

SYBASE®

新機能ガイド

Adaptive Server® Enterprise

12.5.4

ドキュメント ID : DC20137-01-1254-01

改訂 : 2006 年 6 月

Copyright © 1987-2006 by Sybase, Inc. All rights reserved.

このマニュアルは Sybase ソフトウェアの付属マニュアルであり、新しいマニュアルまたはテクニカル・ノートで特に示されないかぎり、後続のリリースにも付属します。このマニュアルの内容は予告なしに変更されることがあります。このマニュアルに記載されているソフトウェアはライセンス契約に基づいて提供されるものであり、無断で使用することはできません。

このマニュアルの内容を弊社の書面による事前許可を得ずに、電子的、機械的、手作業、光学的、またはその他のいかなる手段によっても、複製、転載、翻訳することを禁じます。

マニュアルの注文

マニュアルの注文を承ります。ご希望の方は、サイベース株式会社営業部または代理店までご連絡ください。マニュアルの変更は、弊社の定期的なソフトウェア・リリース時のみ提供されます。

Sybase の商標

Sybase, Sybase のロゴ, AccelaTrade, 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, Adaptive Server IQ, Adaptive Warehouse, Anywhere Studio, Application Manager, AppModeler, APT Workbench, APT-Build, APT-Edit, APT-Execute, APT-FORMS, APT-Translator, APT-Library, AvantGo, AvantGo Application Alerts, AvantGo Mobile Delivery, AvantGo Mobile Document Viewer, AvantGo Mobile Inspection, AvantGo Mobile Marketing Channel, AvantGo Mobile Pharma, AvantGo Mobile Sales, AvantGo Pylon, AvantGo Pylon Application Server, AvantGo Pylon Conduit, AvantGo Pylon PIM Server, AvantGo Pylon Pro, Backup Server, BizTracker, ClearConnect, Client-Library, Client Services, Convoy/DM, Copernicus, Data Pipeline, Data Workbench, DataArchitect, Database Analyzer, DataExpress, DataServer, DataWindow, DB-Library, dbQueue, Developers Workbench, Direct Connect Anywhere, DirectConnect, Distribution Director, e-ADK, E-Anywhere, e-Biz Integrator, E-Whatever, EC Gateway, ECMAP, ECRTP, eFulfillment Accelerator, Embedded SQL, EMS, Enterprise Application Studio, Enterprise Client/Server, Enterprise Connect, Enterprise Data Studio, Enterprise Manager, Enterprise SQL Server Manager, Enterprise Work Architecture, Enterprise Work Designer, Enterprise Work Modeler, eProcurement Accelerator, EWA, Financial Fusion, Financial Fusion Server, Gateway Manager, GlobalFIX, ImpactNow, Industry Warehouse Studio, InfoMaker, Information Anywhere, Information Everywhere, InformationConnect, InternetBuilder, iScript, Jaguar CTS, jConnect for JDBC, Mail Anywhere Studio, MainframeConnect, Maintenance Express, Manage Anywhere Studio, M-Business Channel, M-Business Network, M-Business Server, MDI Access Server, MDI Database Gateway, media.splash, MetaWorks, My AvantGo, My AvantGo Media Channel, My AvantGo Mobile Marketing, MySupport, Net-Gateway, Net-Library, New Era of Networks, ObjectConnect, ObjectCycle, OmniConnect, OmniSQL Access Module, OmniSQL Toolkit, Open Biz, Open Client, Open ClientConnect, Open Client/Server, Open Client/Server Interfaces, Open Gateway, Open Server, Open ServerConnect, Open Solutions, Optima++, PB-Gen, PC APT Execute, PC Net Library, PocketBuilder, Pocket PowerBuilder, Power++, power.stop, PowerAMC, PowerBuilder, PowerBuilder Foundation Class Library, PowerDesigner, PowerDimensions, PowerDynamo, PowerJ, PowerScript, PowerSite, PowerSocket, Powersoft, PowerStage, PowerStudio, PowerTips, Powersoft Portfolio, Powersoft Professional, PowerWare Desktop, PowerWare Enterprise, ProcessAnalyst, Rapport, Report Workbench, Report-Execute, Replication Agent, Replication Driver, Replication Server, Replication Server Manager, Replication Toolkit, Resource Manager, RW-DisplayLib, S-Designer, SDF, Secure SQL Server, Secure SQL Toolset, Security Guardian, SKILS, smart.partners, smart.parts, smart.script, 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, STEP, SupportNow, S.W.I.F.T. Message Format Libraries, Sybase Central, Sybase Client/Server Interfaces, Sybase Financial Server, Sybase Gateways, Sybase MPP, Sybase SQL Desktop, Sybase SQL Lifecycle, Sybase SQL Workgroup, Sybase User Workbench, SybaseWare, Syber Financial, SyberAssist, SyBooks, System 10, System 11, System XI (ロゴ), SystemTools, Tabular Data Stream, TradeForce, Transact-SQL, Translation Toolkit, UltraLite.NET, UNIBOM, Unilib, Uninull, Unisep, Unistring, URK Runtime Kit for UniCode, Viewer, Visual Components, VisualSpeller, 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, および XP Server は、米国法人 Sybase, Inc. の商標です。

Unicode と Unicode のロゴは、Unicode, Inc. の登録商標です。

このマニュアルに記載されている上記以外の社名および製品名は、各社の商標または登録商標の場合があります。

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.

目次

はじめに	vii
第 1 章	概要 1
	機能とプラットフォームの互換性に関する情報..... 1
	新機能の概要..... 3
第 2 章	セキュリティの機能強化 7
	Kerberos の変更..... 7
	Kerberos 認証用の Adaptive Server プリンシパル名の指定..... 7
	sp_modifylogin および
	sp_addlogin authenticate with オプション..... 9
	sybmapname を使用したユーザ・プリンシパル名の処理..... 12
	MIT Kerberos クライアント・ライブラリのサポート..... 16
	MIT Kerberos をサポートするプラットフォームの拡張..... 16
	LDAP ユーザ認証の強化..... 17
	LDAP ユーザ認証のための Adaptive Server の設定..... 17
	セカンダリ検索サーバのサポート..... 19
	LDAP サーバのステータスの移行..... 22
	LDAP UA の堅牢性の強化..... 23
	LDAP ユーザ認証エラーのトラブルシューティング..... 25
	LDAP ユーザ認証の管理..... 26
	LDAP ユーザ認証のチューニング..... 29
	LDAP ユーザ認証パスワード情報の変更..... 29
	ログイン・マッピングに対する制御の強化..... 30
	SSL サポート..... 32
	PAM のサポート..... 33
	暗号化カラムの更新..... 33
	暗号化カラムの参照整合性..... 33
	alter table と暗号化カラム..... 33
	sp_help および暗号化カラム..... 33
	sp_helprotect および暗号化カラム..... 34
	複雑なパスワードとログインのオプション..... 34
	新しい複雑なパスワード・チェック..... 35
	複雑なパスワード・オプションの相互チェック..... 41

	古いパスワード・チェックと 新しい複雑なパスワード・チェックの設定	42
	複雑なパスワードのストアド・プロシージャ	44
	カスタムのパスワード・チェックの有効化	47
	DDLGen のサポート	49
	Adaptive Server プラグインのサポート	49
	ログイン・トリガからの set オプションのエクスポート	50
	グローバル・ログイン・トリガの設定	51
	sp_logintrigger.....	51
第 3 章	アーカイブ・データベースへのアクセス.....	53
	概要	53
	アーカイブ・データベースのコンポーネント	55
	アーカイブ・データベースの操作	58
	アーカイブ・データベースの設定	59
	アーカイブ・データベースの作成	59
	変更済みページ・セクションのサイズ設定	59
	変更済みページ・セクションに割り付けられた領域の拡張	60
	アーカイブ・データベースのマテリアライズ	61
	アーカイブ・データベースのオンライン化	63
	アーカイブ・データベースの削除	63
	アーカイブ・データベースの使用	64
	アーカイブ・データベースでの SQL コマンドの使用	64
	アーカイブ・データベースでの dbcc コマンドの使用	65
	一般的なアーカイブ・データベース・コマンドの順序	65
	アーカイブ・データベースのセキュリティとパーミッション	66
	アーカイブ・データベースの圧縮ダンプ	67
	圧縮メモリ・プールの作成	67
	アーカイブ・データベースのマイグレート	68
	アーカイブ・データベースのアップグレードとダウングレード	68
	アーカイブ・データベースが含まれる Adaptive Server のアップグレード	68
	アーカイブ・データベースが含まれる Adaptive Server のダウングレード	69
	圧縮ダンプの互換性の問題	69
	アーカイブ・データベースのアクセスの DDLGen サポート	70
	アーカイブ・データベースの制限	70
第 4 章	共有ディレクトリの変更.....	73
	共有ディレクトリの変更.....	73
第 5 章	Sybase によるドライバのサポート.....	75
	継続的にサポートされているサード・パーティのドライバ	75
	新しいドライバへのマイグレート	76

第 6 章	TIBCO ライブラリの動的ロード	77
	Adaptive Server メッセージング・ライブラリの動的ロード.....	77
	TIBCO JMS DLL ロケーション情報.....	78
	IBM MQ DLL の LD_LIBRARY_PATH への追加.....	78
第 7 章	JRE のサポート	81
	Adaptive Server 12.5.4 での JRE サポート.....	81
第 8 章	Adaptive Server プラグインの変更	83
	Adaptive Server プラグインのサポート.....	83
第 9 章	モニタリング・テーブルの変更	85
	変更されたモニタリング・テーブル.....	85
第 10 章	Windows Terminal Server 環境での共有メモリ	87
	Windows Terminal Server 環境で 実行される Adaptive Server 共有メモリ.....	87
第 11 章	Adaptive Server Enhancements Linux プラットフォーム版	89
	ラージ・メモリ・サポート拡張機能.....	89
	DIRECTIO サポート.....	89
	ラージ・メモリ・サポートと POSIX Async I/O.....	89
第 12 章	ストアド・プロシージャ、関数、コマンドの変更	91
	shutdown の新しい構文.....	91
	待ち時間の指定.....	92
	select * 構文の拡張.....	93
	dump database と load database での検証.....	93
	システム・カタログの更新の許可.....	94
	数値データ型のモジュロ算術.....	94
	IPv6 IP アドレス要件をサポートする新しい関数.....	94
	外部トランザクションを復号化する関数.....	95
	xa_bqual.....	95
	xa_gtrid.....	97
索引	99

はじめに

対象読者

このマニュアルは、Adaptive Server® バージョン 12.5.4 を使用している Sybase® システム管理者およびデータベース所有者を対象としています。このバージョンの Adaptive Server に含まれる新しい機能について説明します。

このマニュアルの内容

このマニュアルの内容は、次のとおりです。

- 「[第 1 章 概要](#)」では、Adaptive Server 12.5.4 の概要について説明し、使用できる機能についてまとめています。
- 「[第 2 章 セキュリティの機能強化](#)」では、Adaptive Server バージョン 12.5.4 のセキュリティの機能強化について説明します。強化された機能には、LDAP、Kerberos、SSL、複雑なパスワードなどがあります。
- 「[第 3 章 アーカイブ・データベースへのアクセス](#)」では、アーカイブ・データベースの新しいアクセス機能について説明します。アーカイブ・データベースのアクセス機能によりデータベース管理者は、データベース・ダンプからデータを検証したり選択的にリカバリしたりできます。
- 「[第 4 章 共有ディレクトリの変更](#)」では、ディレクトリ構造の変更について説明します。
- 「[第 5 章 Sybase によるドライバのサポート](#)」では、新しいネイティブ・ドライバ・サポートについて説明します。
- 「[第 6 章 TIBCO ライブラリの動的ロード](#)」では、サポートする TIBCO ライブラリの新情報を示します。
- 「[第 7 章 JRE のサポート](#)」では、JRE の最新バージョンのサポートについて説明します。
- 「[第 8 章 Adaptive Server プラグインの変更](#)」では、アーカイブ・データベース・アクセスおよび複雑なパスワードをサポートする Adaptive Server プラグインの変更点について説明します。
- 「[第 9 章 モニタリング・テーブルの変更](#)」では、モニタリング・テーブルの変更点について説明します。
- 「[第 10 章 Windows Terminal Server 環境での共有メモリ](#)」では、Windows Terminal Server 環境で共有メモリを使用する方法について説明します。
- 「[第 12 章 ストアド・プロシージャ、関数、コマンドの変更](#)」では、Adaptive Server バージョン 12.5.4 の追加変更点について説明します。

Sybase Adaptive Server Enterprise には次のマニュアルが用意されています。

- 使用しているプラットフォームの『リリース・ノート』 - マニュアルには記載できなかった最新の情報が記載されています。
『リリース・ノート』の最新版（英語版）にはインターネットからアクセスできます。この製品の CD-ROM がリリースされたあとに追加された重要な製品情報やマニュアル情報を確認する場合は、Sybase Technical Library を参照してください。
- 使用しているプラットフォームの『インストール・ガイド』 - すべての Adaptive Server および関連する Sybase 製品のインストール、アップグレード、設定の手順について説明しています。
- 旧 12.5.x リリースの新機能ガイド
 - 『Adaptive Server Enterprise 新機能ガイド』 - Adaptive Server バージョン 12.5.1 の新しい機能について説明しています。また、新しい機能をサポートするためのシステム変更や、既存のアプリケーションに影響する変更についても説明しています。
 - 『Adaptive Server Enterprise 12.5.2 新機能ガイド』 - Adaptive Server バージョン 12.5.2 の新しい機能と、それらの機能をサポートするために追加されたシステム変更について説明しています。
 - 『Adaptive Server Enterprise 12.5.3 新機能ガイド』 - Adaptive Server バージョン 12.5.3 の新しい機能と、それらの機能をサポートするために追加されたシステム変更について説明しています。
 - 『Adaptive Server Enterprise 12.5.3a 新機能ガイド』 - Adaptive Server バージョン 12.5.3a の新しい機能と、それらの機能をサポートするために追加されたシステム変更について説明しています。
- 『ASE Replicator ユーザーズ・ガイド』 - プライマリ・サーバから 1 つ以上のリモート Adaptive Server に対して基本的な複製を実行するための ASE Replicator 機能の使用方法について説明しています。
- 『コンポーネント統合サービス・ユーザーズ・ガイド』 - リモートの Sybase データベースおよび Sybase 以外のデータベースへ接続するための Adaptive Server コンポーネント統合サービス機能について説明しています。
- 使用しているプラットフォームの『Adaptive Server Enterprise 設定ガイド』 - Adaptive Server の特定の設定作業を行う方法について説明しています。
- 『EJB Server ユーザーズ・ガイド』 - EJB Server を使用して Adaptive Server で Enterprise JavaBeans を展開、実行する方法について説明しています。
- 『トラブルシューティング&エラー・メッセージ・ガイド』 - 発生頻度の高いエラー・メッセージとシステムの問題について、解決方法を説明しています。

- 『Enhanced Full-Text Search Specialty Data Store ユーザーズ・ガイド』 – Verity で全文検索機能を使用して Adaptive Server Enterprise のデータを検索する方法について説明しています。
- 『用語解説』 – Adaptive Server マニュアルで使用されている技術用語について説明しています。
- 『Historical Server ユーザーズ・ガイド』 – Historical Server を使用して、SQL Server® と Adaptive Server のパフォーマンス情報を入手する方法について説明しています。
- 『Adaptive Server Enterprise における Java』 – Adaptive Server データベースで Java クラスをデータ型、関数、ストアド・プロシージャとしてインストールして使用する方法について説明しています。
- 『Job Scheduler ユーザーズ・ガイド』 – コマンド・ラインまたはグラフィカル・ユーザ・インタフェース (GUI) を使用して、ローカルまたはリモートの Adaptive Server でジョブをインストールして設定する方法、および作成してスケジュールする方法について説明しています。
- 『Monitor Client Library プログラマーズ・ガイド』 – Adaptive Server のパフォーマンス・データにアクセスする Monitor Client Library アプリケーションの記述方法について説明しています。
- 『Monitor Server ユーザーズ・ガイド』 – Monitor Server を使用して、SQL Server と Adaptive Server のパフォーマンス統計を取得する方法について説明しています。
- 『パフォーマンス&チューニング・ガイド』 – Adaptive Server で最高のパフォーマンスを実現するためのチューニング方法について説明しています。このマニュアルは以下の 4 冊に分かれています。
 - 『基本』 – Adaptive Server のパフォーマンスに関する問題の理解と調査の基本について説明しています。
 - 『ロック』 – さまざまなロック・スキームを使用して Adaptive Server のパフォーマンスを向上させる方法について説明しています。
 - 『オプティマイザと抽象プラン』 – オプティマイザがクエリを処理する方法と抽象プランを使用してオプティマイザのプランの一部を変更する方法について説明しています。
 - 『モニタリングと分析』 – パフォーマンスのモニタリングと最適化のために、統計を取得し、使用する方法について説明しています。
- 『クイック・リファレンス・ガイド』 – コマンド、関数、システム・プロシージャ、拡張システム・プロシージャ、データ型、ユーティリティの名前と構文の包括的な一覧表を記載したポケット版のマニュアルです。

-
- 『ASE リファレンス・マニュアル』－ 詳細な Transact-SQL® 情報を記載しています。このマニュアルは以下の 4 冊に分かれています。
 - 『ビルディング・ブロック』－ Transact-SQL のデータ型、関数、グローバル変数、式、識別子とワイルドカード、予約語。
 - 『コマンド』－ Transact-SQL のコマンド。
 - 『プロシージャ』－ Transact-SQL のシステム・プロシージャ、カタログ・ストアド・プロシージャ、システム拡張ストアド・プロシージャ、**dbcc** ストアド・プロシージャ。
 - 『テーブル』－ Transact-SQL のシステム・テーブルと **dbcc** テーブル。
 - 『システム管理ガイド』－ サーバとデータベースを管理するための高度な情報について説明しています。このマニュアルでは、物理的なリソース、セキュリティ、ユーザ・データベース、システム・データベースの管理方法、および文字セットの変換、言語の国際化、ソート順の指定方法についての手順とガイドラインを説明しています。
 - 『システム・テーブル・ダイアグラム』－ システム・テーブルと、そのエンティティとの関係をポスター形式で図解しています。印刷版のみが用意されています。
 - 『Transact-SQL ユーザーズ・ガイド』－ リレーショナル・データベース言語の拡張版である Sybase の Transact-SQL について説明しています。このマニュアルでは、データベース管理システムの操作に慣れていない方のために、テキストブック形式で説明しています。また、**pubs2** と **pubs3** サンプル・データベースについても説明しています。
 - 『Adaptive Server 分散トランザクション管理機能の使用』－ 分散トランザクション処理環境での Adaptive Server DTM 機能の設定、使用、トラブルシューティングについて説明しています。
 - 『高可用性システムにおける Sybase フェールオーバーの使用』－ Sybase のフェールオーバー機能を使用して、Adaptive Server を高可用性システムのコンパニオン・サーバとして設定する方法について説明しています。
 - 『ASE ユーティリティ・ガイド』－ オペレーティング・システム・レベルで実行される **isql** および **bcp** などの、Adaptive Server のユーティリティ・プログラムについて説明しています。
 - 『Web Services ユーザーズ・ガイド』－ Adaptive Server 用の Web Services の設定、使用、トラブルシューティングについて説明しています。
 - 『XA インタフェース統合ガイド for CICS, Encina, TUXEDO』－ X/Open XA トランザクション・マネージャを備えた Sybase の DTM XA インタフェースを使用する方法について説明しています。

- 『Adaptive Server Enterprise における XML Services』 – データベースに XML 機能を導入する、Sybase ネイティブの XML プロセッサと Sybase Java ベースの XML のサポートについて、また XML サービスに準拠したクエリとマッピング用の関数について説明しています。

その他の情報

Sybase Getting Started CD、Sybase Technical Library CD、Technical Library Product Manuals Web サイトを利用すると、製品について詳しく知ることができます。

- Getting Started CD には、PDF 形式のリリース・ノートとインストール・ガイド、および Technical Library CD に含まれていないその他のマニュアルや更新情報が収められています。この CD は製品のソフトウェアと同梱されています。Getting Started CD に収録されているマニュアルを参照または印刷するには、Adobe Acrobat Reader が必要です (CD 内のリンクを使用して Adobe の Web サイトから無料でダウンロードできます)。
- Technical Library CD には、製品マニュアルが収録されています。この CD は製品のソフトウェアと同梱されています。DynaText リーダー (Technical Library CD に収録) を使用すると、この製品に関する技術情報に簡単にアクセスできます。

Technical Library のインストールと起動の方法については、マニュアル・パッケージに含まれている『Technical Library Installation Guide』を参照してください。

- Technical Library Product Manuals Web サイトは、Technical Library CD の HTML バージョンで、標準の Web ブラウザを使ってアクセスできます。また、製品マニュアルのほか、EBFs/Updates、Technical Documents、Case Management、Solved Cases、ニュース・グループ、Sybase Developer Network へのリンクもあります。

Technical Library Product Manuals Web サイトにアクセスするには、Product Manuals (<http://www.sybase.com/support/manuals/>) にアクセスしてください。

Web 上の Sybase 製品の動作確認情報

Sybase Web サイトの技術的な資料は頻繁に更新されます。

❖ 製品動作確認の最新情報にアクセスする

- Web ブラウザで Technical Documents を指定します。
(<http://www.sybase.com/support/techdocs/>)
- [Certification Report] をクリックします。
- [Certification Report] フィルタで製品、プラットフォーム、時間枠を指定して [Go] をクリックします。
- [Certification Report] のタイトルをクリックして、レポートを表示します。

❖ **コンポーネント認定の最新情報にアクセスする**

- 1 Web ブラウザで Availability and Certification Reports を指定します。
(<http://certification.sybase.com/>)
- 2 [Search By Base Product] で製品ファミリとベース製品を選択するか、[Search by Platform] でプラットフォームとベース製品を選択します。
- 3 [Search] をクリックして、入手状況と認定レポートを表示します。

❖ **Sybase Web サイト (サポート・ページを含む) の自分専用のビューを作成する**

MySybase プロファイルを設定します。MySybase は無料サービスです。このサービスを使用すると、Sybase Web ページの表示方法を自分専用カスタマイズできます。

- 1 Web ブラウザで Technical Documents を指定します。
(<http://www.sybase.com/support/techdocs/>)
- 2 [MySybase] をクリックし、MySybase プロファイルを作成します。

