SYBASE®

Guide des nouvelles fonctionnalités

Adaptive Server® Enterprise

12.5.4

Réf. du document : DC20132-01-1254-01

Dernière mise à jour : juin 2006

Copyright © 1987-2006 Sybase, Inc. Tous droits réservés.

Cette publication concerne le logiciel Sybase et toutes les versions ultérieures qui ne feraient pas l'objet d'une réédition de la documentation ou de la publication de notes de mise à jour. Les informations contenues dans ce document pourront faire l'objet de modifications sans préavis. Le logiciel décrit est fourni sous contrat de licence et il ne peut être utilisé ou copié que conformément aux termes de ce contrat.

Pour commander des ouvrages supplémentaires ou acquérir des droits de reproduction, si vous habitez aux États-Unis ou au Canada, appelez notre Service Clients au (800) 685-8225, télécopie (617) 229-9845.

Les clients ne résidant ni aux États-Unis ni au Canada et qui disposent d'un contrat de licence pour les États-Unis peuvent joindre notre Service Clients par télécopie. Ceux qui ne bénéficient pas de cette licence doivent s'adresser à leur revendeur Sybase ou au distributeur le plus proche. Les mises à jour du logiciel ne sont fournies qu'à des dates d'édition périodiques. Aucune partie de cette publication ne peut être reproduite, transmise ou traduite sous quelque forme et par quelque moyen que ce soit, électronique, mécanique, manuel, optique ou autre, sans l'autorisation écrite de Sybase, Inc.

Sybase, SYBASE (logo), ADA Workbench, Adaptable Windowing Environment, Adaptive Component Architecture, Adaptive Server, Adaptive Server Anywhere, Adaptive Server Enterprise, Adaptive Server Enterprise Monitor, Adaptive Server Enterprise Replication, Adaptive Server Everywhere, Advantage Database Server, Afaria, Answers Anywhere, Applied Meta, Applied Metacomputing, AppModeler, APT Workbench, APT-Build, APT-Edit, APT-Execute, APT-Translator, APT-Library, ASEP, Avaki, Avaki (Arrow Design), Avaki Data Grid, AvantGo, Backup Server, BayCam, Beyond Connected, Bit-Wise, BizTracker, Certified PowerBuilder Developer, Certified SYBASE Professional, Certified SYBASE Professional Logo, ClearConnect, Client-Library, Client Services, CodeBank, Column Design, ComponentPack, Connection Manager, Convoy/DM, Copernicus, CSP, Data Pipeline, Data Workbench, DataArchitect, Database Analyzer, DataExpress, DataServer, DataWindow, DataWindow .NET, DB-Library, dbQueue, Dejima, Dejima Direct, Developers Workbench, DirectConnect Anywhere, DirectConnect, Distribution Director, Dynamic Mobility Model, e-ADK, E-Anywhere, e-Biz Integrator, E-Whatever, EC Gateway, ECMAP, ECRTP, eFulfillment Accelerator, EII Plus, Electronic Case Management, Embedded SQL, EMS, Enterprise Application Studio, Enterprise Client/ Server, Enterprise Connect, Enterprise Data Studio, Enterprise Manager, Enterprise Portal (logo), Enterprise SQL Server Manager, Enterprise Work Architecture, Enterprise Work Designer, Enterprise Work Modeler, eProcurement Accelerator, eremote, Everything Works Better When Everything Works Together, EWA, ExtendAssist, Extended Systems, ExtendView, Financial Fusion, Financial Fusion (and design), Financial Fusion Server, Formula One, Fusion Powered e-Finance, Fusion Powered Financial Destinations, Fusion Powered STP, Gateway Manager, GeoPoint, GlobalFIX, iAnywhere, iAnywhere Solutions, ImpactNow, Industry Warehouse Studio, InfoMaker, Information Anywhere, Information Everywhere, InformationConnect, InstaHelp, Intelligent Self-Care, InternetBuilder, iremote, irLite, iScript, Jaguar CTS, jConnect for JDBC, KnowledgeBase, Legion, Logical Memory Manager, M2M Anywhere, Mach Desktop, Mail Anywhere Studio, Mainframe Connect, Maintenance Express, Manage Anywhere Studio, MAP, M-Business Anywhere, M-Business Channel, M-Business Network, M-Business Suite, MDI Access Server, MDI Database Gateway, media.splash, Message Anywhere Server, MetaWorks, MethodSet, mFolio, Mirror Activator, ML Query, MobiCATS, MobileQ, MySupport, Net-Gateway, Net-Library, New Era of Networks, Next Generation Learning, Next Generation Learning Studio, O DEVICE, OASiS, OASiS logo, ObjectConnect, ObjectCycle, OmniConnect, OmniQ, OmniSQL Access Module, OmniSQL Toolkit, OneBridge, Open Biz, Open Business Interchange, Open Client, Open ClientConnect, Open Client/Server, Open Client/Server Interfaces, Open Gateway, Open Server, Open ServerConnect, Open Solutions, Optima++, Partnerships that Work, PB-Gen, PC APT Execute, PC DB-Net, PC Net Library, Pharma Anywhere, PhysicalArchitect, Pocket PowerBuilder, PocketBuilder, Power++, Power Through Knowledge, power.stop, PowerAMC, PowerBuilder, PowerBuilder Foundation Class Library, PowerDesigner, PowerDimensions, PowerDynamo, Powering the New Economy, PowerScript, PowerSite, PowerSocket, Powersoft, PowerStage, PowerStudio, PowerTips, Powersoft Portfolio, Powersoft Professional, PowerWare Desktop, PowerWare Enterprise, ProcessAnalyst, Pylon, Pylon Anywhere, Pylon Application Server, Pylon Conduit, Pylon PIM Server, Pylon Pro, QAnywhere, Rapport, Relational Beans, RemoteWare, RepConnector, Report Workbench, Report-Execute, Replication Agent, Replication Driver, Replication Server, Replication Server Manager, Replication Toolkit, Resource Manager, RFID Anywhere, RW-DisplayLib, RW-Library, SAFE, SAFE/PRO, Sales Anywhere, Search Anywhere, SDF, Search Anywhere, Secure SQL Server, Secure SQL Toolset, Security Guardian, ShareSpool, ShareLink, SKILS, smart.partners, smart.parts, smart.script, SOA Anywhere Trademark,SQL Advantage, SQL Anywhere, SQL Anywhere Studio, SQL Code Checker, SQL Debug, SQL Edit, SQL Edit/TPU, SQL Everywhere, SQL Modeler, SQL Remote, SQL Server, SQL Server Manager, SQL SMART, SQL Toolset, SQL Server/CFT, SQL Server/DBM, SQL Server SNMP SubAgent, SQL Station, SQLJ, Stage III Engineering, Startup.Com, STEP, SupportNow, S.W.I.F.T. Message Format Libraries, Sybase Central, Sybase Client/ Server Interfaces, Sybase Development Framework, Sybase Financial Server, Sybase Gateways, Sybase IQ, Sybase Learning Connection, Sybase MPP, Sybase SQL Desktop, Sybase SQL Lifecycle, Sybase SQL Workgroup, Sybase Synergy Program, Sybase Virtual Server Architecture, Sybase User Workbench, SybaseWare, Syber Financial, SyberAssist, SybFlex, SybMD, SyBooks, System 10, System 11, System XI (logo), SystemTools, Tabular Data Stream, The Enterprise Client/Server Company, The Extensible Software Platform, The Future Is Wide Open, The Learning Connection, The Model For Client/Server Solutions, The Online Information Center, The Power of One, TotalFix, TradeForce, Transact-SQL, Translation Toolkit, Turning Imagination Into Reality, UltraLite, UltraLite.NET, UNIBOM, Unilib, Uninull, Unisep, Unistring, URK Runtime Kit for UniCode, Viafone, Viewer, VisualWriter, VQL, WarehouseArchitect, Warehouse Control Center, Warehouse Studio, Warehouse WORKS, Watcom, Watcom SQL, Watcom SQL Server, Web Deployment Kit, Web.PB, Web.SQL, WebSights, WebViewer, WorkGroup SQL Server, XA-Library, XA-Server, XcelleNet, XP Server, XTNDAccess and XTNDConnect sont des marques de Sybase, Inc. ou de ses filiales. 01/06

Unicode et le logo Unicode sont des marques déposées d'Unicode, Inc.

Tous les autres noms de produit, société ou marque apparaissant dans ce document sont des marques ou marques déposées de leurs propriétaires respectifs.

Use, duplication, or disclosure by the government is subject to the restrictions set forth in subparagraph (c)(1)(ii) of DFARS 52.227-7013 for the DOD and as set forth in FAR 52.227-19(a)-(d) for civilian agencies.

Sybase, Inc., One Sybase Drive, Dublin, CA 94568, Etats-Unis d'Amérique.

Sommaire

Préface

À qui s'adresse ce manuel ?

Ce manuel est destiné aux administrateurs système et aux propriétaires de bases de données Sybase® qui utilisent Adaptive Server® version 12.5.4. Il présente les nouvelles fonctionnalités incluses dans cette version d'Adaptive Server.

Comment utiliser ce manuel

Ce document se compose des éléments suivants :

- Le Chapitre 1, « Présentation » contient une présentation et des informations récapitulatives sur les fonctionnalités disponibles dans Adaptive Server version 12.5.4.
- Le Chapitre 2, « Améliorations de la sécurité » contient des informations sur les améliorations apportées à Adaptive Server version 12.5.4 en termes de sécurité. Parmi celles-ci, des améliorations pour LDAP, Kerberos et SSL, ainsi que dans le domaine de la complexité des mots de passe.
- Le Chapitre 3, « Accès à la base de données archive » contient des informations sur les nouvelles fonctionnalités d'accès à la base de données archive. L'accès à la base de données archive offre à l'administrateur de base de données la possibilité de valider ou de récupérer de manière sélective des données depuis une sauvegarde de la base de données.
- Le Chapitre 4, « Modifications du répertoire partagé » contient des informations sur les modifications apportées à la structure de répertoire.
- Le Chapitre 5, « Support des pilotes Sybase » contient des informations sur les nouveaux pilotes natifs pris en charge.
- Le Chapitre 6, « Chargement dynamique des bibliothèques TIBCO » contient des informations sur les nouvelles bibliothèques TIBCO prises en charge.
- Le Chapitre 7, « Prise en charge du protocole JRE » contient des informations sur la prise en charge de la version la plus récente du JRE.
- Le Chapitre 8, « Modifications du module externe d'Adaptive Server » contient des informations sur des modifications apportées au module externe d'Adaptive Server afin de prendre en charge l'accès à la base de données archive et la complexité des mots de passe.

- Le Chapitre 9, « Modifications des tables de contrôle » contient des informations sur les modifications apportées aux tables de contrôle.
- Le Chapitre 10, « Mémoire partagée dans les environnements Terminal Server de Windows » contient des informations sur l'utilisation d'une mémoire partagée dans un environnement Windows Terminal Server.
- Le Chapitre 12, « Modifications apportées aux procédures stockées, aux fonctions et aux commandes » propose des informations complémentaires sur les modifications mises en œuvre dans Adaptive Server version 12.5.4.

Documentation annexe

La documentation de Sybase Adaptive Server Enterprise se compose des documents 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 peut être disponible sur le Web. Pour vérifier si des informations importantes sur le produit ou le document ont été ajoutées après la commercialisation du CD-ROM, consultez le site Technical Library de Sybase.
- Le *Guide d'installation* 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.
- Documentation sur les nouvelles fonctionnalités de chacune des versions 12.5.x antérieures :
  - Le manuel *Nouvelles fonctionnalités d'Adaptive Server Enterprise* décrit les nouvelles fonctionnalités de la version 12.5.4 d'Adaptive Server, les modifications apportées au système pour leur prise en charge et les modifications susceptibles d'avoir des conséquences sur les applications existantes.
  - Le manuel *Nouvelles fonctionnalités dans Adaptive Server 12.5.2* décrit les nouvelles fonctionnalités de la version 12.5.2 d'Adaptive Server ainsi que les modifications apportées au système pour les prendre en charge.
  - Le *Guide des nouvelles fonctionnalités dans Adaptive Server 12.5.3* décrit les nouvelles fonctionnalités de la version 12.5.3 d'Adaptive Server ainsi que les modifications apportées au système pour les prendre en charge.
  - Le manuel *Bulletin des nouvelles fonctionnalités d'Adaptive Server 12.5.3a* décrit les nouvelles fonctionnalités de la version 12.5.3a d'Adaptive Server, ainsi que les modifications apportées au système pour leur prise en charge.

- Le *Guide de l'utilisateur d'ASE Replicator* décrit l'utilisation de la fonctionnalité ASE Replicator d'Adaptive Server pour mettre en œuvre une réplication de base d'un serveur primaire vers un ou plusieurs serveurs Adaptive Server distants.
- Le *Guide de l'utilisateur de Component Integration Services* explique l'utilisation de la fonction Adaptive Server Component Integration Services permettant d'établir des connexions à des bases de données distantes Sybase et non Sybase.
- Le manuel *Configuration d'Adaptive Server Enterprise* pour votre plate-forme fournit des instructions permettant d'effectuer des tâches spécifiques de configuration sur Adaptive Server.
- Le *Guide de l'utilisateur d'EJB Server* explique comment utiliser EJB Server pour déployer et exécuter Enterprise JavaBeans dans Adaptive Server.
- Le manuel *Error Messages and Troubleshooting Guide* explique comment résoudre les messages d'erreur les plus fréquents et décrit les solutions aux problèmes liés au système auxquels les utilisateurs sont le plus souvent confrontés.
- Le *Guide de l'utilisateur de Full-Text Search Specialty Data Store* explique comment utiliser la fonction Full-Text Search avec Verity afin d'effectuer des recherches dans les données d'Adaptive Server Enterprise.
- Le *Glossaire* définit les termes techniques utilisés dans la documentation d'Adaptive Server.
- Le *Guide de l'utilisateur d'Historical Server* décrit comment utiliser Historical Server pour obtenir des statistiques sur les performances de SQL Server® et d'Adaptive Server.
- Le manuel *Java dans Adaptive Server Enterprise* décrit l'installation et l'utilisation des classes Java dans la base de données d'Adaptive Server comme types de données, fonctions et procédures stockées.
- Le *Guide de l'utilisateur de Job Scheduler* décrit les instructions d'installation et de configuration de Job Scheduler ainsi que la création et la planification de tâches sur un serveur Adaptive Server local ou distant à l'aide de la ligne de commande ou d'une interface utilisateur graphique (IUG).
- Le guide *Monitor Client Library Programmer's Guide* explique comment écrire des applications Monitor Client Library accédant aux données de performances d'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 d'Adaptive Server.
- Le *Guide Performances et optimisation* contient quatre manuels qui expliquent comment optimiser les performances d'Adaptive Server :
  - *Concepts de base* décrit les notions fondamentales nécessaires à la compréhension et à l'analyse des questions de performances dans Adaptive Server.
  - *Verrouillage* décrit comment les différents plans de verrouillage peuvent être utilisés pour améliorer les performances d'Adaptive Server.
  - *Optimiseur et plans abstraits* décrit comment l'optimiseur traite les requêtes et comment les plans abstraits peuvent être utilisés pour modifier certains plans de l'optimiseur.
  - *Contrôle et analyse* explique comment les statistiques sont obtenues et utilisées pour contrôler et optimiser les performances.
- Le *Guide de référence rapide* fournit une liste complète des noms et syntaxes pour les commandes, les fonctions, les procédures système, les procédures système étendues, les types de données et les utilitaires dans un format de poche.
- Le *Manuel de référence* se compose de quatre manuels contenant les informations détaillées suivantes sur Transact-SQL® :
  - *Éléments syntaxiques* : types de données, fonctions, variables globales, expressions, identificateurs, caractères joker et mots réservés de Transact-SQL.
  - *Commandes*-: commandes de Transact-SQL.
  - *Procédures* : procédures système, procédures stockées, procédures système stockées étendues et procédures stockées dbcc de Transact-SQL.
  - *Tables* – tables système et tables dbcc Transact-SQL.
- Le *Guide d'administration système* fournit des informations détaillées sur l'administration des serveurs et des bases de données. Il contient des instructions relatives à la gestion des ressources physiques, à la sécurité, aux bases de données système et utilisateur, ainsi qu'à la définition des paramètres de conversion de caractères, de la langue et de l'ordre de tri.
- Le diagramme *System Tables Diagram* est un poster qui illustre les tables système selon le modèle entité/relation. Disponible uniquement en version papier.

- Le *Guide de l'utilisateur Transact-SQL* présente Transact-SQL, version enrichie du langage de base de données relationnelle de Sybase. Ce guide sert de document de référence pour les utilisateurs qui découvrent les systèmes de gestion de bases de données. Il décrit également les bases de données exemple pubs2 et pubs3.
- Le manuel *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 manuel *Utilisation de Sybase Failover en environnement haute disponibilité* fournit les instructions d'utilisation du mode Failover de Sybase pour configurer un Adaptive Server comme serveur compagnon dans un environnement haute disponibilité.
- Le guide *Utilitaires* décrit les utilitaires d'Adaptive Server, tels qu'isql et bcp, qui sont exécutés au niveau du système d'exploitation.
- Le *Guide de l'utilisateur de Web Services* explique comment configurer, utiliser et résoudre les problèmes de Web Services pour Adaptive Server.
- Le guide *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 manuel *XML Services in Adaptive Server Enterprise* décrit le processeur XML natif de Sybase et la prise en charge XML Java de Sybase, introduit XML dans la base de données et présente les fonctions de requête et de mappage qui composent XML Services.

Autres sources d'informations

Consultez les CD-ROM Getting Started et Technical Library de Sybase ainsi que le site Web Technical Library Product Manuals pour obtenir davantage d'informations sur les produits :

- Le CD-ROM Getting Started, qui accompagne votre logiciel, propose les notes de mise à jour et les guides d'installation au format PDF, ainsi que d'autres documents ou des informations de dernière minute qui n'apparaissent pas sur le CD Technical Library. Ce CD-ROM est fourni avec votre logiciel. Pour lire ou imprimer les documents figurant sur le CD-ROM Getting Started, vous avez besoin du logiciel Acrobat Reader d'Adobe (téléchargeable gratuitement sur le site Web d'Adobe, accessible au moyen du lien indiqué sur le CD-ROM).
- Le CD-ROM Technical Library contient les manuels des produits. Il est fourni avec le logiciel. Le lecteur DynaText, également présent sur le CD-ROM, permet d'accéder aux informations techniques relatives aux 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 constitue la version HTML du CD-ROM Technical Library, accessible à l'aide d'un navigateur Web traditionnel. Outre les manuels relatifs aux produits, vous y trouverez des liens vers les sites EBFs/Updates, Technical Documents, Case Management, Solved Cases, des forums et Sybase Developer Network.

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

Certifications Sybase sur le Web

La documentation technique du site Web de Sybase est fréquemment mise à jour.

❖ **Pour obtenir les dernières informations sur les certifications produits**

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

2 Cliquez sur Certification Report.

3 Dans le filtre Certification Report, sélectionnez un produit, une plate-forme et une période, puis cliquez sur Go.

4 Cliquez sur un titre dans Certification Report pour visualiser le rapport.

❖ **Pour obtenir les dernières informations sur les certifications composants**

1 Cliquez sur Availability and Certification Reports à http://certification.sybase.com/.

2 Sélectionnez la famille de produits et le produit sous Search by Base Product ou la plate-forme et le produit sous Search by Platform.

3 Sélectionnez Search pour afficher le rapport de disponibilité et de certification pour le produit sélectionné.

❖ **Pour créer une vue personnalisée du site Web de Sybase (y compris des pages d'assistance)**

Configurez un profil MySybase. MySybase est un service gratuit qui vous permet de créer un affichage personnalisé des pages Web de Sybase.

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

2 Cliquez sur MySybase et créez un profil MySybase.

EBF et maintenance logicielle de Sybase

❖ **Pour obtenir les dernières informations sur les correctifs de bugs et la maintenance logicielle**

1. Cliquez sur the Sybase Support Page à http://www.sybase.com/support.
2. Choisissez EBFs/Maintenance. Saisissez votre nom d'utilisateur et votre mot de passe MySybase si vous y êtes invité.
3. Sélectionnez un produit.
4. Spécifiez une période et cliquez sur Go. Une liste des versions EBF/Maintenance s'affiche.

   Les icônes en forme de cadenas indiquent que vous n'avez pas l'autorisation de télécharger certaines versions EBF/Maintenance parce que vous n'êtes pas enregistré auprès du Support technique. Si vous n'êtes pas enregistré mais que vous disposez d'informations valides fournies par votre représentant Sybase ou via votre contrat de support, cliquez sur Edit Roles pour ajouter le rôle “Technical Support Contact” à votre profil MySybase.
5. Cliquez sur l'icône Info pour afficher le rapport EBF/Maintenance ou cliquez sur la description du produit pour télécharger le logiciel.

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 ne parvenez pas à résoudre un problème en recourant aux manuels ou à l'aide en ligne, veuillez demander à la personne désignée de contacter le Support Technique Sybase ou la filiale Sybase la plus proche.

CHAPITRE 1

Présentation

Ce chapitre comprend une grille de compatibilité des fonctionnalités et des plates-formes, ainsi que des informations récapitulatives sur les nouvelles fonctionnalités introduites dans les versions 12.5.4, 12.5.3a, 12.5.3 et 12.5.2 d'Adaptive Server.

Informations de compatibilité des fonctionnalités et des plates-formes

Le Tableau 1-1 présente la disponibilité des fonctionnalités pour les systèmes d'exploitation pris en charge dans la version 12.5.4 d'Adaptive Server.

