

StorageTek Tape Analytics

管理ガイド

バージョン 2.1.0

E60915-01

2015 年 1 月

StorageTek Tape Analytics
管理ガイド

E60915-01

Copyright © 2012, 2015, Oracle and/or its affiliates. All rights reserved.

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクルまでご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

このソフトウェアまたはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアまたはハードウェアは、危険が伴うアプリケーション (人的傷害を発生させる可能性があるアプリケーションを含む) への用途を目的として開発されていません。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用する際、安全に使用するために、適切な安全装置、バックアップ、冗長性 (redundancy)、その他の対策を講じることは使用者の責任となります。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用したこと起因して損害が発生しても、Oracle Corporation およびその関連会社は一切の責任を負いかねます。

Oracle および Java はオラクルおよびその関連会社の登録商標です。その他の社名、商品名等は各社の商標または登録商標である場合があります。

Intel, Intel Xeon は、Intel Corporation の商標または登録商標です。すべての SPARC の商標はライセンスをもとに使用し、SPARC International, Inc. の商標または登録商標です。AMD, Opteron, AMD ロゴ、AMD Opteron ロゴは、Advanced Micro Devices, Inc. の商標または登録商標です。UNIX は、The Open Group の登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。適用されるお客様と Oracle Corporation との間の契約に別段の定めがある場合を除いて、Oracle Corporation およびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。適用されるお客様と Oracle Corporation との間の契約に定めがある場合を除いて、Oracle Corporation およびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

目次

はじめに	11
対象読者	11
ドキュメントのアクセシビリティ	11
関連ドキュメント	11
STA アプリケーションのユーザー向け	11
STA サーバーおよびアプリケーションのインストール担当者および管理者向け	12
表記規則	12
新機能	13
STA 2.1.0、2015 年 1 月	13
1. サーバー管理	17
1.1. STA コマンドの概要	17
1.2. 管理対象サーバー	17
1.3. メモリー使用要件	18
1.4. グローバル管理コマンド	18
1.5. 個々のサービス管理コマンド	19
2. データベースサービス管理	21
2.1. STA サービスデーモン	21
2.2. STA バックアップサービス	22
2.2.1. 構成	22
2.2.2. 完全バックアッププロセス	23
2.2.3. バックアップサービスのプリファレンス設定の表示	23
2.2.4. プリファレンス設定のクリア	24
2.2.5. ターゲットサーバーにファイルが送信されたことの確認	24
2.2.6. バックアップファイルのローカルコピーが STA サーバーに存在することの確認	26

2.2.7. STA バックアップサービスパスワードのリセット	26
2.3. STA リソースモニターサービス	26
2.3.1. 構成	27
2.3.2. リソースモニターの現在のプリファレンス設定の問い合わせ	27
2.3.3. リソースモニターのプリファレンス設定のクリア	27
2.3.4. STA リソースモニターパスワードのリセット	28
2.4. リソースモニターレポート	28
2.4.1. リソースモニター標準レポート	28
2.4.2. リソース減少警告レポート	29
2.5. ファイルのタイプと場所	30
2.5.1. STA サービスデーモンの開始および停止スクリプト	30
2.5.2. STA 管理ユーティリティ	31
2.5.3. 実行可能プログラムの場所	31
2.5.4. バックアップファイルの場所	32
2.5.4.1. STA サービスデーモンおよびバックアップサービスの管理ロ グ	32
2.5.4.2. MySQL データベースダンプファイル	33
2.5.4.3. MySQL バイナリログ	33
2.5.4.4. STA サービスデーモンおよび WebLogic の構成ファイル	34
2.5.5. リソースモニターファイルの場所	35
2.5.5.1. STA サービスデーモンおよび ResMonAdm のログ	35
2.5.5.2. STA リソースモニターの CSV ファイル	35
2.6. ログイン構成ファイル	37
2.7. STA データベースの復元	39
2.7.1. バックアップファイルのサーバーへのコピー	40
2.7.2. 構成ディレクトリファイルの復元	40
2.7.3. データベースの復元	41
2.7.3.1. データベースのリロード	41
2.7.3.2. Binlog の再生	42
2.7.3.2.1. 複数のサーバー接続の回避	42
2.7.3.3. すべてのサービスの再起動	43
2.7.4. 特定時点の復元	43
2.7.4.1. ログ番号の範囲からの復元	43