Sybase EBF とソフトウェア・メンテナンス

❖ **EBF とソフトウェア・メンテナンスの最新情報にアクセスする**

- 1 Web ブラウザで Sybase Support Page (<http://www.sybase.com/support>) を指定します。
- 2 [EBFs/Maintenance] を選択します。MySybase のユーザ名とパスワードを入力します。
- 3 製品を選択します。
- 4 時間枠を指定して [Go] をクリックします。EBF/Maintenance リリースの一覧が表示されます。

鍵のアイコンは、「Technical Support Contact」として登録されていないため、一部の EBF/Maintenance リリースをダウンロードする権限がないことを示しています。未登録ではあるが、Sybase 担当者またはサポート・コンタクトから有効な情報を得ている場合は、[Edit Roles] をクリックして、「Technical Support Contact」役割を MySybase プロファイルに追加します。

- 5 EBF/Maintenance レポートを表示するには [Info] アイコンをクリックします。ソフトウェアをダウンロードするには製品の説明をクリックします。

不明な点があるときは

Sybase ソフトウェアがインストールされているサイトには、Sybase 製品の保守契約を結んでいるサポート・センタとの連絡担当の方 (コンタクト・パーソン) を決めてあります。マニュアルだけでは解決できない問題があった場合には、担当の方を通して Sybase のサポート・センタまでご連絡ください。

概要

この章には、Adaptive Server バージョン 12.5.4、12.5.3a、12.5.3、12.5.2 で導入された新機能のサマリ情報と、機能とプラットフォームの互換性の一覧が記載されています。

トピック名	ページ
機能とプラットフォームの互換性に関する情報	1
新機能の概要	3

機能とプラットフォームの互換性に関する情報

表 1-1 は、Adaptive Server 12.5.4 でサポートされるオペレーティング・システムで使用できる機能を示しています。

表 1-1: サポートされるオペレーティング・システムでの Adaptive Server の機能

Adaptive Server のオプション	Solaris 32 ビット	Solaris 64 ビット	Solaris x86	Sol Opeteron 64 ビット	HP-UX PA Risc 64 ビット	HP-UX PA Risc 32 ビット	HP Tru64	HP-UX Itanium 64 ビット	IBM AIX 32 ビット	IBM AIX 64 ビット	Windows x86	Macintosh OS X	SGI 32 ビット	SGI 64 ビット	Linux on pSeries	Linux Opteron 64 ビット	Linux Itanium 64 ビット	Linux x86 32 ビット
暗号化カラム	f	f	-	-	f	f	-	-	-	f	f	-	-	-	-	-	-	f
高可用性	Y	Y	-	-	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	-	-	-	Y
DTM (分散トランザクション管理)	Y	Y	-	Y	Y	Y	-	-	Y	Y	Y	-	Y	Y	-	Y	-	Y
XML 管理	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	Y	Y
Java オプション	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y
ネイティブ XML	Y	Y	-	Y	Y	Y	-	§	-	Y	Y	-	-	-	-	§	ž	Y
Java ベースの XML	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	-	Y	Y
Web Services	Y	Y	-	-	Y	Y	-	Y	Y	Y	Y	-	Y	Y	-	-	Y	Y
セキュリティおよびディレクトリ・サービス	Y	Y	-	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y
LDAP サーバ・ディレクトリ	Y	Y	-	Y	Y	Y	Y	Y	Y	f	Y	-	Y	-	-	-	ž	Y
LDAP ユーザ認証	Y	Y	-	-	Y	Y	Y	-	Y	f	Y	-	-	-	-	-	-	Y

凡例：Y - Adaptive Server 12.5.x でサポート。f - 12.5.3a で導入済み。ž - 12.5.4 で導入済み。§ - 12.5.3 ESD5 で導入済み。P - ポートがマージされた。- - サポートなし。

Adaptive Server のオプション	Solaris 32 ビット	Solaris 64 ビット	Solaris x86	Sol Opeteron 64 ビット	HP-UX PA Risc 64 ビット	HP-UX PA Risc 32 ビット	HP Tru64	HP-UX Itanium 64 ビット	IBM AIX 32 ビット	IBM AIX 64 ビット	Windows x86	Macintosh OS X	SGI 32 ビット	SGI 64 ビット	Linux on pSeries	Linux Opeteron 64 ビット	Linux Itanium 64 ビット	Linux x86 32 ビット	
(SSLSecure Sockets Layer)	Y	Y	-	Y	Y	Y	Y	§	Y	Y	Y	-	-	-	-	-	-	Y	
Cybersafe Kerberos	Y	Y	-	-	-	-	-	-	Y	-	Y	-	-	-	-	-	-	-	
MIT Kerberos	Y	Y	-	Y	f	-	-	§	f	f	-	-	-	-	-	Y	-	Y	
プラットフォーム・ネイティブ Kerberos	Y	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
詳細なアクセス制御	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	
PAM (Pluggable Authentication Module)	Y	Y	-	Y	-	-	-	§	-	f	-	Y	-	-	-	Y	Y	Y	
コンテンツ管理 (外部ファイルのサポート)	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	-	Y	Y	Y	
モニタ・クライアント GUI	-	-	-	-	-	-	-	-	-	-	Y	-	-	-	-	-	-	-	
拡張型全文検索 (EFTS)	Y	Y	-	-	Y	Y	Y	-	Y	Y	Y	-	-	-	-	-	-	Y	
リアルタイム・メッセージング	Y	Y	-	-	-	Y	-	-	-	Y	Y	-	-	-	-	-	-	Y	
JMS のサポート	Y	Y	-	-	-	Y	-	-	Y	Y	Y	-	-	-	-	-	-	Y	
WebSphere MQ サポート	f	f	-	-	-	f	-	-	-	f	Y	-	-	-	-	-	-	f	
障害時のリカバリ	Y	-	-	-	Y	-	Y	Y	Y	-	Y	-	Y	-	-	-	-	Y	
基本の Adaptive Server に含まれる機能																			
複雑なパスワード	§	§	§	§	§	§	§	§	§	§	§	§	§	§	§	§	§	§	§
アーカイブ・データベースへのアクセス	§	§	§	§	§	§	§	§	§	§	§	§	§	§	§	§	§	§	§
IPv6	Y	Y	-	-	f	f	-	-	-	-	f	-	-	-	-	-	-	-	
XA ライブラリ	-	-	-	Y	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
異なるプラットフォーム間のダンプとロード	Y	Y	-	Y	Y	Y	-	Y	Y	Y	Y	Y	Y	Y	-	-	Y	Y	
Job Scheduler	Y	Y	-	P	Y	Y	-	-	Y	Y	Y	Y	Y	Y	-	-	-	Y	
ASE Replicator	Y	Y	-	-	Y	Y	-	-	Y	Y	Y	Y	-	-	-	-	-	Y	

凡例：Y - Adaptive Server 12.5.x でサポート。f - 12.5.3a で導入済み。§ - 12.5.4 で導入済み。§ - 12.5.3 ESD5 で導入済み。P - ポートがマージされた。-- サポートなし。

新機能の概要

表 1-2 には、Adaptive Server 12.5.2、12.5.3、12.5.3a、12.5.4 の主な機能が示されています。これらの機能の詳細については、該当するリリースの新機能に関する資料を参照してください。

表 1-2: Adaptive Server Enterprise のバージョンと新しい機能の比較

Adaptive Server の機能	説明
Adaptive Server バージョン 12.5.4	
<i>Kerberos</i> の機能強化	<p>次の Kerberos 機能が強化されました。</p> <ul style="list-style-type: none"> Adaptive Server 名とは異なる Kerberos プリンシパル名を指定する新しいオプション。 Kerberos をサポートするプラットフォームの拡張。 sp_modifylogin の authenticate with オプションを使用して、個別のログインで Kerberos 認証を必要とするようにする。 sybmapname は、外部のユーザ・プリンシパル名を Adaptive Server ログインのネーム・スペースに変換する、カスタマイズ可能なユーティリティ。
LDAP ユーザ認証の強化	<p>次の LDAP ユーザ認証の機能が強化されました。</p> <ul style="list-style-type: none"> プライマリ LDAP サーバに対する認証からセカンダリ LDAP サーバへの自動フェールオーバー。 Adaptive Server は、LDAP サーバとの通信時に発生したエラーからリカバリする。 LDAP サーバから Adaptive Server クライアントに渡されるパスワード有効期限に関するメッセージの強化。
複雑なパスワードの強化	<p>複雑なパスワードの属性を幅広く指定できるようになりました。独自のストアド・プロシージャを作成して、サイト特有のパスワード複雑性チェックを行うこともできます。</p>
アーカイブ・データベースへのアクセスのサポート	<p>データベース・ダンプを従来の読み取り専用データベースと同様に扱えることにより、データベース管理者はアーカイブ・データベースにアクセスして、データベース・ダンプのデータ検証やデータの選択的なりカバリを行えます。</p>
共有ディレクトリの変更	<p>Adaptive Server バージョン 12.5.4 では、共有ディレクトリ構造に多くの変更があります。</p>
<i>Sybase</i> によるドライバのサポート	<p>次の Adaptive Server データ・プロバイダが含まれています。</p> <ul style="list-style-type: none"> ASE ADO.NET データ・プロバイダ 1.1 Sybase 12.5.1 で提供される ASE OLE DB プロバイダ Sybase 12.5.1 で提供される ASE ODBC ドライバ
<i>TIBCO</i> ライブラリの動的ロード	<p>TIBCO JMS は、Adaptive Server の実行プログラムに静的にリンクされるのではなく、動的にロードされるようになりました。</p>
<i>JRE</i> のサポート	<p>Adaptive Server バージョン 12.5.4 には、JRE 1.4 が含まれます。</p>
Adaptive Server プラグインの変更	<p>Adaptive Server プラグインは、アーカイブ・データベースへのアクセスと複雑なパスワードをサポートします。</p>
システム・カタログの更新	<p>サーバ全体のコマンド allow updates to system catalogs は、allow updates ストアド・プロシージャ設定よりも優先されます。</p>

Adaptive Server の機能	説明
モニタリング・テーブルの変更	モニタリング・テーブル <code>monSysStatement</code> と <code>monProcessStatement</code> が変更されました。
<code>syscomments</code> の変更	ストアド・プロシージャまたはトリガのソース・テキストがシステム・テーブル <code>syscomments</code> に格納される場合、 <code>select *</code> を使用するクエリは、 <code>select *</code> で参照されるカラム・リストを拡張する <code>syscomments</code> に格納されます。
Windows Terminal Server 環境での共有メモリ・サポート	Windows Terminal Server の共有メモリ要件に対応するために、Adaptive Server バージョン 12.5.4 では新しい環境変数 <code>SYBASE_TS_MODE</code> を導入しました。
グローバル・ログイン・トリガ	Adaptive Server バージョン 12.5.4 では、各ユーザ・ログインで実行される新しいグローバル・ログイン・トリガを設定できます。
ログイン・トリガからの <code>set</code> オプションのエクスポート	Adaptive Server バージョン 12.5.4 では、ログイン・トリガ内の <code>set</code> オプションをユーザ・セッション全体で有効にできます。
Adaptive Server バージョン 12.5.3a	
暗号化カラムのサポート	Adaptive Server では、データをカラム・レベルで暗号化できます。認証とアクセス制御のメカニズムにより、正しく識別され、正しい権限を持つユーザのみがデータにアクセスできます。Adaptive Server の暗号化カラム機能は、中間層やクライアント・アプリケーションでの暗号化よりも使いやすくなっています。暗号化カラムのサポートを有効にする場合、アプリケーションの変更は不要です。
Adaptive Server バージョン 12.5.3	
SSL (Secure Sockets Layer) の強化	ネットワーク通信の暗号化用の Advanced Encryption Standard (AES : FIPS-197 で定義済み) をサポートする新しい SSL CipherSuites。Advanced Encryption Standards を使用すると、暗号化キーとして 128 ビットと 256 ビットのどちらを使用するかを選択できます。
異なるプラットフォーム間のデータベースのダンプとロードのサポート	Adaptive Server では、エンディアン・アーキテクチャの異なるプラットフォーム間でもデータベースのダンプおよびロードを行えます。 <code>dump database</code> と <code>load database</code> をビッグ・エンディアン・プラットフォームからリトル・エンディアン・プラットフォームに対して (またはリトル・エンディアン・プラットフォームからビッグ・エンディアン・プラットフォームに対して) 実行できます。
プロキシ・テーブルに関する統計のインポート	<code>update statistics</code> をリモート・サーバのプロキシ・テーブルに対して実行すると、関連するテーブルとインデックスの統計情報が利用可能な場合、そのテーブル・カタログがローカルの <code>sysabstats</code> と <code>sysstatistics</code> にインポートされます。
<code>top-N</code> 機能のサポート	<code>top n</code> 句を使用して、結果セットのローの最大数を整数で指定されたロー数に制限します。Adaptive Server Enterprise は、 <code>top n</code> 句を外部クエリの <code>select</code> 文ではサポートしていますが、サブクエリの <code>select</code> リストの中ではサポートしていません。
Historical Server の機能強化	Adaptive Server では、モニタリング・データを Historical Server から特定の Adaptive Server 上のデータベースへ送信することができます。
RTDS (Real Time Data Services) の機能強化	<code>sp_configure</code> を使用して、ネイティブ・スレッドの数とメッセージ送信の待ち時間を設定します。

Adaptive Server の機能	説明
<i>Resource Governor</i>	クエリやトランザクションによるサーバのリソース独占を防ぐために、システム管理者は Adaptive Server のリソース制限機能を使用できます。Adaptive Server バージョン 12.5.3 では、システム管理者がリソース制限を変更すると、そのセッションにログインしているすべてのユーザに変更が反映されます。
分割された <i>DOL</i> テーブルのページ割り付け	Adaptive Server バージョン 12.5.3 は、ターゲットのアロケーション・テーブル内の現在割り付けられているエクステントを、それらのエクステントが他のパーティションに割り当てられても無駄な領域が生じないように、一杯まで使おうとします。
ユーザ接続の強化	ユーザ接続の強化には、エラー・メッセージの更新と、ソケットの予約に関する修正があります。
<i>ddlValidation</i>	<i>ddlValidate</i> オプションには、 no 、 yes 、 strict の3つのパラメータが追加されました。
<i>sybmigrate</i> の強化	<i>sybmigrate</i> は、Adaptive Server Enterprise のバージョン間のマイグレーションをサポートするツールです。バージョン 12.0 ~ 12.5.3 のソース・サーバに対応しています。
新しい <i>EFTS (Enhanced Full-Text Search Specialty Data Store)</i> の言語サポート	EFTS では新たに次の言語がサポートされます。 <ul style="list-style-type: none"> 繁体字中国語 (Windows および Solaris プラットフォーム) アラビア語、ヘブライ語、タイ語、ロシア語 (Linux プラットフォーム)
モニタ・カウンタと <i>sp_sysmon</i>	Adaptive Server バージョン 12.5.3 では、特によく使われるモニタリング・ツールの機能が強化されました。
Adaptive Server バージョン 12.5.2	
<i>Pluggable Authentication Module (PAM)</i> のサポート	Pluggable Authentication Module (PAM) のサポートにより、認証を必要とするアプリケーションを変更せずに、複数の認証サービス・モジュールをまとめて使用できます。
<i>Kerberos</i> ネイティブ・ライブラリのサポート	Adaptive Server では、次の Kerberos ネイティブ・ライブラリがサポートされます。 <ul style="list-style-type: none"> Cybersafe Library のサポート MIT Kerberos ライブラリのサポート ユーザ認証の Active Directory 相互運用性 jConnect での Kerberos サポート
パスワードで保護されたバックアップのサポート	<i>dump database</i> コマンドの <i>password</i> パラメータを使用すると、データベース・ダンプが承認なしにロードされないように保護できます。データベース・ダンプの作成時に <i>password</i> パラメータを指定した場合には、データベースのロード時にもこのパスワードを指定する必要があります。
アクセス制御の強化	次のアクセス制御が強化されました。 <ul style="list-style-type: none"> システム・カタログに対するパーミッションの制限 <i>set proxy</i> の細分性の向上 管理コマンドの付与と取り消し
<i>FIPS-140</i> 認定アルゴリズムのサポート	SSL は、クレジット・カード番号、株式売買、銀行取引などの機密情報を、インターネット上で安全に転送するための標準です。パブリック・キー暗号法に依存します。

Adaptive Server の機能	説明
ステートメント・キャッシュの強化	ステートメント・キャッシュは、キャッシュされた SQL 文を保存するために使用されます。
XML サービスのサポート	<p>XML サービスでは、主に次の 4 つの領域が強化されています。</p> <ul style="list-style-type: none"> • <code>xmlextract</code> 組み込み関数と <code>xmltest</code> 述部に対する XML 問い合わせ言語の拡張 • <code>select</code> 文の <code>for xml</code> 句でサポートされるデータ型の強化 • <code>xmlextract</code>、<code>xmlparse</code>、<code>xmlrepresentation</code> でサポートされるデータ型の強化 • Java-XML サンプル・コードの強化
<i>Real Time Messaging Services</i>	Adaptive Server 12.5.2 には、Real Time Data Services (RTDS) オプション・パッケージによるメッセージング機能が含まれています。このオプションによって、メッセージング・システムおよびデータベースとの対話を行うアプリケーションの開発が簡単になります。
Web サービスのサポート	Web サービスは、ネットワーク接続でアクセスできる独立したモジュール・アプリケーションです。Web サービスを使用することで、パフォーマンスと引き換えに相互運用性が向上します。
IPv6 のサポート	Adaptive Server は、IPv6 (Internet Protocol version 6) をサポートします。
拡張型全文検索 (EFTS) の強化	<p>EFTS の次の点が強化されました。</p> <ul style="list-style-type: none"> • インストールとディレクトリの変更 • 停止を行うためのパーミッション • 最大 16000 バイトをサポートする <code>index_any</code> 句 • 新しい疑似カラム <code>total_docs</code> • プライマリ・キー
圧縮データベース・ダンプのサポート	Adaptive Server バージョン 12.5.2 の <code>dump</code> には、データベース・ダンプを圧縮するための <code>compression</code> パラメータが含まれています。
パスワードで保護されたデータベースのダンプとロード	Adaptive Server 12.5.2 の <code>dump</code> と <code>load database</code> には、データベース・ダンプをパスワードで保護するための <code>password</code> パラメータが含まれています。
<i>Veritas 2.1</i> のフェールオーバーのサポート	Linux プラットフォーム上の Adaptive Server に Veritas 2.1 のフェールオーバーを設定できるようになりました。
ラージ・メモリ・サポート	32 ビット版 Enterprise Linux オペレーティング・システムでの Adaptive Server のラージ・メモリ・サポートによって、Adaptive Server で使用できるメモリ容量が 2.7GB から最大 64GB に増えました。Adaptive Server で使用できるメモリ容量の増加により、サーバがディスクにアクセスする回数が大幅に減少し、パフォーマンスが向上します。

トピック名	ページ
Kerberos の変更	7
LDAP ユーザ認証の強化	17
SSL サポート	32
PAM のサポート	33
暗号化カラムの更新	33
複雑なパスワードとログインのオプション	35
ログイン・トリガからの set オプションのエクスポート	50
グローバル・ログイン・トリガの設定	51

Kerberos の変更

Kerberos は以下のように拡張されました。

- Kerberos 認証用のサーバ・プリンシパル名の指定が可能。
- `sp_modifylogin` および `sp_addlogin authenticate with` オプションを使用した Kerberos 認証のサポート。
- `sybmapname` のサポート。
- MIT Kerberos クライアント・ライブラリのサポート。
- Kerberos をサポートするプラットフォームの拡張。

Kerberos 認証用の Adaptive Server プリンシパル名の指定

プリンシパル名は、KDC (Kerberos Key Distribution Center) で認証するときにサーバが使用する名前です。複数の Adaptive Server インスタンスを実行中の場合は、Adaptive Server ごとに異なるプリンシパル名を使用する必要があります。

Adaptive Server バージョン 12.5.4 では、新しいデータ・サーバ・オプションと新しい環境変数を使用して、Adaptive Server 名とは異なるプリンシパル名を指定できます。Adaptive Server 名は、環境変数 `DSLISTEN` および `DSQUERY`、またはデータサーバ・コマンド・ライン・オプションの `"-s servername"` で指定されます。

SYBASE_PRINCIPAL を使用した Adaptive Server プリンシパル名の指定

デフォルトのプリンシパル名は Adaptive Server の名前です。別の名前を指定するには、Adaptive Server を起動して Kerberos を使用する前に、SYBASE_PRINCIPAL を次のように設定します。

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

Adaptive Server のプリンシパル名を設定すると、Adaptive Server はこの変数の値を使用して自身を Kerberos で認証します。

-k データ・サーバ・オプションを使用した Adaptive Server プリンシパル名の指定

次のコマンド・ライン・オプションを使用して、Adaptive Server の起動時に Adaptive Server プリンシパル名を指定できます。

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

注意 -k で Adaptive Server のプリンシパル名を指定すると、Adaptive Server は環境変数を確認しません。

-k および SYBASE_PRINCIPAL を使用した Adaptive Server プリンシパル名の設定

Adaptive Server が Kerberos セキュリティ・メカニズムを有効にして起動されている場合、Adaptive Server では最初に Kerberos 認証の -k オプションで指定されているプリンシパル名が使用されます。-k オプションが指定されていない場合、Adaptive Server は環境変数 SYBASE_PRINCIPAL でプリンシパル名を確認します。どちらも指定されていない場合、Adaptive Server は認証にサーバ名を使用します。

次の例では、Adaptive Server 名を "ase1254"、現在のレルム名を "MYREALM.COM" とします。Adaptive Server 名は、コマンド・ラインで -s パラメータを使用してデータ・サーバに対して指定されます。現在のレルムは、secbase 属性値により *libtcl.cfg* で指定されます。

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

デフォルトの Adaptive Server プリンシパル名は "ase1254@MYREALM.COM" です。Adaptive Server の *keytab* ファイルで定義されたプリンシパル名が "aseprincipal@MYREALM.COM" の場合、次のオプション 1 または 2 を使用してサーバのプリンシパル名を設定し、デフォルトの Adaptive Server プリンシパル名を上書きできます。