Tableau 1-1 : Fonctionnalités d'Adaptive Server pour les systèmes d'exploitation pris en charge

Options d'Adaptive Server	Solaris 32 bits	Solaris 64 bits	Solaris x86	Sol Opteron 64 bits	HP-UX PA Risc 64 bits	HP-UX PA Risc 32 bits	HP Tru64	HP-UX Itanium 64 bits	IBM AIX 32 bits	IBM AIX 64 bits	Windows x86	Macintosh OS X	SGI 32 bits	SGI 64 bits	Linux sur pSeries	Linux Opteron 64 bits	Linux Itanium 64 bits	Linux x86 32 bits
Colonnes cryptées	ƒ	ƒ	–	–	ƒ	ƒ	–	–	–	ƒ	ƒ	–	–	–	–	–	–	ƒ
Haute disponibilité	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	–	–	–	Y
Gestion des transactions distribuées	Y	Y	–	Y	Y	Y	–	–	Y	Y	Y	–	Y	Y	–	Y	–	Y
Gestion des XML	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y
Option Java	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y
XML natif	Y	Y	–	Y	Y	Y	–	§	–	Y	Y	–	–	–	–	§	ž	Y

Légende : Y : Prise en charge dans Adaptive Server 12.5.x ; ƒ : Introduit dans 12.5.3a ; ž : Introduit dans 12.5.4 ; § : Introduit dans 12.5.3 ESD5 ; Þ : Fusion des ports ; – : Non pris en charge

Options d'Adaptive Server	**Solaris 32 bits**	**Solaris 64 bits**	**Solaris x86**	**Sol Opteron 64 bits**	**HP-UX PA Risc 64 bits**	**HP-UX PA Risc 32 bits**	**HP Tru64**	**HP-UX Itanium 64 bits**	**IBM AIX 32 bits**	**IBM AIX 64 bits**	**Windows x86**	**Macintosh OS X**	**SGI 32 bits**	**SGI 64 bits**	**Linux sur pSeries**	**Linux Opteron 64 bits**	**Linux Itanium 64 bits**	**Linux x86 32 bits**
XML Java	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y
Services Web	Y	Y	–	–	Y	Y	–	Y	Y	Y	Y	–	Y	Y	–	–	Y	Y
Services de sécurité et de répertoire	Y	Y	–	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y
Répertoire du serveur LDAP	Y	Y	–	Y	Y	Y	Y	Y	Y	*ƒ*	Y	–	Y	–	–	–	ž	Y
Authentification utilisateur LDAP	Y	Y	–	–	Y	Y	Y		Y	*ƒ*	Y	–	–	–	–	–	–	Y
Secure Sockets Layer	Y	Y	–	Y	Y	Y	Y	ž	Y	Y	Y	–	–	–	–	–	–	Y
Cybersafe Kerberos	Y	Y	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	–
MIT Kerberos	Y	Y	–	Y	*ƒ*	*ƒ*	–	ž	*ƒ*	*ƒ*	–	–	–	–	–	Y	–	Y
Kerebos natif pour plate-forme	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Contrôle d'accès granulaire	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y
PAM (Pluggable Authentication Module)	Y	Y	–	Y	–	–	–	ž	–	*ƒ*	–	Y	–	–	–	Y	Y	Y
Gestion du contenu (prise en charge de fichiers externes)	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y
IUG Monitor Client	–	–	–	–	–	–	–	–	–	–	Y	–	–	–	–	–	–	–
Enhanced Full-Text Search (EFTS)	Y	Y	–	–	Y	Y	Y	–	Y	Y	Y	–	–	–	–	–	–	Y
Messagerie en temps réel	Y	Y	–	–	–	Y	–	–	–	Y	Y	–	–	–	–	–	–	Y
Prise en charge de JMS	Y	Y	–	–	–	Y	–	–	Y	Y	Y	–	–	–	–	–	–	Y
Prise en charge de WebSphere MQ	*ƒ*	*ƒ*	–	–	–	*ƒ*	–	–	–	*ƒ*	Y	–	–	–	–	–	–	*ƒ*
Reprise en cas d'incident	Y		–	–	Y	–	Y	Y	Y	–	Y	–	Y	–	–	–	–	Y
Fonctions incluses dans la version de base d'Adaptive Server																		
Complexité du mot de passe	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž
Accès à la base de données archive	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž	ž
IPv6	Y	Y	–	–	*ƒ*	*ƒ*	–	–	–	–	*ƒ*	–	–	–	–	–	–	–
Bibliothèques XA	–	–	–	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Sauvegarde et restauration interplate-forme	Y	Y	–	Y	Y	Y	–	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y
Job Scheduler	Y	Y	–	Þ	Y	Y	–	–	Y	Y	Y	Y	Y	Y	–	–	–	Y
ASE Replicator	Y	Y	–	–	Y	Y	–	–	Y	Y	Y	Y	–	–	–	–	–	Y

Légende : Y : Prise en charge dans Adaptive Server 12.5.x ; *ƒ* : Introduit dans 12.5.3a ; ž : Introduit dans 12.5.4 ; § : Introduit dans 12.5.3 ESD5 ; Þ : Fusion des ports ; – : Non pris en charge

Présentation des nouvelles fonctionnalités

Le Tableau 1-2 contient des informations sur les principales fonctionnalités des versions 12.5.2, 12.5.3, 12.5.3a et 12.5.4 d'Adaptive Server. Pour une description détaillée de ces fonctionnalités, reportez-vous à la documentation ad hoc de la version appropriée.

Tableau 1-2 : Comparaisons des nouvelles fonctionnalités dans les différentes versions d'Adaptive Server Enterprise

Fonctionnalité d'Adaptive Server	Description
Adaptive Server version 12.5.4	
Améliorations de Kerberos	Adaptive Server comprend les améliorations de Kerberos suivantes : • Nouvelle option permettant d'indiquer un nom principal Kerberos autre que le nom d'Adaptive Server. • Prise en charge étendue des plates-formes sur Kerberos. • Vous pouvez à présent utiliser l'option sp_modifylogin authenticate with pour demander une authentification Kerberos pour une connexion individuelle. • sybmapname est un utilitaire personnalisable permettant de convertir des noms principaux d'utilisateur externe en espace de nom de logins Adaptive Server.
Améliorations de l'authentification utilisateur LDAP	Adaptive Server comprend les améliorations de l'authentification utilisateur LDAP suivantes : • Basculement automatique de l'authentification d'un serveur LDAP primaire sur un serveur LDAP secondaire • Adaptive Server restaure les données après des erreurs rencontrées lors de la communication avec le serveur LDAP • Améliorations de la communication des messages liés à l'expiration du mot de passe obtenus du serveur LDAP aux clients Adaptive Server
Améliorations de la complexité du mot de passe	Vous pouvez à présent définir une vaste gamme d'attributs concernant la complexité du mot de passe. Il vous est également possible de rédiger vos propres procédures stockées afin de créer des contrôles de la complexité du mot de passe spécifiques au site.
Prise en charge de l'accès à la base de données archive	L'accès à la base de données archive offre à l'administrateur de base de données la possibilité de valider ou de récupérer de manière sélective des données depuis une sauvegarde de la base de données en utilisant celle-ci comme s'il s'agissait d'une base de données traditionnelle en lecture seule.
Modifications du répertoire partagé	Adaptive Server version 12.5.4 comprend plusieurs modifications de la structure du répertoire partagé.

Fonctionnalité d'Adaptive Server	Description
Prise en charge des pilotes de Sybase	Adaptive Server inclut désormais les fournisseurs de données Adaptive Server suivants : • ASE ADO.NET Data Provider 1.1 • ASE OLE DB Provider by Sybase 12.5.1 • ASE ODBC Driver by Sybase 12.5.1
Chargement dynamique des bibliothèques TIBCO	Désormais, les bibliothèques JMS TIBCO sont chargées de manière dynamique et non plus liées de manière statique à l'exécutable d'Adaptive Server.
Prise en charge de JRE	Adaptive Server version 12.5.4 inclut le protocole JRE 1.4.
Modifications du module externe d'Adaptive Server	Le module externe d'Adaptive Server prend en charge l'accès à la base de données archive et la complexité des mots de passe.
Mise à jour des catalogues système	La commande à l'échelle du serveur allow updates to system catalogs est prioritaire sur le paramétrage de la procédure stockée pour la commande allow updates.
Modifications des tables de contrôle	Les tables de contrôle monSysStatement et monProcessStatement ont été modifiées.
Modifications de syscomments	Lorsque le texte source d'une procédure stockée ou d'un trigger est enregistré dans la table système syscomments, une requête utilisant select * est stockée dans syscomments, étendant la liste des colonnes référencées dans la commande select *.
Prise en charge de la mémoire partagée dans les environnements Terminal Server de Windows	Pour répondre aux exigences de mémoire partagée Terminal Server de Windows, Adaptive Server version 12.5.4 introduit la nouvelle variable d'environnement SYBASE_TS_MODE.
Trigger de connexion global	Adaptive Server version 12.5.4 permet de définir un nouveau trigger de connexion global exécuté à chaque connexion d'un utilisateur.
Exportation d'options "set" à partir d'un trigger de connexion	Adaptive Server version 12.5.4 permet aux options set des triggers de connexion de rester valides pendant toute la session d'un utilisateur.
Adaptive Server version 12.5.3a	
Prise en charge des colonnes cryptées	Adaptive Server vous permet de crypter des données au niveau de la colonne. Les mécanismes d'authentification et de contrôle d'accès garantissent que seuls les utilisateurs correctement identifiés et dûment habilités aient accès aux données. La fonctionnalité Colonnes cryptées d'Adaptive Server est plus facile à utiliser que le cryptage de niveau intermédiaire ou au niveau de l'application client. Aucune modification de l'application n'est nécessaire pour activer la prise en charge des colonnes cryptées.

Fonctionnalité d'Adaptive Server	Description
Adaptive Server version 12.5.3	
Améliorations de Secure Sockets Layer	Nouvelles SSL CipherSuites prenant en charge l'algorithme Advanced Encryption Standard (défini dans FIPS-197) pour le cryptage des communications réseau. Les normes Advanced Encryption Standard vous permettent de choisir entre des clés de cryptage 128 ou 256 bits.
Prise en charge de la sauvegarde et de la restauration de bases de données interplate-forme	Adaptive Server prend en charge les sauvegardes et les restaurations de bases de données entre des plates-formes présentant une architecture différente. Vous pouvez exécuter les commandes dump database et load database depuis une plate-forme big endian vers une plate-forme little endian, ou depuis une plate-forme little endian vers une plate-forme big endian.
Importation de statistiques pour des tables proxy	Si les statistiques de table et d'index pertinentes sont disponibles lorsque vous exécutez la commande update statistics sur une table proxy d'un serveur distant, les catalogues de table sont importés dans les objets systabstats et sysstatistics locaux.
Prise en charge de la fonctionnalité n_sup	Utilisez la clause top n pour limiter le nombre de lignes figurant dans le jeu de résultats au nombre de lignes spécifié par le nombre entier. Adaptive Server Enterprise prend en charge la clause top n dans des instructions select de requêtes externes, mais pas dans la liste de sélection d'une sous-requête.
Améliorations de Historical Server	Adaptive Server vous permet d'envoyer des données de contrôle depuis Historical Server vers une base de données située sur un serveur Adaptive Server spécifique.
Améliorations de Real Time Data Services	Utilisez sp_configure pour définir le nombre de threads natifs et le temps d'attente de la messagerie.
Gestionnaire de ressources	Adaptive Server fournit les limites d'utilisation des ressources nécessaires pour permettre aux administrateurs système d'empêcher les requêtes et les transactions de monopoliser les ressources du serveur. Dans Adaptive Server version 12.5.3, lorsque l'administrateur système modifie une limite d'utilisation des ressources, tous les utilisateurs connectés à la session voient le changement.
Allocation de pages pour les tables DOL partitionnées	Adaptive Server version 12.5.3 évite toute utilisation d'espace supplémentaire en remplissant les extents alloués existants dans la page d'allocation cible, même si ces extents sont attribués à d'autres partitions.
Améliorations des connexions utilisateur	Les améliorations apportées aux connexions utilisateur incluent la mise à jour d'un message d'erreur et une correction au niveau des sockets réservés.
dtdValidation	L'option dtdValidate comprend trois paramètres supplémentaires : no, yes et strict.

Fonctionnalité d'Adaptive Server	Description
Améliorations de sybmigrate	L'outil sybmigrate vous permet de migrer d'une version à l'autre d'Adaptive Server Enterprise et prend en charge les serveurs sources des versions 12.0 à 12.5.3.
Prise en charge de nouvelles langues dans Enhanced Full-Text Search Specialty Data Store (EFTS)	EFTS prend désormais en charge les langues suivantes : • le chinois traditionnel sur les plates-formes Windows et Solaris ; • l'arabe, l'hébreu, le thaï et le russe sur la plate-forme Linux.
Compteurs de moniteur et sp_sysmon	Dans Adaptive Server version 12.5.3, plusieurs améliorations ont été apportées afin de rendre plus performants les outils de contrôle les plus souvent utilisés.
Adaptive Server version 12.5.2	
Prise en charge PAM (Pluggable Authentication Module)	La prise en charge du PAM (Pluggable Authentication Module) permet à plusieurs modules de services d'authentification d'être empilés et rendus disponibles, sans modification des applications qui requièrent l'authentification.
Prise en charge des bibliothèques Kerberos natives	Adaptive Server assure la prise en charge des bibliothèques Kerberos natives suivantes : • Prise en charge des bibliothèques Cybersafe • Prise en charge des bibliothèques MIT Kerberos • Interopérabilité des répertoires actifs pour l'authentification des utilisateurs • Prise en charge de Kerberos dans jConnect
Prise en charge des sauvegardes protégées par mot de passe	Vous pouvez protéger vos sauvegardes de bases de données des chargements non autorisés à l'aide du paramètre password de la commande dump database. Si vous activez le paramètre password lors de la sauvegarde de base de données, vous devez également entrer ce mot de passe lorsque vous restaurez la base de données.
Améliorations du contrôle d'accès	Adaptive Server comprend les améliorations du contrôle d'accès suivantes : • Autorisations restreintes sur les catalogues système • Granularité améliorée pour set proxy • Octroi et révocation des commandes d'administration
Prise en charge des algorithmes certifiés FIPS 140	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. Cette norme se base sur la cryptographie par clé publique.
Améliorations du cache d'instructions	Le cache d'instructions est utilisé pour l'enregistrement des instructions SQL mises en cache.

Fonctionnalité d'Adaptive Server	Description
Prise en charge des services XML	Les modifications apportées aux services XML concernent quatre domaines principaux : • Langage de requêtes XML étendu pour la fonction intégrée xmlextract et le prédicat xmltest • Prise en charge améliorée des types de données dans la clause for xml des instructions select • Prise en charge améliorée des types de données pour xmlextract, xmlparse et xmlrepresentation • Exemple de code Java-XML amélioré
Real Time Messaging Services	Adaptive Server 12.5.2 inclut une fonctionnalité de messagerie avec le package d'options Real Time Data Services (RTDS). Cette fonctionnalité simplifie le développement des applications qui interagissent avec les systèmes de messagerie et les bases de données.
Prise en charge des services Web	Un service Web est une application modulaire autonome accessible par le biais d'une connexion réseau. En utilisant un service Web, vous échangez les performances pour une interopérabilité accrue.
Prise en charge de IPv6	Adaptive Server prend en charge Internet Protocol version 6 (IPv6).
Améliorations des moteurs de recherche Enhanced Full-Text (EFTS)	EFTS introduit les améliorations suivantes : • Modifications apportées à l'installation et au répertoire • Autorisation d'arrêt • Les clauses index_any prennent en charge jusqu'à 16 000 octets. • Nouvelle pseudo colonne total_docs • Clés primaires
Prise en charge des sauvegardes de bases de données compressées	La commande dump d'Adaptive Server version 12.5.2 inclut un paramètre compression qui vous permet de réaliser des sauvegardes compressées de vos bases de données.
Sauvegardes et restaurations de bases de données protégées par mot de passe	Les commandes dump et load database d'Adaptive Server 12.5.2 incluent un paramètre password qui vous permet de protéger par mot de passe vos sauvegardes de bases de données.
Prise en charge de la fonctionnalité Failover dans Veritas 3.5	Vous pouvez à présent configurer Adaptive Server sur les plates-formes Linus pour la fonctionnalité Failover sur Veritas 2.1.
Prise en charge des mémoires de grande taille	La prise en charge des mémoires de grande taille par Adaptive Server pour les systèmes d'exploitation Enterprise Linux 32 bits permet d'augmenter la quantité de mémoire disponible dans Adaptive Server de 2,7 Go à 64 Go. L'augmentation de la quantité de mémoire disponible dans Adaptive Server améliore les performances en réduisant significativement le nombre d'accès disque du serveur.

CHAPITRE 2

Améliorations de la sécurité

Améliorations de Kerberos

Kerberos a été amélioré des manières suivantes :

- Vous pouvez désormais définir un nom de serveur principal pour l'authentification Kerberos.
- Les options sp_modifylogin et sp_addlogin authenticate with prennent en charge l'authentification Kerberos.
- Prise en charge de sybmapname
- Prise en charge de la bibliothèque cliente MIT Kerberos
- Prise en charge étendue des plates-formes pour Kerberos

Définition du nom principal d'Adaptive Server pour l'authentification Kerberos

Le nom principal est le nom utilisé par le serveur pour réaliser une authentification à l'aide du Kerberos Key Distribution Center (KDC). Lorsque plusieurs instances d'Adaptive Server tournent, vous devez posséder des noms principaux différents pour chacune d'entre elles.

Dans Adaptive Server version 12.5.4, vous pouvez utiliser une nouvelle option de serveur de données et une nouvelle variable d'environnement pour définir un nom principal différent du nom d'Adaptive Server. Le nom d'Adaptive Server est spécifié par les variables d'environnement DSLISTEN et DSQUERY, ou par l'option de ligne de commande dataserver `"-s servername"`.

Utilisation de SYBASE_PRINCIPAL pour définir le nom principal d'Adaptive Server

Par défaut, le nom principal est le nom d'Adaptive Server. Pour en indiquer un autre, définissez SYBASE_PRINCIPAL avant de démarrer Adaptive Server pour utiliser Kerberos :

```
setenv SYBASE_PRINCIPAL <name of principal>
```

Une fois le nom principal d'Adaptive Server défini, Adaptive Server utilise la valeur de cette variable pour s'authentifier avec Kerberos.

Utilisation de l'option *-k* du serveur de données pour définir le nom principal d'Adaptive Server

Vous pouvez utiliser l'option de ligne de commande suivante pour définir le nom principal d'Adaptive Server au démarrage de celui-ci.

```
-k <server principal name>
```

Remarque Si -k définit le nom principal d'Adaptive Server, Adaptive Server ne tient pas compte de la variable d'environnement.

Utilisation de *-k* et de SYBASE_PRINCIPAL pour définir le nom principal d'Adaptive Server

Lorsqu'Adaptive Server est lancé avec le mécanisme de sécurité Kerberos, Adaptive Server utilise d'abord le nom principal défini avec l'option -k pour l'authentification Kerberos. Si l'option -k n'est pas définie, Adaptive Server recherche le nom principal dans la variable d'environnement SYBASE_PRINCIPAL. Si aucun des deux n'est défini, Adaptive Server utilise le nom du serveur pour l'authentification.

Dans l'exemple suivant, le nom d'Adaptive Server sera `"ase1254"` et le nom de domaine actuel `"MYREALM.COM"`. Le nom d'Adaptive Server est spécifié dans la ligne de commande avec le paramètre -s pour le serveur de données. Le domaine actuel est spécifié dans *libtcl.cfg* par une valeur d'attribut `secbase` :

```
[SECURITY]
csfkrb5=libskrb.so libgss=/krb5/lib/libgss.so
secbase=@MYREALM.COM
```

Le nom principal par défaut d'Adaptive Server est `"ase1254@MYREALM.COM"`. Si le nom principal défini dans le fichier *keytab* d'Adaptive Server est `"aseprincipal@MYREALM.COM"`, vous pouvez ignorer le nom principal par défaut en spécifiant un nom principal de serveur à l'aide de l'option 1 ou 2 ci-dessous :

Option 1 : '-k' est spécifié %

```
$SYBASE/$SYBASE_ASE/bin/dataserver -dmaster.dat
-s ase1254 -k aseprincipal@MYREALM.COM
```

Le nom principal d'Adaptive Server utilisé pour réaliser une authentification à l'aide de Kerberos est `aseprincipal@MYREALM.COM`.

Option 2 : '-k' n'est pas spécifié mais SYBASE_PRINCIPAL est appliqué

```
setenv SYBASE_PRINCIPAL aseprincipal@MYREALM.COM
$SYBASE/$SYBASE_ASE/bin/dataserver –dmaster.dat
-s ase1254
```

Le nom principal d'Adaptive Server utilisé pour réaliser une authentification à l'aide de Kerberos est la valeur de *$SYBASE_PRINCIPAL*, `"aseprincipal@MYREALM.COM"`.

Option 3 : ni '-k' ni SYBASE_PRINCIPAL n'est défini %

```
$SYBASE/$SYBASE_ASE/bin/dataserver –dmaster.dat
-s ase1254
```

Le nom principal d'Adaptive Server utilisé pour réaliser une authentification à l'aide de Kerberos est `ase1254@MYREALM.COM`.

Pour plus d'informations sur Kerberos, reportez-vous à la section Sécurité du *Guide d'administration du système, Volume Un*.

Option *sp_modifylogin* et *sp_addlogin authenticate with*

Dans Adaptive Server version 12.5.4, l'option authenticate with de sp_modifylogin ou sp_addlogin exige que le login utilise *uniquement* un mécanisme d'authentification spécifié. Les mécanismes d'authentification pris en charge sont les suivants :

- ASE
- LDAP
- PAM
- KERBEROS
- ANY

L'utilisation de authenticate with avec ces mécanismes d'authentification pris en charge vous permet d'ignorer les paramètres de configuration à l'échelle du serveur unified login required, enable ldap user auth et enable pam user auth.

Si plus d'un mécanisme d'authentification externe est configuré et si aucune option authenticate with spécifique au login n'a été définie, le mécanisme d'authentification externe est déterminé dans l'ordre suivant :

1 Kerberos

2 LDAP

3 PAM

Par exemple, si PAM et LDAP sont configurés, LDAP est choisi pour une authentification externe, et non PAM.

Au moment de l'authentification, un et un seul mécanisme d'authentification externe est tenté. Selon la valeur des paramètres de configuration, il est possible de tenter une authentification ASE lorsque l'authentification externe échoue.

Lorsqu'aucun des mécanismes d'authentification externe n'est configuré, Adaptive Server utilise l'authentification ASE.

Utilisation de la commande "authenticate with" pour ignorer les options d'authentification à l'échelle du serveur

Remarque Vous devez disposer d'autorisations sso_role pour modifier l'option authenticate with d'un login.

Pour configurer des mécanismes d'authentification externe tels que Kerberos, LDAP ou PAM, Sybase vous recommande de déterminer le paramètre d'authentification à l'échelle du serveur correspondant à la stratégie de votre entreprise en matière de sécurité. Le paramètre à l'échelle du serveur convient pour la plupart des connexions clientes. Ensuite, vous pouvez associer les logins individuels à un autre mécanisme d'authentification à l'aide de l'option authenticate with.

Vous pouvez utiliser "authenticate with" pour spécifier les mécanismes d'authentification externe Kerberos, LDAP et PAM. Vous pouvez également émettre la commande sp_modifylogin ou sp_addlogin authenticate with pour activer le mécanisme d'authentification ASE de manière à n'utiliser que le mécanisme d'authentification interne d'Adaptive Server. Pour autoriser n'importe quel mécanisme d'authentification, utilisez authenticate with ANY.

Remarque Lorsque le mécanisme d'authentification ANY est appliqué pour un login, ce dernier utilise les paramètres de configuration à l'échelle du serveur pour gérer l'authentification. Le paramètre du mécanisme d'authentification par défaut pour un login est ANY.

sp_modifylogin vérifie aussi l'absence de conflit avec tout mappage des logins spécifiés par une commande sp_maplogin précédente. Voir « Renforcement des contrôles sur le mappage des logins » page 32 pour plus de détails.

Exemple 1 : création d'un compte local pour exécuter une application en batch Imaginez un environnement utilisant Kerberos pour un référentiel centralisé de comptes utilisateurs et exigeant que tous ses utilisateurs s'authentifient avec Kerberos. Adaptive Server devrait configurer Kerberos en définissant les paramètres suivants :

```
sp_configure  "use security services", 1
go

sp_configure "unified login required", 1
go
```

Ces paramètres de configuration nécessitent à présent que tous les logins utilisateurs autres que le login “sa” s'authentifient à l'aide de Kerberos pour avoir accès à Adaptive Server.

Imaginez à présent qu'un traitement en batch nocturne soit exécuté par l'administrateur de la base de données ou par l'opérateur d'Adaptive Server, qui peut s'authentifier localement sans qu'un compte n'existe dans le référentiel Kerberos. Pour ce faire, il fait usage de l'option authenticate with poursp_modifylogin ou sp_addlogin.

```
sp_addlogin nightlybatch, localpassword, ...
go
sp_modifylogin nightlybatch, 'authenticate with', 'ASE'
go
```

Exemple 2 : migration des utilisateurs de l'authentification d'Adaptive Server vers l'authentification utilisateur LDAP Dans cet exemple, une approche par étapes visant à faire passer les clients d'une authentification ASE locale vers une authentification utilisateur LDAP est proposée. Le serveur de répertoire LDAP a été installé mais n'a pas encore été alimenté avec tous les comptes utilisateurs. Un petit nombre d'utilisateurs a accepté de participer à un programme pilote pour tester LDAP à des fins d'authentification externe sur Adaptive Server.

```
sp_configure 'enable ldap user auth', 1
go
```

Ce paramètre autorise le basculement vers une authentification ASE lorsque l'authentification avec le serveur de répertoire LDAP échoue ou lorsque le serveur LDAP n'est pas disponible. Utilisateurs sans compte dans LDAP, basculement vers l'authentification ASE. Les utilisateurs participant au programme pilote sont ajoutés au serveur de répertoire LDAP et peuvent commencer à s'authentifier à l'aide de celui-ci.

