuvent modifier que leur nom complet.

L'instruction ci-dessous définit un compte pour l'utilisateur "maryd" avec le mot de passe "100cents", la base de données par défaut (master), la langue par défaut et pas de nom complet :

```
sp_addlogin "maryd", "100cents"
```

Le mot de passe doit être entre guillemets parce qu'il commence par 1.

Après l'exécution de cette instruction, "maryd" peut se connecter à Adaptive Server. Elle est traitée automatiquement comme utilisateur "guest" de la base master, avec des autorisations limitées, sauf si elle a reçu un accès spécifique à master.

L'instruction ci-dessous définit un compte de connexion ("omar_khayyam") et un mot de passe ("rubaiyat") pour un utilisateur et lui attribue la base de données par défaut pubs2 :

```
sp_addlogin omar_khayyam, rubaiyat, pubs2
```

Pour spécifier un nom complet pour un utilisateur et utiliser la base de données et la langue par défaut, vous devez spécifier null à la place des paramètres *base_de_données_par_défaut* et *langue_par_défaut*. Exemple :

```
sp_addlogin omar, rubaiyat, null, null,
    "Omar Khayyam"
```

Il est aussi possible de spécifier un nom de paramètre, dans ce cas il n'est pas obligatoire de spécifier tous les paramètres. Exemple :

```
sp_addlogin omar, rubaiyat,
    @fullname = "Omar Khayyam"
```

A l'exécution de sp_addlogin, Adaptive Server ajoute une ligne à master.dbo.syslogins, attribue un **ID utilisateur** unique sur le serveur (suid) au nouvel utilisateur et remplit toutes les autres informations. A la connexion d'un utilisateur, Adaptive Server recherche dans syslogins le nom et le mot de passe fournis par cet utilisateur. La colonne password est cryptée par un algorithme unidirectionnel pour être illisible par un humain.

La colonne suid de syslogins identifie de façon unique chaque utilisateur sur Adaptive Server. Le suid d'un utilisateur reste toujours le même, quelle que soit la base de données qu'il utilise. Le suid 1 est toujours attribué au compte par défaut "sa" créée à l'installation d'Adaptive Server. Les ID des autres utilisateurs du serveur sont des entiers attribués de façon consécutive par Adaptive Server à chaque exécution de la commande sp_addlogin.

# Création de groupes

Les groupes sont un moyen pratique d'octroyer ou de révoquer des autorisations à plus d'un utilisateur en une seule instruction. Les groupes permettent d'attribuer un nom collectif à un ensemble d'utilisateurs. Ils sont tout particulièrement utiles pour administrer une installation Adaptive Server comportant un grand nombre d'utilisateurs. Un utilisateur est membre du groupe "public" et peut aussi être membre d'un autre groupe. (Les utilisateurs restent membre de "public", même s'ils appartiennent à un autre groupe).

Le plus pratique est sans doute de créer les groupes avant d'ajouter les utilisateurs à une base de données, parce que sp_adduser peut inclure les utilisateurs dans des groupes en les ajoutant à la base de données.

Un administrateur système ou le propriétaire de la base de données peut créer un groupe à tout moment par sp_addgroup. Respectez la syntaxe suivante :

```
sp_addgroup nom_grp
```

Le nom de groupe, paramètre obligatoire, doit être conforme aux règles relatives aux identificateurs. L'administrateur système peut affecter ou réaffecter des utilisateurs à des groupes avec la commande sp_changegroup.

Pour configurer le groupe Senior Engineering, utilisez la commande ci-dessous dans la base de données à laquelle vous souhaitez ajouter le groupe :

```
sp_addgroup senioreng
```

sp_addgroup ajoute une ligne sysusers dans la base de données en cours. Donc, chaque groupe dans une base de données, ainsi que chaque utilisateur, a une entrée dans sysusers.

# Ajout d'utilisateurs aux bases de données

Le propriétaire de base de données ou un administrateur système peut utiliser sp_adduser pour ajouter un utilisateur à une base de données particulière. L'utilisateur doit déjà avoir un login Adaptive Server. Respectez la syntaxe suivante :

sp_adduser *nom_login* [, *nom_dans_base* [, *nom_grp*]]

où :

- *nom_login* est le nom de login d'un utilisateur existant.
- *nom_dans_base* spécifie un nom différent du nom de login, sous lequel l'utilisateur sera connu dans cette base de données.

  Vous pouvez utiliser cette fonction pour adaptation aux préférences des utilisateurs. S'il y a par exemple cinq utilisateurs Adaptive Server dont le prénom est Mary, chacune doit avoir un nom de login différent. Mary Doe peut se connecter sous le nom "maryd", Mary Jones sous le nom "maryj" et ainsi de suite. Mais si ces utilisatrices travaillent sur des bases de données différentes, chacune peut préférer s'appeler simplement "mary" dans une base de données particulière.

  Si aucun *nom_dans_base* n'est donné, le nom dans la base de données est le même que le nom_login.

**Remarque** Cette possibilité est différente du mécanisme d'alias décrit dans la section "Utilisation d'alias dans les bases de données", page 402 qui fait correspondre l'identité et les autorisations d'un utilisateur à celles d'un autre utilisateur.

- *nom_grp* est le nom d'un groupe existant de la base de données. Si vous ne spécifiez pas de nom de groupe, l'utilisateur est inclus comme membre du groupe par défaut "public". Les utilisateurs restent dans le groupe "public" même s'ils sont membres d'un autre groupe. Pour plus d'informations sur la modification de l'appartenance d'un utilisateur à un groupe, reportez-vous à la section "Modification des appartenances d'utilisateur à un groupe", page 399.

sp_adduser ajoute une ligne à la table système sysusers dans la base de données en cours. Quand un utilisateur a une entrée dans la table sysusers d'une base de données, il :

- peut utiliser la commande use *nom_base* pour accéder à cette base de données,
- utilise cette base de données par défaut si le paramètre de base de données par défaut a été inclus dans la commande sp_addlogin,
- peut utiliser sp_modifylogin pour faire de cette base de données sa base par défaut.

Cet exemple montre comment un propriétaire de base de données peut donner l'autorisation d'accès à "maryh" du groupe "eng" qui existe déjà :

```
sp_adduser maryh, mary, eng
```

Cet exemple montre comment donner accès à une base de données à "maryd" en conservant son nom de login comme nom dans la base de données :

```
sp_adduser maryd
```

Cet exemple montre comment ajouter "maryj" au groupe existant "eng", en conservant son nom de login comme nom dans la base de données avec null à la place du nouveau nom d'utilisateur :

```
sp_adduser maryj, null, eng
```

Les utilisateurs qui ont accès à une base de données ont toujours besoin d'autorisations pour lire les données, les modifier et utiliser certaines commandes. Ces autorisations sont octroyées par les commandes grant et revoke, traitées au chapitre 11, "Gestion des autorisations utilisateur".

## Ajout d'un utilisateur "guest" à une base de données

La création d'un utilisateur "guest" dans une base de données permet à tout utilisateur disposant d'un compte Adaptive Server d'accéder à la base de données comme **guest**. Si un utilisateur émet la commande use *nom_base* et si son nom n'est pas trouvé dans les tables sysusers ou *sysalternates* de la base de données, Adaptive Server recherche un utilisateur guest. S'il en existe un, l'utilisateur est autorisé à accéder à la base de données, avec les autorisations de l'utilisateur guest.

Le propriétaire de base de données peut ajouter une entrée à la table sysusers de la base de données par sp_adduser :

```
sp_adduser guest
```

L'utilisateur guest peut être supprimé par sp_dropuser, comme indiqué dans la section "Suppression d'utilisateurs", page 392.

Si vous supprimez l'utilisateur guest de la base de données master, les utilisateurs du serveur qui n'ont pas encore été ajoutés à des bases de données ne pourront pas se connecter à Adaptive Server.

---

**Remarque** Plus d'une personne peut être utilisateur guest d'une base de données, mais vous pouvez utiliser l'ID de l'utilisateur sur le serveur qui est unique, pour contrôler les activités de chacun. Pour plus d'informations sur l'audit, reportez-vous au chapitre 12, "Audit".

---

### Autorisations de l'utilisateur "guest"

L'utilisateur "guest" hérite des privilèges du groupe "public". Le propriétaire de base de données et les propriétaires d'objets peuvent utiliser les commandes grant et revoke pour donner à "guest" plus ou moins d'autorisations que "public". Reportez-vous au chapitre 11, "Gestion des autorisations utilisateur", pour une description des privilèges de "public".

A l'installation d'Adaptive Server, master..sysusers contient une entrée guest. Le script d'installation de la base de données pubs2 contient aussi une entrée guest dans sa table sysusers.

### Utilisateur "guest" dans les bases de données utilisateur

Dans les bases de données utilisateur, le propriétaire de base de données ajoute un utilisateur guest qui donne à tous les utilisateurs l'accès à cette base. Ceci évite au propriétaire d'utiliser explicitement sp_adduser pour chaque nom d'utilisateur.

Vous pouvez utiliser le mécanisme guest pour restreindre l'accès aux objets de base de données tout en autorisant l'accès à la base.

Par exemple, le propriétaire de la table titles peut octroyer l'autorisation select sur la table titles à tous les utilisateurs de la base sauf "guest" par les commandes suivantes :

```
grant select on titles to public
sp_adduser guest
revoke all on titles from guest
```

### Utilisateur "guest" dans *pubs2* et *pubs3*

L'utilisateur "guest" dans les bases de données exemples permet aux nouveaux utilisateur de suivre les exemples du *Guide de l'utilisateur Transact-SQL*. L'utilisateur guest a des privilèges étendus, y compris :

- Autorisation select et de modification de données sur toutes les tables utilisateur
- Autorisation execute sur toutes les procédures
- Autorisations create table, create view, create rule, create default, et create procedure

## Création de comptes de visiteur

Le responsable de la sécurité du système peut utiliser sp_addlogin pour taper un nom de login et un mot de passe pour les utilisateurs visiteurs. Le plus souvent, ces utilisateurs ont des autorisations limitées. Il est possible de leur attribuer une base de données par défaut.

**Avertissement !** Un compte d'utilisateur visiteur n'est pas identique au compte utilisateur "guest". Tous les utilisateurs du compte visiteur ont le même ID d'utilisateur pour le serveur ; il est donc impossible de contrôler leurs activités individuellement. Chaque utilisateur "guest" a un ID unique sur le serveur, il est donc possible de contrôler son activité et d'assurer une comptabilisation individuelle. La configuration d'un compte visiteur utilisable par plus d'un utilisateur n'est pas recommandée à cause de cette perte de possibilité de comptabilisation individuelle.

Vous pouvez ajouter un compte d'utilisateur visiteur sous le nom "guest" dans master..syslogins par sp_addlogin. Ce compte d'utilisateur "guest" a priorité sur le compte utilisateur système "guest". Remarquez que si vous ajoutez un utilisateur visiteur "guest" avec sp_adduser, cet ajout a une influence sur les bases de données système telles que sybsystemprocs et sybsystemdb, qui ont été conçues pour fonctionner avec l'utilisateur système "guest".

### Ajout d'utilisateurs distants

Vous pouvez autoriser des utilisateurs d'un autre Adaptive Server à exécuter des procédures stockées sur votre serveur en activant l'accès distant. En collaboration avec l'administrateur système du serveur distant, vous pouvez aussi autoriser des utilisateurs de votre serveur à exécuter des **appels de procédure à distance** sur le serveur distant.

Pour autoriser les appels de procédure à distance, il faut configurer le serveur local et le serveur distant. Pour plus d'informations sur la configuration des serveurs distants et l'ajout d'utilisateurs distants, reportez-vous au chapitre 13, "Gestion des serveurs distants".

**Remarque** Les utilisateurs distants et les appels de procédure à distance ne sont pas inclus dans la configuration évaluée.

## Nombre d'utilisateurs et ID de login

Adaptive Server supporte plus de 2 000 000 000 de logins par serveur et d'utilisateurs par base de données. Adaptive Server utilise des nombres positifs et négatifs pour augmenter la plage de numéros disponibles pour les ID.

## Limites et plages de numéros ID

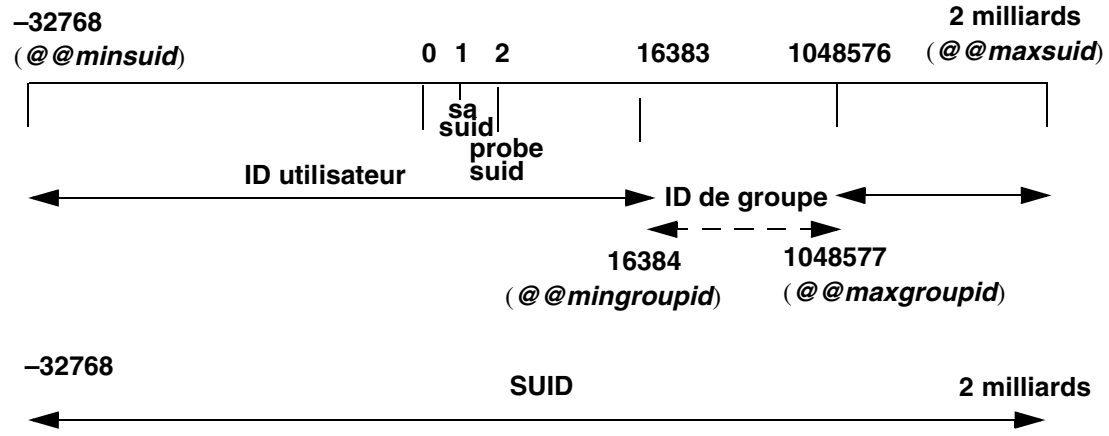
Le tableau 10-2 décrit les plages valides pour les types d'ID.

***Tableau 10-2 : Plages pour les types d'ID***

| Type d'ID | Limites du serveur |
|---|---|
| Logins par serveur (*suid*) | 2 milliards plus 32 ko |
| Utilisateurs par base (*uid*) | 2 milliards moins 1032193 |
| Groupes par base de données (*guid*) | 16 390 à 1 048 576 |

La figure 10-1 illustre les limites et les plages de logins, d'utilisateurs et de groupes.

***Figure 10-1 : Utilisateurs, groupes et logins disponibles dans Adaptive Server***




Adaptive Server peut supporter plus de 2 milliards d'utilisateurs connectés simultanément, mais le nombre effectif d'utilisateurs qui peuvent se connecter à Adaptive Server est limité par :

- Le paramètre de configuration number of user connections
- Le nombre de descripteurs de fichiers disponibles sur le système d'exploitation. Chaque login utilisateur nécessite un descripteur de fichier par connexion

**Remarque** Pour qu'Adaptive Server puisse gérer plus de 64 ko logins et connexions simultanés, vous devez configurer le système d'exploitation pour plus de 64 ko descripteurs de fichiers. Consultez la documentation du système d'exploitation pour plus d'informations sur l'augmentation du nombre de descripteurs de fichiers.

Consultez les notes sur la version pour des informations à jour sur les limites d'Adaptive Server pour les logins, les utilisateurs et les groupes.

## Limitations de connexion

Adaptive Server permet de définir plus de 2 milliards de logins par serveur, mais le nombre effectif d'utilisateurs qui peuvent se connecter à un instant donné à Adaptive Server est limité par :

- la valeur du paramètre de configuration number of user connections et
- le nombre de descripteurs de fichiers disponibles pour Adaptive Server. Chaque login utilise un descripteur de fichier pour la connexion.

**Remarque** Le type de données de l'ID de processus du serveur (*spid*) n'a pas été modifié. Donc, le nombre maximum de tâches actives simultanément sur le serveur est toujours de trente-deux mille.

Pour autoriser un nombre maximal de logins et de connexions simultanées :

1 Configurez le système d'exploitation sur lequel Adaptive Server s'exécute pour au moins trente-deux mille descripteurs de fichiers.

2 Définissez la valeur de number of user connections à au moins trente-deux mille.

**Remarque** Pour qu'Adaptive Server puisse gérer plus de 64 ko logins et connexions simultanés, vous devez configurer le système d'exploitation pour plus de 64 ko descripteurs de fichiers. Consultez la documentation du système d'exploitation pour plus d'informations sur l'augmentation du nombre de descripteurs de fichiers.

## Affichage des limites du serveur pour les logins, les utilisateurs et les groupes

Le tableau 10-3 donne la liste des variables globales pour les limites du serveur en logins, utilisateurs et groupes :

***Tableau 10-3 : Variables globales pour les logins, utilisateurs et groupes***

| Nom de variable | Affichage | Valeur |
|---|---|---|
| @@*invaliduserid* | ID utilisateur non valide | –1 |
| @@*minuserid* | Plus petit ID utilisateur | –32768 |
| @@*guestuserid* | ID utilisateur guest | 2 |
| @@*mingroupid* | Plus petit ID utilisateur de groupe | 16384 |
| @@*maxgroupid* | Plus grand ID utilisateur de groupe | 1048576 |
| @@*maxuserid* | Plus grand ID utilisateur | 2147483647 |
| @@*minsuid* | Plus petit ID utilisateur de serveur | –32768 |
| @@*probesuid* | ID utilisateur probe | 2 |
| @@*maxsuid* | Plus grand ID utilisateur de serveur | 2147483647 |

Pour connaître la valeur d'une variable globale, tapez :

```
select nom_variable
```

Par exemple :

```
select @@minuserid
-----------
-32768
```

# Création et attribution de rôles aux utilisateurs

Les dernières étapes de l'ajout d'utilisateurs de base de données consistent à leur attribuer des rôles spéciaux, selon les besoins et à leur octroyer des autorisations. Pour plus d'informations sur les autorisations, reportez-vous au chapitre 11, "Gestion des autorisations utilisateur".

Les rôles supportés par Adaptive Server vous permettent de mettre en place le principe de traçabilité des utilisateurs. Adaptive Server propose des *rôles système* (administrateur système et responsable de la sécurité du système) et des *rôles utilisateur* créés par un responsable de la sécurité du système. Les propriétaires d'objets peuvent octroyer des droits d'accès à la base de données adaptés à chaque rôle.

Le tableau 10-4 donne la liste des rôles système, la valeur à utiliser pour l'option *role_granted* de la commande grant role ou revoke role, ainsi que les tâches effectuées habituellement par une personne ayant ce rôle.

***Tableau 10-4 : Rôles système et tâches associées***

| Rôle | Valeur de *role_granted* | Description |
|---|---|---|
| Administrateur système (SA) | sa_role | Gère et assure la maintenance du stockage sur disque et des bases de données Adaptive Server |
| Responsable de la sécurité du système (SSO) | sso_role | Effectue les tâches relatives à la sécurité |
| Opérateur | oper_role | Sauvegarde et restaure les bases de données à l'échelle du serveur |

**Remarque** Les rôles sybase_ts_role, replication_role et navigation_role ne sont pas inclus dans la configuration évaluée.

## Planification des rôles définis par l'utilisateur

Avant de mettre en place des rôles définis par l'utilisateur, vous devez définir :

- Les rôles à créer
- Les responsabilités de chaque rôle
- La position de chacun dans la hiérarchie de rôles
- Les rôles de la hiérarchie qui doivent être mutuellement exclusifs
- La mise en place de l'exclusivité au niveau de l'appartenance ou au niveau de l'activation

Les noms de rôles définis par l'utilisateur ne peuvent pas être identiques à des noms d'utilisateurs.

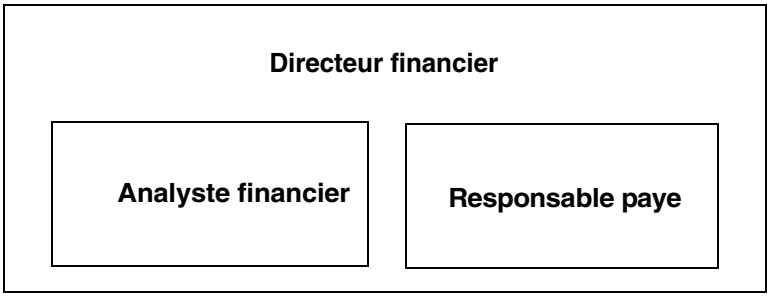
Évitez les conflits de noms lors de la création de rôles définis par l'utilisateur en suivant une convention de noms. Par exemple, vous pouvez utiliser le suffixe "_role" pour les noms de rôles. Adaptive Server ne contrôle pas ces restrictions.

Si un rôle doit avoir le même nom qu'un utilisateur, vous pouvez éviter le conflit en créant un nouveau rôle contenant le rôle d'origine, puis en octroyant le nouveau rôle à l'utilisateur.

## Hiérarchie de rôles et exclusivité mutuelle

Un responsable de la sécurité du système (SSO) peut hiérarchiser les rôles de sorte que, si un utilisateur possède un rôle, il possède aussi ceux qui en dépendent dans la hiérarchie. Par exemple, le rôle "directeur_financier" peut contenir deux rôles, "analyste_financier" et "responsable_paye", comme indiqué à la figure 10-2.

***Figure 10-2 : Hiérarchisation des rôles***




Ainsi, le directeur financier pourra effectuer toutes les tâches et voir toutes les données des analystes et des responsables de paye qui lui sont subordonnés.

Il est possible de définir des rôles qui s'excluent mutuellement au niveau de :

- Appartenance – un utilisateur ne peut pas se voir attribuer deux rôles différents. Par exemple, vous pouvez souhaiter interdire l'octroi des rôles "demandeur_paiement" et "approbateur_paiement" au même utilisateur.

- Activation – un utilisateur ne peut pas activer deux rôles différents. Par exemple, un utilisateur peut se voir octroyer les deux rôles "auditeur" et "acheteur", sans qu'on lui donne l'autorisation d'avoir les deux rôles activés simultanément.

Les rôles système, ainsi que les rôles utilisateur, peuvent être définis dans une hiérarchie ou être mutuellement exclusifs. Ainsi, vous définirez un rôle "super_user" qui contiendra les rôles Administrateur système, Opérateur et "tech_support". Vous indiquerez que les rôles Administrateur système et Responsable de la sécurité du système s'excluent mutuellement au niveau de l'appartenance, de sorte qu'un utilisateur ne pourra pas se voir attribuer les deux rôles.

## Configuration de rôles définis par l'utilisateur

Après planification des rôles à créer et des relations entre eux, configurez votre système pour les rôles définis par l'utilisateur avec le paramètre de configuration max roles enabled per user.

Un utilisateur peut activer au maximum 127 rôles par session. La valeur par défaut est 20. Le nombre minimum de rôles, 10, inclut les rôles système livrés avec Adaptive Server.

Le nombre maximum de rôles pouvant être activés à l'échelle du serveur est 992. Les 32 premiers rôles sont réservés pour les rôles système Sybase.

## Création d'un rôle défini par l'utilisateur

Créez le rôle à l'aide de la commande create role. Respectez la syntaxe suivante :

create role *nom_rôle* [with passwd "*mot_de_passe*"]

où :

- *nom_rôle* est le nom du nouveau rôle.
- *mot_de_passe* est un mot de passe facultatif que l'utilisateur devra donner pour utiliser le rôle.

Par exemple, pour créer le rôle rôle_interne sans mot de passe, tapez :

```
create role rôle_interne
```

Pour créer le rôle rôle_docteur avec le mot de passe "médecin", tapez :

```
create role rôle_docteur with passwd "médecin"
```

## Ajout et suppression de mots de passe pour un rôle

Seul un responsable de la sécurité du système peut ajouter ou supprimer un mot de passe pour un rôle.

Utilisez la commande alter role pour ajouter ou supprimer un mot de passe pour un rôle système ou défini par l'utilisateur. Respectez la syntaxe suivante :

alter role *nom_rôle* [add passwd "*mot_de_passe*" |
drop passwd]

Par exemple pour imposer le mot de passe "oper8x" pour oper_role, tapez :

```
alter role oper_role add passwd oper8x
```

Pour supprimer le mot de passe pour ce rôle, tapez :

```
alter role oper_role drop passwd
```

## Définition et changement de rôles mutuellement exclusifs

Pour définir une exclusivité mutuelle entre deux rôles, utilisez :

alter role *rôle1* { add | drop } exclusive { membership | activation } *rôle2*

Par exemple, pour rendre mutuellement exclusifs rôle_interne et rôle_spécialiste au niveau appartenance, tapez :

```
alter role rôle_interne add exclusive membership
rôle_spécialiste
```

Pour rendre mutuellement exclusifs sso_role et sa_role au niveau activation, tapez :

```
alter role sso_role add exclusive activation sa_role
```

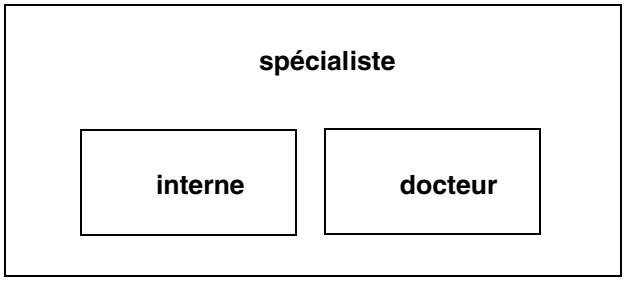
## Définition et modification d'une hiérarchie de rôles

La définition d'une hiérarchie de rôles nécessite le choix du type de hiérarchie et des rôles, avant mise en place de la hiérarchie par octroi de rôles à d'autres rôles.

Par exemple :

```
grant role rôle_interne to rôle_spécialiste
grant role rôle_docteur to rôle_spécialiste
```

***Figure 10-3 : Création d'une hiérarchie de rôles***




Dans la figure 10-3, le rôle "spécialiste" contient les rôles "docteur" et "interne". Donc le rôle "spécialiste" dispose de tous les privilèges des rôles "docteur" et "interne".

Pour établir une hiérarchie avec un rôle "super_user" contenant les rôles système sa_role et oper_role, spécifiez :

```
grant role sa_role to super_user
grant role oper_role to super_user
```

---

**Remarque** Si un rôle nécessitant un mot de passe est contenu dans un autre rôle, l'utilisateur dont le rôle contient l'autre n'a pas besoin d'utiliser le mot de passe du rôle contenu. Par exemple, dans la figure 10-3, supposons que le rôle "docteur" nécessite d'habitude un mot de passe. L'utilisateur ayant le rôle "spécialiste" n'a pas besoin de taper le mot de passe du rôle "docteur" parce que "docteur" est contenu dans "spécialiste". Les mots de passe de rôle ne sont nécessaires que pour le rôle de niveau le plus élevé.

---

Pour créer des hiérarchies de rôles :

- Vous ne pouvez pas octroyer un rôle à un autre rôle qui le contient directement. Ceci évite les duplications.

  Par exemple, dans la figure 10-3, vous ne pouvez pas octroyer le rôle "docteur" à "spécialiste" parce que "spécialiste" contient déjà "docteur".

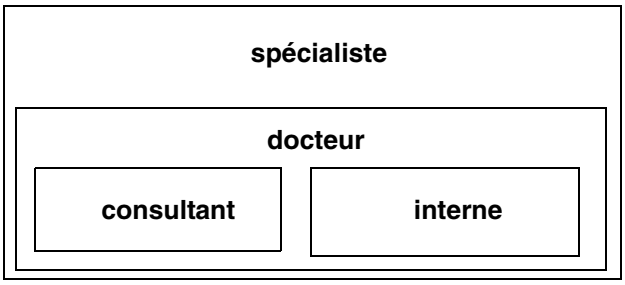
- Vous pouvez octroyer un rôle à un autre rôle qui ne le contient pas directement.

  Par exemple, dans la figure 10-4, vous pouvez octroyer le rôle "interne" au rôle "spécialiste", bien que "spécialiste" contienne déjà le rôle "docteur" qui contient "interne". Si vous supprimez ensuite "docteur" du rôle "spécialiste", le rôle "spécialiste" contiendra toujours "interne".

  Dans la figure 10-4, le rôle "docteur" contient les autorisations du rôle "consultant" parce que "consultant" a été octroyé à "docteur". Le rôle "spécialiste" a aussi les autorisations du rôle "consultant" parce que "spécialiste" contient le rôle "docteur" qui lui-même contient "consultant".

  Mais "interne" n'a pas les privilèges du rôle "consultant", parce que "interne" ne contient pas le rôle "consultant", ni directement ni indirectement.

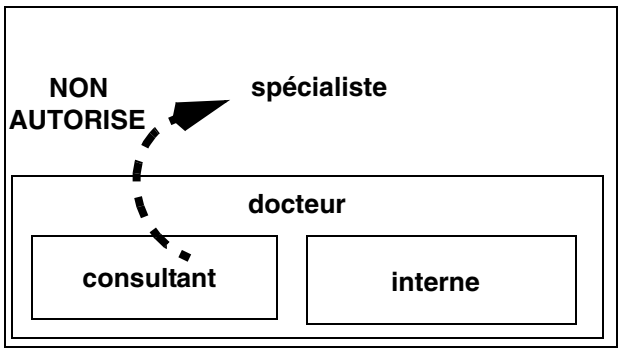
***Figure 10-4 : Privilèges octroyés implicitement et explicitement***




- Vous ne pouvez pas octroyer un rôle à un autre rôle contenu dans le premier. Ceci évite les "boucles" dans la hiérarchie.

  Par exemple, dans la figure 10-5, vous ne pouvez pas octroyer le rôle "spécialiste" au rôle "consultant" ; "consultant" est déjà contenu dans "spécialiste".

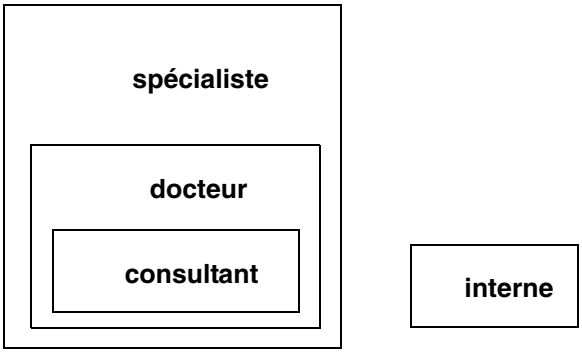
***Figure 10-5 : Octroi d'un rôle à un rôle contenu par l'octroyeur***




- Quand le responsable de la sécurité du système octroie à un utilisateur un rôle contenant d'autres rôles, l'utilisateur obtient implicitement tous les rôles contenus dans le rôle octroyé. Mais un rôle ne peut être activé ou désactivé directement que si l'utilisateur a une appartenance explicite à ce rôle.
- Le responsable de la sécurité du système ne peut pas octroyer un rôle à un autre rôle explicitement ou implicitement mutuellement exclusif au niveau appartenance avec le premier rôle.

  Par exemple, dans la figure 10-6, si le rôle "interne" est défini comme mutuellement exclusif au niveau appartenance avec le rôle "consultant", le responsable de la sécurité du système ne peut pas octroyer le rôle "interne" au rôle "docteur".

***Figure 10-6 : Exclusivité mutuelle au niveau appartenance***

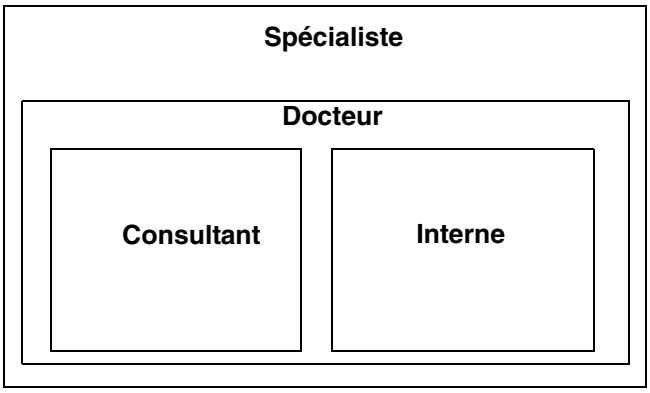


- L'utilisateur ne peut activer ou désactiver que les rôles octroyés directement.

  Par exemple, dans la hiérarchie présentée sur la figure 10-6, supposons que vous ayez le rôle "spécialiste". Vous avez toutes les autorisations du rôle "spécialiste" et implicitement, à cause de la hiérarchie, toutes les autorisations des rôles "docteur" et "consultant". Mais vous ne pouvez activer que le rôle "spécialiste". Vous ne pouvez pas activer les rôles "docteur" ou "consultant" parce qu'ils ne vous ont pas été octroyés directement. Pour plus d'informations, reportez-vous à la section "Activation et désactivation de rôles", page 391.

  La révocation des rôles depuis d'autres rôles est comparable à l'octroi de rôles à d'autres rôles. Elle supprime une relation d'inclusion et cette relation d'inclusion doit être directe, comme indiqué dans la figure 10-7 :

***Figure 10-7 : Effet d'une révocation de rôles sur la hiérarchie des rôles***




Par exemple, dans la figure 10-7 :

- Si le responsable de la sécurité du système révoque le rôle "docteur" du rôle "spécialiste", "spécialiste" ne contient plus le rôle "consultant" ni le rôle "interne".
- Le responsable de la sécurité du système ne peut pas révoquer le rôle "interne" du rôle "spécialiste" parce que "interne" n'est pas contenu directement par "spécialiste".

## Définition de l'activation par défaut à la connexion

Un responsable de la sécurité du système peut modifier le paramètre par défaut d'un rôle pour tout utilisateur. Les utilisateurs individuels ne peuvent modifier que leurs paramètres par défaut.

Quand un utilisateur se connecte à Adaptive Server, ses rôles ne sont pas nécessairement actifs, selon la valeur par défaut définie par le rôle. Si un rôle a un mot de passe associé, l'utilisateur doit émettre la commande set role pour activer le rôle.

Le responsable de la sécurité du système ou l'utilisateur détermine si les rôles octroyés doivent être activés par défaut à la connexion. sp_modifylogin définit l'état par défaut des rôles utilisateur individuellement pour chacun. sp_modifylogin ne modifie que les rôles utilisateur et non pas les rôles système.

Par défaut, les rôles définis par l'utilisateur ne sont pas activés à la connexion, mais les rôles système sont activés automatiquement s'ils n'ont pas de mot de passe associé.

Pour configurer un rôle comme activé à la connexion :

```
sp_modifylogin nom_login, "add default role", nom_rôle
```

Pour garantir qu'un rôle est inactif à la connexion :

```
sp_modifylogin nom_login, "drop default role", nom_rôle
```

Par exemple, pour changer le paramètre par défaut du rôle_interne de Ralph de façon à l'activer automatiquement à la connexion, exécutez :

```
sp_modifylogin ralph, "add default role", rôle_interne
```

## Activation et désactivation de rôles

Les rôles doivent être actifs pour bénéficier des privilèges d'accès de chaque rôle. Selon la valeur par défaut définie pour un rôle, celui-ci peut être actif ou non à la connexion. Si le rôle est associé à un mot de passe, il est toujours inactif à la connexion.

Pour activer ou désactiver un rôle :

```
set role nom_rôle [on|off]
```

Pour activer ou désactiver un rôle associé à un mot de passe, utilisez :

```
set role nom_rôle with passwd "mot_de_passe" [on|off]
```

Par exemple, pour activer le rôle "analyste_financier" avec le mot de passe "sailing19", tapez :

```
set role analyste_financier with passwd "sailing19" on
```

Vous ne devez activer les rôles que quand vous en avez besoin et les désactiver quand vous ne les utilisez plus. Par exemple, quand le sa_role est actif, vous prenez l'identité du propriétaire de base de données dans toute base de données que vous utilisez. Pour désactiver le rôle d'administrateur système et reprendre votre identité d'utilisateur "réelle", utilisez :

```
set role sa_role off
```

Si un rôle vous est octroyé pendant une session, pour l'activer immédiatement, utilisez set role.

# Suppression d'utilisateurs, de groupes et de rôles définis par l'utilisateur

Le tableau 10-5 donne la liste des procédures système qui permettent à un administrateur système ou un propriétaire de base de données de supprimer des utilisateurs et des groupes.

***Tableau 10-5 : Suppression d'utilisateurs et de groupes***

| Tâche | Rôle nécessaire | Procédure système | Base de données |
|---|---|---|---|
| Suppression d'un utilisateur de la base de données | Propriétaire de la base de données ou administrateur système | sp_dropuser | Utilisateur de base de données |
| Suppression d'un groupe de la base de données | Propriétaire de la base de données ou administrateur système | sp_dropgroup | Utilisateur de base de données |

## Suppression d'utilisateurs

Un propriétaire de base de données ou un administrateur système peut utiliser sp_dropuser pour interdire à un utilisateur Adaptive Server l'accès à la base de données dans laquelle sp_dropuser est exécuté. (Si un utilisateur "guest" est défini dans cette base, l'utilisateur peut toujours accéder à la base en tant que "guest").

Respectez la syntaxe suivante :

sp_dropuser *nom_dans_base*

où *nom_dans_base* est le plus souvent le nom de login, sauf si un autre nom a été attribué à l'utilisateur.

Vous ne pouvez pas supprimer un utilisateur propriétaire d'objets. Il n'y a pas de commande permettant de transférer la propriété d'objets, vous devez donc supprimer les objets dont l'utilisateur est propriétaire avant de supprimer l'utilisateur avec sp_dropuser. Pour interdire l'accès à un utilisateur propriétaire d'objets, utilisez sp_locklogin pour verrouiller son compte.

Vous ne pouvez pas supprimer d'une base de données un utilisateur qui a octroyé des autorisations à d'autres utilisateurs. Utilisez revoke with cascade pour révoquer les autorisations de tous les utilisateurs qui se sont vu octroyer des autorisations par l'utilisateur à supprimer, avant de supprimer l'utilisateur. Vous devrez ensuite octroyer à nouveau les autorisations aux utilisateurs, si nécessaire.

## Suppression de groupes

Utilisez sp_dropgroup pour supprimer un groupe. Respectez la syntaxe suivante :

```
sp_dropgroup nom_groupe
```

Il est impossible de supprimer un groupe contenant des membres. Si vous tentez de le faire, l'état d'erreurs affiche une liste des membres du groupe que vous tentez de supprimer. Pour supprimer des utilisateurs d'un groupe, utilisez sp_changegroup, détaillé dans la section "Modification des appartenances d'utilisateur à un groupe", page 399.

## Suppression de rôles définis par l'utilisateur

Pour supprimer un rôle, utilisez :

drop role *nom_rôle* [with override]

où *nom_rôle* est le nom d'un rôle défini par l'utilisateur. with override révoque tous les droits d'accès octroyés au rôle dans chaque base de données à l'échelle du serveur.

Si le rôle a déjà des privilèges d'accès octroyés, vous devez révoquer tous les privilèges octroyés au rôle dans toutes les bases de données pour pouvoir supprimer le rôle. Sinon, la commande échoue. Pour révoquer des privilèges :

- utilisez la commande revoke ou
- utilisez l'option with override avec la commande drop role. L'option with override demande à Adaptive Server de supprimer automatiquement les informations d'autorisation pour le rôle dans toutes les bases de données.

Vous n'avez pas besoin de supprimer les liens d'appartenance à un rôle avant de supprimer ce dernier. La suppression d'un rôle annule automatiquement l'appartenance de l'utilisateur à ce rôle, que vous utilisiez ou non l'option with override.

# Verrouillage ou suppression de comptes de connexion Adaptive Server

Pour empêcher un utilisateur de se connecter à Adaptive Server, vous pouvez verrouiller ou supprimer son compte de connexion. Le verrouillage d'un login est plus sûr que la suppression parce que le verrouillage d'un compte de connexion conserve le suid pour éviter qu'il soit réutilisé.

---

**Avertissement !** Adaptive Server peut réutiliser l'ID utilisateur du serveur (suid) d'un compte de connexion supprimé lors de la création du login suivant. Cette situation survient uniquement lorsque le login supprimé détient le suid le plus élevé dans syslogins. La gestion des comptes peut être compromise si l'exécution de sp_droplogin ne fait pas l'objet d'un audit. L'utilisateur d'un suid réutilisé peut aussi accéder aux objets de base de données qui étaient autorisés à l'ancien détenteur du suid.

---

Vous ne pouvez pas supprimer un login quand :

- l'utilisateur est dans une base de données quelconque,
- le login appartient au dernier responsable de la sécurité du système ou administrateur système.

***Tableau 10-6 : Verrouillage ou suppression de comptes de connexion***

| Tâche | Rôle requis | Procédure système | Base de données |
|---|---|---|---|
| Verrouillage du compte de connexion, ce qui conserve le suid pour éviter toute réutilisation | Responsable de la sécurité du système ou administrateur système | sp_locklogin | master |
| Suppression du compte de connexion, autorisant la réutilisation du suid | Administrateur système (SA) | sp_droplogin | master |

## Verrouillage et déverrouillage des comptes de connexion

Utilisez sp_locklogin pour verrouiller et déverrouiller des comptes ou afficher une liste des comptes verrouillés. Vous devez être administrateur système ou responsable de la sécurité du système pour utiliser sp_locklogin.

Respectez la syntaxe suivante :

```
sp_locklogin [nom_login, "{lock | unlock}"]
```

où :

- *nom_login* désigne le compte à verrouiller ou à déverrouiller. Ce doit être un compte existant et valide.
- lock | unlock indique si le compte doit être verrouillé ou déverrouillé.

Pour afficher une liste des logins verrouillés, utilisez sp_locklogin sans paramètres.

Vous ne pouvez pas verrouiller un compte quand il est connecté, le compte de l'utilisateur n'est verrouillé que quand il se déconnecte. Vous pouvez verrouiller le compte d'un propriétaire de base de données et un compte verrouillé peut être propriétaire d'objets dans des bases de données. De plus, vous pouvez utiliser sp_changedbowner pour spécifier un compte verrouillé comme propriétaire d'une base de données.

Adaptive Server s'assure qu'il reste toujours au moins un compte de responsable de la sécurité du système déverrouillé et un compte d'administrateur système déverrouillé.