オプション1: '-k' を指定する %

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

Kerberos での認証に使用される Adaptive Server のプリンシパル名は aseprincipal@MYREALM.COM です。

オプション2: '-k' を指定せず、SYBASE_PRINCIPAL を設定する

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

Kerberos での認証に使用される Adaptive Server のプリンシパル名は、`$SYBASE_PRINCIPAL` の値の "aseprincipal@MYREALM.COM" です。

オプション3: '-k' も SYBASE_PRINCIPAL も設定しない %

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

Kerberos での認証に使用される Adaptive Server のプリンシパル名は ase1254@MYREALM.COM です。

Kerberos の詳細については、『システム管理ガイド』第1巻のセキュリティに関するセクションを参照してください。

***sp_modifylogin* および *sp_addlogin authenticate with* オプション**

Adaptive Server バージョン 12.5.4 のログインでは、`sp_modifylogin` または `sp_addlogin` に対して `authenticate with` オプションを設定する場合は、指定された認証メカニズムのみを使用する必要があります。サポートされる認証メカニズムは以下のとおりです。

- ASE
- LDAP
- PAM
- KERBEROS
- ANY

サポートされるこれらのメカニズムで `authenticate with` を使用すると、サーバ全体の設定パラメータ `unified login required`、`enable ldap user auth`、および `enable pam user auth` を上書きできます。

複数の外部認証メカニズムが設定され、ログイン固有の `authenticate with` オプションが設定されていない場合は、次の順序に基づいて外部認証メカニズムが決定されます。

- 1 Kerberos
- 2 LDAP
- 3 PAM

たとえば、PAM および LDAP の両方が設定されている場合は、外部認証として、PAM ではなく LDAP が選択されます。

認証時には、1 つの外部認証メカニズムのみ使用されます。外部認証が失敗した場合、設定パラメータの値によっては、ASE 認証が試行される場合があります。

外部認証メカニズムのいずれも設定しない場合、ASE 認証が使用されます。

authenticate with を使用したサーバ全体の認証オプションの上書き

注意 ログインの `authenticate with` オプションを変更するには、`sso_role` パーミッションが必要です。

Kerberos、LDAP、または PAM などの外部認証メカニズムを設定するには、会社のセキュリティ・ポリシーに合致するサーバ全体の認証設定を決定することをお勧めします。このサーバ全体の設定は、多くのクライアント接続に適しています。次に、`authenticate with` オプションを使用して個々のログインを別の認証メカニズムに設定できます。

`authenticate with` を使用して、外部の認証メカニズムの Kerberos、LDAP、および PAM を指定できます。また、`sp_modifylogin` または `sp_addlogin authenticate with` を使用して認証メカニズムを ASE に設定し、Adaptive Server の内部認証メカニズムのみを使用することもできます。任意の認証メカニズムを許可するには、`authenticate with ANY` を使用します。

注意 ログインの認証メカニズムが `ANY` に設定されている場合、ログインはサーバ全体の設定を使用して認証を制御します。ログインのデフォルトの認証メカニズム設定は `ANY` です。

`sp_modifylogin` では、前の `sp_maplogin` で指定したログイン・マッピングとの競合もチェックされます。詳細については、「[ログイン・マッピングに対する制御の強化](#)」(30 ページ)を参照してください。

例 1：バッチ・アプリケーションを実行するためのローカル・アカウントの作成
集中型ユーザ・アカウント・リポジトリに対して Kerberos を使用し、一般的な数のユーザが Kerberos を使用して認証を行う必要がある環境の場合、Adaptive Server では次のパラメータを設定して Kerberos を設定する必要があります。

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

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

これらの設定パラメータでは、ログイン“sa”以外のすべてのユーザ・ログインが、Adaptive Server にアクセスするために Kerberos を使用して認証を行う必要があります。

次に、Adaptive Server データベース管理者またはオペレータによって実行される夜間のバッチ・オペレーションの例を示します。この場合、Kerberos リポジトリにアカウントが存在しなくてもローカルで認証できます。これは、`sp_modifylogin` または `sp_addlogin` で `authenticate with` オプションを使用して実行されます。

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

例 2 : Adaptive Server 認証から LDAP ユーザ認証へのユーザのマイグレート

この例では、ローカルの ASE 認証から LDAP 認証へクライアントを移動するための段階的なアプローチを示します。LDAP ディレクトリ・サーバは設定されていますが、このサーバにはまだすべてのユーザ・アカウントが移動していません。少数のユーザが、Adaptive Server に対する外部認証として LDAP をテストするパイロット・プログラムに同意しています。

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

この設定では、LDAP ディレクトリ・サーバでの認証が失敗した場合や、LDAP サーバが使用できない場合に、ASE 認証へのフェールオーバーが許可されます。LDAP でのアカウントを持たないユーザは、ASE 認証にフェールオーバーします。パイロット・プログラムのユーザは、LDAP ディレクトリ・サーバに追加されて、LDAP ディレクトリ・サーバを使用して認証を開始できます。

ユーザは、グローバル変数 `@@authmech` を使用して、`authenticate with` に使用する認証メカニズムを決定できます。

```
select @@authmech
```

パイロット・プログラムが進み、LDAP 認証が使用されると、パイロット・プログラムのユーザは、LDAP 認証だけを使用しなければならない場合があります。

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

パイロット・プログラムが完成し、すべてのユーザに対して LDAP 認証が必要になったら、設定パラメータをレベル 2 に変更します。パイロット・プログラム中に **authenticate with LDAP** に設定されたすべてのログインは、デフォルト値の ANY にリセットできます。設定パラメータが 2 に設定されている場合、ログインは LDAP を使用して認証を行う必要があります。

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

注意 ログインの **authenticate with** が LDAP、Kerberos、PAM、または ASE など特定の認証メカニズムに設定されている場合、そのログインでは認証に設定されているメカニズムしか使用できません。サーバ全体の設定に対して例外を設定し、特定の認証メカニズムを強制的に実行するのが最適な利用方法です。

sybmapname を使用したユーザ・プリンシパル名の処理

sybmapname の目的は、Kerberos 環境で使用される外部のユーザ・プリンシパル名を Adaptive Server のユーザ・ログインのネームスペースに変換することです。**sybmapname** は、ユーザがカスタマイズできる共有オブジェクトで、その入力バッファで指定された名前を、その出力バッファの Adaptive Server ログインに適した名前にマップできます。

sybmapname 共有オブジェクトを使用して、ユーザのプリンシパル名と Adaptive Server のログイン名との間のカスタム・マッピングを実行できます。この共有オブジェクトは、オプションでサーバの起動時にロードされ、共有オブジェクトに含まれている関数 **syb__map_name** は、Kerberos 認証が成功した後およびユーザ・プリンシパルが **syslogins** テーブル内のログインにマップされる直前に呼び出されます。これは、ユーザのニーズに合わせてカスタマイズできます。この関数は、マップされるユーザのプリンシパル名とログイン名が同一ではない場合に役に立ちます。

カスタマイズ可能なロジックは、次の関数です。

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

各パラメータの意味は、次のとおりです。

- **NAMEMAPTYPE *protocol** — この関数の使用のために予約されている構造体を表す。
- **char *orig** — Null で終了する入力バッファ。
- **int origlen** — 入力バッファの長さを表す。255 文字以内にする必要がある。

- `char *mapped` – Null で終了しない出力バッファ。
- `int *mappedlen` – 出力バッファの長さ。30 文字以内にする必要がある。

この関数は、マッピングが成功した場合は 0 よりも大きい値を返し、マッピングが実行されなかった場合は 0 の値を返し、`syb_map_name()` でエラーが発生した場合は 0 よりも小さい値を返します。エラーが発生すると、Adaptive Server のエラーログにマッピングの失敗をレポートするメッセージが表示されます。

たとえば、Adaptive Server で Kerberos ユーザを認証するには、まず、Kerberos セキュリティ・メカニズムを使用するように Adaptive Server を設定する必要があります。Kerberos 設定については、Adaptive Server の『システム管理者ガイド』および Open Client/Server のドキュメント、およびホワイトペーパー「Configuring Kerberos for Sybase」(<http://www.sybase.com/detail?id=1029260>) を参照してください。

サンプルの `sybmapname.c` ファイルは、`$SYBASE/$SYBASE_ASE/sample/server/sybmapname.c` にあります。

注意 ファイルを修正する場合は、簡単なエラーのないロジックを使用してロジックを実装します。Adaptive Server を正しく実行できなくなる場合があるため、コーディング時には注意が必要です。「[sybmapname を使用する場合の注意事項](#)」(15 ページ) を参照してください。

提供されている汎用プラットフォーム固有の `makefile` を使用して共有オブジェクトまたは DLL を構築します。`makefile` は、プラットフォーム固有の設定に合わせて変更しなければならない場合があります。

生成された共有オブジェクトは、UNIX マシンでは `$LD_LIBRARY_PATH` で指定したロケーション、Windows マシンでは `PATH` 変数で指定したロケーションに保存されます。ファイルには、'sybase' オペレーティング・システム・ユーザに対する読み取りおよび実行パーミッションが必要です。

注意 'sybase' ユーザにのみ読み取りパーミッションや実行パーミッションを許可し、他のアクセスはすべて拒否することをお勧めします。

Kerberos 認証を使用した Adaptive Server へのログインの確認

Kerberos 認証を使用して Adaptive Server へのログインを確認するには、次のことを前提とします。

- `$$SYBASE` は、リリースおよびインストールディレクトリを参照する。
- `$$SYBASE_ASE` は、サーバ・バイナリを含む Adaptive Server バージョン・ディレクトリを参照する。
- `$$SYBASE_OCS` は、Open Client/Server バージョン・ディレクトリを参照する。

例 1 クライアントのプリンシパル名が `user@REALM` の場合、および `syslogins` テーブルの対応するエントリが `user_REALM` の場合、入力文字列 `user@realm` を受け取って、その入力文字列を出力文字列 `user_REALM` に変換するように `sybmapname` をコード化できます。

例 2 クライアントのプリンシパル名が `user` の場合、および `syslogins` テーブルの対応するエントリが `USER` の場合、入力文字列 `user` を受け取って、この文字列を大文字の文字列 `USER` に変換するように `sybmapname` をコード化できます。

`sybmapname` は、Adaptive Server によって実行時に読み込まれ、そのロジックを使用して必要なマッピングを実行します。

次の操作と出力は、例 2 の `sybmapname` 関数についてより詳しく示しています。`syb__map_name()` に対してカスタマイズされた定義を含む `sybmapname.c` ファイルはコンパイルして、共有オブジェクト (または DLL) としてビルドした後に、適切なパスのロケーションに保存する必要があります。Adaptive Server は、Kerberos のセキュリティ・メカニズムを有効にして起動する必要があります。

TGT を初期化するには、次のように入力します。

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

TGT を一覧表示するには、次のように入力します。

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

“sa” としてログインし、‘johnd’ のユーザ・ログインを確認します。

```
$ $$SYBASE/$$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)
```

Kerberos 認証が成功すると、**sybmapname** ユーティリティを使用して小文字の johnd が大文字の JOHND にマップされ、ユーザ johnd は Adaptive Server にログインできるようになります。

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

sybmapname を使用する場合の注意事項

sybmapname のコーディングを行う場合は、次の点に注意する必要があります。

- サンプルの **sybmapname.c** プログラムで変更を行う場合には注意が必要です。segfault するコード、**exit()** を呼び出すコード、**system calls()** を呼び出すコード、UNIX シグナルを変更したり、ブロック呼び出しを行うコードは避けてください。不適切なコーディングや呼び出しは、現在実行中の Adaptive Server エンジンに妨害する場合があります。

注意 **sybmapname** におけるコード・エラーは、Sybase の責任ではありません。このコードはユーザが所有し、サポートします。

- コードを注意深く作成し、すべてのポインタを使用前にチェックして、システム・コールを回避します。これは、クイック・ネーム・フィルタリング関数にする必要があります。
- 'goto' 文の使用は避けてください。プラットフォームによっては、これらの文によって予期しない悪影響を受ける場合があります。

- 複数のレルムが使用される場合は、ユーザ・プリンシパル名を適切なログイン名に注意深くマップし、レルム情報が反映されるようにします。たとえば、ユーザ・プリンシパル名が userA@REALMONE および userB@REALMTWO の 2 人のユーザが存在するとします。これらのユーザは、userA または userB ではなくログイン名 userA_REALMONE および userB_REALMTWO にそれぞれマップされます。この動作は、異なるレルムに属する 2 人のユーザを区別するためのものです。

MIT Kerberos クライアント・ライブラリのサポート

Adaptive Server は、MIT Kerberos クライアント・ライブラリを使用して MIT クライアント・ライブラリの新しいバージョンで認証およびテストされています。MIT 製品レベルは、UNIX プラットフォームの場合 MIT Kerberos バージョン 1.4.x です。

厳しい条件下で Kerberos を使用する Adaptive Server の信頼性をさらに高めるために、Adaptive Server 12.5.4 リリースでは追加の修正が行われています。

MIT Kerberos をサポートするプラットフォームの拡張

Adaptive Server では、次のプラットフォームで MIT Kerberos をサポートします。

- HP-UX Itanium 64 ビット版

LDAP ユーザ認証の強化

LDAP ユーザ認証の機能が、次の 5 つの点において強化されました。

- セカンダリ・サーバ検索のサポート
- LDAP UA の堅牢性の強化
- LDAP サーバとの通信中にエラーが発生した場合のフェールオーバー
- パスワード有効期限関連の通信の強化
- ログイン・マッピングに対する制御の強化

LDAP ユーザ認証のための Adaptive Server の設定

LDAP ユーザ認証を使用すると、クライアント・アプリケーションは Adaptive Server にユーザ名とパスワードの情報を送信し、`syslogins` ではなく LDAP サーバによる認証を行えるようになります。LDAP サーバを使用する認証では、Adaptive Server またはアプリケーション固有のパスワードではなく、サーバ全体のパスワードを使用できます。LDAP ユーザ認証を使用すると、ユーザの管理を簡素化し、集中管理できます。

LDAP ユーザ認証は、LDAP プロトコル標準のバージョン 3 に準拠したディレクトリ・サーバ (Active Directory、iPlanet、OpenLDAP Directory Server など) で機能します。

LDAP ユーザ認証では 2 つの認証アルゴリズムを使用できます。これらのアルゴリズムでは、ユーザの識別名 (DN) の取得方法がそれぞれ異なります。これらのアルゴリズムでは、次のいずれかを使用します。

- 生成 DN (認証用、Adaptive Server バージョン 12.5.1 以降で使用可能)
- 検索 DN (認証用、Adaptive Server バージョン 12.5.2 以降で使用可能)

LDAP プロトコルで使用されるプライマリ・データ構造は LDAP URL です。

LDAP URL は、LDAP サーバ上のオブジェクトまたは値のセットを指定します。Adaptive Server は、LDAP URL を使用して、ログイン要求の認証に使用する LDAP サーバと検索基準を指定します。

LDAP URL では、次の構文を使用します。

```
ldapurl::=ldap://host:port/node/?attributes?base | one | sub?filter
```

各パラメータの意味は、次のとおりです。

- *host* – LDAP サーバのホスト名。
- *port* – LDAP サーバのポート番号。
- *node* – 検索を開始するオブジェクト階層内でのノードを指定する。
- *attributes* – 結果セットで返す属性のリスト。属性リストは、LDAP サーバによって異なることがある。

- **base | one | sub** – 検索条件を修飾する。**base** は、ベース・ノードの検索を指定する。**one** は、ベース・ノードとその1つ下のレベルのノードの検索を指定する。**sub** は、ベース・ノードとその下位レベルのすべてのノードの検索を指定する。
- **filter** – 認証する属性を指定する。フィルタは、`uid=*` のように簡潔にしたり、`(uid=*)(ou=group)` のように複雑にしたりすることもできる。

生成 DN アルゴリズム

生成 DN アルゴリズムを使用する場合のログインの手順を次に示します。

- 1 Open Client™ は、Adaptive Server のリスナ・ポートに接続します。
- 2 Adaptive Server リスナは、接続を受け付けます。
- 3 Open Client は、内部ログイン・レコードを送信します。
- 4 Adaptive Server は、ログイン・レコードを読み込みます。
- 5 Adaptive Server は、プライマリ URL から生成した DN とログイン・レコードのログイン名を使用して LDAP サーバにバインドします。このとき、ログイン・レコードのパスワードも使用します。
- 6 LDAP サーバは、ユーザを認証し、成功か失敗かを示すメッセージを返します。
- 7 プライマリ URL で検索が指定されている場合、Adaptive Server は LDAP サーバに検索要求を送信します。
- 8 LDAP サーバは、検索結果を返します。
- 9 Adaptive Server は、検索結果に基づいてログインを受け入れるか、または拒否します。

検索 DN アルゴリズム

検索 DN アルゴリズムを使用する場合のログインの手順を次に示します。

- 1 Open Client は、Adaptive Server のリスナ・ポートに接続します。
- 2 Adaptive Server リスナは、接続を受け付けます。
- 3 Open Client は、内部ログイン・レコードを送信します。
- 4 Adaptive Server は、ログイン・レコードを読み込みます。
- 5 Adaptive Server は、ディレクトリ・サーバのアクセス・アカウントを使用して LDAP サーバにバインドします。

- 6 LDAP サーバは、ユーザを認証し、成功か失敗かを示すメッセージを返します。
手順 5 ～ 6 で確立された接続は、次に Adaptive Server が認証を試行して DN 検索への接続を再利用するまで続きます。
- 7 Adaptive Server は、ログイン・レコードのログイン名と DN 検索 URL に基づいて、LDAP サーバに検索要求を送信します。
- 8 LDAP サーバは、検索結果を返します。
- 9 Adaptive Server は、検索結果を読み込み、DN 検索 URL から属性値を取得します。
- 10 Adaptive Server は、取得した属性値を DN として使用し、パスワードを使用して LDAP サーバにバインドします。
- 11 LDAP サーバは、ユーザを認証し、成功か失敗かを示すメッセージを返します。
- 12 プライマリ URL で検索が指定されている場合、Adaptive Server は LDAP サーバに検索要求を送信します。
- 13 LDAP サーバは、検索結果を返します。
- 14 Adaptive Server は、検索結果に基づいてログインを受け入れるか、または拒否します。

上記のいずれかの認証基準が満たされない場合、Adaptive Server は一般的なログインの失敗をレポートします。

プライマリ URL 文字列またはセカンダリ URL 文字列の検索基準を指定しない場合は、手順 12 ～ 13 を省略できます。プライマリ URL 文字列またはセカンダリ URL 文字列で検索基準を指定しない場合は、認証が完了し、手順 11 で返される成功か失敗かを示すメッセージが表示されます。

セカンダリ検索サーバのサポート

Adaptive Server バージョン 12.5.4 では、LDAP サーバによって認証された Adaptive Server クライアントの継続的なサポートを提供します。LDAP サーバで障害が発生したり、計画されたダウンタイムがある場合に、プライマリ LDAP サーバからフェールオーバーするセカンダリ LDAP 検索サーバを指定できるようになりました。

URL セットの状態は、次のステータスを通じて監視されます。

- INITIAL – LDAP ユーザ認証が設定されていないことを示す。
- RESET – Adaptive Server の管理コマンドで URL が入力されていることを示す。
- READY – URL が接続を受け入れる準備ができていることを示す。

- ACTIVE – URL で LDAP ユーザ認証が成功したことを示す。
- FAILED – LDAP サーバへの接続中に問題が発生したことを示す。
- SUSPENDED – URL がメンテナンス・モードになっており、使用されないことを示す。

以下の手順で、フェールオーバーと手動によるフェールバックについて説明します。

- 1 プライマリおよびセカンダリの URL セットが設定されて READY ステータスになります。
- 2 接続が、プライマリ・サーバ・インフラストラクチャを使用して認証されます。
- 3 プライマリ・サーバで障害が発生すると、ステータスが FAILED に変わります。
- 4 セカンダリ・サーバ・インフラストラクチャによる認証が接続で自動的に開始されます。
- 5 LDAP 管理者によってプライマリ・サーバが修復されて、オンラインに戻ります。Adaptive Server 管理者によりプライマリ LDAP サーバのステータスが READY に変更されます。
- 6 新しい接続が、プライマリ・サーバを使用して認証されます。

注意 Adaptive Server がセカンダリ LDAP サーバにフェールオーバーしたら、データベース管理者は、プライマリ LDAP サーバを手動でアクティブにしてから使用する必要があります。

Adaptive Server で LDAP サーバへの接続時にエラーが発生した場合は、認証が 3 回再試行されます。エラーが続く場合、LDAP サーバのステータスは FAILED になります。Adaptive Server で再試行ループが発生する原因となる LDAP エラーについては、「[LDAP ユーザ認証エラーのトラブルシューティング](#)」(25 ページ)を参照してください。

Adaptive Server バージョン 12.5.4 には、セカンダリ検索 LDAP サーバをサポートするための、次の新しい `sp_ldapadmin` オプションが導入されています。

- セカンダリ DN 検索 URL を設定するには、次のように入力します。

```
sp_ldapadmin set_secondary_dn_lookup_url, <URL>
```
- セカンダリ DN 検索 URL の管理アクセス・アカウントを設定するには、次のように入力します。

```
sp_ldapadmin set_secondary_access_acct, <DN>, <パスワード>
```


- 認証のためにプライマリまたはセカンダリ URL の使用をサスペンドするには、次のように入力します。

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

- 認証のためにプライマリまたはセカンダリ URL のセットをアクティブ化するには、次のように入力します。

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

- プライマリおよびセカンダリ LDAP サーバの設定の詳細を表示するには、次のように入力します。

```
sp_ldapadmin list
```

`sp_ldapadmin list` は、`list_access_acct` および `list_urls` からの前回の出力を結合します。プライマリ・サーバとセカンダリ・サーバでは次が出力されます。

- 検索 URL
- 識別名検索 URL
- アクセス・アカウント DN
- アクティブ [True | False]
- ステータス [Ready | Active | Failed | Suspended | Reset]

Adaptive Server バージョン 12.5.4 では、セカンダリ・サーバをサポートするために、`sp_ldapadmin` オプションが次のように変更されています。

- セカンダリ・サーバの DN 検索 URL を表示するには、次のように入力します。

```
sp_ldapadmin list_urls
```

- セカンダリ DN 検索の管理アクセス・アカウントを表示するには、次のように入力します。

```
sp_ldapadmin list_access_acct
```