Un utilisateur peut déterminer quel mécanisme d'authentification a été utilisé pour authenticate with avec la variable globale @@*authmech* :

```
select @@authmech
```

À mesure que le programme pilote avance et que l'authentification LDAP est utilisée, il est possible de demander aux participants de ne plus utiliser que l'authentification LDAP :

```
sp_maplogin loginame, 'authenticate with', 'ldap'
go
```

Lorsque le programme pilote arrive à son terme et que l'authentification utilisateur LDAP est appliquée à tous les utilisateurs, appliquez au paramètre de configuration la valeur 2. Tous les logins dont le paramètre authenticate with a la valeur LDAP pendant le programme pilote peuvent être réinitialisés à la valeur par défaut ANY. Les logins devront toujours s'authentifier à l'aide de LDAP, parce que le paramètre de configuration a la valeur 2.

```
sp_configure 'enable ldap user auth', 2
go
sp_maplogin loginame, 'authenticate with', 'any'
go
```

Remarque Si le paramètre authenticate with du login est réglé sur un mécanisme d'authentification spécifique tel que LDAP, Kerberos, PAM ou ASE, ce login ne peut utiliser que ce mécanisme d'authentification. Le mieux consiste à l'utiliser pour définir des exceptions aux paramètres à l'échelle du serveur et pour imposer l'utilisation d'un mécanisme d'authentification particulier.

Utilisation de *sybmapname* pour gérer les noms principaux des utilisateurs

Le rôle de sybmapname consiste à convertir les noms principaux d'utilisateurs externes employés dans l'environnement Kerberos dans l'espace de nom des logins utilisateurs d'Adaptive Server. sybmapname est un objet partagé, personnalisable par l'utilisateur, qui peut mapper les noms donnés sur son buffer d'entrée avec un nom adapté pour le login d'Adaptive Server sur son buffer de sortie.

L'objet sybmapname partagé peut être utilisé pour effectuer un mappage personnalisé entre le nom principal de l'utilisateur et le nom de login d'Adaptive Server. Cet objet partagé est chargé de manière facultative au démarrage du serveur, et la fonction syb__map_name contenue dans l'objet partagé est appelée après une authentification Kerberos fructueuse et juste avant que le nom principal de l'utilisateur ne soit mappé avec un login dans la table syslogins. Il peut être personnalisé pour répondre aux besoins de l'utilisateur. Cette fonction est utile lorsque le nom principal de l'utilisateur et le nom de login à mapper ne sont pas identiques.

La logique personnalisable est la fonction :

```
syb__map_name(NAMEMAPTYPE *protocol, char *orig,
int origlen, char *mapped, int *mappedlen)
```

où :

- `NAMEMAPTYPE *protocol` fait référence à une structure réservée à l'usage de cette fonction.
- `char *orig` est un buffer d'entrée qui ne se termine pas par une valeur NULL.
- `int origlen` est la longueur du buffer d'entrée. Elle doit être inférieure ou égale à 255 caractères.
- `char *mapped` est un buffer de sortie qui ne doit pas se terminer par une valeur NULL.
- `int *mappedlen` est une longueur de buffer de sortie. Elle doit être inférieure ou égale à 30.

La fonction renvoie une valeur supérieure à 0 si le mappage réussit, une valeur de 0 si aucun mappage n'a lieu et une valeur inférieure à 0 lorsqu'une erreur se produit dans syb__map_name(). Lorsqu'une erreur se produit, un message s'affiche dans le journal d'erreurs d'Adaptive Server afin de faire état de l'échec du mappage.

Par exemple, pour effectuer une authentification utilisateur Kerberos sur Adaptive Server, vous devez commencer par configurer Adaptive Server afin qu'il utilise le mécanisme de sécurité Kerberos. Pour obtenir de plus amples informations sur la configuration de Kerberos, reportez-vous au *Guide d'administration système* d'Adaptive Server et à la documentation Open Client/Server, ainsi qu'au livre blanc intitulé “Configuring Kerberos for Sybase” (Configuration de Kerberos pour Sybase)the Sybase Web site à http://www.sybase.com/detail?id=1029260

Un fichier exemple *sybmapname.c* se trouve sous *$SYBASE/$SYBASE_ASE/sample/server/sybmapname.c*

Remarque Modifiez le fichier de manière à mettre en œuvre votre logique à l'aide d'une logique simple et sans erreur. Faites preuve de prudence lors du codage, étant donné que celui-ci peut entraver le bon fonctionnement d'Adaptive Server. Voir « Précautions à respecter lors de l'utilisation de sybmapname » page 18.

Compilez l'objet partagé ou le fichier dll en utilisant la commande makefile générique fournie pour votre plate-forme. Il est possible que vous deviez modifier la commande makefile afin de l'adapter aux paramètres de votre plate-forme.

Placez l'objet partagé résultant à un emplacement spécifié dans votre variable *$LD_LIBRARY_PATH* sur les machines UNIX ou *PATH* sur les machines Windows. Le fichier doit posséder une autorisation en lecture et un droit d'exécuter pour l'utilisateur ‘sybase’ du système d'exploitation.

Remarque Sybase recommande que seul l'utilisateur ‘sybase’ possède ces autorisations et que tout autre accès soit interdit.

Vérification du nom de connexion (login) à Adaptive Server à l'aide de l'authentification Kerberos

Pour vérifier votre nom de connexion (login) à Adaptive Server à l'aide de l'authentification Kerberos, supposez que :

- *$SYBASE* fait référence à votre version et à votre répertoire d'installation.
- *$SYBASE_ASE* fait référence au répertoire d'installation d'Adaptive Server contenant le binaire de votre serveur.
- *$SYBASE_OCS* fait référence au répertoire d'installation d'Open Client/Server.

Exemple 1 Si le nom principal d'un client est `user@REALM`, et que l'entrée correspondante dans la table syslogins est `user_REALM`, alors sybmapname peut être codé pour accepter la chaîne d'entrée `user@realm` et convertir la chaîne d'entrée dans la chaîne de sortie `user_REALM`.

Exemple 2 Si le nom principal du client est `user`, et si l'entrée correspondante dans la table syslogins est `USER`, alors sybmapname peut être codé pour accepter la chaîne d'entrée `user` et la convertir dans la chaîne de majuscules `USER`.

sybmapname est chargé par Adaptive Server au moment de l'exécution et utilise sa logique pour effectuer le mappage nécessaire.

Les actions et le résultat suivants illustrent la fonction "sybmapname" décrite dans l'exemple 2. Le fichier *sybmapname.c* contenant la définition personnalisée de syb__map_name() doit être compilé et généré sous la forme d'un objet partagé (ou DLL), puis placé à l'endroit approprié dans le chemin d'accès. Adaptive Server doit être démarré avec le mécanisme de sécurité Kerberos activé.

Pour initialiser la TGT :

```
$ /krb5/bin/kinit johnd@public
Password for johnd@public:
$
```

Pour lister la TGT :

```
$ /krb5/bin/klist
   Cache Type: Kerberos V5 credentials cache
   Cache Name: /krb5/tmp/cc/krb5cc_9781
Default principal: johnd@public
```

Connectez-vous en tant que “sa” et vérifiez le login utilisateur de `'johnd'` :

```
$ $SYBASE/$SYBASE_OCS/bin/isql -Usa -P
      -Ipwd`/interfaces
1>

1> sp_displaylogin johnd
2> go
No login with the specified name exists.
(return status = 1)

1> sp_displaylogin JOHND
2> go
Suid: 4
Loginame: JOHND
Fullname:
Default Database: master
Default Language:
Auto Login Script:
Configured Authorization:
Locked: NO
Password expiration interval: 0
Password expired: NO
Minimum password length: 6
Maximum failed logins: 0
Current failed login attempts:
Authenticate with: ANY
(return status = 0)
```

Authentification Kerberos réussie, avec mappage de `johnd` en minuscules avec les majuscules `JOHND` à l'aide de l'utilitaire sybmapname. L'utilisateur `johnd` est autorisé à se connecter à Adaptive Server :

```
$ $SYBASE/$SYBASE_OCS/bin/isql -V -I`pwd`/interfaces
1>
```

Précautions à respecter lors de l'utilisation de *sybmapname*

Vous devez tenir compte des considérations suivantes lors du codage relatif à sybmapname :

- Faites preuve de prudence avec le programme exemple sybmapname.c program et toute modification apportée à celui-ci. Évitez tout code susceptible d'appeler les commandes segfault, exit(), system calls(), de modifier les signaux UNIX ou d'effectuer un appel bloquant. Des codes ou appels erronés risquent d'entraver le bon fonctionnement du moteur Adaptive Server en cours d'exécution.

  Remarque Sybase ne peut être tenu pour responsable des erreurs de codage dans sybmapname. Le code est la propriété de l'utilisateur, qui en assume la pleine responsabilité.

- Optez pour une approche de codage défensive, vérifiez tous les pointeurs avant d'en supprimer les références et évitez les appels système. Il doit s'agir d'une fonction rapide de filtrage des noms.
- Évitez d'utiliser des instructions `'goto'`. En effet, selon la plate-forme utilisée, celles-ci peuvent avoir des effets secondaires inattendus.
- Si vous utilisez plusieurs domaines, veillez à mapper les noms principaux des utilisateurs avec un nom de login adapté, qui reflète les informations relatives au domaine. Prenons l'exemple de deux utilisateurs ayant les noms principaux `userA@REALMONE` et `userB@REALMTWO`. Ils sont mappés avec les noms de login `userA_REALMONE` et `userB_REALMTWO` respectivement, au lieu de `userA` ou `userB`. Ceci permet de distinguer les deux utilisateurs qui appartiennent à des domaines différents.

Prise en charge de la bibliothèque cliente MIT Kerberos

Adaptive Server a été testé avec une version plus récente des librairies clientes MIT à l'aide de librairies clientes MIT Kerberos et est désormais certifié pour celles-ci. Le niveau produit MIT est MIT Kerberos version 1.4.x pour les plates-formes UNIX.

D'autres correctifs destinés à améliorer la fiabilité d'Adaptive Server avec Kerberos dans des conditions très astreignantes sont disponibles dans la version 12.5.4 d'Adaptive Server.

Prise en charge étendue des plates-formes pour MIT Kerberos

Adaptive Server prend en charge MIT Kerberos sur la nouvelle plate-forme suivante :

- HP-UX Itanium 64 bits

Améliorations de l'authentification utilisateur LDAP

L'authentification utilisateur LDAP a été améliorée de cinq manières, que voici :

- Prise en charge de la recherche de serveurs secondaires
- Améliorations en termes de robustesse de l'AU LDAP
- Basculement en cas d'erreurs de communication avec le serveur LDAP
- Améliorations de la communication liées à l'expiration du mot de passe
- Renforcement des contrôles sur le mappage des logins

Configuration d'Adaptive Server pour l'authentification utilisateur LDAP

L'authentification utilisateur LDAP permet aux applications clientes d'envoyer le nom de l'utilisateur et le mot de passe à Adaptive Server pour une authentification via le serveur LDAP et non syslogins. L'utilisation du serveur LDAP à des fins d'authentification vous permet d'avoir recours à des mots de passe à l'échelle du serveur, et non plus à des mots de passe spécifiques à Adaptive Server ou à une application donnée. Grâce à l'authentification utilisateur LDAP, vous pouvez simplifier et centraliser l'administration des utilisateurs.

L'authentification utilisateur LDAP fonctionne avec des serveurs de répertoire répondant aux normes du protocole LDAP version 3, dont Active Directory, iPlanet et OpenLDAP Directory Server.

Vous pouvez utiliser deux algorithmes d'authentification avec l'authentification utilisateur LDAP, la différence étant la manière d'obtenir un nom distinctif (DN) pour l'utilisateur. Les algorithmes utilisent :

- un DN composé pour l'authentification, disponible pour Adaptive Server version 12.5.1 ou ultérieure, ou

- un DN recherché pour l'authentification, disponible pour Adaptive Server version 12.5.2 et ultérieure.

La structure de données primaire utilisée avec le protocole LDAP est l'URL LDAP.

Un URL LDAP définit un jeu d'objets ou de valeurs sur un serveur LDAP. Adaptive Server utilise les URL LDAP pour définir un serveur LDAP et des critères de recherche à appliquer pour authentifier les requêtes de connexion.

L'URL LDAP utilise la syntaxe suivante :

ldapurl::=ldap://hôte:port/noeud/?attributs?base | one | sub?filtre

où :

- *hôte* est le nom d'hôte du serveur LDAP.
- *port* est le numéro de port du serveur LDAP.
- *noeud* spécifie le nœud dans la hiérarchie d'objets où démarrer la recherche.
- *attributs* est une liste d'attributs à renvoyer dans le jeu de résultats. Chaque serveur LDAP peut prendre en charge une liste différente d'attributs.
- base | one | sub qualifie les critères de recherche. base spécifie une recherche de nœud de base ; one spécifie une recherche de nœud de base et un sous-niveau du nœud de base ; sub spécifie une recherche de nœud de base et tous les sous-niveaux de nœuds.
- filtre spécifie le ou les attributs à authentifier. Le filtre peut être simple, tel que `uid=*`, ou composé, tel que `(uid=*)(ou=group)`.

Algorithme DN composé

Les étapes suivantes décrivent la séquence de connexion lorsque vous utilisez l'algorithme DN composé :

1 Open Client™ se connecte à un port d'écoute d'Adaptive Server.

2 Celui-ci accepte la connexion.

3 Open Client envoie un enregistrement interne du login.

4 Adaptive Server lit l'enregistrement du login.

5 Adaptive Server se lie au serveur LDAP avec un DN composé de l'URL primaire et du nom de login contenu dans l'enregistrement. Cette liaison utilise également le mot de passe de l'enregistrement du login.

6 Le serveur LDAP authentifie l'utilisateur, puis renvoie un message de réussite ou d'erreur.

7 Si l'URL primaire spécifie une recherche, Adaptive Server envoie la requête de recherche au serveur LDAP.

8 Le serveur LDAP renvoie les résultats de la recherche.

9 Adaptive Server accepte ou rejette le login, selon les résultats de la recherche.

Algorithme DN recherché

Les étapes suivantes décrivent la séquence de connexion lorsque vous utilisez l'algorithme DN recherché :

1 Open Client se connecte à un port d'écoute d'Adaptive Server.

2 Celui-ci accepte la connexion.

3 Open Client envoie un enregistrement interne du login.

4 Adaptive Server lit l'enregistrement du login.

5 Adaptive Server se lie au serveur LDAP avec un compte d'accès au serveur de répertoire.

6 Le serveur LDAP authentifie l'utilisateur, puis renvoie un message de réussite ou d'erreur.

La connexion établie aux étapes 5 et 6 peut rester active entre les tentatives d'authentification depuis Adaptive Server afin de réutiliser les connexions aux recherches de DN.

7 Adaptive Server envoie des requêtes de recherche au serveur LDAP sur la base du nom de login contenu dans l'enregistrement et de l'URL de recherche du DN.

8 Le serveur LDAP renvoie les résultats de la recherche.

9 Adaptive Server lit les résultats afin d'obtenir une valeur d'attribut de l'URL de recherche du DN.

10 Adaptive Server utilise la valeur de l'attribut comme DN et le mot de passe de l'enregistrement du login pour effectuer une liaison au serveur LDAP.

11 Le serveur LDAP authentifie l'utilisateur, puis renvoie un message de réussite ou d'erreur.

12 Si l'URL primaire spécifie une recherche, Adaptive Server envoie la requête de recherche au serveur LDAP.

13 Le serveur LDAP renvoie les résultats de la recherche.

14 Adaptive Server accepte ou rejette le login, selon les résultats de la recherche.

Adaptive Server signale une erreur de connexion générique au client si l'un des critères d'authentification n'est pas rempli.

Vous pouvez passer les étapes 12 et 13 en ne spécifiant pas de critères de recherche dans les chaînes d'URL primaire ou secondaire. Dans ce cas, l'authentification se termine et indique si l'opération a réussi ou échoué, comme décrit à l'étape 11.

Prise en charge d'un serveur de recherche secondaire

Adaptive Server version 12.5.4 fournit un support ininterrompu aux clients Adaptive Server authentifiés par un serveur LDAP. Vous pouvez désormais spécifier un serveur de recherche LDAP secondaire vers lequel basculer en cas d'échec ou d'arrêt planifié du serveur primaire.

La santé du jeu d'URL est surveillée par le biais des états suivants :

- INITIAL indique que l'authentification utilisateur LDAP n'est pas configurée.
- RESET indique que l'URL a été saisi avec des commandes d'administration Adaptive Server.
- READY indique que l'URL est prêt à accepter des connexions.
- ACTIVE indique que l'URL a effectué une authentification utilisateur LDAP fructueuse.
- FAILED indique qu'un problème est survenu lors de la connexion au serveur LDAP.
- SUSPENDED indique que l'URL est en mode de maintenance et ne sera pas utilisée.

La séquence d'événements suivante décrit le basculement vers le serveur secondaire et le retour manuel au serveur primaire :

1 Les jeux d'URL primaires et secondaires sont configurés et à l'état READY.

2 Les connexions sont authentifiées à l'aide de l'infrastructure du serveur primaire.

3 Le serveur primaire rencontre un échec, et son état passe à FAILED.

4 Les connexions commencent automatiquement l'authentification par le biais de l'infrastructure du serveur secondaire.

5 Le serveur primaire est réparé et remis en ligne par un administrateur LDAP. L'état du serveur LDAP primaire est réglé sur READY par un administrateur Adaptive Server.

6 Les nouvelles connexions sont authentifiées à l'aide du serveur primaire.

Remarque Après le basculement d'Adaptive Server vers le serveur LDAP secondaire, un administrateur de base de données doit activer manuellement le serveur LDAP primaire pour que celui-ci puisse être réutilisé.

Lorsqu'Adaptive Server rencontre des erreurs en se connectant à un serveur LDAP, il effectue trois nouvelles tentatives d'authentification. Si les erreurs persistent, le serveur LDAP est considéré comme FAILED. Reportez-vous à « Détection et résolution des erreurs liées à l'authentification utilisateur LDAP » page 27 pour plus d'informations sur les erreurs LDAP qui obligent Adaptive Server à effectuer de nouvelles tentatives.

Adaptive Server version 12.5.4 introduit les nouvelles options sp_ldapadmin suivantes pour la prise en charge des serveurs LDAP de recherche secondaires :

- Pour définir l'URL de recherche de DN secondaire, entrez :

  ```
  sp_ldapadmin set_secondary_dn_lookup_url, <URL>
  ```

- Pour définir le compte d'accès administrateur correspondant à l'URL de recherche de DN secondaire, entrez :

  ```
  sp_ldapadmin set_secondary_access_acct, <DN>,
  <mot de passe>
  ```

- Pour suspendre l'utilisation d'un URL primaire ou secondaire à des fins d'authentification, entrez :

  ```
  sp_ldapadmin suspend, {primary | secondary}
  ```

- Pour activer le jeu d'URL primaires ou secondaires à des fins d'authentification, entrez :

  ```
  sp_ldapadmin activate, {primary | secondary}
  ```

- Pour afficher des détails sur les paramètres et l'état du serveur LDAP primaire et secondaire, entrez :

  ```
  sp_ldapadmin list
  ```

  sp_ldapadmin list combine les sorties précédentes de list_access_acct et list_urls. Le résultat prévu pour les serveurs primaire et secondaire est le suivant :

  - URL de recherche
  - URL de recherche du DN
  - DN du compte d'accès
  - Active [True | False]
  - Status [Ready | Active | Failed | Suspended | Reset]

Adaptive Server version 12.5.4 comprend les modifications suivantes de l'option sp_ldapadmin pour la prise en charge des serveurs secondaires.

- Pour afficher les URL de recherche de DN pour le serveur secondaire, entrez :

  ```
  sp_ldapadmin list_urls
  ```

- Pour afficher le compte administrateur correspondant à l'URL de recherche de DN secondaire, entrez :

  ```
  sp_ldapadmin list_access_acct
  ```

- Pour afficher les nouvelles sous-commandes, entrez :

  ```
  sp_ldapadmin [help | invalid sub-command]
  ```

Transitions de l'état du serveur LDAP

Les tables suivantes listent les transitions de l'état du serveur LDAP lorsque chacune des commandes sp_ldapadmin est exécutée.

La Tableau 2-1 montre les transitions de l'état lorsque vous exécutez sp_ldapadmin set_URL, où set_URL représente l'une des commandes suivantes :

- set_dn_lookup_url
- set_primary_url
- set_secondary_dn_lookup_url
- set_secondary_url

Tableau 2-1 : Transitions de l'état lors de l'exécution de la commande sp_ldapadmin set_URL

État initial	État final
INITIAL	RESET
RESET	RESET
READY	READY
ACTIVE	RESET
FAILED	RESET
SUSPENDED	RESET

La Tableau 2-2 montre les transitions de l'état lorsque vous exécutez sp_ldapadmin suspend.

Tableau 2-2 : Transitions de l'état lors de l'exécution de la commande sp_ldapadmin suspend

État initial	État final
INITIAL	Erreur
RESET	SUSPENDED
READY	SUSPENDED
ACTIVE	SUSPENDED
FAILED	SUSPENDED
SUSPENDED	SUSPENDED

La Tableau 2-3 montre les transitions de l'état lorsque vous exécutez sp_ldapadmin activate.

Tableau 2-3 : Transitions de l'état lors de l'exécution de la commande sp_ldapadmin activate

État initial	État final
INITIAL	Erreur
RESET	READY
READY	READY
ACTIVE	ACTIVE
FAILED	READY
SUSPENDED	READY

Les tables suivantes montrent les transitions de l'état du serveur LDAP exécutées implicitement par Adaptive Server.

La Tableau 2-4 montre les transitions de l'état lorsqu'Adaptive Server est redémarré :

Tableau 2-4 : Transitions de l'état lorsqu'Adaptive Server est redémarré

État initial	État final
INITIAL	INITIAL
RESET	RESET
READY	READY
ACTIVE	READY
FAILED	FAILED
SUSPENDED	SUSPENDED

Adaptive Server ne tente une connexion LDAP que si le serveur LDAP est à l'état READY ou ACTIVE. La Tableau 2-5 montre les transitions de l'état :

Tableau 2-5 : Transactions de l'état lorsqu'une connexion LDAP réussit

État initial	État final
READY	ACTIVE
ACTIVE	ACTIVE

La Tableau 2-6 montre les transactions de l'état lorsqu'une connexion LDAP échoue :

Tableau 2-6 : Transactions de l'état lorsqu'une connexion LDAP échoue

État initial	État final
READY	FAILED
ACTIVE	FAILED

Améliorations en termes de robustesse de l'AU LDAP

Adaptive Server version 12.5.4 introduit plusieurs nouvelles options sp_ldapadmin pour améliorer la robustesse, que voici.

Nombre maximal de threads natifs ldapua par moteur set_max_ldapua_native_threads définit le nombre maximal de threads natifs qui peuvent être exécutés simultanément dans un moteur traitant une requête d'authentification LDAP.

```
sp_ldapadmin 'set_max_ldapua_native_threads', 'an integer'
```

La valeur minimale de set_max_ldapua_native_threads est 1. La valeur maximale est égale à max native threads moins number of dump threads tel que défini à l'aide de sp_configure. La valeur par défaut est identique à la valeur maximale.

sp_configure garantit que le nombre maximal de threads natifs est suffisant pour set_max_ldapua_native_threads et la valeur du paramètre de configuration number of dump threads.