3. パスワード管理	45
3.1. STA データベースアカウントパスワードの変更	45
3.2. STA バックアップサービスおよびリソースモニターのパスワードの変更	51
A. サービス拒否攻撃の防止	53
A.1. 概要	53
A.2. iptables ルールの構成	54
A.3. iptables サンプルスクリプト	54
索引	57

表の一覧

1.1. メモリー使用要件	18
2.1. 実行可能プログラムの場所	31
2.2. バックアップソース/ターゲットの場所	34
2.3. リソースモニターの CSV ファイル形式	36
2.4. Java ログイングプロパティ	38
2.5. STA サービスのログイングプロパティ	39

例の一覧

2.1. 標準レポートの例 (切り捨て後)	29
2.2. リソース減少警告レポートの例	29

はじめに

このドキュメントでは、Oracle の StorageTek Tape Analytics (STA) およびそれを実行する専用サーバーの管理方法について説明します。

対象読者

このドキュメントは Linux および STA の管理者を対象としています。

ドキュメントのアクセシビリティ

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility Program の Web サイト (<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>) を参照してください。

Oracle Support へのアクセス

サポートをご契約のお客様には、My Oracle Support を通して電子支援サービスを提供しています。詳細情報は (<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>) か、聴覚に障害のあるお客様は (<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>) を参照してください。

関連ドキュメント

STA のドキュメントセットは、次のドキュメントで構成されています。

STA アプリケーションのユーザー向け

- 『STA クイックスタートガイド』 — このガイドは、STA アプリケーションおよびユーザーインターフェースのいくつかの機能について概要を知るときに使用します。
- 『STA ユーザーズガイド』 — このガイドは、STA アプリケーションのすべての機能 (ダッシュボード、テンプレート、フィルタ、アラート、Executive Reports、論理グループ、STA メディア検証など) を使用する手順について使用します。このガイドでは、STA のユーザー名、電子メールアドレス、サービスログ、およびモニター対象ライブラリとの SNMP 接続を管理する手順も説明されています。
- 『STA 画面基本ガイド』 — このガイドは、STA ユーザーインターフェースの詳細について使用します。画面の移動およびレイアウト、グラフおよび表の使用について説明します。
- 『STA データリファレンスガイド』 — このガイドは、すべての STA テープライブラリシステムの画面およびデータ属性についての定義を参照するときに使用します。

STA サーバーおよびアプリケーションのインストール担当者および管理者向け

- 『STA リリースノート』 — STA のインストールおよび使用の前に、このドキュメントをお読みください。既知の問題など、リリースに関する重要な情報が記載されています。このドキュメントは、STA メディアパックダウンロードに含まれています。
- 『STA 要件ガイド』 — このガイドは、STA の使用について最小および推奨要件を学習するときに使用します。このガイドには、ライブラリ、ドライブ、サーバー、ユーザーインターフェース、STA メディア検証、および IBM RACF アクセス制御の要件が含まれています。
- 『STA インストールおよび構成ガイド』 — このガイドは、STA のインストールの計画、Linux オペレーティングシステムのインストール、STA アプリケーションのインストール、そしてライブラリのモニタリングを開始するための STA の構成を行うときに使用します。このガイドでは、STA の新しいバージョンにアップグレードする手順も説明されています。
- 『STA 管理ガイド』 — このガイドは、STA サービス構成、データベースのバックアップおよび復元、データベースアカウントのパスワード管理など、STA サーバーの管理タスクの情報について使用します。
- 『STA セキュリティーガイド』 — 要件、推奨事項、一般的なセキュリティー原則といった重要な STA のセキュリティー情報については、このドキュメントをお読みください。
- 『STA ライセンス情報ユーザーマニュアル』 — STA 製品とともに配布されるサードパーティーのテクノロジーの使用については、このドキュメントをお読みください。