- 新しいサブコマンドを表示するには、次のように入力します。

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

LDAP サーバのステータスの移行

次の表に、sp_ldapadmin の各コマンドを実行したときの LDAP サーバのステータスの移行を示します。

表 2-1 に、sp_ldapadmin set_URL を実行したときのステータスの移行を示します。ここで set_URL は次のコマンドのいずれかを表します。

- set_dn_lookup_url
- set_primary_url
- set_secondary_dn_lookup_url
- set_secondary_url

表 2-1: sp_ldapadmin set_URL 実行時のステータスの移行

初期状態	最終状態
INITIAL	RESET
RESET	RESET
READY	READY
ACTIVE	RESET
FAILED	RESET
SUSPENDED	RESET

表 2-2 に、sp_ldapadmin suspend を実行したときのステータスの移行を示します。

表 2-2: sp_ldapadmin suspend 実行時のステータスの移行

初期状態	最終状態
INITIAL	エラー
RESET	SUSPENDED
READY	SUSPENDED
ACTIVE	SUSPENDED
FAILED	SUSPENDED
SUSPENDED	SUSPENDED

表 2-3 に、sp_ldapadmin activate を実行したときのステータスの移行を示します。

表 2-3: sp_ldapadmin set activate 実行時のステータスの移行

初期状態	最終状態
INITIAL	エラー
RESET	READY
READY	READY
ACTIVE	ACTIVE
FAILED	READY
SUSPENDED	READY

次の表に、Adaptive Server で暗黙に実行される LDAP サーバのステータスの移行を示します。

表 2-4 に、Adaptive Server を再起動するときのステータスの移行を示します。

表 2-4: Adaptive Server 再起動時のステータスの移行

初期状態	最終状態
INITIAL	INITIAL
RESET	RESET
READY	READY
ACTIVE	READY
FAILED	FAILED
SUSPENDED	SUSPENDED

Adaptive Server は、LDAP サーバが READY または ACTIVE ステータスの場合にのみ LDAP ログインを実行します。表 2-5 にステータスの移行を示します。

表 2-5: LDAP ログイン成功時のステータスの移行

初期状態	最終状態
READY	ACTIVE
ACTIVE	ACTIVE

表 2-6 に LDAP ログインが失敗した場合のステータスの移行を示します。

表 2-6: LDAP ログイン失敗時のステータスの移行

初期状態	最終状態
READY	FAILED
ACTIVE	FAILED

LDAP UA の堅牢性の強化

Adaptive Server バージョン 12.5.4 には、堅牢性を強化するための多くの `sp_ldapadmin` オプションが新たに導入されています。

エンジンあたりの最大 `ldapua` ネイティブ・スレッド数

`set_max_ldapua_native_threads` では、LDAP 認証要求を処理するエンジンで同時に実行できるネイティブ・スレッドの最大数を設定します。

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

`set_max_ldapua_native_threads` の最小値は 1 です。最大値は、`max native threads` の値から、`sp_configure` を使用して指定した `number of dump threads` の値を差し引いた値です。デフォルト値は、最大値と同じです。

`sp_configure` は、最大ネイティブ・スレッド数が、`set_max_ldapua_native_threads` および設定パラメータ `number of dump threads` の値に対して十分であるか確認します。

LDAP 要求のタイムアウト `set_timeout` では、認証要求が放棄されるまで Adaptive Server が LDAP サーバからの応答を待機する時間をミリ秒単位で設定します。

このオプションは、次のように入力して設定できます。

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

`set_timeout` のデフォルト値は、10,000 ミリ秒 (10 秒) です。有効な値は、1 ~ 3,600,000 (1 時間) です。

満杯の場合は LDAP 認証を放棄する `set_abandon_ldapua_when_full` では、エンジンあたりの最大ネイティブ・スレッド数を超えた場合の LDAP ユーザ認証の代替方法を設定できます。

`set_abandon_ldapua_when_full` が `true` に設定されている状態で、使用可能なスレッドがない場合は、要求が放棄されます。`enable ldap user auth` が 1 に設定されている場合、クライアントは Adaptive Server の `syslogins` を使用して認証されます。`enable ldap user auth` が 2 に設定されている場合、クライアントのログインは失敗します。

`set_abandon_ldapua_when_full` が `false` に設定されている場合は、LDAP 記述子が新しい認証要求を受け取ることができるようになるまで認証要求はブロックされます。

`set_abandon_ldapua_when_full` を設定するには、次のように入力します。

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

デフォルト値は `false` です。有効な値は、`true` および `false` です。

エンジンあたりの LDAP 記述子数 検索 DN アルゴリズムのログイン手順では、Adaptive Server で、検索を実行する前にアクセス・アカウントを使用して LDAP サーバにバインドする必要があります。Adaptive Server は、バインドの結果として LDAP 記述子 (ハンドル) を取得します。この記述子は、LDAP サーバでログインの DN を検索するために使用されます。

12.5.4 よりも前の Adaptive Server バージョンでは、エンジンごとに 1 つの記述子しかありませんでした。1 つの着信接続が検索の実行にこの記述子を使用している間、他の接続はその記述子を使用できるようになるまで待機していました。Adaptive Server バージョン 12.5.4 では、エンジンごとに最大 20 個の記述子を開くことができます。これにより同時実行性およびログインのパフォーマンスが向上しました。

検索 DN アルゴリズムの詳細については、「[検索 DN アルゴリズム](#)」(18 ページ) を参照してください。

LDAP ユーザ認証エラーのトラブルシューティング

Adaptive Server では、LDAP サーバと通信中に次のような一時的なエラーが発生する場合があります。通常、再接続するとこれらのエラーは解決します。再接続した後も同様のエラーが解決しない場合は、Adaptive Server によって LDAP サーバに FAILED のステータスが設定されます。

- LDAP_BUSY – サーバがビジー。
- LDAP_CONNECT_ERROR – 接続中のエラー。
- LDAP_LOCAL_ERROR – クライアント側のエラー。
- LDAP_NO_MEMORY – クライアント側にメモリを割り当てることができない。
- LDAP_OPERATIONS_ERROR – サーバ側のエラー。
- LDAP_OTHER – 不明なエラー・コード。
- LDAP_ADMINLIMIT_EXCEEDED – 検索が制限を超えている。
- LDAP_UNAVAILABLE – サーバが要求を処理できない。
- LDAP_UNWILLING_TO_PERFORM – サーバが要求を処理しない。
- LDAP_LOOP_DETECT – 参照中にループが検出された。
- LDAP_SERVER_DOWN – サーバに到達できない (接続が失敗した)。
- LDAP_TIMEOUT – ユーザ指定の時間内にオペレーションが完了しないために LDAP API が失敗した。

一時的なエラーや多数の同時ログイン要求によって、大量のエラー・メッセージが繰り返されるエラーログが生成される場合があります。ログを読みやすくするために、次のエラー・メッセージ・ログ・アルゴリズムが使用されます。

- 1 初めてログに記録されるメッセージは、そのまま記録されます。
- 2 メッセージが最後に記録されてから3分を超えた場合は、次のようになります。
 - エラー・メッセージが記録される。
 - メッセージが最後に出力されてからメッセージが繰り返された回数が記録される。
 - メッセージが出力されてから経過した時間が分単位で記録される。

次の原因で発生した認証エラーは、LDAP エラーとはみなされず、認証要求を再試行する条件にはなりません。

- 不正なパスワードまたは無効な識別名によるバインド・エラー。
- 0 の結果セットを返すか、属性値を返さない、バインドが成功した後の検索。

URL 解析中に検出される構文エラーは LDAP URL の設定時にキャッチされるため、上記のいずれのカテゴリにも該当しません。

LDAP ユーザ認証の管理

sp_ldapadmin コマンドの構文は次のとおりです。

sp_ldapadmin 使用方法 : sp_ldapadmin コマンド [option1 [option2]]

次の sp_ldapadmin コマンドがあります。

- 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'

クライアント管理セッションの出力例を次に示します。

```
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://seclldap:31001/'  
2> go  
The URL 'ldap://seclldap:31001/' is set for LDAP User  
Authentication.  
(return status = 0)  
  
1> sp_ldapadmin 'set_secondary_dn_lookup_url',  
'ldap://seclldap:31001//dc=sybase,dc=com??sub?uid=*'  
2> go  
The URL 'ldap://seclldap: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', 'secpasspassword'  
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://seclldap:31001/'
  DN Lookup URL:
  'ldap://seclldap: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://seclldap:31001/'
Distinguished Name Lookup URL:
'ldap://primldap:30001/dc=sybase,dc=com??sub?uid=*'
Secondary Distinguished Name Lookup URL:
'ldap://seclldap: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)
```


LDAP ユーザ認証のチューニング

着信接続の負荷および Adaptive Server-LDAP サーバ・インフラストラクチャに基づいて Adaptive Server のオプションを設定およびチューニングできます。同時着信要求の数に基づいて、次の2つのオプションを設定できます。

- `sp_configure` を使用して、エンジンあたりのネイティブ・スレッド数を指定する `max native threads` を設定する。
- `sp_ldapadmin` を使用して、エンジンあたりの LDAP ユーザ認証ネイティブ・スレッド数を指定する `max_ldapua_native_threads` を設定する。

ネットワークおよび Adaptive Server/LDAP サーバ・インフラストラクチャの状態に基づいて次のオプションを設定します。

- `sp_ldapadmin` を使用して、LDAP サーバのバインドおよび検索タイムアウトを指定する `set_timeout` を設定する。

次のオプションを設定して、着信接続が `max_ldapua_native_threads` に達した場合の Adaptive Server の動作を指定します。

- `sp_ldapadmin` を使用して `set_abandon_ldapua_when_full` を設定する。

LDAP ユーザ認証パスワード情報の変更

Adaptive Server が LDAP サーバから取得してクライアントに渡す、新しい LDAP ユーザ認証関連の通知メッセージが2つあります。

- 期限が切れそうな LDAP ユーザ認証パスワードを使用する LDAP 認証メカニズムを使用して Adaptive Server にログインした場合は、次のメッセージが表示される。

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

- LDAP サーバ管理者がパスワードをリセットした後、または LDAP サーバのパスワードの期限が切れた後に、LDAP 認証メカニズムを使用して Adaptive Server にログインすると、次のメッセージ 4002 が表示される。

```
Login failed
```

次のように、監査が有効で、`errors` 監査オプションがオンになっている場合は、

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

4099 メッセージが監査ログに送信されます。次のような 4099 メッセージが表示されます。

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

注意 この追加の情報を提供できるように LDAP サーバを設定してください。また、Adaptive Server は、LDAP クライアントに対する LDAP パスワード制御の転送をサポートしている必要があります。

ログイン・マッピングに対する制御の強化

外部のクライアント名をローカルの Adaptive Server ログインにマップするには、`sp_maplogin` を使用します。これは、LDAP または PAM で認証されるユーザをローカルの Adaptive Server ログインにマップする場合に使用します。

Kerberos で認証されたユーザをマップするには、`sp_maplogin` ではなく、`sybmapname` を使用します。手順と例については、「[sybmapname を使用したユーザ・プリンシパル名の処理](#)」(12 ページ) を参照してください。

`sp_maplogin` を使用してログイン・マッピングを作成または変更できるのは、`sso_role` を持っているユーザだけです。

Adaptive Server バージョン 12.5.4 では、`sp_maplogin` の制御が強化され、ログインの認証メカニズム設定とログインを使用するマッピング間の競合を回避できるようになりました。潜在的なマッピングの競合は、ストアド・プロシージャ `sp_maplogin`、`sp_modifylogin`、または `sp_addlogin` によって検出されます。

制御の強化により、次のマッピングは許可されなくなりました。

- 1 つの Adaptive Server ログイン名から別のログイン名へのマッピング
- ローカルのログインとして既に存在している外部名からのマッピング
- 存在しないログイン名へのマッピング

また、マッピングを使用して認証メカニズムが指定されている場合、メカニズムはターゲットのログインに設定されている認証メカニズムによりチェックされます。

ターゲットのログインの認証メカニズムによって、特定の認証メカニズムを使用するようにログインが制限されている場合は、マッピングで指定されたメカニズムはログインに指定されているメカニズムに一致するか、**ANY** 認証メカニズムと一致する必要があります。

`sp_maplogin` で、競合が存在することが検出されると、`sp_maplogin` は失敗し、競合を特定するエラーがレポートされます。

同様に、`sp_modifylogin` および `sp_addlogin` は、ユーザ・ログインの `authenticate with` オプションと競合する可能性がある既存のマッピングをチェックします。

`sp_modifylogin` または `sp_addlogin` で競合が検出されると、ログイン・マッピングとの競合を特定するためのエラーがレポートされます。

例1：LDAP ユーザの Adaptive Server “sa” ログインへのマッピング ある企業は、すべてのユーザ・アカウントに対するリポジトリとして LDAP を採用しており、数百台の Adaptive Server を管理できるデータベース管理者 "adminA" および "adminB" を含むすべてのユーザに LDAP 認証を要求するセキュリティ・ポリシーを使用しています。監査は有効になっており、ログイン・イベントは、監査証跡に記録されます。

これらの管理アカウントを “sa” にマップするには、次のように入力します。

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

すべてのユーザに対して LDAP 認証を使用した認証を要求するには、`enable ldap user auth` を使用します。

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

'adminA' が Adaptive Server へのログイン中に認証されると、“sa” だけでなく 'adminA' に関連付けられた識別名がログイン監査イベントに記録されます。これにより、アクションを実行している各ユーザを監査証跡で識別することができます。

'adminA' および 'adminB' のパスワードが LDAP サーバで設定されている場合は、管理対象のすべての Adaptive Server で “sa” パスワードを維持する必要はありません。

この例では、外部の異なる ID やパスワードを認証に使用することもできますが、Adaptive Server 内でこれを行うには、“sa” アカウントに関連付けられた特殊な権限も必要です。

例2：PAM および LDAP の両方を使用したアプリケーション・ログインへのユーザのマッピング ある企業は、PAM および LDAP 認証の両方を採用していますが、それぞれ別の目的で使用しています。会社のセキュリティ・ポリシーでは、LDAP を一般的なユーザ・アカウントの認証メカニズムとして定義し、PAM を中間層アプリケーションなどの特殊なユーザ用として定義しています。中間層アプリケーションは、Adaptive Server への接続プールを設定して、中間層アプリケーションのユーザに代わって要求を処理する場合があります。

LDAP および PAM 両方のユーザ認証のための Adaptive Server の設定は、次のように行います。

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

Adaptive Server のログイン appX を、中間層アプリケーションに適したパーミッションを使用してローカルに設定します。

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

単純なパスワードを appX にハードコードしていくつかの異なる Adaptive Server でそのパスワードを統一して管理するのではなく、中間層アプリケーションを検証するための追加の情報を使用して中央リポジトリでアプリケーションを認証するカスタムの PAM モジュールを開発します。

クライアント・アプリケーションのログイン appY には、LDAP ID とパスワードによるユーザの LDAP 認証が必要です。すべての LDAP 認証ユーザをログイン appY にマップするには、sp_maplogin を使用します。

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

appY のユーザは会社の ID とパスワードを使用して認証されてから、ローカルの Adaptive Server のログイン appY にマップされ、データベース・アクションを実行します。LDAP ユーザの ID を使用して認証が行われると、監査証跡に記録され、アプリケーションのログイン appY に適したパーミッションで実行されます。

SSL サポート

Adaptive Server バージョン 12.5.4 は、次の新しいプラットフォームで SSL をサポートします。

- HP-IA64
- Linux64

PAM のサポート

Adaptive Server バージョン 12.5.4 は、次のプラットフォームで PAM をサポートします。

- HP-IA64
- Macintosh OS X

暗号化カラムの更新

Adaptive Server バージョン 12.5.4 では、次のような暗号化カラムの拡張が行われています。バージョン 12.5.3a の一部になっている暗号化カラム機能の最初のバージョンについては、『Encrypted Columns Guide』を参照してください。

暗号化カラムの参照整合性

2つの暗号化カラム間に参照整合性を設定できるのは、次のような場合です。

- 参照される側と参照する側のカラムは、同じキーを使用して暗号化する。
- カラムの暗号化に使用されるキーは、初期化ベクトル NULL およびランダム埋め込み NULL を指定する。

参照チェックは暗号化された値に対して実行されるため、効率的です。

alter table と暗号化カラム

alter table は、クラスタ化インデックスまたは配置インデックスに属するカラムの暗号化または復号化には使用できません。このカラムを暗号化または復号化するには、インデックスを削除し、カラムを変更して、インデックスを再作成します。

テーブルでトリガが定義されている場合、カラムの復号化には *alter table* を使用できません。カラムを復号化するには、トリガを削除し、カラムを変更して、トリガを再作成します。

sp_help および暗号化カラム

sp_help では、暗号化キーについての情報が表示されます。キー名が *sp_help* に対するパラメータとして指定されている場合、コマンドの実行結果には、キーの名前、所有者、オブジェクトの種類、および作成日がリストされます。

sp_helprotect および暗号化カラム

sp_helprotect では、暗号化カラム、暗号化キー、およびユーザについての新しい情報が次のようにレポートされます。

- テーブルとカラム – decrypt パーミッションが付与されているユーザとカラムをレポートする。
- 暗号化キー – select パーミッションが付与されているユーザをレポートする。
- ユーザ – create encryption key パーミッションが付与されているユーザを示す。

複雑なパスワードとログインのオプション

Adaptive Server バージョン 12.5.4 では、新しいログインまたはリセットされたパスワードについてのルールを設定できる新しいメカニズムと古いメカニズムの組み合わせが導入されています。

Adaptive Server の以前のバージョンでは、次の指定を行えました。

- パスワードに 1 桁以上の数値を含めることを要求する。
- パスワードの長さが最小の長さ以上になることを要求する。
- パスワード有効期間を設定する。
- ログインが特定の回数失敗した後にログインのロックを要求する。
- ログインごとに、数値の桁数、最小の長さ、およびログインの失敗回数についての独自のルールを設定する。ログイン単位のルールは、そのユーザのグローバル・ログインよりも優先される。

Adaptive Server バージョン 12.5.4 では、次の指定も行えます。

- パスワードにログイン名を含めないことを指定する。
- パスワードで使用する特殊文字の最小文字数を設定する。
- パスワードのアルファベット文字の最小文字数を設定する。
- パスワードの大文字の最小文字数を設定する。
- パスワードの小文字の最小文字数を設定する。
- 初回ログイン時にパスワードをリセットする必要があることを指定する。
- パスワードの最小桁数を指定する。
- パスワード有効期限の警告間隔を設定する。

Adaptive Server プラグインでこれらの新しいオプションをそれぞれ設定するか、次の新しいストアド・プロシージャを使用できます。

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

新しい各オプションとその有効な値については、以下の[新しい複雑なパスワード・チェック](#)を参照してください。

新しい複雑なパスワード・オプションを設定すると、`sysattributes` テーブルにオプションごとに1つのローが作成されます。新しいオプションのローが存在している限り、優先度チェックでは新しいオプションが使用され、対応する古いオプション値は無視されます。

以前のバージョンのパスワード・ルールに戻す場合は、Adaptive Server プラグインを使用して複雑なパスワード・オプションの選択を解除するか、次を使用します。

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

新しい複雑なパスワード・オプションには、相互チェックもあります。たとえば、`min lower case in password` と `min upper case in password` の合計が `min alpha in password` よりも大きい場合は、警告メッセージが表示されます。

新しい複雑なパスワード・チェック

ここでは、複雑なパスワード・チェックをサポートするオプションについて説明します。これらのオプションは新しいストアド・プロシージャ・インタフェースで使用できます。その値は、`master.dbo.sysattributes` テーブルに格納されます。

これらのパスワード・オプションをオフにするには、`sp_passwordpolicy` を使用します。個々のオプションをオフにするには、次のように入力します。

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

すべてのパスワードのパスワード・ポリシー・オプションをオフにするには、次のように入力します。

```
sp_passwordpolicy 'clear'
```

単純なパスワードの禁止

`disallow simple password` では、パスワードにログイン名が部分文字列として含まれていないかチェックします。次の値を設定できます。

- 0 – このオプションをオフにし、単純なパスワードを許可する。
- 1 – このオプションをオンにし、単純なパスワードを禁止する。

デフォルトでは、このオプションはオフになっており、このチェックはパスワードに適用されません。

このオプションを設定するには、次のように入力します。

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

単純なパスワードを禁止する場合は、ログイン名をパスワードの部分文字列として使用できません。パスワードは複雑な文字列に設定する必要があります。次に例を示します。

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

ログイン johnd のパスワードは、BHotAcha789 で、ログイン名は部分文字列として含まれていません。

ただし、ログイン・パスワードを次のように変更すると、

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

ログイン johnd が新しいパスワード johnd123 の部分文字列となり、このコマンドは失敗します。

カスタムの複雑なパスワード・チェック

Adaptive Server バージョン 12.5.4 では、複雑なパスワードのルールに加えて、次の2つのストアド・プロシージャを使用してパスワード・チェックをカスタム設定できます。

- `sp_extrapwdchecks`
- `sp_cleanpwdchecks`

これらは、システム・セキュリティ担当者によって指定され、master データベースで定義、保存されるストアド・プロシージャです。これらのカスタム・ストアド・プロシージャは、Adaptive Server による複雑なパスワード・チェック中に自動的に呼び出され、この時点でログインがそれぞれ破棄されます。これらのカスタムのストアド・プロシージャの作成例については、「[カスタムのパスワード・チェックの有効化](#)」(47 ページ)を参照してください。

パスワードの最小桁数の指定

パスワードの最小桁数を指定するには、`min digits in password` を使用します。有効な値は次のとおりです。

- 0 ~ 16 – パスワードに必要な最小桁数。
- -1 – パスワードに数値を含めることはできない。

デフォルトでは、この複雑なパスワード・オプションはオフになっており、このチェックはパスワードに適用されません。

このオプションを設定するには、次のように入力します。

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


たとえば、`min digits in password` を 4 に設定している場合は、パスワードに 4 桁以上の数値を含める必要があります。この要件を満たすためには、次のように入力して、複雑なパスワード `SEcret6789` を使用するログイン `johnd` を追加します。

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

ただし、次のように入力すると、

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

許可される最小桁数が 4 であるため、このコマンドは失敗します。

パスワードのアルファベット文字の最小文字数の指定

`min alpha in password` では、パスワードで使用できるアルファベットの最小文字数を指定します。この値は、大文字と小文字の最小数を合わせた文字数以上の値にする必要があります。