Temporisation de la requête LDAP set_timeout définit le délai, en millisecondes, pendant lequel Adaptive Server attend une réponse du serveur LDAP avant d'abandonner la requête d'authentification.

Vous pouvez définir cette option en tapant :

```
sp_ldapadmin, 'set_timeout', 'time_in_milli_seconds'
```

La valeur par défaut de la commande set_timeout est de 10.000 millisecondes (10 secondes). Les valeurs possibles sont comprises entre 1 et 3.600.000 (une heure).

Abandon de l'authentification LDAP en cas de saturation set_abandon_ldapua_when_full vous permet de rechercher une autre solution pour l'authentification utilisateur LDAP lorsque la capacité des threads natifs par moteur est dépassée.

Lorsque plus aucun thread n'est disponible, la requête est abandonnée si set_abandon_ldapua_when_full a la valeur true (vrai). Si enable ldap user auth a la valeur 1, le client est authentifié à l'aide de l'objet syslogins d'Adaptive Server. Si enable ldap user auth a la valeur 2, la connexion cliente échoue.

Si set_abandon_ldapua_when_full a la valeur false (faux), la requête d'authentification est bloquée jusqu'à ce que le descripteur LDAP puisse accepter de nouvelles requêtes d'authentification.

Pour définir set_abandon_ldapua_when_full, entrez :

```
sp_ldapadmin 'set_abandon_ldapua_when_full',
      'true | false'
```

La valeur par défaut est "false". Les valeurs possibles sont "true" et "false".

Descripteurs LDAP par moteur La séquence de connexion de l'algorithme DN recherché nécessite qu'Adaptive Server établisse une liaison au serveur LDAP à l'aide du compte d'accès avant de pouvoir effectuer des recherches. Adaptive Server obtient un descripteur LDAP (pointeur) suite à la liaison. Ce descripteur est utilisé pour rechercher le DN du login sur le serveur LDAP.

Dans les versions d'Adaptive Server antérieures à 12.5.4, il n'y avait qu'un seul descripteur par moteur. Si ce descripteur était utilisé par une connexion entrante pour effectuer une recherche, les autres connexions attendaient que le descripteur soit disponible. Adaptive Server version 12.5.4 peut ouvrir jusqu'à 20 descripteurs par moteur. Ceci améliore la concurrence d'accès et les performances à la connexion.

Pour obtenir de plus amples informations sur l'algorithme DN recherché, reportez-vous à « Algorithme DN recherché » page 21.

Détection et résolution des erreurs liées à l'authentification utilisateur LDAP

Adaptive Server peut de temps à autre rencontrer des erreurs lors de la communication avec le serveur LDAP. Ces erreurs sont généralement résolues par une nouvelle tentative de connexion. Si les erreurs persistent après trois tentatives, Adaptive Server marque le serveur LDAP comme FAILED.

- LDAP_BUSY : le serveur est occupé.
- LDAP_CONNECT_ERROR : erreur lors d'une connexion.
- LDAP_LOCAL_ERROR : erreur du côté client.
- LDAP_NO_MEMORY : impossible d'allouer de la mémoire du côté client.
- LDAP_OPERATIONS_ERROR : erreur du côté serveur.
- LDAP_OTHER : code d'erreur inconnu.
- LDAP_ADMINLIMIT_EXCEEDED : une recherche a dépassé une limite.
- LDAP_UNAVAILABLE : le serveur ne peut pas traiter la requête.
- LDAP_UNWILLING_TO_PERFORM : le serveur refuse de traiter la requête.
- LDAP_LOOP_DETECT : une boucle a été détectée au cours d'une réorientation.
- LDAP_SERVER_DOWN : serveur injoignable (échec de la connexion).
- LDAP_TIMEOUT : l'API LDAP échoue parce que l'opération ne s'est pas terminée dans les délais définis par l'utilisateur.

Des erreurs passagères et un grand nombre de requêtes de connexion simultanées peuvent générer un journal d'erreurs avec un grand nombre de répétitions. Pour rendre le journal plus lisible, l'algorithme de journalisation des erreurs suivant est utilisé :

1 Si un message est consigné pour la première fois, il est journalisé.

2 Si le délai écoulé depuis la dernière consignation du message dépasse 3 minutes :

- Journalisation du message d'erreur.
- Journalisation du nombre de répétitions du message depuis sa dernière impression.
- Journalisation du délai (en minutes) écoulé depuis l'impression du message.

Les échecs d'authentification découlant des situations suivantes ne sont pas considérés comme des erreurs LDAP et n'entraînent pas de nouvelle tentative d'authentification.

- Échec de la liaison due à un mot de passe erroné ou à un nom distinctif incorrect.
- Une recherche qui, après une liaison réussie, renvoie un jeu de résultats de 0 ou aucune valeur d'attribut.

Les erreurs de syntaxe trouvées lors de l'analyse de l'URL sont détectées lors du réglage d'un URL LDAP et n'entrent donc dans aucune des catégories ci-dessus.

Administration de l'authentification utilisateur LDAP

La syntaxe de la commande sp_ldapadmin est la suivante :

```
sp_ldapadmin Usage: sp_ldapadmin command [, option1 [, option2]]
```

Les commandes sp_ldapadmin comprennent les commandes suivantes :

- `sp_ldapadmin 'set_primary_url', 'url'`
- `sp_ldapadmin 'set_secondary_url', 'url'`
- `sp_ldapadmin 'set_dn_lookup_url', 'url'`
- `sp_ldapadmin 'set_secondary_dn_lookup_url', 'url'`
- `sp_ldapadmin 'set_access_acct', 'distinguished name', 'password'`
- `sp_ldapadmin 'set_secondary_access_acct', 'distinguished name', 'password'`

- `sp_ldapadmin 'suspend', {'primary' | 'secondary'}`
- `sp_ldapadmin 'activate', {'primary' | 'secondary'}`
- `sp_ldapadmin 'list'`
- `sp_ldapadmin 'list_urls'`
- `sp_ldapadmin 'list_access_acct'`
- `sp_ldapadmin 'check_url', 'url'`
- `sp_ldapadmin 'check_login', 'name'`
- `sp_ldapadmin 'set_timeout', timeout_in_milli_seconds`
- `sp_ldapadmin 'set_max_ldapua_native_threads', max_ldapua_native_threads`
- `sp_ldapadmin 'set_abandon_ldapua_when_full', {true|false}`
- `sp_ldapadmin 'help'`

Voici un exemple de résultat provenant d'une session d'administration client :

```
1> sp_configure 'enable ldap', 2
2> go

 Parameter Name                 Default     Memory Used Config Value
         Run Value   Unit                  Type
------------------------------ ----------- ----------- ------------
         ----------- -------------------- ----------
enable ldap user auth                     0           0            2
                   2 not applicable       dynamic

(1 row affected)
```

```
1> sp_ldapadmin
'set_primary_url','ldap://primldap:30001/'
2> go
The URL 'ldap://primldap:30001/' is set for LDAP User
Authentication.
(return status = 0)

1> sp_ldapadmin 'set_dn_lookup_url',
'ldap://primldap:30001/dc=sybase,dc=com??sub?uid=*'
2> go
The URL
'ldap://primldap:30001/dc=sybase,dc=com??sub?uid=*'
is set for LDAP User Authentication.
(return status = 0)
```

```
1> sp_ldapadmin
'set_access_acct','cn=directorymanager,dc=sybase,
dc=com', 'primpassword'
2> go
The LDAP account distinguished name 'cn=directory
manager,dc=sybase,dc=com' is set for LDAP user
authentication.
(return status = 0)

1> sp_ldapadmin 'set_secondary_url',
'ldap://secldap:31001/'
2> go
The URL 'ldap://secldap:31001/' is set for LDAP User
Authentication.
(return status = 0)

1> sp_ldapadmin 'set_secondary_dn_lookup_url',
'ldap://secldap:31001//dc=sybase,dc=com??sub?uid=*'
2> go
The URL
'ldap://secldap:31001//dc=sybase,dc=com??sub?uid=*'
is set for LDAP User Authentication.
(return status = 0)
2> sp_ldapadmin 'set_secondary_access_acct',
'cn=Manager,dc=sybase,dc=com', 'secpassword'
3> go
The LDAP account distinguished name
'cn=Manager,dc=sybase,dc=com' is set for LDAP user
authentication.
(return status = 0)
1> sp_ldapadmin activate, primary
2> go
(return status = 0)

1> sp_ldapadmin activate, secondary
2> go
(return status = 0)


1> sp_ldapadmin 'list'
2> go
Primary:
      URL:                 'ldap://primldap:30001/'
      DN Lookup URL:
      'ldap://primldap:30001/dc=sybase,dc=com??sub?uid
      =*'
      Access Account:
```

```
      'cn=directory manager,dc=sybase,dc=com
      Active:              'TRUE'
      Status:              'READY'
Secondary:
      URL:                 'ldap://secldap:31001/'
      DN Lookup URL:
     'ldap://secldap:31001/dc=syase,dc=com??sub?uid=*'
      Access Account:     'cn=Manager,dc=sybase,dc=com'
      Active:              'TRUE'
      Status:              'READY'
Timeout value:           '-1'(10000) milliseconds
Maximum LDAPUA native threads per Engine: '49'
Abandon LDAP user authentication when full: 'false'
(return status = 0)

1> sp_ldapadmin 'list_urls'
2> go
Primary URL:         'ldap://primldap:30001/'
Secondary URL:       'ldap://secldap:31001/'
Distinguished Name Lookup URL:
'ldap://primldap:30001/dc=sybase,dc=com??sub?uid=*'
Secondary Distinguished Name Lookup URL:
'ldap://secldap:31001/dc=sybase,dc=com??sub?uid=*'
(return status = 0)

1> sp_ldapadmin 'list_access_acct'
2> go
Access Account DN:
'cn=directory manager,dc=sybase,dc=com'
Secondary Access Account DN:
'cn=Manager,dc=sybase,dc=com'
(return status = 0)
```

Optimisation de l'authentification utilisateur LDAP

Vous pouvez configurer et optimiser les options d'Adaptive Server sur la base de la charge des requêtes de connexion et de l'infrastructure serveur LDAP d'Adaptive Server. Vous pouvez paramétrer les deux options suivantes en fonction du nombre de requêtes entrantes simultanées :

- Utilisez sp_configure pour régler max native threads, valeur qui indique le nombre de threads natifs par moteur.
- Utilisez sp_ldapadmin pour configurer max_ldapua_native_threads, valeur qui indique le nombre de threads natifs d'authentification utilisateur LDAP par moteur.

Configurez l'option suivante en fonction du réseau et de la santé de l'infrastructure Adaptive Server/serveur LDAP :

- Utilisez sp_ldapadmin pour configurer set_timeout, valeur qui indique les temporisations de la recherche et de la liaison au serveur LDAP.

Configurez l'option suivante pour spécifier le comportement d'Adaptive Server lorsque les connexions entrantes ont consommé max_ldapua_native_threads :

- Utilisez sp_ldapadmin pour configurer set_abandon_ldapua_when_full.

Modifications des informations de mot de passe utilisées pour l'authentification utilisateur LDAP

Il existe deux nouveaux messages d'information liés à l'authentification utilisateur LDAP qu'Adaptive Server obtient du serveur LDAP et transmet au client :

- Si vous vous connectez à un serveur Adaptive Server à l'aide d'un mécanisme d'authentification LDAP avec un mot de passe ad hoc sur le point d'expirer, le message suivant s'affiche :

  ```
  Your password will expire in <number> days.
  ```

- Si vous tentez de vous connecter à un serveur Adaptive Server à l'aide d'un mécanisme d'authentification LDAP après que l'administrateur du serveur LDAP a réinitialisé votre mot de passe ou une fois votre mot de passe venu à expiration, vous obtiendrez un message 4002 :

  ```
  Login failed
  ```

  Si le système d'audit est actif et que l'option d'audit errors est activée :

  ```
  sp_audit 'errors', 'all', 'all', 'on'
  ```

  un message 4099 est envoyé au journal d'audit. Le texte du message 4099 est le suivant :

  ```
  Your LDAP password has expired.
  ```

Remarque Configurez votre serveur LDAP de manière à fournir cette information complémentaire. En outre, Adaptive Server doit prendre en charge la transmission des contrôles de mot de passe LDAP à un client LDAP.

Renforcement des contrôles sur le mappage des logins

Utilisez sp_maplogin pour mapper des noms de clients externes avec des logins locaux d'Adaptive Server. Cette commande sert à mapper les utilisateurs authentifiés à l'aide de LDAP ou PAM avec le login local d'Adaptive Serveur.

Pour mapper un utilisateur authentifié avec Kerberos, utilisez sybmapname au lieu de sp_maplogin. Voir instructions et exemples sous « Utilisation de sybmapname pour gérer les noms principaux des utilisateurs » page 14.

Seuls les utilisateurs possédant un rôle_sso peuvent créer ou modifier des mappages à l'aide de sp_maplogin.

Dans Adaptive Server version 12.5.4, des contrôles ont été ajoutés à sp_maplogin afin d'éviter les conflits entre un paramètre du mécanisme d'authentification d'un login et un mappage qui utilise ce login. Les conflits de mappage potentiels sont détectés par les procédures stockées sp_maplogin, sp_modifylogin ou sp_addlogin.

Les contrôles renforcés ne permettent plus le mappage :

- d'un nom de login Adaptive Server vers un autre nom de login ;
- d'un nom externe existant en tant que login local ;
- vers un nom de login inexistant.

En outre, lorsque le mécanisme d'authentification est spécifié avec un mappage, il est contrôlé à l'aide du mécanisme d'authentification défini dans le login cible.

Si le mécanisme d'authentification d'un login cible oblige le login à utiliser un mécanisme d'authentification donné, le mécanisme spécifié avec le mappage doit correspondre à celui spécifié pour le login ou au mécanisme d'authentification ANY.

Lorsque sp_maplogin détecte un conflit, sp_maplogin échoue et signale une erreur afin d'identifier le conflit.

De la même manière, sp_modifylogin et sp_addlogin vérifient l'absence d'un mappage existant susceptible d'entrer en conflit avec l'option authenticate with utilisée pour la connexion de l'utilisateur.

Lorsque sp_modifylogin ou sp_addlogin détecte un conflit, une erreur est signalée afin d'identifier tout conflit avec un mappage de logins.

Exemple 1 : mappage d'un utilisateur LDAP sur le login “sa” d'Adaptive Server Une société a adopté LDAP comme référentiel pour tous ses comptes utilisateurs et a mis en place une stratégie de sécurité nécessitant une authentification LDAP de tous les utilisateurs, y compris les administrateurs de bases de données, `"adminA"` et `"adminB"`, qui peuvent gérer des centaines de serveurs Adaptive Server. Un système d'audit est activé et les événements de connexion sont enregistrés dans la trace d'audit.

Pour mapper ces comptes administrateurs avec “sa”, entrez :

```
sp_maplogin LDAP, 'adminA', 'sa'
go
sp_maplogin LDAP, 'adminB', 'sa'
go
```

Utilisez enable ldap user auth pour exiger que tous les utilisateurs s'authentifient à l'aide de l'authentification LDAP :

```
sp_configure 'enable ldap user auth', 2
go
```

Lorsque `'adminA'` s'authentifie au cours de la connexion à Adaptive Server, le nom distinctif associé à `'adminA'` est enregistré dans l'événement d'audit, au lieu du seul “sa”. Ceci permet d'identifier dans la trace d'audit tout individu qui effectue une action.

Les mots de passe `'adminA'` et `'adminB'` étant définis dans le serveur LDAP, il n'est pas nécessaire de gérer le mot de passe “sa” sur tous les serveurs Adaptive Server administrés.

Cet exemple permet également d'utiliser différents identifiants et mots de passe externes à des fins d'authentification, alors que les actions dans Adaptive Server nécessitent toujours les privilèges spéciaux associés au compte “sa”.

Exemple 2 : utilisation de PAM et LDAP pour mapper les utilisateurs avec les logins d'application Une entreprise a adopté l'authentification PAM et LDAP mais à des fins différentes. La stratégie de sécurité de l'entreprise définit LDAP comme le mécanisme d'authentification pour les comptes utilisateurs généraux et PAM pour les utilisateurs spéciaux comme une application de niveau intermédiaire. Une application de niveau intermédiaire peut établir une zone de connexions à Adaptive Server pour gérer des requêtes pour les utilisateurs de cette application.

Configurez Adaptive Server pour l'authentification utilisateur LDAP et PAM :

```
sp_configure 'enable ldap user auth', 2
go
sp_configure 'enable pam user auth', 2
go
```

Établissez une connexion `appX` à Adaptive Server en local, avec des autorisations appropriées pour l'application de niveau intermédiaire :

```
sp_addlogin 'appX', password
go
sp_modifylogin appX, 'authenticate with', PAM
go
```

Au lieu de coder en dur un mot de passe simple dans `appX` et de gérer le mot de passe de manière cohérente sur plusieurs serveurs Adaptive Server différents, un module PAM personnalisé est développé afin d'authentifier l'application dans un référentiel centralisé à l'aide de faits supplémentaires servant à la vérifier.

Le login de l'application cliente `appY` nécessite une authentification LDAP de l'utilisateur avec son identifiant et son mot de passe LDAP. Utilisez sp_maplogin pour mapper tous les utilisateurs authentifiés par LDAP avec le login `appY`.

```
sp_addlogin 'appY', password
go
sp_maplogin LDAP, NULL, 'appY'
go
```

Les utilisateurs de `appY` sont authentifiés avec leur identifiant et mot de passe d'entreprise, puis mappés avec un login Adaptive Server local `appY` pour exécuter des actions sur des bases de données. L'authentification a eu lieu avec l'identifiant de l'utilisateur LDAP, qui est enregistré dans la trace d'audit, et s'exécute avec les autorisations correspondant au login `appY` de l'application.

Prise en charge de SSL

Adaptive Server version 12.5.4 prend en charge SSL sur les nouvelles plates-formes suivantes :

- HP-IA64
- Linux64

Prise en charge de PAM

Adaptive Server version 12.5.4 prend PAM en charge sur :

- HP-IA64
- Macintosh OS X

Mises à jour des colonnes cryptées

Adaptive Server version 12.5.4 comprend les améliorations suivantes des colonnes cryptées. Pour obtenir de plus amples informations sur la première version de la fonctionnalité "colonnes cryptées" intégrée à la version 12.5.3a, reportez-vous au *Encrypted Columns Guide*.

Intégrité référentielle avec les colonnes cryptées

Vous pouvez établir une intégrité référentielle entre deux colonnes cryptées lorsque :

- Vous utilisez la même clé pour crypter les colonnes qui sont référencées et qui référencent.
- La clé utilisée pour crypter les colonnes spécifie un vecteur d'initialisation NULL et un remplissage aléatoire NULL.

Les contraintes de vérification référentielles sont efficaces, car elles sont effectuées sur des valeurs cryptées.

alter table et colonnes cryptées

Vous ne pouvez pas utiliser alter table pour crypter ou décrypter une colonne appartenant à un index clustérisé ou d'emplacement. Pour crypter ou décrypter cette colonne, supprimez l'index, modifiez la colonne et régénérez l'index.

Vous ne pouvez pas utiliser alter table pour décrypter une colonne si la table possède un trigger défini. Pour décrypter la colonne, supprimez le trigger, modifiez la colonne et régénérez le trigger.

sp_help et colonnes cryptées

sp_help affiche des informations sur les clés de cryptage. Lorsqu'un nom de clé est spécifié en tant que paramètre pour sp_help, la commande liste le nom de la clé, son propriétaire, son type d'objet et la date de sa création.

sp_helprotect et colonnes cryptées

sp_helprotect fournit de nouvelles informations sur les colonnes cryptées, les clés de cryptage et les utilisateurs comme suit :

- Tables et colonnes : indique qui a reçu l'autorisation decrypt et sur quelles colonnes.
- Clés de cryptage : indique qui a reçu l'autorisation select.
- Utilisateurs : indique les utilisateurs qui ont reçu l'autorisation create encryption key.

Options de login et de complexité du mot de passe

Adaptive Server version 12.5.4 introduit une combinaison de nouveaux et d'anciens mécanismes vous permettant d'établir des règles concernant les mots de passe pour les nouveaux logins ou pour les mots de passe réinitialisés.

Comme dans les versions antérieures d'Adaptive Server, vous pouvez :

- exiger que tous les mots de passe comprennent au moins un chiffre ;
- exiger que tous les mots de passe aient une longueur minimale ;
- définir une période d'expiration pour le mot de passe ;
- exiger qu'un login soit bloqué après un certain nombre de tentatives de connexion infructueuses ;
- définir un login individuel qui puisse obéir à ses propres règles en matière de chiffres, de longueur minimale et d'échec de connexion. Les règles de login spécifiques sont prioritaires sur les logins globaux pour cet utilisateur.

Toutefois, dans Adaptive Server version 12.5.4, vous pouvez également :

- spécifier que le nom de login ne peut pas correspondre à une portion du mot de passe ;
- définir un nombre minimal de caractères spéciaux pour le mot de passe ;
- définir un nombre minimal de caractères alphabétiques pour le mot de passe ;
- définir un nombre minimal de lettres majuscules pour le mot de passe ;
- définir un nombre minimal de lettres minuscules pour le mot de passe ;
- spécifier que le mot de passe doit être réinitialisé à la première connexion ;
- définir un nombre minimal de chiffres pour le mot de passe ;
- définir un intervalle d'avertissement concernant l'expiration du mot de passe.

Vous pouvez définir chacune de ces nouvelles options dans le module externe d'Adaptive Server ou utiliser une nouvelle procédure stockée :

```
sp_passwordpolicy 'set', option, value
```

Pour plus d'informations sur chaque nouvelle option et ses valeurs possibles, voir Nouvelles contraintes de vérification de la complexité du mot de passe ci-dessous.

La définition de nouvelles options de complexité du mot de passe crée une ligne pour chaque option dans la table sysattributes. Aussi longtemps que la ligne de la nouvelle option existe, le contrôle des priorités utilise la valeur de celle-ci et ignore les valeurs plus anciennes.

Pour revenir à une version antérieure des règles relatives aux mots de passe, désélectionnez les options de complexité du mot de passe à l'aide du module externe d'Adaptive Server ou utilisez :

```
sp_passwordpolicy 'clear', option
```

Les nouvelles options de complexité du mot de passe comportent également des contrôles croisés. Par exemple, si la somme de min lower case in password et de min upper case in password est supérieure à min alpha in password, un message d'avertissement apparaît.

Nouvelles contraintes de vérification de la complexité du mot de passe

Cette rubrique aborde les options qui supportent les contraintes de vérification de la complexité du mot de passe. Vous pouvez utiliser ces options dans une nouvelle interface de procédure stockée ; leurs valeurs sont stockées dans la table master.dbo.sysattributes.

Pour désactiver ces options, utilisez sp_passwordpolicy. Pour désactiver une option individuelle, entrez :

```
sp_passwordpolicy 'clear', option
```

Pour désactiver les options de stratégie en matière de mot de passe pour tous les mots de passe, entrez :

```
sp_passwordpolicy 'clear'
```

Interdiction des mots de passe simples

disallow simple password vérifie si le mot de passe contient le nom de login. Cette option peut être définie comme suit :

- 0 désactive l'option, et les mots de passe simples sont autorisés.
- 1 active l'option, et les mots de passe simples sont interdits.

Par défaut, cette option est désactivée et cette contrainte de vérification n'est pas appliquée aux mots de passe.