## Suppression de comptes de connexion

Un administrateur système peut utiliser sp_droplogin pour interdire à un utilisateur l'accès à Adaptive Server. Respectez la syntaxe suivante :

```
sp_droplogin nom_login
```

Vous ne pouvez pas utiliser sp_droplogin pour supprimer un utilisateur d'une base de données sur le serveur. Pour supprimer un utilisateur d'une base de données, exécutez sp_dropuser. Vous ne pouvez pas supprimer un utilisateur d'une base de données s'il possède des objets situés dans cette dernière. Pour plus d'informations, reportez-vous à la section "Suppression d'utilisateurs", page 392.

## Verrouillage de logins propriétaires de seuils

Cette section traite des seuils et de l'effet des verrouillages des logins utilisateur sur ces seuils.

- Par mesure de sécurité, les procédures stockées de seuil sont exécutées sous le nom de compte et les rôles du login qui a créé la procédure.
  - Vous ne pouvez pas supprimer le login d'un utilisateur propriétaire d'un seuil.
  - Si vous verrouillez le login d'un utilisateur propriétaire d'un seuil, le seuil ne peut pas exécuter la procédure stockée correspondante.
- Les procédures de seuil sont exécutées dans le moins limitatif des ensembles de rôles attribués à un utilisateur. L'utilisateur doit avoir à la fois :
  - l'ensemble de rôles actifs pour l'utilisateur au moment de l'ajout ou de la dernière modification du seuil et
  - l'ensemble de rôles octroyés directement à l'utilisateur à chaque "déclenchement" du seuil.
- Si un seuil nécessite un rôle particulier, ce rôle doit être actif pour l'utilisateur à la création du seuil. Si ce rôle est révoqué ultérieurement, le seuil ne peut pas exécuter la procédure.
- Le seuil ultime et les seuils créés par le login "sa" ne sont pas concernés par sp_locklogin. Si vous verrouillez le login "sa", le seuil ultime et les seuils créés ou modifiés par l'utilisateur "sa" se déclenchent toujours.

# Modification des informations utilisateur

Le tableau 10-7 donne la liste des procédures système utilisables pour changer les mots de passe, la base de données par défaut, la langue par défaut, le nom complet ou l'appartenance à un groupe.

***Tableau 10-7 : Procédures système de modification des informations utilisateur***

| Tâche | Rôle requis | Procédure système | Base de données |
|---|---|---|---|
| Changement de votre mot de passe | Aucun | sp_password | Toute base de données |
| Changement du mot de passe d'un autre utilisateur | Responsable de la sécurité du système (SSO) | sp_password | Toute base de données |
| Changement de votre base de données par défaut, langue par défaut ou nom complet | Aucun | sp_modifylogin | Toute base de données |
| Changement de la base de données par défaut, langue par défaut ou nom complet d'un compte de connexion | Administrateur système (SA) | sp_modifylogin | Toute base de données |
| Changement de l'appartenance à un groupe d'un utilisateur | Administrateur système, propriétaire de la base de données | sp_changegroup | Utilisateur de base de données |

## Changement des mots de passe

Tous les utilisateurs peuvent changer leur mot de passe à tout moment par sp_password. Le responsable de la sécurité du système peut exécuter sp_password pour changer le mot de passe de tout utilisateur. Respectez la syntaxe suivante :

```
sp_password motdepasse_demandeur, nouveau_motdepasse
[,nom_login]
```

où :

- *motdepasse_demandeur* est le mot de passe du compte de connexion qui exécute sp_password.
- *nouveau_motdepasse* est le nouveau mot de passe pour l'utilisateur qui exécute sp_password ou pour l'utilisateur indiqué par *nom_login*. Pour des règles de choix et de création de mots de passe sécurisés, reportez-vous à la section "Choix et création d'un mot de passe", page 371.

- *nom_login* ne peut être utilisé pour changer le mot de passe d'un autre utilisateur que par un responsable de la sécurité du système.

Par exemple, un utilisateur peut changer son mot de passe de "3blindmice" en "2mediumhot" par :

```
sp_password "3blindmice", "2mediumhot"
```

Ces mots de passe sont entre guillemets car ils commencent par des chiffres.

Dans l'exemple ci-dessous, le responsable de la sécurité du système dont le mot de passe est "2tomato" change le mot de passe de Victoria en "sesame1" :

```
sp_password "2tomato", sesame1, victoria
```

## Exigence de nouveaux mots de passe

Votre site peut choisir d'utiliser le paramètre de configuration systemwide password expiration pour définir un intervalle de péremption de mot de passe qui force tous les utilisateurs à changer régulièrement leur mot de passe. Pour plus d'informations, reportez-vous au chapitre 5, "Définition des paramètres de configuration". Même si vous n'utilisez pas systemwide password expiration, il est important, pour des raisons de sécurité, que les utilisateurs changent régulièrement leur mot de passe.

La colonne pwdate dans la table syslogins enregistre la date de dernier changement de mot de passe. La requête ci-dessous sélectionne tous les noms de logins dont les mots de passe n'ont pas changé depuis le 15 septembre 1997 :

```
select name, pwdate
from syslogins
where pwdate < "Sep 15 1997"
```

## mots de passe null

N'utilisez pas de mot de passe null. A l'installation d'Adaptive Server, le compte "sa" par défaut a un mot de passe null (vide). L'exemple ci-dessous montre comment changer un mot de passe vide en un mot de passe valide :

```
sp_password null, "8M4LNCH"
```

Remarquez que "null" n'est pas entre guillemets dans l'instruction.

## Modification des valeurs par défaut utilisateur

Tout utilisateur peut appeler sp_modifylogin pour changer sa base de données par défaut, sa langue par défaut ou son nom complet. sp_modifylogin ne peut modifier que les rôles utilisateur et non pas les rôles système. Un administrateur système peut modifier ces paramètres pour tout utilisateur. Respectez la syntaxe suivante :

sp_modifylogin *compte*, *colonne*, *valeur*

- *compte* est le nom de l'utilisateur dont vous modifiez le compte.
- *colonne* spécifie l'option à modifier. Les options sont les suivantes :
  - base_de_données_par_défaut : Répertoire d'"accueil" auquel l'utilisateur est connecté lorsqu'il ouvre une session
  - deflanguage : Nom officiel de la langue par défaut de l'utilisateur, tel qu'il est enregistré dans master..syslanguages
  - fullname : Nom complet de l'utilisateur
- *valeur* : désigne la nouvelle valeur de l'option spécifiée.

Après l'exécution de sp_modifylogin pour modifier la base de données par défaut, l'utilisateur est connecté à la nouvelle base à sa prochaine connexion. Mais sp_modifylogin n'attribue pas automatiquement le droit d'accès de l'utilisateur à la base de données. Sauf si le propriétaire de base de données a configuré l'accès avec sp_adduser, sp_addalias ou un utilisateur guest, l'utilisateur est connecté à master même après changement de sa base de données par défaut.

Cet exemple change la base de données par défaut pour "anna" en pubs2 :

```
sp_modifylogin anna, defdb, pubs2
```

Cet exemple change la langue par défaut pour "claire" en français :

```
sp_modifylogin claire, deflanguage, french
```

Cet exemple change le nom complet pour "mtwain" en "Samuel Clemens".

```
sp_modifylogin mtwain, fullname, "Samuel Clemens"
```

## Modification des appartenances d'utilisateur à un groupe

Un administrateur système ou le propriétaire de base de données peut utiliser sp_changegroup pour changer l'affiliation d'un utilisateur à un groupe. Chaque utilisateur ne peut être membre que d'un seul groupe autre que "public", dont tous les utilisateurs sont toujours membres.

Avant d'exécuter sp_changegroup :

- Le groupe doit exister. (Utilisez sp_addgroup pour créer un groupe).
- L'utilisateur doit avoir accès à la base de données en cours (il doit apparaître dans sysusers).

La syntaxe de sp_changegroup est la suivante :

```
sp_changegroup nom_grp, nom_utilisateur
```

Par exemple, pour passer l'utilisateur "jim" de son groupe en cours au groupe "manage", utilisez :

```
sp_changegroup manage, jim
```

Pour supprimer un utilisateur d'un groupe sans l'inclure dans un autre groupe, vous devez changer son affiliation de groupe en "public" :

```
sp_changegroup "public", jim
```

Le nom "public" doit être entre guillemets parce que c'est un mot réservé. Cette commande réduit l'affiliation de groupe de Jim au groupe "public" seulement.

Lorsqu'un utilisateur passe d'un groupe à un autre, il perd toutes les autorisations qu'il détenait de par son appartenance à l'ancien groupe et obtient les autorisations octroyées au nouveau groupe.

L'affiliation d'utilisateurs à des groupes peut être modifiée à tout moment.

## Modification des informations sur le processus utilisateur

La commande set inclut des options permettant d'attribuer à chaque client un nom, un nom d'hôte et un nom d'application. C'est utile pour faire la différence entre clients sur un système où plusieurs clients se connectent à Adaptive Server avec le même nom, nom d'hôte ou nom d'application.

La syntaxe partielle de la commande set est la suivante :

```
set [clientname nom_client | clienthostname nom_hôte |
clientapplname nom_application]
```

Où *nom_client* est le nom à attribuer au client, *nom_hôte* le nom de l'hôte depuis lequel le client se connecte et *nom_application* le nom de l'application avec laquelle il se connecte à Adaptive Server. Ces paramètres sont enregistrés dans les colonnes clientname, clienthostname, clientapplname de la table sysprocesses.

Par exemple, si un utilisateur se connecte à Adaptive Server comme "client1", vous pouvez lui attribuer un nom de client, un nom d'hôte et un nom d'application par des commandes telles que celles-ci :

```
set clientname 'alison'
set clienthostname 'money1'
set clientapplname 'webserver2'
```

Cet utilisateur apparaît maintenant dans la table sysprocesses sous le nom d'utilisateur "alison" connecté depuis "money1" et utilisant l'application "webserver2". Mais, bien que ces nouveaux noms apparaissent dans sysprocesses, ils ne sont pas utilisés pour les contrôles d'autorisations et sp_who affiche toujours la connexion client comme appartenant au login d'origine (dans le cas ci-dessus, client1). set clientname n'effectue pas la même fonction que set proxy qui permet de bénéficier des autorisations, du nom de login et du suid d'un autre utilisateur.

Vous ne pouvez définir un nom de client, un nom d'hôte ou un nom d'application que pour votre session client en cours (mais vous pouvez consulter les informations de toute connexion client). Ces informations sont perdues lorsque l'utilisateur se déconnecte. Ces paramètres doivent être réattribués à chaque connexion d'un utilisateur. Par exemple, l'utilisateur alison ne peut pas définir le nom de client, le nom d'hôte ou le nom d'application pour une autre connexion client.

Utilisez le spid du client pour afficher ses informations de connexion. Par exemple, si le client "alison" décrit ci-dessus se connecte avec le spid 13, la commande ci-dessous permet d'afficher toutes les informations de connexion sur ce client :

```
select * from sysprocesses where spid = 13
```

Pour afficher les informations correspondant à la connexion client en cours (par exemple, si l'utilisateur alison souhaite consulter ses informations de connexion), tapez :

```
select * from sysprocesses where spid = @@spid
```

# Utilisation d'alias dans les bases de données

Le mécanisme d'alias permet de traiter deux ou plusieurs utilisateurs comme un même utilisateur à l'intérieur d'une base de données, avec les mêmes privilèges. Ce mécanisme est souvent utilisé pour permettre à plus d'un utilisateur de prendre le rôle de propriétaire de base de données. Un propriétaire de base de données peut utiliser la commande setuser pour incarner un autre utilisateur dans la base. Vous pouvez aussi utiliser le mécanisme d'alias pour définir une identité utilisateur collective.

Par exemple, supposons que plusieurs vice-présidents souhaitent utiliser une base de données avec des privilèges et des relations de propriété identiques. Si vous ajoutez le login "vp" à Adaptive Server et si chaque vice-président se connecte comme "vp", il n'y a pas moyen de distinguer les individus. Vous pouvez plutôt créer des alias de tous les vice-présidents, avec un compte Adaptive Server pour chacun, comme équivalent du nom d'utilisateur de base de données "vp".

**Remarque** Plusieurs utilisateurs peuvent utiliser l'alias dans une base de données, mais vous pouvez conserver la possibilité de comptabilisation individuelle par audit des opérations de base de données effectué par chaque utilisateur. Pour plus d'informations sur l'audit, reportez-vous au chapitre 12, "Audit".

Le tableau 10-8 donne la liste des procédures système utilisées pour gérer les alias :

***Tableau 10-8 : Procédures système pour la gestion des alias***

| Tâche | Rôle requis | Procédure système | Base de données |
|---|---|---|---|
| Ajouter un alias pour un utilisateur | Propriétaire de la base de données ou administrateur système | sp_addalias | Utilisateur de base de données |
| Supprimer un alias | Propriétaire de la base de données ou administrateur système | sp_dropalias | Utilisateur de base de données |

**Remarque** Depuis la version 12.0, il n'est plus possible de supprimer l'alias d'un login si ce login a créé des objets dans la base de données. Dans la plupart des cas, vous devez n'utiliser des alias que pour les utilisateurs qui ne sont pas propriétaires de tables, de procédures, de vues ou de triggers.

## Ajout d'alias

Pour ajouter un alias pour un utilisateur, utilisez sp_addalias. Respectez la syntaxe suivante :

sp_addalias *nom_login*, *nom_dans_base*

où :

*nom_login* est le nom de l'utilisateur qui souhaite un alias dans la base de données en cours. Cet utilisateur doit avoir un compte dans Adaptive Server, mais ne peut pas être un utilisateur de la base de données en cours.

*nom_dans_base* est le nom de l'utilisateur de base de données auquel l'utilisateur spécifié par *nom_login* doit être lié. Le *nom_dans_base* doit exister à la fois dans master..syslogins et dans sysusers de la base de données en cours.

L'exécution de sp_addalias fait correspondre le nom d'utilisateur spécifié par *nom_login* au nom d'utilisateur spécifié par *nom_dans_base*. Pour cela il ajoute une ligne à la table système sysalternates.

Quand un utilisateur tente d'utiliser une base de données, Adaptive Server recherche le numéro ID utilisateur de serveur (suid) dans sysusers. S'il ne le trouve pas, Adaptive Server recherche dans sysalternates. Si le *suid* de l'utilisateur est trouvé dans cette table et s'il correspond à un *suid* d'utilisateur de base de données, le premier utilisateur est traité comme le second tant que le premier utilise la base de données.

Par exemple, supposons que Mary soit propriétaire d'une base de données. Elle souhaite autoriser Jane et Sarah à utiliser la base de données comme si elles en étaient propriétaires. Jane et Sarah disposent de logins sur Adaptive Server mais ne sont pas autorisées à utiliser la base de données de Mary. Mary exécute la commande suivante :

```
sp_addalias jane, dbo
exec sp_addalias sarah, dbo
```

---

**Avertissement !** Les utilisateurs alias du propriétaire de base de données ont toutes les autorisations et peuvent effectuer toutes les actions que peut effectuer le vrai propriétaire de base de données, sur cette base. Un propriétaire de base de données doit prendre en compte soigneusement toutes les implications de l'autorisation d'accès complet à une base de données pour un autre utilisateur.

---

## Suppression d'alias

Utilisez sp_dropalias pour supprimer la correspondance entre un *suid* d'alias et un ID utilisateur. Ceci supprime la ligne correspondante de sysalternates. Respectez la syntaxe suivante :

sp_dropalias *nom_login*

où *nom_login* est le nom de l'utilisateur spécifié par *nom_login* au moment de la correspondance effectuée avec sp_addalias. Après suppression de l'alias de l'utilisateur, celui-ci n'a plus accès à la base de données.

Vous ne pouvez pas supprimer un alias pour un utilisateur propriétaire d'objets de la base de données créés avec la version 12.0 ou ultérieure. Vous devez supprimer les objets (en les recréant sous un login différent, si nécessaire) pour supprimer l'alias.

## Obtention d'informations relatives aux alias

Pour afficher des informations sur les alias, utilisez sp_helpuser. Par exemple, pour trouver les alias de "dbo", exécutez :

```
                        sp_helpuser dbo
Users_name      ID_in_db    Group_name   Login_name
----------      --------    ----------   ----------
dbo             1           public       sa

(1 row affected)
                        Users aliased to user.
                        Login_name
                        ----------------------
                        andy
                        christa
                        howard
                        linda

                        (4 rows affected)
```

# Obtention d'informations relatives aux utilisateurs

Le tableau 10-9 donne la liste des procédures utilisables pour obtenir des informations sur les utilisateurs, les groupes et les utilisations d'Adaptive Server en cours.

***Tableau 10-9 : Obtention d'informations sur les utilisateurs et les groupes Adaptive Server***

| Tâche | Procédure |
|---|---|
| Donne les utilisateurs et processus en cours sur Adaptive Server | sp_who |
| Affiche des informations sur les comptes de connexion | sp_displaylogin |
| Donne les utilisateurs et les alias d'une base de données | sp_helpuser |
| Donne les groupes d'une base de données | sp_helpgroup |

## Obtention d'états sur les utilisateurs et les processus

Utilisez sp_who pour obtenir des informations sur les utilisateurs et processus en cours sur Adaptive Server:

```
sp_who [nom_login | "spid"]
```

où :

- *nom_login* est le nom de login Adaptive Server de l'utilisateur. Si vous donnez un nom de login, sp_who donne des informations sur les processus exécutés par cet utilisateur.
- *spid* est le numéro d'un processus spécifique.

Pour chaque processus en cours d'exécution, sp_who donne l'ID de processus du serveur, son état, le nom de login de l'utilisateur du processus, le nom de l'ordinateur hôte, l'ID de processus du serveur d'un processus qui bloque celui-ci (le cas échéant), le nom de la base de données et la commande en cours d'exécution.

Si vous ne donnez pas de nom de login ou de *spid*, sp_who donne des informations sur les processus en cours d'exécution par tous les utilisateurs.

L'exemple ci-dessous présente le résultat de l'exécution de sp_who sans paramètre :

```
spid   status   loginame hostname blk dbname cmd
------ -------- -------- -------- --- ------ ----------------
     1 running  sa       sunbird  0   pubs2  SELECT
     2 sleeping NULL              0   master NETWORK HANDLER
     3 sleeping NULL              0   master MIRROR HANDLER
     4 sleeping NULL              0   master AUDIT PROCESS
     5 sleeping NULL              0   master CHECKPOINT SLEEP

(5 rows affected, return status = 0)
```

sp_who affiche la valeur NULL pour le *nom_login* de tous les processus système.

## Obtention d'informations sur les comptes de connexion

Utilisez sp_displaylogin pour afficher des informations sur un compte de connexion spécifié, y compris les rôles octroyés à ce compte :

sp_displaylogin [*nom_login*]

où *nom_login* est le compte de connexion utilisateur sur lequel vous souhaitez obtenir des informations. Si vous n'êtes pas responsable de la sécurité du système ou administrateur système, vous ne pouvez obtenir des informations que sur votre compte. Si vous êtes responsable de la sécurité du système ou administrateur système, vous pouvez utiliser le paramètre *nom_login* pour accéder aux informations de n'importe quel compte.

sp_displaylogin affiche votre ID utilisateur sur le serveur, votre nom de login, votre nom complet, les rôles qui vous ont été octroyés, la date de dernier changement de mot de passe, la base de données par défaut, la langue par défaut et l'état de verrouillage de votre compte.

sp_displaylogin affiche tous les rôles qui vous ont été octroyés ; même si vous avez désactivé un rôle par la commande set, ce rôle est affiché.

## Obtention d'informations relatives aux utilisateurs de base de données

Utilisez sp_helpuser pour afficher des informations sur les utilisateurs autorisés de la base de données en cours.

sp_helpuser [*nom_dans_base*]

où *nom_dans_base* désigne l'utilisateur de la base de données courante. Si vous donnez un nom d'utilisateur, sp_helpuser donne des informations sur cet utilisateur. Si vous ne donnez pas de nom, elle donne des informations sur tous les utilisateurs.

L'exemple ci-dessous présente les résultats de l'exécution de sp_helpuser sans paramètre dans la base de données pubs2 :

```
sp_helpuser
Users_name  ID_in_db  Group_name Login_name
----------  --------  ---------- ----------
dbo         1         public     sa
marcy       4         public     marcy
sandy       3         public     sandy
judy        5         public     judy
linda       6         public     linda
anne        2         public     anne
jim         7         senioreng  jim
```

## Recherche de noms et ID d'utilisateurs

Pour trouver l'ID utilisateur de serveur ou le nom de login d'un utilisateur, utilisez suser_id et suser_name.

***Tableau 10-10 : Fonctions système suser_id et suser_name***

| Pour trouver | Utiliser | Avec l'argument |
|---|---|---|
| ID d'utilisateur du serveur | suser_id | (["nom_utilisateur_serveur"]) |
| Nom d'utilisateur de serveur (nom de login) | suser_name | ([ID_utilisateur_serveur]) |

Les arguments de ces fonctions système sont facultatifs. Si vous n'en fournissez pas, Adaptive Server affiche les informations sur l'utilisateur en cours.

Cet exemple montre comment trouver l'ID utilisateur de "sandy" :

```
select suser_id("sandy")
------
     3
```

Cet exemple montre comment un administrateur système dont le nom de login est "mary" émet les commandes sans arguments :

```
select suser_name(), suser_id()
------------------------------ ------
mary                                4
```

Pour trouver le numéro ID ou le nom d'un utilisateur dans une base de données, utilisez user_id et user_name.

***Tableau 10-11 : Fonction système user_id et user_name***

| Pour trouver | Utiliser | Avec l'argument |
|---|---|---|
| ID utilisateur | user_id | (["nom_utilisateur_ basededonnées"]) |
| Nom d'utilisateur | user_name | ([ID_utilisateur_basededonnées]) |

Les arguments de ces fonctions sont facultatifs. Si vous n'en fournissez pas, Adaptive Server affiche les informations sur l'utilisateur en cours. Exemple :

```
select user_name(10)
select user_name( )
select user_id("joe")
```

## Affichage d'informations sur les rôles

Le tableau 10-12 donne la liste des procédures système et fonctions à utiliser pour trouver des informations sur les rôles et la section de ce chapitre qui fournit les détails correspondants.

***Tableau 10-12 : Recherche d'informations sur les rôles***

| Pour afficher des informations sur | Utiliser | Voir |
|---|---|---|
| L'ID d'un nom de rôle | fonction système role_id | "Recherche de noms et d'ID de rôles", page 409 |
| Le nom d'un ID de rôle | fonction système role_name | "Recherche de noms et d'ID de rôles", page 409 |
| Les rôles système | fonction système show_role | "Affichage des rôles actifs", page 410 |
| Les hiérarchies de rôles et les rôles octroyés à un ou plusieurs utilisateurs | procédure système sp_displayroles | "Affichage d'une hiérarchie de rôles", page 410 |
| L'état d'inclusion d'autres rôles dans une hiérarchie de rôles | fonction système role_contain | "Affichage des rôles d'utilisateur dans une hiérarchie", page 410 |
| L'état d'exclusion mutuelle de deux rôles | fonction système mut_excl_roles | "Détermination de l'exclusivité mutuelle", page 411 |
| Les rôles actifs pour la session en cours | procédure système sp_activeroles | "Détermination de l'activation des rôles", page 411 |
| L'activation du rôle correct pour exécuter une procédure | fonction système proc_role | "Recherche de rôles dans des procédures stockées", page 411 |
| Les connexions, y compris les rôles qui ont été octroyés | procédure système sp_displaylogin | "Obtention d'informations sur les comptes de connexion", page 406 |
| Les autorisations d'un utilisateur, d'un groupe ou d'un rôle | procédure système sp_helprotect | "Rapport sur les autorisations", page 460 |

## Recherche de noms et d'ID de rôles

Pour trouver l'ID du rôle dont vous connaissez le nom, utilisez role_id :

```
role_id(nom_rôle)
```

Tous les utilisateurs peuvent exécuter role_id. Si le rôle est valide, role_id renvoie l'ID à l'échelle du serveur du rôle (srid). La table système syssrvroles contient une colonne srid avec l'ID du rôle et une colonne name avec le nom du rôle. Si le rôle n'est pas valide, role_id renvoie NULL.

Pour trouver un nom de rôle dont vous connaissez l'ID, utilisez role_name :

```
role_name(id_rôle)
```

Tous les utilisateurs peuvent exécuter role_name.

## Affichage des rôles actifs

Utilisez show_role pour afficher les *rôles système* actifs actuellement pour le login spécifié :

```
show_role()
```

Si vous n'avez activé aucun rôle système, show_role renvoie NULL. Si vous êtes propriétaire de base de données et si vous exécutez show_role après utilisation de setuser pour incarner un autre utilisateur, show_role renvoie vos rôles système actifs et non ceux en lesquels vous êtes incarné.

Tous les utilisateurs peuvent exécuter show_role.

---

**Remarque** La fonction show_role ne donne pas d'informations sur les rôles définis par l'utilisateur.

---

## Affichage d'une hiérarchie de rôles

Vous pouvez consulter tous les rôles octroyés à votre nom de login ou voir la totalité de l'arbre hiérarchique des rôles affiché sous format tabulaire avec sp_displayroles :

```
sp_displayroles {nom_login | nom_rôle [, expand_up |
expand_down]}
```

Tout utilisateur peut exécuter sp_displayroles et afficher ses propres rôles. Seul le responsable de la sécurité du système ou l'administrateur système peut consulter les informations sur les rôles octroyés à d'autres utilisateurs.

## Affichage des rôles d'utilisateur dans une hiérarchie

Utilisez role_contain pour savoir si un rôle spécifié contient un autre rôle spécifié :

```
role_contain ("rôle1", "rôle2")
```

Si *rôle1* contient *rôle2*, role_contain renvoie 1.

Tous les utilisateurs peuvent exécuter role_contain.

### Détermination de l'exclusivité mutuelle

Utilisez la fonction mut_excl_roles pour savoir si deux rôles sont mutuellement exclusifs et connaître le niveau de cette exclusivité :

```
mut_excl(rôle1, rôle2, {membership | activation})
```

Tous les utilisateurs peuvent exécuter mut_excl_roles. Si les rôles spécifiés ou tout rôle contenu par l'un ou l'autre, sont mutuellement exclusifs, mut_excl_roles renvoie 1 ; si les rôles ne sont pas mutuellement exclusifs, mut_excl_roles renvoie 0.

### Détermination de l'activation des rôles

Pour trouver tous les rôles actifs pour la session de login en cours d'Adaptive Server, utilisez sp_activeroles :

```
sp_activeroles [expand_down]
```

expand_down affiche la hiérarchie de tous les rôles contenus dans les rôles qui vous sont octroyés.

Tout utilisateur peut exécuter sp_activeroles.

### Recherche de rôles dans des procédures stockées

Utilisez proc_role dans une procédure stockée pour garantir l'exécution de la procédure par les seuls utilisateurs ayant le rôle spécifié. Seul proc_role fournit une méthode sûre pour empêcher l'accès intempestif à une procédure stockée particulière.

Vous pouvez utiliser grant execute pour octroyer l'autorisation d'exécution sur une procédure stockée à tous les utilisateurs ayant un rôle spécifié. De même, revoke execute supprime cette autorisation.

Toutefois, l'autorisation grant execute n'empêche pas les utilisateurs non dotés du rôle spécifié de se voir attribuer l'autorisation d'exécution sur une procédure stockée. Pour assurer par exemple que tous les utilisateurs qui ne sont pas administrateur système ne reçoivent jamais l'autorisation d'exécuter une procédure stockée, utilisez proc_role dans la procédure stockée elle-même. Cette fonction vérifie si l'utilisateur appelant dispose du rôle approprié pour exécuter la procédure.

proc_role prend comme argument une chaîne pour le rôle nécessaire et renvoie 1 si l'appelant le possède. Sinon, elle renvoie 0.

Voici par exemple une procédure utilisant proc_role pour savoir si l'utilisateur a le rôle sa_role :

```
create proc test_proc
as
if (proc_role("sa_role") = 0)
begin
    print "You don't have the right role"
    return -1
end
else
    print "You have System Administrator role"
    return 0
```

# Contrôle de l'utilisation des licences

Le contrôleur d'utilisation des licences permet à un administrateur système de contrôler le nombre de licences utilisateur d'Adaptive Server pour gérer en toute sécurité les données du contrat de licence. Vous pouvez par exemple vérifier que le nombre de licences utilisées sur votre Adaptive Server ne dépasse pas le nombre spécifié dans votre contrat de licence.

Le contrôleur d'utilisation de licences suit le nombre de licences émises ; il n'applique par les restrictions du contrat de licence. Si le contrôleur d'utilisation de licences signale que vous utilisez plus de licences utilisateur que ce qui est spécifié dans votre contrat de licence, prenez contact avec votre interlocuteur commercial Sybase.

Vous devez avoir des privilèges d'administrateur système pour configurer le contrôleur d'utilisation de licences.

Par défaut, le contrôleur d'utilisation de licences est désactivé lors de la première installation ou mise à niveau d'Adaptive Server. L'administrateur système doit configurer le contrôleur d'utilisation de licences pour contrôler effectivement l'utilisation de ces licences. Pour plus d'informations sur la configuration, reportez-vous à la section "Configuration du gestionnaire de licences pour contrôler les licences utilisateur", page 413.

## Comptage des licences

Une licence est l'association d'un nom d'ordinateur et d'un nom d'utilisateur. Si un utilisateur se connecte plusieurs fois à Adaptive Server depuis la même machine, il ne compte que pour une licence. Mais si l'utilisateur se connecte une fois depuis l'ordinateur A et une fois depuis l'ordinateur B, il compte pour deux licences. Si plusieurs utilisateurs se connectent à Adaptive Server depuis le même ordinateur, sous des noms différents, chaque combinaison de nom d'utilisateur et de nom d'hôte est comptée comme une licence.

## Configuration du gestionnaire de licences pour contrôler les licences utilisateur

Utilisez sp_configure pour spécifier le nombre de licences de votre contrat :

```
sp_configure "license information" , nombre
```

où *nombre* est le nombre de licences. Exemple :

```
sp_configure "license information", 300
```

définit un nombre maximal de 300 licences utilisateur et signale une utilisation excédentaire dès le numéro de licence 301. Si vous augmentez le nombre de licences utilisateur, vous devez aussi changer le paramètre de configuration license number.

Le paramètre de configuration housekeeper free write percent doit être à 1 ou plus pour que le gestionnaire de licences puisse contrôler l'utilisation des licences.

## Contrôle de l'utilisation des licences avec la tâche housekeeper

Après configuration du contrôleur d'utilisation des licences, la tâche housekeeper détermine le nombre de licences utilisateur en cours, en fonction de l'ID utilisateur et du nom d'ordinateur de chaque utilisateur connecté à Adaptive Server. Quand la tâche housekeeper contrôle les licences, le contrôleur d'utilisation des licences met à jour une variable qui suit le nombre maximal de licences utilisateur en cours :

- Si le nombre de licences en cours est identique ou a diminué depuis l'exécution précédente de housekeeper, le contrôleur d'utilisation des licences ne fait rien.

- Si le nombre de licences en cours a augmenté depuis la dernière exécution de housekeeper, le contrôleur d'utilisation des licences définit ce nombre comme le nombre maximal de licences en cours.
- Si le nombre de licences en cours est supérieur au nombre autorisé par le contrat de licence, le contrôleur d'utilisation des licences émet un message dans le journal d'erreurs :

```
Exceeded license usage limit. Contact Sybase
Sales for additional licenses.
```

La tâche housekeeper s'exécute pendant les cycles d'inactivité d'Adaptive Server. La tâche housekeeper contrôle le nombre de licences utilisateur seulement si le paramètre de configuration housekeeper free write percent a une valeur au moins égale à 1.

Pour plus d'informations sur la tâche housekeeper, reportez-vous à la section "housekeeper free write percent", page 205 et au chapitre 3, "Utilisation des moteurs et des CPU", dans le document *Performances et optimisation*.

## Journalisation du nombre de licences utilisateur

La table système *syblicenseslog* est créée dans la base de données master lors de l'installation ou de la mise à niveau d'Adaptive Server. Le contrôleur d'utilisation de licences met à jour les colonnes de syblicenseslog à la fin de chaque période de 24 heures, comme indiqué dans le tableau 10-13.

***Tableau 10-13 : Colonnes de la table syblicenseslog***

| Colonne | Description |
|---|---|
| état | –1 – Housekeeper ne peut pas contrôler les licences.<br>0 – Nombre de licences non dépassé.<br>1 – Nombre de licences dépassé. |
| logtime | Date et heure d'insertion des informations de journalisation. |
| maxlicenses | Nombre maximum de licences utilisées dans les précédentes 24 heures. |

syblicenseslog se présente comme suit :

```
status logdate                    maxlicenses
 ------ -------------------------- -----------
      0         Jul 17 1998 11:43AM         123
      0         Jul 18 1998 11:47AM         147
      1         Jul 19 1998 11:51AM         154
      0         Jul 20 1998 11:55AM         142
      0         Jul 21 1998 11:58AM         138
      0         Jul 21 1998  3:14PM         133
```

Dans cet exemple, le nombre de licences utilisateur a dépassé la limite le 19 juillet 1998.

Si Adaptive Server est arrêté, le gestionnaire de licences met à jour syblicenseslog avec le nombre maximal de licences utilisées actuellement. Adaptive Server démarre une nouvelle période de contrôle de 24 heures au redémarrage.

La deuxième ligne pour le 21 juillet 1998 a été causée par un arrêt et un redémarrage du serveur.

# Obtention d'informations sur l'utilisation : taux de charge du processeur

Quand un utilisateur se connecte à Adaptive Server, le serveur commence à cumuler les utilisations de temps CPU et d'entrées/sorties pour cet utilisateur. Adaptive Server peut donner l'utilisation totale pour un utilisateur individuel ou pour tous les utilisateurs. Les informations pour chaque utilisateur sont conservées dans la table système syslogins de la base de données master.

## État des statistiques d'utilisation en cours

L'administrateur système peut utiliser sp_reportstats ou sp_clearstats pour obtenir ou effacer les données d'utilisation totale en cours pour des utilisateurs individuels ou pour tous les utilisateurs d'Adaptive Server.

### Affichage des totaux de comptabilisation en cours

sp_reportstats affiche les totaux de comptabilisation en cours pour les utilisateurs d'Adaptive Server. Elle donne l'utilisation CPU totale et l'utilisation d'entrées/sorties totale, ainsi que le pourcentage utilisé de ces ressources. Elle n'enregistre pas les statistiques pour le login "sa" (processus dont le *suid* est égal à 1), les gestionnaires de points d'arrêt, de réseau et de miroirs.

### Démarrage d'un nouvel intervalle de comptabilisation

Adaptive Server cumule les statistiques d'utilisation CPU et d'entrées/sorties jusqu'à l'effacement des totaux de syslogins par l'exécution de sp_clearstats. sp_clearstats démarre un nouvel intervalle de comptabilisation pour les utilisateurs d'Adaptive Server et exécute sp_reportstats pour imprimer des statistiques pour la période précédente.

Choisissez la longueur de votre intervalle de comptabilisation en décidant quand vous souhaitez utiliser les statistiques sur votre site. Par exemple, pour une facturation mensuelle entre services du pourcentage d'utilisation CPU et d'entrées/sorties d'Adaptive Server, l'administrateur système peut exécuter sp_clearstats une fois par mois.

Pour des informations détaillées sur ces procédures stockées, reportez-vous au *Manuel de référence d'Adaptive Server*.

## Spécification de l'intervalle pour l'ajout des statistiques de comptabilisation

Un administrateur système peut utiliser des paramètres de configuration pour définir la fréquence d'ajout des statistiques de comptabilisation à syslogins.

Pour spécifier le nombre de tics d'horloge machine cumulés avant l'ajout des statistiques de comptabilisation à syslogins, utilisez le paramètre de configuration cpu accounting flush interval. La valeur par défaut est 200. Par exemple :

```
sp_configure "cpu accounting flush interval", 600
```

Pour savoir à combien de microsecondes correspond un tic d'horloge sur votre système, utilisez la requête suivante dans Adaptive Server :

```
select @@timeticks
```

Pour spécifier le nombre d'opérations de lecture ou d'écriture d'entrées/sorties cumulées avant l'ajout d'informations (vidage) vers syslogins, utilisez le paramètre de configuration i/o accounting flush interval. La valeur par défaut est 1000. Par exemple :

```
sp_configure "cpu accounting flush interval", 2000
```

Les statistiques d'entrées/sorties et d'utilisation CPU sont vidées quand un utilisateur cumule plus d'utilisation d'entrées/sorties ou de temps CPU que la valeur spécifiée. Les informations sont aussi vidées quand l'utilisation quitte une session Adaptive Server.

La valeur minimale autorisée pour les deux paramètres de configuration est 1. La valeur maximale est 2 147 483 647.

CHAPITRE 11

# Gestion des autorisations utilisateur

Ce chapitre décrit l'utilisation et la mise en œuvre des autorisations utilisateur.

Les sujets traités dans ce chapitre sont les suivants :



## Présentation

Les **contrôles d'accès discrétionnaires** (DAC) permettent de restreindre l'accès à des objets et à des commandes en fonction de l'identité de l'utilisateur ou de son appartenance à un groupe. Ces contrôles sont dits "discrétionnaires" car un utilisateur disposant d'une certaine autorisation d'accès, tel qu'un propriétaire d'objet, peut choisir de la transmettre à d'autres personnes.

Les administrateurs système opèrent en dehors du système DAC et ont, à tout moment, des droits d'accès sur tous les objets des bases de données. Le responsable de la sécurité du système a toujours accès aux tables de trace d'audit contenues dans la base sybsecurity.

Les propriétaires de base de données ne disposent pas automatiquement de droits sur les objets détenus par les utilisateurs de leur base.

- Acquérir temporairement toutes les autorisations d'un utilisateur de la base en prenant son identité à l'aide de la commande setuser.
- Acquérir de façon permanente les autorisations sur un objet spécifique en utilisant la commande setuser pour prendre l'identité du propriétaire de l'objet, puis en exécutant des commandes grant pour octroyer des autorisations.

Pour des détails sur la prise d'identité d'un utilisateur afin d'obtenir ses autorisations sur une base de données ou sur un objet, reportez-vous à "Obtention des autorisations d'un autre utilisateur", page 455.

Les propriétaires d'objets peuvent octroyer l'accès à leurs objets à d'autres utilisateurs. Ils peuvent également autoriser d'autres utilisateurs à transmettre ces droits d'accès à des tiers. Vous pouvez attribuer diverses autorisations à des utilisateurs, des groupes et des rôles avec la commande grant, puis les révoquer avec la commande revoke. Utilisez-les pour définir des droits de création de bases de données, de création d'objets dans une base, d'exécution de certaines commandes (comme set proxy) et d'accès à des tables, des vues et des colonnes spécifiques. Pour que les autorisations prennent par défaut la valeur "public", aucune instruction grant ou revoke n'est nécessaire.

Certaines commandes sont utilisables à tout moment par les utilisateurs, sans autorisation. D'autres ne sont utilisables que par des utilisateurs ayant un statut particulier, et ne sont pas transférables.

La possibilité de définir des autorisations pour les commandes susceptibles d'être octroyées et révoquées est déterminée, d'une part, par le rôle ou le statut de chaque utilisateur (administrateur système, propriétaire de bases de données ou propriétaire d'objets de base de données) et, d'autre part, par le fait que ce rôle comporte des droits d'octroyer des autorisations à d'autres utilisateurs.

Vous pouvez également utiliser les vues et les procédures stockées en tant que mécanismes de sécurité. Pour plus d'informations, reportez-vous à la section "Utilisation de vues et de procédures stockées comme mécanismes de sécurité", page 465.

# Types d'utilisateurs et privilèges associés

Le système de contrôle d'accès discrétionnaire d'Adaptive Server reconnaît les types d'utilisateurs suivants :

- administrateur système (SA),
- responsable de la sécurité du système (SSO),
- opérateur (OPER),
- propriétaire de base de données,
- propriétaire d'objets de base de données,
- autres utilisateurs (groupe "public").

## Privilèges des administrateurs système

Les administrateurs système :

- effectuent des tâches non liées aux applications,
- opèrent en dehors du système DAC (Discretionary Access Control) d'Adaptive Server.

Le rôle d'administrateur système est, en général, octroyé à des logins Adaptive Server spécifiques. Toutes les actions effectuées par cet utilisateur permettent de remonter à son ID utilisateur sur le serveur. Si les tâches d'administration de serveur, sur votre site, sont traitées par une seule personne, vous pouvez utiliser le compte "sa" défini à cet effet lors de l'installation d'Adaptive Server à l'installation. Ce compte a le droit d'assurer les rôles d'administrateur système, de responsable de la sécurité du système et d'opérateur. Tout utilisateur connaissant le mot de passe "sa" peut se connecter à ce compte et adopter toute une partie des rôles supportés.

Le fait qu'un SA opère en dehors du système de protection constitue une mesure de sécurité. Par exemple, si le propriétaire d'une base de données supprime par erreur toutes les entrées de la table sysusers, le SA peut restaurer cette table (à condition, bien entendu, que des sauvegardes aient été effectuées). Plusieurs commandes ne peuvent être exécutées que par un administrateur système. Il s'agit de disk init, disk refit, disk reinit, shutdown, kill et des commandes de mise en miroir des disques.

Lors de l'octroi d'autorisations, le SA est considéré comme le propriétaire de l'objet traité. Si les autorisations qu'il octroie s'appliquent à un objet appartenant à un autre utilisateur, le nom de l'utilisateur apparaît dans sysprotects et dans le résultat de sp_helprotect comme étant l'utilisateur ayant octroyé ces autorisations.

Les SA sont chargés de la suppression des logins et peuvent les verrouiller et les déverrouiller. Les SSO partagent la gestion des logins avec les administrateurs système. Les SSO sont chargés d'ajouter des logins et peuvent aussi les verrouiller et les déverrouiller.