表記規則

このドキュメントでは、次のテキスト表記規則を使用しています。

表記規則	意味
boldface	太字は、アクションに関連付けられたグラフィカルユーザーインターフェースの要素、またはテキストや用語集で定義される用語を示します。
<i>italic</i>	斜体は、マニュアルタイトル、強調、または特定の値を指定するプレースホルダ変数を示します。
<code>monospace</code>	モノスペースは、段落内のコマンド、URL、例のコード、画面に表示されるテキスト、またはユーザーが入力するテキストを示します。

新機能

このセクションでは、StorageTek Tape Analytics 2.1.0 の新機能および拡張機能の概要について説明します。

STA 2.1.0、2015 年 1 月

新機能および拡張機能の詳細については、指定されたマニュアルを参照してください。

『STA 要件ガイド』の記載内容

- STA 2.1.0 をサポートするための、ライブラリおよびドライブの新しい推奨ファームウェアレベル。
- Oracle の StorageTek T10000C および T10000D ドライブ用の TTI 5.50 プロトコルのサポート。
- STA 2.1.0 をサポートするための、ライブラリおよびドライブの更新された推奨要件。
- 更新された推奨 STA サーバー構成。

『STA インストールおよび構成ガイド』の記載内容

- 次の新機能を提供する、新しい STA 2.1.0 インストーラおよびデインストーラ。
 - Oracle インストールユーザーおよびグループ — STA サーバーで Oracle 製品のインストールとアップグレードを行うためだけに使用される Linux ユーザーおよびグループ。
 - ユーザー定義の Oracle ストレージホームの場所 — STA アプリケーションおよび関連する Oracle ソフトウェアを十分な容量のある任意のファイルシステムにインストールできます。
 - ユーザー定義のデータベースおよびローカルのバックアップ場所。
 - Oracle セントラルインベントリの場所 — STA サーバーにインストールされた Oracle 製品についての情報を追跡するためのディレクトリ。
 - STA インストーラおよびデインストーラのサイレントモード — グラフィカルユーザーインタフェースを省略し、XML プロパティファイルでインストールオプションを指定できます。
 - 新しい詳細な STA インストーラおよびデインストーラのログ。
 - すべての STA グラフィカルインストーラおよびデインストーラの画面用の状況依存ヘルプ。

- 追加の Linux RPM パッケージ要件 — STA グラフィカルインストーラを実行するには、*xorg-x11-utils* パッケージをインストールする必要があります。
- WebLogic 管理コンソールのデフォルトポートは、7019 (HTTP) および 7020 (HTTPS) に変更されました。以前のデフォルトの割り当てを使用していた場合には、新しいものに変更します。
- STA および MySQL ユーザー名の新しいパスワード要件。
- STA 1.0.x および STA 2.0.x データベースを STA 2.1.0 にアップグレードする新しいプロセス。

『STA クイックスタートガイド』の記載内容

- 大きな変更なし

『STA ユーザーズガイド』の記載内容

- 追加情報の提供および使いやすさ向上のため、次のテンプレートに細かい更新が加えられました。
 - STA-Complex-Configuration
 - STA-Complex-Utilization
 - STA-Lib-Configuration
 - STA-Drive-MV
 - STA-Media-All
 - STA-Media-MV-Calibration
 - 「Media Validation Overview」画面、STA-Default テンプレート
- ドキュメントの変更 — 次の章が『STA 管理ガイド』から移動されました。『STA ユーザーズガイド』には、STA ユーザーインタフェースから実行できるすべての機能とアクティビティが記載されるようになりました。
 - STA ユーザー名と電子メール
 - STA サービスログ
 - STA での SNMP 接続の管理