Pour définir cette option, entrez :

```
sp_passwordpolicy 'set', 'disallow simple passwords', 1
```

Lorsque vous interdisez les mots de passe simples, vous ne pouvez pas utiliser votre nom de login dans votre mot de passe. Vous devez lui donner une valeur complexe. Par exemple :

```
sp_password 'old_complex_password', BHotAcha789, johnd
```

Le login `johnd` est désormais associé au mot de passe `BHotAcha789`, qui n'inclut donc pas le nom de login.

Toutefois, si vous modifiez le mot de passe de ce login en indiquant :

```
sp_password 'old_complex_password', johnd123, johnd
```

le login `johnd` est à présent contenu dans le nouveau mot de passe `johnd123`, et cette commande échoue.

Contraintes de vérification personnalisées de la complexité du mot de passe

Adaptive Server version 12.5.4 vous permet de configurer des contraintes de vérification personnalisées du mot de passe en plus ou à la place des règles de complexité du mot de passe, et ce à l'aide de deux procédures stockées.

- sp_extrapwdchecks
- sp_cleanpwdchecks

Il s'agit de procédures stockées fournies par le responsable de la sécurité du système, définies et localisées dans la base de données master. Ces procédures stockées personnalisées sont appelées automatiquement lors des contrôles de la complexité du mot de passe d'Adaptive Server et lors de la suppression d'un login, respectivement. Voir « Activation de contraintes de vérification personnalisées du mot de passe » page 50 pour obtenir un exemple de la manière de créer ces procédures stockées personnalisées.

Indication du nombre minimal de chiffres requis dans un mot de passe

Utilisez min digits in password pour spécifier le nombre minimal de chiffres requis dans un mot de passe. Les valeurs possibles sont les suivantes :

- 0 à 16 : le nombre minimal de chiffres à inclure dans un mot de passe.
- -1 : le mot de passe ne peut pas contenir de chiffres.

Par défaut, cette option de complexité du mot de passe est désactivée et cette contrainte de vérification n'est pas appliquée aux mots de passe.

Pour définir cette option, entrez :

```
sp_passwordpolicy 'set', 'min digits in password',
      number
```

Par exemple, si vous avez appliqué à min digits in password la valeur 4, votre mot de passe doit comporter au moins quatre chiffres. Pour satisfaire à cette contrainte, vous pouvez ajouter un login `johnd` avec un mot de passe complexe `SEcret6789` en entrant :

```
sp_addlogin 'johnd', 'SEcret6789'
```

Toutefois, si vous entrez :

```
sp_addlogin 'johnd', 'secret123'
```

la commande échoue parce que le nombre minimal de chiffres autorisé est de 4.

Indication du nombre minimal de caractères alphabétiques requis dans un mot de passe

min alpha in password spécifie le nombre minimal de caractères alphabétiques autorisés dans un mot de passe. Cette valeur doit être au moins égale à la somme du nombre minimal de caractères majuscules et minuscules.

Les valeurs possibles sont les suivantes :

- 0 à 16 : le nombre de caractères alphabétiques requis dans le mot de passe.
- -1 : le mot de passe ne peut pas contenir de caractères alphabétiques.

Par défaut, cette option de complexité du mot de passe est désactivée et cette contrainte de vérification n'est pas appliquée aux mots de passe.

Pour définir le nombre minimal de caractères alphabétiques requis dans un mot de passe, entrez :

```
sp_passwordpolicy 'set', 'min alpha in password',
      number
```

Par exemple, si vous avez appliqué à min alpha in password la valeur 4, votre mot de passe doit comporter au moins quatre caractères alphabétiques. Pour satisfaire à cette contrainte, vous pouvez définir le mot de passe `SEcret6789` pour le nouveau login `johnd` en entrant :

```
sp_addlogin 'johnd', SECret123456
```

Toutefois, si vous tentez de créer le nouveau login :

```
sp_addlogin 'johnd', 'sec123456'
```

et si le nombre minimal de caractères alphabétiques est toujours de 4, la commande échoue.

Indication du nombre minimal de caractères spéciaux requis dans un mot de passe

min special char in password spécifie le nombre minimal de caractères spéciaux autorisés dans un mot de passe. Les valeurs possibles sont les suivantes :

- 0 à 16 : le nombre minimal de caractères spéciaux requis dans le mot de passe.
- -1 : le mot de passe ne peut pas contenir de caractères spéciaux.

Par défaut, cette option de complexité du mot de passe est désactivée et cette contrainte de vérification n'est pas appliquée aux mots de passe.

Pour définir le nombre minimal de caractères spéciaux requis dans un mot de passe, entrez :

```
sp_passwordpolicy 'set', 'min special char in
      password',number
```

Par exemple, si vous appliquez à set min special char in password la valeur 3, vous pouvez créer un nouveau login `johnd` avec le mot de passe `abcDE1&#$`, en entrant :

```
sp_addlogin, 'johnd', 'abcDE1&#$'
```

Toutefois, si vous déterminez que le nouveau login `johnd` doit être associé au mot de passe `abcDE1#` :

```
sp_addlogin, 'johnd', 'abcDE1#'
```

et si le nombre de caractères spéciaux requis est toujours de 3, la commande échoue.

Indication du nombre minimal de lettres majuscules requis dans un mot de passe

min upper char in password vous permet de définir le nombre minimal de lettres majuscules autorisées dans un mot de passe. Les valeurs possibles sont les suivantes :

- 0 à 16 : le nombre de lettres majuscules requis dans le mot de passe.
- -1 : le mot de passe ne peut pas contenir de caractères majuscules.

Par défaut, cette option de complexité du mot de passe est désactivée et cette contrainte de vérification n'est pas appliquée aux mots de passe.

Pour définir le nombre minimal de caractères majuscules requis dans un mot de passe, entrez :

```
sp_passwordpolicy 'set', 'min upper char in password''
      number
```

Par exemple, si vous appliquez à min upper char in password la valeur 3, vous pouvez créer un login `johnd` avec le mot de passe `abCDE1#`, en entrant :

```
sp_addlogin 'johnd', 'abCDE1#'
```

Toutefois, si vous tentez d'ajouter le login suivant :

```
sp_addlogin 'johnd', 'abcDE1#'
```

et si le nombre minimal de lettres majuscules requis est de 3, la commande échoue.

Indication du nombre minimal de lettres minuscules requis dans un mot de passe

min lower char in password définit le nombre minimal de lettres minuscules requis dans un mot de passe. Les valeurs possibles sont les suivantes :

- 0 à 16 : indique le nombre de lettres minuscules requis dans le mot de passe.
- -1 : indique que le mot de passe ne peut pas contenir de caractères minuscules.

Par défaut, cette option de complexité du mot de passe est désactivée et cette contrainte de vérification n'est pas appliquée aux mots de passe.

Pour définir le nombre minimal de lettres minuscules requis dans un mot de passe, entrez :

```
sp_passwordpolicy 'set', 'min lower char in password',
      number
```

Par exemple, si vous appliquez à min lower char in password la valeur 3, vous pouvez créer un login `johnd` avec le mot de passe `abcdEF1#`, en entrant :

```
sp_addlogin 'johnd', 'abcdEF1#'
```

Toutefois, si vous tentez d'ajouter le login suivant :

```
sp_addlogin 'johnd', 'abCDE#1'
```

et si le nombre minimal de lettres minuscules requis est de 3, la commande échoue.

Indication de la longueur minimale du mot de passe

minimum password length définit la longueur minimale du mot de passe. Vous pouvez définir une longueur minimale de mot de passe comprise entre 0 et 30 caractères. La valeur spécifiée ici doit être au moins égale à la somme de toutes les autres exigences minimales.

Par exemple, minimum password length doit avoir une valeur au moins égale à 10 si vous avez défini les options suivantes :

minimum digits in password de 3
minimum special characters in password de 2
minimum uppercase characters in password de 2
minimum lowercase characters in password de 3

Dans cet exemple, si la longueur du mot de passe est inférieure à 10, un message d'avertissement s'affiche, mais la configuration de l'option de stratégie en matière de mots de passe réussit.

Pour définir la longueur minimale du mot de passe, entrez :

```
sp_passwordpolicy 'set', 'minimum password length',
      number
```

Par exemple, si vous appliquez à minimum password length la valeur 6, vous pouvez créer un nouveau mot de passe de six caractères pour le login `johnd` en entrant :

```
sp_password 'old_complex_password', 'ABcd12$%', 'johnd'
```

Toutefois, si vous tentez de modifier votre mot de passe comme suit :

```
sp_password 'old_complex_password', 'joh12', 'johnd'
```

et si la longueur minimale du mot de passe est de 6, la commande échoue.

Indication du délai d'expiration du mot de passe

password expiration spécifie le nombre de jours pendant lequel un mot de passe est valable. Cette valeur s'applique globalement. Les valeurs possibles sont notamment les suivantes :

- 0 : le mot de passe ne vient jamais à expiration.
- 1 à 32767 : le nombre minimal de jours pendant lequel le mot de passe peut exister avant son expiration.

Par défaut, cette option de complexité du mot de passe est désactivée et cette contrainte de vérification n'est pas appliquée aux mots de passe.

Pour définir la date d'expiration du mot de passe, entrez :

```
sp_passwordpolicy 'set', 'password expiration', number
```

Indication de l'intervalle d'avertissement relatif à l'expiration du mot de passe

password exp warn interval indique le nombre de jours avant l'expiration du mot de passe à partir duquel les messages d'avertissement relatifs à celle-ci s'affichent. Ces messages s'affichent à chaque connexion réussie jusqu'à la modification ou l'expiration du mot de passe. Cette valeur doit être inférieure ou égale à l'expiration du mot de passe.

Les valeurs possibles sont comprises entre 0 et 365. Cette option est désactivée par défaut.

Pour définir l'intervalle d'avertissement relatif à l'expiration du mot de passe, entrez :

```
sp_passwordpolicy 'set', 'password exp warn interval',
      number
```

Indication du nombre d'échecs de connexion autorisé

maximum failed logins indique le nombre maximal d'échecs de connexion possibles avant que le login soit bloqué. Cette valeur s'applique globalement. Les valeurs possibles sont les suivantes :

- 0 : les logins ne sont jamais bloqués, quel que soit le nombre de tentatives de connexion infructueuses.
- 1 à 32767 : le nombre d'échecs de connexion possibles avant que le login ne soit bloqué.

Par défaut, cette valeur est désactivée et cette contrainte de vérification n'est pas appliquée aux mots de passe.

Pour définir le nombre d'échecs de connexion autorisé, entrez :

```
sp_passwordpolicy 'set', 'maximum failed logins',
      number
```

Réinitialisation du mot de passe à la première connexion

expire login attribue à l'état du login la valeur "expired" (expiré) lorsqu'un responsable de la sécurité du système crée ou réinitialise un login. Le login doit alors être modifié à la première connexion. Les valeurs possibles sont les suivantes :

- 0 : les logins nouveaux ou réinitialisés ne viennent pas expiration.
- 1 – les logins nouveaux ou réinitialisés ne viennent pas à expiration ; réinitialisez votre mot de passe à la première connexion.

Par défaut, cette valeur est désactivée et cette contrainte de vérification n'est pas appliquée aux mots de passe.

Pour configurer l'option de manière à ce qu'un changement de login soit exigé à la première connexion, entrez :

```
sp_password policy 'set', 'expire login', [ 1 | 0 ]
```

Contrôles croisés de l'option de complexité du mot de passe

Soyez attentif au fait que certaines options de complexité du mot de passe peuvent interagir avec d'autres options.

- minimum password length doit être au moins égal à la somme de min digits in password, min alpha in password, min special characters in password.
- min alpha in password doit être au moins égal à la somme de min upper char in password et de min lower char in password.
- systemwide password expiration doit être supérieur à password exp warn interval.

Dans le cadre des contrôles croisés ci-dessus, si Adaptive Server rencontre une valeur d'option de -1 pour la complexité du mot de passe, il l'interprète comme une valeur de 0. Si l'une des options n'est pas définie, Adaptive Server l'interprète également comme une valeur de 0.

Adaptive Server affiche des avertissements pour chaque nouvelle option de complexité du mot de passe ne satisfaisant pas aux contrôles croisés. Toutefois, la configuration de l'option réussit.

Configuration des contraintes de vérification de la complexité des anciens et nouveaux mots de passe

Tableau 2-7 : Contraintes de vérification de la complexité des anciens et nouveaux mots de passe

Contraintes de vérification et stratégies relatives aux mots de passe pour l'authentification d'Adaptive Server	Paramètres de configuration existants spécifiés à l'aide de sp_configure	Nouvelles options de complexité du mot de passe spécifiées à l'aide sp_passwordpolicy	Contournements existants spécifiques au login définis à l'aide de sp_modifylogin
Expiration du mot de passe	system-wide password expiration	system-wide password expiration	password expiration
Chiffres dans les mots de passe	check password for digit	min digits in password	N/A
Caractères alphabétiques dans les mots de passe	N/A	min alpha in password	N/A
Longueur du mot de passe	minimum password length	minimum password length	min passwd length
Blocage après des échecs de connexion	maximum failed logins	maximum failed logins	max failed_logins
Interdiction des mots de passe simples	N/A	disallow simple passwords	N/A
Caractères spéciaux dans les mots de passe	N/A	min special char in password	N/A
Lettres majuscules dans les mots de passe	N/A	min upper char in password	N/A
Lettres minuscules dans les mots de passe	N/A	min lower char in password	N/A
Intervalle d'avertissement concernant l'expiration du mot de passe	N/A	password exp warn interval	N/A
Réinitialisation du mot de passe à la première connexion	N/A	expire login	N/A
Contraintes de vérification personnalisées de la complexité du mot de passe	N/A	N/A	N/A

Vous pouvez définir les options de complexité du mot de passe aux niveaux suivants :

- Login, avec sp_addlogin ou sp_modifylogin
- Global, avec la nouvelle commande sp_passwordpolicy ou sp_configure

Étant donné qu'il est possible de définir les options de configuration du mot de passe sur une base globale ou spécifique au login, à l'aide de paramètres nouveaux et anciens, il est important de connaître l'ordre des priorités dans lequel celles-ci s'appliquent.

Lors de l'application des options liées au mot de passe : Adaptive Server examine d'abord les paramètres spécifiques au login existants, puis les nouvelles options de complexité du mot de passe, puis les options globales liées au mot de passe.

Exemple 1. Si vous entrez :

```
sp_addlogin @login_name = 'johnd',
      @passwd = 'complex_password',
      @minpwdlen = 6
```

vous avez défini la longueur minimale du mot de passe pour `johnd` à 6 caractères.

Si vous entrez les options globales suivantes (préexistantes) pour le login `johnd` :

```
sp_configure 'minimum password length', 8
sp_configure 'check password for digit', 'true'
sp_passwordpolicy 'set', 'min digits in password', 2
```

vous avez créé deux contraintes d'entrée minimales concernant la longueur du mot de passe pour le login `johnd` et avez défini des restrictions concernant l'utilisation de chiffres dans le mot de passe.

Si vous tentez ensuite de créer un mot de passe pour le login `johnd` comme suit :

```
sp_password @caller_password = 'old_complex_password',
@new_password = 'abcd123', @login_name = 'johnd'
```

Adaptive Server vérifie le mot de passe dans l'ordre suivant :

1 Vérification des options spécifiques au login existantes : la longueur minimale du mot de passe doit être supérieure à 6. Cette exigence est respectée et le contrôle réussit.

2 Nouvelles options : le nombre minimal de chiffres dans le mot de passe doit être supérieur à 2. Cette exigence est respectée et le contrôle réussit.

3 Options globales existantes : la longueur minimale du mot de passe spécifiée ici n'est pas vérifiée, car il existe déjà un contrôle spécifique au login pour `johnd`.

4 L'option "check password for digit" est redondante, puisqu'elle est déjà vérifiée lorsque le nombre minimal de chiffres est activé et a la valeur 2.

Une fois ces contrôles effectués dans la séquence désignée, si le nouveau mot de passe du login `johnd` a réussi le test, celui-ci est créé avec succès.

Exemple 2. Si, pour le même login, vous entrez :

```
sp_password @caller_password = 'old_complex_password',
@new_password = 'abcd', @login_name = 'johnd'
```

Adaptive Server vérifie d'abord les options spécifiques au login existantes et détermine que la longueur minimale du mot de passe a la valeur 6. Or, vous avez tenté de créer un mot de passe avec seulement 4 caractères. Le contrôle échoue, et Adaptive Server affiche un message d'erreur. Lorsqu'une contrainte de vérification de la complexité du mot de passe se solde par un échec, les autres options ne sont pas vérifiées.

Exemple 3. Si vous tentez de créer un nouveau login avec les options de configuration du mot de passe suivantes :

```
sp_addlogin @login_name = 'johnd', @passwd =
'complex_password', @minpwdlen = 4
```

ceci définit la longueur minimale du mot de passe de `johnd` à 4 caractères. Il s'agit d'une option spécifique au login existante. Si vous ajoutez :

```
sp_passwordpolicy 'set', 'min digits in password', 1
```

vous avez créé une contrainte d'entrée globale, qui spécifie que le nombre minimal de chiffres dans le mot de passe doit être de 1.

Si vous tentez ensuite de créer un mot de passe pour le login `johnd` comme suit :

```
sp_password @caller_password = 'old_complex_password',
@ new_password = 'abcde', @login_name = 'johnd'
```

Adaptive Server effectue les contrôles dans l'ordre suivant :

1 Vérification des options spécifiques au login existantes : la longueur minimale d'un nouveau mot de passe est de 4. Le mot de passe `abcde` comporte plus de 4 caractères, donc le contrôle réussit.

2 Contrôle des nouvelles contraintes d'entrée globales : le nombre minimal de chiffres dans un mot de passe appliqué globalement est de 1. Ce contrôle échoue.

Adaptive Server ne crée pas le nouveau mot de passe et affiche un message d'erreur.

Pour qu'un nouveau mot de passe soit créé, tous les contrôles doivent être passés avec succès.

Procédures stockées relatives à la complexité du mot de passe

Adaptive Server propose plusieurs nouvelles procédures stockées qui contribuent à configurer la complexité du mot de passe.

sp_extrapwdchecks

sp_extrapwdchecks est une nouvelle procédure stockée personnalisée contenant une logique définie par l'utilisateur pour les contraintes de vérification de la complexité du mot de passe. Vous pouvez configurer sp_extrapwdchecks en fonction de vos besoins en matière de sécurité. Installez sp_extrapwdchecks dans la base de données master.

```
sp_extrapwdchecks motdepasse_demandeur, nouveau_mot_de_passe,
nom_login
```

où :

- *motdepasse_demandeur* spécifie le mot de passe actuel.
- *nouveau_mot_de_passe* spécifie le nouveau mot de passe défini.
- *nom_login* spécifie le login associé au mot de passe modifié ou ajouté.

sp_extrapasswordchecks doit utiliser raiserror pour signaler une erreur à Adaptive Server. Le message d'erreur correspondant doit être ajouté dans Adaptive Server à l'aide de sp_addmessage.

sp_cleanpwdchecks

sp_cleanpwdchecks est une nouvelle procédure stockée personnalisée qui vous permet de définir quand et comment supprimer des attributs associés à un login et à un mot de passe enregistrés dans des tables définies par l'utilisateur. sp_cleanpwdchecks est défini par l'utilisateur et appelé de manière dynamique dans la base de données master lorsque vous supprimez un login.

```
sp_cleanpwdchecks, nom_login
```

où :

- *nom_login* spécifie le login à nettoyer.

sp_passwordpolicy

sp_passwordpolicy est une interface qu'un utilisateur possédant un rôle_sso peut employer pour définir, supprimer et lister les nouvelles options de complexité du mot de passe. Ces informations sont enregistrées dans la table master.dbo.sysattributes.

```
sp_passwordpolicy {set | clear | list }, option_strategie, valeur_option
```

où :

- set applique une valeur à une option.
- clear supprime la ligne de l'option spécifiée dans la table master.dbo.sysattributes. Si aucune option de stratégie n'est spécifiée, clear supprime toutes les lignes d'option de la table sysattributes.
- list liste la valeur des options spécifiées.
- *option_strategie* correspond au paramètre d'option sur lequel effectuer une opération. Les valeurs possibles sont les suivantes :
  - disallow simple passwords : une valeur de 1 active cette option et une valeur de 0 la désactive.
  - min digits in password indique le nombre minimal de chiffres autorisé dans un mot de passe.
  - min alpha in password indique le nombre minimal de caractères alphabétiques autorisé dans un mot de passe.
  - min special char in password indique le nombre minimal de caractères spéciaux autorisé dans un mot de passe.
  - min upper char in password indique le nombre minimal de lettres majuscules autorisé dans un mot de passe.
  - min lower char in password indique le nombre minimal de lettres minuscules autorisé dans un mot de passe.
  - systemwide password expiration indique le délai d'expiration du mot de passe à l'échelle du système (exprimé en jours).
  - password exp warn interval indique l'intervalle d'avertissement avant l'expiration du mot de passe (exprimé en jours).
  - minimum password length définit la longueur minimale du mot de passe.
  - maximum failed logins définit le nombre maximal d'échecs de connexion possibles dans une session avant que le compte ne soit bloqué.
  - expire login spécifie que l'état du login passe à la valeur "expired" (expiré) lorsque vous créez ou réinitialisez un login. Vous êtes invité à modifier votre mot de passe à la première connexion.
- *valeur_option*est la valeur de *option_strategie*.

Exemple 1

Pour définir un intervalle d'avertissement relatif à l'expiration du mot de passe de sept jours avant celle-ci, entrez :

```
sp_passwordpolicy 'set',
      'password exp warn interval', 7
```

Exemple 2 Pour lister l'option relative au nombre minimal de caractères spéciaux requis, entrez :

```
sp_passwordpolicy 'list',
      'min special char in password'
```

Exemple 3 Pour réinitialiser "disallow simple password" à sa valeur par défaut, entrez :

```
sp_passwordpolicy 'clear', 'disallow simple passwords'
```

Procédures stockées modifiées

Les procédures stockées suivantes ont été modifiées pour la mise en œuvre de la complexité du mot de passe :

- sp_addlogin et sp_password appellent les nouvelles contraintes de vérification de la complexité du mot de passe.
- sp_droplogin : si sp_cleanpwdchecks est présent dans la base de données master, cette commande est exécutée après la suppression d'un login à l'aide de sp_droplogin.
- sp_displaylogin : de nouvelles options de sécurité sp_passwordpolicy sont prises en compte lors de l'affichage des informations de connexion associées à l'expiration du mot de passe, au nombre maximal d'échecs de connexion et à la longueur du mot de passe.

Activation de contraintes de vérification personnalisées du mot de passe

Adaptive Server version 12.5.4 permet à un responsable de la sécurité du système de rédiger des procédures stockées définies par l'utilisateur autorisant des contraintes de vérification du mot de passe personnalisées.