### Droits de création de bases de données

Seul un administrateur système peut octroyer l'autorisation d'utiliser la commande create database. L'utilisateur qui reçoit l'autorisation create database doit être enregistré dans la base master, car toutes les bases de données sont créées à partir de master.

Dans de nombreuses installations, le SA garde le monopole sur l'autorisation create database afin de centraliser le contrôle du placement des bases de données et de l'allocation d'espace sur les devices. Dans ce cas, le SA crée les nouvelles bases pour le compte des autres utilisateurs, puis transfère à ces derniers les droits de propriété.

Pour créer une base de données destinée à un autre utilisateur :

1 Exécutez la commande create database dans la base master.

2 Activez la nouvelle base à l'aide de la commande use.

3 Exécutez la procédure système sp_changedbowner.

## Privilèges des responsables de la sécurité du système

Les responsables de la sécurité du système (SSO) effectuent des tâches liées à la sécurité dans Adaptive Server, notamment :

- l'octroi des rôles de responsable de la sécurité du système et d'opérateur ;
- l'administration du système d'audit ;
- le changement des mots de passe ;
- l'ajout de nouveaux logins ;
- le verrouillage et le déverrouillage des comptes ;

- la création et l'octroi de rôles définis par l'utilisateur ;
- l'administration de la sécurité réseau ;
- l'octroi de l'autorisation d'utiliser la commande set proxy ou set session authorization.

Le SSO peut *accéder* à toutes les bases de données mais, en général, ne détient aucune autorisation spéciale sur les objets qu'elles contiennent. La base sybsecurity constitue une exception, car seul un responsable de la sécurité du système a le droit d'accéder à sa table sysaudits. Il existe également plusieurs procédures système qui ne peuvent être exécutées que par un SSO.

Les responsables de la sécurité du système sont en mesure de réparer les éventuels dommages causés par mégarde au système de protection par un utilisateur. Par exemple, si le propriétaire d'une base de données oublie son mot de passe, un SSO peut changer celui-ci pour permettre au propriétaire de se connecter.

Les SSO ont également la possibilité de créer des rôles personnalisés et de les octroyer à des utilisateurs, à des groupes ou à d'autres rôles. Pour plus d'informations sur la création et l'octroi de rôles définis par l'utilisateur, reportez-vous au chapitre , "Création et attribution de rôles aux utilisateurs".

## Privilèges des opérateurs

Les utilisateurs détenant le rôle d'opérateur peuvent sauvegarder et restaurer toutes les bases de données d'un serveur, même s'ils n'en sont pas propriétaires. Ce rôle permet d'utiliser les commandes suivantes sur une base quelconque :

```
dump database
dump transaction
load database
load transaction
```

## Privilèges des propriétaires de bases de données

Les propriétaires de bases de données (DBO) et les administrateurs système (SA) sont les seuls utilisateurs pouvant octroyer des droits de création d'objets à d'autres personnes. Le DBO a les pleins pouvoirs dans sa propre base de données, et doit octroyer explicitement des autorisations aux autres utilisateurs à l'aide de la commande grant.

Le droit d'utiliser les commandes suivantes est automatiquement donné au DBO et n'est pas transférable aux autres utilisateurs :

checkpoint
dbcc
drop database
dump database
dump transaction
grant (droits de création d'objets)
load database
load transaction
revoke (droits de création d'objets)
setuser

Les DBO peuvent octroyer à d'autres personnes le droit d'utiliser les commandes suivantes :

create default
create procedure
create rule
create table
create view
grant (autorisations sur les tables système)
grant (autorisations d'utiliser select, insert, delete, update, references et execute dans les objets de base de données)
revoke (autorisations sur les tables système)
revoke (autorisations d'utiliser select, insert, delete, update, references et execute dans les objets de base de données)

## Autorisations sur les tables système

Le droit d'utiliser les tables système peut être contrôlé par le propriétaire de la base de données, de la même façon que les autorisations sur les autres tables. Par défaut, lorsqu'Adaptive Server est installé, le script installmodel octroie le droit d'accès select au groupe "public" (tous les utilisateurs) pour la plupart des tables système et des champs de ces tables. Cependant, l'accès à certaines tables système, telles que systhresholds et à certains champs est interdit. Par exemple, tous les utilisateurs peuvent, par défaut, sélectionner toutes les colonnes de sysobjects, à l'exception d'audflags.

Pour connaître les autorisations définies pour une table système particulière, exécutez :

sp_helprotect *nom_table_système*

Par exemple, pour vérifier les autorisations de systhresholds dans your_database, exécutez :

```
use your_database
go
sp_helprotect systhresholds
go
```

Par défaut, aucun utilisateur (y compris un DBO) ne peut modifier directement les tables système. Au lieu de cela, les procédures système disponibles dans Adaptive Server modifient les tables système, ce qui permet de garantir l'intégrité.

---

**Avertissement !** Bien que cela soit possible, il est vivement déconseillé de modifier les tables système.

---

## Autorisations des procédures système

Les autorisations sur les procédures système sont définies dans la base sybsystemprocs, où ces dernières sont stockées.

Les procédures liées à la sécurité ne peuvent être exécutées que par les responsables de la sécurité du système.Tandis que d'autres ne sont utilisables que par les administrateurs système.

Certaines procédures système sont réservées aux DBO. Elles vérifient que la personne qui les exécute est bien le propriétaire de la base de données à partir de laquelle elles sont lancées.

Enfin, il existe des procédures exécutables par tout utilisateur détenant l'autorisation appropriée. Le droit d'exécuter une même procédure système est valable pour toutes les bases de données.

Les personnes non répertoriées dans sybsystemprocs..sysusers sont considérées comme des utilisateurs "guest" dans sybsystemprocs, et se voient attribuer automatiquement des droits sur de nombreuses procédures système. Pour interdire à un utilisateur d'exécuter une procédure, l'administrateur système doit ajouter celui-ci dans sybsystemprocs..sysusers et utiliser une instruction revoke s'appliquant à cette procédure. Le propriétaire d'une base de données utilisateur ne peut pas contrôler directement les droits sur les procédures système à partir de sa propre base.

## Changement d'appartenance de la base de données

Pour changer l'appartenance d'une base de données, utilisez la procédure système sp_changedbowner. En général, les administrateurs système créent les bases utilisateur, puis en attribuent le droit de propriété à l'utilisateur adéquat une fois le travail de préparation terminé. Seul un SA peut exécuter sp_changedbowner.

Il est conseillé de transférer le droit de propriété avant que l'utilisateur soit ajouté dans la base ou qu'il ait commencé à y créer des objets. Le nouveau propriétaire doit déjà disposer d'un nom de login dans Adaptive Server, mais ne doit pas avoir un nom d'utilisateur ou un alias dans la base de données. Vous devrez peut-être utiliser sp_dropuser ou sp_dropalias avant de changer l'appartenance d'une base, ou supprimer des objets pour pouvoir effacer le nom d'utilisateur.

Exécutez sp_changedbowner dans la base de données dont l'appartenance doit être changée. La syntaxe est la suivante :

```
sp_changedbowner nom_login [, true ]
```

L'exemple suivant rend l'utilisateur "albert" propriétaire de la base de données courante et supprime les alias des éventuels DBO antérieurs :

```
sp_changedbowner albert
```

Pour transférer les alias et leurs autorisations vers le nouveau DBO, spécifiez le paramètre true.

---

**Remarque** Il n'est pas possible de changer l'appartenance de la base master et il est déconseillé de modifier celle de toute autre base système.

---

## Privilèges des propriétaires des objets de bases de données

Tout utilisateur qui crée un objet de base de données (table, vue ou procédure stockée) en est le propriétaire et dispose automatiquement de tous les droits d'accès sur cet objet. Les autres personnes, y compris le DBO, n'ont aucune autorisation sur l'objet, sauf si des droits leur ont été explicitement octroyés par le propriétaire ou par un utilisateur détenant l'autorisation grant sur cet objet.

Supposons, par exemple, que Mary soit le propriétaire de la base pubs2 et qu'elle ait autorisé Joe à y créer des tables. Joe ayant créé la table new_authors, cet objet lui appartient.

Par défaut, les droits d'accès sur new_authors sont attribués uniquement à Joe. Celui-ci peut octroyer des autorisations à d'autres utilisateurs ou les révoquer.

Le propriétaire d'une table dispose automatiquement des droits de création suivants, non transférables à d'autres personnes :

alter table
drop table
create index
truncate table
update statistics

Il est possible de transférer l'autorisation d'utiliser les commandes grant et revoke pour octroyer des droits select, insert, update, delete, references et execute à certains utilisateurs sur des objets spécifiques. Pour ce faire, exécutez la commande grant with grant option.

L'autorisation de supprimer un objet (table, vue, index, procédure stockée, règle ou valeur par défaut) à l'aide de drop est attribuée par défaut au propriétaire de l'objet et n'est pas transférable.

## Privilèges des autres utilisateurs de base de données

Tout en bas de la hiérarchie se trouvent les autres utilisateurs de base de données. Leurs autorisations sont définies par les propriétaires d'objets, les DBO, les personnes ayant le droit d'octroyer des autorisations ou les SA. Ces utilisateurs sont désignés par leur nom, par celui de leur groupe ou par le mot-clé public.

# Octroi et révocation d'autorisations sur les objets de base de données

Il existe deux types d'autorisations relatives aux objets :

- **Droits d'accès aux objets** permettant d'utiliser les commandes qui accèdent à des objets de base de données. Pour plus d'informations, reportez-vous à la section "Octroi et révocation de droits d'accès aux objets", page 428.
- **Droits de création d'objets** permettant de créer des objets. Ils ne peuvent être octroyés que par un administrateur système ou un propriétaire de base de données. Pour plus d'informations, reportez-vous à la section "Octroi et révocation de droits de création d'objets", page 434.

Ces deux types d'autorisation sont contrôlés à l'aide des commandes grant et revoke.

Chaque base de données est dotée de son propre système de protection indépendant. Le droit d'exécuter une certaine commande dans une base ne permet pas de l'employer dans d'autres bases.

## Octroi et révocation de droits d'accès aux objets

Les autorisations d'accès aux objets contrôlent l'application de certaines commandes à des objets de base de données. Par exemple, vous devez disposer de l'autorisation explicite d'utiliser la commande select sur la table authors. Ces droits sont octroyés et révoqués par le propriétaire des objets (et les SA), et sont transférables à d'autres utilisateurs.

Le tableau 11-1 répertorie les types de droit d'accès avec les objets auxquels ils s'appliquent :

***Tableau 11-1 : Autorisations applicables aux différents types d'objet***

| Autorisation | Objet |
|---|---|
| select | Table, vue, colonne |
| update | Table, vue, colonne |
| insert | Table, vue |
| delete | Table, vue |
| references | Table, colonne |
| execute | Procédure stockée |

Le droit references se rapporte aux contraintes d'intégrité référentielle pouvant être spécifiées dans une commande alter table ou create table. Les autres autorisations s'appliquent à des commandes SQL. Les autorisations d'accès aux objets prennent par défaut les valeurs des administrateurs système et du propriétaire des objets et peuvent être octroyées aux autres utilisateurs.

La commande grant permet d'octroyer des droits d'accès aux objets. La syntaxe est la suivante :

```
grant {all [privileges]| liste_autorisations}
    on { nom_table [(liste_colonnes)]
       | nom_vue[(liste_colonnes)]
       | nom_proc_stockée}
    to {public | liste_noms | nom_rôle}
    [with grant option]
```

Pour révoquer ces mêmes autorisations, employez la commande revoke. La syntaxe est la suivante :

```
revoke [grant option for]
    {all [privileges] | liste_autorisations}
    on { nom_table [(liste_colonnes)]
       |  nom_vue[(liste_colonnes)]
       | nom_proc_stockée}
    from {public | liste_noms | nom_rôle}
    [cascade]
```

Commentaires sur les mots-clés et paramètres disponibles :

- all ou all privileges permet d'octroyer ou de révoquer toutes les autorisations applicables à l'objet spécifié. Chaque propriétaire peut utiliser all, avec un nom d'objet, pour définir des droits sur ses propres objets. Si vous octroyez ou révoquez des autorisations sur une procédure stockée, all a le même effet que execute.

  **Remarque** Les droits insert et delete ne s'appliquant pas aux colonnes, vous ne pouvez pas les inclure dans une liste d'autorisations (ni indiquer le mot-clé all) si vous spécifiez une liste de colonnes.

- *liste_autorisations* correspond à la liste des autorisations octroyées. Si vous désignez plusieurs autorisations, séparez-les par des virgules. Le tableau tableau 11-2 illustre les autorisations d'accès qui peuvent être octroyées pour chaque type d'objet :

***Tableau 11-2 : Autorisations d'accès aux objets***

| Objet | permission_list peut contenir |
|---|---|
| Table ou vue | select, insert, delete, update, references.<br><br>references s'applique aux tables, mais pas aux vues ; les autres autorisations s'appliquent aux deux types d'objet. |
| Colonne | select, update, references |
| Procédure stockée | execute |

Vous pouvez spécifier des colonnes dans *liste_autorisations* ou dans *liste_colonnes*, mais pas dans les deux.

- Le mot-clé on indique l'objet pour lequel l'autorisation est octroyée ou révoquée. Vous pouvez définir des droits pour une seule table, vue ou procédure stockée à la fois. Il est possible de traiter plusieurs colonnes en même temps, à condition qu'elles appartiennent toutes à la même table ou vue. Vous ne pouvez octroyer ou révoquer des autorisations sur des objets que dans la base de données courante.
- Le mot-clé public fait référence au groupe "public", qui comprend tous les utilisateurs d'Adaptive Server. La signification de public est légèrement différente pour grant et pour revoke :
  - Pour grant, vous (le propriétaire de l'objet) êtes inclus dans public. Par conséquent, si vous avez révoqué vos propres autorisations sur votre objet et que, par la suite, vous en octroyez au groupe public, ces autorisations vous sont réattribuées.
  - Pour revoke, public exclut le propriétaire de l'objet.
- name_list comprend :
  - les noms de groupes,
  - les noms d'utilisateur,
  - une combinaison d'utilisateurs et de groupes, chaque nom étant séparé du suivant par une virgule.
- *nom_rôle* représente le nom d'un rôle Adaptive Server défini par le système ou par l'utilisateur. Vous pouvez créer et configurer une hiérarchie de rôles utilisateur, puis leur octroyer différents privilèges. Les rôles système sont sa_role (administrateur système), sso_role (responsable de la sécurité du système) et oper_role (opérateur). Il n'est pas possible de les modifier ou d'en créer.

- Dans une instruction grant, le mot-clé with grant option permet aux utilisateurs indiqués dans *liste_noms* d'octroyer à d'autres personnes les droits d'accès spécifiés. Si un utilisateur possède le droit with grant option sur un objet, il le conserve même lorsque des autorisations sont révoquées du groupe public ou d'un groupe dont cette personne fait partie.
- grant option for permet de révoquer les droits with grant option, de sorte que les utilisateurs indiqués dans *liste_noms* ne puissent plus octroyer à d'autres personnes les autorisations spécifiées. Si ces personnes ont bénéficié d'autorisations, vous devez employer l'option cascade pour les leur retirer également. Les utilisateurs indiqués dans *liste_noms* conservent le droit d'accéder à l'objet, mais ne peuvent plus le transmettre à autrui. grant option for ne s'applique pas aux droits de création d'objets.
- Dans une instruction revoke, l'option cascade retire les droits d'accès spécifiés aux utilisateurs indiqués dans *liste_noms*, ainsi qu'à toute personne à laquelle ces utilisateurs ont octroyé des droits.

Vous ne pouvez octroyer ou révoquer des autorisations sur des objets que dans la base de données courante.

Si plusieurs utilisateurs autorisent une même personne à accéder à un objet, ses droits d'accès restent actifs tant qu'ils n'ont pas été révoqués par chaque donateur ou par un administrateur système. Autrement dit, si un SA révoque ces droits, la personne ne peut plus accéder à l'objet, même si d'autres utilisateurs l'y avaient autorisée.

Seul un responsable de la sécurité du système est en mesure d'octroyer ou de révoquer l'autorisation de créer des triggers. Le propriétaire de la base de données peut créer des triggers dans toutes les tables utilisateur. Les utilisateurs ne peuvent créer des triggers que dans les tables qui leur appartiennent.

Par défaut, le droit d'émettre la commande create trigger est accordé à l'ensemble des utilisateurs.

Lorsque vous interdisez à un utilisateur de créer des triggers, une ligne revoke est ajoutée dans la table sysprotects correspondante. Pour octroyer à cet utilisateur l'autorisation d'émettre create trigger, vous devez émettre deux commandes grant : la première supprime la ligne revoke de sysprotects et la seconde insère une ligne grant. Si vous retirez ce droit à l'utilisateur, il ne peut créer aucun trigger, même sur les tables qui lui appartiennent. Cette révocation n'est valable que dans la base de données où la commande revoke a été émise.

## Identification concrète

Lors d'une session, Adaptive Server identifie les utilisateurs par leur nom de login. Cette identification s'applique à toutes les bases de données du serveur. Lorsque l'utilisateur crée un objet, le serveur associe l'ID utilisateur base de données du propriétaire (*uid*) et le nom de login du créateur à l'objet dans la table sysobjects. Ces informations identifient concrètement les objets comme appartenant à cet utilisateur, ce qui permet au serveur de reconnaître les cas où les autorisations sur cet objet peuvent être octroyées implicitement.

Si un utilisateur Adaptive Server crée une table, puis une procédure pour y accéder, tous les utilisateurs ayant reçu l'autorisation d'exécuter la procédure n'ont pas besoin d'autorisation pour accéder directement à l'objet. Par exemple, en accordant à l'utilisateur "mary" l'autorisation sur proc1, elle peut visualiser les colonnes id et descr de la table table1, alors qu'elle ne possède pas l'autorisation explicite d'utiliser select dans la table :

```
create table table1 (id     int,
                     amount money,
                     descr    varchar(100))

create procedure proc1 as select id, descr from
table1

grant execute on proc1 to mary
```

Il existe des cas, cependant, dans lesquels les autorisations implicites ne sont utiles que si les objets peuvent être identifiés concrètement. Par exemple, lorsque cela implique en même temps d'utiliser des alias et d'accéder aux objets de bases de données croisées.

Vous ne pouvez pas supprimer un alias si le login correspondant à cet alias a créé des objets ou des seuils. Avant d'utiliser sp_dropalias pour supprimer un alias qui a réalisé ces opérations, supprimez les objets ou les procédures. Si vous en avez toujours besoin après la suppression de l'alias, recréez-les avec un autre propriétaire.

## Exigences spéciales pour la conformité avec la norme SQL92

Si vous utilisez la commande set pour activer (on) l'option ansi_permissions, les instructions update et delete requièrent des autorisations supplémentaires, décrites dans le tableau 11-3.

***Tableau 11-3 : Autorisations ANSI pour update et delete***

| | **Autorisations requises :** ***set ansi_permissions off*** | **Autorisations requises :** ***set ansi_permissions on*** |
|---|---|---|
| update | Autorisation update sur les colonnes dans lesquelles des valeurs sont définies. | Autorisation update sur les colonnes dans lesquelles des valeurs sont définies.<br>et<br>Autorisation select sur toutes les colonnes apparaissant dans la clause where.<br>Autorisation select sur toutes les colonnes indiquées à droite de la clause set. |
| delete | Autorisation delete sur la table. | Autorisation delete sur la table dans laquelle des lignes sont supprimées.<br>et<br>autorisation select sur toutes les colonnes apparaissant dans la clause where. |

Si l'option ansi_permissions est activée et que vous tentez une mise à jour ou une suppression sans avoir les autorisations select supplémentaires, la transaction est annulée et un message d'erreur s'affiche. Dans ce cas, le propriétaire de l'objet doit vous attribuer des droits select sur toutes les colonnes appropriées.

## Exemples d'octroi de droits d'accès sur des objets

L'instruction suivante donne à Mary et au groupe "sales" le droit d'effectuer des insertions et des suppressions dans la table titles :

```
grant insert, delete
on titles
to mary, sales
```

L'instruction suivante donne à Harold le droit d'utiliser la procédure stockée makelist :

```
grant execute
on makelist
to harold
```

L'instruction ci-après octroie l'autorisation d'exécuter la procédure stockée sa_only_proc aux utilisateurs disposant du rôle d'administrateur système uniquement :

```
grant execute
on sa_only_proc
to sa_role
```

L'instruction suivante donne à Aubrey le droit de sélectionner, mettre à jour et supprimer des lignes de la table authors, ainsi que d'octroyer les mêmes autorisations à d'autres utilisateurs :

```
grant select, update, delete
on authors
to aubrey
with grant option
```

### Exemples d'octroi de droits d'accès sur des objets

Les deux instructions ci-après ont le même effet : elles retirent à tous les utilisateurs, à l'exception du propriétaire de l'objet, le droit de mettre à jour les colonnes price et total_sales de la table titles :

```
revoke update
on titles (price, total_sales)
from public
revoke update(price, total_sales)
on titles
from public
```

Les instructions suivantes retirent à Clare l'autorisation de mettre à jour la table authors, ainsi qu'à tous les utilisateurs auxquels elle aurait pu transmettre cette autorisation :

```
revoke update
on authors
from clare
cascade
```

L'instruction suivante ôte à tous les opérateurs le droit d'exécuter la procédure stockée new_sproc :

```
revoke execute
on new_sproc
from oper_role
```

## Octroi et révocation de droits de création d'objets

Les autorisations de création d'objets réglementent l'emploi des commandes permettant de créer des objets. Ils ne peuvent être octroyés que par un administrateur système ou un propriétaire de base de données.

Les commandes permettant de créer des objets sont les suivantes :

create database
create default
create procedure
create rule
create table
create view

La syntaxe employée pour les droits de création diffère légèrement de celle requise pour les droits d'accès. La syntaxe de grant est :

```
grant {all [privileges] | liste_commandes}
    to {public | liste_noms | nom_rôle}
```

La syntaxe de revoke est :

```
revoke {all [privileges] | liste_commandes}
    from {public | liste_noms | nom_rôle}
```

où :

- all ou all privileges ne peut être utilisé que par un administrateur système (SA) ou par le propriétaire de la base de données (DBO). Si un SA exécute grant all à partir de la base de données master, tous les droits grant all assigns all create sont octroyés, y compris le droit create database. Si un SA exécute grant all à partir d'une autre base, tous les droits create sont octroyés sauf create database. Si le DBO utilise grant all, Adaptive Server octroie tous les droits create sauf create database, puis affiche un message d'information.
- *command_list* représente l'ensemble des droits de création qui doivent être octroyés ou révoqués. Séparez les commandes par des virgules. Cette liste peut comporter les autorisations create database, create default, create procedure, create rule, create table et create view. L'autorisation create database ne peut être octroyée que par un administrateur système, et uniquement à partir de la base master.
- public représente tous les utilisateurs, excepté le propriétaire de la base de données (qui "détient" ces droits dans la base).
- liste_noms est une liste de noms d'utilisateur ou de groupe, séparés par des virgules.
- *nom_rôle* est le nom d'un rôle Adaptive Server défini par le système ou par l'utilisateur. Vous pouvez créer et configurer une hiérarchie de rôles utilisateur, puis leur octroyer différents privilèges.

### Exemples d'octroi de droits de création d'objets

La première instruction donne à Mary et à John l'autorisation d'utiliser les commandes create database et create table. En raison de la présence de create database, cette instruction ne peut être exécutée que par un administrateur système à partir de la base master. L'autorisation create table de Mary et John ne s'applique qu'à la base de données master.

```
grant create table, create database
to mary, john
```

La commande suivante donne à tous les utilisateurs le droit de créer des tables et des vues dans la base de données courante :

```
grant create table, create view
to public
```

### Exemple de révocation de droits de création d'objets

Dans l'exemple suivant, nous retirons à "mary" le droit de créer des tables et des règles :

```
revoke create table, create rule
from mary
```

## Combinaison d'instructions *grant* et *revoke*

Vous pouvez octroyer des autorisations particulières à des utilisateurs spécifiques. Cependant, si la plupart des utilisateurs doivent détenir la majorité des privilèges, il est plus facile de donner tous les droits à tout le monde, puis de révoquer certaines autorisations pour des utilisateurs spécifiques.

Par exemple, un propriétaire de base de données (DBO) peut octroyer toutes les autorisations sur la table titles à tous les utilisateurs à l'aide de l'instruction suivante :

```
grant all
on titles
to public
```

Ensuite, le DBO peut exécuter une série d'instructions revoke, comme suit :

```
revoke update
on titles (price, advance)
from public
revoke delete
on titles
from mary, sales, john
```

L'exécution des instructions grant et revoke est liée à l'ordre d'émission de ces dernières : en cas de conflit, l'instruction la plus récente prévaut sur toutes les autres.

---

**Remarque** En langage SQL, la commande grant doit être exécutée avant revoke, mais ces deux commandes ne peuvent pas être utilisées au sein d'une même transaction. Par conséquent, lorsque vous octroyez une autorisation d'accès "public" sur des objets, puis que vous révoquez ce droit pour un individu, ce dernier conserve néanmoins l'accès à cet objet pendant un certain temps. Pour éviter cela, il convient d'inclure les deux clauses grant et revoke au sein d'une même transaction, à l'aide de la commande create schema.

---

## Ordre des autorisations et hiérarchie

L'ordre d'exécution des commandes grant et revoke est déterminant. Par exemple, si le groupe de Jose dispose du droit select sur la table titles, puis que l'autorisation de Jose d'exécuter select sur la colonne advance est révoquée, ce dernier a accès à toutes les colonnes sauf à advance, tandis que les autres utilisateurs du groupe ne sont pas soumis à cette restriction.

Appliquée à un groupe ou à un rôle, la commande grant ou revoke modifie toutes les autorisations conflictuelles ayant été attribuées à divers membres de ce groupe ou de ce rôle. Par exemple, si le propriétaire de la table titles a octroyé différents droits à des membres du groupe sales, puis a décidé d'homogénéiser, il pourrait exécuter les instructions suivantes :

```
revoke all on titles from sales
grant select on titles(title, title_id, type,
        pub_id)
    to sales
```

De même, une instruction grant ou revoke avec le mot-clé public modifie, pour tous les utilisateurs, les éventuelles autorisations antérieures entrant en conflit avec le nouveau régime.

Exécutées dans des ordres différents, les mêmes instructions grant et revoke peuvent aboutir à des situations complètement différentes. Par exemple, le jeu d'instructions suivantes ôte à Jose, qui appartient au groupe public, tout droit select sur titles :

```
grant select on titles(title_id, title) to jose
revoke select on titles from public
```

Si elles sont émises dans l'ordre inverse, Jose devient le seul utilisateur disposant de droits select, mais uniquement sur les colonnes title_id et title.

```
revoke select on titles from public
grant select on titles(title_id, title) to jose
```

Si vous spécifiez le mot-clé public avec grant, vous êtes inclus dans le résultat. Lors de l'utilisation de revoke sur des droits de création d'objets, vous êtes inclus dans public sauf si la base de données vous appartient. Pour revoke sur des droits d'accès aux objets, vous êtes inclus dans public sauf si l'objet vous appartient. Il est possible de s'interdire soi-même d'utiliser sa propre table, tout en s'octroyant un droit d'accès à une vue basée sur cette table. A cet effet, vous devez émettre les instructions grant et revoke qui définissent explicitement vos autorisations. Vous pouvez restaurer l'autorisation avec une instruction grant.

# Octroi et révocation de rôles

Une fois défini, un rôle peut être octroyé à n'importe quel login ou rôle sur le serveur, à condition de respecter les règles de hiérarchie et d'exclusivité ponctuelle. Le tableau 11-4 répertorie les tâches liées aux rôles, les rôles requis pour exécuter les différentes tâches et les commandes à utiliser.

***Tableau 11-4 : Tâches, rôles requis et commandes à utiliser***

| Tâche | Rôle requis | Commande |
|---|---|---|
| Octroyer le rôle sa_role | Administrateur système | grant role |
| Octroyer le rôle sso_role | Responsable de la sécurité du système | grant role |
| Octroyer le rôle oper_role | Responsable de la sécurité du système | grant role |
| Octroyer des rôles définis par l'utilisateur | Responsable de la sécurité du système | grant role |
| Créer des hiérarchies de rôles | Responsable de la sécurité du système | grant role |
| Modifier des hiérarchies de rôles | Responsable de la sécurité du système | revoke role |
| Révoquer des rôles système | Responsable de la sécurité du système | revoke role |
| Révoquer des rôles définis par l'utilisateur | Responsable de la sécurité du système | revoke role |

## Octroi de rôles

Pour octroyer des rôles à des utilisateurs ou à d'autres rôles, exécutez la commande ci-dessous :

grant role rôle_octroyé [{, *rôle_octroyé*}...]
to *bénéficiaire* [{, *bénéficiaire*}...]

où :

- *rôle_octroyé* est le rôle octroyé. Vous pouvez spécifier autant de rôles que vous le souhaitez.
- *bénéficiaire* est le nom du rôle ou de l'utilisateur. Vous pouvez spécifier autant de bénéficiaires que vous le souhaitez.

Tous les rôles répertoriés dans l'instruction grant sont octroyés à tous les bénéficiaires. Si vous attribuez un rôle à un autre rôle, vous créez une hiérarchie de rôles.

Par exemple, pour octroyer les rôles "financial_analyst" et "payroll_specialist" à Sue, Mary et John, exécutez la commande suivante :

```
grant role financial_analyst, payroll_specialist
  to susan, mary, john
```

## Rôles et commande *grant*

Vous pouvez utiliser la commande grant pour octroyer des autorisations sur des objets à tous les utilisateurs dotés d'un rôle particulier, que celui-ci ait été défini par le système ou par l'utilisateur. Cela vous permet de restreindre l'utilisation d'un objet aux seuls utilisateurs possédant l'un des rôles suivants :

- administrateur système,
- responsable de la sécurité du système,
- opérateur,
- tout rôle défini par l'utilisateur.

Vous pouvez également utiliser la commande grant pour octroyer un rôle à un groupe, un utilisateur ou à un ou plusieurs autres rôles.

Toutefois, l'autorisation grant n'empêche pas les utilisateurs *non* dotés du rôle spécifié de se voir attribuer l'autorisation d'exécution sur une procédure stockée. Pour vous assurer, par exemple, que seuls les administrateurs système peuvent exécuter et mener à bien une procédure stockée, insérez la fonction système proc_role au sein de la procédure stockée elle-même. Pour plus d'informations, reportez-vous à la section "Affichage d'informations sur les rôles", page 408.

Les autorisations attribuées à des rôles sont prioritaires sur celles octroyées à des utilisateurs ou à des groupes. Supposons, par exemple, que John ait été nommé responsable de la sécurité du système et que le rôle sso_role ait des droits d'accès à la table sales. Même si les droits de l'utilisateur John sur sales sont révoqués, ce dernier a toujours accès à sales grâce à son rôle sso_role qui prévaut sur son autorisation individuelle.

Lors de l'octroi d'autorisations, le SA est considéré comme le propriétaire de l'objet traité. Si les autorisations qu'il octroie s'appliquent à un objet appartenant à un autre utilisateur, le nom de l'utilisateur apparaît dans sysprotects et dans le résultat de sp_helprotect comme étant l'utilisateur ayant octroyé ces autorisations.

Si plusieurs utilisateurs autorisent une même personne à accéder à un objet, ses droits d'accès restent actifs tant qu'ils n'ont pas été révoqués par tous ceux qui les ont octroyés. Si un SA révoque ces droits, la personne ne peut plus accéder à l'objet, même si d'autres utilisateurs l'y avaient autorisée.

## Révocation de rôles

La commande revoke role permet de révoquer les rôles attribués à des utilisateurs et à d'autres rôles :

revoke role *nom_rôle* [{*, nom_rôle*}...]from *bénéficiaire* [{*,bénéficiaire*}...]

où :

- *nom_rôle* est le rôle révoqué. Vous pouvez spécifier autant de rôles que vous le souhaitez.
- *bénéficiaire* est le nom du rôle ou de l'utilisateur. Vous pouvez spécifier autant de bénéficiaires que vous le souhaitez.

Tous les rôles répertoriés dans l'instruction revoke sont révoqués de tous les bénéficiaires.

Vous ne pouvez révoquer un rôle d'un utilisateur lorsque celui-ci est connecté.

# Contrôle d'accès aux lignes

Les propriétaires de bases de données et de tables peuvent limiter l'accès aux lignes de données d'une table en définissant des règles d'accès et en associant ces règles à la table en question. L'accès aux données peut, en outre, être contrôlé en définissant des contextes applicatifs et en créant des triggers de login.

Ces fonctions peuvent être regroupées sous la notion de contrôle d'accès aux lignes. Le contrôle d'accès aux lignes permet au propriétaire d'une base de données ou d'une table de contrôler les lignes d'une table auxquelles les utilisateurs peuvent accéder après s'être authentifiés ou en fonction de leur profil et des privilèges dont ils bénéficient au niveau applicatif. Adaptive Server applique le contrôle d'accès aux lignes pour tous les langages de manipulation de données (DML), ce qui évite que les utilisateurs puissent contourner le contrôle d'accès pour accéder aux données.

## Règles d'accès

Les règles de domaine permettent aux propriétaires de tables de contrôler les valeurs saisies par les utilisateurs dans une colonne donnée utilisant un type de données standard ou dans toute autre colonne contenant un type de données défini par l'utilisateur. Les règles sont appliquées lors des insertions et des mises à jour.

Adaptive Server applique la protection des lignes par l'intermédiaire de règles d'accès. Les règles d'accès sont appliquées lors des opérations select, update et delete. Adaptive Server applique les règles d'accès sur toutes les colonnes lues lors d'une requête, même si les colonnes ne figurent pas dans la liste select. En d'autres termes, pour une requête donnée, Adaptive Server applique la règle de domaine sur la table mise à jour et la règle d'accès sur les tables lues.

L'utilisation de règles d'accès est semblable à l'utilisation de vues ou d'une requête ad hoc avec des clauses where et ne nuit pas aux performances. La requête est compilée et optimisée après association des règles d'accès. Par conséquent, si les colonnes associées à des règles d'accès comportent des index, les requêtes sont mieux réalisées.

## Règles d'accès utilisant Java et les contextes applicatifs

Les développeurs d'applications peuvent créer des règles d'accès souples à l'aide de Java et des contextes applicatifs, décrits à la section "Contextes applicatifs", page 451. Il est possible, par exemple, de créer une règle hiérarchique. Si la table T contient les plannings de tous les employés, le directeur peut visualiser tous ces plannings. Les VP individuels peuvent visualiser leur propre planning et la charge de travail du rapport direct, mais pas le planning du directeur.

Les règles d'accès peuvent être liées aux types de données configurés par l'utilisateur, définis à l'aide de sp_addtype. Adaptive Server applique les règles d'accès aux tables utilisateur qui utilisent ces types de données définis par l'utilisateur. Cela évite au propriétaire de la base de données et de la table d'avoir à associer les règles d'accès à des colonnes dans leur forme normalisée. Par exemple, un utilisateur peut avoir défini un type de données appelé username dont le type standard est varchar(30). Le propriétaire de la base de données ou de la table peut créer une règle d'accès et l'associer au type de données username. Le propriétaire peut alors utiliser username pour toutes les tables utilisées par ses applications. Adaptive Server applique la règle d'accès aux tables dont les colonnes contiennent des données du type username.

## Syntaxe des règles d'accès

Le paramètre access est utilisé dans la syntaxe create rule pour vous permettre de créer des règles d'accès. Par exemple, le propriétaire d'une table crée et remplit la table T (username char(30), title char(20), classified_data char(1024)) :

```
AA, "Administrative Assistant","Memo to President"
AA, "Administrative Assistant","Tracking Stock Movements"
VP1, "Vice President", "Meeting Schedule"
VP2, "Vice President", "Meeting Schedule"
```

Le propriétaire de la table crée une valeur par défaut et une règle de domaine dans la colonne username. La règle de domaine est destinée à veiller à ce que la mise à jour de la colonne soit effectuée avec des valeurs correctes. Si la valeur par défaut et la règle de domaine ne sont pas créées, il existe un risque de problème de sécurité : l'utilisateur peut insérer une ligne dans la table contenant des données arbitraires auxquelles ne s'appliquera pas la règle d'accès.

Le propriétaire de la table crée alors une règle d'accès qu'il associe à la colonne username à l'aide de la commande sp_bindrule.

```
create default uname_default
as suser_name()
go

sp_bindefault uname_default, "T.username"
go

*/
create accessrule uname_acc_rule
as @username = suser_name()
go

sp_bindrule uname_acc_rule, "T.username"
go
```

Un utilisateur émet la requête suivante :

```
select * from T
```

Adaptive Server traite la règle d'accès liée à la colonne username de la table T et l'associe à l'arbre de requête. L'arbre est alors optimisé et un plan d'exécution est généré et exécuté comme si l'utilisateur avait réalisé la requête avec la clause de filtre fournie dans la règle d'accès. En d'autres termes, Adaptive Server associe la règle d'accès et exécute la requête comme suit :

```
select * from T where T.username = suser_name().
```

Si un assistant administratif exécute la requête select, le résultat est le suivant :

```
AA, "Administrative Assistant","Memo to President"
AA, "Administrative Assistant","Tracking Stock Movements"
```

La partie where T.username = suser_name() de la requête est appliquée par le serveur. L'utilisateur ne peut pas passer outre la règle d'accès.

## Syntaxe de règle d'accès étendue

Vous pouvez créer deux types de règles d'accès : la règle AND et la règle OR. La règle d'accès peut être liée à une colonne, à un nom d'utilisateur ou à un type de données défini par l'utilisateur. Il est possible de lier plusieurs règles d'accès aux différentes colonnes ou aux différents types de données d'une table. Lors de l'accès à la table, différentes règles d'accès prennent effet et interagissent les unes avec les autres. Les règles d'accès OR sont utilisées conjointement et si au moins l'une des règles d'accès OR aboutit, la ligne devient accessible. Les règles d'accès AND sont utilisées conjointement et si toutes les règles d'accès AND aboutissent, la ligne devient accessible.

---

**Remarque** Si une ligne d'une table ne comprend qu'une règle d'accès et qu'il s'agit d'une règle OR, elle agit comme une règle AND.

---

Syntaxe

Pour créer une règle d'accès :

```
create rule [ [ and | or ] access]
    [propriétaire.]nom_règle
    as expression_conditionnelle
```

Pour lier des types de données :

```
sp_bindrule nom_règle, type_données
```

Pour lier des colonnes :

```
sp_bindrule nom_règle, colonne
```

Pour annuler le lien sur accessrule, le cas échéant :

```
sp_unbindrule type_données, null, "accessrule"
```

ou :

```
sp_unbindrule colonne, null, "accessrule"
```

Pour annuler le lien sur accessrule et domain_rule, le cas échéant :

```
sp_unbindrule type_données, null, "all"
```

ou

```
sp_unbindrule colonne, null, "all"
```

Pour appliquer ultérieurement unbindrule uniquement à accessrule, le cas échéant :

```
sp_unbindrule datatype, futureonly, "accessrule"
```

Pour appliquer ultérieurement unbindrule à accessrule et à la règle de domaine, le cas échéant :

sp_unbindrule *type_données*, futureonly, "all"

drop rule *nom_règle*

Exemple :

```
create  access rule empid1_access
as @empid = 1

create access rule deptno1_access
as @deptid =2

/*
**      create OR ACCESS rule by
**      "create or access rule rule_name as ..."
*/
create or access rule name1_access
as @name = "smith"

create or access rule phone_access
as @phone ="9999"

create table testtab1 (empno int, deptno int,name char(10), phone char(4))

/* Bound access rule to the columns */
sp_bindrule empid1_access, "testtab1.empno"
Rule bound to table column.
(return status = 0)

sp_bindrule deptno1_access,"testtab1.deptno"
Rule bound to table column.
(return status = 0)

sp_bindrule name1_access,"testtab1.name"
Rule bound to table column.
(return status = 0)

sp_bindrule phone_access,"testtab1.phone"
Rule bound to table column.
(return status = 0)

insert testtab1 values (1,1,"smith","3245")
(1 row affected)

insert testtab1 values(2,1,"jones","0283")
(1 row affected)
```

```
insert testtab1 values(1,2,"smith","8282")
(1 row affected)

insert testtab1 values(2,2,"smith","9999")
(1 row affected)

insert testtab1 values(3,2,"smith","8888")
(1 row affected)

insert testtab1 values(1,2,"jones","9999")
(1 row affected)

insert testtab1 values(2,3,"jones","9999")
(1 row affected)

/* return rows when empno = 1 and deptno = 2
** and ( name = "smith" or phone = "9999" )
*/
select * from testtab1
 empno       deptno      name       phone
 ----------- ----------- ---------- -----
 1           2           smith      8282
 1           2           jones      9999

(2 rows affected)

/* unbound accessrule from specific column */
sp_unbindrule "testtab1.empno",NULL,"accessrule"
Rule unbound from table column.
(return status = 0)

/* return rows when deptno = 2 and ( name = "smith"
** or phone = "9999" )
*/
select * from testtab1
 empno       deptno      name       phone
 ----------- ----------- ---------- -----
 1           2           smith      8282
 2           2           smith      9999
 3           2           smith      8888
 1           2           jones      9999

(4 rows affected)

/* unbound all rules from specific column */
sp_unbindrule "testtab1.deptno",NULL,"all"
Rule unbound from table column.
(return status = 0)
```

```
/* return the rows when name = "smith" or phone = "9999" */
select * from testtab1
 empno       deptno      name       phone
 ----------- ----------- ---------- -----
 1           1           smith      3245
 1           2           smith      8282
 2           2           smith      9999
 3           2           smith      8888
 1           2           jones      9999
 2           3           jones      9999

(6 rows affected)
```

## Règles d'accès et commande *alter table*

Lorsque le propriétaire de la table utilise la commande alter table, Adaptive Server désactive les règles d'accès lors de l'exécution de la commande et les réactive après exécution de la commande. Les règles d'accès sont désactivées afin d'éviter le filtrage des données de la table pendant l'exécution de la commande alter table.