有効な値は次のとおりです。

- 0 ~ 16 – パスワードに必要なアルファベットの文字数。
- -1 – パスワードにアルファベット文字を含めることはできない。

デフォルトでは、この複雑なパスワード・オプションはオフになっており、このチェックはパスワードに適用されません。

パスワードのアルファベット文字の最小数を設定するには、次のように入力します。

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

たとえば、`min alpha in password` を 4 に設定している場合は、パスワードに 4 文字以上のアルファベットを含める必要があります。この要件を満たすためには、次のように入力して、新しいログイン `johnd` のパスワードを `SEcret123456` に設定します。

```
sp_addlogin 'johnd', SEcret123456
```

ただし、新しいログインを次のように作成すると、

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

アルファベット文字の最小文字数が 4 の場合、コマンドは失敗します。

パスワードの特殊文字の最小文字数の指定

`min special char in password` では、パスワードの特殊文字の最小文字数を指定します。有効な値は次のとおりです。

- 0～16 – パスワードの特殊文字の最小文字数。
- -1 – パスワードに特殊文字を含めることはできない。

デフォルトでは、この複雑なパスワード・オプションはオフになっており、このチェックはパスワードに適用されません。

パスワードの特殊文字の最小文字数を設定するには、次のように入力します。

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

たとえば、`set min special char in password` を 3 に設定した場合は、次のように入力して、パスワード `abcDE1&#$$` を使用する新しいログイン `johnd` を設定できます。

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

ただし次のように、新しいログイン `johnd` でパスワード `abcDE1#` を使用するよう設定すると、

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

特殊文字の最小文字数が 3 に設定されている場合、コマンドは失敗します。

パスワードの大文字の最小文字数の指定

`min upper char in password` では、パスワードの大文字の最小文字数を設定できます。有効な値は次のとおりです。

- 0～16 – パスワードに必要な大文字の文字数。
- -1 – パスワードに大文字を含めることはできない。

デフォルトでは、この複雑なパスワード・オプションはオフになっており、このチェックはパスワードに適用されません。

パスワードで許可される大文字の最小文字数を設定するには、次のように入力します。

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

たとえば、`min upper char in password` を 3 に設定した場合は、次のように入力して、パスワード `abcDE1#` を使用するログイン `johnd` を作成できます。

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

ただし、次のログインを追加しようとすると、

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

大文字の最小文字数が 3 に設定されている場合、コマンドは失敗します。

パスワードの小文字の最小文字数の指定

`min lower char in password` では、パスワードの小文字の最小文字数を設定できます。有効な値は次のとおりです。

- 0 ~ 16 – パスワードに必要な小文字の文字数を指定する。
- -1 – パスワードに小文字を含めることはできないことを示す。

デフォルトでは、この複雑なパスワード・オプションはオフになっており、このチェックはパスワードに適用されません。

パスワードの小文字の最小文字数を設定するには、次のように入力します。

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

たとえば、`min lower char in password` を 3 に設定した場合は、次のように入力して、パスワード `abcdEF1#` を使用するログイン `johnd` を作成できます。

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

ただし、次のログインを追加しようとする時、

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

小文字の最小文字数が 3 に設定されている場合、コマンドは失敗します。

最小パスワード長の指定

`minimum password length` では、最小パスワード長を設定します。最小パスワード長は 0 ~ 30 の範囲で設定できます。指定する値は、他の最小要件をすべて組み合わせた長さ以上にする必要があります。

たとえば、次のように設定している場合は、`minimum password length` を 10 以上に設定する必要があります。

```
minimum digits in password を 3 に設定  
minimum special characters in password を 2 に設定  
minimum uppercase characters in password を 2 に設定  
minimum lowercase characters in password を 3 に設定
```

この例では、パスワードの長さが 10 未満の場合、警告メッセージが表示されますが、パスワード・ポリシー・オプションの設定は成功します。

最小パスワード長を設定するには、次のように入力します。

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

たとえば、`minimum password length` を 6 に設定した場合は、次のように入力して、ログイン `johnd` の 6 文字の新しいパスワードを作成できます。

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

ただし、パスワードを次のように変更すると、

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

最小パスワード長が6文字の場合、コマンドは失敗します。

パスワード有効期限の指定

`password expiration` は、期限が切れるまでの、パスワードが存在できる日数を指定します。この値はグローバルな単位で指定します。有効な値は次のとおりです。

- 0 – パスワードの期限は切れない。
- 1 ~ 32767 – 期限が切れるまでの、パスワードが存在できる日数。

デフォルトでは、この複雑なパスワード・オプションはオフになっており、このチェックはパスワードに適用されません。

パスワード有効期限を指定するには、次のように入力します。

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

パスワード有効期限の警告間隔の指定

`password exp warn interval` は、パスワードの期限が切れるまで、パスワード有効期限の警告メッセージを表示する間隔(日数)を指定します。これらのメッセージは、パスワードが変更されるか、期限が切れるまで、成功したすべてのログインで表示されます。この値は、パスワード有効期限以下の値にする必要があります。

有効な値は0 ~ 365です。このオプションはデフォルトでオフになっています。

パスワード有効期限の警告間隔を指定するには、次のように入力します。

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

許可されるログイン失敗数の指定

`maximum failed logins` では、ログインがロックされるまで実行できる、ログイン失敗の最大回数を指定します。この値はグローバルに指定します。有効な値は次のとおりです。

- 0 – ログイン失敗回数に関係なく、ログインはロックされない。
- 1 ~ 32767 – ログインがロックされるまでに許可されるログイン失敗回数。

デフォルトでは、この値はオフになっており、このチェックはパスワードに適用されません。

許可されるログイン失敗回数を設定するには、次のように入力します。

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

初回ログイン時のパスワードのリセット

`expire login` では、システム・セキュリティ担当者がログインを作成またはリセットすると、ログインのステータスを期限切れに変更します。ログインは、初回ログイン時にパスワードを変更する必要があります。有効な値は次のとおりです。

- 0 – 新しいログインまたはリセットされたログインには期限を設定しない。
- 1 – 新しいログインまたはリセットされたログインの期限が切れた場合は、初回ログイン時にパスワードをリセットする。

デフォルトでは、この値はオフになっており、このチェックはパスワードに適用されません。

初回ログイン時にパスワードの変更を要求するようにオプションを設定するには、次のように入力します。

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

複雑なパスワード・オプションの相互チェック

いくつかの複雑なパスワード・オプションでは、オプション間の相互関係に注意する必要があります。

- `minimum password length` には、`min digits in password`、`min alpha in password`、`min special characters in password` の合計以上の値を設定する。
- `min alpha in password` には、`min upper char in password` および `min lower char in password` の合計以上の値を設定する。
- `systemwide password expiration` には、`password exp warn interval` よりも大きい値を設定する。

上記の相互チェックを行うために、Adaptive Server では、値が -1 の複雑なパスワード・オプションが検出された場合、この値は 0 とみなされます。いずれかのオプションが設定されていない場合も、そのオプションの値は 0 とみなされます。

Adaptive Server では、相互チェックに合格しない新しい複雑なパスワード・オプションそれぞれについて警告を表示します。ただし、オプションの設定は成功します。

古いパスワード・チェックと新しい複雑なパスワード・チェックの設定

表 2-7: 古いパスワード・チェックと新しい複雑なパスワード・チェック

Adaptive Server 認証のパスワード・チェックとポリシー	sp_configure を使用して指定される既存の設定パラメータ	sp_passwordpolicy を使用して指定される新しい複雑なパスワード・オプション	sp_modifylogin を使用して指定される既存のログイン単位の上書き
パスワードの有効期限	system-wide password expiration	system-wide password expiration	password expiration
パスワードの桁数	check password for digit	min digits in password	該当なし
パスワードのアルファベット文字数	該当なし	min alpha in password	該当なし
パスワードの長さ	minimum password length	minimum password length	min passwd length
ロックされるまでのログイン失敗回数	maximum failed logins	maximum failed logins	max failed_logins
単純なパスワードの禁止	該当なし	disallow simple passwords	該当なし
パスワードの特殊文字数	該当なし	min special char in password	該当なし
パスワードの大文字数	該当なし	min upper char in password	該当なし
パスワードの小文字数	該当なし	min lower char in password	該当なし
パスワード有効期限の警告間隔	該当なし	password exp warn interval	該当なし
初回ログイン時のパスワードのリセット	該当なし	expire login	該当なし
カスタムの複雑なパスワード・チェック	該当なし	該当なし	該当なし

複雑なパスワード・オプションは次のレベルで設定できます。

- ログイン・レベル。sp_addlogin または sp_modifylogin を使用する。
- グローバル・レベル。新しい sp_passwordpolicy または sp_configure を使用する。

グローバル単位およびログイン単位で、古いパラメータと新しいパラメータを使用してパスワード設定オプションを設定できるため、パスワード・オプションが適用される優先順位を把握しておくことが重要です。

パスワード・オプションを適用すると、Adaptive Server は最初に既存のログイン単位のパラメータを参照してから、新しい複雑なパスワード・オプションを参照し、最後に既存のグローバル・オプションを参照します。

例1 次のように入力します。

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

johnd の最小パスワード長は6に設定されます。

次に、ログイン johnd に対して以下のような既存のグローバル・オプションを入力します。

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

ログイン johnd に対して2つの最小パスワード長要件を作成し、パスワードの桁数の制限についても設定しています。

次に、ログイン johnd のパスワードを次のように作成します。

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

Adaptive Server では、次の順序でパスワードをチェックします。

- 1 ログイン単位の既存のオプションのチェック:パスワードの最小長は6より大きい値にする必要があります。これには該当するため、チェックは合格です。
- 2 新しいオプション:パスワードの最小桁数は2より大きい値にする必要があります。これには該当するため、チェックは合格です。
- 3 既存のグループ・オプション:ログイン johnd についてはログイン単位のチェックが既に行われているため、この例で指定されている最小パスワード長はチェックされません。
- 4 パスワードの桁のチェック・オプションは、最小桁数がオンで、値が2に設定されているときに既にチェックされているため、不要です。

これらのチェックが指定された順序で実行され、ログイン johnd の新しいパスワードがこれらのチェックに合格すると、新しいパスワードの作成は成功します。

例2 同じログインについて、次のように入力するとします。

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

Adaptive Server は最初にログイン単位の既存のオプションをチェックし、最小パスワード長が6に設定されることを確認しますが、ユーザは、4文字のみが含まれるパスワードを作成しようとしていました。この場合チェックは失敗し、Adaptive Server はエラー・メッセージを示します。1つの複雑なパスワード・チェックが失敗すると、それ以外のオプションはチェックされません。

例 3 次のパスワード設定オプションを指定して新しいログインを作成するとします。

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

この場合、ログイン johnd の最小パスワード長は 4 に設定されます。これはログイン単位の既存のオプションです。次に、以下を追加します。

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

パスワードの最小桁数を 1 に設定する必要があるグローバル要件が作成されます。

次に、ログイン johnd のパスワードを次のように作成します。

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

Adaptive Server では、次の順序でチェックを実行します。

- 1 ログイン単位の既存のオプションのチェック：新しいパスワードの最小パスワード長は 4 です。パスワード abcde は 4 文字を超えているため、このチェックは合格です。
- 2 新しいグローバル要件のチェック：パスワードの最小桁数はグローバル単位で 1 に設定されています。このチェックは失敗します。

Adaptive Server は新しいパスワードを作成せずに、エラー・メッセージを示します。

新しいパスワードを作成するには、すべてのチェックに合格する必要があります。

複雑なパスワードのストアード・プロシージャ

Adaptive Server には、複雑なパスワードの設定に役立ついくつかの新しいストアード・プロシージャがあります。

sp_extrapwdchecks

`sp_extrapwdchecks` は、複雑なパスワード・チェックのユーザ定義ロジックを含むことができる新しいカスタムのストアード・プロシージャです。セキュリティのニーズに応じて、`sp_extrapwdchecks` を設定できます。`master` データベースに `sp_extrapwdchecks` をインストールします。

```
sp_extrapwdchecks caller_password, new_password, login_name
```

各パラメータの意味は、次のとおりです。

- `caller_password` には、現在のパスワードを指定します。
- `new_password` には、設定する新しいパスワードを指定します。

- `login_name` には、変更または追加されているパスワードと関連付けられたログイン名を指定します。

`sp_extrapasswordchecks` では、Adaptive Server に対して失敗を通知するために `raiserror` を使用する必要があります。この失敗のエラー・メッセージは、`sp_addmessage` を使用する Adaptive Server に追加されます。

`sp_cleanpwdchecks`

`sp_cleanpwdchecks` では、ユーザ定義のテーブルでログインおよびパスワード関連の属性を削除する日時と方法を定義できます。`sp_cleanpwdchecks` はユーザ定義で、ログインを削除したときに `master` データベースで動的に呼び出されます。

`sp_cleanpwdchecks, login_name`

各パラメータの意味は、次のとおりです。

- `login_name` – 実行するクリーンアップのログイン名を指定します。

`sp_passwordpolicy`

`sp_passwordpolicy` は、`sso_role` を持つユーザが新しい複雑なパスワード・オプションの指定、削除、およびリストを実行する際に使用できるインタフェースです。この情報は、`master.dbo.sysattributes` に格納されます。

`sp_passwordpolicy {set | clear | list }, policy_option, option_value`

各パラメータの意味は、次のとおりです。

- `set` – オプションの値を設定します。
- `clear` – `master.dbo.sysattributes` テーブルで指定されたオプションのローを削除します。ポリシー・オプションが指定されていない場合、`clear` によって、`sysattributes` テーブル内のすべてのオプション・ローが削除されます。
- `list` – 指定されたオプションの値を一覧表示します。
- `policy_option` – オペレーションを実行するオプション・パラメータです。有効な値は次のとおりです。
 - `disallow simple passwords` – 1 の値を指定するとオプションはオンになり、0 の値を指定するとオフになる。
 - `min digits in password` – パスワードで許可される最小桁数を指定する。
 - `min alpha in password` – パスワードで許可されるアルファベットの最小文字数を指定する。
 - `min special char in password` – パスワードで許可される特殊文字の最小文字数を指定する。

- **min upper char in password** – パスワードで許可される大文字の最小文字数を指定する。
- **min lower char in password** – パスワードで許可される小文字の最小文字数を指定する。
- **systemwide password expiration** – システム全体のパスワード有効期限を日数で指定する。
- **password exp warn interval** – パスワード有効期限の警告間隔を日数で指定する。
- **minimum password length** – 最小パスワード長を設定する。
- **maximum failed logins** – アカウントがロックされるまでセッションで許可されるログイン失敗の最大回数を設定する。
- **expire login** – ログインを作成またはリセットするときにログインのステータスが期限切れのステータスに変更されることを指定する。初回ログイン時にはパスワードを変更する必要がある。
- *option_value* – *policy_option* の値です。

例 1 パスワードの期限が切れるまでのパスワード有効期限の警告間隔を 7 日間に設定するには、次のように入力します。

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

例 2 特殊文字の最小文字数のオプションを一覧表示するには、次のように入力します。

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

例 3 単純なパスワードの禁止をデフォルト値にリセットするには、次のように入力します。

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

変更されたストアド・プロシージャ

次のストアド・プロシージャは、複雑なパスワードの実装に伴って変更されています。

- **sp_addlogin** および **sp_password** – 新しい複雑なパスワード・チェックを呼び出す。
- **sp_droplogin** – **sp_cleanpwdchecks** が **master** データベースに存在する場合は、**sp_droplogin** を使用してログインを削除した後に行われる。
- **sp_displaylogin** – パスワード有効期限、最小失敗ログイン回数、およびパスワード長に関連するログイン情報を表示するときに、新しい **sp_passwordpolicy** セキュリティ・オプションが考慮される。

カスタムのパスワード・チェックの有効化

Adaptive Server バージョン 12.5.4 では、システム・セキュリティ担当者が、カスタムのパスワード・チェックを有効にするユーザ定義のストアド・プロシージャを作成できます。

たとえば、パスワード履歴のチェックを実装するには、次のように入力して、パスワードの履歴を保存するための新しいユーザ・テーブルを作成します。

```
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
```

このユーザ定義のストアド・プロシージャは、新しいパスワードを **pwdhistory** テーブルに暗号化フォームで保存することを指定する場合に呼び出すことができます。

```
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
```

`sp_addmessage` を使用して、ユーザ定義のメッセージ 22001 を追加します。`raiserror 22001` は、カスタムの複雑なパスワード・チェックのエラーが発生し、それが原因で `sp_addlogin` または `sp_password` が失敗したことを示します。

次のユーザ定義のストアード・プロシージャは、`sp_extrapwdchecks` を使用して履歴を追加した後のクリーンアップのために使用できます。

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

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

上記の 2 つのパラメータが定義され、`master` データベースにインストールされると、これらのパラメータは複雑なパスワード・チェック中に動的に呼び出されます。

DDLGen のサポート

ログイン - TL は、1 つまたはすべてのログインに対して DDL を生成します。この例では、ポート 1955 を使用する HARBOR というマシン上のすべてのログインの DDL を生成します。

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

注意 すべてのログインに対して生成された DDL のパスワードは “password” です。

または、-N% の代わりに **-Nusername** を使用して個々のログインを指定することもできます。

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

サーバ全体の複雑なパスワード・オプションが 1 つまたは複数のログインに指定されている場合、すべての `sp_addlogin` および `sp_modifylogin` DDL 文が最初に生成され、次に、複雑なパスワード・オプションに対する DLL 文が生成されます。

この例では、ポート 1955 を使用する HARBOR というマシン上のログイン “george” の DDL を生成します。

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

Adaptive Server プラグインのサポート

Adaptive Server プラグインは、複雑なパスワードの GUI 管理をサポートします。詳細については、「[第 8 章 Adaptive Server プラグインの変更](#)」を参照してください。

ログイン・トリガからの set オプションのエクスポート

Adaptive Server バージョン 12.5.4 では、ログイン・トリガ内の set オプションをユーザ・セッション全体で有効にできます。

次の set オプションは自動的にエクスポートされます。

- 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_truncation
- prefetch
- triggers
- 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

グローバル・ログイン・トリガの設定

Adaptive Server バージョン 12.5.4 には、新しいグローバル・ログイン・トリガを設定する機能があります。グローバル・ログイン・トリガを設定するには、`sp_logintrigger` を使用します。これは、ユーザのログインごとに実行されます。ユーザ固有のアクションを取得する場合は、`sp_modifylogin` または `sp_addlogin` を使用してユーザ固有のログイン・トリガを設定する必要があります。

sp_logintrigger

説明

`sp_logintrigger` は、グローバル・ログイン・トリガを設定、表示するために使用できる新しいプロシージャです。このグローバル・ログイン・トリガの特性は、個人のログイン・スクリプトと同じです。これは、システム管理者やセキュリティ担当者を含め、ログインしようとしているすべてのユーザの個人のログイン・スクリプトよりも前に実行されます。

構文

```
sp_logintrigger <global login trigger name>
```

パラメータ

global login trigger name

グローバル・ログイン・トリガの名前です。

`sp_logintrigger` にパラメータが含まれない場合、現在のログイン・トリガのステータスと名前が表示されます (存在する場合)。グローバル・ログイン・トリガが定義されていない場合、ローは表示されません。

例

例 1 `sp_logintrigger` を使用してグローバル・ログイン・トリガを設定するには、次のように入力します。

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

例 2 更新されたグローバル・ログイン・トリガを表示するには、次のように入力します。

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

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

例 3 グローバル・ログイン・トリガが存在しない場合は、次のように表示されます。

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

例 4 `sp_logintrigger` で以前指定したグローバル・ログイン・トリガを削除するには、次のように入力します。

```
sp_logintrigger 'drop'
```

使用法

- 新しいグローバル変数 `@@logintrigger` は、グローバル・ログイン・トリガが定義されて有効になっているかどうかを確認するために使用されます。
- このグローバル・ログインと個人のログイン・スクリプト間には違いがあります。このグローバル・ログイン・トリガは、`sysattributes` で名前別に保存されますが、個人のログイン・スクリプトはオブジェクト ID のみ保存されます。

パーミッション

すべてのユーザは、`sp_logintrigger` を実行して、現在のグローバル・ログイン・トリガを表示できます。新しいログイン・トリガを設定するには、SSO の役割が必要です。

トピック名	ページ
概要	53
アーカイブ・データベースの設定	59
アーカイブ・データベースの使用	64
アーカイブ・データベースのセキュリティとパーミッション	66
アーカイブ・データベースの圧縮ダンプ	67
アーカイブ・データベースのマイグレート	68
アーカイブ・データベースのアップグレードとダウングレード	68
アーカイブ・データベースのアクセスの DDLGen サポート	70
アーカイブ・データベースの制限	70

アーカイブ・データベースへのアクセス機能により、データベース管理者は、従来の読み取り専用データベース(このタイプのデータベースは「アーカイブ・データベース」と呼ばれます)と同様の方法でダンプにアクセスし、データベース・ダンプ(アーカイブ)のデータを検証したり、選択的にリカバリしたりできます。

従来のデータベースとは異なり、アーカイブ・データベースは実際のデータベース・ダンプを主要なディスク記憶領域デバイスとして使用し、従来の記憶領域を最小限にすることによって、データベース・ダンプのリカバリの結果生成される新しいページまたは変更済みのページを表します。データベース・ダンプには、すでに多くの(ほとんどではない場合)データベース・ページのイメージが含まれているため、Backup Server を使用してページをアーカイブから従来のデータベース記憶領域に転送しなくてもアーカイブ・データベースをロードできます。その結果、従来のデータベースよりもロードが大幅に速くなります。

概要

アーカイブ・データベースのアクセスでは、さまざまな操作をデータベース・ダンプに対して直接実行できます。

従来のデータベースをロードするには、ソース・データベースのサイズと同じか、それ以上の記憶領域が必要になります。Backup Server を使用してデータベース・ダンプをロードするには、データベース・ダンプから、従来のデータベースとは別に設定されたストレージにページをコピーすることが必要です。