『STA 画面基本ガイド』の記載内容

- 大きな変更なし

『STA データリファレンスガイド』の記載内容

- 使いやすさ向上のため、一部の画面で属性が再編成されました。

- CAP、ドライブ、エレベータ、ライブラリ、PTP、およびロボットのそれぞれの画面で「Last Messages」属性を使用できます。

『STA 管理ガイド』の記載内容

- ドキュメントの変更 — 次の章が『STA ユーザーズガイド』に移動されました。
 - ユーザーと電子メール
 - ログイン
 - SNMP 管理

サーバー管理

STA コマンドは、各種 STA コンポーネントの管理とステータスの確認に使用します。この章は次のセクションで構成されています。

- [STA コマンドの概要](#)
- [管理対象サーバー](#)
- [メモリー使用要件](#)
- [グローバル管理コマンド](#)
- [個々のサービス管理コマンド](#)

1.1. STA コマンドの概要

STA コマンドのバリエーションは次のカテゴリに分類できます。

- STA 環境全体の起動または停止や、STA 環境全体のステータス確認を行うためのコマンド
- 個々の STA サービスの起動または停止や、個々の STA サービスのステータス確認を行うためのコマンド。

注意:

個々の STA サービスのコマンドは参照用として記載されています。Oracle Support から指示されないかぎり、これらのコマンドは実行しないでください。

有効な STA コマンド引数のリストは、`STA help` コマンドを使用していつでも取得できます。

1.2. 管理対象サーバー

STA プロセスは次の 3 つの管理対象サーバーに分類できます。

- `staUi` — STA ユーザーインターフェース
- `staEngine` — 基本的な STA 内部機能
- `staAdapter` — SNMP 通信

サーバーは個々に管理できます。「[個々のサービス管理コマンド](#)」を参照してください。

1.3. メモリー使用要件

表1.1「メモリー使用要件」は、STA ドメインサーバー、STA 管理対象サーバー、および MySQL のメモリー使用要件を示しています。

表1.1 メモリー使用要件

項目	メモリー要件
STA ドメインサーバー	2G バイトのヒープサイズ
STA 管理対象サーバー	2G バイトのヒープサイズ
MySQL	2G バイトのメモリー

1.4. グローバル管理コマンド

次の STA コマンドは、STA 環境全体の開始と停止、およびステータス確認に使用できます。

- *STA start all* は、STA 環境全体を開始します。例:

```
# STA start all

Starting mysql Service..
mysql service was successfully started
Starting staservd Service.
staservd service was successfully started
Starting weblogic Service.....
weblogic service was successfully started
Starting staengine Service.....
staengine service was successfully started
Starting staadapter Service.....
staadapter service was successfully started
Starting stauai Service.....
stauai service was successfully started
#
```

- *STA stop all* は、STA 環境全体を停止します。例:

```
# STA stop all

Stopping the stauai service.....
Successfully stopped the stauai service
```

```
Stopping the staadapter service.....
Successfully stopped the staadapter service
Stopping the staengine service.....
Successfully stopped the staengine service
Stopping the weblogic service.....
Successfully stopped the weblogic service
Stopping the staservd Service...
Successfully stopped staservd service
Stopping the mysql service.....
Successfully stopped mysql service
#
```

- *STA status all* は、STA 環境全体のステータスを表示します。例:

```
# STA status all

mysql is running
staservd service is running
weblogic service is running
staengine service is running
.... and the deployed application for staengine is in an ACTIVE state
staadapter service is running
.... and the deployed application for staadapter is in an ACTIVE state
staiui service is running
.... and the deployed application for staiui is in an ACTIVE state
```

1.5. 個々のサービス管理コマンド

次の *STA* コマンドは、個々の *STA* コンポーネントの開始と停止や、それらのコンポーネントのステータス確認に使用できます。

注意:

個々の *STA* サービスのコマンドは参照用として記載されています。Oracle Support から指示された場合にのみ、これらのコマンドを使用してください。

- *STA start|stop|status mysql*

MySQL の開始または停止、またはそのステータスを表示します。

- *STA start|stop|status staservd*

STA サービスデーモンの開始または停止、またはそのステータスを表示します。

- *STA start|stop|status weblogic*

WebLogic 管理サーバーの開始または停止、またはそのステータスを表示します。

- *STA start|stop|status staadapter*

staAdapter 管理対象サーバーの開始または停止、またはそのステータスを表示します。

- *STA start|stop|status staengine*

staEngine 管理対象サーバーの開始または停止、またはそのステータスを表示します。

- *STA start|stop|status stau*

staUi 管理対象サーバーの開始または停止、またはそのステータスを表示します。

データベースサービス管理

この章では、各種 STA サービスの管理について説明します。これらのサービスの最初の構成を行うには、『STA インストールおよび構成ガイド』を参照してください。

この章は次のセクションで構成されています。

- [STA サービスデーモン](#)
- [STA バックアップサービス](#)
- [STA リソースモニターサービス](#)
- [リソースモニターレポート](#)
- [ファイルのタイプと場所](#)
- [ロギング構成ファイル](#)
- [STA データベースの復元](#)

2.1. STA サービスデーモン

STA サービスデーモン *staservd* は常時実行の Linux サービスで、STA バックアップサービスと STA リソースモニターサービスを管理および実行します。STA バックアップサービスと STA リソースモニターサービスは、STA サービスデーモン内でそれぞれ別の実行スレッドとして実行します。

STA *start all* コマンドを使用して STA サーバーをブートすると STA サービスデーモンが開始し、サーバーを停止するとサービスデーモンは終了します。次のコマンドを使用すると STA サービスデーモンの開始、停止、およびステータスの確認を実行できます。

- STA サービスデーモンを開始するには:

```
# STA start staservd

Starting staservd Service...

staservd service was successfully started
```

- STA サービスデーモンを停止するには:

```
# STA stop staservd
```

```
Stopping the staservd Service...
```

```
Successfully stopped staservd service
```

- STA サービスデーモンのステータスを確認するには:

```
# STA status staservd
```

```
staservd service is running
```

STA コマンドの詳細は、1章「[サーバー管理](#)」を参照してください。

注:

STA をインストールすると、STA サービスデーモンが STA バックアップサービスと STA リソースモニターサービスを開始しますが、未構成の状態ではこれらのサービスは有効になりません。これらのサービスを構成するには、『[STA インストールおよび構成ガイド](#)』を参照してください。

2.2. STA バックアップサービス

STA バックアップサービスは STA サービスデーモン内で実行するサービスの 1 つです。これは STA データベースおよび鍵構成ディレクトリの自動完全バックアップを実行し、それらのファイルを STA サーバー上の指定場所または圧縮形式でリモートサーバーに書き込みます。Oracle では、リモートバックアップサーバーを構成することをお勧めしています。

続行する前に、STA サービスデーモンが実行していることを確認します。「[STA サービスデーモン](#)」を参照してください。

- 「[構成](#)」
- 「[完全バックアッププロセス](#)」
- 「[バックアップサービスのプリファレンス設定の表示](#)」
- 「[プリファレンス設定のクリア](#)」
- 「[ターゲットサーバーにファイルが送信されたことの確認](#)」
- 「[バックアップファイルのローカルコピーが STA サーバーに存在することの確認](#)」
- 「[STA バックアップサービスパスワードのリセット](#)」

2.2.1. 構成

STA バックアップサービスは、`/Oracle_storage_home/StorageTek_Tape_Analytics/common/bin` にある `staservadm` という管理ユーティリティーを使用して構