## Règles d'accès et *bcp*

Adaptive Server applique les règles d'accès lorsque les données sont copiées d'une table à l'aide de l'utilitaire de bulkcopy (bcp). Adaptive Server ne peut pas désactiver les règles d'accès comme avec la commande alter table car bcp peut être utilisé par quiconque possède les droits de sélection dans la table.

Pour des raisons de sécurité, le propriétaire de la base de données doit verrouiller la table exclusivement et désactiver les règles d'accès pendant l'utilisation de bulkcopy. Le verrouillage a pour effet d'empêcher l'accès aux autres utilisateurs alors que les règles d'accès sont désactivées. Le propriétaire de la base de données doit activer les règles d'accès et déverrouiller la table après la copie des données.

---

**Remarque** Si les règles d'accès sont activées, bcp out n'extrait que les données que l'utilisateur qui exécute bcp est autorisé à copier. Si c'est la table entière qui doit être copiée, verrouillez la table, supprimez les règles d'accès, copiez les données à l'aide de bcp out et réappliquez les règles d'accès avant de déverrouiller la table.

---

## Scénarios d'utilisation de règles d'accès

Dans cet exemple, considérez qu'il existe une règle de domaine pour la colonne region et une règle d'accès pour la colonne custid qui n'est pas utilisée dans cette requête. Pour les mises à jour, le système lit la table customer_table et la met à jour. Adaptive Server applique la règle d'accès lors de la lecture de customer_table sur la colonne custid et, suite à la mise à jour, applique la règle de domaine sur la colonne region.

```
update customer_table
    set region = 'northwest'
    where region = 'north'
```

Dans cet exemple, considérez que des règles de domaine sont appliquées à orders_table et que des règles d'accès sont appliquées à old_orders_table. Adaptive Server applique la règle de domaine à orders_table car orders_table est mise à jour et la règle d'accès à old_orders_table car old_orders_table est lue.

```
insert into orders_table
select *
    from old_orders_table
```

## Règles d'accès utilisant des fonctions Java définies par l'utilisateur

Les règles d'accès peuvent utiliser des fonctions Java définies par l'utilisateur qui utilisent JDBC pour consulter des données dans d'autres tables. Grâce aux fonctions Java, vous pouvez, par exemple, créer des règles élaborées qui utilisent le profil de l'application, l'utilisateur connecté à l'application en vue d'une utilisation et les rôles mis à disposition de l'utilisateur pour l'application.

La classe Java ci-dessous utilise la méthode GetSecVal pour illustrer comment utiliser des méthodes Java comme fonctions définies par l'utilisateur dans des règles d'accès.

```
import java.sql.*;
import java.util.*;

public class sec_class {
static String _url = "jdbc:sybase:asejdbc";
public static int GetSecVal(int c1)
{
try
{
PreparedStatement pstmt;
ResultSet rs = null;
```

```
Connection con = null;
int pno_val;

pstmt = null;

Class.forName("sybase.asejdbc.ASEDriver");
con = DriverManager.getConnection(_url);

if (con == null)
{
return (-1);
}

pstmt = con.prepareStatement("select classification from sec_tab where id = ?");

if (pstmt == null)
{
return (-1);
}

pstmt.setInt(1, c1);

rs = pstmt.executeQuery();
rs.next();

pno_val = rs.getInt(1);

rs.close();

pstmt.close();

con.close();

return (pno_val);

}
catch (SQLException sqe)
{
return(sqe.getErrorCode());
}
catch (ClassNotFoundException e)
{

System.out.println("Unexpected exception : " + e.toString());
System.out.println("\nThis error usually indicates that " + "your Java CLASSPATH
environment has not been set properly.");
e.printStackTrace();
```

```
return (-1);
}

catch (Exception e)
{
System.out.println("Unexpected exception : " + e.toString());
e.printStackTrace();
return (-1);
}
}
}
```

```
(from Shell)
javac sec_class.java
```

```
jar cufo sec_class. jar sec_class.class
installjava -Usa -Password -f/work/work/FGAC/sec_class.jar -
-D testdb
```

```
(from isql)
```

```
create table sec_tab (id int, classification int)
go
insert into sec_tab values (1,10)
insert into sec_tab values (2,9)
insert into sec_tab values (3,7)
insert into sec_tab values (4,7)
insert into sec_tab values (5,4)
insert into sec_tab values (6,4)
insert into sec_tab values (7,4)
go

sp_addtype class_level, int
go

create table sec_data (c1 varchar(30),
c2 varchar(30),
c3 varchar(30),
clevel class_level)
go

declare @v1 int
select @v1 = 5
while @v1 > 0
begin
insert into sec_data values('8', 'aaaaaaaaaa', 'aaaaaaaaaa', 8)
insert into sec_data values('7', 'aaaaaaaaaa', 'aaaaaaaaaa', 7)
insert into sec_data values('5', 'aaaaaaaaaa', 'aaaaaaaaaa', 5)
insert into sec_data values('5', 'aaaaaaaaaa', 'aaaaaaaaaa', 5)
```

```
insert into sec_data values('2', 'aaaaaaaaaa', 'aaaaaaaaaa', 2)
insert into sec_data values('3', 'aaaaaaaaaa', 'aaaaaaaaaa', 3)
select @v1 = @v1 -1
end
go

create access rule clevel as
@clevel <= sec_class.GetSecVal(suser_id())
go

create default clevel_def as sec_class.GetSecVal(suser_id())
go

sp_bindefault clevel_def, class_level
go

sp_bindrule clevel, class_level
go

grant all on sec_data to public
go
grant all on sec_tab to public
go
```

## Contextes applicatifs

Les applications sur un serveur de base de données doivent être programmées de manière à limiter l'accès aux données en fonction des utilisateurs et des profils utilisateur.

Le développeur de l'application est chargé de coder l'application de manière appropriée. Par exemple, une application de ressources humaines est programmée pour connaître les utilisateurs autorisés à mettre à jour les informations relatives aux salaires.

Les contextes applicatifs permettent aux utilisateurs de définir, stocker et extraire des profils utilisateur (les rôles que les différents utilisateurs peuvent utiliser et les groupes auxquels ils appartiennent) et l'application utilisée par les différents utilisateurs. Les contextes applicatifs peuvent servir à stocker et à extraire des données client arbitraires, et peuvent utiliser Adaptive Server pour stocker les informations du client.

Les contextes applicatifs sont spécifiques à une session. Ils ne perdurent pas au-delà des sessions mais restent disponibles sur tous les niveaux imbriqués d'exécution des instructions, contrairement aux variables locales.

Un contexte applicatif se compose de *nom_contexte*, *nom_attribut* et *valeur_attribut*. Les utilisateurs définissent le *nom_contexte*, les *attributs* et values pour chaque contexte. Sybase propose de nombreux attributs dans le contexte applicatif système, sys_session. Pour plus d'informations, reportez-vous au point 11 de la section Exemples.

Vous pouvez également créer vos propres contextes applicatifs comme décrit dans la section "Création et gestion des contextes applicatifs", page 453.

## Définition d'autorisations pour l'utilisation de fonctions de contexte applicatif

Les contextes applicatifs sont définis, extraits et supprimés à l'aide de fonctions, ce qui signifie que tout utilisateur connecté peut réinitialiser les profils de la session. Même si l'exécution d'une fonction est soumise à un audit, la sécurité peut être atteinte avant que le problème soit détecté. Vous pouvez limiter l'accès aux fonctions à l'aide des privilèges grant et revoke. Seules les fonctions de contexte applicatif effectuent des vérifications de contrôle sur l'utilisateur.

L'octroi ou la révocation de privilèges pour les autres fonctions n'ont aucun impact sur Adaptive Server.

L'exécution des fonctions de contexte applicatif est traitée comme un langage de manipulation de données. Le propriétaire de la fonction est l'administrateur système du serveur. Seuls les utilisateurs dotés du rôle sa_role peuvent octroyer ou révoquer des privilèges sur les fonctions. Seul le privilège select est vérifié dans le cadre des vérifications de contrôle d'accès aux données appliquées au serveur effectuées par les fonctions.

Par défaut, les privilèges sur les fonctions sont révoqués pour PUBLIC et correspondent aux valeurs par défaut courantes pour les privilèges au niveau des tables.

Vous pouvez octroyer et révoquer des privilèges aux utilisateurs, aux rôles et aux groupes dans une base de données déterminée pour les objets figurant dans cette base de données. Parmi les quelques exceptions figurent create database, set session authorization et connect. Un utilisateur qui se voit octroyer ces privilèges doit être un utilisateur correct dans la base de données master. En ce qui concerne les autres privilèges, l'utilisateur doit être correct dans la base de données dans laquelle se trouve l'objet.

En revanche, les fonctions ne possèdent pas d'ID objet ni de base de données locale. Dans chaque base de données, le propriétaire de la base de données doit octroyer à l'utilisateur approprié le privilège select pour les fonctions. Adaptive Server cherche la base de données par défaut pour l'utilisateur et vérifie les autorisations vis-à-vis de cette base de données. Grâce à cette approche, seul le propriétaire de la base de données par défaut doit octroyer le privilège select. Si d'autres bases de données doivent être limitées, le propriétaire desdites bases de données doit révoquer explicitement l'autorisation pour l'utilisateur dans ces bases de données.

Un administrateur système peut exécuter les commandes ci-dessous pour octroyer ou révoquer des privilèges de sélection pour des fonctions de contexte applicatif spécifiques :

set_appcontext où le type de données de *nom_contexte* et de *nom_attribut* correspond à char(30).

Si l'attribut n'existe pas dans le contexte applicatif, get_appcontext renvoie la valeur "null".

La valeur de l'attribut est renvoyée sous forme de type de données char.

Si la règle doit comparer la valeur de l'attribut aux autres types de données, elle doit convertir les données char au type de données approprié, list_appcontext rm_appcontext.

## Création et gestion des contextes applicatifs

Les fonctions ci-dessous permettent de créer et de gérer les contextes applicatifs :

```
grant select on set_appcontext to user_role
grant select on set_appcontext to joe_user
revoke select on set_appcontext from joe_user
set_appcontext
set_appcontext is used to set a context name, attribute name, and attribute
value for the user session.
set_appcontext ("context_name", "attribute_name", "attribute_value")
```

Où le type de données de *nom_contexte* et de *nom_attribut* correspond à char(30) et le type de données de *valeur_attribut* correspond à char(2048). Cette fonction renvoie 0 en cas de réussite et -1 en cas d'échec. set_appcontext ne peut pas remplacer les valeurs d'un contexte applicatif existant. Si vous souhaitez affecter de nouvelles valeurs à un contexte, supprimez le contexte et recréez-le avec ces nouvelles valeurs. Si les valeurs en cours de définition existent déjà dans la session, la fonction renvoie -1. Les attributs sont enregistrés comme données de type char. Si la règle doit comparer la valeur de l'attribut aux autres types de données, elle doit convertir les données char au type de données approprié.

Exemples

Cet exemple présente set_appcontext dont la conversion du type de données apparaît dans la valeur :

```
select set_appcontext("CONTEXT1","ATTR1", "VALUE1")
------------
0
This example creates an application context named CONTEXT1. The attribute
is named ATTR1 with a value of VALUE1.
select set_appcontext("CONTEXT1", "ATTR2", convert(char(20), @numericvar)
-----------
0
```

Cet exemple présente le résultat découlant de la tentative de remplacement d'un contexte applicatif existant. Ce contexte a été créé dans l'exemple 1. Il doit être supprimé, puis recréé avec les nouvelles valeurs :

```
select set_appcontext("CONTEXT1", "ATTR1", "VALUE1")
----------
-1
```

Cet exemple présente ce qui résulte de la tentative d'un utilisateur ne disposant pas des autorisations appropriées de définir le contexte applicatif :

```
select set_appcontext("CONTEXT1", "ATTR2", "VALUE1")
Select permission denied on function set_appcontext, database dbid
set_appcontext
get_appcontext returns the value of the attribute in a given context.
get_appcontext ("context_name", "attribute_name")
```

Où le type de données de *nom_contexte* et *nom_attribut* correspond à char(30). Si l'attribut n'existe pas dans le contexte applicatif, get_appcontext renvoie la valeur "null". La valeur de l'attribut est renvoyée sous forme de type de données char. Si la règle doit comparer la valeur de l'attribut aux autres types de données, elle doit convertir les données char au type de données approprié.

# Obtention des autorisations d'un autre utilisateur

Adaptive Server offre deux moyens d'emprunter l'identité et les autorisations d'un utilisateur tiers :

- Un DBO peut exécuter la commande setuser pour "prendre l'identité" d'un autre utilisateur, ainsi que ses autorisations dans la base de données courante. Pour plus d'informations, reportez-vous à la section "Utilisation de setuser", page 455.
- **procuration** permet à un utilisateur d'emprunter l'identité d'un autre utilisateur à l'échelle d'un serveur. Pour plus d'informations, reportez-vous à la section "Utilisation de la procuration", page 456.

## Utilisation de setuser

Un propriétaire de base de données peut utiliser setuser pour :

- accéder à un objet appartenant à une autre personne ;
- octroyer des autorisations sur un objet propriétaire par un autre utilisateur ;
- créer un objet qui appartiendra à un autre utilisateur ;
- acquérir temporairement les autorisations DAC d'un autre utilisateur, pour une quelconque raison.

Même si la commande setuser permet au DBO d'obtenir automatiquement les autorisations DAC d'un autre utilisateur, elle n'affecte pas les rôles qui ont été octroyés.

Par défaut, les droits setuser sont attribués au DBO et ne sont pas transférables. La personne dont il prend l'identité doit être un utilisateur valable de la base de données. Adaptive Server vérifie les autorisations de l'utilisateur dont l'identité a été empruntée.

Les administrateurs système peuvent exécuter setuser pour créer des objets destinés à une autre personne. Cependant, comme les SA opèrent en dehors du système d'autorisations DAC, ils n'ont pas besoin d'utiliser setuser pour acquérir les droits d'un autre utilisateur. Cette commande reste active jusqu'à ce qu'une nouvelle commande setuser soit exécutée, que la base de données courante soit changée, ou que l'utilisateur se déconnecte.

La syntaxe est la suivante :

```
setuser ["nom_utilisateur"]
```

où *nom_utilisateur* est un utilisateur défini dans la base de données, et dont l'identité doit être empruntée.

Pour rétablir votre identité initiale, utilisez setuser sans définir *nom_utilisateur*.

L'exemple suivant montre comment le propriétaire de la base de données courante octroierait à Joe le droit de lire la table authors, qui appartient à Mary :

```
setuser "mary"

grant select on authors to joe

setuser     /*re-establishes original identity*/
```

## Utilisation de la procuration

La fonction de procuration d'Adaptive Server permet aux responsables de la sécurité du système d'octroyer à certains logins la possibilité de prendre le contexte de sécurité d'un autre utilisateur. En outre, une application peut exécuter des tâches de façon contrôlée pour le compte de différents utilisateurs. S'il est autorisé à utiliser une procuration, le login peut emprunter tout autre login dans Adaptive Server.

---

**Avertissement !** La possibilité d'emprunter l'identité d'un autre utilisateur est une fonction très puissante. Elle doit donc être restreinte à des administrateurs et des applications sûrs. En effet, un utilisateur doté de cette autorisation peut même prendre l'identité du login "sa" et ainsi disposer d'un accès illimité dans Adaptive Server.

---

Un utilisateur exécutant les commandes set proxy ou set session authorization se sert à la fois du nom de login et de l'ID de l'utilisateur dont il emprunte l'identité. Le nom de login et l'ID utilisateur du serveur sont respectivement stockés dans les colonnes name et suid de master..syslogins. Ces valeurs sont actives sur tout le serveur, dans toutes les bases de données.

---

**Remarque** Les commandes set proxy et set session authorization ont la même fonction et sont interchangeables. Elles se distinguent uniquement par le fait que set session authorization est compatible ANSI SQL92, alors que set proxy est une extension Transact-SQL.

---

## Octroi d'une procuration

Les responsables de la sécurité du système utilisent les commandes grant set proxy ou grant set session authorization pour accorder le droit à un utilisateur d'emprunter l'identité d'un autre utilisateur sur le serveur. L'utilisateur doté de cette autorisation peut alors exécuter la commande set proxy ou set session authorization pour prendre l'identité d'un utilisateur tiers.

Seul le responsable de la sécurité du système est habilité à octroyer une procuration. En outre, il doit exécuter la commande grant à partir de la base master. La syntaxe est la suivante :

grant *set proxy*
to {public | *liste_noms* | *nom_rôle*}

ou

grant *set session authorization*
to {public | *liste_noms* | *nom_rôle*}

où :

- *public* représente tous les utilisateurs. Il est recommandé de ne pas accorder ce droit à "public".
- *nom_rôle* est un rôle Adaptive Server défini par le système ou par l'utilisateur. Vous pouvez accorder des autorisations à des utilisateurs en fonction du rôle qui leur a été attribué.
- *liste_noms* est une liste de noms d'utilisateur ou de groupe, séparés par des virgules. L'utilisateur doit figurer dans la base de données master.

Pour octroyer l'autorisation set proxy à une application de login "appl" lorsque votre rôle sso_role n'est pas actif, et que vous n'êtes pas sur la base master, exécutez la commande suivante :

```
use master
go
set role sso_role on
go
grant set proxy to appl
go
```

Pour octroyer l'autorisation set proxy au rôle "accountant" défini par l'utilisateur, exécutez la commande suivante :

```
grant set proxy to accountant
```

Pour octroyer l'autorisation set session authorization au login "sa", répertorié en tant que "dbo" dans toutes les bases de données, exécutez la commande suivante :

```
grant set proxy to dbo
```

## Exécution de la procuration

Les règles suivantes doivent être observées lorsque vous exécutez les commandes set proxy ou set session authorization :

- Vous ne pouvez pas exécuter set proxy ou set session authorization dans une transaction.
- Vous ne pouvez pas utiliser un login verrouillé pour le proxy d'un autre utilisateur. Par exemple, si le login "joseph" est verrouillé, la commande ci-dessous n'est pas autorisée :

```
set proxy "joseph"
```

- Vous pouvez exécuter set proxy ou set session authorization à partir de n'importe quelle base à laquelle vous avez accès. Toutefois, le *nom_login* spécifié doit correspondre à un utilisateur répertorié dans la base ou un utilisateur "guest" doit y avoir été défini.
- Un seul niveau est admis. Pour prendre l'identité de plusieurs utilisateurs, vous devez reprendre votre identité initiale entre deux emprunts d'identité.
- Si vous exécutez set proxy ou set session authorization à partir d'une procédure, vous reprenez automatiquement votre identité initiale lorsque vous quittez la procédure.

Si votre login s'est vu attribuer le droit d'utiliser les commandes set proxy ou set session authorization, vous pouvez emprunter l'identité d'un autre utilisateur. La syntaxe est la suivante :

set proxy *nom_login*

ou

set session authorization *nom_login*

où *nom_login* est le nom d'un login répertorié dans master..syslogins. Placez le nom de login entre guillemets.

Par exemple, pour prendre l'identité de "mary", exécutez :

```
set proxy mary
```

Après avoir exécuté la commande set proxy, vérifiez votre nom de login sur le serveur et votre nom d'utilisateur dans la base de données. Supposons que votre login soit "ralph" et que vous soyez doté de l'autorisation de procuration (set proxy). Vous voulez exécuter certaines commandes sous le login "sallyn" et "rudolph" dans la base pubs2. "sallyn" est bien répertorié ("sally") dans la base, tandis que Ralph et Rudolph ne le sont pas. Un utilisateur "guest" a néanmoins été défini dans la base pubs2. Vous pouvez exécuter la commande suivante :

```
set proxy "sallyn"
go
use pubs2
go
select suser_name(), user_name()
go
------------------------------ ------------------
sallyn                         sally
```

Pour utiliser Rudolph, vous devez dans un premier temps revenir à votre identité initiale. Pour ce faire, exécutez la commande suivante :

```
set proxy "ralph"
select suser_name(), user_name()
go
------------------------------ ------------------
ralph                          guest
```

Notez que Ralph est un utilisateur "guest" dans la base de données.

Exécutez ensuite :

```
set proxy "rudolph"
go
select suser_name(), user_name()
go
------------------------------ ------------------
rudolph                        guest
```

Rudolph est également un utilisateur guest dans la base de données car son nom n'est pas répertorié dans la base.

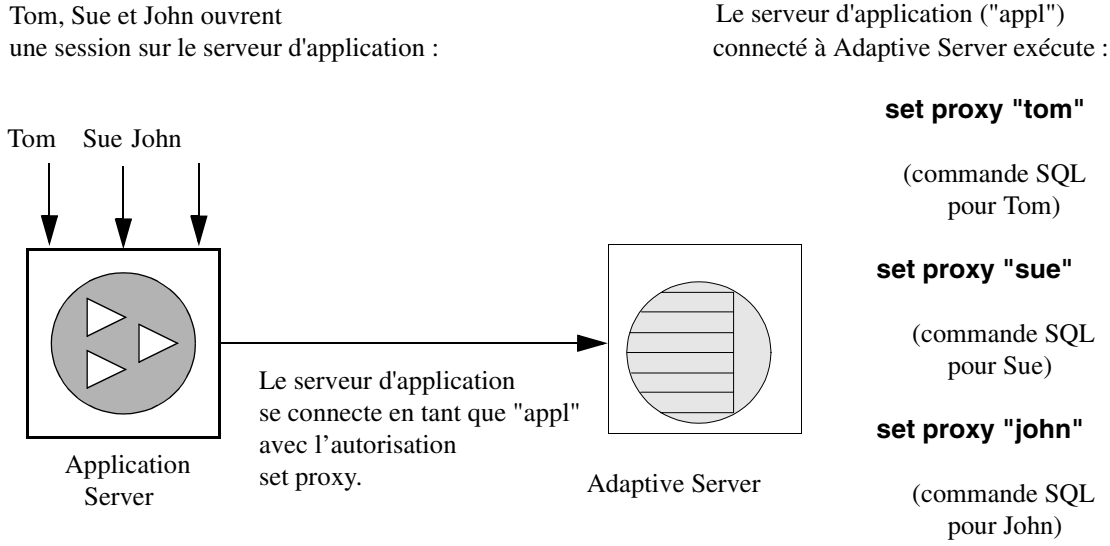
A présent, prenez l'identité du login "sa". Exécutez la commande suivante :

```
set proxy "ralph"
go
set proxy "sa"
go
select suser_name(), user_name()
go
--------------------------- -------------------
sa                          dbo
```

### Procuration pour des applications

La figure 11-1 présente un serveur d'application se connectant à Adaptive Server sous le login générique "appl" afin d'exécuter des procédures et des commandes pour le compte de plusieurs utilisateurs. Lorsque "appl" prend l'identité de Tom, l'application dispose des autorisations de Tom. De même, lorsque "appl" emprunte l'identité de Sue et de John, l'application bénéficie uniquement des autorisations de Sue et de John respectivement.

***Figure 11-1 : Applications et procuration***




# Rapport sur les autorisations

Le tableau 11-5 répertorie les procédures système permettant d'obtenir des informations sur les droits de création et d'accès relatifs aux objets :

***Tableau 11-5 : Procédures système affichant les autorisations***

| Pour obtenir des informations sur les autorisations suivantes | Utiliser |
|---|---|
| Serveurs proxy | Tables système |
| Utilisateurs et processus | sp_who |
| Autorisations sur les objets ou les utilisateurs de base de données | sp_helprotect |

| Pour obtenir des informations sur les autorisations suivantes | Utiliser |
|---|---|
| Autorisations sur des tables spécifiques | sp_table_privileges |
| Autorisations sur des colonnes spécifiques dans une table | sp_column_privileges |

## Interrogation de la table *sysprotects* concernant les procurations

Pour afficher des informations relatives aux autorisations octroyées ou révoquées aux utilisateurs, aux groupes ou aux rôles concernés, interrogez la table sysprotects. La colonne action spécifie l'autorisation. Par exemple, la valeur de la colonne action pour les commandes set proxy ou set session authorization peut être 167.

Vous pouvez exécuter cette requête :

```
select * from sysprotects where action = 167
```

Le résultat indique l'ID de l'utilisateur qui a octroyé ou révoqué l'autorisation (colonne grantor), l'ID de l'utilisateur qui dispose de l'autorisation (colonne uid) et le type de protection (colonne protecttype). Cette dernière colonne peut contenir les valeurs ci-dessous :

- 0 pour grant with grant
- 1 pour grant
- 2 pour revoke

Pour plus d'informations sur la table sysprotects, reportez-vous au document *Manuel de référence d'Adaptive Server*.

## Affichage d'informations relatives aux utilisateurs et aux processus

La procédure système sp_who affiche des informations relatives à tous les utilisateurs et les processus courants d'Adaptive Server ou à un utilisateur ou processus particulier. Le résultat de sp_who fait état de loginame et de orignamе. Si un utilisateur exécute des opérations par procuration, la valeur de orignamе correspond au login initial. Supposons que "ralph" a exécuté la commande :

```
set proxy susie
```

suivie de commandes SQL.

sp_who renvoie "susie" comme loginame et "ralph" comme origname.

sp_who interroge la table système master..sysprocesses, qui contient les colonnes suid (ID utilisateur sur le serveur) et origsuid (ID utilisateur initial sur le serveur).

Pour plus d'informations, reportez-vous à la section sp_who dans le document *Manuel de référence d'Adaptive Server*.

## Rapport sur les autorisations sur les objets ou les utilisateurs de base de données

Utilisez la procédure système sp_helprotect pour afficher les droits classés par objet ou par utilisateur de base de données et, si nécessaire, par utilisateur pour un objet spécifique. Toute personne peut exécuter cette procédure. La syntaxe est la suivante :

```
sp_helprotect [nom [, nom_utilisateur [, "grant"
    [,"none"|"granted"|"enabled"|role_name]]]]
```

où :

- *nom* représente soit le nom d'un objet (table, vue ou procédure stockée), soit celui d'un utilisateur, d'un groupe ou d'un rôle de la base de données courante. Si ce paramètre est omis, sp_helprotect affiche toutes les autorisations définies dans la base de données.
- *nom_utilisateur* est le nom d'un utilisateur de la base courante.

Si vous spécifiez le second paramètre *nom_utilisateur*, seuls les droits de cet utilisateur sur l'objet spécifié sont affichés. Si *nom* ne correspond pas à un objet, sp_helprotect vérifie s'il s'agit d'un utilisateur, d'un groupe ou d'un rôle et dans l'affirmative, répertorie les autorisations associées. Si vous spécifiez le mot-clé grant et que *nom* n'est pas un objet, sp_helprotect affiche toutes les autorisations octroyées avec with grant option.

grant indique les droits octroyés à *nom* with grant option.

none ignore les rôles octroyés à l'utilisateur.

granted inclut des informations sur tous les rôles octroyés à l'utilisateur.

enabled inclut des informations sur tous les rôles activés par l'utilisateur.

*nom_rôle* affiche des informations relatives au rôle spécifié uniquement, même s'il n'a pas été octroyé à l'utilisateur.

Supposons, par exemple, que vous exécutiez la série d'instructions grant et revoke suivante :

```
grant select on titles to judy
grant update on titles to judy
revoke update on titles(contract) from judy
grant select on publishers to judy
with grant option
```

Pour connaître les autorisations détenues par Judy sur chaque colonne de la table titles, entrez :

```
sp_helprotect titles, judy
```

```
grantor grantee type   action   object     column      grantable
------- ------ -----   ------   ------     ------      -------
dbo     judy   Grant   Select   titles     All         FALSE
dbo     judy   Grant   Update   titles     advance     FALSE
dbo     judy   Grant   Update   titles     notes       FALSE
dbo     judy   Grant   Update   titles     price       FALSE
dbo     judy   Grant   Update   titles     pub_id      FALSE
dbo     judy   Grant   Update   titles     pubdate     FALSE
dbo     judy   Grant   Update   titles     title       FALSE
dbo     judy   Grant   Update   titles     title_id    FALSE
dbo     judy   Grant   Update   titles     total_sales FALSE
dbo     judy   Grant   Update   titles     type        FALSE
```

La première ligne du résultat indique que le propriétaire de la base de données ("dbo") a donné à Judy le droit de sélectionner toutes les colonnes de la table titles. Les lignes suivantes montrent que Judy ne peut mettre à jour que les colonnes répertoriées. Judy n'a pas la possibilité d'octroyer le droit select ou update à quiconque.

Pour voir les autorisations de Judy sur la table publishers, entrez :

```
sp_helprotect publishers, judy
```

Dans le résultat ci-dessous, la colonne grantable indique TRUE, ce qui signifie que Judy peut transmettre ses droits à d'autres utilisateurs.

```
grantor grantee type   action   object     column      grantable
------- ------ -----   ------   ------     ------      -------
dbo     judy   Grant   Select   publishers all         TRUE
```

## Rapport sur les autorisations sur des tables spécifiques

Utilisez sp_table_privileges pour obtenir des informations relatives aux autorisations accordées sur une table spécifiée. La syntaxe est la suivante :

```
sp_table_privileges nom_table [, propriétaire_table
    [, qualificatif_table]]
```

où :

- *nom_table* représente le nom de la table. Ce paramètre est obligatoire.
- *propriétaire_table* sert à spécifier le nom du propriétaire de la table, s'il ne s'agit ni du DBO ni de l'utilisateur exécutant sp_table_privileges.
- *qualificatif_table* est le nom de la base de données courante.

Utilisez null pour les paramètres à ignorer.

Par exemple, l'instruction suivante :

```
sp_table_privileges titles
```

renvoie des informations sur toutes les autorisations octroyées sur la table titles. Pour une description détaillée du résultat de sp_table_privileges, consultez le document *Manuel de référence d'Adaptive Server*.

## Rapport sur les autorisations sur des colonnes spécifiques

Utilisez la procédure stockée catalogue sp_column_privileges pour connaître les autorisations définies sur les colonnes d'une table. La syntaxe est la suivante :

```
sp_column_privileges nom_table [, propriétaire_table
    [, qualificatif_table [, nom_colonne]]]
```

où :

- *nom_table* représente le nom de la table.
- *propriétaire_table* sert à spécifier le nom du propriétaire de la table, s'il ne s'agit ni du DBO ni de l'utilisateur exécutant sp_column_privileges.
- *qualificatif_table* est le nom de la base de données courante.
- *nom_colonne* est le nom de la colonne pour laquelle vous voulez obtenir des informations.

Utilisez null pour les paramètres à ignorer.

Par exemple, l'instruction suivante :

```
sp_column_privileges publishers, null, null, pub_id
```

renvoie des informations sur la colonne pub_id de la table publishers. Pour une description détaillée du résultat de sp_column_privileges, consultez le *Manuel de référence d'Adaptive Server*.

## Utilisation de vues et de procédures stockées comme mécanismes de sécurité

Les vues et les procédures stockées peuvent servir de mécanismes de sécurité. Il est ainsi possible de donner à des utilisateurs un accès contrôlé à des objets de base de données, sans qu'ils puissent accéder directement aux données. Par exemple, vous pouvez octroyer à un employé le droit execute sur une procédure qui met à jour des informations de coût dans une table projects sans permettre à cet utilisateur de voir les données confidentielles de la table. Pour tirer parti de cette fonctionnalité, vous devez être le propriétaire de la procédure ou de la vue et de ses objets sous-jacents. Si ces derniers ne vous appartiennent pas, les utilisateurs doivent avoir le droit d'accéder aux objets. Pour en savoir plus sur les conditions d'emploi des autorisations, reportez-vous à la section "Présentation des chaînes d'appartenance", page 469.

Adaptive Server effectue des vérifications d'autorisations en cas d'utilisation de la vue ou de la procédure. Lorsque vous créez la vue ou la procédure, Adaptive Server n'effectue aucune vérification sur les objets sous-jacents.

## Utilisation de vues comme mécanismes de sécurité

Par le biais d'une vue, les utilisateurs ne peuvent sélectionner et modifier que les données visibles. Le reste de la base de données n'est pas accessible.

L'autorisation d'accéder à la vue doit être explicitement octroyée ou révoquée, quelles que soient les autorisations en vigueur sur les tables sous-jacentes. Si la vue et ses tables sous-jacentes appartiennent au même propriétaire, il est inutile de donner des autorisations sur ces dernières. Les données d'une table sous-jacente qui ne sont pas incluses dans la vue sont transparentes pour les utilisateurs autorisés à accéder à la vue mais pas à la table.

En définissant différentes vues et en leur associant des autorisations sélectives, il est possible de limiter l'accès d'un utilisateur (ou d'une combinaison d'utilisateurs) à différents sous-ensembles de données. L'accès peut être restreint :

- A un sous-ensemble des lignes d'une table sous-jacente (sous-ensemble dépendant de la valeur). Par exemple, vous pouvez définir une vue qui ne contient que les lignes sur les ouvrages traitant de commerce et de psychologie, afin de cacher à certains utilisateurs les informations sur les autres types d'ouvrages.
- A un sous-ensemble des colonnes d'une table sous-jacente (sous-ensemble indépendant de la valeur). Par exemple, vous pouvez définir une vue qui contient toutes les lignes de la table titles, mais masque les colonnes price et advance, dont les données sont confidentielles.
- A un sous-ensemble de lignes et de colonnes d'une table sous-jacente.
- Aux lignes correspondant à une jointure de plusieurs tables sous-jacentes. Par exemple, vous pouvez définir une vue joignant les tables titles, authors et titleauthor. Cette vue masquerait les données personnelles sur les auteurs et les informations financières sur les ouvrages.
- A des informations statistiques sur les données d'une table sous-jacente. Par exemple, vous pouvez définir une vue ne contenant que le prix moyen de chaque type d'ouvrage.
- A un sous-ensemble d'une autre vue ou d'une quelconque combinaison de vues et de tables sous-jacentes.

Supposons que vous vouliez empêcher certains utilisateurs d'accéder aux colonnes de données financières de la table titles. Vous pourriez créer une vue de la table titles omettant ces colonnes. Ensuite, vous donneriez à tous les utilisateurs des droits sur la vue, mais seul le service commercial (Sales) aurait des droits sur la table.

```
grant all on bookview to public
grant all on titles to sales
```

Une méthode équivalente pour configurer ces privilèges sans recourir à une vue est d'exécuter les instructions suivantes :

```
grant all on titles to public
revoke select, update on titles (price, advance,
    total_sales)
from public
grant select, update on titles (price, advance,
    total_sales)
to sales
```

Cette seconde solution peut poser un problème si des utilisateurs n'appartenant pas au groupe sales entrent la commande :

```
select * from titles
```

En effet, ils verraient s'afficher un message contenant la phrase suivante :

```
permission denied
```

Adaptive Server convertit l'astérisque en une liste de toutes les colonnes de la table titles. Mais comme les autorisations sur certaines de ces colonnes ont été retirées aux utilisateurs non commerciaux, leur accès est refusé. Le message d'erreur répertorie toutes les colonnes auxquelles l'utilisateur n'a pas accès.

Pour pouvoir consulter les colonnes sur lesquelles ils ont des droits, les utilisateurs non commerciaux doivent les nommer de façon explicite. Pour cette raison, la création d'une vue dotée des autorisations appropriées constitue une meilleure solution.

Vous pouvez également utiliser des vues à des fins de **protection contextuelle**. Par exemple, vous pouvez créer une vue restreignant l'accès d'un opérateur de saisie aux lignes qu'il a ajoutées ou mises à jour. Pour ce faire, il faut ajouter dans une table une colonne dans laquelle, pour chaque ligne entrée, l'ID de l'utilisateur est automatiquement enregistré en tant que valeur par défaut. Vous pouvez définir cette valeur par défaut dans l'instruction create table, comme suit :

```
create table testtable
    (empid       int,
    startdate    datetime,
    username     varchar(30) default user)
```

Ensuite, définissez une vue incluant toutes les lignes de la table dans lesquelles uid représente l'utilisateur courant :

```
create view context_view
as
    select *
    from testtable
    where username = user_name()
with check option
```

Les lignes extractibles par le biais de cette vue dépendent de l'identité de la personne qui exécute la commande select. En ajoutant with check option à la définition de la vue, vous rendez impossible à quiconque la falsification des informations de la colonne username.

## Utilisation de procédures stockées comme mécanismes de sécurité

Si une procédure stockée et tous les objets sous-jacents appartiennent à la même personne, celle-ci peut octroyer aux utilisateurs le droit d'exécuter cette procédure sans leur donner accès aux objets sous-jacents. Par exemple, un utilisateur peut avoir l'autorisation d'utiliser une procédure stockée qui met à jour un sous-ensemble de lignes et de colonnes d'une table spécifique, même s'il n'a aucune autre autorisation sur cette table.

### Rôles et procédures stockées

Vous pouvez utiliser la commande grant execute pour octroyer des droits d'exécution d'une procédure stockée à tous les utilisateurs possédant un rôle spécifique. revoke execute permet de retirer ce droit. Cependant, l'autorisation grant execute *n'*empêche *pas* les utilisateurs dépourvus du rôle en question d'obtenir le droit d'exécution sur la procédure stockée.

Pour plus de sécurité, vous pouvez restreindre l'emploi d'une procédure stockée en y intégrant la fonction système proc_role, qui permet de vérifier si le rôle de l'utilisateur ayant lancé l'exécution est adéquat. proc_role renvoie 1 si elle détecte un rôle système ou utilisateur spécifique (sa_role, sso_role, oper_role ou tout rôle défini par l'utilisateur), et 0 dans le cas contraire. Exemple de procédure utilisant proc_role pour savoir si l'utilisateur est un administrateur système :

```
create proc test_proc
as
if (proc_role("sa_role") = 0)
begin
```

```
        print "You don't have the right role"
        return -1
    end
    else
        print "You have SA role"
        return 0
```

Pour plus d'informations sur proc_role, reportez-vous à "Fonctions système" dans le document Manuel de référence d'Adaptive Server.

## Présentation des chaînes d'appartenance

Les vues dépendent des autres vues et/ou des tables. Les procédures peuvent, elles aussi, dépendre d'autres procédures, vues et/ou tables. Toutes ces relations d'interdépendance sont considérées comme une *chaîne d'appartenance*.

En général, le propriétaire d'une vue détient également ses objets sous-jacents (les autres vues et tables), tandis que le propriétaire d'une procédure stockée détient tous les objets (procédures, tables et vues) auxquels elle fait référence.

Bien que cela ne soit pas obligatoire, une vue et ses objets sous-jacents se trouvent généralement tous dans la même base de données, au même titre qu'une procédure stockée et tous les objets qui y sont référencés. Si ce n'est pas le cas, tout utilisateur souhaitant utiliser la vue ou procédure stockée doit être dûment enregistré dans toutes les bases contenant les différents objets, ou doit faire partie des utilisateurs "guest" de ces bases. (Ce mécanisme empêche quiconque d'accéder à une base de données sans autorisation de la part du DBO.)

Lorsqu'une personne se sert d'une procédure ou d'une vue pour laquelle elle détient le droit execute, Adaptive Server ne vérifie pas les autorisations sur les objets sous-jacents :

- Si ces objets et la vue ou procédure appartiennent au même utilisateur, et
- si l'utilisateur accédant à la vue ou procédure est dûment enregistré dans toutes les bases de données contenant les objets sous-jacents, ou fait partie des utilisateurs "guest" de ces bases.

Dans le cas où les objets n'appartiennent pas tous à la même personne, Adaptive Server vérifie leurs autorisations lorsque la chaîne d'appartenance est interrompue. Par exemple, si l'objet A fait référence à l'objet B et que B n'appartient pas à la même personne que A, Adaptive Server vérifie les autorisations pour l'objet B. Ainsi, Adaptive Server permet au propriétaire des données d'origine de garder le contrôle des utilisateurs autorisés à y accéder.

En général, l'utilisateur qui crée une vue ne doit s'occuper que de définir les autorisations qui s'y rapportent. Supposons que Mary ait créé une vue appelée auview1 sur la table authors, qui lui appartient également. Si Mary octroie à Sue le droit select sur auview1, Adaptive Server permettra à Sue d'accéder à la vue sans vérifier les autorisations sur authors.

Il n'en va pas de même, cependant, pour l'utilisateur qui crée une vue ou une procédure stockée dépendant d'un objet qui appartient à une autre personne. Dans ce cas, les autorisations qu'il est possible d'octroyer dépendent de celles définies par cet autre propriétaire.

## Exemple de vues dans des chaînes d'appartenance

Supposons que Joe crée une vue appelée auview2, qui dépend de la vue auview1 de Mary. Joe octroie à Sue l'autorisation select sur auview2.

***Figure 11-2 : Chaînes d'appartenance et vérification des autorisations sur les vues, cas 1***

| Autorisation de Sue | Objet | Appartenance | Vérifications |
|---|---|---|---|
| **select** | ***auview2*** | **Joe** | **Sue n'est pas propriétaire**<br>**Autorisations vérifiées** |
| | ↓ | | |
| **select** | ***auview1*** | **Mary** | **Propriétaires différents**<br>**Autorisations vérifiées** |
| | ↓ | | |
| **Aucune** | ***authors*** | **Mary** | **Même propriétaire**<br>**Pas de vérification** |

Adaptive Server vérifie les autorisations sur auview2 et auview1, et constate que Sue a le droit de s'en servir. Adaptive Server contrôle l'appartenance sur auview1 et authors, et constate qu'elles ont le même propriétaire. Par conséquent, Sue peut utiliser auview2.

En approfondissant cet exemple, supposons que la vue de Joe, auview2, dépende de auview1, qui dépend elle-même d'authors. Mary apprécie la vue auview2 de Joe et décide de s'en servir pour créer auview3. auview1 et authors appartiennent tous deux à Mary.