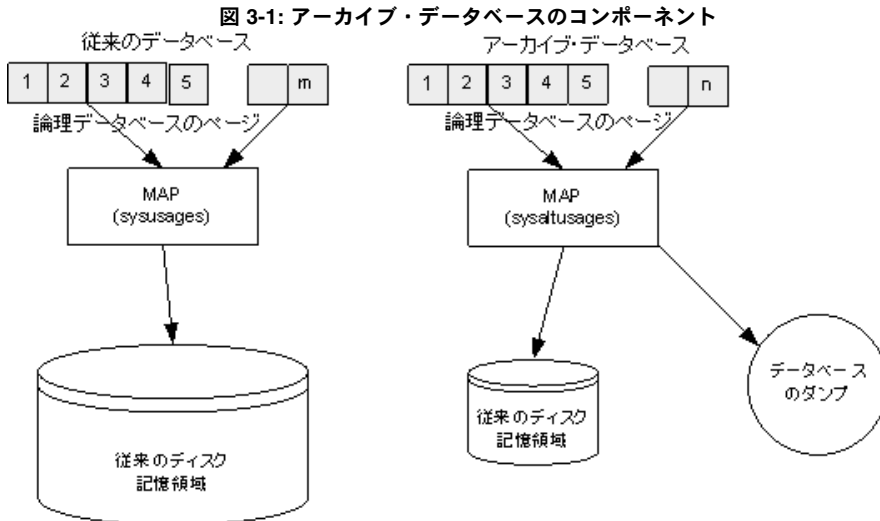
対照的に、アーカイブ・データベースは最小限の従来のディスク記憶領域を使用して作成できます。アーカイブ・データベースをロードするとき、データベース・ダンプ内に存在するページは Backup Server によりコピーされません。代わりに、アーカイブ内のページの「論理ページから仮想ページへの」マッピングを表すマップが Adaptive Server により作成されます。これにより、データベース・ダンプのデータの表示に必要な時間が大幅に短縮され、ダンプのロードに必要な記憶領域のサイズも減少します。

アーカイブ・データベースでは、元のデータベース全体をコピーする必要はありません。`sp_dumpoptimize` を使用してデータベースをダンプするときに行われる最適化に応じて、データがアーカイブ・データベースに完全に格納される (データベースのすべてのページがデータベース・ダンプに格納される) か、部分的に格納されます (割り付けられたページだけがデータベース・ダンプに格納される)。

データベース・ダンプは、データベースとして存在するため、データベース管理者は次のような使いやすいつールと手法を使用してクエリを実行できます。

- 運用データベースからダンプされた最新のコピーに対する、データベース一貫性検査。これらの検査を別のサーバで実行することにより、運用環境におけるリソースの競合を避けることができる。リソースを考慮する必要のない場合は、アーカイブが作成されたのと同じサーバでアーカイブを直接検査できる。アーカイブでの検証により、リストア操作の実行前に必要な保証を得られる。
- データベース・ダンプの整合性が問題となる場合、アーカイブ・データベースにデータベース・ダンプをロードすると問題ないかどうかを簡単にテストできるため、従来のデータベースのリストアに使用される適切なデータベース・ダンプを特定するのに良いツールとなる。
- データベース・ダンプからのオブジェクト・レベルのリストア。失われたデータは、`select into` を使用してアーカイブ・データベース内のテーブルからリストア対象のローをコピーすることにより、リカバリされる。`select into` 操作は、アーカイブ・データベースを持つサーバで直接実行するか、オブジェクトのリストアが必要なサーバとは別のサーバでアーカイブ・データベースが使用可能な場合はコンポーネント統合サービス・プロキシ・テーブルを使用することにより実行できる。

次の図に、アーカイブ・データベースと従来のデータベース構造の相違点を示します。



アーカイブ・データベースのコンポーネント

アーカイブ・データベースは、連携して機能する3つのコンポーネントで構成されており、データベース・ダンプが従来のデータベースとして機能しているかのように見せかけることができます。使用されるコンポーネントは次のとおりです。

- データベース・ダンプ(アーカイブ)
- 変更済みページ・セクションの格納に使用される従来のディスク記憶領域
- sysaltusages テーブルを持つスクラッチ・データベース

データベース・ダンプ

データベース・ダンプは、ほとんどの未変更ページのリポジトリとして使用されます。

データベース・ダンプは、読み込み専用です。データベース・ダンプに変更を加えることはできません。ダンプ内のデータに加えた変更はすべて、変更済みページ・セクションに格納されます。

Adaptive Server では、このデータベース・ダンプとストライプは、アーカイブ・データベースによってのみ使用可能なデータベース・デバイスと見なされます。

変更済みページ・セクション

データベース・ダンプには、特定の時間のデータベースのスナップショットが反映されます。データベース・ダンプを表すアーカイブ・データベースは読み込み専用です。ユーザ・トランザクションは実行できません。アーカイブ・データベースは読み込み専用ですが、ある種の変更については実行可能です。次に例を示します。

- アーカイブ・データベースの一貫性を保つためのリカバリを実行できる。
- テーブルの修正バージョンをリストアするための修正を実行する `dbcc` コマンドを使用できる。

これらの変更済みデータベース・ページ、および新しく割り付けられたデータベース・ページはデータベース・ダンプとそのストライプ内に格納できないため、アーカイブ・データベースには従来のデータベース記憶領域が若干必要です。このディスク領域は変更済みページ・セクションと呼ばれ、`create archive database` コマンドおよび `alter database` コマンドを使用して割り付けることができます。

スクラッチ・データベースと `sysaltusages` テーブル

`sysaltusages` テーブル

`sysaltusages` システム・テーブルは、アーカイブ・データベースのページ番号を、データベース・ダンプとそのストライプ内、または変更済みページ・セクション内の実際のページにマップするために使用される新しいデータオンリーロック・テーブルです。しかし、従来のデータベースの `sysusages` テーブルとは異なり、`sysaltusages` テーブルはデータベースのすべての論理ページをマップするわけではありません。`sysaltusages` は、次のページをマップします。

- データベース・ダンプに格納されたページ
- 変更されたために、変更済みページ・セクションに移動されたページ

`sysaltusages` には、次のカラムがあります。

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

各カラムの意味は、次のとおりです。

- `dbid` – アーカイブ・データベースのデータベース ID。
- `location` – ページの物理的に連続したブロックが存在するアーカイブ・データベース・セグメントのロケーション。

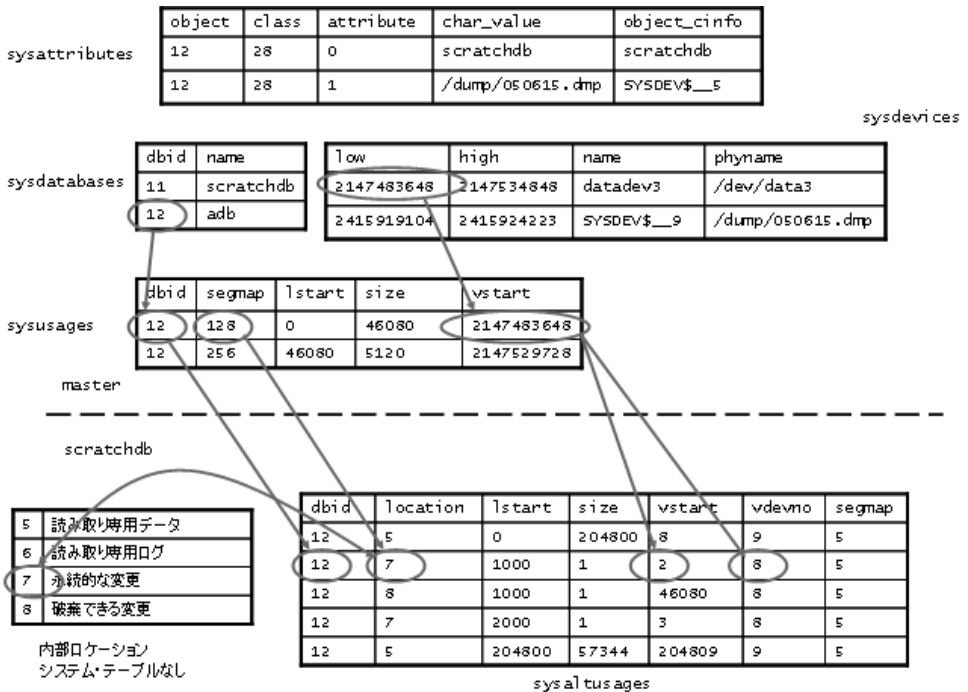
値 5 および 6 は、セグメントのロケーションがデータベース・ダンプまたはそのストライプ内であることを示し、値 7 および 8 はセグメントのロケーションが変更済みページ・セクション内であることを示しています。値 4 は、物理的に使用できないページのギャップを埋めるために使用されます。

- `lstart` – 物理的に連続するページのブロックが開始する論理ページ番号。
- `size` – 物理的に連続するページのブロックにある論理ページの数。

- vstart - vdevno により指定されたデバイス上のページの連続するブロックが開始するオフセット。
- vdevno - ページの連続するブロックが存在するデバイス番号。
- segmap - ページのこのブロックが割り付けられたセグメントのマップ。
sysaltusages テーブルは、図 3-2 のようになります。

注意 sysaltusages はロー・ロック・カタログであるため、reorg を定期的的に使用して、論理的に削除された領域を再利用する必要があります。

図 3-2: sysaltusages テーブル



スクラッチ・データベース

スクラッチ・データベースには、新しい `sysaltusages` テーブルが格納されず。スクラッチ・データベースは、`sysaltusages` テーブルを柔軟に配置するために使用されます。

スクラッチ・データベースは、任意のデータベースにすることができます (`master` データベースや テンポラリ・データベースなどの例外を除く)。以下の理由から、スクラッチ・データベース専用のデータベースを使用することをおすすめします。

- `sysaltusages` のサイズが、サポートされるアーカイブ・データベースの数によって変化する場合があります。データベースのサイズを小さくすることはできないが、大きすぎる場合はそれを削除して、必要に応じて再作成できる。
- データベース・ログが自動的にトランケートされるように、"`trunc log on checkpoint`" オプションを有効にできる。

`sysaltusages` テーブルを持つ点を除けば、このデータベースは他のデータベースと同様です。スレッシュホールド・プロシージャと他の領域管理メカニズムを使用して、データベース内の領域を管理できます。

次のように入力することにより、スクラッチ・データベースとして使用可能なデータベースを指定できます。

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

各アーカイブ・データベースに割り当てることができるスクラッチ・データベースは一度に 1 つのみですが、複数のデータベースが同じスクラッチ・データベースを使用することはできません。多数のアーカイブ・データベースがある場合は、複数のスクラッチ・データベースを定義できます。

アーカイブ・データベースの操作

従来のデータベースの多くの操作を、アーカイブ・データベースで行うことができます。ただし、データベースを変更するユーザ定義トランザクションやコマンド (`insert`、`update`、`delete` など) は実行できません。

データが格納されたアーカイブ・データベースは、`sp_dboption` ストアド・プロシージャを使用して '`readonly`' オプションが適用された読み込み専用データベースと同様です。

アーカイブ・データベースの設定

この項では、アーカイブ・データベースを作成および設定する方法について説明します。

アーカイブ・データベースの作成

アーカイブ・データベースは、`create archive database` コマンドを発行することにより作成できます。構文は次のとおりです。

```
create archive database <db name>
  [on <db device> [= <size>]
  [, <db device> [= <size>]] ... ]
  with scratch_database = <db name>
```

各パラメータの意味は、次のとおりです。

- `on` - 変更済みページ・セクションを指定する。変更済みページを格納する従来のデータベース記憶領域が必要。変更済みページ・セクションのロケーションとサイズを指定するには、`on` 句を使用する。
- `db device` - 変更済みページ・セクションを作成するデータベース・デバイス指定する。
- `size` - 作成する変更済みページ・セクションのサイズを指定する。`size` が省略された場合、5120 ページが割り付けられる。
- `with scratch_database` - (必須) アーカイブ・データベースに関する情報が保持される既存のデータベースの名前を指定する。アーカイブ・データベース内のすべての論理ページを物理ページにマップする `sysaltusages` システム・テーブルは、スクラッチ・データベースに格納される。

変更済みページ・セクションのサイズ設定

変更済みページ・セクションは、変更されたデータベース・ページまたは新しく割り付けられたデータベース・ページの格納に使用されます。

- ページは、変更済みページ・セクションに1回だけ再マップ可能です。
- リカバリは、ほとんどのページ再マップにおいて重要な位置を占めます。
- `dbcc checkalloc` にも、有効な領域割り付けが必要です。
- 変更済みページ・セクションのサイズは、`alter database` コマンドを使用して拡張できます。ただし、変更済みページ・セクションのサイズを小さくするには、アーカイブ・データベースを削除して再作成する必要があります。

変更済みページ・セクションの最小サイズは、データベースで変更されたページの数または新しく割り付けられたページの数によって決まります。これらのページの多くは、リカバリの再実行およびリカバリの取り消しによって変更されます。

変更済みページの数をもっと少なくし、変更済みページ・セクションに必要な領域の量を減らすには、`load database with norecovery` コマンドを使用します。これを行うことには、マイナス面もあります。詳細については、「[load database with norecovery の使用](#)」(62 ページ)を参照してください。

注意 `dbcc checkalloc` は、`nofix` オプションを使用する場合でも、変更済みページ・セクションの領域を大量に消費します。`dbcc checkalloc` を実行すると、すべてのアロケーション・ページ (256 ページごと) に情報が書き込まれます。これらのアロケーション・ページの変更結果は、変更済みページ・セクションに格納されます。また、`dbcc checkalloc` を使用する場合は、少なくとも元のデータベースの 256 分の 1 のサイズの変更済みページ・セクションが必要であることを意味しています。

変更済みページ・セクションに十分な領域がない場合、領域が必要なコマンドがサスペンドされ、次のようなエラーが表示されます。

```
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.
```

変更済みページ・セクションの領域を増やすには、次のいずれかの操作を行います。

- `alter database` を使用して、変更済みページ・セクションのサイズを大きくする。
- 変更済みページ・セクションに追加の領域を割り付けられない場合は、[Ctrl+C] を押して現在のコマンドをアボートする。

注意 スレッシュホールドを使用して、変更済みページ・セクションの領域を管理することはできません。

変更済みページ・セクションに割り付けられた領域の拡張

`alter database` を使用すると、アーカイブ・データベースの変更済みページ・セクションの領域を追加できます。変更済みページ・セクションの領域を増やすと、サスペンドされたコマンドの処理を再開できます。

`alter database` は、領域がなくなったときに限らず、いつでも実行して変更済みページ・セクションのサイズを大きくすることができます。

```
alter database <db name>
  [on <db device> [= <size>]
  [, <db device> {= <size>}] ...]
```


アーカイブ・データベースのマテリアライズ

アーカイブ・データベースは、データベース・ダンプとともにロードされたときにだけ有用なプレースホルダです。ロード処理では、実際にはページはコピーされませんが、ページ・マッピングを使用してデータベースがマテリアライズされます。

アーカイブ・データベースをマテリアライズするには、`load database` コマンドを使用します。構文は次のとおりです。

```
load database <db name>
  from <dump device>
  [ [stripe on <stripe device>] ... ]
  [with [norecovery,][passwd=<password>]
```

各パラメータの意味は、次のとおりです。

- *db name* – ロード先のアーカイブ・データベースの名前を指定する。
- *dump device* – ダンプのロード元のディスク・データベース・ダンプの名前を指定する。
- *stripe device* – 追加のディスク・データベース・ダンプ・ストライプを指定する。
- *norecovery* – `load database` コマンドによりリカバリを実行せず、`load database` コマンドが完了した後データベースを自動的にオンラインにすることを指定する。詳細については、「[load database with norecovery の使用](#)」(62 ページ)を参照してください。

注意 `norecovery` は、アーカイブ・データベースのアクセスを可能にするために、Adaptive Server バージョン 12.5.4 で導入されました。従来のデータベースでは、`norecovery` を使用できません。

- *passwd =<password>* – アーカイブ・データベースのロード元のダンプがパスワードで保護されている場合は指定する必要がある。パスワードの長さは、6～30 文字にする。

注意 ダンプをアーカイブ・データベースにロードするときに、Backup Server が実行されている必要はありません。

load database with norecovery の使用

load database コマンドの with norecovery オプションを使用すると、リカバリを行わずにデータベース・ダンプをアーカイブ・データベースにロードすることで、ロードに必要な時間を減らすことができます。多くのデータベース・ページは、リカバリ中に変更や割り付けを行い、変更済みページ・セクションに格納することができます。そのため、リカバリを省略すると、消費される変更済みページ・セクションの領域が最小限に抑えられます。with norecovery オプションを使用すると、アーカイブ・データベースをすばやく表示できます。

with norecovery を使用した場合、データベースは自動的にオンラインになります。

ただし、リカバリが必要なデータベースに load database with norecovery を使用すると、トランザクションの一貫性と物理的な一貫性が保たれないままになる可能性があります。物理的な一貫性がないデータベースで dbcc 検査を実行すると、エラーが発生することがあります。

with norecovery を使用してアーカイブ・データベースをロードした場合、アーカイブ・データベースを使用するには sa_role またはデータベース所有者の権限が必要です。

アーカイブ・データベースでの論理デバイスの使用

sp_addumpdevice を使用すると、アーカイブ・データベースをロード可能な論理デバイスを作成できます。構文は次のとおりです。

```
sp_addumpdevice 'archive database', '<logical name>',
'<physical name>'
```

このコマンドを実行すると、load database コマンドの dump device または stripe device として、physical name の代わりに logical name を使用できるようになります。

アーカイブ・データベースでの load database の制限

load database をアーカイブ・データベースに対して使用する場合は、次の制限があります。

- アーカイブ・データベースのデータベース・ダンプは、ローカル・マシンにマウントされたファイル・システムのディスク・ダンプでなければならない。これは、ローカル記録領域でも、NFS 記憶領域でもよい。load database ... at <remote server> 構文はサポートされず、テープ上のデータベース・ダンプもサポートされない。
- 異なるアーキテクチャ間のロードはサポートされない。バイト順序を合わせるために、データベース・ダンプおよび load database コマンドは同じアーキテクチャで実行する必要がある。
- ダンプしたデータベースのページ・サイズは、アーカイブ・データベースを持つサーバが使用するページ・サイズと同じでなければならない。

- ダンプが行われたサーバのメジャー・バージョンは、アーカイブ・データベースを持つサーバのメジャー・バージョン以前のバージョンでなければならない。
- データベース・ダンプが行われたサーバの文字セットおよびソート順は、アーカイブ・データベースを持つサーバの文字セットおよびソート順と同じでなければならない。
- データベース・ダンプの各ストライプの最大サイズは 32GB。

注意 ストライプのサイズが 32GB より大きい場合、`dump database` コマンドを発行するときに追加のストライプを指定します。このようにして、最大サイズ内に収まるように各ストライプのサイズを小さくします。

アーカイブ・データベースのオンライン化

アーカイブ・データベースをオンラインにするには、次のコマンドを使用します。

```
online database <db name>
```

`db name` は、オンラインにするアーカイブ・データベースの名前です。

`online database` は、変更済みページおよび割り付けられたページを変更済みページ・セクションに再マップ可能なときに、リカバリの取り消しを実行します。

データベースをロードすると、リカバリの取り消しパスを実行しなくても自動的にオンラインになるため、`with norecovery` を使用してデータベースをロードした場合はデータベースをオンラインにする必要はありません。

アーカイブ・データベースの削除

アーカイブ・データベースを削除するには、次のコマンドを使用します。

```
drop database <db name>
```

`db name` は、削除するデータベースの名前です。

アーカイブ・データベースを削除すると、そのデータベースのすべてのローが、スクラッチ・データベースの `sysaltusages` テーブルから削除されます。これにより、スクラッチ・データベースにログ領域が必要になります。

注意 `drop database` の実行時にスクラッチ・データベースのログ領域を使い果たした場合、`[Ctrl+C]` を押してスクラッチ・データベースのログをトランケートし、`drop database` コマンドをリトライします。`[Ctrl+C]` を最初に押して `drop database` コマンドを終了せずにスクラッチ・データベースのログをトランケートしようとする、`drop` コマンドにより取得されたロックが原因でトランケートがサスペンドされます。

アーカイブ・データベースの使用

この項では、アーカイブ・データベースで実行可能なコマンドについて説明します。

アーカイブ・データベースでの SQL コマンドの使用

すでに説明したコマンド (`alter database`、`load database`、`online database`、および `drop database`) に加えて、アーカイブ・データベースでは次の SQL コマンドを使用できます。

- `use`
- `select`
- `select into` – ターゲット・データベースがアーカイブ・データベースでない場合に使用する。
- 読み取りを実行するカーソル処理。次のコマンドが含まれる。
 - `declare cursor`
 - `deallocate cursor`
 - `open`
 - `fetch`更新可能カーソルは使用できない。
- `checkpoint` – サポートされるコマンド。ただし、アーカイブ・データベースはチェックポイント処理により自動的にチェックポイントを実行されない。
- `execute` – アーカイブ・データベースを参照する文がアーカイブ・データベース内で使用可能であれば、実行できる。ストアード・プロシージャ内部または外部でのトランザクションは、`execute` コマンドでは使用できない。
- `lock table`
- `readtext`

注意 `insert`、`update`、および `delete` などの DML コマンドは使用できず、ユーザ・トランザクションを開始できません。

アーカイブ・データベースでの dbcc コマンドの使用

アーカイブ・データベースでは、次の dbcc コマンドを使用できます。

- checkdb
- checkcatalog

注意 checkcatalog の fix バージョンはサポートされていません。

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

dbcc コマンドの実行中は、他のユーザがアーカイブ・データベースにアクセスすることはできません。dbcc コマンドの実行中にアーカイブ・データベースにアクセスしようとする、データベースがシングルユーザ・モードになっていることを示すメッセージが表示されます。

上記の dbcc コマンドの変形は、アーカイブ・データベースがオンラインでもオフラインでも使用できます。ただし、fix オプションが設定された dbcc コマンドは、オンラインのアーカイブ・データベースでのみ使用できます。

一般的なアーカイブ・データベース・コマンドの順序

次の構文は、一般的なアーカイブ・データベース・コマンドの順序です。

まず、必要な場合は create database コマンドを使用してスクラッチ・データベースを作成します。

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

これにより、scratchdb という名前の 150 MB の従来のデータベースが作成されます。

sp_dboption を使用して、上の手順で作成したデータベースをスクラッチ・データベースとして指定します。

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

アーカイブ・データベースを作成します。

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

これにより、20 MB の変更済みページ・セクションが含まれる、**archivedb** という名前のアーカイブ・データベースが作成されます。

load database を使用して、アーカイブ・データベースをマテリアライズします。

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

データベースをオンラインにします。

```
online database archivedb
```

dbcc コマンドを使用して、アーカイブ・データベースの一貫性を検査します。次に例を示します。

```
dbcc checkdb(archivedb)
```

select into コマンドまたは **bcp** コマンドを使用すると、オブジェクトをアーカイブ・データベースからリストアできます。たとえば、**orders** というテーブルをアーカイブ・データベースからリストアするには、次のコマンドを使用します。