Par exemple, pour mettre en œuvre des contraintes de vérification de l'historique des mots de passe, créez une nouvelle table utilisateur afin d'y enregistrer l'historique.

```
create table pwdhistory
(
      name varchar(30)not null,  -- Login name.
      passwordvarbinary(30)not null,  -- old password.
      pwdate datetime not null,  -- datetime changed.
      changedby varchar(30)not null  -- Who changed.
)
go
```

Cette procédure stockée définie par l'utilisateur peut être appelée lorsque vous définissez un nouveau mot de passe, afin de l'enregistrer sous une forme cryptée dans la table pwdhistory :

```
create proc sp_extrapwdchecks
(
@caller_password varchar(30), --the current password of caller
@new_password    varchar(30),-- the new password of the target acct
@loginame        varchar(30)-- user to change password on
)
as

begin
declare @current_time    datetime,
        @encrypted_pwd   varbinary(30),
        @changedby       varchar(30),
        @cutoffdate      datetime


select @changedby = suser_name()

-- Change this line according to your installation.
-- This keeps history of 12 months only.
select @current_time = getdate(),
       @cutoffdate = dateadd(month,-12,getdate())
select @encrypted_pwd = internal_encrypt(@new_password)

delete master..pwdhistory
    where  name = @loginame
    and    pwdate < @cutoffdate

if not exists ( select 1 from master..pwdhistory
                where name = @loginame
                and   password = @encrypted_pwd )
begin
      insert master..pwdhistory
      select @loginame, internal_encrypt(@caller_password),
             @current_time, @changedby
      return (0)
end
else
begin
      raiserror 22001  --user defined error message
      return (1)
end
end
go
```

Utilisez sp_addmessage pour ajouter le message 22001 défini par l'utilisateur. Un message "raiserror" 22001 indique une erreur au niveau d'une contrainte de vérification personnalisée de la complexité du mot de passe et entraîne un échec de sp_addlogin ou de sp_password.

La procédure stockée suivante, définie par l'utilisateur, peut être employée à des fins de nettoyage après avoir ajouté un historique à l'aide de la commande sp_extrapwdchecks.

```
create proc sp_cleanpwdchecks
(
            @loginame      varchar(30)
                        -- user to change password on
)
as
begin

delete master..pwdhistory
where name = @loginame
end
      go
```

Une fois les deux procédures ci-dessous définies et installées dans la base de données master, elles sont appelées de manière dynamique lors du contrôle de la complexité du mot de passe.

Prise en charge de DDLGen

Logins : TL génère le DDL pour un login ou tous ceux-ci. Cet exemple génère le DDL pour tous les logins sur une machine appelée HARBOR à l'aide du port 1955 :

```
ddlgen -Uroy -Proy123 -SHARBOR:1955 -TL -N%
```

Remarque Le mot de passe contenu dans le DDL généré pour tous les logins est “mot_de_passe”.

Vous pouvez également spécifier un login particulier en utilisant -N*username* au lieu de -N% :

```
ddlgen -Ulogin -Ppassword -Sserver:port -TL -Nusername
```

Si des options de complexité du mot de passe ont été définies à l'échelle du serveur pour le ou les logins, toutes les instructions DDL sp_addlogin et sp_modifylogin sont générées en premier lieu, suivies des instructions DDL pour les options de complexité du mot de passe.

Cet exemple génère le DDL pour le login “george” sur le machine appelée HARBOR à l'aide du port 1955 :

```
ddlgen -Uroy -Proy123 -SHARBOR:1955 -TL -Ngeorge
```

Prise en charge du module externe d'Adaptive Server

Le module externe d'Adaptive Server fournit une administration de la complexité du mot de passe via l'IUG. Pour de plus amples informations, reportez-vous au Chapter 8, « Modifications du module externe d'Adaptive Server. ».

Exportation d'options "set" à partir d'un trigger de connexion

Adaptive Server version 12.5.4 permet aux options set des triggers de connexion de rester valables pendant toute la session de l'utilisateur.

Les options "set" suivantes sont automatiquement exportées :

- showplan
- arithabort [overflow | numeric_truncation]
- arithignore [overflow]
- colnames
- format
- statistics io
- procid
- rowcount
- altnames
- nocount
- quoted_identifier
- forceplan
- fmtonly
- close on endtran
- fipsflagger
- self_recursion

- ansinull
- dup_in_subquery
- or_strategy
- flushmessage
- ansi_permissions
- string_rtruncation
- prefetch
- trigger
- replication
- sort_resources
- transactional_rpc
- cis_rpc_handling
- strict_dtm_enforcement
- raw_object_serialization
- textptr_parameters
- sort_merge
- remote_indexes
- explicit_transaction_required
- statement_cache
- command_status_reporting
- proc_return_status
- proc_output_params

Configuration de triggers de connexion globaux

Adaptive Server version 12.5.4 permet de définir un nouveau trigger de connexion global. Utilisez sp_logintrigger pour configurer un trigger de connexion global exécuté à chaque connexion d'un utilisateur. Si vous souhaitez effectuer des actions spécifiques à l'utilisateur, configurez un trigger de connexion spécifique à l'utilisateur à l'aide de sp_modifylogin ou de sp_addlogin.

sp_logintrigger

Description

sp_logintrigger est la nouvelle procédure à utiliser pour configurer et afficher le trigger de connexion global. Ce trigger de connexion global présente les mêmes caractéristiques qu'un script de connexion personnel. Il est exécuté avant tout script de connexion personnel pour chaque utilisateur qui tente de se connecter, y compris les administrateurs système et les responsables de la sécurité.

Syntaxe

sp_logintrigger <*nom du trigger de connexion global*>

Paramètres

nom du trigger de connexion global

est le nom du trigger de connexion global.

Si aucun paramètre n'est inclus, sp_logintrigger affiche l'état et le nom du trigger de connexion actuel, s'il existe, et aucune ligne si aucun trigger de connexion global n'est défini.

Exemples

Exemple 1 Pour définir un trigger de connexion global à l'aide de sp_logintrigger :

```
sp_logintrigger 'master.dbo.myproc'
```

Exemple 2 Pour visualiser un trigger de connexion global mis à jour :

```
1> sp_logintrigger
2> go
Global login trigger               Status
---------------------------------- -------
sybsystemprocs.dbo.myproc          Enabled

(1 row affected)
(return status = 0
```

Exemple 3 Lorsqu'aucun trigger de connexion global n'existe :

```
1> sp_logintrigger
2> go
Global login trigger Status
-------------------- ------
(0 rows affected)
```

Exemple 4 Pour supprimer un trigger de connexion global spécifié précédemment avec sp_logintrigger, entrez :

```
sp_logintrigger 'drop'
```

Syntaxe

- Une nouvelle variable globale *@@logintrigger* est utilisée pour déterminer si un trigger de connexion global est défini et autorisé.
- Il existe une différence entre ce trigger de connexion global et le script de connexion privé. Ce trigger de connexion global est stocké en fonction de son nom dans sysattributes, alors que le script de login privé n'est enregistré qu'en fonction de son ID d'objet.

Autorisations

Tout le monde peut exécuter sp_logintrigger pour afficher le trigger de connexion global actuel. Pour configurer un nouveau trigger de connexion, un rôle SSO est nécessaire.

CHAPITRE 3

Accès à la base de données archive

L'accès à la base de données archive offre à l'administrateur de base de données la possibilité de valider ou de récupérer de manière sélective des données depuis une sauvegarde de la base de données (une “archive”) en utilisant celle-ci comme s'il s'agissait d'une base de données traditionnelle en lecture seule. Ce type de base de données est appelé “base de données archive”.

Contrairement aux bases de données traditionnelles, la base de données archive utilise la sauvegarde de la base de données à proprement parler comme device de stockage principal, et une quantité minimale de stockage traditionnel, qui lui sert à représenter les pages nouvelles ou modifiées résultant de la récupération de la sauvegarde de la base de données. Une sauvegarde de base de données contient déjà les images de nombreuses pages de la base de données (voire de la plupart d'entre elles). Par conséquent, il est possible de charger une base de données archive sans avoir recours au Backup Server pour transférer des pages de celle-ci vers le stockage traditionnel de la base de données. Raison pour laquelle le chargement s'effectue considérablement plus vite que celui d'une base de données traditionnelle.

Présentation

L'accès à la base de données archive permet d'effectuer diverses opérations directement sur une sauvegarde de la base de données.

La capacité de stockage nécessaire pour le chargement d'une base de données traditionnelle doit être égale ou supérieure à la taille de la base de données source ; le chargement de la sauvegarde de la base de données à l'aide du Backup Server implique de copier les pages de la sauvegarde de la base de données vers le stockage réservé à cet effet.

En revanche, vous pouvez créer une base de données archive avec un minimum d'espace disque traditionnel. Lorsque vous chargez une base de données archive, les pages résidant dans la sauvegarde de la base de données ne sont pas copiées par le Backup Server. Au lieu de cela, Adaptive Server crée un mappage "logique/virtuel" des pages de l'archive. Ceci réduit considérablement le temps requis pour visualiser les données de la sauvegarde de la base de données et réduit l'espace disque requis pour le chargement de celle-ci.

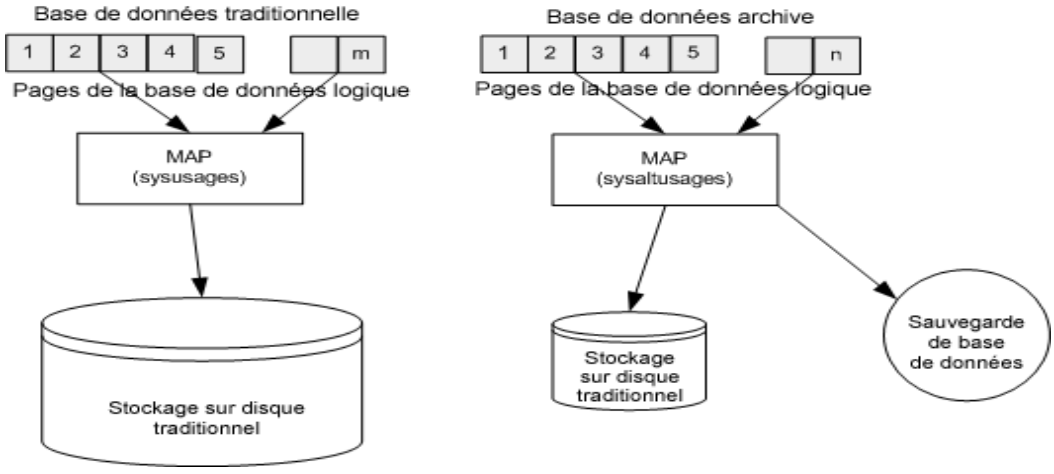
Une base de données archive ne doit pas nécessairement être la copie fidèle de la base de données d'origine. Selon l'optimisation utilisée lors de la sauvegarde de la base de données à l'aide de la commande sp_dumpoptimize, la base de données archive peut être complète (chaque page de la base de données se retrouve dans la sauvegarde) ou partielle (seules certaines pages sont enregistrées).

La sauvegarde de la base de données se présentant sous la forme d'une base de données (en lecture seule), un administrateur de base de données peut y effectuer des requêtes à l'aide d'outils et techniques habituels tels que :

- Contrôles d'intégrité sur la dernière copie d'une sauvegarde effectuée depuis une base de données de production. Ces contrôles peuvent être confiés à un autre serveur, afin d'éviter une saturation des ressources dans l'environnement de production. Si les ressources ne posent aucun problème, l'archive peut être vérifiée directement sur le serveur où elle a été créée. La vérification de l'archive offre toutes les garanties nécessaires avant une opération de restauration.
- Si l'intégrité d'une sauvegarde de la base de données pose question, la restaurer dans une base de données archive permet de déterminer rapidement s'il y a un problème. Il s'agit donc d'un outil efficace pour identifier la base de données à utiliser pour restaurer une base de données traditionnelle.
- Restauration au niveau de l'objet depuis la sauvegarde de la base de données. Les données perdues sont restaurées en utilisant la commande select into pour copier les lignes à restaurer depuis la table de la base de données archive. L'opération select into peut être effectuée directement sur le serveur qui héberge la base de données archive ou à l'aide des tables proxy Component Integration Services si la base de données archive se trouve sur un serveur autre que celui de l'objet nécessitant la restauration.

La figure suivante illustre les différences entre la structure d'une base de données archive et celle d'une base de données traditionnelle.

Figure 3-1 : Composants de la base de données archive



Composants d'une base de données archive

Une base de données archive se compose de trois éléments qui interagissent pour créer l'illusion qu'une sauvegarde de base de données fonctionne comme une base de données traditionnelle. Ces composants sont les suivants :

- La sauvegarde de la base de données (l'archive)
- Le stockage sur disque traditionnel utilisé pour enregistrer la section des pages modifiées
- La base de données scratch, qui héberge la table sysaltusages

La sauvegarde de la base de données

La sauvegarde de la base de données sert de référentiel pour la plupart des pages non modifiées.

La sauvegarde de la base de données est accessible en lecture seule. Vous ne pouvez pas la modifier. Tout changement apporté aux données de la sauvegarde sera enregistré dans la section des pages modifiées.

Adaptive Server considère la sauvegarde de la base de données et ses devices de sauvegarde comme des devices de base de données qui ne peuvent être utilisés que par la base de données archive.

La section des pages modifiées

Les sauvegardes de la base de données sont des clichés de la base de données à un moment donné. La base de données archive qui représente une sauvegarde de la base de données n'est accessible qu'en lecture seule. Aucune transaction utilisateur n'est autorisée. Toutefois, certaines modifications sont permises. Par exemple :

- Vous pouvez effectuer une restauration afin d'assurer la cohérence de la base de données archive.
- Les commandes dbcc qui apportent des corrections sont autorisées, de manière à pouvoir restaurer des versions corrigées des tables.

Ces pages de base de données modifiées et nouvellement allouées ne peuvent pas être stockées dans la sauvegarde de la base de données ni sur ses devices de sauvegarde. Par conséquent, une base de données archive requiert un stockage de base de données traditionnel. Cet espace disque est également appelé "section des pages modifiées", et vous pouvez l'allouer à l'aide des commandes create archive database et alter database.

La base de données scratch et la table sysaltusages

La table *sysaltusages*

La table système sysaltusages est une nouvelle table verrouillée au niveau des pages de données uniquement, qui est utilisée pour mapper les numéros de page de la base de données archive avec la page réelle de la sauvegarde et de ses devices ou de la section des pages modifiées. Toutefois, contrairement à la table sysusages d'une base de données traditionnelle, la table sysaltusages ne mappe pas chaque page logique de la base de données. sysaltusages mappe :

- les pages stockées dans une sauvegarde de base de données ;
- les pages modifiées et dès lors déplacées vers la section des pages modifiées.

sysaltusages comporte les colonnes suivantes :

```
dbid    location    lstart    start    size    vstart    vdevno    segmap
```

où :

- dbid est l'ID de la base de données archive.
- location est l'emplacement du segment de la base de données archive où réside le bloc de pages physiquement contiguës.

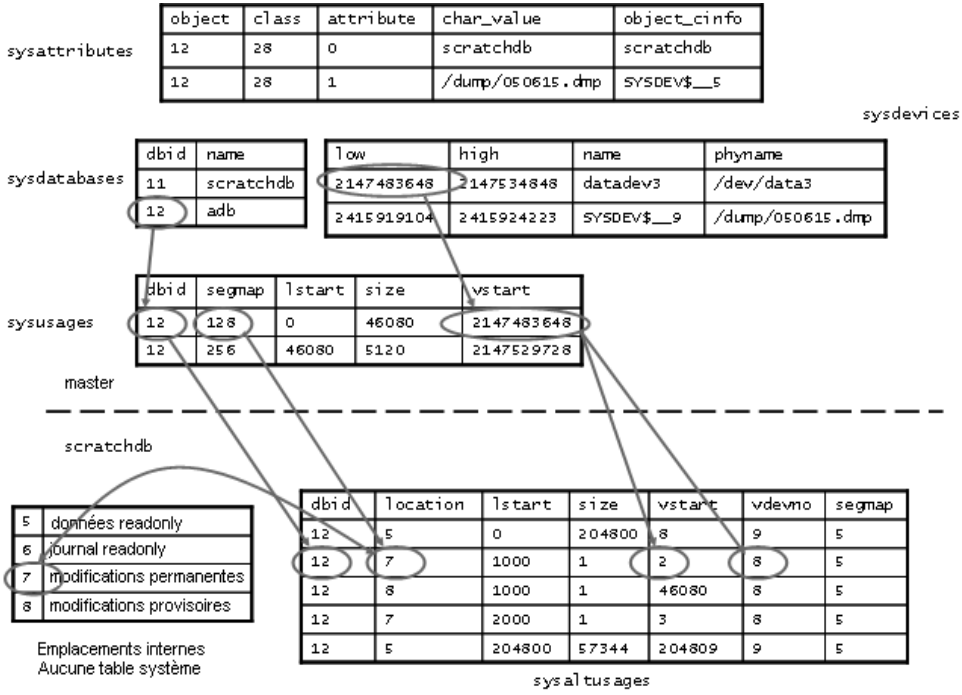
  Une valeur de 5 et 6 signifie que l'emplacement se trouve dans la sauvegarde de la base de données ou dans ses devices de sauvegarde, et une valeur de 7 ou 8 signifie que l'emplacement se trouve dans la section des pages modifiées. Une valeur de 4 est utilisée pour combler les lacunes correspondant à des pages qui ne sont pas physiquement disponibles.

- lstart est le numéro de page logique du début du bloc de pages physiquement contiguës.
- size est le nombre de pages logiques du bloc de pages physiquement contiguës.
- vstart est l'offset du début du bloc de pages physiquement contiguës sur le device indiqué par vdevno.
- vdevno est le numéro du device sur lequel réside le bloc de pages physiquement contiguës.
- segmap est un mappage des segments auxquels est alloué ce bloc de pages.

La table sysaltusages ressemble à celle illustrée dans la Figure 3-2.

Remarque sysaltusages étant un catalogue verrouillé au niveau des lignes, il se peut que vous deviez de temps à autre utiliser la commande reorg pour récupérer de l'espace logique supprimé.

Figure 3-2 : La table sysaltusages



La base de données scratch

La base de données scratch contient la nouvelle table sysaltusages. La base de données scratch est utilisée pour rendre l'emplacement de la table sysaltusages souple.

La base de données scratch peut être n'importe quelle base de données (à quelques exceptions près, telles les bases de données master et temporary). Sybase vous recommande de réserver une base de données exclusivement à cet effet, pour les raisons suivantes :

- La taille de sysaltusages peut varier en fonction du nombre de bases de données archives gérées. Vous ne pouvez pas réduire la taille de la base de données. Toutefois, si elle devient trop volumineuse, vous pouvez la supprimer et en créer une plus petite lorsque cela s'avère nécessaire.
- Cela vous permet d'activer l'option "trunc log on checkpoint" de sorte que le journal de la base de données soit tronqué automatiquement.

Outre le fait qu'elle héberge la table sysaltusages, cette base de données est comme toutes les autres. Vous pouvez utiliser des procédures associées au seuil et d'autres mécanismes ad hoc pour gérer l'espace dans la base de données.

Vous pouvez spécifier une base de données à utiliser comme base de données scratch en entrant :

```
sp_dboption <db name>, "scratch database", "true"
```

Chaque base de données archive ne peut être affectée qu'à une seule base de données scratch à la fois, mais plusieurs bases de données archives peuvent utiliser la même base de données scratch. Si vous possédez un grand nombre de bases de données archives, il peut être préférable de définir plusieurs bases de données scratch.

Manipulation d'une base de données archive

De nombreuses opérations de base de données traditionnelles sont possibles sur une base de données archive. Toutefois, les transactions et les commandes définies par l'utilisateur qui modifient la base de données, telles que insert, update et delete, ne sont pas autorisées.

Une base de données archive remplie ressemble à une base de données en lecture seule, où l'option 'readonly' a été appliquée à l'aide de la procédure stockée sp_dboption.

Configuration d'une base de données archive

Cette section fournit des informations sur la manière de créer et de configurer une base de données archive.

Création d'une base de données archive

Vous pouvez créer une base de données archive en exécutant la commande create archive database. La syntaxe est la suivante :

```
create archive database <nom_base>
    [on <device_base> [= <taille>]
        [, <device_base> [= <taille>] ] ... ]
    with scratch_database = <nom_base>
```

où :

- on spécifie la section des pages modifiées. Adaptive Server a besoin d'un stockage de base de données traditionnel pour stocker les pages modifiées. Utilisez la clause on pour spécifier l'emplacement et la taille de la section des pages modifiées.
  - *device_base* spécifie le device de base de données sur lequel vous souhaitez créer votre section des pages modifiées.
  - *taille* spécifie la taille de la section des pages modifiées à créer. Si *taille* est omis, 5120 pages sont allouées.
- with scratch_database (obligatoire) spécifie le nom d'une base de données existante dans laquelle sont gérées les informations relatives à la base de données archive. La table sysaltusages, qui mappe chaque page logique de la base de données archive avec une page physique, est stockée dans la base de données scratch.

Dimensionnement de la section des pages modifiées

La section des pages modifiées est utilisée pour stocker les pages de base de données modifiées ou nouvellement allouées.

- Une page ne peut être remappée qu'une seule fois à la section des pages modifiées.
- La restauration est responsable de la plupart des remappages de pages.
- dbcc checkalloc exige également une allocation d'espace significative.
- La taille de la section des pages modifiées peut être augmentée à l'aide de la commande alter database. Toutefois, pour diminuer la taille de la section des pages modifiées, vous devez supprimer la base de données archive et la régénérer.

La taille minimale de la section des pages modifiées dépend du nombre de pages modifiées ou nouvellement allouées dans la base de données. Beaucoup de ces pages sont modifiées par des restaurations de reprises ou d'annulations.

Utilisez la commande load database with norecovery pour minimiser le nombre de pages modifiées et donc l'espace requis dans la section des pages modifiées. Toutefois, cette opération présente également des inconvénients. Pour plus d'informations, voir « Utilisation de load database with norecovery », page 66.

Remarque dbcc checkalloc occupe un grand espace dans la section des pages modifiées, même si vous utilisez l'option nofix. Lorsque vous exécutez dbcc checkalloc, des informations sont écrites sur chaque page d'allocation (toutes les 256èmes pages). Ces modifications apportées aux pages d'allocation sont stockées dans la section des pages modifiées et signifient que, lorsque vous utilisez dbcc checkalloc, votre section des pages modifiées doit être équivalente à au moins 1/256ème de la taille de la base de données d'origine.

Si vous ne disposez pas de suffisamment d'espace dans la section des pages modifiées, la commande est suspendue et vous voyez apparaître une erreur qui ressemble à ceci :

```
There is no more space in the modified pages section for
the archive database <database name>. Use the ALTER
DATABASE command to increase the amount of space
available to the database.
```

Pour augmenter l'espace de la section des pages modifiées, deux solutions s'offrent à vous :

- Utilisez alter database pour accroître la taille de la section des pages modifiées, ou
- Si vous ne souhaitez pas allouer davantage d'espace à la section des pages modifiées, entrez Ctrl+C pour annuler la commande en cours.

Remarque Vous ne pouvez pas avoir recours à des seuils pour gérer l'espace de la section des pages modifiées.

Accroissement de l'espace alloué à la section des pages modifiées

Vous pouvez utiliser alter database pour ajouter de l'espace à la section des pages modifiées de la base de données archive. Ceci permettra à la commande suspendue de poursuivre sa tâche.

Vous pouvez utiliser alter database à tout moment pour augmenter la taille de la section des pages modifiées, et pas seulement lorsque l'espace devient insuffisant.

```
alter database <nom_base>
    [on <device_base> [= <taille>]
        [, <device_base> {= <taille>] ] ...]
```

Matérialisation d'une base de données archive

Une base de données archive est une marque de réservation qui ne sert qu'une fois alimentée par une sauvegarde de la base de données. La procédure de chargement ne copie pas réellement les pages. Toutefois, elle matérialise la base de données en mappant celles-ci.

Utilisez la commande load database pour matérialiser une base de données archive. La syntaxe est la suivante :

```
load database <nom_base>
    from <device_de_sauvegarde>
    [ [stripe on <device_sauvegarde>] ... ]
    [with [norecovery,][passwd=<mot_de_passe>]
```

où :

- *nom_base* spécifie le nom de la base de données archive dans laquelle vous souhaitez effectuer le chargement.
- *device_de_sauvegarde* spécifie le nom de la sauvegarde de base de données sur disque à partir de laquelle vous souhaitez effectuer le chargement.
- *device_sauvegarde* spécifie les devices de sauvegarde supplémentaires pour la base de données (disques).
- norecovery indique que la commande load database n'effectuera pas de restauration et que la base de données sera mise en ligne automatiquement dès que la commande load database se sera terminée. Pour plus d'informations, voir « Utilisation de load database with norecovery », page 66.