La chaîne d'appartenance se présente comme suit :

***Figure 11-3 : Chaînes d'appartenance et vérification des autorisations sur les vues, cas 2***

| Autorisation de Sue | Objet | Appartenance | Vérifications |
|---|---|---|---|
| **select** | ***auview3*** | **Mary** | **Sue n'est pas propriétaire** |
| | ↓ | | **Autorisations vérifiées** |
| **select** | ***auview2*** | **Joe** | **Propriétaires différents** |
| | ↓ | | **Autorisations vérifiées** |
| **select** | ***auview1*** | **Mary** | **Propriétaires différents** |
| | ↓ | | **Autorisations vérifiées** |
| **Aucune** | ***authors*** | **Mary** | **Même propriétaire Pas de vérification** |

Lorsque Sue tente d'accéder à auview3, Adaptive Server vérifie les autorisations sur auview3, auview2 et auview1. Si Joe a octroyé des droits à Sue sur auview2 et que Mary lui a octroyé des droits sur auview3 et auview1, Adaptive Server autorise l'accès. Adaptive Server ne vérifie les droits que si l'objet placé juste avant la vue dans la chaîne a un propriétaire différent (ou s'il s'agit du premier objet de la chaîne). Par exemple, il contrôle auview2 car l'objet qui la précède (auview3) appartient à une autre personne. Il ne vérifie pas les autorisations sur authors, car l'objet qui en dépend directement (auview1) appartient au même utilisateur.

## Exemple de procédures dans des chaînes d'appartenance

Les procédures suivent les mêmes règles que les vues. Supposons que la chaîne d'appartenance se présente comme suit :

***Figure 11-4 : Chaînes d'appartenance et vérification des autorisations sur les procédures stockées***

| Autorisation de Sue | Objet | Appartenance | Vérifications |
|---|---|---|---|
| execute | *proc4* | Mary | Sue n'est pas propriétaire<br>Autorisations vérifiées |
| Aucune | *proc3* | Mary | Même propriétaire<br>Pas de vérification |
| execute | *proc2* | Joe | Propriétaires différents<br>Autorisations vérifiées |
| execute | *proc1* | Mary | Propriétaires différents<br>Autorisations vérifiées |
| Aucune | *authors* | Mary | Même propriétaire<br>Pas de vérification |

Pour exécuter proc4, Sue doit avoir le droit d'utiliser proc4, proc2 et proc1. L'autorisation d'exécuter proc3 n'est pas nécessaire, dans la mesure où proc3 et proc4 ont le même propriétaire.

Chaque fois que Sue utilise proc4, Adaptive Server vérifie ses autorisations sur la procédure (proc4) et sur tous les objets auxquels celle-ci fait référence. Adaptive Server sait quels objets il doit vérifier : il en a déterminé la liste lors de la première utilisation de proc4 par Sue, puis a enregistré ces informations avec le plan d'exécution de la procédure. A moins que l'un des objets référencés soit supprimé ou redéfini, Adaptive Server ne revient pas sur sa décision initiale concernant les objets à contrôler.

Ce type de hiérarchie permet au propriétaire de chaque objet de contrôler pleinement l'accès à ce dernier. Les propriétaires peuvent donc contrôler l'accès aux vues, aux procédures stockées, ainsi qu'aux tables.

## Autorisations sur les triggers

Un **trigger** est un type de procédure stockée spécial servant à appliquer des règles d'intégrité, notamment l'intégrité référentielle. Les triggers ne sont jamais exécutés directement, mais comme un effet secondaire de la modification d'une table. Vous ne pouvez pas octroyer (grant) ou révoquer (revoke) des autorisations sur des triggers.

Seul un propriétaire d'objet est habilité à créer un trigger. Cependant, la chaîne d'appartenance peut être interrompue si un trigger sur une table fait référence à des objets appartenant à différents utilisateurs. Les règles de hiérarchie de protection applicables aux procédures sont également valables pour les triggers.

Bien que les objets affectés par un trigger appartiennent généralement à l'utilisateur qui détient ce dernier, vous pouvez écrire un trigger qui modifie un objet appartenant à une autre personne. Dans ce cas, tout utilisateur modifiant votre objet de telle sorte que le trigger soit activé doit également avoir des droits sur l'autre objet.

Si Adaptive Server refuse d'exécuter une commande de modification de données car un trigger affecte un objet pour lequel l'utilisateur n'a pas les droits appropriés, la totalité de la transaction de modification est annulée.

Pour plus d'informations sur les triggers, consultez le *Guide de l'utilisateur Transact-SQL* ou le *Manuel de référence d'Adaptive Server*.

CHAPITRE 12

# Audit

Ce chapitre explique comment configurer l'audit de votre installation.

Les sujets traités dans ce chapitre sont les suivants :



## Présentation de l'audit dans Adaptive Server

La traçabilité des utilisateurs est un élément majeur de la sécurité d'un système. L'audit des événements sur le système constitue l'un des moyens de mettre en oeuvre cette traçabilité. Nombre des événements se produisant dans Adaptive Server peuvent être enregistrés.

L'audit constitue un aspect important de la sécurité dans un système de gestion de bases de données. Une trace d'audit permet de détecter toute intrusion et toute utilisation inappropriée des ressources. En examinant cette trace, un responsable de la sécurité du système (SSO) peut relever des profils d'accès à des objets de base de données et surveiller l'activité de certaines personnes. Les enregistrements d'audit permettent de remonter à des utilisateurs spécifiques et, par conséquent, de décourager quiconque tenterait d'utiliser le système de façon abusive.

Dans chaque enregistrement d'audit peuvent être consignés la nature de l'événement, la date et heure de son occurrence, l'utilisateur concerné et le succès ou l'échec de l'événement. Parmi les événements susceptibles d'être audités, citons : les connexions et déconnexions, les démarrages du serveur, l'utilisation des commandes d'accès aux données, les tentatives d'accès à certains objets et les actions d'un utilisateur particulier. La **trace d'audit**, ou journal des enregistrements d'audit, permet au SSO (System Security Officer) de reconstruire les événements qui ont eu lieu sur le système et d'évaluer leur impact.

Le responsable de la sécurité du système (SSO) est le seul utilisateur autorisé à lancer et à arrêter l'audit, à configurer ses options et à traiter les données générées. En tant que SSO, vous pouvez établir un audit pour des événements tels que :

- des événements liés à la sécurité au niveau serveur,
- la création, la suppression et la modification d'objets de base de données,
- toutes les actions réalisées par un utilisateur spécifique ou par des utilisateurs détenant un rôle particulier,
- l'octroi ou la révocation des accès aux bases de données,
- l'importation ou l'exportation de données,
- les connexions et les déconnexions.

## Corrélation d'Adaptive Server et des enregistrements d'audit du système d'exploitation

Le plus simple, pour établir une liaison entre les enregistrements d'audit d'Adaptive Server et ceux du système d'exploitation est de définir des noms de login pour Adaptive Server identiques aux noms de login du système d'exploitation.

Le SSO peut également définir une correspondance entre les noms de connexion des utilisateurs dans le système d'exploitation et leurs noms de connexion dans Adaptive Server. L'inconvénient de cette approche est qu'elle requiert une maintenance continue, les logins des nouveaux utilisateurs devant être enregistrés manuellement.

## Le système d'audit

Le système d'audit comprend les éléments suivants :

- la base de données sybsecurity qui contient les options d'audit globales et la trace d'audit ;
- la file d'attente d'audit en mémoire, dans laquelle les enregistrements d'audit sont envoyés avant d'être écrits dans la trace ;
- les paramètres de configuration permettant de gérer l'audit ;
- les procédures système permettant de gérer l'audit.

## Base de données *sybsecurity*

La base de données sybsecurity est créée au cours du processus d'installation de l'audit. En plus des tables système figurant dans la base de données model, elle contient sysauditoptions, une table système permettant de stocker la valeur des options d'audit valables sur le serveur, ainsi que des tables réservées à la trace d'audit.

sysauditoptions contient la valeur courante des options d'audit globales, telles que l'activation de l'audit pour les commandes de disque, les appels de procédure à distance, les enregistrements d'audit définis par l'utilisateur ad hoc, ou les événements relatifs à la sécurité. Ces options ont une incidence sur Adaptive Server dans son intégralité.

### Trace d'audit

Adaptive Server stocke la trace d'audit dans des tables système nommées sysaudits_01 à sysaudits_08. Lorsque vous installez l'audit, vous déterminez le nombre de tables nécessaires pour votre configuration. Par exemple, si vous décidez d'utiliser deux tables d'audit, elles porteront les noms sysaudits_01 et sysaudits_02. *Une seule* table d'audit est active (ou *courante*) à un moment précis.Toutes les données générées sont écrites dans la table d'audit courante par Adaptive Server. Un SSO peut exécuter sp_configure pour définir la table courante ou en changer.

Il est recommandé d'utiliser deux tables ou plus, chacune étant placée sur un device d'audit distinct. Ceci vous permet de configurer un processus d'audit fonctionnant sans incident, au cours duquel les tables sont archivées et traitées sans perte d'enregistrements ni intervention manuelle.

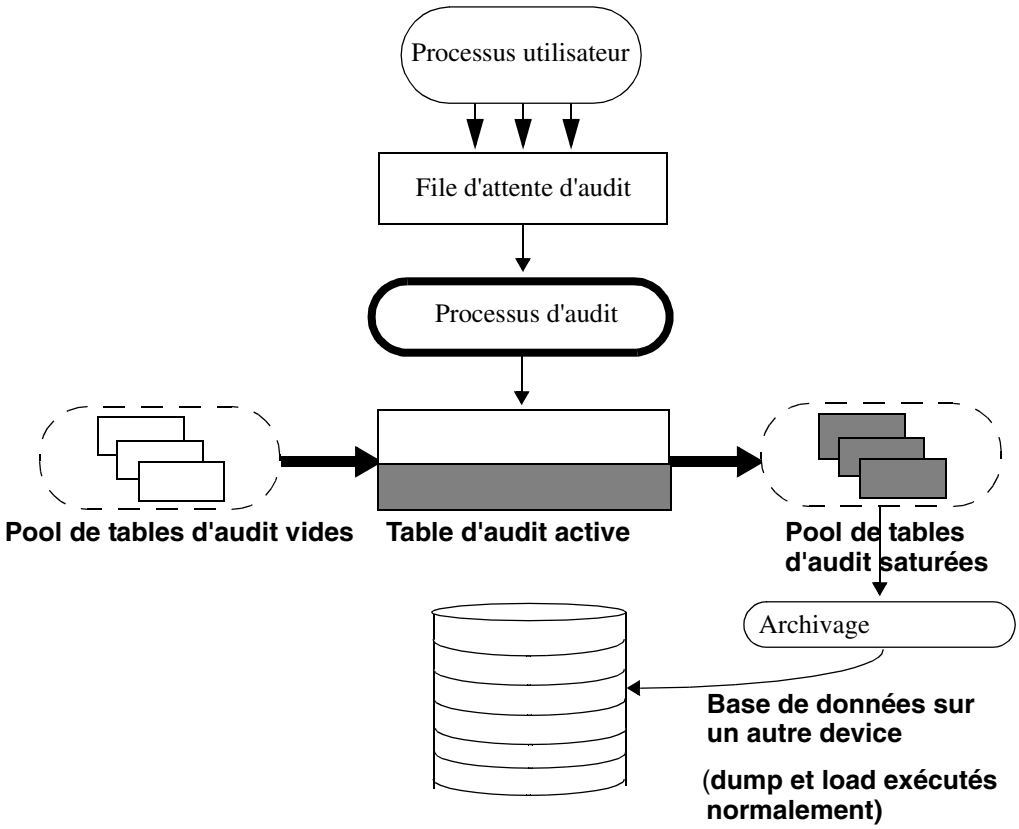
---

**Avertissement !** Sybase déconseille vivement d'utiliser une seule table d'audit sur les systèmes de production. Lorsqu'une seule table est utilisée, des enregistrements d'audit peuvent être perdus. Si vous ne pouvez pas faire autrement en raison de ressources système limitées, reportez-vous à la section "Audit à partir d'une seule table", page 494 pour obtenir des instructions.

---

La figure 12-1 montre comment le processus d'audit fonctionne avec plusieurs tables.

***Figure 12-1 : Audit avec plusieurs tables***




Le système d'audit écrit dans la table courante les enregistrements de la file d'attente d'audit en mémoire. Lorsque cette table est presque saturée, une procédure relative aux seuils peut archiver automatiquement son contenu dans une autre base de données. Il est possible de sauvegarder et de restaurer cette base d'archivage à l'aide des commandes dump et load. Pour plus d'informations sur la gestion de la trace d'audit, reportez-vous à "Configuration de l'audit pour gérer la trace d'audit", page 484.

## File d'attente d'audit

Lorsqu'un événement auditable se produit, l'enregistrement correspondant est d'abord envoyé dans la file d'attente d'audit. Cet enregistrement reste en mémoire jusqu'à ce qu'il soit écrit dans la trace d'audit par le processus. Vous pouvez configurer la taille de la file d'attente à l'aide du paramètre audit queue size de sp_configure.

Avant de définir cette taille, il est important de faire un compromis entre le risque de perdre les enregistrements de la file, si le système se bloque, et l'éventuelle dégradation des performances si cette file est saturée. En effet, tant qu'un enregistrement d'audit est stocké en mémoire, il peut être perdu en cas de blocage. Mais si la file d'attente sature de manière répétée, les performances de tout le système risquent d'en souffrir. Si la file d'attente d'audit est saturée quand un processus utilisateur tente de générer un enregistrement d'audit, le processus se met en veille jusqu'à ce que de la place soit libérée dans la file d'attente.

**Remarque** Les événements n'étant pas consignés directement dans la trace d'audit, vous ne pouvez pas compter sur le stockage immédiat d'un enregistrement d'audit dans la table d'audit courante.

## Paramètres de configuration d'audit

Pour gérer le processus d'audit, utilisez les paramètres de configuration suivants :

- auditing permet d'activer ou de désactiver l'audit dans l'ensemble d'Adaptive Server. Ce paramètre prend effet dès l'exécution de sp_configure. L'audit n'est lancé que si cette option est activée.
- audit queue size définit la taille de la file d'attente d'audit. Ce paramètre affectant l'allocation de mémoire, il ne prend effet qu'au redémarrage d'Adaptive Server.
- suspend audit when device full détermine le comportement du processus d'audit lorsqu'un device est saturé. Ce paramètre prend effet dès l'exécution de sp_configure.
- current audit table définit la table d'audit courante. Ce paramètre prend effet dès l'exécution de sp_configure.

## Procédures système utilisées pour l'audit

Pour gérer le processus d'audit, utilisez ces procédures système :

- sp_audit permet d'activer et de désactiver les options d'audit. Il s'agit de la seule procédure système nécessaire pour définir les événements à auditer.
- sp_displayaudit affiche les options d'audit actives.

- sp_addauditrecord permet d'ajouter dans la trace d'audit des enregistrements (ou commentaires) définis par l'utilisateur. Les utilisateurs ne peuvent ajouter ce type d'enregistrement que si le SSO a activé un audit ad hoc à l'aide de sp_audit.

# Installation et configuration de l'audit

Le tableau 12-1 présente la procédure générale à suivre pour configurer les systèmes d'audit.

***Tableau 12-1 : Procédure générale d'audit***

| Action | Description | Voir |
|---|---|---|
| 1. Mise en place de l'audit | La mise en place de l'audit implique de définir le nombre de tables d'audit et d'affecter des devices à la trace d'audit et au journal de transactions syslogs de la base de données sybsecurity. | "Installation du système d'audit", page 481 et les manuels d'installation et de configuration d'Adaptive Server |
| 2. Configuration de l'audit pour gérer la trace d'audit. | Création et mise en œuvre d'une procédure relative aux seuils qui sera appelée lorsque la table d'audit arrive à saturation. Cette procédure bascule automatiquement sur une nouvelle table d'audit et archive le contenu de la table courante.<br>Cette étape implique, en outre, de définir les paramètres de configuration audit queue size et suspend audit when device full. | "Configuration de l'audit pour gérer la trace d'audit", page 484<br>Pour l'audit d'une seule table, voir "Audit à partir d'une seule table", page 494 |
| 3. Configuration de la gestion du journal de transaction dans la base de données sybsecurity. | Choix du mode de gestion du journal de transactions syslogs de la base sybsecurity. Cette tâche comprend la définition de l'option trunc log on chkpt, ainsi que la mise en œuvre d'une procédure de seuil ultime pour syslogs au cas où trunc log on chkpt est désactivé. | "Définition de la gestion du journal de transactions", page 491 |
| 4. Définition des options d'audit. | Utilisation de sp_audit pour définir les événements à auditer. | "Définition des options d'audit globales", page 499 |
| 5. Activation de l'audit | Activation du paramètre de configuration auditing à l'aide de sp_configure. Adaptive Server commence à enregistrer les événements audités dans la table d'audit courante. | "Activation et désactivation de l'audit", page 493. |

## Installation du système d'audit

Le système d'audit est généralement installé à l'aide d'auditinit, le programme d'installation de Sybase. Il est également possible d'installer l'audit sans recourir à auditinit. Pour plus de détails, reportez-vous à la section "Installation de l'audit avec installsecurity", page 481. Pour plus d'informations sur l'installation et sur auditinit, consultez les manuels d'installation et de configuration d'Adaptive Server relatifs à votre plate-forme.

Lorsque vous installez l'audit, vous pouvez définir le nombre de tables système à utiliser pour la trace d'audit, le device sur lequel sera placée chaque table et le device du journal de transaction syslogs.

### Tables et devices destinés à la trace d'audit

Vous pouvez spécifier jusqu'à huit tables systèmes (sysaudits_01 à sysaudits_08). Prévoyez au moins deux tables pour la trace d'audit. Placez chaque table sur son propre device, différent du device master. Dans ce cas, vous pouvez utiliser une procédure relative aux seuils afin d'archiver automatiquement la table d'audit courante avant saturation puis basculer sur une nouvelle table vide pour les enregistrements suivants.

### Device destiné à la table *syslogs* du journal de transactions

Lors de l'installation de l'audit, vous devez spécifier un device distinct pour le journal de transactions, qui est constitué de la table système syslogs. Cette table syslogs existe dans chaque base de données et comporte un journal des transactions qui y sont effectuées.

### Installation de l'audit avec *installsecurity*

Le répertoire *$SYBASE/scripts* contient le script d'installation de l'audit installsecurity.

---

**Remarque** Cet exemple suppose un serveur dont la page possède une page logique de 2 ko.

---

Pour utiliser installsecurity :

1 Créez les devices et la base de données d'audit à l'aide des commandes Transact-SQL disk init et create database. Exemple :

```
disk init name = "auditdev",
    physname = "/dev/dsk/c2d0s4",
     size = "10"
disk init name = "auditlogdev",
    physname = "/dev/dsk/c2d0s5",
    size = "2M"
create database sybsecurity on auditdev
    log on auditlogdev
```

2 Utilisez isql pour exécuter le script installsecurity :

```
cd $SYBASE/scripts
setenv DSQUERY nom_serveur
isql -Usa -Pmot de passe -Snom_serveur <
installsecurity
```

3 Arrêtez Adaptive Server, puis redémarrez-le.

Une fois ces opérations effectuées, la base sybsecurity comporte une seule table (sysaudits_01) créée sur son propre segment. Vous pouvez d'ores et déjà activer l'audit, mais il est recommandé d'ajouter d'autres tables à l'aide de sp_addaudittable. Pour obtenir des informations sur disk init, create database et sp_addaudittable, consultez le Manuel de référence d'Adaptive Server.

## Déplacement de la base d'audit sur plusieurs devices

Placez la base de données sybsecurity sur son propre device, distinct de celui de la base master. Si vous utilisez plusieurs tables d'audit, chacune doit également être placée sur son propre device. Il peut également s'avérer utile de placer chaque table sur un segment distinct pointant vers un autre device. Si votre base sybsecurity est installée sur le même device que master, ou si vous voulez la déplacer sur un autre device, utilisez l'une des procédures décrites dans les sections suivantes. Lors du déplacement de la base, vous pouvez spécifier de conserver ou non vos paramètres d'audit globaux.

#### Déplacement de *sybsecurity* sans conserver les paramètres d'audit globaux

Pour déplacer la base sybsecurity sans sauvegarder les paramètres d'audit globaux :

1 Supprimez la base sybsecurity.

2 Réinstallez sybsecurity en suivant la procédure décrite dans :

- le guide de configuration de votre plate-forme.
- "Installation de l'audit avec installsecurity", page 481.

3 Au cours du processus d'installation, assurez-vous de placer la base sybsecurity sur un ou plusieurs devices distincts du device master.

#### Déplacement de *sybsecurity* sans conserver les paramètres d'audit globaux

Pour déplacer la base sybsecurity et sauvegarder les paramètres d'audit globaux :

1 Sauvegardez la base sybsecurity.

```
dump database sybsecurity to "/remote/sec_file"
```

2 Supprimez la base sybsecurity.

```
database sybsecurity
```

3 Initialisez le premier device sur lequel vous voulez placer la base sybsecurity.

```
disk init name = "auditdev",
    physname = "/dev/dsk/c2d0s4",
    size = "10M"
```

4 Initialisez le device dans lequel vous voulez placer le journal de sécurité.

```
disk init name = "auditlogdev",
    physname = "/dev/dsk/c2d0s5",
    size = "2M"
```

5 Créez la nouvelle base sybsecurity.

```
create database sybsecurity on auditdev
    log on auditlogdev
```

6 Chargez le contenu de l'ancienne base sybsecurity dans la nouvelle base. Les paramètres d'audit globaux sont préservés.

```
load database sybsecurity from
"/remote/sec_file"
```

7 Lancez online database, qui mettra à niveau sysaudits et sysauditoptions si nécessaire.

```
online database sybsecurity
```

8 Chargez les procédures du système d'audit comme décrit dans le Manuel de configuration pour votre plate-forme.

Pour créer plusieurs tables sysaudits dans sybsecurity :

1 Initialisez le device dans lequel vous voulez placer la table supplémentaire.

```
disk init name = "auditdev2",
    physname = "/dev/dsk/c2d0s6",
    size = "10M"
```

2 Etendez sybsecurity sur le device initialisé à l'étape 1.

```
alter database sybsecurity on auditdev2 = "2M"
```

3 Lancez sp_addaudittable pour créer la nouvelle table sysaudits sur le device initialisé à l'étape 1.

```
sp_addaudittable auditdev2
```

4 Répétez les étapes 1 à 3 pour chaque table sysaudits.

## Configuration de l'audit pour gérer la trace d'audit

Pour gérer la trace d'audit de façon efficace :

1 Assurez-vous que le système d'audit est installé avec deux tables ou plus, chacune étant placée sur un device distinct. Si ce n'est pas le cas, il est conseillé d'ajouter de nouvelles tables d'audit (avec leur device).

2 Ecrivez une procédure relative aux seuils, puis associez-la à chaque segment de table d'audit.

3 Définissez des paramètres de configuration pour la taille de la file d'attente d'audit et en indiquant l'action à effectuer si la table d'audit courante arrive à saturation.

Les sections suivantes présument que l'audit est installé avec plusieurs tables placées sur des devices distincts. Si vous ne disposez que d'un seul device pour ces tables, passez directement à la section "Audit à partir d'une seule table", page 494.

## Des procédures relatives aux seuils

Avant d'activer l'audit, créez une procédure relative aux seuils qui basculera automatiquement sur une nouvelle table d'audit lorsque la table courante est saturée.

La procédure relative aux seuils rattachée aux segments de device d'audit doit effectuer les opérations suivantes :

- activation de la prochaine table d'audit vide à l'aide de sp_configure ;
- archivage de la table d'audit presque saturée à l'aide des commandes insert et select.

### Changement de table d'audit courante

Le paramètre de configuration current audit table définit la table dans laquelle Adaptive Server écrit des lignes d'audit. En tant que responsable de la sécurité du système (SSO), vous pouvez changer de table d'audit courante à l'aide de sp_configure.

```
sp_configure "current audit table", n
  [, "with truncate"]
```

où n est un nombre entier indiquant le numéro de la nouvelle table d'audit courante. Valeurs de *n* admises :

- 1 représente sysaudits_01, 2 représente sysaudits_01, etc.
- 0 indique à Adaptive Server d'activer automatiquement la table qui suit la table d'audit courante. Par exemple, si votre installation comporte trois tables d'audit (sysaudits_01, sysaudits_02, et sysaudits_03), Adaptive Server active la table dont le numéro est :
  - 2 si la table courante est sysaudits_01
  - 3 si la table courante est sysaudits_02
  - 1 si la table courante est sysaudits_03

L'option with truncate précise qu'Adaptive Server doit tronquer la nouvelle table si elle n'est pas vide. Si cette option est omise et que la table n'est pas vide, sp_configure échoue.

---

**Remarque** Si Adaptive Server tronque la table d'audit courante alors que ses données n'ont pas été archivées, tous les enregistrements d'audit qu'elle contenait sont perdus. Avant d'utiliser l'option with truncate, archivez les données d'audit.

---

Pour exécuter sp_configure afin de changer de table d'audit courante, votre rôle actif doit être sso_role. Vous pouvez écrire une procédure relative aux seuils qui réalise cette opération automatiquement.

### Archivage de la table d'audit

Pour copier les données d'audit dans une table existante qui comporte les mêmes colonnes que les tables d'audit de sybsecurity, vous pouvez utiliser la commande insert avec select.

Assurez-vous que la procédure relative aux seuils copie avec succès les données de la table d'archivage dans une autre base :

1 Créez la base d'archivage sur un device distinct de celui contenant les tables d'audit de sybsecurity.

2 Créez une table d'archivage comportant les mêmes colonnes que les tables d'audit de sybsecurity. Pour ce faire, vous pouvez utiliser select into avec une condition fausse dans la clause where afin de générer une table vide. Exemple :

```
use aud_db
go
select *
  into audit_data
  from sybsecurity.dbo.sysaudits_01
  where 1 = 2
```

La condition where étant toujours fausse, cette requête crée une table vide ayant la même structure que sysaudits_01.

Avant que vous puissiez utiliser select into, l'option select into/bulk copy doit être activée dans la base d'archivage à l'aide de sp_dboption.

La procédure relative aux seuils peut utiliser insert et select, après avoir exécuté sp_configure pour changer de table d'audit, afin de copier des données dans la table de la base d'archivage. Pour ce faire, elle exécutera des commandes telles que :

```
insert aud_db.sso_user.audit_data
select * from sybsecurity.dbo.sysaudits_01
```

#### Exemple de procédure relative aux seuils pour des segments d'audit

L'exemple de procédure relative aux seuils ci-après présume que trois tables ont été configurées pour l'audit :

```
declare @audit_table_number int
/*
** Select the value of the current audit table
*/
select @audit_table_number = scc.value
from master.dbo.syscurconfigs scc, master.dbo.sysconfigures sc
where sc.config=scc.config and sc.name  = "current audit table"
/*
** Set the next audit table to be current.
** When the next audit table is specified as 0,
** the value is automatically set to the next one.
*/
exec sp_configure "current audit table", 0, "with truncate"
/*
** Copy the audit records from the audit table
** that became full into another table.
*/
if @audit_table_number = 1
    begin
        insert aud_db.sso_user.sysaudits
            select * from sysaudits_01
        truncate table sysaudits_01
    end
else if @audit_table_number = 2
    begin
        insert aud_db.sso_user.sysaudits
            select * from sysaudits_02
        truncate table sysaudits_02
    end
return(0)
```

#### Rattachement de la procédure relative aux seuils à chaque segment d'audit

Pour rattacher la procédure relative aux seuils à chaque segment de table d'audit, utilisez sp_addthreshold.

Avant d'exécuter sp_addthreshold :

- déterminez le nombre de tables d'audit configuré pour votre installation, ainsi que le nom du segment de device de chaque table ;
- assurez-vous que vous disposez des autorisations et des rôles requis pour sp_addthreshold pour toutes les commandes de la procédure relative aux seuils.

**Avertissement !** sp_addthreshold et sp_modifythreshold contrôlent que seul un utilisateur détenant le rôle sa_role octroyé directement est autorisé à ajouter ou à modifier un seuil. Tous les rôles système actifs lorsque vous définissez un seuil sont insérés dans la table systhresholds en tant que rôles valables pour votre login. Cependant, seuls les rôles octroyés directement sont activés lorsque la procédure relative aux seuils est déclenchée.

### Tables d'audit et leur segment

Lorsque vous mettez en place le système d'audit, auditinit affiche le nom de chaque table d'audit et celui de son segment. Les noms de segment sont "aud_seg1" pour sysaudits_01, "aud_seg2" pour sysaudits_02 et ainsi de suite. Pour afficher des informations sur les segments de la base sybsecurity, exécutez sp_helpsegment après avoir activé sybsecurity. Pour connaître le nombre de tables d'audit défini pour votre installation, exécutez les commandes SQL suivantes :

```
use sybsecurity
go
select count(*) from sysobjects
  where name like "sysaudit%"
go
```

En outre, vous pouvez obtenir des informations sur les tables d'audit et sur la base sybsecurity en exécutant les commandes SQL ci-après :

```
sp_helpdb sybsecurity
go
use sybsecurity
go
sp_help sysaudits_01
go
sp_help sysaudits_02
go
  ...
```

#### Rôles et autorisations requis

Pour pouvoir utiliser sp_addthreshold, vous devez être soit le Propriétaire de la base de données (DBO), soit un Administrateur Système (SA). La base sybsecurity appartenant en général à un SSO, il a également le droit d'exécuter sp_addthreshold. En plus de ce droit, vous devez être autorisé à exécuter toutes les commandes de votre procédure relative aux seuils. Par exemple, pour définir current audit table à l'aide de sp_configure, le rôle sso_role doit être actif. Lorsque la procédure est déclenchée, Adaptive Server tente d'activer tous les rôles et autorisations en vigueur lorsque vous avez lancé sp_addthreshold.

Pour rattacher la procédure relative aux seuils audit_thresh à trois segments de device :

```
use sybsecurity
go
sp_addthreshold sybsecurity, aud_seg_01, 250, audit_thresh
sp_addthreshold sybsecurity, aud_seg_02, 250, audit_thresh
sp_addthreshold sybsecurity, aud_seg_03, 250, audit_thresh
go
```

La procédure exemple audit_thresh est déclenchée lorsqu'il reste moins de 250 pages disponibles dans la table d'audit courante.

Pour plus d'informations sur l'ajout de procédures relatives aux seuils, consultez le chapitre 29, "Gestion de l'espace libre avec des seuils".

#### Audit réalisé à l'aide de la procédure exemple

Une fois l'audit activé, toutes les données générées sont écrites par Adaptive Server dans sysaudits_01, la table d'audit courante initiale. Lorsque sysaudits_01 se trouve à 250 pages de la saturation, la procédure relative aux seuils audit_thresh se déclenche. Immédiatement après, Adaptive Server commence à écrire les nouveaux enregistrements d'audit dans sysaudits_02. La procédure copie également toutes les données de sysaudits_01 dans la table d'archivage audit_data de la base audit_db. La rotation des tables d'audit continue ainsi sans intervention manuelle.

## Définition des paramètres de configuration de l'audit

Pour votre installation d'audit, définissez les paramètres de configuration suivants :

- audit queue size détermine le nombre d'enregistrements que contient la file d'attente d'audit en mémoire.

- suspend audit when device full détermine le comportement d'Adaptive Server si la table d'audit courante est complètement saturée. La condition "full" (saturation) ne se produit que si la procédure relative aux seuils rattachée au segment de la table courante ne fonctionne pas correctement.

#### Définition de la taille de la file d'attente d'audit

Un enregistrement d'audit occupe 424 octets en mémoire. Par défaut, la file d'attente d'audit peut contenir 100 enregistrements, ce qui nécessite environ 42 ko.

Pour fixer la taille de la file d'attente, utilisez sp_configure. Respectez la syntaxe suivante :

```
sp_configure "audit queue size", [valeur]
```

valeur est le nombre d'enregistrements que la file d'attente d'audit peut contenir. Valeur minimale : 1, valeur maximale : 65 535. Par exemple, pour définir une taille de file d'attente d'audit de 300, exécutez :

```
sp_configure "audit queue size", 300
```

Pour plus d'informations sur la définition de cette taille et d'autres paramètres de configuration, consultez le chapitre 5, "Définition des paramètres de configuration".

#### Suspension de l'audit en cas de saturation des devices

Si vous utilisez plusieurs tables d'audit (chacune étant placée sur un device distinct du device master) et avez créé une procédure relative aux seuils pour chaque segment de table, les devices d'audit ne devraient jamais être saturés. La condition "full" (saturation) ne se produit que si votre procédure ne fonctionne pas correctement. Pour déterminer l'action à effectuer dans ce cas, définissez le paramètre suspend audit when device full à l'aide de sp_configure. Options possibles :

- Suspendre le processus d'audit et tous les processus utilisateur susceptibles de générer un événement auditable. Relancer le fonctionnement normal dès qu'un SSO a tronqué la table d'audit courante.
- Tronquer la table d'audit suivante, puis l'activer. Cela permet au système de fonctionner normalement, sans aucune intervention de la part d'un SSO.

Pour définir ce paramètre de configuration, utilisez sp_configure. Votre rôle actif doit être sso_role. Respectez la syntaxe suivante :

```
sp_configure "suspend audit when device full",
    [0|1]
```

0 tronque la table d'audit suivante et l'active dès que la table d'audit courante arrive à saturation. En définissant la valeur 0, le processus d'audit ne sera jamais suspendu ; cependant, les anciens enregistrements d'audit risquent d'être perdus s'ils n'ont pas été archivés.

1 (valeur par defaut) suspend le processus d'audit et tous les processus utilisateur susceptibles de générer un événement auditable. Pour relancer le fonctionnement normal, le SSO doit se connecter et activer une table vide comme table d'audit courante. Au cours de cette période, les actions du SSO sont exemptées d'audit. Si elles devaient générer des enregistrements d'audit en fonctionnement normal, Adaptive Server enverrait dans le journal d'erreurs un message d'erreur et des informations sur l'événement.

Si vous avez créé une procédure relative aux seuils rattachée aux segmentsde table d'audit, définissez suspend audit when device full à 1 (on). Avec la valeur 0 (off), Adaptive Server est susceptible de tronquer la table d'audit saturée avant même que la procédure ait la possibilité d'archiver vos enregistrements d'audit.

## Définition de la gestion du journal de transactions

Cette section donne des indications sur la gestion du journal de transactions dans sybsecurity.

Si l'option trunc log on chkpt est activée, Adaptive Server tronque syslogs chaque fois qu'il exécute un checkpoint automatique. Une fois l'audit installé, la valeur de trunc log on chkpt est on, mais vous pouvez utiliser sp_dboption pour la modifier.

## Troncature du journal de transactions

Si vous activez l'option trunc log on chkpt pour la base de données sybsecurity, vous n'avez pas à vous soucier de l'éventuelle saturation du journal de transactions. En effet, Adaptive Server tronque le journal chaque fois qu'il exécute un point de reprise. L'activation de cette option ne vous permet pas d'utiliser dump transaction pour sauvegarder le journal de transactions mais vous pouvez utiliser dump database pour sauvegarder la base de données.

Si vous suivez les indications fournies dans la section "Des procédures relatives aux seuils", page 485, les tables d'audit sont automatiquement archivées dans les tables d'une autre base. Vous pouvez vous servir de procédures de sauvegarde et de restauration standard pour cette base d'archivage.

Si un incident se produit sur le device sybsecurity, vous pouvez restaurer la base et relancer l'audit. Au pire, seuls les enregistrements placés dans la file d'attente en mémoire et dans la table d'audit courante sont perdus, car la base d'archivage contient toutes les autres données d'audit. Après le rechargement, utilisez sp_configure with truncate pour définir et tronquer la table d'audit courante.

Si vous n'avez modifié aucune option d'audit globale depuis la sauvegarde de la base, toutes les options stockées dans sysauditoptions sont automatiquement restaurées lors du rechargement de sybsecurity. Dans le cas contraire, vous pouvez exécuter un script définissant les options avant de relancer l'audit.

## Gestion du journal de transactions sans troncature

Si vous utilisez db_option pour désactiver trunc log on chkpt, il est possible que le journal de transactions arrive à saturation. Aussi, prévoyez de rattacher une *procédure* de *seuil ultime* au segment du journal. Elle sera appelée dès que l'espace libre restant sur le segment est inférieur à un seuil calculé automatiquement par Adaptive Server. Ce seuil est une estimation du nombre des pages disponibles nécessaires pour sauvegarder le journal de transactions.

Par défaut, le nom de la procédure de seuil ultime est sp_thresholdaction, mais vous pouvez le changer avec sp_modifythreshold, tant que vous détenez le rôle sa_role (actif).

**Remarque** sp_modifythreshold vérifie que votre rôle actif est "sa_role". Pour plus d'informations, reportez-vous à la section "Rattachement de la procédure relative aux seuils à chaque segment d'audit", page 487.

Adaptive Server ne fournit aucune procédure de seuil ultime par défaut, mais le chapitre 29, "Gestion de l'espace libre avec des seuils" en contient plusieurs exemples. Votre procédure doit exécuter la commande dump transaction, qui tronque le journal. Lorsque le journal de transactions atteint le seuil ultime défini, toutes les transactions en cours sont suspendues jusqu'à ce que de la place se libère. Cette suspension se produit dans la mesure où l'option abort xact when log is full est toujours fixée à FALSE pour la base sybsecurity. Vous ne pouvez pas modifier cette valeur.

Si l'option trunc log on chkpt est désactivée (off), vous pouvez vous servir de procédures de sauvegarde et de restauration standards pour sybsecurity. Notez cependant que, en cas de panne de device, les tables d'audit de la base restaurée risquent de ne pas correspondre à leur état.

## Activation et désactivation de l'audit

Pour activer ou désactiver l'audit, définissez le paramètre de configuration auditing à l'aide de sp_configure. Respectez la syntaxe suivante :

```
sp_configure "auditing", [0 | 1 ]
```

1 active l'audit. 0 désactive l'audit. Par exemple, pour mettre en œuvre l'audit, entrez :

```
sp_configure "auditing", 1
```

**Remarque** Lorsque vous activez ou désactivez l'audit, Adaptive Server génère automatiquement un enregistrement d'audit. Reportez-vous aux codes d'événement 73 et 74 dans le tableau 12-6, page 511.

## Audit à partir d'une seule table

Sybase conseille vivement de ne *pas* configurer d'audit avec une seule table sur les systèmes de production. Si vous n'utilisez qu'une seule table, les enregistrements d'audit entrants sont perdus pendant la durée nécessaire à l'archivage des données d'audit et la troncature de la table d'audit. Il n'existe aucun moyen d'éviter cela avec une seule table d'audit.

Si vous n'utilisez qu'une seule table, elle risque d'être rapidement saturée. Les conséquences de cette saturation dépendent de la configuration de l'option suspend audit when device full. Si vous avez activé l'option suspend audit when device full, le processus d'audit est suspendu, de même que tous les processus utilisateur susceptibles de générer des événements auditables. Si l'option suspend audit when device full est désactivée, la table d'audit est tronquée et vous perdez les enregistrements d'audit qui s'y trouvaient.

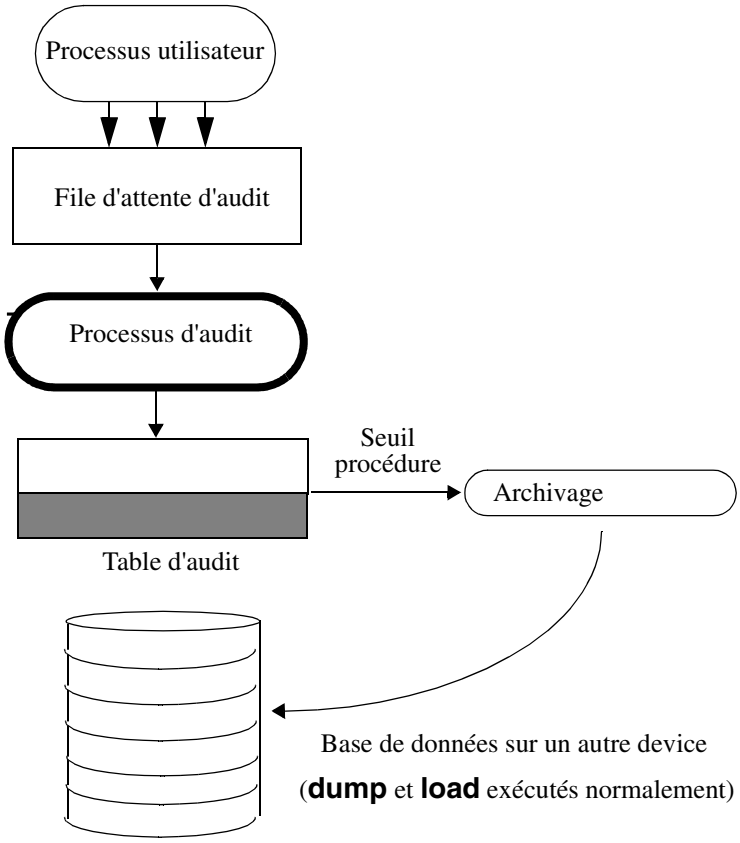
Sur un système *non productif*, lorsque la perte de quelques enregistrements d'audit ne porte pas à conséquence, vous pouvez vous contenter d'une seule table d'audit si vous ne disposez pas de suffisamment d'espace disque ou de devices disponibles.

Utiliser une seule ou plusieurs tables d'audit est similaire, à ceci près que :

- pendant l'installation, vous ne spécifiez qu'une table système pour le processus d'audit ;
- pendant l'installation, vous ne spécifiez qu'un seul device pour la table système d'audit ;
- la procédure associée au seuil que vous créez pour archiver les enregistrements d'audit est différente.

La figure 12-2 décrit le fonctionnement du processus d'audit avec une seule table.