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

アーカイブ・データベースのセキュリティとパーミッション

コマンドとストアド・プロシージャを実行するパーミッション、およびアーカイブ・データベースのオブジェクトへのアクセス権は、同じサーバ上の同じデータベース・ダンプとともにロードされた従来のデータベースのものと同じです。

with norecovery を使用してアーカイブ・データベースがロードされる場合、そのデータベースへのアクセス権は **sa_role** を持つユーザまたはデータベース所有者に制限されます。

アーカイブ・データベースの圧縮ダンプ

アーカイブ・データベースの圧縮ダンプを使用するには、次の操作を行う必要があります。

- `dump database` コマンドの `with compression = <compression level>` オプションを使用して、圧縮ダンプを作成する。
- アーカイブ・データベースにアクセスするためのメモリ・プールを作成する。

注意 “compress:” を使用して生成されたダンプは、アーカイブ・データベースにロードできません。そのため、この章で圧縮に言及している場合は、`with compression = <compression level>` オプションを使用して生成されたダンプのことを指しています。

圧縮ロジックは、バージョン 12.5.4 で変更されました。互換性の問題の詳細については、「[圧縮ダンプの互換性の問題](#)」(69 ページ) を参照してください。

圧縮メモリ・プールの作成

Adaptive Server は、圧縮ダンプからページを読み込むとき、ダンプから圧縮されたブロックを選択してその圧縮を解除し、必要なページを抽出します。Adaptive Server での圧縮解除は、特別メモリ・プールのバッファより大きいバッファを使用して行われます。プールのサイズは、次のコマンドを使用して設定します。

```
sp_configure 'compression memory size', <size>
```

これは、動的な設定パラメータで、サイズは 2KB のページで指定されます。サイズが 0 に設定された場合、プールは作成されず、圧縮ダンプをロードできません。

プールに最適なサイズを判断するには、次の 2 つの要素について考慮します。

- Backup Server により使用されるブロック I/O。デフォルトでは、このブロック I/O は 64KB だが、`dump database` コマンドで `with blocksize` オプションを使用して変更できる。
- すべてのアーカイブ・データベース内のブロックを圧縮解除する「同時」ユーザの数。各同時ユーザには、ブロック I/O と同じサイズごとに 2 つのバッファが必要。

絶対最小値として、アーカイブ・データベースごとに 1 人の同時ユーザ (2 つのバッファ) を許可します。

アーカイブ・データベースのマイグレート

サーバ全体をマイグレートする場合、`sybmigrate` を実行してもアーカイブ・データベースはマイグレートされません。

`sybmigrate` は、アーカイブ・データベースがマイグレーション対象として明確に選択されている場合のみ、アーカイブ・データベースをマイグレートします。アーカイブ・データベースをターゲット・サーバにマイグレートすると、`sybmigrate` によりターゲット・サーバにはアーカイブ・データベースではなく従来のデータベースが作成されます。

アーカイブ・データベースのアップグレードとダウングレード

この項では、アーカイブ・データベースのアップグレードおよびダウングレードの方法について説明します。

アーカイブ・データベースが含まれる Adaptive Server のアップグレード

アーカイブ・データベースはアップグレードできません。データベース・ダンプを以前のバージョンの Adaptive Server から、新しいバージョンの Adaptive Server に保持されているアーカイブ・データベースにロードした場合、`online database` コマンドが実行されるときにデータベースは内部ではアップグレードされません。

アーカイブ・データベースが含まれる Adaptive Server をアップグレードした場合、アーカイブ・データベースを除くすべてのデータベースがアップグレードされます。アーカイブ・データベースは、古いバージョンの Adaptive Server のままになります。

すでにアップグレードされたデータベースから生成されたダンプを使用して、アーカイブ・データベースを再ロードすることをおすすめします。

Adaptive Server のアップグレード方法の詳細については、使用しているプラットフォームの『インストール・ガイド』を参照してください。

アーカイブ・データベースが含まれる Adaptive Server のダウングレード

アーカイブ・データベースがサポートされないバージョンの Adaptive Server にダウングレードするときは、次の点に注意してください。

- アーカイブ・データベースを含む Adaptive Server を、アーカイブ・データベースがサポートされないバージョンの Adaptive Server にダウングレードする場合は、ダウングレードする前にアーカイブ・データベースを削除することが推奨される。

新しい `sysaltusages` テーブルを消去するには、ダウングレード手順を実行する前にスクラッチ・データベースを削除する。スクラッチ・データベースが削除された場合は、`sysaltuages` により問題が発生することはない。

- Backup Server バージョン 12.5.4 は、ダンプをアーカイブ・データベースにロードできるように、圧縮を新しいフォーマットで書き込む (`with compression = <compression level>`)。そのため、アーカイブ・データベースのアクセスがサポートされないバージョンの Adaptive Server に圧縮ダンプをロードする必要がある場合は、圧縮ダンプが作成されたのと同じバージョンの Backup Server を使用して圧縮データベース・ダンプをロードする。以前のバージョンの Backup Server では、新しいフォーマットの圧縮データベース・ダンプはサポートされない。

圧縮せずにダウングレードする場合は、Backup Server に関する注意は不要です。

圧縮ダンプの互換性の問題

- “`compress::`” を使用して生成されたダンプは、アーカイブ・データベースにロードできない。従来のデータベースでこの圧縮オプションを使用する場合、ダンプに関する互換性の問題は発生しない。
- `with compression = <compression level>` オプションを使用して生成された圧縮ダンプのフォーマットが変更された。Backup Server バージョン 12.5.4 は、新しい圧縮フォーマットで書き込むコンポーネント。そのため、次の結果が生じる。
 - Backup Server バージョン 12.5.4 を使用して生成された圧縮ダンプは、Backup Server 12.5.4 以降を使用する 12.5.3 以前のサーバにのみロードできる。
 - 12.5.3 以前のサーバを使用していて、アーカイブ・データベースにダンプを使用する場合は、バージョン 12.5.4 の Backup Server を使用して圧縮データベース・ダンプを作成する。

注意 Backup Server 12.5.4 は、12.5.4 の圧縮フォーマットとそれより前の圧縮フォーマットの両方を認識できるため、どちらのダンプおよびロードにも使用できます。

アーカイブ・データベースのアクセスの DDLGen サポート

すべてのアーカイブ・データベースの DDL を生成するには、拡張フィルタ・オプション“OA”を使用します。

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

1つのアーカイブ・データベースの DDL を生成するには、標準的なデータベースの構文を使用します。次の例では、アーカイブ・データベース `archivedb` の DDL を作成します。

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

アーカイブ・データベースの制限

アーカイブ・データベースには、次の制限があります。

- アーカイブ・データベースは読み込み専用。
- アーカイブ・データベースに変更を加えるコマンド (`dbcc` コマンドなど) を実行すると、アーカイブ・データベースは自動的にシングルユーザ・モードになる。
- アーカイブ・データベースでは、ディスク上のデータベース・ダンプのみを使用する。テープ・ダンプはサポートされない。
- データベース・ダンプは、アーカイブ・データベースを持つサーバからアクセス可能である必要がある。リモート・ダンプはサポートされない。
- `load tran` は、Adaptive Server バージョン 12.5.4 ではサポートされない。
- `dbcc checkstorage` は、Adaptive Server バージョン 12.5.4 ではサポートされない。
- アーカイブ・データベースが圧縮ダンプにアクセスするには、ダンプが“`compress::`” オプションではなく `with compression` オプションを使用して作成されている必要がある。
- チェックポイント処理では、アーカイブ・データベースに対してチェックポイントが自動的に実行されない。アーカイブ・データベースにチェックポイントを実行するには、`checkpoint` コマンドを使用する。
- データベース・リカバリ・シーケンスで、`sp_dbrecovery_order` を使用してアーカイブ・データベースを指定することはできない。アーカイブ・データベースは、`dbid` 順の最後にリカバリされる。
- ページがアーカイブ・データベースにキャッシュされると、キャッシュされたページは、サーバと同じページ・サイズでメモリ・プール内にとどまる。つまり、2K のサーバでは、ページは常に 2K のプールにキャッシュされる。16K のサーバでは、ページは常に 16K のプールにキャッシュされる。

- アーカイブ・データベースおよびデータベース内のオブジェクトは、ユーザ定義キャッシュにバインドすることはできない。アーカイブ・データベース内のオブジェクトのデフォルトは、デフォルトのデータ・キャッシュに設定される。
- **disk resize** は、アーカイブ・データベースにより使用されるデバイス、またはデータベース・ダンプやトランザクション・ログにマップされるデバイスでは機能しない。
- **disk refit** を実行しても、**master** データベースの **sysusages** エントリは、アーカイブ・データベースによって使用されるデバイスから再構築されない。これは、ダンプ・デバイスと、変更済みページ・セクションに使用されるデバイスの両方に該当する。ただし、アーカイブ・データベースの既存の **sysusages** エントリは残る。
- アーカイブ・データベースは複写できない。
- アーカイブ・データベースは、高可用性サーバではフェイルオーバーされない。
- アーカイブ・データベースでは、空き領域スレッショルドを確立できない。

共有ディレクトリの変更

Adaptive Server バージョン 12.5.4 では、共有ディレクトリ構造に以下の変更が加えられています。

共有ディレクトリの変更

Adaptive Server バージョン 12.5.4 では、共有ディレクトリ構造に多くの変更が行われました。表 4-1 にディレクトリを示します。

表 4-1: UNIX および Linux プラットフォームの共有ディレクトリ構造の変更

コンポーネント	以前のロケーション	新しいロケーション
共有ディレクトリ	<code>\$\$SYBASE/shared-1_0</code>	<code>\$\$SYBASE/shared</code>
Sybase Central	<code>\$\$SYBASE/sybcnt41</code>	<code>\$\$SYBASE/shared/sybcnt43</code>
JRE	<code>\$\$SYBASE/shared-1_0/JRE-1_3</code>	<code>\$\$SYBASE/shared/jre142</code>
共有 JAR ファイル	<code>\$\$SYBASE/shared-1_0/lib</code>	<code>\$\$SYBASE/shared/lib</code>

表 4-2: Microsoft Windows プラットフォームの共有ディレクトリ構造の変更

コンポーネント	以前のロケーション	新しいロケーション
共有ディレクトリ	<code>%SYBASE%\%shared-1_0</code>	<code>%SYBASE%\%Shared</code>
Sybase Central	<code>%SYBASE%\%sybcnt41</code>	<code>%SYBASE%\%Shared%\Sybase Central 4.3</code>
JRE	<code>%SYBASE%\%shared-1_0\JRE-1_3</code>	<code>%SYBASE%\%Shared%\Sun\jre142</code>
共有 JAR ファイル	<code>%SYBASE%\%shared-1_0\lib</code>	<code>%SYBASE%\%Shared\lib</code>

注意 すべての Adaptive Server コンポーネントが変更されて新しい構造を使用するようになりました。

Adaptive Server には、この変更によって影響を受ける次の Java アプリケーションが含まれています。

- Sybase Central
- ASE Plug-in
- DDLGen
- ASE Replicator
- Web Services Producer および Web Services Consumer

- SQL デバッガ
- マイグレーション・ツール
- Job Scheduler

Sybase によるドライバのサポート

Adaptive Server バージョン 12.5.4 には、Sybase が開発した新しい ODBC および OLE DB ドライバが含まれています。Adaptive Server の以前のバージョンに含まれていた、OEM のサード・パーティ ODBC および OLE DB ドライバ・キットは、現在は付属していません。付属しなくなったドライバのサポートは、後述のスケジュールで継続されます。

以前の ODBC ドライバ・キットは %SYBASE%\%ODBC にインストールされ、ODBC ドライバ・マネージャに “Sybase ASE ODBC Driver” として登録されていました。Sybase 製の新しい ASE ODBC ドライバは、%SYBASE%\%DataAccess%\%ODBC にインストールされ、“Adaptive Server Enterprise” として登録されます。Adaptive Server バージョン 12.5.4 に付属しているのは、バージョン 12.5.1.510 です。

以前の OLE DB ドライバ・キットは、%SYBASE%\%OLEDB にインストールされ、プロバイダの短い名前 “Sybase.ASEOLEDBProvider” および長い名前 “Sybase ASE OLE DB Provider” を使用していました。Sybase 製の新しい ASE OLE DB プロバイダは %SYBASE%\%DataAccess%\%OLEDB にインストールされ、プロバイダの短い名前 “ASEOLEDB” を使用します。Adaptive Server バージョン 12.5.4 に付属しているのは、バージョン 12.5.1.510 です。

継続的にサポートされているサード・パーティのドライバ

すでにサード・パーティの ODBC ドライバおよび OLE DB プロバイダを使用していて、サポート契約が有効な既存のユーザは、ASE 12.5 のサポート期間中は、これらの製品のサポートを継続的に受けることができます。

サポート・プログラムは、2007 年 7 月 30 日まで現在と同様に継続されません。2007 年 7 月 30 日以降は、P1 (重大度レベル 1) の問題にのみ対応します。これらのドライバに対する新しい更新は、スタンドアロン・ダウンロードとしてのみ配布されます。

現在所有している ODBC ドライバおよび OLE プロバイダは、ASE 12.5.3 およびそれ以前の ASE 機能のみをサポートするため、注意が必要です。Sybase は、これらのドライバの問題が ASE 12.5.3 で再現できる場合のみ対応します。ASE 12.5.3 以降の ASE のリリースでサード・パーティ製品を使用している場合、Sybase では問題の特定や修正のサポートを行えない場合があります。

これらのドライバのサポート終了通知については、Sybase の Web サイト (<http://www.sybase.com/detail?id=1040652>) を参照してください。

新しいドライバへのマイグレート

できるだけ早く新しい ODBC および OLE DB ドライバへのマイグレーション・プロセスを開始することをおすすめします。サード・パーティのドライバでは、Adaptive Server バージョン 12.5.4 およびそれ以降に追加される Adaptive Server の機能がサポートされません。

新しいドライバへのマイグレーション方法については、「新機能 OpenServer 12.5.1 と SDK 12.5.1 Microsoft Windows、Linux、および UNIX 版」を参照してください。

TIBCO ライブラリの動的ロード

Adaptive Server 12.5.4 では、動的にロードされる TIBCO JMS ライブラリのサポートが導入されています。

Adaptive Server メッセージング・ライブラリの動的ロード

Adaptive Server version 12.5.4 では、TIBCO EMS および IBM MQ メッセージ・バスと対話するために必要なメッセージング・ライブラリを動的にロードします。

Adaptive Server メッセージング・ライブラリにはメッセージ・ロジックが含まれ、これは、TIBCO や IBM などのベンダが提供するメッセージ・ライブラリの上に存在するラップアとして機能します。これらの Adaptive Server メッセージング・ライブラリは、RTDS 3.5 およびそれ以上のバージョンを購入すると使用できます。Adaptive Server をインストールした後に、Adaptive Server メッセージング DLL をインストールするには、RTDS 3.5 をインストールする必要があります。これらのライブラリは、`$SYBASE/ASE-12_5/lib` ディレクトリにインストールします。

Adaptive Server メッセージング・ライブラリに加え、ベンダ (TIBCO および IBM) が提供するメッセージング・ライブラリおよび DLL も必要です。

Adaptive Server メッセージング・ライブラリおよびベンダ固有のメッセージ・バス・ライブラリをインストールしたら、`LD_LIBRARY_PATH` または等価の設定をこれらのライブラリのロケーションに変更します。

Adaptive Server メッセージング・ライブラリは、デフォルトで `$SYBASE/ASE-12_5/lib` にあります。

`LD_LIBRARY_PATH` または等価の設定に、ベンダが提供する DLL のロケーションを追加する必要もあります。

TIBCO JMS DLL ロケーション情報

TIBCO EMS バージョン 4.2 または 4.3 がインストールされているロケーションを TIBCO_HOME とした場合、プラットフォーム固有のパスは次のとおりです。

- Solaris 32 ビット・プラットフォームでは、*\$TIBCO_HOME/clients/c/lib* を LD_LIBRARY_PATH に追加する。
- Solaris 64 ビット・プラットフォームでは、次を LD_LIBRARY_PATH に追加する。
 - *\$TIBCO_HOME/clients/c/lib/64*
 - *\$TIBCO_HOME/clients/c/lib*
- Linux 32 ビット・プラットフォームでは、*\$TIBCO_HOME/clients/c/lib* を LD_LIBRARY_PATH に追加する。
- Windows 32 ビット・プラットフォームでは、*%TIBCO_HOME%\clients%c%bin* を PATH に追加する。
- HP-UX 64 ビット・プラットフォームでは、次を LD_LIBRARY_PATH に追加する。
 - *\$TIBCO_HOME/clients/c/lib/64*
 - *\$TIBCO_HOME/clients/c/lib*
- IBM AIX 64 ビット・プラットフォームでは、次を LIBPATH に追加する。
 - *\$TIBCO_HOME/clients/c/lib/64*
 - *\$TIBCO_HOME/clients/c/lib*

IBM MQ DLL の LD_LIBRARY_PATH への追加

MQ クライアント・ライブラリがインストールされているロケーションを MQM_HOME とした場合、プラットフォーム固有のパスは次のとおりです。

- Solaris 32 ビット・プラットフォームでは、*\$MQM_HOME/lib* を LD_LIBRARY_PATH に追加する。
- Solaris 64 ビット・プラットフォームでは、*\$MQM_HOME/lib64* を LD_LIBRARY_PATH に追加する。
- Linux 32 ビット・プラットフォームでは、*\$MQM_HOME/lib* を LD_LIBRARY_PATH に追加する。
- Windows 32 ビット・プラットフォームでは、*%MQM_HOME%\bin* を PATH に追加する。
- HP-UX 64 ビット・プラットフォームでは、*\$MQM_HOME/lib64* を LD_LIBRARY_PATH に追加する。

- IBM AIX 64 ビット・プラットフォームでは、`$MQM_HOME/lib64` を `LIBPATH` に追加する。

注意 `MQM_HOME` は、Solaris、Linux および HP-UX の場合は `/opt/mqm`、IBM AIX の場合は `/usr/mqm` です。Windows の場合は、Websphere MQ がインストールされているディレクトリになります。

また、`sp_configure 'enable real time messaging'` が変更されて、有効にするメッセージングのタイプを指定できるようになりました。

- `sp_configure 'enable real time messaging', 1` の場合は、TIBCO JMS および IBM MQ の両方のメッセージングが有効になる。このコマンドは、Adaptive Server が TIBCO JMS および IBM MQ に対応する DLL を見つけることができた場合に成功する。
- `sp_configure 'enable real time messaging', 1, 'tibco_jms'` の場合は、TIBCO JMS のメッセージングだけが有効になる。このコマンドは、Adaptive Server が TIBCO JMS に対応する DLL を見つけることができた場合に成功する。
- `sp_configure 'enable real time messaging', 1, 'ibm_mq'` の場合は、IBM MQ のメッセージングだけが有効になる。このコマンドは、Adaptive Server が IBM MQ に対応する DLL を見つけることができた場合に成功する。

Adaptive Server 12.5.4 での JRE サポート

Adaptive Server バージョン 12.5.4 には、Java Runtime Environment (JRE) 1.4 が含まれます。JRE 1.4 は、完全インストールおよび標準インストールではデフォルトでインストールされます。また、カスタム・インストールでは、実行するために JRE が必要なコンポーネントが選択されるとインストールされます。

Adaptive Server プラグインのサポート

Sybase Central Adaptive Server プラグインは、Adaptive Server バージョン 12.5.4 のアーカイブ・データベース・アクセスと、複雑なパスワードの設定オプションをサポートします。

Sybase Central Adaptive Server プラグインを使用して、アーカイブ・データベースを管理します。データベース・フォルダの下にアーカイブ・データベースと呼ばれる新しいフォルダがあります。

Sybase Central Adaptive Server プラグインを使用して、サーバ・プロパティ・シートから Adaptive Server に複雑なパスワードを設定します。Adaptive Server バージョン 12.5.4, には、サーバ・プロパティ・シートに [Login Password Configuration] という新しいタブがあります。

Adaptive Server プラグインを使用してアーカイブ・データベースのアクセスを管理するための詳細については、『Adaptive Server Enterprise の管理』の「Adaptive Server へのアクセス制御」を参照してください。プラグインを使用して複雑なパスワードを設定するオプションについては、『Adaptive Server Enterprise の管理』の「第 7 章 データベースの管理」を参照してください。

モニタリング・テーブルの変更

Adaptive Server 12.5.4 では、モニタリング・テーブルに以下の変更が行われました。

変更されたモニタリング・テーブル

表 9-1 は、モニタリング・テーブルの更新について説明しています。

表 9-1: モニタリング・テーブルの更新

カラム名	モニタリング・テーブル	説明
RowsAffected	monSysStatement と monProcessStatement	現在の文によって影響を受けるロー数を示します。効率の低いクエリ・プランを使用するクエリを検索するときに便利です。このようなクエリを使用すると、返される各ローに対して多数の論理 I/O が生じることがあります。

Windows Terminal Server 環境での共有メモリ

Windows Terminal Server 環境で実行される Adaptive Server 共有メモリ

Windows Terminal Server の共有メモリ要件に対応するために、Adaptive Server バージョン 12.5.4 では新しい環境変数 SYBASE_TS_MODE を導入しました。

Windows Terminal Server は、複数のリモート・ユーザが Windows システムに同時にログインできるようにする、Microsoft Windows の機能です。各ユーザがローカルのワークステーションから中央の Windows サーバに接続すると、ローカルのワークステーションの表示を示す仮想の Windows 環境が提供されます。Windows サーバは、これらの Terminal Server セッションのメモリ領域およびその他のリソース割り当てを完全に個別に維持するため、ユーザの多くは、他の Terminal Server セッションの存在には気づきません。また、ユーザは通常の方法でマシンにログインできるので、これは「コンソール・セッション」と呼ばれます。