  Remarque norecovery a été introduit dans Adaptive Server version 12.5.4 à des fins d'accès à la base de données archive. Vous ne pouvez pas utiliser norecovery sur une base de données traditionnelle.

- passwd =*<mot_de_passe>* doit être spécifié si la sauvegarde à partir de laquelle vous chargez la base de données archive est protégée par un mot de passe. Le mot de passe doit comporter entre 6 et 30 caractères.

Remarque Il n'est pas nécessaire que le Backup Server tourne lors du chargement d'une sauvegarde dans une base de données archive.

Utilisation de *load database with norecovery*

L'option with norecovery de la commande load database permet de charger une sauvegarde de base de données dans une base de données archive sans rien restaurer, ce qui réduit le délai de chargement. De nombreuses pages de la base de données peuvent être modifiées ou allouées au cours de la restauration et sont donc stockées dans la section des pages modifiées. Par conséquent, omettre la restauration limite l'espace occupé dans la section des pages modifiées. L'option with norecovery permet de visualiser rapidement une base de données archive.

Si vous utilisez with norecovery, la base de données est mise en ligne automatiquement.

Toutefois, l'utilisation de la commande load database with norecovery pour une base de données nécessitant une restauration risque de la rendre incohérente sur le plan transactionnel et physique. L'exécution de contraintes de vérification dbcc sur une base de données incohérente sur le plan physique peut générer de nombreuses erreurs.

Une fois une base de données archive chargée with norecovery, vous devez posséder un rôle_sa ou des privilèges de propriétaire de base de données pour pouvoir l'utiliser.

Utilisation de devices logiques avec une base de données archive

Vous pouvez utiliser sp_addumpdevice pour créer un device logique au départ duquel une base de données archive peut être chargée. La syntaxe est la suivante :

```
sp_addumpdevice 'base_de_données_archive', '<nom_logique>',
'<nom_physique>'
```

Une fois cette commande exécutée, vous pouvez utiliser le *nom_logique* au lieu du *nom_physique* en tant que *device_de_sauvegarde* ou *device_sauvegarde* dans une commande load database.

Restrictions de *load database* avec une base de données archive

La commande load database présente les restrictions suivantes lorsqu'elle est utilisée avec une base de données archive :

- La sauvegarde de la base de données pour une base de données archive doit être une sauvegarde sur disque présente dans un système de fichiers monté sur la machine locale. Il peut s'agir d'un stockage local ou NFS. La syntaxe `load database ... at <remote server>` n'est pas prise en charge, tout comme les sauvegardes de bases de données sur bandes.

- Les chargements inter-architectures ne sont pas pris en charge. La sauvegarde de la base de données et la commande load database doivent être effectuées sur la même architecture, du fait de l'agencement des octets.
- La base de données sauvegardée doit avoir la même taille de page que le serveur qui héberge la base de données archive.
- La version principale du serveur sur lequel la sauvegarde a été effectuée doit être antérieure ou égale à celle du serveur hébergeant la base de données archive.
- Le jeu de caractères et l'ordre de tri du serveur sur lequel la sauvegarde a été effectuée doivent être identiques à ceux du serveur qui héberge la base de données.
- La taille maximale de tous les devices de sauvegarde de la sauvegarde la base de données ne peut pas dépasser 32 Go.

Remarque Dans le cas contraire, spécifiez des devices supplémentaires lorsque vous exécutez une commande dump database. De cette manière, la taille de chaque device est réduite de manière à respecter la taille maximale.

Mise en ligne d'une base de données archive

Pour mettre une base de données archive en ligne, utilisez :

online database *<nom_base>*

où *nom_base* est le nom de la base de données archive à mettre en ligne.

La commande online database effectue une restauration des annulations au cours de laquelle il est possible que des pages modifiées ou allouées soient remappées dans la section des pages modifiées.

Il n'est pas nécessaire de mettre une base de données en ligne si elle a été chargée avec with norecovery. En effet, la procédure de chargement le fait automatiquement sans exécuter la commande "recovery undo pass".

Suppression d'une base de données archive

Pour supprimer une base de données archive, utilisez :

drop database *<nom_base>*

où *nom_base* est le nom de la base de données à supprimer.

Lorsque vous supprimez une base de donnée archive, toutes les lignes de celles-ci sont effacées de la table sysaltusages dans la base de données scratch. Pour ce faire, de l'espace de journalisation est nécessaire dans la base de données scratch.

Remarque Si l'espace de journalisation vient à manquer dans la base de données scratch pendant l'exécution de drop database, entrez Ctrl+C, tronquez le journal dans la base de données scratch et relancez la commande drop database. Si vous tentez de tronquer le journal de la base de données scratch *sans* avoir préalablement tapé Ctrl+C pour mettre un terme à la commande drop database, la troncation sera suspendue, car elle attendra un accès verrouillé par la commande drop.

Utilisation d'une base de données archive

Cette section fournit des informations sur les commandes qui peuvent exécutées sur une base de données archive.

Utilisation de commandes SQL avec une base de données archive

Outre les commandes déjà documentées, (alter database, load database, online database et drop database), les commandes SQL suivantes sont autorisées dans une base de données archive.

- use
- select
- select into lorsque la base de données cible n'est pas une base de données archive.
- Opérations de curseur effectuant des lectures, dont :
  - declare cursor
  - deallocate cursor
  - open
  - fetch

  Il est impossible d'utiliser un curseur modifiable.

- checkpoint est pris en charge. Toutefois, la procédure "checkpoint" n'effectue pas de points de reprise automatiquement sur une base de données archive.
- La commande execute est possible pour autant que toute instruction faisant référence à la base de données archive soit autorisée dans celle-ci. Une transaction dans ou en dehors d'une procédure stockée n'est pas autorisée avec une commande execute.
- lock table
- readtext

Remarque Les commandes DML, dont insert, update et delete, ne sont pas autorisées, et il est impossible de démarrer des transactions utilisateurs.

Utilisation de commandes dbcc avec une base de données archive

Les commandes dbcc suivantes sont autorisées dans une base de données archive :

- checkdb
- checkcatalog

  Remarque La version fix de checkcatalog n'est pas prise en charge.

- checktable
- checkindex
- checkalloc
- indexalloc
- tablealloc
- textalloc

Les commandes dbcc empêchent d'autres utilisateurs d'accéder à une base de données archive pendant leur exécution. Si vous tentez d'accéder à une base de données archive pendant l'exécution de commandes dbcc, vous recevez un message vous indiquant que la base de données se trouve en mode "single user".

Vous pouvez utiliser des variantes des commandes dbcc ci-dessus sur une base de données archive en ligne ou hors ligne. Toutefois, vous ne pouvez utiliser une commande dbcc avec une option fix que sur une base de données en ligne.

Séquence typique des commandes sur une base de données archive

La syntaxe suivante est typique de la séquence des commandes effectuées sur une base de données :

Pour commencer, créez la base de données scratch à l'aide de la commande create database, si nécessaire.

```
create database scratchdb
      on datadev1 = 100
      log on logdev1 = 50
```

Cette opération crée une base de données traditionnelle de 150 Mo appelée scratchdb.

Utilisez sp_dboption pour désigner la base de données créée comme base de données scratch :

```
sp_dboption "scratchdb", "scratch database", "true"
```

Créez la base de données archive.

```
create archive database archivedb
      on datadev2 = 20
      with scratch_database = scratchdb
```

Cette opération crée une base de données archive appelée archivedb, avec une section des pages modifiées de 20 Mo.

Matérialisez votre base de données archive à l'aide de la commande load database :

```
load database archivedb
      from "/dev/dumps/050615/proddb_01.dmp"
      stripe on "/dev/dumps/050615/proddb_02.dmp"
```

Mettez la base de données en ligne :

```
online database archivedb
```

Vérifiez l'intégrité de la base de données archive à l'aide des commandes dbcc. Par exemple :

```
dbcc checkdb(archivedb)
```

Il est possible de restaurer un objet de la base de données archive à l'aide des commandes select into ou bcp. Par exemple, pour restaurer une table appelée orders de la base de données archive, utilisez :

```
select * into proddb.dbo.orders from
      archivedb.dbo.orders
```

Sécurité et autorisations relatives à une base de données archive

L'autorisation d'exécuter des commandes et des procédures stockées, ainsi que d'accéder à des objets dans une base de données, est identique à celle d'une base de données traditionnelle chargée avec la même sauvegarde sur le même serveur.

Une fois une base de données archive chargée with norecovery, vous devez posséder un rôle_sa ou des privilèges de propriétaire de base de données pour pouvoir y accéder.

Sauvegardes compressées pour une base de données archive

Pour pouvoir utiliser une sauvegarde compressée pour une base de données archive, vous devez effectuer les opérations suivantes :

- Créez la sauvegarde compressée avec l'option with compression = <niveau_compression> de la commande dump database.
- Créez une zone de mémoire pour l'accès à la base de données archive.

Remarque Les sauvegardes générées avec “compress::” ne peuvent pas être chargées dans une base de données archive. Par conséquent, toute référence à la compression dans ce chapitre se rapporte aux sauvegardes générées à l'aide de l'option with compression = <niveau_compression>.

La logique de compression a changé dans la version 12.5.4. Pour obtenir des informations sur les problèmes de compatibilité, voir « Problèmes de compatibilité liés aux sauvegardes compressées », page 74.

Création d'une zone de mémoire de compression

Lorsqu'Adaptive Server lit une page provenant d'une sauvegarde compressée, il sélectionne un bloc compressé dans la sauvegarde, le décompresse et en extrait la page requise. Dans Adaptive Server, la compression s'effectue à l'aide de grands buffers provenant d'une zone de mémoire spéciale. La taille de la zone est configurée à l'aide de :

```
sp_configure ‘taille de la mémoire de compression’, <taille>
```

Il s'agit d'un paramètre de configuration dynamique, et la taille est donnée en pages de 2 Ko. Si la taille a la valeur 0, aucune zone n'est créée et il est impossible de charger une sauvegarde compressée.

Pour déterminer la taille optimale pour votre zone, prenez les deux facteurs suivants en considération :

- L'E/S de bloc utilisée par le Backup Server. Par défaut, cette E/S de bloc fait 64 Ko, mais elle peut avoir été modifiée à l'aide de l'option with blocksize de la commande dump database.
- Le nombre d'utilisateurs *simultanés* qui décompressent des blocs dans toutes les bases de données archives. Chaque utilisateur simultané nécessite deux buffers de la même taille que l'E/S de bloc.

Au minimum, autorisez un utilisateur simultané (deux buffers) par base de données archive.

Migration d'une base de données archive

sybmigrate ne déplace pas une base de données archive si toute une installation fait l'objet d'une migration.

sybmigrate ne migre une base de données archive que si celle-ci a été spécifiquement sélectionnée à cette fin. Lorsque vous migrez une base de données archive vers un serveur cible, sybmigrate crée automatiquement une base de données traditionnelle - plutôt qu'une base de données archive - sur le serveur cible.

Mise à niveau ascendante et descendante d'une base de données archive

Cette section fournit des instructions relatives à la mise à niveau ascendante et descendante d'une base de données archive.

Mise à niveau ascendante d'un serveur Adaptive Server avec base de données archive

Il est impossible de mettre une base de données archive à niveau. Si vous chargez une sauvegarde de base de données depuis une version antérieure d'Adaptive Server dans une base de données archive hébergée sur une version plus récente d'Adaptive Server, la base de données ne sera pas mise à niveau sur le plan interne à l'exécution de la commande online database.

Si un serveur Adaptive Server contenant une base de données archive est mis à niveau, toutes les bases de données, à l'exception des bases de données archives, sont mises à niveau. La base de données archive reste sur la version antérieure d'Adaptive Server.

Sybase vous recommande de recharger la base de données archive avec une sauvegarde générée depuis une base de données déjà mise à niveau.

Pour plus d'informations sur la mise à niveau d'Adaptive Server, reportez-vous au *Guide d'installation* d'Adaptive Server pour votre plate-forme.

Mise à niveau descendante d'un serveur Adaptive Server avec base de données archive

Lorsque vous effectuez une mise à niveau descendante vers une version d'Adaptive Server qui ne prend pas en charge les bases de données archives, soyez attentif aux points suivants :

- Si vous devez mettre un serveur Adaptive Server contenant une base de données archive à niveau vers une version d'Adaptive Server qui ne prend pas en charge les bases de données archives, Sybase vous recommande de supprimer la base de données archive avant d'effectuer la mise à niveau descendante.

  Pour éliminer la nouvelle table sysaltusages, supprimez la base de données scratch avant d'effectuer la mise à niveau descendante. sysaltuages ne cause aucun problème si la base de données scratch n'est pas supprimée.

- Backup Server version 12.5.4 contient un nouveau format de compression (with compression = <niveau_compression>), de telle sorte que la sauvegarde puisse être chargée dans une base de données archive. Par conséquent, si vous devez charger une sauvegarde compressée dans une version d'Adaptive Server qui ne prend pas en charge l'accès à la base de données archive, utilisez la version du Backup Server qui a créé la sauvegarde pour la charger. Les versions antérieures de Backup Server ne prennent pas en charge le nouveau format de sauvegarde de base de données compressée.

  Lorsque vous effectuez une mise à niveau descendante sans compression, vous n'avez pas à vous préoccuper de Backup Server.

Problèmes de compatibilité liés aux sauvegardes compressées

- Vous ne pouvez pas charger de sauvegardes générées avec “compress::” dans une base de données archive. Il n'existe aucun problème de compatibilité avec les sauvegardes utilisant cette option de compression dans les bases de données traditionnelles.
- Le format des sauvegardes compressées générées avec l'option with compression = <niveau_compression> a changé. Backup Server version 12.5.4 est le composant qui introduit le nouveau format de compression. Par conséquent :
  - Une sauvegarde compressée effectuée à l'aide d'un Backup Server 12.5.4 ne peut être chargée dans une installation 12.5.3 ou antérieure qu'à l'aide d'un Backup Server 12.5.4 ou supérieur.
  - Si vous utilisez une installation 12.5.3 ou antérieure et souhaitez utiliser vos sauvegardes pour une base de données archive, utilisez une version 12.5.4 de Backup Server pour créer des sauvegardes de base de données compressées.

Remarque Un Backup Server 12.5.4 comprend tant les formats de compression 12.5.4 que les formats antérieurs. Vous pouvez donc utiliser un Backup Server 12.5.4 pour les sauvegardes et les chargements.

Prise en charge de DDLGen pour l'accès à la base de données archive

Pour générer du DDL pour toutes les bases de données archives, utilisez l'option de filtre étendue “OA”.

```
ddlgen -Uroy -Proy123 -SHARBAR:1955 -TDB -N% -XOA
```

Pour générer du DDL pour une seule base de données archive, utilisez la syntaxe relative aux bases de données normales. L'exemple suivant crée du DDL pour la base de données archive archivedb :

```
ddlgen -Uroy -Proy123 -SHARBAR:1955 -TDB -Narchivedb
```

Restrictions de la base de données archive

Les bases de données archives présentent les restrictions suivantes :

- Une base de données archive est accessible en lecture seule.
- Une base de données archive passe automatiquement en mode "single user" lorsqu'une commande résultant dans des modifications de la base de données, telle que les commandes dbcc, est exécutée.
- Une base de données archive n'utilise que des sauvegardes de base de données sur disque. Les sauvegardes sur bande ne sont pas prises en charge.
- La sauvegarde de base de données doit être visible depuis le serveur qui héberge la base de données archive. Les sauvegardes à distance ne sont pas prises en charge.
- load tran n'est pas pris en charge dans Adaptive Server version 12.5.4.
- dbcc checkstorage n'est pas pris en charge dans Adaptive Server version 12.5.4.
- Pour qu'une base de données archive ait accès à des sauvegardes compressées, celles-ci doivent avoir été créées avec l'option with compression plutôt qu'avec l'option “compress::”.
- La procédure "checkpoint" n'effectue pas de points de reprise automatiquement sur une base de données archive. Pour ce faire, utilisez la commande checkpoint.
- Vous ne pouvez pas utiliser sp_dbrecovery_order pour spécifier une base de données archive dans la séquence de restauration de la base de données. Les bases de données archives sont restaurées en dernier lieu, dans l'ordre de leur *idbase*.
- Lorsque des pages sont mises en mémoire cache dans une base de données archive, elles sont conservées dans une zone de mémoire présentant la même taille de page que le serveur. Ainsi, sur un serveur de 2 Ko, les pages sont toujours mises en mémoire cache dans une zone de 2 Ko. Sur un serveur de 16 Ko, les pages sont toujours mises en mémoire cache dans une zone de 16 Ko.
- Il est impossible de lier une base de données archive ou un objet de cette base à un cache défini par l'utilisateur. Par défaut, les objets d'une base de données archive se trouvent dans le cache de données par défaut.

- disk resize ne fonctionne sur aucun device utilisé par une base de données archive et effectuant un mappage avec une sauvegarde de base de données ou un journal de transactions.
- disk refit ne régénère pas les entrées sysusages de la base de données master à partir d'un device utilisé par une base de données archive. Ceci s'applique à la fois aux devices de sauvegarde et à ceux utilisés pour la section des pages modifiées. Toutefois, les entrées sysusages relatives à une base de données archive subsistent.
- Il est impossible de répliquer une base de données archive.
- Une base de données archive ne bascule pas vers un serveur haute disponibilité.
- Il n'est pas possible d'établir des seuils d'espace disponible sur une base de données archive.

CHAPITRE 4

Modifications du répertoire partagé

Adaptive Server version 12.5.4 comprend plusieurs modifications de la structure du répertoire partagé.

Modifications du répertoire partagé

Adaptive Server version 12.5.4 comprend plusieurs modifications de la structure du répertoire partagé. Le tableau1 montre le répertoire.

Tableau 1 : La structure du répertoire partagé change pour les plates-formes UNIX et LINUX.

Composant	Ancien emplacement	Nouvel emplacement
Répertoire partagé	*$SYBASE/shared-1_0*	*$SYBASE/shared*
Sybase Central	*$SYBASE/sybcent41*	*$SYBASE/shared/sybcentral43*
JRE	*$SYBASE/shared-1_0/JRE-1_3*	*$SYBASE/shared/jre142*
Fichier JAR partagé	*$SYBASE/shared-1_0/lib*	*$SYBASE/shared/lib*

Tableau 2 : La structure du répertoire partagé change pour les plates-formes Microsoft Windows.

Composant	Ancien emplacement	Nouvel emplacement
Répertoire partagé	*%SYBASE%\shared-1_0*	*%SYBASE%\Shared*
Sybase Central	*%SYBASE%\sybcent41*	*%SYBASE%\Shared\Sybase Central 4.3*
JRE	*%SYBASE%\shared-1_0\JRE-1_3*	*%SYBASE%\Shared\Sun\jre142*
Fichier JAR partagé	*%SYBASE%\shared-1_0\lib*	*%SYBASE%\Shared\lib*

Remarque Tous les composants d'Adaptive Server ont été modifiés de manière à utiliser la nouvelle structure de répertoire.

Adaptive Server contient les applications Java suivantes, qui sont concernées par cette modification :

- Sybase Central
- Module externe ASE
- DDLGen

- ASE Replicator
- Web Services Producer et Web Services Consumer
- SQL Debugger
- Outil de migration
- Job Scheduler

CHAPITRE 5

Support des pilotes Sybase

Adaptive Server version 12.5.4 contient de nouveaux pilotes ODBC et OLE DB développés par Sybase. Les pilotes ODBC et OLE DB Driver Kit de fournisseurs tiers disponibles avec les précédentes versions ne sont plus fournis avec Adaptive Server. Toutefois, ils continueront à faire l'objet d'un support conformément au calendrier ci-dessous.

L'ODBC Driver Kit retiré était installé sous *%SYBASE%\ODBC* et enregistré en tant que “Sybase ASE ODBC Driver” auprès du gestionnaire de pilotes ODBC. Le nouvel ASE ODBC Driver de Sybase est installé dans *%SYBASE%\DataAccess\ODBC* et enregistré sous le nom “Adaptive Server Enterprise”. La version fournie avec Adaptive Server 12.5.4 est 12.5.1.510.

L'OLE DB Driver Kit retiré était installé sous *%SYBASE%\OLEDB,* et utilisait le nom court “Sybase.ASEOLEDBProvider” et le nom long “Sybase ASE OLE DB Provider” pour le fournisseur. Le nouvel ASE OLE DB Provider de Sybase est installé dans *%SYBASE%\DataAccess\OLEDB* et utilise le nom court du fournisseur “ASEOLEDB”. La version fournie avec Adaptive Server 12.5.4 est 12.5.1.510.

Poursuite du support pour les pilotes de fournisseurs tiers

Les clients existants possédant des contrats de support valables et utilisant déjà ODBC Driver et OLE DB Provider pourront continuer à bénéficier d'un support pour ces produits tout au long du cycle de vie d'ASE 12.5.

Le programme de support sera maintenu à son état actuel jusqu'au 30 juillet 2007. Passé cette date, Sybase ne répondra plus qu'aux problèmes P1 (degré de sévérité 1). Des mises à jour pour ces pilotes seront fournies sur la base de téléchargements autonomes.

Veuillez noter que les ODBC Driver et OLE DB Provider de fournisseurs tiers que vous possédez aujourd'hui ne prennent pas en charge les fonctionnalités introduites après la version 12.5.3 d'ASE. Les problèmes détectés avec ces pilotes ne feront l'objet d'un support Sybase que s'ils sont reproductibles dans ASE 12.5.3. Si vous utilisez ces produits tiers avec des versions postérieures à ASE 12.5.3, il est possible que Sybase ne puisse pas identifier ou corriger le problème.

Reportez-vous à the Sybase Web site à l'adresse http://www.sybase.com/detail?id=1040652 pour lire la note relative à la fin de vie de ces pilotes.

Migration vers de nouveaux pilotes

Sybase vous recommande de procéder dès que possible à la migration vers les nouveaux pilotes ODBC et OLE DB. Les pilotes tiers ne prennent pas en charge les fonctionnalités d'Adaptive Server ajoutées dans Adaptive Server version 12.5.4 ou ultérieures.

Reportez-vous au document *Nouvelles fonctionnalités de OpenServer 12.5.1 et SDK 12.5.1 pour Windows, Linux et UNIX* pour obtenir des instructions concernant la migration vers les nouveaux pilotes.

CHAPITRE 6

Chargement dynamique des bibliothèques TIBCO

Adaptive Server version 12.5.4 introduit une possibilité de chargement dynamique des bibliothèques JMS TIBCO.

Chargement dynamique des bibliothèques de messages d'Adaptive Server

Adaptive Server version 12.5.4 charge de manière dynamique les bibliothèques de messages dont il a besoin pour interagir avec les bus de messages TIBCO EMS et IBM MQ.

Les bibliothèques de messages d'Adaptive Server contiennent la logique de message et agissent comme des encapsuleurs en plus des bibliothèques de messages fournies par les fournisseurs comme TIBCO et IBM. Ces bibliothèques de messages Adaptive Server sont disponibles à l'achat de RTDS 3.5 et ultérieur. Après avoir installé Adaptive Server, vous devez installer RTDS 3.5 pour bénéficier des DLL de messages d'Adaptive Server. Pour ce faire, utilisez le répertoire *$SYBASE/ASE-12_5/lib*.

Outre les bibliothèques de messages d'Adaptive Server, vous devez disposer des bibliothèques de messages et DLL des fournisseurs (TIBCO et IBM).