***Figure 12-2 : Audit avec une seule table***



## Définition et gestion de l'audit avec une seule table

Le tableau 12-2 présente la procédure de gestion du processus d'audit avec une seule table.

***Tableau 12-2 : Processus d'audit avec une seule table***

| Action | Description | Voir |
|---|---|---|
| 1. Mise en place de l'audit | La mise en place de l'audit implique de définir le nombre de tables d'audit et d'affecter des devices à la trace d'audit et au journal de transactions syslogs de la base de données sybsecurity. | Le Guide d'installation pour votre plate-forme. |
| 2. Configuration de l'audit pour gérer la trace d'audit. | Création et mise en œuvre d'une procédure relative aux seuils qui sera appelée lorsque la table d'audit arrive à saturation. Cette procédure bascule automatiquement sur une nouvelle table d'audit, puis tronque la table d'audit.<br>Cette étape implique, en outre, de définir les paramètres de configuration audit queue size et suspend audit when device full. | "Définition et gestion de l'audit avec une seule table", page 496.<br>"Processus d'audit avec une seule table", page 497. |
| 3. Configuration de l'audit pour gérer le journal de transactions syslogs de la base de données sybsecurity. | Choix du mode de gestion du journal de transactions syslogs de la base sybsecurity. Cette tâche comprend la définition de l'option trunc log on chkpt, ainsi que la mise en œuvre d'une procédure de seuil ultime pour syslogs au cas où cette option est désactivée (off). | "Définition de la gestion du journal de transactions", page 491. |
| 4. Définition des options d'audit. | Utilisation de sp_audit pour définir les événements à auditer.<br>**Remarque** Aucun enregistrement n'est généré tant que l'audit n'est pas démarré à l'aide de sp_configure. | "Définition des options d'audit globales", page 499. |
| 5. Activation de l'audit | Activation du paramètre de configuration auditing à l'aide de sp_configure. Adaptive Server commence à enregistrer les événements audités dans la table d'audit courante. | "Activation et désactivation de l'audit", page 493. |

## Processus d'audit avec une seule table

Pour un audit avec une seule table, la procédure associée au seuil doit :

- archiver la table d'audit qui arrive à saturation dans une autre table, à l'aide des commandes insert et select.
- tronquer la table d'audit pour libérer de l'espace pour les nouveaux enregistrements d'audit, à l'aide de la commande truncate table.

Pour archiver les enregistrements d'audit, vous devez créer une table d'archive dotée du même nombre de colonnes que la table d'audit. Cette table créée, votre procédure associée au seuil peut utiliser insert avec select pour copier les enregistrements dans la table d'archive.

Voici un exemple de procédure associée au seuil dans le cas d'un audit avec table seule :

```
create procedure audit_thresh as
/*
** Copy the audit records from the audit table
** the archive table
*/
insert aud_db.sso_user.audit_data
    select * from sysaudits_01
return(0)
go
/*
** truncate the audit table to make room for new
** audit records
*/
truncate table "sysaudits_01"
go
```

Une fois que vous avez créé la procédure, vous devez la rattacher au segment de la table d'audit. Pour les instructions, reportez-vous à la section "Rattachement de la procédure relative aux seuils à chaque segment d'audit", page 487.

---

**Avertissement !** Sur un système multiprocesseur, la table d'audit peut arriver à saturation même s'il existe une procédure associée au seuil qui se déclenche avant la saturation. Par exemple, si la procédure associée au seuil est exécutée sur une CPU soumise à une forte charge, et qu'un processus utilisateur exécutant des événements auditables est en cours sur une CPU moins chargée, il se peut que la table d'audit soit saturée avant que la procédure associée au seuil se déclenche. Le paramètre de configuration suspend audit when device full détermine ce qui se passe lorsque la table d'audit est saturée. Pour en savoir plus sur ce paramètre, reportez-vous à la section "Suspension de l'audit en cas de saturation des devices", page 490.

---

## Lorsque la table d'audit courante est saturée

Lorsque la table d'audit courante est saturée :

1 Le processus d'audit tente d'insérer l'enregistrement d'audit suivant dans la table. La tentative échouant, le processus d'audit est interrompu. Un message d'erreur est consigné dans le journal d'erreurs.

2 Si un utilisateur tente d'exécuter un événement auditable, il n'y parvient pas car l'audit ne peut être effectué. Le processus utilisateur est interrompu. Les utilisateurs qui ne tentent pas d'exécuter un événement auditable ne sont pas concernés.

3 Si l'audit des connexions est activé, personne à l'exception du SSO ne peut se connecter au serveur.

4 Si vous auditez des commandes exécutées avec le rôle sso_role actif, le SSO sera dans l'incapacité d'exécuter les commandes.

## Reprise lorsque la table d'audit courante est saturée

Si le device et la file d'attente d'audit courants sont saturés, le SSO est dispensé d'audit. Tout événement auditable exécuté par le SSO à partir de ce moment génère un message d'avertissement qui est consigné dans le journal d'erreurs. Le message indique la date et l'heure de l'événement, avertit qu'un audit est manquant, et précise le nom de login, le code event et d'autres informations, normalement stockées dans la colonne extrainfo de la table d'audit.

Lorsque la table d'audit courante est saturée, le SSO peut l'archiver et la tronquer, comme décrit à la section "Archivage de la table d'audit", page 486. L'administrateur système peut exécuter shutdown pour arrêter le serveur, puis le relancer pour rétablir la fonction d'audit.

S'il se produit un arrêt anormal du système d'audit, le SSO peut arrêter le serveur une fois que la table d'audit a été archivée et tronquée. Normalement, seul l'administrateur système est habilité à exécuter shutdown.

# Définition des options d'audit globales

Après avoir installé l'audit, vous pouvez définir ses options à l'aide de sp_audit. Syntaxe de sp_audit :

sp_audit *option*, *nom_login*, *nom_objet* [,*définition*]

Si vous lancez sp_audit sans paramètre, elle affiche la liste complète des options. Pour la description de sp_audit, consultez le Manuel de référence d'Adaptive Server.

**Remarque** Aucun événement n'est audité tant que vous n'activez pas l'audit sur le serveur. Pour plus d'informations, reportez-vous à "Activation et désactivation de l'audit", page 493.

## Options d'audit : types et conditions

Les valeurs admises pour les paramètres *nom_login* et *nom_objet* de sp_audit dépendent du type d'option d'audit que vous spécifiez :

- Les options globales s'appliquent aux commandes qui concernent l'intégralité du serveur (démarrage du serveur, commandes disque, etc.) et qui permettent de générer des enregistrements d'audit définis par l'utilisateur ad hoc. Les paramètres relatifs aux événements globaux sont stockés dans la table système sybsecurity..sysauditoptions.
- Les options spécifiques d'une base de données s'appliquent à la base de données : modification d'une base de données, bulk copy (bcp in) de données dans une base, octroi et révocation de droits d'accès à des objets dans une base et création d'objets dans une base. Les paramètres des options relatives à des événements spécifiques de la base de données sont stockés dans la table système master..sysdatabases.
- Les options spécifiques d'un objet s'appliquent à un objet particulier : sélection, insertion, mise à jour ou suppression de lignes dans une table ou une vue donnée et exécution d'un certain trigger ou d'une certaine procédure. Les paramètres des options relatives à des événements spécifiques d'un objet sont stockés dans la table système sysobjects de la base de données concernée.

- Les options spécifiques d'un utilisateur s'appliquent à un objet ou à un rôle système particulier : accès d'un utilisateur à une table ou une vue, toutes les actions exécutées lorsqu'un rôle déterminé, tel que sa_role, est actif. Les paramètres des options relatives à chaque utilisateur sont stockés dans master..syslogins. Les paramètres relatifs aux rôles système sont stockés dans master..sysauditoptions.

Le tableau 12-3 indique :

- les valeurs admises pour l'option et le type de chaque option : globale, ou spécifique d'une base de données, d'un objet ou d'un utilisateur ;
- les valeurs admises pour les paramètres *nom_login* et *nom_objet* ;
- la base de données à partir de laquelle définir l'option d'audit ;
- la commande ou l'accès audité lorsque vous activez l'option :
- un exemple pour chaque option.

Par défaut, toutes les options sont désactivées (off).

***Tableau 12-3 : Options d'audit, conditions et exemples***

| Option (type) | *nom_login* | *nom_objet* | Base de données à partir de laquelle définir l'option | Commande ou accès à auditer |
|---|---|---|---|---|
| adhoc<br>(spécifique de l'utilisateur) | tout | tout | Quelconque | Autorise les utilisateurs à exécuter sp_addauditrecord |
| Exemple : | `sp_audit "adhoc", "all", "all", "on"`<br>(Active les enregistrements d'audit définis par l'utilisateur ad hoc.) | | | |
| tout<br>(spécifique de l'utilisateur) | Nom de login ou rôle | tout | Quelconque | Toutes les actions d'un utilisateur ou des utilisateurs détenteurs d'un rôle actif déterminé |
| Exemple : | `sp_audit "all", "sa_role", "all", "on"`<br>(Active l'audit de toutes les actions dans lesquelles le rôle sa_role est actif.) | | | |
| alter<br>(spécifique de la base) | tout | Base de données à auditer | Quelconque | alter database, alter table |
| Exemple : | `sp_audit @option = "alter", @login_name = "all", @object_name = "master", @setting = "on"`<br>(Active l'audit de toutes les exécutions de alter database et de alter table dans la base de données master). | | | |

| Option (type) | *nom_login* | *nom_objet* | Base de données à partir de laquelle définir l'option | Commande ou accès à auditer |
|---|---|---|---|---|
| bcp (spécifique de la base) | tout | Base de données à auditer | Quelconque | bcp in |
| Exemple : | `sp_audit "bcp", "all", "pubs2"` | | | |
| | (Renvoie l'état de l'audit de bcp dans la base de données pubs2. Si vous ne spécifiez pas *définition*, Adaptive Server renvoie l'état de l'audit pour l'option que vous spécifiez) | | | |
| bind (spécifique de la base) | tout | Base de données à auditer | Quelconque | sp_bindefault, sp_bindmsg, sp_bindrule |
| Exemple : | `sp_audit "bind", "all", "planning", "off"` | | | |
| | (Désactive l'audit de liaison pour la base de données planning). | | | |
| cmdtext (spécifique de l'utilisateur) | Nom de login ou rôle | tout | Quelconque | Toutes les actions d'un utilisateur ou des utilisateurs détenteurs d'un rôle actif déterminé<br>(N'indique pas si le texte en question a réussi les contrôles d'autorisation. La valeur de *eventmod* est toujours égale à 1). |
| Exemple : | `sp_audit "cmdtext", "dbo", "off"` | | | |
| | (Désactive l'audit de texte pour les DBO (propriétaires de bases de données)). | | | |
| create (spécifique de la base) | tout | Base de données à auditer<br>Spécifiez master comme *nom_objet* si vous souhaitez auditer create database. Vous auditerez aussi la création d'autres objets dans master. | Quelconque | create database, create table, create procedure, create trigger, create rule, create default, sp_addmessage, create view |
| Exemple : | `sp_audit "create", "all", "planning", "pass"` | | | |
| | (Active l'audit de la création d'objet aboutie dans la base de données planning. L'état actuel de l'audit de create database n'est pas modifié car vous n'avez pas spécifié la base de données master). | | | |
| dbaccess (spécifique de la base) | tout | Base de données à auditer | Quelconque | Tout accès à la base de données à partir d'une autre base |
| Exemple : | `sp_audit "dbaccess", "all", "project", "on"` | | | |
| | (Active l'audit de tous les accès externes à la base de données project). | | | |

| Option (type) | *nom_login* | *nom_objet* | Base de données à partir de laquelle définir l'option | Commande ou accès à auditer |
|---|---|---|---|---|
| dbcc (globale) | tout | tout | Quelconque | dbcc |
| Exemple : | `sp_audit "dbcc", "all", "all", "on"` | | | |
| | (Active l'audit de toutes les exécutions de la commande dbcc). | | | |
| delete (spécifique d'un objet) | tout | Table ou vue, default table ou default view | Base où se trouve la table ou la vue (sauf tempdb) | delete à partir d'une table, delete à partir d'une vue |
| Exemple : | `sp_audit "delete", "all", "default table", "on"` | | | |
| | (Active l'audit de toutes les actions de suppression pour toutes les futures tables dans la base de données courante). | | | |
| disk (globale) | tout | tout | Quelconque | disk init, disk refit, disk reinit, disk mirror, disk unmirror, disk remirror |
| Exemple : | `sp_audit "disk", "all", "all", "on"` | | | |
| | (Active l'audit de toutes les actions sur le disque pour le serveur). | | | |
| drop (spécifique de la base) | tout | Base de données à auditer | Quelconque | drop database, drop table, drop procedure, drop trigger, drop rule, drop default, sp_dropmessage, drop view |
| Exemple : | `sp_audit "drop", "all", "financial", "fail"` | | | |
| | (Active l'audit de toutes les commandes de suppression dans la base de données financial qui échouent aux contrôles d'autorisation). | | | |
| dump (spécifique de la base) | tout | Base de données à auditer | Quelconque | dump database, dump transaction |
| Exemple : | `sp_audit "dump", "all", "pubs2", "on"` | | | |
| | (Active l'audit des commandes de sauvegarde dans la base de données pubs2). | | | |
| errors (globale) | tout | tout | Quelconque | Erreur fatale, erreur non fatale |
| Exemple : | `sp_audit "errors", "all", "all", "on"` | | | |
| | (Active l'audit des erreurs au sein du serveur). | | | |
| exec_procedure (spécifique d'un objet) | tout | Procédure ou default procedure | Base de données de la procédure (sauf tempdb) | execute |
| Exemple : | `sp_audit "exec_procedure", "all", "default procedure", "off"` | | | |
| | (Désactive l'audit automatique des nouvelles procédures dans la base de données courante). | | | |

| Option (type) | *nom_login* | *nom_objet* | Base de données à partir de laquelle définir l'option | Commande ou accès à auditer |
|---|---|---|---|---|
| exec_trigger (spécifique d'un objet) | tout | Trigger ou default trigger | Base de données du trigger (sauf tempdb) | Toute commande déclenchant le trigger |
| Exemple : | `sp_audit "exec_trigger", "all", "trig_fix_plan", "fail"`<br>(Active l'audit de toutes les exécutions infructueuses du trigger trig_fix_plan dans la base de données courante). | | | |
| func_dbaccess (spécifique de la base de données) | tout | Base de données | Quelconque | Accès à la base de données via les fonctions intégrées Transact-SQL |
| Exemple : | `sp_audit @option="func_dbaccess", @login_name="all", @object_name = "strategy", @setting = "on"`<br>(Active l'audit des accès à la base de données strategy via les fonctions intégrées). | | | |
| func_obj_access (spécifique de l'objet) | tout | Objet | Quelconque | Accès à un objet via les fonctions intégrées Transact-SQL |
| Exemple : | `sp_audit @option="func_obj_access", @login_name="all", @object_name = "customer", @setting = "on"`<br>(Active l'audit des accès à la table customer via les fonctions intégrées). | | | |
| grant (spécifique de la base) | tout | Base de données à auditer | Quelconque | grant |
| Exemple : | `sp_audit @option="grant", @login_name="all", @object_name = "planning", @setting = "on"`<br>(Active l'audit de tous les octrois d'autorisations dans la base de données planning). | | | |
| insert (spécifique d'un objet) | tout | Table ou vue, default table ou default view | Base de données de l'objet (sauf tempdb) | insert dans une table, insert dans une vue |
| Exemple : | `sp_audit "insert", "all", "dpt_101_view", "on"`<br>(Active l'audit de toutes les insertions dans la vue dpt_101_view dans la base de données courante). | | | |
| load (spécifique de la base) | tout | Base de données à auditer | Quelconque | load database, load transaction |
| Exemple : | `sp_audit "load", "all", "projects_db", "fail"`<br>(Active l'audit de toutes les exécutions infructueuses de chargement de la base et de transaction dans la base de données projects_db). | | | |
| login (globale) | tout | tout | Quelconque | Toute connexion à Adaptive Server |
| Exemple : | `sp_audit "login", "all", "all", "fail"`<br>(Active l'audit de toutes les tentatives infructueuses de connexion au serveur). | | | |

| Option (type) | *nom_login* | *nom_objet* | Base de données à partir de laquelle définir l'option | Commande ou accès à auditer |
|---|---|---|---|---|
| logout (globale) | tout | tout | Quelconque | Toute déconnexion d'Adaptive Server |
| Exemple : | `sp_audit "logout", "all", "all", "off"` | | | |
| | (Désactive l'audit des déconnexions du serveur). | | | |
| reference (spécifique d'un objet) | tout | Table à auditer | Quelconque | Création d'une référence entre tables |
| Exemple : | `sp_audit "reference", "all", "titles", "off"` | | | |
| | (Désactive l'audit de la création de références entre la table titles et les autres tables). | | | |
| revoke (spécifique de la base) | tout | Base de données à auditer | Quelconque | revoke |
| Exemple : | `sp_audit "revoke", "all", "payments_db", "off"` | | | |
| | (Désactive l'audit de l'exécution de revoke dans la base de données payments_db). | | | |
| rpc (globale) | tout | tout | Quelconque | Appels de procédure à distance (RPC) entrants ou sortants |
| Exemple : | `sp_audit "rpc", "all", "all", "on"` | | | |
| | (Active l'audit de tous les appels de procédure à distance (RPC) entrants ou sortants du serveur). | | | |
| security (globale) | tout | tout | Quelconque | Evénements relatifs à la sécurité à l'échelle du serveur. Voir l'option "security" dans le tableau 12-3. |
| Exemple : | `sp_audit "security", "all", "all", "on"` | | | |
| | (Active l'audit des événements relatifs à la sécurité à l'échelle du serveur). | | | |
| select (spécifique d'un objet) | tout | Table ou vue, default table ou default view | Base de données de l'objet (sauf tempdb) | select dans une table, select dans une vue |
| Exemple : | `sp_audit "select", "all", "customer", "fail"` | | | |
| | (Active l'audit de toutes les sélections infructueuses à partir de la table customer dans la base de données courante. ) | | | |
| setuser (spécifique de la base) | tout | tout | Quelconque | setuser |
| Exemple : | `sp_audit "setuser", "all", "projdb", "on"` | | | |
| | (Active l'audit de toutes les exécutions de setuser dans la base de données projdb). | | | |

| Option (type) | *nom_login* | *nom_objet* | Base de données à partir de laquelle définir l'option | Commande ou accès à auditer |
|---|---|---|---|---|
| table_access (spécifique de l'utilisateur) | Nom de login | tout | Quelconque | select, delete, update ou insert un accès dans une table |
| Exemple : | `sp_audit "table_access", "smithson", "all", "on"` | | | |
| | (Active l'audit de tous les accès à la table par le nom de login "smithson"). | | | |
| truncate (spécifique de la base) | tout | Base de données à auditer | Quelconque | truncate table |
| Exemple : | `sp_audit "truncate", "all", "customer", "on"` | | | |
| | (Active l'audit de toutes les troncatures de table dans la base de données customer). | | | |
| unbind (spécifique de la base) | tout | Base de données à auditer | Quelconque | sp_unbindefault, sp_unbindrule, sp_unbindmsg |
| Exemple : | `sp_audit "unbind", "all", "master", "fail"` | | | |
| | (Active l'audit de toutes les tentatives infructueuses d'annulation de liaison dans la base de données master). | | | |
| update (spécifique d'un objet) | tout | Vue, default table ou default view | Base de données de l'objet (sauf tempdb) | update une table, update une vue |
| Exemple : | `sp_audit "update", "all", "projects", "on"` | | | |
| | (Active l'audit de toutes les tentatives des utilisateurs de mettre à jour la table projects dans la base de données courante). | | | |
| view_access (spécifique de l'utilisateur) | Nom de login | tout | Quelconque | select, delete, insert ou update sur une vue |
| Exemple : | `sp_audit "view_access", "joe", "all", "off"` | | | |
| | (Désactive l'audit des vues de l'utilisateur "joe"). | | | |

## Exemples de définition d'options d'audit

Supposons que vous souhaitiez auditer toutes les opérations de suppression ayant échoué sur la table projects de la base company_operations et sur toutes les nouvelles tables de cette base. Utilisez l'option delete spécifique de l'objet pour la table projects et l'option default table pour les tables créées par la suite. Pour définir des options d'audit relatives aux objets, vous devez vous trouver dans la base qui contient l'objet avant d'exécuter sp_audit :

```
sp_audit "security", "all", "all", "fail"
```

- Pour cet exemple, exécutez :

```
use company_operations
go
sp_audit "delete", "all", "projects", "fail"
go
sp_audit "delete", "all", "default table",
"fail"
go
```

## Affichage des options d'audit courantes

Pour connaître la valeur d'une option d'audit spécifique, utilisez sp_displayaudit. Respectez la syntaxe suivante :

sp_displayaudit [*procedure* | *object* | *login* | *database* | *global* | *default_object* | *default_procedure* [, *name*]]

Pour plus d'informations, reportez-vous à sp_displayaudit dans le Manuel de référence d'Adaptive Server.

## Ajout d'enregistrements utilisateur dans la trace d'audit

sp_addauditrecord permet aux utilisateurs d'entrer des commentaires dans la trace d'audit. Respectez la syntaxe suivante :

sp_addauditrecord [*texte*] [, *nom_base*] [, *nom objet*] [, *nom_propriétaire*] [, *id_base*] [, *id_obj*]

Tous les paramètres sont facultatifs.

- *texte* correspond au texte du message à ajouter dans la table d'audit extrainfo.
- *nom_base* correspond au nom de la base de données à laquelle l'enregistrement fait référence, qui est inséré dans la colonne dbname de la table d'audit courante.
- *nom_objet* est le nom de l'objet auquel l'enregistrement fait référence, qui est inséré dans la colonne objname de la table d'audit courante.
- *nom_propriétaire* représente le propriétaire de l'objet auquel l'enregistrement fait référence, qui est inséré dans la colonne objowner de la table d'audit courante.

- *id_base* est une valeur entière représentant le numéro d'ID correspondant à nom_base, qui est insérée dans la colonne dbid de la table d'audit courante. Ne la mettez pas entre guillemets.
- *id_objet* est une valeur entière représentant le numéro d'ID correspondant à nom_objet. Cette valeur ne doit pas être écrite entre guillemets. Elle est insérée dans la colonne objid de la table d'audit courante.

Vous pouvez utiliser sp_addauditrecord si :

- vous disposez du droit d'exécution sur sp_addauditrecord ;
- le paramètre de configuration auditing a été activé avec sp_configure ;
- l'option d'audit adhoc a été activée avec sp_audit.

Par défaut, seul un SSO et le DBO de sybsecurity ont le droit d'exécuter sp_addauditrecord. Cette autorisation peut être octroyée à d'autres utilisateurs.

## Exemples d'ajout d'enregistrements d'audit utilisateur

L'exemple suivant ajoute un enregistrement dans la table d'audit courante. Les éléments ci-après sont insérés dans la colonne correspondante : la partie texte dans extrainfo, "corporate" dans dbname, "payroll" dans objname, "dbo" dans objowner, "10" dans dbid et "1004738270" dans objid :

```
sp_addauditrecord "J'ai autorisé A. Smith à
consulter la table payroll de la base corporate.
Cette autorisation était valable de 15:10 à 15:30,
le 22/09/92.", "corporate", "payroll", "dbo", 10,
1004738270
```

L'exemple suivant insère des informations uniquement dans les colonnes extrainfo et dbname de la table d'audit courante :

```
sp_addauditrecord @text="Je désactive brièvement
l'audit pendant que nous reconfigurons le système",
@db_name="corporate"
```

# Requête de trace d'audit

Pour interroger la trace d'audit, sélectionnez et agrégez les données d'audit à l'aide de SQL. Si vous avez suivi les procédures décrites dans "Configuration de l'audit pour gérer la trace d'audit", page 484, les données sont automatiquement archivées dans une ou plusieurs tables d'une autre base. Supposons, par exemple, que les données d'audit résident dans la table audit_data de la base audit_db. Pour sélectionner les enregistrements relatifs aux tâches effectuées par "bob" le 5 juillet 1993, exécutez :

```
use audit_db
go
select * from audit_data
  where loginname = "bob"
  and eventtime like "Jul 5% 93"
go
```

La requête suivante extrait les enregistrements d'audit relatifs aux commandes exécutées dans la base pubs2 par les utilisateurs ayant le rôle de SSO :

```
select * from audit_data
  where extrainfo like "%sso_role%"
  and dbname = "pubs2"
go
```

La requête suivante extrait tous les enregistrements d'audit relatifs aux troncatures de table (événement 64) :

```
select * from audit_data
  where event = 64
go
```

# Caractéristiques des tables d'audit

Seul le SSO est habilité à accéder aux tables d'audit système et à lire les tables via des commandes SQL. Les seules commandes autorisées sur les tables d'audit système sont select et truncate.

Le tableau 12-4 décrit les colonnes de toutes les tables d'audit.

***Tableau 12-4 : Colonnes de chaque table***

| Nom de colonne | Type de données | Description |
|---|---|---|
| event | smallint | Type d'événement audité. Reportez-vous au tableau 12-6, page 511. |
| eventmod | smallint | Complément d'informations au sujet de l'événement audité. Indique si l'événement a réussi les contrôles d'autorisation. Les valeurs possibles sont :<br>• 0 = aucun modificateur pour cet événement<br>• 1 = le contrôle des autorisations a réussi<br>• 2 = le contrôle des autorisations a échoué |
| spid | smallint | ID serveur du processus ayant généré l'enregistrement d'audit à consigner. |
| eventtime | datetime | Date et heure de l'occurrence de l'événement. |
| sequence | smallint | Numéro d'ordre de l'enregistrement au sein d'un événement unique. Certains événements requièrent plusieurs enregistrements d'audit. |
| suid | smallint | ID de login serveur de l'utilisateur ayant généré l'événement audité. |
| dbid | int null | ID de la base de données dans laquelle l'événement audité est survenu ou dans laquelle réside l'objet, la procédure stockée ou le trigger (en fonction du type de l'événement). |
| objid | int null | ID de l'objet, de la procédure stockée ou du trigger auquel le processus a accédé. |
| xactid | binary(6) null | ID de la transaction contenant l'événement audité. Dans le cas d'une transaction multibase, il s'agit de l'ID provenant de la base d'origine de la transaction. |
| loginname | varchar(30) null | Nom de login correspondant à suid. |
| dbname | varchar(30) null | Nom de la base de données correspondant à dbid. |
| objname | varchar(30) null | Nom de l'objet correspondant à objid. |
| objowner | varchar(30) null | Nom du propriétaire de l'objet objid. |
| extrainfo | varchar(255) null | Complément d'informations au sujet de l'événement audité. Cette colonne contient une série d'éléments séparés par des points-virgules. Pour plus de détails, reportez-vous à la section "Lecture de la colonne extrainfo", page 510. |

## Lecture de la colonne *extrainfo*

La colonne extrainfo contient une série de données, séparées par des points-virgules et organisées en différentes catégories. Ces catégories sont décrites ci-dessous.

***Tableau 12-5 : Informations de la colonne extrainfo***

| Position | Catégorie | Description |
|---|---|---|
| 1 | Rôles | Liste de rôles actifs, séparés par des blancs. |
| 2 | Mots clés ou options | Nom du mot clé ou de l'option utilisé pour l'événement. Par exemple, pour la commande alter table, il est possible d'utiliser l'option add column ou drop constraint. Si plusieurs mots clés ou options sont indiqués, ils sont séparés par des virgules. |
| 3 | Valeur antérieure | Si l'événement a entraîné la mise à jour d'une valeur, cet élément contient l'ancienne valeur. |
| 4 | Valeur courante | Si l'événement a entraîné la mise à jour d'une valeur, cet élément contient la nouvelle valeur. |
| 5 | Autres informations | Informations complémentaires sur la sécurité enregistrées pour l'événement. |
| 6 | Informations de proxy | Nom de login d'origine, si l'événement est survenu après l'exécution d'une commande set proxy. |
| 7 | Nom principal | Nom principal passé par le mécanisme de sécurité sous-jacent, si le login de l'utilisateur est le login sécurisé par défaut et si l'utilisateur a ouvert la session dans Adaptive Server par login unifié. La valeur de cet élément est NULL si aucun login sécurisé par défaut n'est utilisé. |

Cet exemple montre une entrée de la colonne extrainfo correspondant à un événement qui a changé un paramètre de configuration d'audit :

```
sso_role;suspend audit when device full;1;0;;ralph;
```

Cette entrée indique qu'un responsable de la sécurité du système a changé (de 1 à 0) la valeur du paramètre suspend audit when device full. Aucune "autre information" n'est définie. La sixième catégorie indique que l'utilisateur "ralph" se servait d'un login proxy. Aucun nom principal n'est fourni.

Les autres champs de l'enregistrement d'audit fournissent des données pertinentes. Par exemple, l'enregistrement contient l'ID serveur (suid) et le nom de login (loginname) de l'utilisateur.

Le tableau 12-6 répertorie les valeurs possibles de la colonne event, classées par nom d'option sp_audit. La colonne "Informations dans extrainfo" décrit les données susceptibles de figurer dans la colonne extrainfo d'une table d'audit, en fonction des catégories mentionnées dans le tableau 12-5.

***Tableau 12-6 : Valeurs des colonnes event et extrainfo***

| Option d'audit | Commande ou accès à auditer | event | Informations dans extrainfo |
|---|---|---|---|
| (Evénement audité automatiquement, non contrôlé par une option) | Activation de l'audit avec : sp_configure auditing | 73 | - |
| (Evénement audité automatiquement, non contrôlé par une option) | Désactivation de l'audit avec : sp_configure auditing | 74 | - |
| adhoc | Enregistrement d'audit défini par l'utilisateur | 1 | extrainfo contient les données du paramètre *texte* de sp_addauditrecord |
| alter | alter database | 2 | *Mots clés ou options :*<br>alter maxhold<br>alter size |
| | alter table | 3 | *Mots clés ou options :*<br>add column<br>drop column<br>replace column<br>add constraint<br>drop constraint |
| bcp | bcp in | 4 | - |
| bind | sp_bindefault | 6 | *Autres informations :* nom de la valeur par défaut |
| | sp_bindmsg | 7 | *Autres informations :* ID du message |
| | sp_bindrule | 8 | *Autres informations :* nom de la règle |
| create | create database | 9 | - |
| | create default | 14 | - |
| | create procedure | 11 | - |
| | create rule | 13 | - |
| | create table | 10 | - |
| | create trigger | 12 | - |
| | create view | 16 | - |
| | sp_addmessage | 15 | *Autres informations :* numéro du message |
| dbaccess | Tout accès à une base de données par tout utilisateur | 17 | *Mots clés ou options :*<br>use cmd<br>outside reference |
| dbcc | dbcc (all keywords) | 81 | *Mots clés ou options :*<br>Tout mot clé de la commande dbcc, tel que checkstorage, avec les options correspondantes. |

| Option d'audit | Commande ou accès à auditer | event | Informations dans extrainfo |
|---|---|---|---|
| delete | delete dans une table | 18 | *Mots-clés ou options :* delete |
| | delete dans une vue | 19 | *Mots clés ou options :* delete |
| disk | disk init | 20 | *Mots clés ou options :* disk init *Autres informations :* nom du disque |
| | disk mirror | 23 | *Mots clés ou options :* disk mirror *Autres informations :* nom du disque |
| | disk refit | 21 | *Mots clés ou options :* disk refit *Autres informations :* nom du disque |
| | disk reinit | 22 | *Mots clés ou options :* disk reinit *Autres informations :* nom du disque |
| | disk remirror | 25 | *Mots clés ou options :* disk remirror *Autres informations :* nom du disque |
| | disk unmirror | 24 | *Mots clés ou options :* disk unmirror *Autres informations :* nom du disque |
| drop | drop database | 26 | - |
| | drop default | 31 | - |
| | drop procedure | 28 | - |
| | drop table | 27 | - |
| | drop trigger | 29 | - |
| | drop rule | 30 | - |
| | drop view | 33 | - |
| | sp_dropmessage | 32 | *Autres informations :* numéro du message |
| dump | dump database | 34 | - |
| | dump transaction | 35 | - |
| errors | Erreur fatale | 36 | *Autres informations : Numéro de l'erreur.Gravité.Etat* |
| | Erreur non fatale | 37 | *Autres informations : Numéro de l'erreur.Gravité.Etat* |
| exec_procedure | Exécution d'une procédure | 38 | *Autres informations :* tous les paramètres d'entrée |
| exec_trigger | Exécution d'un trigger | 39 | - |

| Option d'audit | Commande ou accès à auditer | event | Informations dans extrainfo |
|---|---|---|---|
| func_obj_access, func_dbaccess | Accès aux objets et aux bases de données via des fonctions Transact-SQL | 85 | - |
| grant | grant | 40 | - |
| insert | insert dans une table | 41 | *Mots clés ou options :* Avec insert : insert Avec select into : insert into suivie du nom d'objet entièrement qualifié |
| | insert dans une vue | 42 | *Mots clés ou options* : insert |
| load | load database | 43 | - |
| | load transaction | 44 | - |
| login | Toute connexion au serveur | 45 | *Autres informations :* nom d'hôte de la machine sur laquelle la connexion a été effectuée |
| logout | Toute déconnexion du serveur | 46 | *Autres informations :* nom d'hôte de la machine sur laquelle la connexion a été effectuée |
| reference | Création de références à des tables | 91 | *Mots clés ou options* : reference *Autres informations :* nom de la table de référence |
| revoke | revoke | 47 | - |
| rpc | Appel de procédure à distance provenant d'un autre serveur | 48 | *Mots-clés ou options :* nom du programme client *Autres informations :* nom du serveur, nom d'hôte de la machine à partir de laquelle le RPC a été émis. |
| | Appel de procédure à distance vers un autre serveur | 49 | *Mots clés ou options :* nom de la procédure |
| security | connect to (CIS seulement) | 90 | *Mots-clés ou options :* connect to |
| | commande kill (CIS seulement) | 89 | *Mots clés ou options :* kill |
| | online database | 83 | - |
| | fonction proc_role (exécutée depuis une procédure système) | 80 | *Autres informations :* rôles requis |
| | Nouvelle génération d'un mot de passe par un SSO | 76 | *Mots-clés ou options :* définition du mot de passe du SSO *Autres informations :* nom de login |

| Option d'audit | Commande ou accès à auditer | event | Informations dans extrainfo |
|---|---|---|---|
| | Changement de rôle | 55 | *Valeur antérieure :* on ou off<br>*Valeur courante :* on ou off<br>*Autres informations :* nom du rôle défini |
| | Démarrage du serveur | 50 | *Autres informations :*<br>-d*nom_device_master*<br>-i*chemin_fichier_interface*<br>-S*nom_serveur*<br>-e*nom_fichier_erreurs* |
| | Arrêt du serveur | 51 | *Mots clés ou options :*<br>shutdown |
| | set proxy ou<br>set session authorization | 88 | *Valeur antérieure :* suid précédent<br>*Valeur courante :* nouveau suid |
| | sp_configure | 82 | *Autres informations :*<br>• En cas de définition d'un paramètre :<br>nombre de paramètres de configuration<br>• En cas d'utilisation d'un fichier de configuration pour définir des paramètres :<br>nom du paramètre de configuration |
| | valid_user | 85 | *Mots clés ou options :*<br>valid_user |
| select | select dans une table | 62 | *Mots clés ou options :*<br>select into<br>select<br>readtext |
| | select dans une vue | 63 | *Mots clés ou options :*<br>select into<br>select<br>readtext |
| setuser | setuser | 84 | *Autres informations :* nom de l'utilisateur défini |

| Option d'audit | Commande ou accès à auditer | event | Informations dans extrainfo |
|---|---|---|---|
| table_access | delete | 18 | *Mots clés ou options :*<br>delete |
| | insert | 41 | *Mots clés ou options :*<br>insert |
| | select | 62 | *Mots clés ou options :*<br>select into<br>select<br>readtext |
| | update | 70 | *Mots clés ou options :*<br>update<br>writetext |
| truncate | truncate table | 64 | - |
| unbind | sp_unbindefault | 67 | - |
| | sp_unbindmsg | 69 | - |
| | sp_unbindrule | 68 | - |
| update | update dans une table | 70 | *Mots clés ou options :*<br>update<br>writetext |
| | update dans une vue | 71 | *Mots clés ou options :*<br>update<br>writetext |
| view_access | delete | 19 | *Mots clés ou options :*<br>delete |
| | insert | 42 | *Mots clés ou options :*<br>insert |
| | select | 63 | *Mots clés ou options :*<br>select into<br>select<br>readtext |
| | update | 71 | *Mots clés ou options :*<br>update<br>writetext |

CHAPITRE 13

# Gestion des serveurs distants

Ce chapitre présente les étapes à effectuer par l'administrateur système et le responsable de la sécurité du système (SSO) de chaque Adaptive Server pour activer les **appels de procédure à distance** (RPC).

Les sujets traités dans ce chapitre sont les suivants :



## Présentation

Les utilisateurs d'un Adaptive Server local peuvent exécuter des procédures stockées sur un Adaptive Server distant. L'exécution d'un RPC (appel de procédure à distance) renvoie les résultats du processus distant au processus appelant, affichés généralement sur l'écran de l'utilisateur.

---

**Remarque** L'utilisation de serveurs distants n'est pas prévue dans la configuration évaluée.

---

Pour autoriser les RPC, l'administrateur système (SA) et le responsable de la sécurité du système de chaque Adaptive Server doivent effectuer les opérations suivantes :

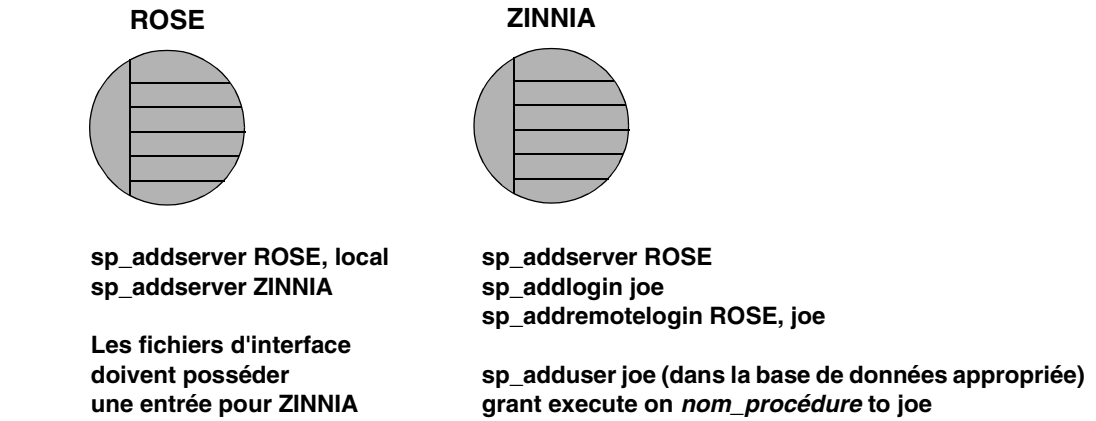
- Sur le serveur local :
  - Le responsable de la sécurité du système utilise la procédure système sp_addserver pour enregistrer le serveur local et le serveur distant dans la table système master..sysservers.
  - Il enregistre le serveur distant dans le fichier d'interface ou service de répertoire du serveur local.

- Il redémarre le serveur local pour que la variable globale @@servername contienne son nom. Si cette variable n'est pas définie correctement, les utilisateurs ne peuvent pas exécuter de RPC depuis le serveur local vers un serveur distant.

- Sur le serveur distant :
  - Le responsable de la sécurité du système utilise la procédure système sp_addserver pour enregistrer, dans la table système master..sysservers, le serveur à l'origine du RPC.
  - Pour autoriser l'utilisateur émettant la procédure distante à accéder au serveur, le responsable de la sécurité du système utilise la procédure sp_addlogin, tandis que l'administrateur système se sert de sp_addremotelogin.
  - Le responsable de la sécurité du système ajoute le nom de login distant comme un utilisateur de la base de données appropriée et octroie à ce login l'autorisation d'exécuter la procédure. (Si le droit execute est octroyé à "public", l'utilisateur n'a pas besoin d'autorisation spécifique.)

La figure 13-1 montre comment configurer un serveur pour l'accès à distance.

***Figure 13-1 : Configuration des serveurs pour les appels de procédure à distance***




Pour plus d'informations sur la gestion des serveurs distants spécifiques du système d'exploitation, reportez-vous au Guide d'installation pour votre plate-forme.

# Gestion des serveurs distants

Le tableau 13-1 répertorie les tâches relatives à la gestion des serveurs distants et les procédures système requises pour effectuer ces tâches.

***Tableau 13-1 : Tâches relatives à la gestion des serveurs distants***

| Pour | Utiliser | Voir |
|---|---|---|
| Ajouter un serveur distant | sp_addserver | "Ajout d'un serveur distant", page 519 |
| Gérer les noms des serveurs distants | sp_addserver | "Gestion des noms de serveurs distants", page 521 |
| Modifier les options de connexion du serveur | sp_serveroption | "Définition des options de connexion du serveur", page 521 |
| Afficher des informations sur les serveurs | sp_helpserver | "Recherche d'informations sur les serveurs", page 523 |
| Supprimer un serveur | sp_dropserver | "Suppression de serveurs distants", page 524 |

## Ajout d'un serveur distant

Le responsable de la sécurité du système exécute sp_addserver pour ajouter des entrées dans la table sysservers. Sur le serveur émettant l'appel, vous devez ajouter une entrée pour le serveur local et une autre pour chaque serveur distant que votre serveur doit appeler.

Lorsque vous créez des entrées pour un serveur distant, vous pouvez choisir :

- de faire référence au serveur distant en utilisant le nom figurant dans le fichier d'interface, ou
- de lui donner un nom local. Par exemple, si le nom défini dans le fichier d'interface est "MAIN_PRODUCTION", vous pouvez nommer le serveur distant simplement "main".