Adaptive Server データ・サーバは Terminal Server セッションで起動するか、Windows サービスとして起動できます。後者の場合は、コンソール・セッションの一部とみなされます。通常、Adaptive Server の共有メモリ領域は他の Terminal Server からアクセスできないため、パフォーマンス・モニタなどの特定のツールと Sybase の内部診断ツール (sybmon) は、Adaptive Server を所有する同じセッションから起動しない限り機能せず、これらのツールはそのサーバの共有メモリ領域に接続する必要があります。Adaptive Server がサービスとして実行している場合は、コンソール・セッションから起動した場合に限りこれらのツールは機能します。

Adaptive Server 12.5.4 は環境変数 SYBASE_TS_MODE を探し、この環境変数が GLOBAL に設定されている場合は、その共有メモリを作成して、すべての Terminal Server セッションで使用できるようにします。同様に、パフォーマンス・モニタと sybmon に加えられた変更もこの環境変数を探して、GLOBAL に設定されている場合は共有メモリに接続します。この方法では、コンソール・セッションまたは別の Terminal Server セッションで実行されている Adaptive Server を監視できるようにリモートの Terminal Server セッションを設定できます。SYBASE_TS_MODE は通常、システム環境変数として作成され、Windows マシンを再起動すると有効になります。

SYBASE_TS_MODE は、Windows NT 4.0 Workstation および Server、および Windows 2000 Professional ではサポートされません。

この変数を設定しない場合、デフォルトでは、ローカルの Terminal Server セッションでのみ共有メモリが作成されます。

警告！ SYBASE_TS_MODE は、Terminal Server をサポートしないマシンには設定しないでください。設定すると、共有メモリの作成は失敗し、Adaptive Server は起動しません。

Adaptive Server Enhancements Linux プラットフォーム版

この章では、Adaptive Server Linux プラットフォーム版の拡張機能について説明します。

トピック名	ページ
ラージ・メモリ・サポート拡張機能	89
DIRECTIO サポート	89
ラージ・メモリ・サポートと POSIX Async I/O	89

ラージ・メモリ・サポート拡張機能

ラージ・メモリ・サポートを使用すると、extended cache size 設定パラメータを 0 以外の値に設定できます。

Adaptive Server の以前のバージョンでは、プライマリ・データ・キャッシュ内の最小 I/O メモリ・プールのウォッシュ・サイズは固定値でした。設定値はすべて無効にされていました。

Adaptive Server バージョン 12.5.4 では、プライマリ・データ・キャッシュ内の最小 I/O メモリ・プールのウォッシュ・サイズを設定できます。

DIRECTIO サポート

Adaptive Server バージョン 12.5.4 は、ファイル・システム・デバイスで DIRECTIO をサポートしません。

ラージ・メモリ・サポートと POSIX Async I/O

Adaptive Server バージョン 12.5.4 は、POSIX Async I/O を使用するように設定された Linux プラットフォームで、ラージ・メモリ・サポートをサポートします。

ストアド・プロシージャ、関数、 コマンドの変更

この章では、他では説明されていない Adaptive Server バージョン 12.5.4 の主な変更点を示します。

トピック名	ページ
shutdown の新しい構文	91
select * 構文の拡張	93
dump database と load database での検証	93
システム・カタログの更新の許可	94
数値データ型のモジュロ算術	94
IPv6 IP アドレス要件をサポートする新しい関数	94
外部トランザクションを復号化する関数	95

shutdown の新しい構文

Adaptive Server バージョン 12.5.4 では、shutdown に次のような新しい構文が使用されています。

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

パラメータ

srvname

Adaptive Server の `sys.servers` システム・テーブルで Backup Server を認識する論理名です。このパラメータは、ローカル Adaptive Server を停止する場合は不要です。

with wait

デフォルトです。このオプションは、Adaptive Server または Backup Server を停止します。

hh:mm:ss

実行中またはスリープ中のすべてのプロセスがジョブを終了するまでにサーバが待つ最大時間を指定します。この設定は省略可能です。

with nowait

現在実行している文の終了を待たずに、Adaptive Server または Backup Server をただちに停止します。

注意 shutdown with nowait を使用すると、IDENTITY カラムの値にギャップが発生する可能性があります。

待ち時間の指定

サーバを停止する準備ができると、次が実行されます。

- 1 すべてのデータベースでチェックポイントを実行します。
- 2 新しいユーザがログインできないようにします。
- 3 実行中のプロセスまたはスリープ中のプロセスのジョブが終了されるまで待ちます。
- 4 データベースに別のチェックポイント・タスクを実行します。今回は、フラッシュする必要のある以下の項目にフラグを追加します。
 - 混合ログデータ・データベースにあるすべての動的スレッシュホールド
 - すべてのオブジェクト統計
 - リカバリ後の欠損を避けるための identity フィールドの値

with wait オプションと *hh:mm:ss* オプションを一緒に使用する場合、指定する時間は、Adaptive Server 自体を停止するために与えられる最大合計時間になりません。Adaptive Server は、最初のチェックポイントを実行するためにかかる時間を計算し、指定された時間からこの値を自動的に差し引きます。

たとえば、最大待ち時間を 20 分に指定し、最初のチェックポイントの実行に 3 分かかった場合、Adaptive Server はプロセスの終了を最大 17 分まで待ちます。ただし、何らかの理由で 2 回目のチェックポイントの実行時間が長くなった場合、この値は指定する with wait の *hh:mm:ss* パラメータからは差し引かれません。

また、チェックポイントでは with wait の *hh:mm:ss* で指定したよりも長い時間を使用できます。たとえば、待ち時間を 10 分に指定し、最初のチェックポイントを完了するのに 20 分かかる場合、Adaptive Server はチェックポイントを中断せずに完了するまで待ちます。この場合、チェックポイントが完了した時点で指定した時間が過ぎているため、Adaptive Server はただちに停止処理を開始し、フラッシュする項目を示すフラグを追加する最後のチェックポイントを実行します。

select * 構文の拡張

ストアド・プロシージャまたはトリガのソース・テキストがシステム・テーブル `syscomments` に格納される場合、`select *` を使用するクエリは、`select *` で参照されるカラム・リストを拡張する `syscomments` に格納されます。

たとえば、カラム `col1` と `col2` を含むテーブルの `select *` は、次のように格納されます。

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

12.5.4 では、識別子 (テーブル名、カラム名など) が識別子のルールに準じているかどうかを確認するよう、カラム・リストの拡張が強化されました。

たとえば、カラム `col1` と `2col` を持つテーブルがあるとします。2 番目のカラム名は番号で開始しますが、`create table` ステートメントで角カッコを使用した場合のみ、このようになります。これらは、角カッコの付いた識別子です。

そのテーブルから、ストアド・プロシージャまたはトリガで `select *` を実行すると、`syscomments` 内のテキストは次のようになります。

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

`select *` を拡張したテキストで使用されるすべての識別子で、識別子が識別子のルールに従わない場合は角カッコが追加されます。

最新リリースにアップグレードしても Adaptive Server が SQL テキストを使用できるように、識別子の前後に角カッコを追加します。

dump database と load database での検証

Adaptive Server 12.5.4 の `dump database` コマンドと `load database` コマンドに、データベースをダンプおよびロードするときに検証を行うオプションが導入されました。`dump database` の構文は次のとおりです。

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

`load database` の構文は次のとおりです。

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

`dump database` を実行すると、Backup Server は、アーカイブにコピーするデータ・ページに対して最小限のヘッダ検査またはロー構造検査を実行します。現時点では、GAM ページ、OAM ページ、アロケーション・ページ、インデックス・ページ、テキスト・ページ、ログ・ページへの構造検査は実行されません。

`load with verify[only]` コマンドを使用してアーカイブをロードすると、同じ検査を実行できます。

`load database with verify[only]` コマンドを使用すると、アーカイブを物理的にロードしなくても検査できます。このオプションでは、`with headeronly` のロード・オプションと同様のダンプ・ヘッダ情報が表示されます。

システム・カタログの更新の許可

サーバ全体の設定オプション `allow updates to system catalogs` は、ストアド・プロシージャ設定 `allow updates` よりも優先されます。サーバ全体で有効でない場合、ストアド・プロシージャ設定によりシステム・ログを変更できるかどうかが決まります。

数値データ型のモジュロ算術

Adaptive Server バージョン 12.5.4 では、実数、浮動小数点、小数、数値にも整数と同様のモジュロ算術が実行できます。

IPv6 IP アドレス要件をサポートする新しい関数

IPv6 アーキテクチャでは、IP アドレスの長さは 64 バイトです。sysprocesses のサイズは増加できないため、完全な IP アドレスを取得する方法が必要とされました。Adaptive Server バージョン 12.5.4 には、pss からの情報を返す以下の新しい関数が導入されています。

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

各パラメータの意味は、次のとおりです。

- *spid* – プロセス ID。0 を指定すると現在のプロセスが使用されます。
- *pss field* – 有効な値は以下のとおりです。
 - *ipaddr* – クライアントの IP アドレス
 - *extusername* – PAM や LDAP のような外部認証を使用する場合、使用される外部 PAM ユーザ名または LDAP ユーザ名を返す。
 - *dn* – LDAP 認証を使用する場合の識別名。

pssinfo 関数には、外部ユーザ名と識別名を表示するオプションもあります。

外部トランザクションを復号化する関数

Adaptive Server バージョン 12.5.4 には、外部トランザクションを復号化する 2 つの関数が追加されています。それぞれの詳細は次のとおりです。

xa_bqual

- 説明** ASCII XA トランザクション ID の bqual コンポーネントのバイナリ・バージョンを返します。
- 構文** `xa_bqual(xid, 0)`
- パラメータ** `xid`
`systransactions` の `xactname` カラム、または `sp_transactions` で取得される Adaptive Server トランザクションの ID です。
- 0**
 今後のために予約済みです。
- 例** **例 1** Adaptive Server トランザクション ID “0000000A_IphIT596iC7bF2#AUfkzaM_8DY6OE0” の分岐修飾子をバイナリ変換した “0x227f06ca80” を返します。Adaptive Server トランザクション ID は、最初は `sp_transactions` を使用して次のように取得されます。

```
1> sp_transactions

xactkey          type      coordinator starttime      state
connection dbid  spid  loid  failover  srvname  namelen  xactname
-----
-----
0x531600000600000017e4885b0700 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
```

例 2 `xa_bqual` は、`xa_grid` と一緒に使用されることが多くあります。この例は、`systransactions` のすべてのローからグローバル・トランザクション ID と分岐修飾子を返します。`coordinator` カラムの値は “3” です。

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

```
2> go
```

```
gtrid
```

```
bqual
```

```
-----  
-----  
  
0xb1946cdc52464a61cba42fe4e0f5232b
```

```
0x227f06ca80
```

使用法

Adaptive Server で外部トランザクションがブロックされており、ブロックされているトランザクションを `sp_lock` および `sp_transactions` を使用して識別する場合、XA トランザクション・マネージャを使用してグローバル・トランザクションを終了させることができます。ただし、`sp_transactions` を実行する場合、返される *xactname* の値は ASCII 文字列フォーマットです。一方、XA Server は、復号化されていないバイナリ値を使用します。`xa_bqual` を使用することにより、XA トランザクション・マネージャが解読できる形式のトランザクション名の `bqual` 部分を特定できます。

`xa_bqual` は、以下を返します。

- 2 番目の “_” (アンダースコア) より後にあり、3 番目の “_” または end-of-string 値のうち先に出現した方の前にある、この文字列の変換バージョン。
- トランザクション ID が復号化できないか予想外の形式の場合は NULL。

注意 `xa_bqual` は、`xid` に対して検証チェックを実行せず、単に変換された文字列を返します。

標準

ANSI SQL – 準拠レベル：Transact-SQL 拡張機能

パーミッション

すべてのユーザは、`xa_bqual` を使用できます。

参照

関数 `xa_gtrid`

ストアド・プロシージャ – `sp_lock`、`sp_transactions`

xa_gtrid

説明 ASCII XA トランザクション ID の `gtrid` コンポーネントのバイナリ・バージョンを返します。

構文 `xa_gtrid(xactname, 0)`

パラメータ `xactname`
`systransactions` の `xactname` カラム、または `sp_transactions` で取得される Adaptive Server トランザクションの ID です。

0

今後のために予約済みです。

例 **例 1** 一般的な状況では、Adaptive Server トランザクション ID “0000000A_IphIT596iC7bF2#AUfkzaM_8DY6OE0” に対して “0x227f06ca80” (分岐修飾子のバイナリ変換)、“0xb1946cdc52464a61cba42fe4e0f5232b” (グローバル・トランザクション ID) が返されます。

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

...

```
-----
0xb1946cdc52464a61cba42fe4e0f5232b
```

(1 row affected)

例 2 `xa_bqual` は、`xa_gtrid` と一緒に使用されることが多くあります。この例は、`systransactions` のすべてのローからのグローバル・トランザクション ID と分岐修飾子を返します。`coordinator` カラムの値は “3” です。

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

```
gtrid
```

```
bqual
```

```
-----
0xb1946cdc52464a61cba42fe4e0f5232b
```

```
0x227f06ca80
```

使用法

Adaptive Server で外部トランザクションがブロックされており、ブロックされているトランザクションを `sp_lock` および `sp_transactions` を使用して識別する場合、XA トランザクション・マネージャを使用してグローバル・トランザクションを終了させることができます。ただし、`sp_transactions` を実行する場合、返される `xactname` の値は ASCII 文字列フォーマットです。一方、XA Server は、復号化されていないバイナリ値を使用します。`xa_gtrid` を使用することにより、XA トランザクション・マネージャが解読できる形式のトランザクション名の `gtrid` 部分を特定できます。

`xa_gtrid` は、以下を返します。

- 最初の “_” (アンダースコア) より後にあり、2 番目の “_” または end-of-string 値のうち先に出現した方の前にある、この文字列の変換バージョン。
- トランザクション ID が復号化できないか予想外の形式の場合は NULL。

注意 `xa_gtrid` は、`xid` に対して検証チェックを実行せず、単に変換された文字列を返します。

標準

ANSI SQL – 準拠レベル：Transact-SQL 拡張機能

パーミッション

すべてのユーザは、`xa_gtrid` を使用できます。

参照

関数 [xa_bqual](#)

ストアド・プロシージャ – `sp_lock`、`sp_transactions`

索引

A

- Adaptive Server のプリンシパル名 7
- Adaptive Server プラグイン 83
 - 複雑なパスワード 49
- Adaptive Server プリンシパル名 7
- alter database 60, 64
- alter table
 - および暗号化カラム 33
- authenticate with 9

D

- dbcc コマンド (dbcc commands)
 - アーカイブ・データベースへのアクセス 65
- DDLGen
 - アーカイブ・データベースのアクセスのサポート 70
- drop database 64

H

- Historical Server 4

J

- JRE 1.4 のサポート 81

K

- k オプション 8
- Kerberos サポート
 - authenticate with 9
- Kerberos による認証 7
 - 確認 14
- Kerberos 認証の確認 14

L

- LDAP UA 用の Adaptive Server の設定 17
- LDAP サーバ
 - ステータスの移行 22
- LDAP サーバのサポート 19
- LDAP ユーザ認証 17, 29
 - Adaptive Server の設定 17
 - LDAP 要求のタイムアウト 24
 - エンジンあたりの LDAP 記述子数 24
 - エンジンあたりの最大 ldapua ネイティブ・スレッド数 23
 - 管理 26
 - 検索 DN アルゴリズム 18
 - 堅牢性の強化 23
 - 識別名 17
 - 生成 DN アルゴリズム 18
 - チューニング 29
 - トラブルシューティング 25
 - パスワードの変更 29
 - 満杯の場合は LDAP 認証を放棄する 24
 - ログイン・マッピングに対する制御の強化 30
- LDAP ユーザ認証の最大ネイティブ・スレッド数 29
- LDAP ユーザ認証のタイムアウトの設定 29
- LDAP ユーザ認証のチューニング 29
- LDAP ユーザ認証のトラブルシューティング 25
- LDAP ユーザ認証のパスワードの変更 29
- LDAP 要求のタイムアウト 24
- Linux
 - オペレーティング・システム 6
 - ラージ・メモリ・サポート 6
- Linux でのラージ・メモリ・サポート 6
- load database 61, 62, 64

M

- MIT Kerberos
 - プラットフォームのサポート 16
- MIT Kerberos クライアント・ライブラリ 16

索引

O

online database 63, 64

P

PAM のサポート 33

R

Real Time Messaging Services

概要 6

Resource Governor 5

S

Secure Socket Layer のサポート 32

select * 構文の機能変更

select * 構文 93

set オプション

exportable 50

set オプションのエクスポート 50

shutdown 構文の変更 91

sp_addlogin authenticate with 9

sp_cleanpwdchecks 45

sp_extrapwdchecks 44

sp_helprotect

および暗号化カラム 34

sp_ldapadmin 20

sp_ldapadmin 構文 26

sp_logintrigger 51

sp_maplogin 30

sp_modifylogin authenticate with 9

sp_passwordpolicy 45

SQL コマンド

アーカイブ・データベースへのアクセス 64

syb_map_name 12

Sybase によるドライバのサポート 75

SYBASE_PRINCIPAL 8

sybmapname 12

sybmigrate 5

sysaltusages テーブル 56

T

TIBCO ライブラリ

動的ロード 77

W

Windows Terminal Server

共有メモリ 87

Windows Terminal Server 環境での共有メモリ 87

あ

アーカイブ・データベースのアクセスの

セキュリティ 66

アーカイブ・データベースのアクセスの設定 59

アーカイブ・データベースのアップグレード 68

アーカイブ・データベースの互換性 69

アーカイブ・データベースの削除 63

アーカイブ・データベースの作成 59

アーカイブ・データベースのダウングレード 69

アーカイブ・データベースのマイグレート 68

アーカイブ・データベースへのアクセス 53

dbcc コマンド (dbcc commands) 65

DDLGen サポート 70

sysaltusages テーブル 66

アーカイブ・データベースの作成 59

アーカイブ・データベースのマテリアライズ 61

圧縮ダンプ 67

アップグレード 68

移行 68

オンラインにする 63

互換性 69

コンポーネント 55

削除 63

使用 64

スクラッチ・データベース 56

制限事項 70

セキュリティ 66

設定 59

ダウングレード 69

データベース・ダンプ 55

変更済みページ・セクション 56

変更済みページ・セクションのサイズ設定 59

変更済みページ・セクションの領域の拡張 60

- リカバリなし 62
- 論理デバイス 62
- 圧縮ダンブ
 - アーカイブされたデータベースを使用 67
- 暗号化
 - FIPS 認定の SSL 暗号化アルゴリズム 5
- 暗号化カラム 33
 - alter table 33
 - sp_helpprotect 34
 - 参照整合性 33

え

- エンジンあたりの記述子数 24
- エンジンあたりの
 - 最大 Idapua ネイティブ・スレッド数 23

お

- オンラインにする
 - アーカイブ・データベース 63

か

- 概要 3
- カスタムのパスワード・チェック 47
- カスタムの複雑なパスワード・チェック 36

き

- 機能
 - Adaptive Server プラグイン 83
 - JRE 1.4 81
 - shutdown 構文の変更 91
 - sybase によるドライバのサポート 75
 - Windows Terminal Server 環境での共有メモリ 87
 - アーカイブ・データベースへのアクセス 53
 - 概要 3
 - 共有ディレクトリの変更 73
 - セキュリティ 7
 - 動的にロードされる TIBCO ライブラリ 77
 - モニタリング・テーブルの変更 85
 - 共有ディレクトリの変更 73

く

- グローバル・ログイン・トリガ 51

け

- 言語 5
- 検索 DN アルゴリズム 18
- 検索サーバ
 - セカンダリ 19

こ

- 互換性 1

さ

- サーバ全体の認証オプションの上書き 10
- 最小パスワード長 39
- 参照整合性
 - 暗号化カラム 33

し

- 識別名 17
- 初回ログイン時のパスワードのリセット 41

す

- スクラッチ・データベース 56
- ステータスの移行
 - LDAP サーバ 22

せ

- 制限事項
 - アーカイブ・データベースへのアクセス 70
- 生成 DN アルゴリズム 18
- セカンダリ検索サーバ
 - sp_ldapadmin の使用 20
- セカンダリ検索サーバのサポート 19
- セキュリティ機能 7

索引

た

単純なパスワードの禁止 35

て

データベース・ダンプ

アーカイブ・データベースへのアクセス 55

と

動的にロードされる TIBCO ライブラリ 77

に

認証オプション 10

は

パスワードの大文字の最小文字数 38

パスワードの小文字の最小文字数 39

パスワードの最小アルファベット文字数 37

パスワードの最小桁数 36

パスワードの特殊文字の最小文字数 38

パスワード有効期限 40

パスワード有効期限の警告 40

ふ

複雑なパスワード 34

Adaptive Server プラグインのサポート 49

DDLGen のサポート 49

sp_cleanpwdchecks 45

sp_extrapwdchecks 44

sp_passwordpolicy 45

カスタムのパスワード・チェック 47

相互チェック 41

古い、新しい 42

複雑なパスワード・チェック 35

アルファベット文字の最小文字数の指定 37

カスタムの複雑なパスワード・チェック 36

最小桁数の指定 36

最小パスワード長の指定 39

単純なパスワードの禁止 35

パスワードの大文字の最小文字数の指定 38

パスワードの小文字の最小文字数の指定 39

パスワードの特殊文字の最小文字数の指定 38

パスワードのリセット 41

パスワード有効期限 40

パスワード有効期限の警告 40

ログイン失敗の最大回数 40

複雑なパスワードをサポートする DDLGen 49

プリンシパル名

-k オプションの使用 8

SYBASE_PRINCIPAL の使用 8

sybmapname の使用 12

古いパスワード・チェックと

新しい複雑なパスワード・チェック 42

へ

変更済みページ・セクション

アーカイブ・データベースへのアクセス 56

サイズ変更 59

領域の拡張 60

変更済みページ・セクションの領域の拡張 60

ま

マイグレーション 5

マテリアライズ

アーカイブ・データベース 61

満杯の場合は LDAP 認証を放棄する 24

も

モニタリング・テーブル 85

り

リカバリせずにデータベースをロード 62

リカバリなし 62

ろ

- ログイン失敗の最大回数 40
- ログイン・トリガ
 - および set オプション 50
- ログイン・マッピング
 - 制御の強化 30
- 論理デバイス
 - アーカイブ・データベースへのアクセス 62