Une fois les bibliothèques de messages d'Adaptive Server et les bibliothèques de bus de messages spécifiques au fournisseur installées, modifiez LD_LIBRARY_PATH (ou équivalent) en y indiquant l'emplacement de celles-ci.

Par défaut, les bibliothèques de messages d'Adaptive Server se trouvent sous *$SYBASE/ASE-12_5/lib*.

Vous devez également ajouter l'emplacement des DLL proposées par le fournisseur dans LD_LIBRARY_PATH (ou équivalent). Voir

Ajout d'informations sur l'emplacement des DLL JMS TIBCO

À supposer que TIBCO_HOME soit l'emplacement où a été installé TIBCO EMS version 4.2 ou 4.3, les chemins spécifiques a la plate-forme sont les suivants :

- Sur les plates-formes Solaris 32 bits, ajoutez *$TIBCO_HOME/clients/c/lib* à LD_LIBRARY_PATH.
- Sur les plates-formes Solaris 64 bits, ajoutez la chaîne suivante à LD_LIBRARY_PATH :
  - *$TIBCO_HOME/clients/c/lib/64*
  - *$TIBCO_HOME/clients/c/lib*
- Sur les plates-formes Linux 32 bits, ajoutez *$TIBCO_HOME/clients/c/lib* à LD_LIBRARY_PATH.
- Sur les plates-formes Windows 32 bits, ajoutez *%TIBCO_HOME%\clients\c\bin* à PATH.
- Sur les plates-formes HP-UX 64 bits, ajoutez la chaîne suivante à LD_LIBRARY_PATH :
  - *$TIBCO_HOME/clients/c/lib/64*
  - *$TIBCO_HOME/clients/c/lib*
- Sur les plates-formes IBM AIX 64 bits, ajoutez la chaîne suivante à LIBPATH :
  - *$TIBCO_HOME/clients/c/lib/64*
  - *$TIBCO_HOME/clients/c/lib*

Ajout de DLL IBM MQ à LD_LIBRARY_PATH

À supposer que MQM_HOME soit l'emplacement où a été installé MQ Client Library, les chemins spécifiques a la plate-forme sont les suivants :

- Sur les plates-formes Solaris 32 bits, ajoutez *$MQM_HOME/lib* à LD_LIBRARY_PATH.
- Sur les plates-formes Solaris 64 bits, ajoutez *$MQM_HOME/lib64* à LD_LIBRARY_PATH.
- Sur les plates-formes Linux 32 bits, ajoutez *$MQM_HOME/lib* à LD_LIBRARY_PATH.

- Sur les plates-formes Windows 32 bits, ajoutez *%MQM_HOME%\bin* à PATH.
- Sur les plates-formes HP-UX 64 bits, ajoutez *$MQM_HOME/lib64* à LD_LIBRARY_PATH.
- Sur les plates-formes IBM AIX 64 bits, ajoutez *$MQM_HOME/lib64* à LIBPATH.

Remarque MQM_HOME est */opt/mqm* pour Solaris, Linux et HP-UX et */usr/mqm* sur IBM AIX. Sous Windows, il s'agit du répertoire où est installé Websphere MQ.

En outre, la sp_configure 'enable real time messaging' a été modifiée afin d'accepter le type de messages à activer :

- `sp_configure 'enable real time messaging', 1` autorise les messages TIBCO JMS et IBM MQ. Cette commande réussit si Adaptive Server peut localiser les bibliothèques DLL pour TIBCO JMS et IBM MQ.
- `sp_configure 'enable real time messaging', 1, 'tibco_jms'` n'autorise que les messages JMS TIBCO. Cette commande réussit si Adaptive Server peut localiser les bibliothèques DLL pour TIBCO JMS.
- `sp_configure 'enable real time messaging', 1, 'ibm_mq'` n'autorise que les messages IBM MQ. Cette commande réussit si Adaptive Server peut localiser les bibliothèques DLL pour IBM MQ.

CHAPITRE 7

Prise en charge du protocole JRE

Prise en charge du protocole JRE par Adaptive Server 12.5.4

Adaptive Server version 12.5.4 inclut le protocole JRE 1.4. JRE 1.4 est installé de manière complète et typique par défaut, et de manière personnalisée lorsqu'un composant requérant le protocole JRE pour fonctionner est sélectionné.

CHAPITRE 8

Modifications du module externe d'Adaptive Server

Prise en charge du module externe d'Adaptive Server

Le module externe d'Adaptive Server pour Sybase Central prend en charge l'accès à la base de données archive et la configuration d'options de complexité du mot de passe dans Adaptive Server version 12.5.4.

Utilisez le module externe d'Adaptive Server pour Sybase Central pour gérer les bases de données archives. Un nouveau dossier, appelé Archive Databases, apparaît sous le dossier Databases.

Utilisez le module externe d'Adaptive Server pour Sybase Central pour configurer des options de complexité du mot de passe dans la feuille des propriétés du serveur Adaptive Server. Pour Adaptive Server version 12.5.4, il existe un nouvel onglet dans la feuille des propriétés du serveur, appelé Login Password Configuration.

Pour obtenir de plus amples informations sur l'utilisation du module externe d'Adaptive Server pour gérer l'accès à la base de données archive, reportez-vous au Chapitre 19, « Contrôle de l'accès à Adaptive Server » sous *Gestion d'Adaptive Server Enterprise*. Pour obtenir de plus amples informations sur l'utilisation du module externe d'Adaptive Server pour configurer les options de complexité du mot de passe, reportez-vous au Chapitre 7, « Gestion des bases de données » sous *Gestion d'Adaptive Server Enterprise*.

CHAPITRE 9

Modifications des tables de contrôle

Adaptive Server 12.5.4 apporte les modifications suivantes aux tables de contrôle.

Modifications des tables de contrôle

Le tableau 9-1 décrit les mises à jour des tables de contrôle.

Tableau 9-1 : Mises à jour des tables de contrôle

Nom de colonne	Table de contrôle	Description
RowsAffected	monSysStatement etmonProcessStatement	Indique le nombre de lignes concernées par l'instruction en cours. Cette fonction est utile lorsque vous recherchez des requêtes utilisant un plan d'exécution de requête inefficace, parce que celles-ci présentent vraisemblablement un nombre élevé d'E/S logiques par ligne renvoyée.

CHAPITRE 10

Mémoire partagée dans les environnements Terminal Server de Windows

Mémoire partagée d'Adaptive Server dans les environnements Terminal Server de Windows

Pour répondre aux exigences de mémoire partagée dans les environnements Terminal Server de Windows, Adaptive Server version 12.5.4 introduit la nouvelle variable d'environnement SYBASE_TS_MODE.

Terminal Server est une fonctionnalité de Microsoft Windows permettant à plusieurs utilisateurs distants de se connecter simultanément au système Windows. Chaque utilisateur se connecte depuis un poste de travail local à un serveur Windows centralisé et obtient ainsi un environnement Windows virtuel, qui apparaît sur son poste de travail. Le serveur Windows conserve bien séparés les espaces mémoires et autres allocations de ressources de ces sessions Terminal Server, de sorte que l'existence des autres sessions est dans une large mesure transparente pour les utilisateurs. En outre, un utilisateur peut être connecté à la machine normalement. Dans ce cas, on parle de "session console".

Le serveur de données Adaptive Server peut être démarré dans une session Terminal Server ou sous la forme d'un service Windows. Dans ce dernier cas, il est considéré comme faisant partie de la session console. Les régions de la mémoire partagée d'Adaptive Server ne sont normalement pas accessibles depuis d'autres sessions Terminal Server, et par conséquent, certains outils, tels que les moniteurs des performances et l'outil diagnostique interne de Sybase (sybmon), ne peuvent pas fonctionner à moins d'être lancés depuis la session du serveur Adaptive Server, étant donné qu'ils doivent se connecter à la région de la mémoire partagée de ce serveur. Si Adaptive Server tourne sous la forme d'un service, ces outils ne peuvent fonctionner que s'ils sont lancés depuis la session console.

Adaptive Server 12.5.4 recherche une variable d'environnement SYBASE_TS_MODE, et si celle-ci a la valeur GLOBAL, Adaptive Server crée sa mémoire partagée de manière à ce qu'elle soit disponible dans toutes les sessions Terminal Server. De la même manière, des modifications apportées au moniteur des performances et à l'outil sybmon recherchent également cette variable d'environnement et se connectent à la mémoire partagée de manière globale si elle a la valeur GLOBAL. De cette manière, vous pouvez configurer une session Terminal distante pour surveiller le fonctionnement d'Adaptive Server dans la session console ou dans toute autre session Terminal Server. La variable SYBASE_TS_MODE devrait normalement être créée en tant que variable d'environnement système, et la machine Windows redémarrée pour l'appliquer.

La variable SYBASE_TS_MODE n'est pas prise en charge par les postes de travail et serveurs Windows NT 4.0 et Windows 2000 Édition professionnelle.

Par défaut, si cette variable n'est pas spécifiée plus avant, elle crée une mémoire partagée uniquement pour la session Terminal Server locale.

Avertissement ! La variable SYBASE_TS_MODE ne doit pas être définie sur une machine ne prenant pas en charge les services Terminal Services, car cela entraînerait un échec de création de la mémoire partagée et Adaptive Server ne démarrait pas.

CHAPITRE 11

Améliorations d'Adaptive Server sur des plates-formes Linux

Ce chapitre présente les améliorations apportées à Adaptive Server sur les plates-formes Linux.

Amélioration de la prise en charge des mémoires de grande taille

La prise en charge des mémoires de grande taille vous permet de définir le paramètre de configuration de la taille de la mémoire cache étendue à une valeur autre 0.

Dans les versions antérieures d'Adaptive Server, la taille de la zone de vidage de la plus petite zone de mémoire E/S des caches primaires avait une valeur fixe. Les valeurs configurées étaient ignorées.

Adaptive Server version 12.5.4 vous permet de configurer la taille de la zone de vidage de la plus petite zone de mémoire E/S du cache primaire.

Prise en charge DIRECTIO

Adaptive Server version 12.5.4 ne prend pas en charge DIRECTIO sur les devices du système de fichiers.

Prise en charge des mémoires de grande taille et des E/S asynchrones POSIX

Adaptive Server version 12.5.4 prend en charge les mémoires de grande taille sur les plates-formes configurées de manière à utiliser les E/S asynchrones POSIX.

CHAPITRE 12

Modifications apportées aux procédures stockées, aux fonctions et aux commandes

Ce chapitre présente les principales modifications apportées dans la version 12.5.4. d'Adaptive Server qui ne sont documentées nulle part ailleurs.

Nouvelle syntaxe pour la commande *shutdown*

Adaptive Server version 12.5.4 propose la nouvelle syntaxe suivante pour la commande "shutdown" :

```
shutdown [srvname] [with {wait [="hh:mm:ss"] | nowait}]]
```

Paramètres

srvname

est le nom logique du Backup Server dans la table système sysservers d'Adaptive Server. Ce paramètre n'est pas requis pour l'arrêt du serveur Adaptive Server local.

with wait

est la valeur par défaut. Celle-ci provoque l'arrêt en douceur d'Adaptive Server ou du Backup Server.

hh:mm:ss

est un paramètre facultatif qui indique le délai maximum pendant lequel le serveur attend que tous les processus en cours ou en veille terminent leurs tâches.

with nowait

arrête immédiatement Adaptive Server ou le Backup Server, sans attendre la fin de l'exécution courante des instructions.

Remarque L'utilisation de shutdown with nowait peut créer des discontinuités dans les valeurs de la colonne IDENTITY.

Indication d'un délai d'attente

Lorsque le serveur se prépare à son arrêt, il :

1 effectue un point de reprise sur toutes les bases de données ;

2 empêche tout nouvel utilisateur de se connecter ;

3 attend que tous les processus en cours ou en veille aient terminé leurs tâches ;

4 effectue un autre point de reprise sur les bases de données, indiquant cette fois qu'il est nécessaire d'effectuer une sauvegarde :

- de tous les seuils dynamiques dans des bases de données à segments de données et journal mixtes,
- de toutes les statistiques d'objets,
- des valeurs des champs identity pour éviter des lacunes après la restauration.

Lorsque vous utilisez le paramètre "with wait" avec l'option *hh:mm:ss*, le temps total indiqué ne correspond pas au délai maximal de fermeture d'Adaptive Server. Au contraire, Adaptive Server tient compte du temps nécessaire pour effectuer le premier point de reprise et le soustrait automatiquement du délai spécifié.

Par exemple, si vous indiquez un délai d'attente maximal de 20 minutes et que le premier point de reprise prend 3 minutes, Adaptive Server laisse 17 minutes aux processus pour se clôturer. Il est possible que, pour une quelconque raison, le second point de reprise prenne plus de temps. Toutefois, celui-ci n'est pas calculé dans le paramètre "with wait" *hh:mm:ss* défini.

Adaptive Server permet également qu'un point de reprise prenne plus de temps que le délai spécifié dans le paramètre "with wait" *hh:mm:ss*. Par exemple, si vous indiquez un délai d'attente de 10 minutes et que le premier point de reprise prend 20 minutes, Adaptive Server n'interrompt pas le premier point de reprise à mi-chemin mais attend qu'il se termine. Dans ce cas, Adaptive Server s'arrête immédiatement après la fin du point de reprise, le délai défini s'étant écoulé, et exécute le dernier point de reprise avec l'indicateur vous informant des sauvegardes à effectuer.

Syntaxe *select ** étendue

Lorsque le texte source d'une procédure stockée ou d'un trigger est enregistré dans la table système syscomments, une requête utilisant select * est stockée dans syscomments, étendant la liste des colonnes référencées dans la commande select *.

Par exemple, une commande select * provenant d'une table contenant les colonnes col1 et col2 est enregistrée sous :

```
select <table>.col1, <table>.col2 from <table>
```

Dans 12.5.4, l'expansion de la liste de colonnes est optimisée de manière telle que la conformité des identifiants (noms de tables, noms de colonnes, etc.) avec les règles ad hoc est vérifiée.

Par exemple, il existe une table comportant les colonnes col1 et 2col. Le nom de la seconde colonne commence par un nombre, ce qui n'est possible que si des crochets sont utilisés dans l'instruction create table. Il s'agit des identifiants entre crochets.

Lorsque vous effectuez une commande select * dans une procédure stockée ou un trigger provenant de cette table, le texte de syscomments ressemble à ceci :

```
select <table>.col1, <table>[2col] from <table>
```

Pour les identifiants utilisés dans le texte visant à étendre un objet select *, des crochets sont ajoutés lorsque l'identifiant ne répond pas aux règles ad hoc.

Vous devez ajouter des crochets autour des identifiants afin de vous assurer qu'Adaptive Server puisse utiliser le texte SQL lors d'une mise à niveau vers une version plus récente.

dump database et *load database* avec vérification

Dans Adaptive Server 12.5.4, les commandes "dump database" et "load database" introduisent une option vous permettant de sauvegarder et de restaurer les bases de données en les soumettant à une vérification. La syntaxe de dump database est la suivante :

```
dump database <dbname> with verify [ = header | full ]
```

La syntaxe de "load database" est la suivante :

```
load database <dbname> with verify[only] [= header |
full ]
```

Lorsque vous exécutez la commande dump database, le Backup Server effectue un contrôle minimal des en-têtes et un contrôle structurel des lignes pour les pages de données, à mesure que celles-ci sont copiées dans les archives. Aucun contrôle structurel n'est effectué à ce stade sur les pages de GAM, d'OAM et d'allocation, sur les index, le texte ou les pages de journal.

Vous pouvez effectuer les mêmes contrôles lorsque vous restaurer une archive à l'aide de la commande load with verify[only].

Une archive peut être vérifiée sans chargement physique, à l'aide de la commande load database with verifyonly : cette option affiche les informations d'en-tête de la sauvegarde, de la même manière que l'option de chargement de with headeronly.

Autorisation de mise à jour des catalogues système

L'option de configuration à l'échelle du serveur allow updates to system catalogs est prioritaire sur le paramétrage de la procédure stockée pour la commande allow updates. Si cette option n'est pas activée à l'échelle du serveur, le paramétrage de la procédure stockée détermine si vous pouvez modifier les catalogues système.

Arithmétique modulo pour les types de données numériques

Dans Adaptive Server version 12.5.4, vous pouvez appliquer une arithmétique modulo aux valeurs réelles, flottantes, décimales et numériques ainsi qu'aux entiers.

Nouvelle fonction de prise en charge des exigences d'adresse IPv6IP

L'architecture IPv6 définit une longueur d'adresse IP de 64 octets. La taille de sysprocesses ne pouvant pas être augmentée, Adaptive Server avait besoin d'un moyen permettant de récupérer l'adresse IP complète. Adaptive Server version 12.5.4 introduit une nouvelle fonction permettant de renvoyer des informations depuis le pss :

```
pssinfo(<spid | 0>, '<pss field>')
```

où :

- ID processus*spid* –. Lorsque vous entrez 0, le processus en cours est utilisé.
- Les valeurs possibles pour *pss field* sont les suivantes :
  - ipaddr – Adresse IP client
  - extusername – Lorsque vous utilisez une authentification externe telle que (PAM, LDAP), elle renvoie le nom d'utilisateur PAM ou LDAP externe utilisé.
  - dn – Distinguished Name (nom distinctif) lorsque vous utilisez une authentification LDAP.

  La fonction pssinfo inclut également l'option permettant d'afficher le nom d'utilisateur externe et le nom distinctif.

Fonctions de décodage des transactions externes

Adaptive Server version 12.5.4 ajoute deux fonctions de décodage des transactions externes. Une page man pour chacune d'entre elles suit.

xa_bqual

Description — renvoie la version binaire du composant bqual d'un ID de transaction ASCII XA.

Syntaxe — xa_bqual(*xid*, 0)

Paramètres

xid
est l'ID d'une transaction d'Adaptive Server, obtenu de la colonne xactname dans systransactions ou de sp_transactions.

0
est réservé pour une utilisation ultérieure.

Exemples — **Exemple 1** renvoie “0x227f06ca80”, la traduction binaire du qualifieur de branche pour l'ID de transaction d'Adaptive Server “0000000A_IphIT596iC7bF2#AUfkzaM_8DY6OE0”. L'ID de transaction d'Adaptive Server est obtenu à l'aide de la commande sp_transactions :

```
1> sp_transactions
```

```
xactkey                          type     coordinator starttime           stat
e      connection dbid  spid  loid  failover    srvname  namelen  xactname
------------------------------ -------- ----------- ------------------- ----
------ ---------- ----- ----- ----- ----------- -------  -------  ----------
------------------------------
0x5316000006000000017e4885b0700 External XA          Dec 9 2005  5:15PM In
Command  Attached     7   20    877  Resident Tx  NULL         39
0000000A_IphIT596iC7bF2#AUfkzaM_8DY6OE0
```

```
1> select xa_bqual("0000000A_IphIT596iC7bF2#AUfkzaM_8DY6OE0", 0)
2> go
```

```
...

------------------------------------------------------------------

0x227f06ca80
```

Exemple 2 xa_bqual est souvent utilisé avec xa_gtrid. Cet exemple renvoie les ID de transaction globaux et qualifieurs de branche de toutes les lignes de systransactions dont la colonne coordinator a une valeur de “3” :

```
1> select gtrid=xa_gtrid(xactname,0),
    bqual=xa_bqual(xactname,0)
    from systransactions where coordinator = 3
2> go
        gtrid

        bqual

------------------------------------------------------------------------

------------------------------------------------------------------------

         0xb1946cdc52464a61cba42fe4e0f5232b

         0x227f06ca80
```

Syntaxe

Si une transaction externe est bloquée sur Adaptive Server et que vous utilisez sp_lock et sp_transactions pour identifier la transaction responsable du blocage, vous pouvez utiliser le gestionnaire de transactions XA pour interrompre la transaction globale. Toutefois, lorsque vous exécutez sp_transactions, la valeur de *xactname* renvoyée est au format de chaîne ASCII, alors que le serveur XA utilise une valeur binaire non décodée. L'utilisation de la commande xa_bqual vous permet donc de déterminer la portion bqual du nom de la transaction dans un format compréhensible par le gestionnaire de transactions XA.

xa_bqual renvoie :

- la version traduite de cette chaîne qui suit le second "_" (tiret bas) et précède soit le troisième "_" soit la valeur de fin de chaîne, selon celui de ces éléments qui se présente en premier lieu.
- NULL si l'ID de transaction ne peut pas être décodé ou s'il présente un format inattendu.

Remarque xa_bqual n'effectue pas de contrôle de validation sur l'objet xid, mais ne renvoie qu'une chaîne traduite.

Normes — SQL ANSI – Niveau de conformité : extension Transact-SQL.

Autorisations — Tous les utilisateurs peuvent utiliser xa_bqual.

Voir aussi — **Fonctions** xa_gtrid

Procédures stockées sp_lock, sp_transactions

xa_gtrid

Description — renvoie la version binaire du composant gtrid d'un ID de transaction ASCII XA.

Syntaxe — xa_gtrid(*xactname*, *int*)

Paramètres

xid
est l'ID d'une transaction d'Adaptive Server, obtenu de la colonne xactname dans systransactions ou de sp_transactions.

0
est réservé pour une utilisation ultérieure.

Exemples — **Exemple 1** Dans cette situation typique, renvoie "0x227f06ca80", la traduction binaire du qualifieur de branche, et "0xb1946cdc52464a61cba42fe4e0f5232b", l'ID de transaction global, pour l'ID de transaction d'Adaptive Server "0000000A_IphIT596iC7bF2#AUfkzaM_8DY6OE0" :

```
1> select xa_gtrid("0000000A_IphIT596iC7bF2#AUfkzaM_8DY6OE0", 0)
2> go

       ...

------------------------------------------------------------------------
          0xb1946cdc52464a61cba42fe4e0f5232b

(1 row affected)
```

Exemple 2 xa_bqual est souvent utilisé avec xa_gtrid. Cet exemple renvoie les ID de transaction globaux et qualifieurs de branche de toutes les lignes de systransactions dont la colonne coordinator a une valeur de “3” :

```
1> select gtrid=xa_gtrid(xactname,0),
    bqual=xa_bqual(xactname,0)
    from systransactions where coordinator = 3
2> go
        gtrid

        bqual

------------------------------------------------------------------------

------------------------------------------------------------------------

         0xb1946cdc52464a61cba42fe4e0f5232b

         0x227f06ca80
```

Syntaxe

Si une transaction externe est bloquée sur Adaptive Server et que vous utilisez sp_lock et sp_transactions pour identifier la transaction responsable du blocage, vous pouvez utiliser le gestionnaire de transactions XA pour interrompre la transaction globale. Toutefois, lorsque vous exécutez sp_transactions, la valeur de *xactname* renvoyée est au format de chaîne ASCII, alors que le serveur XA utilise une valeur binaire non décodée. L'utilisation de la commande xa_gtrid vous permet donc de déterminer la portion gtrid du nom de la transaction dans un format compréhensible par le gestionnaire de transactions XA.

xa_gtrid renvoie :

- la version traduite de cette chaîne qui suit le premier “_” (tiret bas) et précède soit le deuxième “_” soit la valeur de fin de chaîne, selon celui de ces éléments qui se présente en premier lieu.
- NULL si l'ID de transaction ne peut pas être décodé ou s'il présente un format inattendu.

Remarque xa_gtrid n'effectue pas de contrôle de validation sur l'objet xid, mais ne renvoie qu'une chaîne traduite.

Normes

SQL ANSI – Niveau de conformité : extension Transact-SQL.

Autorisations

Tous les utilisateurs peuvent utiliser xa_gtrid.

Voir aussi

Fonctions xa_bqual

Procédures stockées sp_lock, sp_transactions

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

V

W