Respectez la syntaxe suivante :

```
sp_addserver nom_l [{, local | null}
    [, nom_p]]
```

où :

- *nom_l* est le "nom d'appel" local du serveur distant. Si ce nom *n'est pas* celui indiqué dans le fichier d'interface pour le serveur distant, vous devez le spécifier comme troisième paramètre, *nom_p*.

Le serveur distant doit figurer dans le fichier d'interface sur la machine locale. S'il n'y figure pas, copiez l'entrée du fichier d'interface du serveur distant et ajoutez-la à votre fichier d'interface. Veillez à conserver les mêmes numéros de port.

- local identifie le serveur ajouté comme un serveur local. La valeur local n'est utilisée qu'après le démarrage, ou le redémarrage, pour identifier le nom du serveur local de sorte qu'il apparaisse dans les messages générés par Adaptive Server. null indique que le serveur est un serveur distant.

**Remarque** Pour que les utilisateurs puissent lancer des RPC à partir du serveur local, celui-ci doit être ajouté via l'option local et redémarré. Le redémarrage est requis pour définir la variable globale @@servername.

- *nom_p* est le serveur distant figurant dans le fichier d'interface pour le serveur appelé *nom_l*. Cet argument facultatif permet de définir des alias locaux pour tout autre Adaptive Server, Open Server™ ou Backup Server avec lequel vous souhaitez communiquer. Si vous ne spécifiez pas *nom_p*, il prend par défaut la valeur *nom_l*.

## Exemples d'ajout de serveurs distants

L'exemple suivant crée une entrée pour le serveur local DOCS :

```
sp_addserver DOCS, local
```

L'exemple suivant crée une entrée pour le serveur distant GATEWAY :

```
sp_addserver GATEWAY
```

Pour exécuter un procédure distante telle que sp_who sur le serveur GATEWAY, exécutez :

```
GATEWAY.sybsytemprocs.dbo.sp_who
```

ou :

```
GATEWAY...sp_who
```

Cet exemple attribue l'alias local "main" au serveur distant MAIN_PRODUCTION :

```
sp_addserver main, null, MAIN_PRODUCTION
```

L'utilisateur peut alors entrer :

```
main...sp_who
```

## Gestion des noms de serveurs distants

La table master.dbo.sysservers possède deux colonnes nommées :

- srvname est le nom unique du serveur, que les utilisateurs doivent spécifier pour exécuter des appels de procédure à distance.
- srvnetname est le nom réseau du serveur, qui doit correspondre au nom figurant dans le fichier *d'interfaces*.

Pour ajouter ou supprimer des serveurs du réseau, vous pouvez utiliser sp_addserver pour mettre à jour le nom réseau du serveur dans srvnetname.

Par exemple, pour supprimer du réseau le serveur MAIN et déplacer vos applications distantes dans TEMP, vous pouvez utiliser l'instruction suivante, pour modifier le nom réseau du serveur tout en conservant l'alias local :

```
sp_addserver MAIN, null, TEMP
```

L'instruction sp_addserver affiche un message indiquant qu'elle modifie le nom réseau d'une entrée serveur existante.

## Définition des options de connexion du serveur

sp_serveroption définit les options du serveur timeouts, net password encryption, rpc security model A et rpc security model B, qui concernent les connexions avec les serveurs distants. En outre, si vous avez défini le modèle de sécurité des procédures distantes à rpc security model B, vous pouvez utiliser sp_serveroption pour définir les options supplémentaires suivantes : security mechanism, mutual authentication, use message confidentiality et use message integrity.

Les options spécifiées pour sp_serveroption n'ont pas d'incidence sur les communications entre Adaptive Server et Backup Server.

Les sections suivantes décrivent les paramètres timeouts, net password encryption, rpc security model A et rpc security model B. Pour plus d'informations sur les options complémentaires disponibles lorsque rpc security model B est activé, reportez-vous à la section "Etablissement de la sécurité pour les procédures à distance", page 555.

## Option *timeouts*

L'administrateur système dispose de l'option timeouts pour activer et désactiver le code de temporisation normal utilisé par le serveur local.

Par défaut, timeouts prend la valeur true et le processus gestionnaire des sites distants, qui gère les connexions à distance, déclare le délai imparti dépassé si aucune activité de l'utilisateur distant n'est détectée pendant une minute. Si vous donnez à timeouts la valeur false sur les deux serveurs concernés par les appels de procédure à distance, la temporisation automatique est désactivée. L'instruction suivante définit timeouts sur la valeur false :

```
sp_serveroption GATEWAY, "timeouts", false
```

Si timeouts a la valeur false sur les deux serveurs, et qu'un utilisateur exécute un RPC quelque soit le sens, le gestionnaire de sites distants sur chaque machine reste actif jusqu'à ce qu'un des serveurs soit arrêté. Lorsque le serveur est remis en fonction, l'option reste false et le gestionnaire de sites distants est réactivé dès qu'un utilisateur exécute un RPC. Si les utilisateurs exécutent de fréquents RPC, il est judicieux, en termes de ressources système, d'employer la valeur false, dans la mesure où l'établissement de la connexion physique impose une charge non négligeable au système.

## Option *net password encryption*

Le responsable de la sécurité du système dispose de l'option net password encryption pour spécifier si les connexions avec un serveur distant doivent être établies via une prise de contact avec mot de passe crypté côté client ou via la séquence habituelle de prise de contact avec mot de passe non crypté. La valeur par défaut est false.

Si l'option net password encryption prend la valeur true :

1 Le paquet de connexion initial est envoyé sans mots de passe.

2 Le client indique au serveur distant qu'un cryptage est souhaité.

3 Le serveur distant renvoie une clé de cryptage, que le client utilise pour crypter ses mots de passe en clair.

4 Le client crypte ensuite ses propres mots de passe et le serveur distant les authentifie à leur arrivée à l'aide de la clé.

L'instruction suivante définit l'option net password encryption sur la valeur true :

```
sp_serveroption GATEWAY, "net password encryption",
    true
```

Cette option n'a aucune incidence sur l'interaction entre Adaptive Server et Backup Server.

### Options *rpc security model*

Les options rpc security model A et rpc security model B déterminent le type de sécurité disponible pour les RPC. Si vous optez pour le modèle A (valeur par défaut), Adaptive Server ne supporte pas les services de sécurité tels que la confidentialité des messages par cryptage entre les deux serveurs.

Avec le modèle de sécurité B, l'Adaptive Server local obtient une accréditation par le mécanisme de sécurité et l'utilise pour établir une connexion physique sûre avec l'Adaptive Server distant. Avec ce modèle, vous pouvez choisir un ou plusieurs des services de sécurité suivants : authentification réciproque, confidentialité des messages par cryptage ou intégrité des messages.

Pour configurer le modèle de sécurité A pour le serveur GATEWAY, exécutez :

```
sp_serveroption GATEWAY, "rpc security model A",
   true
```

Pour savoir comment configurer les serveurs pour le modèle de sécurité B, reportez-vous à la section "Etablissement de la sécurité pour les procédures à distance", page 555.

## Recherche d'informations sur les serveurs

sp_helpserver donne des informations sur les serveurs. Sans argument, cette commande donne des informations sur tous les serveurs figurant dans la liste sysservers. Si vous spécifiez le nom d'un serveur, elle donne des informations sur ce seul serveur. Respectez la syntaxe suivante :

sp_helpserver [*serveur*]

sp_helpserver vérifie la présence de srvname et de srvnetname dans la table master..sysremotelogins.

Pour plus d'informations sur la configuration des serveurs distants, spécifiques du système d'exploitation, reportez-vous au Guide d'installation pour votre plate-forme.

## Suppression de serveurs distants

Le responsable de la sécurité du système dispose de la procédure système sp_dropserver pour supprimer des serveurs de sysservers. Respectez la syntaxe suivante :

```
sp_dropserver serveur [, droplogins]
```

où :

- *serveur* est le nom du serveur à supprimer.
- droplogins permet de supprimer en une seule opération un serveur distant et toutes les informations de connexion à distance qui le concernent. Si vous n'utilisez pas droplogins, vous ne pouvez pas supprimer un serveur auquel sont associés des logins distants.

L'instruction suivante supprime le serveur GATEWAY et tous les logins distants qui lui sont associés :

```
sp_dropserver GATEWAY, droplogins
```

Vous n'êtes pas obligé d'exécuter droplogins si vous souhaitez supprimer le serveur local : aucune information de connexion à distance n'est associée à ce serveur.

# Ajout de logins distants

Le responsable de la sécurité du système et l'administrateur système de n'importe quel Adaptive Server contrôlent à la fois l'accès au serveur par des utilisateurs distants et l'identité de ces utilisateurs. L'administrateur système utilise sp_addremotelogin pour ajouter des logins distants et sp_dropremotelogin pour en supprimer. Le responsable de la sécurité du système utilise sp_remoteoption pour vérifier si le contrôle des mots de passe est requis.

## Correspondance des ID serveur des utilisateurs

Il existe trois moyens d'associer les logins d'un serveur distant à un serveur local :

- Associer un login distant particulier à un nom de login local défini. Vous pouvez, par exemple, associer l'utilisateur "jean" sur le serveur distant à "jeanschmit".
- Associer tous les logins d'un serveur distant à un seul nom local. Vous pouvez, par exemple, associer à "remusers" tous les utilisateurs envoyant des RPC (appels de procédure à distance) à partir du serveur MAIN.
- Conserver les noms distants de tous les logins d'un serveur distant.

Vous pouvez combiner la première option avec les deux autres, sachant qu'elle prime, de par sa spécificité, sur les deux autres, plus générales. Les deuxième et troisième options s'excluent mutuellement : vous pouvez spécifier l'une ou l'autre, mais pas les deux en même temps.

Pour modifier l'option de correspondance :

Exécutez sp_dropremotelogin pour supprimer l'ancienne correspondance.

Exécutez sp_addremotelogin pour ajouter des logins distants. Respectez la syntaxe suivante :

```
sp_addremotelogin serveur_distant [, nom_login
    [, nom_distant]]
```

Si les noms locaux ne figurent pas dans la liste master..syslogins, ajoutez-les en tant que logins Adaptive Server via sp_addlogin, avant d'ajouter les logins distants.

Seul l'administrateur système est habilité à exécuter sp_addremotelogin. Pour plus d'informations, reportez-vous au document *Manuel de référence d'Adaptive Server*.

## Correspondance entre logins distants et noms locaux définis

Dans l'exemple suivant, le login "pogo" d'un système distant est associé au nom local "bob". L'utilisateur se connecte au système distant sous "pogo". Lorsque cet utilisateur lance des RPC (appels de procédure à distance) à partir de GATEWAY, le système local associe le login distant à "bob".

```
sp_addlogin bob
sp_addremotelogin GATEWAY, bob, pogo
```

## Correspondance entre tous les logins distants et un nom local

Dans l'exemple suivant, une entrée est créée, qui associe tous les noms de logins distants au nom local "albert". Tous les noms sont associés à "albert", excepté ceux dotés de correspondants spécifiques, comme indiqué à la section précédente. Par exemple, si vous avez associé "pogo" à "bob", puis le reste des logins à "albert", "pogo" reste associé à "bob".

```
sp_addlogin albert
sp_addremotelogin GATEWAY, albert
```

Si vous utilisez sp_addremotelogin pour associer tous les utilisateurs d'un serveur distant à un même nom local, exécutez sp_remoteoption pour spécifier l'option "trusted" pour ces utilisateurs. Par exemple, si tous les utilisateurs du serveur GATEWAY associés à "albert" doivent être sécurisés, spécifiez :

```
sp_remoteoption GATEWAY, albert, NULL, trusted, true
```

Si vous ne sécurisez pas les logins, ils ne pourront pas exécuter de RPC sur le serveur local, à moins qu'ils ne spécifient les mots de passe du serveur local lors de leur connexion au serveur distant. Les utilisateurs qui se servent de Client-Library d'Open Client peuvent utiliser la routine ct_remote_pwd pour spécifier un mot de passe pour les connexions de serveur à serveur. isql et bcp n'autorisent pas les utilisateurs à spécifier un mot de passe pour les connexions RPC. Pour plus d'informations sur sp_sremoteoption, reportez-vous à la section "Contrôle des mots de passe pour les utilisateurs distants", page 529.

---

**Avertissement !** N'associez pas plus d'un login distant à un login local, pour ne pas diminuer la traçabilité des utilisateurs sur le serveur. Les actions auditées ne sont enregistrées que sur le login du serveur local, et non sur les logins individuels sur le serveur distant.

---

### En cas d'utilisation de la sécurité réseau

Si des utilisateurs sont connectés au serveur distant via une "connexion unifiée", les logins doivent également être sécurisés sur le serveur local ou spécifier des mots de passe pour se connecter au serveur distant. Pour plus d'informations sur le login "unified login", reportez-vous à la section "Utilisation de l'unification des logins", page 547.

---

**Avertissement !** L'utilisation du mode trusted de sp_remoteoption affaiblit la sécurité de votre serveur, les mots de passe des utilisateurs "sécurisés" n'étant pas contrôlés.

---

## Conservation des noms de logins distants pour les serveurs locaux

Pour que les utilisateurs distants puissent conserver leur nom de login distant lorsqu'ils utilisent un serveur local :

1 Exécutez sp_addlogin pour créer un login pour chaque login du serveur distant.

2 Exécutez sp_addremotelogin au niveau du serveur pour créer une entrée dans master..sysremotelogins avec la valeur null pour le nom de login distant et la valeur -1 pour le suid. Exemple :

```
sp_addremotelogin GATEWAY
```

## Exemple de correspondance du login d'un utilisateur distant

L'instruction suivante affiche des informations sur les serveurs local et distant enregistrées dans master..sysservers :

```
select srvid, srvname from sysservers
srvid  srvname
-----  ----------
    0  SALES
    1  CORPORATE
    2  MARKETING
    3  PUBLICATIONS
    4 ENGINEERING
```

Le serveur SALES est local. Les autres serveurs sont distants.

L'instruction suivante affiche des informations sur les serveurs et les utilisateurs distants, enregistrées dans master..sysremotelogins :

```
select remoteserverid, remoteusername, suid
  from sysremotelogins
remoteserverid   remoteusername   suid
--------------   --------------   ------
1                joe              1
1                nancy            2
1                NULL             3
3                NULL             4
4                NULL             -1
```

En comparant la valeur de remoteserverid dans ce résultat avec la valeur de srvid dans le résultat précédent, vous pouvez déterminer le nom du serveur pour lequel remoteusername est correct. Par exemple, dans le premier résultat, srvid 1 indique le serveur CORPORATE et, dans le second résultat, remoteserverid 1 indique le même serveur. Les noms de login de l'utilisateur distant "joe" et "nancy" sont donc admis sur le serveur CORPORATE.

L'instruction suivante affiche les entrées dans master..syslogins :

```
select suid, name from syslogins
suid    name
------  ------------
    1   sa
    2   vp
    3   admin
    4   writer
```

Les résultats des trois requêtes indiquent que :

- le nom de l'utilisateur distant "joe" (suid 1) sur le serveur distant CORPORATE (srvid et remoteserverid 1) est associé au login "sa" (suid 1) ;
- le nom de l'utilisateur distant "nancy" (suid 2) sur le serveur distant CORPORATE (srvid et remoteserverid 1) est associé au login "vp" (suid 2) ;
- les autres logins du serveur CORPORATE (remoteusername "NULL") sont associés au login "admin" (suid 3) ;
- tous les logins du serveur PUBLICATIONS (srvid et remoteserverid 3) sont associés au login "writer" (suid 4) ;
- tous les logins du serveur ENGINEERING (srvid et remoteserverid 4) sont recherchés dans master..syslogins par leur nom d'utilisateur distant (suid -1) ;
- il n'existe pas d'entrée remoteserverid pour le serveur MARKETING dans sysremotelogins. De ce fait, les utilisateurs qui se connectent au serveur MARKETING ne peuvent pas exécuter d'appels de procédure à distance à partir de ce serveur.

Grâce aux procédures de correspondance pour les utilisateurs distants et à la possibilité de définir des autorisations sur les procédures stockées individuelles, vous contrôlez les accès des utilisateurs distants aux procédures locales. Par exemple, vous pouvez autoriser le login "vp" du serveur CORPORATE à exécuter certaines procédures locales et tous les autres logins de CORPORATE à exécuter les procédures pour lesquelles le login "admin" détient une autorisation.

**Remarque** Dans de nombreux cas, les mots de passe pour les utilisateurs sur le serveur distant doivent correspondre aux mots de passe sur le serveur local.

## Contrôle des mots de passe pour les utilisateurs distants

Le responsable de la sécurité du système dispose de sp_remoteoption pour déterminer si le contrôle des mots de passe est réalisé lorsque des utilisateurs distants se connectent au serveur local. Par défaut, les mots de passe sont vérifiés (mode "untrusted"). En mode trusted, le serveur local accepte les logins distants des autres serveurs et des applications frontales sans vérification de l'accès utilisateur pour le login concerné.

Utilisée avec des arguments, l'instruction sp_remoteoption change le mode pour l'utilisateur nommé. Respectez la syntaxe suivante :

sp_remoteoption [*serveur_distant*, *nom_login*, *nom_distant*, *nom_opt*, {true | false}]

Dans l'exemple suivant, le mode trusted est activé pour l'utilisateur "bob" :

```
sp_remoteoption GATEWAY, pogo, bob, trusted,
    true
```

## Effets de l'utilisation du mode non sécurisé

Les effets du mode "non sécurisé" dépendent du programme client de l'utilisateur. isql et certaines autres applications utilisateur requièrent que les logins aient le même mot de passe sur le serveur distant et sur le serveur local. Les applications Open Client™ peuvent être écrites de façon à autoriser les logins locaux à détenir des mots de passe distincts sur les différents serveurs.

Pour modifier votre mot de passe en mode "non sécurisé", vous devez d'abord le changer sur tous les systèmes distants auxquels vous avez accès, puis sur le serveur local. Cela est requis du fait du contrôle du mot de passe. Si vous commencez par changer votre mot de passe sur le serveur local, lorsque vous émettez l'appel de procédure à distance pour exécuter sp_password sur le serveur distant, votre mot de passe ne correspondra plus.

La syntaxe pour modifier le mot de passe sur le serveur distant est la suivante :

> *serveur_distant*...mot_de_passe_sp *mot_de_passe_appelant*, *nouveau_mot_de_passe*

Sur le serveur local, la syntaxe est la suivante :

> mot_de_passe_sp *mot_de_passe_appelant*, *nouveau_mot_de_passe*

Pour plus d'informations sur le changement de mot de passe, reportez-vous à la section "Changement des mots de passe", page 397.

# Recherche d'informations sur les logins distants

sp_helpremotelogin génère des informations sur les logins distants sur un serveur. Dans l'exemple suivant, le login distant "pogo" est associé localement au nom de login "bob", tous les autres logins distants conservant leur nom distant.

```
sp_helpremotelogin

server     remote_user_name     local_user_name      options
-------    ----------------     -----------------    --------
GATEWAY    **mapped locally**   **use local name**   untrusted
GATEWAY    pogo                 bob                  untrusted
```

# Paramètres de configuration pour les logins distants

Le tableau 13-2 répertorie les paramètres de configuration qui concernent les RPC. Tous ces paramètres de configuration sont définis via sp_configure et n'entrent en vigueur qu'au redémarrage d'Adaptive Server.

***Tableau 13-2 : Paramètres de configuration concernant les RPC***

| Paramètre de configuration | Valeur par défaut |
|---|---|
| allow remote access | 1 |
| number of remote logins | 20 |
| number of remote sites | 10 |
| number of remote connections | 20 |
| remote server pre-read packets | 3 |

## Autorisation des accès à distance

Pour autoriser l'accès à distance vers ou à partir d'un serveur, Backup Server compris, donnez à allow remote access la valeur 1 :

```
sp_configure "allow remote access", 1
```

Pour annuler l'autorisation d'accès à distance, à tout moment, définissez allow remote access sur la valeur 0 :

```
sp_configure "allow remote access", 0
```

Seul le responsable de la sécurité du système est habilité à définir le paramètre allow remote access.

**Remarque** Vous ne pouvez pas sauvegarder la base de données ni le journal de transactions si le paramètre allow remote access est défini sur la valeur 0.

## Contrôle du nombre de connexions utilisateur actives

Pour définir (set) le nombre de connexions utilisateur actives à partir de ce site vers les serveurs distants, utilisez number of remote logins. La commande suivante définit le paramètre number of remote logins sur 50 :

```
sp_configure "number of remote logins", 50
```

Seul l'administrateur système est habilité à définir le paramètre number of remote logins.

## Contrôle du nombre de sites distants

Pour contrôler le nombre de sites distants accessibles simultanément par un serveur, utilisez number of remote sites. Tous les accès à partir d'un site individuel sont gérés par un seul gestionnaire de site. Ce paramètre contrôle le nombre de gestionnaires de site, et non le nombre d'appels de procédures individuelles simultanées. Par exemple, si vous définissez number of remote sites sur 5 et que chaque site lance trois appels de procédures à distance, sp_who indique 5 processus de gestionnaire de site pour les 15 processus. Seul l'administrateur système est habilité à définir le nombre de sites distants.

## Contrôle du nombre de connexions à distance actives

Pour définir le nombre maximal de connexions distantes actives pouvant être établies dans les deux sens sur un serveur, utilisez le paramètre number of remote connections. Il contrôle les connexions effectuées depuis le serveur, ainsi que celles établies depuis des sites distants vers ce serveur. Seul l'administrateur système est habilité à définir le paramètre number of remote connections.

## Contrôle du nombre de paquets en lecture anticipée

Toutes les communications entre deux serveurs sont gérées par un seul gestionnaire de site afin de réduire le nombre de connexions requises. Ce gestionnaire peut effectuer une lecture anticipée des paquets de données et en assurer le suivi pour chaque processus utilisateur avant que le processus auquel ils sont destinés soit prêt.

Pour définir le nombre de paquets que le gestionnaire de site doit lire par avance, utilisez le paramètre remote server pre-read packets. La valeur par défaut est 3. Elle est appropriée dans tous les cas ; des valeurs plus élevées peuvent utiliser trop de mémoire. Seul un administrateur système est habilité à définir remote server pre-read packets. Pour plus d'informations, reportez-vous à la section "remote server pre-read packets", page 171.

CHAPITRE 14

# Utilisation de Kerberos, DCE et Windows NT LAN Manager

Ce chapitre décrit les services de sécurité basés sur le réseau vous permettant d'authentifier les utilisateurs et de protéger les données transmises d'une machine à l'autre sur un réseau.

Pour plus d'informations sur le mécanisme de sécurité SSL (Secure Socket Layer), reportez-vous au chapitre 9, "Administration de la sécurité".

Les sujets traités dans ce chapitre sont les suivants :



## Présentation

Dans un environnement client/serveur distribué, les utilisateurs non autorisés dans votre environnement informatique peuvent afficher ou modifier des données confidentielles. Adaptive Server fait appel à des fournisseurs tiers pour mettre à votre disposition des services de sécurité :

- l'authentification des utilisateurs, des clients et des serveurs afin de s'assurer de leur identité réelle ;

- la confidentialité des données par le biais du cryptage afin de s'assurer que les données ne peuvent pas être lues par un utilisateur non autorisé ;
- l'intégrité des données afin d'empêcher l'altération des données et de détecter les cas où cela se produit.

Le tableau 14-1 répertorie les mécanismes de sécurité supportés par Adaptive Server sur UNIX et les plates-formes PC :

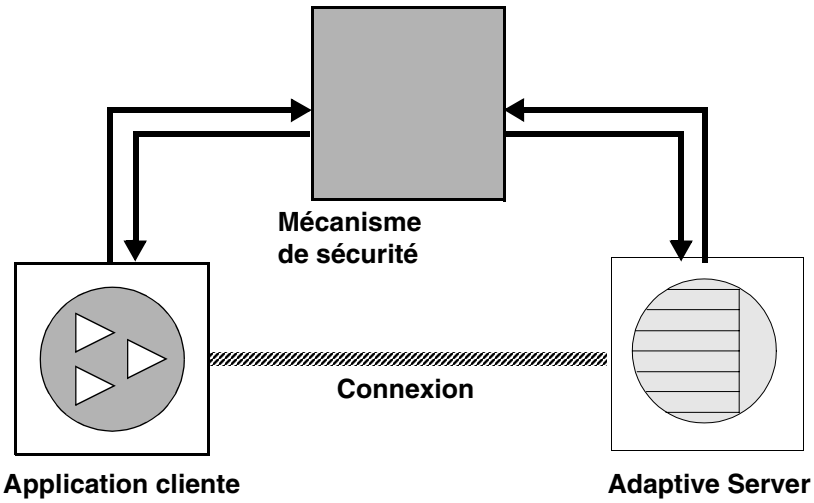
***Tableau 14-1 : Mécanismes de sécurité supportés par Adaptive Server***

| Plates-formes UNIX | Plates-formes PC |
|---|---|
| Environnement informatique distribué (DCE) | Windows NT LAN Manager |
| CyberSAFE Kerberos | |

## Utilisation des services de sécurité par les applications

L'illustration ci-dessous présente une application cliente utilisant un mécanisme de sécurité pour assurer des connexions sûres avec Adaptive Server.

***Figure 14-1 : Etablissement de connexions sécurisées entre un client et Adaptive Server***



Les connexions sécurisées entre un client et un serveur peuvent servir pour :

- l'authentification des logins,
- la protection des messages.

## Authentification des logins

Si un client demande des services d'authentification :

1 Le client valide le login avec le mécanisme de sécurité. Le mécanisme de sécurité renvoie une *accréditation*, contenant des informations pertinentes pour la sécurité.

2 Le client envoie l'accréditation à Adaptive Server.

3 Adaptive Server authentifie l'accréditation du client avec le mécanisme de sécurité. Si l'accréditation est correcte, une connexion sécurisée est établie entre le client et Adaptive Server.

## Protection des messages

Si le client demande des services de protection des messages :

1 Le client utilise le mécanisme de sécurité pour préparer le paquet de données à envoyer à Adaptive Server.

En fonction des services de sécurité demandés, le mécanisme de sécurité peut crypter les données ou créer une signature cryptée associée aux données.

2 Le client envoie le paquet de données à Adaptive Server.

3 Lorsqu'Adaptive Server reçoit le paquet de données, il utilise le mécanisme de sécurité pour le décryptage et la validation du paquet.

4 Adaptive Server renvoie les résultats au client à l'aide du mécanisme de sécurité afin d'exécuter les fonctions de sécurité demandées. Adaptive Server peut, par exemple, renvoyer les résultats sous forme cryptée.

## Services de sécurité et Adaptive Server

Selon le mécanisme de sécurité que vous choisissez, Adaptive Server vous permet d'utiliser un ou plusieurs des services de sécurité suivants :

- Unification des logins : authentifie les utilisateurs *une fois* sans leur demander d'indiquer leur nom et leur mot de passe à chaque connexion à Adaptive Server.
- Confidentialité des messages : cryptage des données qui transitent sur le réseau.
- Authentification réciproque : vérifie l'identité du client et du serveur. Cette procédure doit être demandée par le client et ne peut pas être imposée par Adaptive Server.
- Intégrité des messages : vérifie que les données transmises n'ont pas été modifiées.
- Détection par ré-exécution : vérifie que les données n'ont pas été interceptées par un intrus.
- Vérification de l'ordre : vérifie l'ordre des données transmises.
- Contrôles de l'origine des messages : vérifie l'origine du message.
- Sécurité des procédures distantes : établit l'authentification réciproque, la confidentialité des messages et l'intégrité des messages pour les transmissions de procédures distantes.

**Remarque** Il se peut que le mécanisme de sécurité que vous utilisez ne supporte pas tous ces services. Pour plus d'informations sur les services disponibles, reportez-vous à la section "Recherche d'informations relatives aux services de sécurité disponibles", page 567

# Administration de la sécurité réseau

Le tableau 14-2 présente une procédure globale d'utilisation des fonctions de sécurité réseau d'Adaptive Server. Vous devez installer Adaptive Server avant de suivre la procédure présentée dans le tableau 14-2.

***Tableau 14-2 : Procédure d'administration de la sécurité du réseau***

| Etape | Description | Voir |
|---|---|---|
| 1. Modifiez les fichiers de configuration :<br>• *libtcl.cfg*<br>• *objectid.dat*<br>• *interfaces* (ou Directory Service) | Modifiez le fichier *libtcl.cfg*.<br>Modifiez le fichier *objectid.dat*.<br>Modifiez le fichier *interfaces* ou Directory Service. | • "Paramétrage des fichiers de configuration pour la sécurité", page 538<br>• Le document *Open Client/Server – Manuel de configuration* pour votre plate-forme. |
| 2. Vérifiez que l'administrateur du mécanisme de sécurité a défini des logins pour tous les utilisateurs et pour Adaptive Server et Backup Server. | L'administrateur de la sécurité doit ajouter des noms et des mots de passe pour les utilisateurs et les serveurs dans le mécanisme de sécurité.<br>En environnement DCE, l'administrateur de la sécurité doit créer un fichier *keytab* pour les entrées du serveur. | • La documentation fournie avec votre mécanisme de sécurité.<br>• "Identification des utilisateurs et des serveurs dans le mécanisme de sécurité", page 545 |
| 3. Configurez la sécurité de votre installation. | Utilisez sp_configure. | "Configuration d'Adaptive Server pour la sécurité", page 546 |
| 4. Redémarrez Adaptive Server. | Active le paramètre use security services. | "Redémarrage du serveur pour activer les services de sécurité", page 551 |
| 5. Ajoutez des logins dans Adaptive Server pour le support des connexions à l'échelle de l'entreprise. | Ajoutez des utilisateurs à l'aide de sp_addlogin. Vous pouvez également spécifier un login sécurisé à l'aide de sp_configure. | "Ajout de logins pour supporter l'unification des logins", page 553 |
| 6. Déterminez le modèle de sécurité pour les procédures à distance et configurez les serveurs locaux et distants pour la sécurité RPC. | Utilisez sp_serveroption pour choisir le modèle de sécurité (A ou B). | "Etablissement de la sécurité pour les procédures à distance", page 555 |

| Etape | Description | Voir |
|---|---|---|
| 7. Connectez-vous au serveur et utilisez les services de sécurité. | Utilisez isql_dce ou isql_r (si vous utilisez les services de bibliothèques ou les services de sécurité DCE) ou Open Client Client-Library pour vous connecter à Adaptive Server, en spécifiant les services de sécurité à utiliser. | • "Connexion au serveur et utilisation des services de sécurité", page 563<br>• Le document *Open Client/Server – Manuel de configuration* pour votre plate-forme.<br>• Section "Security Features" du manuel *Open Client Client-Library Reference Manual.* |
| 8. Vérifiez les services de sécurité et les mécanismes de sécurité disponibles. | Utilisez les fonctions show_sec_services et is_sec_services_on pour vérifier les services de sécurité disponibles.<br>Pour obtenir la liste des mécanismes de sécurité et de leurs services de sécurité supportés par Adaptive Server, utilisez la commande select pour transmettre une requête dans la table système syssecmechs. | "Recherche d'informations relatives aux services de sécurité disponibles", page 567 |

# Paramétrage des fichiers de configuration pour la sécurité

Les fichiers de configuration sont créés lors de l'installation à un emplacement par défaut dans la structure de répertoires de Sybase. Le tableau 14-3 présente les fichiers de configuration nécessaires à l'utilisation de la sécurité réseau.

***Tableau 14-3 : Noms et emplacements des fichiers de configuration***

| Nom de fichier | Description | Emplacement |
|---|---|---|
| *libtcl.cfg* | Le fichier de configuration des gestionnaires contient des informations relatives aux gestionnaires de répertoire, de sécurité et de réseau, ainsi que des informations sur l'initialisation. | Plates-formes UNIX : *$SYBASE/config*<br><br>Plates-formes PC : *SYBASE_home\ini* |

| Nom de fichier | Description | Emplacement |
|---|---|---|
| *objectid.dat* | Ce fichier d'identificateurs d'objets établit des correspondances entre les noms des identificateurs d'objets globaux et les noms locaux pour le jeu de caractères, la séquence de tri et les mécanismes de sécurité. | Plates-formes UNIX : *$SYBASE/config*<br><br>Plates-formes PC : *SYBASE_home\ini* |
| UNIX : *interfaces*<br><br>Plates-formes PC : sql.ini | Le fichier d'interface contient des informations relatives aux connexions et à la sécurité pour chaque serveur figurant dans la liste.<br><br>**Remarque** Dans cette version, vous pouvez utiliser un service de répertoire au lieu du fichier d'interface. | Plates-formes UNIX : *$SYBASE*<br><br>Plates-formes PC : *SYBASE_home\ini* |

Pour plus d'informations sur les fichiers de configuration, reportez-vous au document *Open Client/Server Configuration Guide* de votre plate-forme.

## Préparation de *libtcl.cfg* pour utiliser la sécurité réseau

*libtcl.cfg* contient des informations relatives aux trois types de gestionnaires :

- Réseau (Net-Library)
- Services de répertoire
- Sécurité

Un **gestionnaire** est une bibliothèque Sybase qui met à votre disposition une interface vers un fournisseur de services externe. Les gestionnaires sont chargés de manière dynamique afin que vous puissiez changer le gestionnaire utilisé par une application sans avoir à modifier l'application.

### Entrées de gestionnaires de réseau

La syntaxe d'une entrée de gestionnaire de réseau est la suivante :

*gestionnaire=protocole description*

où :

- *gestionnaire* représente le nom du gestionnaire de réseau,
- *protocole* le nom du protocole réseau,

- *description* la description de l'entrée (ce paramètre est facultatif).

**Remarque** Si vous ne spécifiez pas de gestionnaire de réseau, le système utilise automatiquement un gestionnaire approprié pour votre application et votre plate-forme. Par exemple, pour les plates-formes UNIX, un gestionnaire peut gérer des threads sélectionnés automatiquement lors de d'utilisation des services de sécurité.

## Entrées de services de répertoire

Les entrées de services de répertoire sont prises en compte lorsque vous utilisez les services de répertoire à la place du fichier d'interface. Pour plus d'informations sur les entrées de répertoire, reportez-vous au Manuel de configuration pour votre plate-forme et au document *Open Client/Server Configuration Guide* de votre plate-forme.

## Entrées des gestionnaires de sécurité

La syntaxe d'une entrée de gestionnaire de sécurité est la suivante :

*fournisseur=gestionnaire chaîne_init*

où :

- *fournisseur* représente le nom local du mécanisme de sécurité. Le mappage du nom local vers un identificateur d'objet global est défini dans le fichier *objectid.dat*.

  Les noms locaux par défaut sont les suivants :

  - "dce", pour le mécanisme de sécurité DCE,
  - "csfkrb5", pour le mécanisme de sécurité CyberSAFE Kerberos,
  - "LIBSMSSP", pour Windows LAN Manager sous Windows NT ou Windows 95 (clients uniquement).

  Si vous utilisez un nom de mécanisme autre que le nom par défaut, vous devez changer le nom local dans le fichier objectid.dat (pour un exemple, reportez-vous à la section "Le fichier objectid.dat", page 543)

- *gestionnaire* représente le nom du gestionnaire de sécurité. L'emplacement par défaut de tous les gestionnaires pour la plate-forme UNIX est *$SYBASE/lib*. L'emplacement par défaut pour les plates-formes PC est SYBASE_home\dll.

- *chaîne_init* est une chaîne d'initialisation pour le gestionnaire. (ce paramètre est facultatif). La valeur de *chaîne_init* varie en fonction des gestionnaires :
  - Pour le gestionnaire DCE, la syntaxe de la *chaîne_init* est la suivante :

    secbase=/.../*nom_cellule*

    où *nom_cellule* correspond au nom de votre cellule DCE.
  - Pour le gestionnaire CyberSAFE Kerberos, la syntaxe de la *chaîne_init* est la suivante :

    secbase=@*domaine*

    où *domaine* correspond au nom de domaine CyberSAFE Kerberos par défaut.
  - Pour Windows NT LAN Manager, *chaîne_init* ne s'applique pas.

## Informations relatives à la plate-forme UNIX

Cette section contient des informations spécifiques aux plates-formes UNIX. Pour plus d'informations, reportez-vous au document *Open Client/Server Configuration Guide*.

Pour les plates-formes UNIX, il n'y a pas d'outil de modification du fichier *libtcl.cfg* disponible. Utilisez votre éditeur habituel pour placer ou supprimer des commentaires dans les entrées figurant déjà dans le fichier après l'installation d'Adaptive Server.

Après l'installation d'Adaptive Server sur une plate-forme UNIX, le fichier *libtcl.cfg* contient déjà des entrées pour les trois sections du fichier :

- [DRIVERS]
- [DIRECTORY]
- [SECURITY]

Ces sections ne sont pas tenues d'apparaître dans un ordre spécifique.

Assurez-vous que les entrées à ne pas utiliser sont commentées (elles commencent par ";") et que les entrées à utiliser ne contiennent pas de commentaire (elles ne commencent pas par ";").

#### Exemple de fichier *libtcl.cfg* pour Sun Solaris

```
[DRIVERS]
;libtli.so=tcp unused ; This is the non-threaded tli driver.
;libtli_r.so=tcp unused ; This is the threaded tli driver.


[DIRECTORY]
;dce=libddce.so ditbase=/.:/subsys/sybase/dataservers
;dce=libddce.so ditbase=/.:/users/cfrank

[SECURITY]
dce=libsdce.so secbase=/.../svrsole4_cell
```

Le fichier *libtcl.cfg* est configuré de manière à utiliser le service de sécurité DCE. Notez que ce fichier n'utilise par les services de répertoire car toutes les entrées de section [DIRECTORY] sont commentées.

Comme toutes les entrées de la section [DRIVERS] des gestionnaires de réseau sont aussi commentées, le système choisit automatiquement les gestionnaires appropriés. Le système sélectionne automatiquement un gestionnaire utilisant des threads lorsque des services de sécurité sont utilisés et un gestionnaire sans thread pour les applications qui ne peuvent pas utiliser de tels gestionnaires. Par exemple, Backup Server ne supporte pas des services de sécurité et n'emploie pas de gestionnaire utilisant des threads.

## Informations relatives aux plates-formes PC

Cette section contient des informations spécifiques aux plates-formes PC. Pour plus d'informations, reportez-vous au document *Open Client/Server Configuration Guide*.

Modifiez le fichier *libtcl.cfg* à l'aide de l'utilitaire ocscfg. Pour savoir comment utiliser ocscfg, reportez-vous au document *Open Client/Server Configuration Guide*.

L'utilitaire ocscfg crée automatiquement des en-têtes de section pour le fichier *libtcl.cfg*.

#### Exemple de fichier *libtcl.cfg* pour les plates-formes PC

```
[NT_DIRECTORY]
ntreg_dsa=LIBDREG
ditbase=software\sybase\serverdsa

[DRIVERS]
```

```
NLWNSCK=TCP  Winsock TCP/IP Net-Lib driver
NLMSNMP=NAMEPIPE  Named Pipe Net-Lib driver
NLNWLINK=SPX  NT NWLINK SPX/IPX Net-Lib driver
NLDECNET=DECNET  DecNET Net-Lib driver

[SECURITY]
NTLM=LIBSMSSP
```

## Le fichier *objectid.dat*

Le fichier objectid.dat mappe les identificateurs d'objets, comme celui du service DCE ("1.3.6.1.4.1.897.4.6.1"), vers les noms locaux comme "dce". Ce fichier contient des sections telles que [CHARSET], pour les jeux de caractères, et [SECURITY], pour les services de sécurité. C'est cette dernière qui nous intéresse ici. Voici un exemple de fichier objectid.dat :

```
[secmech]
        1.3.6.1.4.1.897.4.6.1   = dce
        1.3.6.1.4.1.897.4.6.3   = NTLM
        1.3.6.1.4.1.897.4.6.6   = csfkrb5
```

Ce fichier ne doit être modifié que si vous changez le nom local du service de sécurité dans le fichier *libtcl.cfg*. Pour modifier ce fichier, utilisez n'importe quel éditeur de texte.

Par exemple, si vous avez changé

```
[SECURITY]
dce=libsdce.so secbase=/.../svrsole4_cell
```

en

```
[SECURITY]
dce_group=libsdce.so secbase=/.../svrsole4_cell
```

dans *libtcl.cfg*, vous devez modifier le fichier objectid.dat afin de répercuter le changement. Ne changez que le nom local dans la ligne concernant le DCE dans objectid.dat :

```
1.3.6.1.4.1.897.4.6.1   = dce_group
```

---

**Remarque** Vous ne pouvez spécifier qu'un seul nom local par mécanisme de sécurité.

---

## Spécification d'informations de sécurité pour le serveur

Vous pouvez choisir d'utiliser un fichier *interfaces* ou un *service de répertoire* pour obtenir des informations sur les serveurs de votre installation.

Le fichier d'interface contient des informations de réseau et de sécurité pour les serveurs. Si vous envisagez l'utilisation de services de sécurité, le fichier d'interface doit inclure une ligne "secmech" qui indique les identificateurs des services de sécurité que vous prévoyez d'utiliser.

Au lieu d'utiliser le fichier d'interface, Adaptive Server supporte des services de répertoire pour garder la trace des informations relatives aux serveurs. Le service de répertoire assure la gestion de la création, de la modification et de la recherche d'informations relatives aux serveurs réseau. L'avantage d'utiliser un service de répertoire est que vous n'avez pas à mettre à jour plusieurs fichiers d'interface en cas d'ajout d'un nouveau serveur au réseau ou en cas de déplacement d'un serveur vers une nouvelle adresse. Si vous envisagez d'utiliser des services de sécurité avec un service de répertoire, vous devez définir l'attribut de sécurité secmech. Il doit pointer vers un ou plusieurs identificateurs des services de sécurité que vous prévoyez d'utiliser.

### Outils UNIX permettant de spécifier le mécanisme de sécurité

Pour spécifier le ou les mécanismes de sécurité à utiliser :

- Si vous utilisez le fichier interfaces, faites appel à l'utilitaire dscp.
- Si vous utilisez un service de répertoire, faites appel à l'utilitaire dscp_r ou dscp_dce.

**Remarque** L'outil dsedit, qui permet de créer des entrées pour le fichier interfaces ou pour un service de répertoire, est disponible pour les plates-formes UNIX. Cependant, il ne supporte pas la création des entrées secmech des mécanismes de sécurité.

Pour plus d'informations sur dscp, reportez-vous au document *Open Client/Server - Manuel de configuration pour plates-formes UNIX*.

### Outils PC permettant de spécifier les attributs du serveur

Pour placer des informations relatives aux serveurs pour votre installation dans le fichier sql.ini ou dans un service de répertoire, utilisez l'utilitaire dsedit. Cet utilitaire offre une interface utilisateur graphique permettant de spécifier les attributs de serveur, tels que la version et le nom du serveur, ou le mécanisme de sécurité. Comme attribut du mécanisme de sécurité, vous pouvez spécifier un ou plusieurs identificateurs d'objets pour les mécanismes de sécurité que vous envisagez d'utiliser. Pour plus d'informations sur l'utilisation de dsedit, reportez-vous au document *Open Client/Server - Manuel de configuration pour plates-formes PC*.

## Identification des utilisateurs et des serveurs dans le mécanisme de sécurité

L'administrateur du mécanisme de sécurité doit définir les *"principaux"* qui comprend à la fois les utilisateurs et les serveurs du mécanisme de sécurité. Le tableau 14-4 répertorie les outils servant à ajouter des utilisateurs et des serveurs.

***Tableau 14-4 : Définition des utilisateurs et des serveurs dans le mécanisme de sécurité***

| Mécanisme de sécurité | Commande ou outil |
|---|---|
| DCE | Pour créer un utilisateur ou un serveur principal, utilisez la commande user create de l'outil DCE dcecp. Utilisez également la commande keytab create pour créer un fichier keytab DCE qui contient le mot de passe de l'utilisateur ou du serveur principal sous forme cryptée.<br>Lorsque vous définissez un serveur comme DCE, utilisez les options de commande qui spécifient que le "principal" peut servir de serveur. |
| CyberSAFE Kerberos | Utilisez la commande add de l'utilitaire kadmin CyberSAFE. Pour créer une clé dans le fichier keytab du serveur CyberSAFE Kerberos, utilisez également l'utilitaire kadmin avec la commande ext.<br>Lorsque vous définissez un serveur comme CyberSAFE Kerberos, utilisez les options de commande qui spécifient que le "principal" peut servir de serveur. |
| Windows NT LAN Manager | Exécutez l'outil User Manager pour définir les utilisateurs dans Windows NT LAN Manager. Veillez à définir le nom Adaptive Server comme utilisateur de Windows NT LAN Manager et à donner ce nom à Adaptive Server lors du démarrage de ce dernier. |

**Remarque** Dans un environnement de production, vous devez contrôler l'accès aux fichiers contenant les clés des serveurs et des utilisateurs. Si les utilisateurs peuvent accéder aux clés, ils peuvent créer un serveur qui emprunte l'identité de votre serveur.

Pour plus d'informations sur la manière de réaliser des tâches d'administration, reportez-vous à la documentation, disponible auprès des fournisseurs tiers, pour le mécanisme de sécurité.

# Configuration d'Adaptive Server pour la sécurité

Adaptive Server comprend plusieurs paramètres de configuration pour l'administration de la sécurité réseau. Ces paramètres doivent être définis par un responsable de la sécurité du système. Tous les paramètres de la sécurité réseau entrent dans le groupe des paramètres de configuration "security related".

Les paramètres de configuration servent à :

- activer la sécurité réseau ;
- demander l'unification des logins ;
- demander la confidentialité des messages avec le cryptage des données ;
- demander un ou plusieurs services de sécurité de messages.

## Activation de la sécurité réseau

Pour activer ou désactiver la sécurité réseau, définissez le paramètre de configuration use security services à l'aide de sp_configure. Pour activer la sécurité réseau, donnez la valeur 1 à ce paramètre. Si ce paramètre vaut 0 (valeur par défaut), les services de sécurité réseau ne sont pas disponibles. La syntaxe est la suivante :

```
sp_configure "use security services", [0|1]
```

Pour activer les services de sécurité, par exemple, exécutez :

```
sp_configure "use security services", 1
```

**Remarque** Ce paramètre de configuration est statique, aussi devez-vous redémarrer Adaptive Server pour qu'il soit appliqué. Pour plus d'informations, reportez-vous à la section "Redémarrage du serveur pour activer les services de sécurité", page 551

## Utilisation de l'unification des logins

Les paramètres de configuration servent à :

- activer l'unification des logins ;
- définir un login sécurisé par défaut.

Tous les paramètres d'unification des logins sont appliqués immédiatement. Ces paramètres doivent être définis par un responsable de la sécurité du système.

### Unification des logins

Pour établir que tous les utilisateurs soient déjà authentifiés par un mécanisme de sécurité, définissez le paramètre de configuration unified login required sur 1. Si ce paramètre vaut 0 (valeur par défaut), Adaptive Server accepte tout aussi bien les noms de login et les mots de passe classiques que les accréditations déjà authentifiées. La syntaxe est la suivante :

```
sp_configure "unified login required", [0|1]
```

Par exemple, pour que toutes les connexions soient authentifiées par un mécanisme de sécurité, entrez la commande suivante :

```
sp_configure "unified login required", 1
```

## Définition d'un login sécurisé par défaut

Lorsqu'un utilisateur avec une accréditation correcte d'un mécanisme de sécurité se connecte à Adaptive Server, le serveur vérifie si le nom d'utilisateur existe dans master..syslogins. Si c'est le cas, Adaptive Server l'utilise. Par exemple, si un utilisateur se connecte au mécanisme de sécurité DCE en tant que "ralph" et que le nom "ralph" figure dans master..syslogins, Adaptive Server utilise tous les rôles et les autorisations définis pour "ralph" sur le serveur.

Cependant, si un utilisateur avec une accréditation correcte se connecte à Adaptive Server, mais est inconnu sur le serveur, le login est accepté uniquement si *secure default login* est défini avec sp_configure. Adaptive Server utilise le login par défaut pour tout utilisateur défini dans master..syslogins mais qui est préauthentifié par un mécanisme de sécurité. La syntaxe est la suivante :

```
sp_configure "secure default login", 0, nom_login
```

La valeur par défaut de secure default login est "guest".

Ce login doit être un login correct dans master..syslogins. Par exemple, si vous voulez définir "gen_auth" comme login par défaut, procédez comme suit :

1 Ajoutez le login dans Adaptive Server à l'aide de sp_addlogin :

```
sp_addlogin gen_auth, pwgenau
```

Cette procédure définit que le mot de passe est "pwgenau".

2 Définissez le login comme login sécurisé par défaut à l'aide de sp_configure :

```
sp_configure "secure default login", 0, gen_auth
```

Adaptive Server utilise ce login pour un utilisateur préauthentifié par un mécanisme de sécurité mais inconnu d'Adaptive Server.

---

**Remarque** Plusieurs utilisateurs peuvent prendre en compte le suid associé au login par défaut sécurisé. Par conséquent, vous pouvez activer les fonctions d'audit pour toutes les opérations effectuées par les utilisateurs connectés sous le login par défaut. Pour ajouter tous les utilisateurs au serveur, vous pouvez également envisager d'utiliser sp_addlogin.

---

Pour plus d'informations sur les logins, reportez-vous aux sections "Ajout de logins pour supporter l'unification des logins", page 553 et "Ajout de logins à Adaptive Server", page 372

## Mappages des noms de login des mécanismes de sécurité vers les noms de serveur

Certains mécanismes de sécurité peuvent autoriser des noms incorrects dans Adaptive Server. Par exemple, les noms comportant plus de 30 caractères ou des caractères spéciaux (!, %, * et &) ne respectent pas les conventions de dénomination d'Adaptive Server. Tous les logins Adaptive Server doivent être des identificateurs corrects. Pour plus d'informations sur les identificateurs corrects, reportez-vous au chapitre 7, "Expressions, identificateurs et caractères joker", du *Manuel de référence d'Adaptive Server*.

Le tableau 14-5 indique les caractères non admis par Adaptive Server et leur correspondance :

***Tableau 14-5 : Conversion des caractères incorrects dans les noms de login***

| Caractères non admis | Conversion |
|---|---|
| Perluète (&) | Trait de soulignement (_) |
| Apostrophe (') | |
| Barre oblique inverse (\) | |
| Deux-points (:) | |
| Virgule (,) | |
| Signe égal (=) | |
| Guillemet gauche (') | |
| Pourcentage (%) | |
| Signe supérieur à (>) | |
| Guillemet droit (') | |
| Tilde (~) | |
| Caret (^) | Signe dollar ($) |
| Accolades ({ }) | |
| Point d'exclamation (!) | |
| Signe inférieur à (<) | |
| Parenthèses ( ) | |
| Point (.) | |
| Point d'interrogation (?) | |

| Caractères non admis | Conversion |
|---|---|
| Astérisque (*) | Dièse (#) |
| Signe moins (–) | |
| Barre verticale (\|) | |
| Signe plus (+) | |
| Guillemets droits (") | |
| Point-virgule (;) | |
| Barre oblique (/) | |
| Crochets ([ ]) | |

## Confidentialité des messages avec le cryptage des données

Pour que tous les messages qui se trouvent dans Adaptive Server ou qui en proviennent soient cryptés, donnez au paramètre de configuration msg confidentiality reqd la valeur 1. Si ce paramètre vaut 0 (valeur par défaut), la confidentialité des messages n'est pas requise mais elle peut être établie par le client.

La syntaxe de ce paramètre est la suivante :

```
sp_configure paramètre_configuration, [0 | 1]
```

Pour demander, par exemple, que tous les messages soient cryptés, exécutez :

```
sp_configure "msg confidentiality reqd", 1
```

## Intégrité des données garantie

Adaptive Server vous permet d'utiliser ces paramètres de configuration pour demander la verification de différents types d'intégrité des données pour tous les messages :

- msg integrity reqd : donnez à ce paramètre la valeur 1 pour demander que l'altération générale éventuelle soit vérifiée dans tous les messages. Si ce paramètre vaut 0 (valeur par défaut), l'intégrité des messages n'est pas requise mais elle peut être demandée par le client si le mécanisme de sécurité la supporte.

### Mémoire nécessaire pour la sécurité réseau

Allouez approximativement 2 ko de mémoire supplémentaire par connexion sécurisée. La valeur du paramètre de configuration max total_memory indique la quantité de mémoire requise par Adaptive Server au démarrage. Par exemple, si votre serveur utilise des pages logiques de 2 ko et si vous estimez que le nombre maximal de connexions sécurisées simultanées est de 150, augmentez la valeur du paramètre max total_memory de 150, ce qui a pour effet d'augmenter la mémoire allouée de 150 blocs de 2 Ko.

La syntaxe est la suivante :

sp_configure "max total_memory", *valeur*

Par exemple, si Adaptive Server requiert un espace mémoire total de 75 000 blocs de 2 Ko, utilisez la commande suivante :

```
sp_configure "max total_memory", 75000
```

Pour plus d'informations sur l'estimation et la spécification de la mémoire nécessaire, reportez-vous au chapitre 18, "Configuration de la mémoire"..

## Redémarrage du serveur pour activer les services de sécurité

Une fois que vous avez configuré les services de sécurité, redémarrez Adaptive Server.

Pour Windows NT, reportez-vous à la documentation qui traite de la configuration de votre plate-forme.

Pour les plates-formes UNIX, notez que :

- Après avoir terminé l'installation d'Adaptive Server, votre fichier runserver contient un appel de l'utilitaire dataserver permettant de lancer Adaptive Server.
- Il existe deux versions de l'utilitaire dataserver : dataserver_dce et dataserver. De même, il existe deux versions de diagserver : diagserver_dce et diagserver. L'utilitaire utilisé dépend de la plate-forme utilisée :

  - Pour les plates-formes Sun Solaris, utilisez dataserver_dce si vous avez l'intention d'utiliser des services de sécurité et dataserver dans le cas contraire.
  - Pour les plates-formes HP et RS/6000, utilisez dataserver ou diagserver. Vous pouvez utiliser un binaire unique, que vous utilisiez des services de sécurité ou non.

- Si vous utilisez le service de sécurité DCE, veillez à définir le fichier keytab. Vous pouvez spécifier l'option -K avec dataserver_dce pour spécifier l'emplacement du fichier keytab. Si vous ne spécifiez pas d'emplacement, Adaptive Server considère que le fichier se trouve dans $SYBASE/config/$DSLISTEN_key. Vous avez la possibilité, mais cela est facultatif, d'indiquer l'emplacement comme suit :

  ```
  $SYBASE/bin/dataserver_dce -Stest4 -dd_master
     -K/opt/dcelocal/keys/test4_key
  ```

  Cette commande dataserver_dce démarre le serveur à l'aide du device master d_master et du fichier keytab stocké dans */opt/dcelocal/keys/test4_key*.

  Si vous utilisez l'emplacement par défaut pour keytab et que $DSLISTEN correspond à la valeur de votre serveur (test4), vous pouvez exécutez la commande suivante :

  ```
  $SYBASE/bin/dataserver_dce -dd_master
  ```

  Ensuite, Adaptive Server cherche le fichier keytab dans $SYBASE/config/test4_key.

  Pour plus d'informations sur la configuration du fichier keytab pour DCE, reportez-vous à la documentation d'administration DCE.

## Détermination des mécanismes de sécurité à supporter

use security services vaut 0 et Adaptive Server supporte les mécanismes de sécurité.

Si use security services vaut 1, Adaptive Server supporte un mécanisme de sécurité lorsque les deux conditions sont vraies :

- L'identificateur global du mécanisme de sécurité figure dans le fichier d'interface ou dans le service de répertoire.
- L'identificateur global est mappé dans *objectid.dat* vers un nom local qui se trouve dans *libtcl.cfg*.

Pour plus d'informations sur la manière dont Adaptive Server détermine le mécanisme de sécurité à utiliser pour un client donné, reportez-vous à la section "Utilisation des mécanismes de sécurité pour le client", page 566

## Ajout de logins pour supporter l'unification des logins

Lorsque les utilisateurs se connectent à Adaptive Server avec une accréditation préauthentifiée, Adaptive Server :

1 Vérifie si l'utilisateur est défini dans la table master..syslogins. Si l'utilisateur figure dans master..syslogins, Adaptive Server accepte le login sans demander de mot de passe.

2 Si le nom d'utilisateur ne figure pas dans master..syslogins, Adaptive Server vérifie si un login par défaut sécurisé a été défini. Si c'est le cas, l'utilisateur est connecté sous ce login. Si aucun login par défaut n'a été défini, Adaptive Server refuse le login.

Par conséquent, déterminez si vous souhaitez autoriser uniquement les connexions des utilisateurs disposant d'un login défini dans Adaptive Server ou celles de tous les utilisateurs avec le login par défaut. Pour définir le login par défaut, vous devez ajouter le login par défaut dans master..syslogins et utiliser sp_configure. Pour plus de détails, reportez-vous à la section "Définition d'un login sécurisé par défaut", page 548

## Procédure générale d'ajout de logins

Suivez la procédure générale décrite dans le tableau 14-6 pour ajouter des logins au serveur et, de manière facultative, pour ajouter des utilisateurs à une ou plusieurs bases de données avec les rôles appropriés et les autorisations sur une ou plusieurs bases de données.

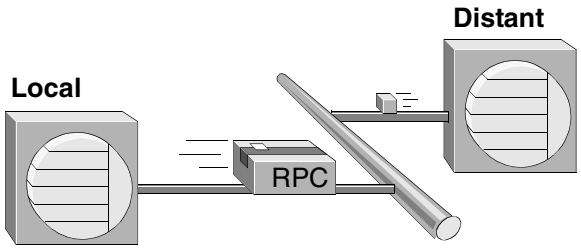
***Tableau 14-6 : Ajout de logins et définition de droits d'accès aux bases de données***

| Tâche | Rôle requis | Commande ou procédure | Voir |
|---|---|---|---|
| 1. Ajouter un login pour un utilisateur. | Responsable de la sécurité du système | sp_addlogin | "Ajout de logins à Adaptive Server", page 372 |
| 2. Ajouter l'utilisateur dans une ou plusieurs bases de données. | Administrateur système ou propriétaire de la base de données | sp_adduser<br>Exécutez cette procédure depuis la base de données. | "Ajout d'utilisateurs aux bases de données", page 375 |
| 3. Ajouter l'utilisateur à un groupe d'une base de données. | Administrateur système ou propriétaire de la base de données | sp_changegroup<br>Exécutez cette procédure depuis la base de données. | • "Modification des appartenances d'utilisateur à un groupe", page 399<br>• sp_changegroup dans le *Manuel de référence d'Adaptive Server* |
| 4. Octroyer des rôles système à l'utilisateur. | Responsable de la sécurité du système ou administrateur système | grant role | • "Création et attribution de rôles aux utilisateurs", page 382<br>• grant dans le *Manuel de référence d'Adaptive Server* |
| 5. Créer des rôles définis par l'utilisateur et octroyer des rôles aux utilisateurs. | Responsable de la sécurité du système | create role<br>grant role | • "Création et attribution de rôles aux utilisateurs", page 382 dans le *Manuel de référence d'Adaptive Server*<br>• grant dans le Manuel de référence d'Adaptive Server<br>• create role dans le *Manuel de référence d'Adaptive Server* |
| 6. Octroyer des accès aux objets de base de données. | Propriétaires d'objets de base de données | | chapitre 11, "Gestion des autorisations utilisateur" |

# Etablissement de la sécurité pour les procédures à distance

Adaptive Server agit comme client lorsqu'il se connecte à un autre serveur pour exécuter un appel de procédure à distance (RPC) comme l'illustre la figure 14-2.

***Figure 14-2 : Adaptive Server agissant comme client pour exécuter un RPC***




Une connexion *physique* est établie entre les deux serveurs. Les serveurs utilisent la connexion physique pour établir une ou plusieurs connexions *logiques* (une connexion logique par RPC).

Adaptive Server 11.5 et supérieur supporte deux modèles de sécurité pour les RPC : *modèle de sécurité A* et *modèle de sécurité B*.

## Modèle de sécurité A

Pour le modèle de sécurité A, Adaptive Server ne supporte pas les services de sécurité comme la confidentialité des messages via le cryptage entre les deux serveurs. Le modèle de sécurité A est la valeur par défaut.

## Modèle de sécurité B

Avec le modèle de sécurité B, l'Adaptive Server local obtient une accréditation par le mécanisme de sécurité et l'utilise pour établir une connexion physique sûre avec l'Adaptive Server distant. Avec ce modèle, vous pouvez utiliser un ou plusieurs des services de sécurité suivants :

- Authentification réciproque : le serveur local authentifie le serveur distant en extrayant son accréditation et en la vérifiant à l'aide du mécanisme de sécurité. Grâce à ce service, les accréditations des deux serveurs sont authentifiées et vérifiées.

- Confidentialité des messages via le cryptage : les messages envoyés au serveur distant et les réponses reçues de ce dernier sont cryptés.
- Intégrité des messages : les messages échangés entre les serveurs sont soumis à des tests d'intégrité.

## Unification des logins et modèles de procédures à distance

Si le serveur local et le serveur distant sont configurés de manière à utiliser des services de sécurité, vous pouvez utiliser l'unification des logins sur les deux serveurs avec *l'un ou l'autre* de ces modèles, à l'aide de l'une de ces deux méthodes :

- Le responsable de la sécurité du système définit un utilisateur comme "sécurisé" avec sp_remoteoption sur le serveur distant. Avec cette méthode, un mécanisme de sécurité comme DCE authentifie l'utilisateur et le mot de passe. L'utilisateur accède au serveur local via "l'unification des login" et exécute un RPC sur le serveur distant. L'utilisateur est habilité sur le serveur distant et ne nécessite pas de mot de passe.
- Un utilisateur spécifie un mot de passe pour le serveur distant lorsqu'il se connecte au serveur local. Le fonction permettant de spécifier un mot de passe pour le serveur distant se trouve dans la routine ct_remote_pwd accompagnant Open Client Client-Library/C. Pour plus d'informations sur cette routine, reportez-vous au document *Open Client Client-Library/C Reference Manual*.

## Etablissement du modèle de sécurité pour les RPC

Pour établir le modèle de sécurité pour les RPC, utilisez sp_serveroption. La syntaxe est la suivante :

sp_serveroption *serveur, nom_option,* [true | false]

Pour établir le modèle de sécurité, définissez *nom_option* sur la valeur rpc security model A ou rpc security model B. *serveur* désigne le serveur distant.

Par exemple, pour définir le modèle B pour le serveur distant TEST3, exécutez la commande suivante :

```
sp_serveroption test3, "rpc security model B", true
```

Le modèle par défaut est "A", c'est-à-dire que les appels de procédures à distance sont gérés de la même manière que dans la version précédente. Il n'est pas nécessaire de définir d'option de serveur pour le modèle A.

## Définition des options de serveur pour le modèle de sécurité B pour les RPC

Pour le modèle de sécurité B pour les RPC, vous pouvez définir des options avec la procédure système sp_serveroption. La syntaxe est la suivante :

sp_serveroption *serveur, nom_option,* optvalue

où :

- *serveur* désigne le serveur distant.
- *nom_option* désigne l'option. Les valeurs possibles sont les suivantes :
  - security mechanism : nom du mécanisme de sécurité à utiliser lors de l'exécution d'un RPC sur un serveur distant.
  - mutual authentication : définissez cette option à 1 pour que l'Adaptive Server local authentifie et vérifie le serveur distant. Si ce paramètre vaut 0 (valeur par défaut), le serveur distant vérifie toujours le serveur local lorsqu'il envoie un RPC mais le serveur local ne vérifie par la validité du serveur distant.
  - use message confidentiality : définissez cette option à 1 pour que tous les messages des RPC soient cryptés lorsqu'ils sont envoyés au serveur distant et reçus du serveur distant. Si ce paramètre vaut 0 (valeur par défaut), les données des RPC ne seront pas cryptées.
  - use message integrity : définissez cette option à 1 pour que l'altération éventuelle soit vérifiée pour tous les messages de RPC. Si ce paramètre vaut 0 (valeur par défaut), l'altération éventuelle des données RPC n'est pas vérifiée.
- *valeur_option* doit prendre la valeur "true" pour toutes les valeurs de *nom_option*, *sauf* security mechanism. Si l'option que vous définissez est security mechanism, indiquez le nom du mécanisme de sécurité. Pour trouver la liste des mécanismes de sécurité, exécutez la commande :

```
select * from syssecmechs
```

Pour plus d'informations sur la table système syssecmechs, reportez-vous à la section "Détermination des services de sécurité activés", page 568

Par exemple, pour configurer le serveur local pour exécuter des RPC sur un serveur distant, TEST3, qui utilise le mécanisme de sécurité "dce" et pour utiliser l'authentification réciproque pour tous les RPC entre les deux serveurs, exécutez la commande :

```
sp_serveroption TEST3, "security mechanism", dce
sp_serveroption TEST3, "mutual authentication",
     true
```

## Règles de configuration du modèle de sécurité B pour les RPC

Suivez ces règles lorsque vous configurez le modèle de sécurité B pour les RPC :

- Les deux serveurs doivent utiliser le modèle de sécurité B.
- Les deux serveurs doivent utiliser le même mécanisme de sécurité et ce mécanisme doit supporter les services de sécurité définis avec sp_serveroption.
- Le responsable de la sécurité du système du serveur local doit spécifier les services de sécurité requis par le serveur distant. Par exemple, si le serveur distant exige que tous les messages utilisent les services de sécurité de type confidentialité des messages, le responsable de la sécurité du système doit utiliser sp_serveroption pour activer use message confidentiality.
- Les logins authentifiés par un mécanisme de sécurité et connectés à Adaptive Server à l'aide de "l'unification des logins" n'ont pas la possibilité d'exécuter des RPC dans le serveur distant sauf si les logins sont définis comme "sécurisés" sur le serveur distant ou si le login spécifie le mot de passe pour le serveur distant. Lorsqu'ils utilisent Open Client Client-Library, les utilisateurs peuvent utiliser la routine ct_remote_pwd pour spécifier un mot de passe pour les connexions serveur à serveur. Un administrateur système d'Adaptive Server peut utiliser sp_remoteoption pour spécifier qu'un utilisateur est habilité à utiliser le serveur distant sans spécifier de mot de passe.

## Préparation à l'utilisation du modèle de sécurité B pour les RPC

Le tableau 14-7 présente la procédure permettant d'utiliser le modèle de sécurité B pour les RPC.

***Tableau 14-7 : Procédure d'utilisation du modèle de sécurité B pour les RPC***

| Tâche – Qui ? Où ? | Commande, procédure système ou outil | Voir |
|---|---|---|
| *Administrateur système du système d'exploitation :*<br>1. Assurez-vous que le fichier interfaces ou le service de répertoire contient une entrée pour les deux serveurs et une ligne secmech mentionnant le mécanisme de sécurité. | UNIX : dscp ou dscp_dce<br>PC : dsedit | "Spécification d'informations de sécurité pour le serveur", page 544<br>Pour plus d'informations sur l'utilisation de dscp ou de dscp_dce, reportez-vous au document *Open Client/Server - Guide de configuration pour plates-formes UNIX*.<br>Pour plus d'informations sur l'utilisation de dsedit, reportez-vous au document *Open Client/Server - Manuel de configuration pour plates-formes PC*. |
| *Le responsable de la sécurité du système sur le serveur distant :*<br>2. Ajoutez le serveur local à master..sysservers. | sp_addserver<br>Exemple :<br>`sp_addserver "lcl_server"` | "Ajout d'un serveur distant", page 519<br>sp_addserver dans le *Manuel de référence d'Adaptive Server*. |
| *Le responsable de la sécurité du système sur le serveur distant :*<br>3. Ajoutez les logins dans la table master..syslogins. | sp_addlogin<br>Exemple :<br>`sp_addlogin user1, "pwuser1"` | "Ajout de logins à Adaptive Server", page 372<br>sp_addlogin dans le *Manuel de référence d'Adaptive Server*. |

| Tâche – Qui ? Où ? | Commande, procédure système ou outil | Voir |
|---|---|---|
| *Le responsable de la sécurité du système sur le serveur distant :*<br>4. Activez use security services et définissez rpc security model B comme modèle pour les connexions avec le serveur local. | sp_configure (pour définir use security services)<br>sp_serveroption (pour définir le modèle de sécurité des RPC)<br>Exemple :<br>`sp_configure "use security services", 1`<br>`sp_serveroption lcl_server, "rpc security model B", true` | "Etablissement du modèle de sécurité pour les RPC", page 556<br>"Activation de la sécurité réseau", page 546<br>use security services (Windows NT uniquement) du chapitre 5, "Définition des paramètres de configuration" du présent manuel.<br>sp_configure dans le *Manuel de référence d'Adaptive Server*.<br>sp_serveroption dans le *Manuel de référence d'Adaptive Server*. |
| *L'administrateur système sur le serveur distant :*<br>5. Vous avez la possibilité, mais cela est facultatif, de spécifier certains utilisateurs comme "sécurisés" pour la connexion au serveur distant à partir du serveur local sans avoir à indiquer de mot de passe. | sp_remoteoption<br>Exemple :<br>`sp_remoteoption lcl_server, user1, user1, trusted, true` | "Contrôle des mots de passe pour les utilisateurs distants", page 529<br>sp_remoteoption dans le *Manuel de référence d'Adaptive Server*. |
| *Le responsable de la sécurité du système sur le serveur local :*<br>6. Ajoutez le serveur local et le serveur distant dans la table master..sysservers. | sp_addserver<br>Exemple :<br>`sp_addserver lcl_server, local`<br>`sp_addserver rem_server` | "Ajout d'un serveur distant", page 519<br>sp_addserver dans le *Manuel de référence d'Adaptive Server*. |
| *Le responsable de la sécurité du système sur le serveur local :*<br>7. Ajoutez les logins dans la table master..logins. | sp_addlogin<br>Exemple :<br>`sp_addlogin user1, "pwuser1"` | "Ajout de logins à Adaptive Server", page 372<br>sp_addlogin dans le *Manuel de référence d'Adaptive Server*. |

| Tâche – Qui ? Où ? | Commande, procédure système ou outil | Voir |
|---|---|---|
| *Le responsable de la sécurité du système sur le serveur local :*<br>8. Activez use security services et définissez rpc security model B comme modèle pour les connexions avec le serveur distant. | sp_configure (pour définir use security services)<br>sp_serveroption (pour définir le modèle de sécurité des RPC)<br>Exemple :<br>`sp_configure "use security services", 1`<br>`sp_serveroption rem_server, "rpc security model B", true` | "Etablissement du modèle de sécurité pour les RPC", page 556<br>"Activation de la sécurité réseau", page 546<br>use security services (Windows NT uniquement) du chapitre 5, "Définition des paramètres de configuration" du présent manuel.<br>sp_configure dans le *Manuel de référence d'Adaptive Server*.<br>sp_serveroption dans le *Manuel de référence d'Adaptive Server*. |
| *Le responsable de la sécurité du système sur le serveur local :*<br>9. Spécifiez le mécanisme de sécurité et les services de sécurité à utiliser pour les connexions avec le serveur distant. | sp_serveroption<br>Exemple :<br>`sp_serveroption rem_server, "security mechanism", dce`<br>`sp_serveroption rem_server, "use message integrity", true` | "Définition des options de connexion du serveur", page 521<br>sp_serveroption dans le *Manuel de référence d'Adaptive Server*. |

## Exemple de configuration du modèle de sécurité B pour les RPC

Considérez :

- qu'un serveur local, lcl_serv, exécute des RPC sur un serveur distant, rem_serv ;
- que les deux serveurs utilisent le modèle de sécurité B et le service de sécurité DCE ;
- que les services de sécurité RPC de type authentification réciproque et intégrité des messages soient en vigueur ;
- que les utilisateurs "user1" et "user2" utilisent l'unification des logins pour se connecter au serveur local, lcl_serv, et pour exécuter des RPC sur rem_serv. Ces utilisateurs sont définis comme "sécurisés" sur rem_serv et ne sont pas tenus de spécifier un mot de passe pour le serveur distant.

- L'utilisateur "user3" n'utilise pas l'unification des logins, n'est pas habilité et doit indiquer un mot de passe à Adaptive Server à la connexion.

Utilisez la séquence de commandes suivante pour configurer la sécurité pour les RPC entre les serveurs :

Le responsable de la sécurité du système sur le serveur distant (rem_serv) :

```
sp_addserver 'lcl_serv'
sp_addlogin user1, "eracg12"
sp_addlogin user2, "esirpret"
sp_addlogin user3, "drabmok"
sp_configure "use security services", 1
sp_serveroption lcl_serv, "rpc security model B",
   true
sp_serveroption lcl_serv, "security mechanism", dce
```

L'administrateur système sur le serveur distant (rem_serv) :

```
sp_remoteoption lcl_serv, user1, user1, trusted,
   true
sp_remoteoption lcl_serv, user2, user2, trusted,
   true
```

Le responsable de la sécurité du système sur le serveur local (lcl_serv) :

```
sp_addserver lcl_serv, local
sp_addserver rem_serv
sp_addlogin user1, "eracg12"
sp_addlogin user2, "esirpret"
sp_addlogin user3, "drabmo1"
sp_configure "use security services", 1
sp_configure rem_serv, "rpc security model B", true
sp_serveroption rem_serv, "security mechanism", dce
sp_serveroption rem_serv, "mutual authentication"
   true
sp_serveroption rem_serv, "use message integrity"
   true
```

Par ailleurs, le fichier interfaces ou le service de répertoire doit posséder des entrées pour rem_serv et lcl_serv. Chaque entrée doit spécifier le service de sécurité "dce". Par exemple, vous pouvez disposer de ces entrées dans le fichier interfaces, telles qu'elles sont créées par l'utilitaire dscp :

```
## lcl_serv (3201)
lcl_serv
master tli tcp /dev/tcp \x00020c8182d655110000000000000000
```

```
query tli tcp /dev/tcp \x00020c8182d655110000000000000000
secmech 1.3.6.1.4.1.897.4.6.1
## rem_serv (3519)
rem_serv
master tli tcp /dev/tcp \x000214ad82d655110000000000000000
query tli tcp /dev/tcp \x000214ad82d655110000000000000000
secmech 1.3.6.1.4.1.897.4.6.1
```

**Remarque** Pour réellement utiliser les services de sécurité sur l'un ou l'autre serveur, vous devez redémarrer le serveur afin que le paramètre statique use security services soit appliqué.

Pour plus d'informations sur la configuration des serveurs pour les appels de procédures à distance, reportez-vous au chapitre 13, "Gestion des serveurs distants"..

### Recherche d'informations sur les serveurs distants

La procédure système sp_helpserver affiche des informations sur les serveurs. Sans argument, cette commande donne des informations sur tous les serveurs figurant dans la table sysservers. Vous pouvez spécifier un serveur en particulier pour recevoir des informations sur ce serveur. La syntaxe est la suivante :

sp_helpserver [*serveur*]

Par exemple, pour afficher des informations sur le serveur GATEWAY, exécutez la commande suivante :

```
sp_helpserver GATEWAY
```

## Connexion au serveur et utilisation des services de sécurité

Les utilitaires isql et bcp comprennent les options de lignes de commande suivantes qui permettent d'activer les services de sécurité réseau à la connexion :

-K *fichier_keytab*

-R *principal_serveur_distant*

-V *options_sécurité*

-Z *mécanisme_sécurité*

---

**Remarque** Il existe des versions des utilitaires isql et bcp pour le service de répertoire et pour les services de sécurité DCE, respectivement appelés isql_dce et bcp_dce. Vous devez utiliser ces versions lorsque vous utilisez DCE.

---

Ces options sont décrites dans les paragraphes qui suivent.

-K *fichier_keytab* ne peut être utilisé qu'avec la sécurité DCE. Cette option spécifie un fichier keytab contenant la clé de sécurité pour la connexion de l'utilisateur au serveur. Les fichiers keytab peuvent être créés avec l'utilitaire DCE dcecp (pour plus d'informations, reportez-vous à la documentation de votre DCE).

Si l'option -K n'est pas indiquée, l'utilisateur de isql doit être connecté au DCE. Si l'utilisateur spécifie l'option -U, le nom spécifié avec -U doit correspondre au nom défini pour l'utilisateur dans DCE.

-R *principal_serveur_distant* spécifie le nom du "principal" du serveur tel qu'il est défini pour le mécanisme de sécurité. Par défaut, le nom principal d'un serveur correspond à son nom de réseau (qui est spécifié avec l'option -S ou la variable d'environnement DSQUERY). L'option -R doit être utilisée lorsque le nom du "principal" et le nom réseau du serveur sont différents.

-V *options_sécurité* spécifie l'authentification des utilisateurs sur le réseau. Avec cette option, l'utilisateur doit se connecter au système de sécurité du réseau avant d'exécuter l'utilitaire. Dans ce cas, si l'utilisateur indique l'option -U, il doit entrer son nom d'utilisateur réseau admis par le mécanisme de sécurité. S'il indique un mot de passe avec l'option -P, le système n'en tiendra pas compte.

-V peut être suivi d'une chaîne *options_sécurité* composée de lettres-clés permettant d'activer des services supplémentaires. Ces lettres-clés sont les suivantes :

c, qui active le service de confidentialité des données ;

i, qui active le service d'intégrité des données ;

m, qui active l'authentification réciproque pour l'établissement de la connexion ;

o, qui active le service d'estampille des données d'origine ;

r, qui active la détection de ré-exécution ;

q, qui active la détection de l'ordre.

-Z *mécanisme_sécurité* spécifie le nom d'un mécanisme de sécurité à utiliser à la connexion.

Les noms des mécanismes de sécurité sont définis dans le fichier de configuration *libtcl.cfg*. Si aucun nom de *mécanisme_sécurité* n'est indiqué, le mécanisme par défaut est utilisé. Pour plus d'informations sur les noms des mécanismes de sécurité, reportez-vous au document *Open Client/Server Configuration Guide* de votre plate-forme.

Si vous vous connectez au mécanisme de sécurité, puis à Adaptive Server, il n'est pas nécessaire de spécifier l'option -U de l'utilitaire car Adaptive Server extrait le nom d'utilisateur du mécanisme de sécurité. Par exemple, envisagez la commande suivante :

```
svrsole4% dce_login user2
Enter Password:
svrsole4% $SYBASE/bin/isql_dce -V
1> select suser_name()
2> go

------------------------------
user2
```

Dans cet exemple, l'utilisateur "user2" se connecte au DCE avec dce_login, puis à Adaptive Server sans spécifier l'option -U. L'option -V sans paramètre spécifie implicitement un seul service de sécurité : l'unification des logins.

Pour plus d'informations sur les utilitaires Adaptive Server, reportez-vous au *Guide Utilitaires*.

Si vous utilisez Client-Library pour vous connecter à Adaptive Server, vous pouvez définir des propriétés avant de vous connecter au serveur. Par exemple, pour vérifier l'ordre des messages, définissez la propriété CS_SEC_DETECTSEQ. Pour plus d'informations sur l'utilisation des services de sécurité de Client-Library, reportez-vous au document *Open Client Client-Library/C Reference Guide*.

## Exemple d'utilisation des services de sécurité

Imaginez que votre login est "mary" et que vous souhaitiez utiliser le mécanisme de sécurité DCE avec l'unification des logins (toujours active si vous spécifiez l'option -V de isql_dce ou de bcp_dce), la confidentialité des messages et l'authentification réciproque pour les procédures à distance. Vous souhaitez vous connecter au serveur WOND et exécuter des procédures à distance sur le serveur GATEWAY avec l'authentification réciproque. En partant du principe qu'un responsable de la sécurité du système a configuré à la fois WOND et GATEWAY pour le modèle de sécurité B pour les RPC, vous ajoute comme utilisateur sur les deux serveurs et vous définit comme utilisateur distant et habilité sur le serveur GATEWAY, vous pouvez utiliser la procédure suivante :

1 Connectez-vous au mécanisme de sécurité DCE pour recevoir une accréditation :

```
dce_login mary
```

2 Connectez-vous à Adaptive Server à l'aide de isql_dce :

```
isql_dce -SWOND -Vcm
```

3 Exécutez :

```
GATEWAY...sp_who
GATEWAY...mary_prc1
GATEWAY...mary_prc2
```

Dorénavant, tous les messages envoyés par Mary au serveur et reçus du serveur sont cryptés (confidentialité des messages) et lorsqu'elle exécute des procédures à distance, les serveurs WOND et GATEWAY sont tous deux authentifiés.

## Utilisation des mécanismes de sécurité pour le client

Au démarrage, Adaptive Server détermine l'ensemble de mécanismes de sécurité supportés. Pour plus d'informations, reportez-vous à la section "Détermination des mécanismes de sécurité à supporter", page 552 Dans la liste des mécanismes de sécurité supportés par Adaptive Server, le mécanisme à utiliser pour un client en particulier doit être choisi.

Si le client spécifie un mécanisme de sécurité (par exemple, avec l'option -Z de isql_dce), Adaptive Server utilise le mécanisme de sécurité en question. Autrement, c'est le mécanisme de sécurité qui apparaît en premier dans la liste du fichier *libtcl.cfg* qui est utilisé.

# Recherche d'informations relatives aux services de sécurité disponibles

Adaptive Server vous permet de :

- déterminer les mécanismes et les services de sécurité supportés par Adaptive Server ;
- déterminer les services de sécurité actifs pour la session en cours ;
- déterminer si un service de sécurité donné est activé pour la session.

## Détermination des services et des mécanismes de sécurité supportés

Une table système, syssecmechs, fournit des informations sur les mécanismes et les services de sécurité supportés par Adaptive Server. La table, dont le contenu est créé dynamiquement lorsque vous exécutez la requête, contient les colonnes suivantes :

- sec_mech_name représente le nom du mécanisme de sécurité. Ce peut être, par exemple, "dce" ou "NT LANMANAGER".
- available_service représente le service de sécurité supporté par le mécanisme de sécurité. Ce peut être, par exemple, "l'unification des logins".

La table peut contenir plusieurs lignes pour un seule mécanisme de sécurité : une ligne par service de sécurité supporté par le mécanisme.

Pour dresser la liste de tous les mécanismes et services de sécurité supportés par Adaptive Server, exécutez cette requête :

```
select * from syssecmechs
The result might look something like:
sec_mech_name                  available_service
------------------------------ --------------------
 dce                            unifiedlogin
 dce                            mutualauth
 dce                            delegation
 dce                            integrity
 dce                            confidentiality
 dce                            detectreplay
 dce                            detectseq
```

## Détermination des services de sécurité activés

Pour déterminer les services de sécurité activés pour la session courante, utilisez la fonction show_sec_services. Exemple :

```
                show_sec_services()
------------------------------------------------------------------
          unifiedlogin mutualauth confidentiality
(1 row affected)
```

## Détermination de l'activation d'un service de sécurité

Pour déterminer si un service de sécurité en particulier, comme "mutualauth" est activé, utilisez la fonction is_sec_service_on. La syntaxe est la suivante :

is_sec_service_on (*nom_service_sécurité*)

où *nom_service_sécurité* représente un service de sécurité disponible. Utilisez le nom affiché lorsque vous transmettez la requête à syssecmechs.

Par exemple, pour déterminer si "mutualauth" est activé, exécutez la commande :

```
select is_sec_service_on("mutualauth")
-----------
          1

(1 row affected)
```

Le résultat 1 indique que le service de sécurité est activé pour la session, tandis que le résultat 0 indique que le service n'est pas utilisé.