成します。STA バックアップサービスを構成するには、『STA インストールおよび構成ガイド』を参照してください。

2.2.2. 完全バックアッププロセス

STA バックアップサービスを構成すると、次のプロセスが 24 時間ごとに 1 回実行されます。

1. 次のファイルタイプの高速度ダンプ (ホットバックアップとも呼ばれています) を開始します。
 - MySQL データベースダンプファイル
 - MySQL バイナリログファイル
 - STA サービスデーモンおよび STA WebLogic の構成ファイル
 - STA サービスデーモンおよび STA バックアップサービスの管理ログ
2. 指定されたバックアップホストにダンプファイルを転送します
3. 前日の完全ダンプファイルを STA サーバーから削除します
4. 現在日のダンプファイルのコピーを STA サーバー上の `/sta_db_backup/local` ディレクトリに書き込みます。

2.2.3. バックアップサービスのプリファレンス設定の表示

1. 現在のプリファレンス設定のステータスを表示します。

```
# ./staservadm -Q

Contacting daemon...connected.
Querying Preferences.

Current STA Backup Service Settings:
  Configured           [yes]
  File Transfer        -S [SCP]
  Full Backup          -T [11:00]
  Sleep Interval       -i [350 sec]
  Backup Hostname      -s [stabaksvr]
  Backup Username      -u [stabck]
  Backup Password      -p [*****]
  Backup Directory     -d [/home/stabck/STAbackups]
  Database Username    -U [stadba]
  Database Password    -P [*****]
```

2. *Configured* フィールドが *[no]* の場合、バックアップサービスはアイドルモードで実行されているため、バックアップは実行されていません。適切な構成設定を行う必要があります。詳細については、『*STA インストールおよび構成ガイド*』を参照してください。

2.2.4. プリファレンス設定のクリア

1. 現在のプリファレンス設定をクリアします。

```
# ./staservadm -C

Contacting daemon...connected.
Clearing Preferences.
Done.

Current STA Backup Service Settings:
Configured          [no]
File Transfer       -S [SCP]
Full Backup         -T [00:00]
Sleep Interval      -i [300 sec]
Backup Hostname     -s []
Backup Username     -u []
Backup Password     -p []
Backup Directory    -d []
Database Username   -U []
Database Password   -P []
```

2. バックアップサービスが未構成の状態になり、アイドル状態に戻ります。新しい設定を指定できます。詳細については、『*STA インストールおよび構成ガイド*』を参照してください。

2.2.5. ターゲットサーバーにファイルが送信されたことの確認

ターゲットサーバーにファイルが正常に送信されたかどうかを確認するには:

- STA サーバー上のログを確認します。
 - ターゲットバックアップサーバーにログオンし、バックアップディレクトリの内容を一覧表示します。
1. STA サーバーにシステムの root ユーザーとしてログオンします。
 2. ディレクトリを STA データベースのバックアップログディレクトリに変更します。

```
# cd /sta_logs/db/backups
```


3. `staservd.log.0` ファイルで、「INFO: done. Database dump completed」という文字列を検索します。このファイルにはバックアップサービス構成ユーティリティーのアクティビティーが記録されます。

```
# grep "INFO: done.Database dump completed" staservd.log.0
```

```
INFO: done. Database dump completed, file located at
/dbbackup/local/20130721_133755.stafullbackup.sql
INFO: done. Database dump completed, file located at
/dbbackup/local/20130722_133755.stafullbackup.sql
INFO: done. Database dump completed, file located at
/dbbackup/local/20130723_133755.stafullbackup.sql
INFO: done. Database dump completed, file located at
/dbbackup/local/20130724_133755.stafullbackup.sql
```

4. ターゲットバックアップサーバーにログオンします。
5. データベースのバックアップディレクトリのファイルを一覧表示します。

この例では、STA サーバー「tbivb01」からのバックアップファイルを受信するディレクトリとして `/backups/tbivb01` が設定されています。

```
# ls -l /backups/tbivb01
```

```
0.stadb-bin.000023.gz
0.stadb-bin.000024.gz
0.stadb-bin.000026.gz
0.stadb-bin.000027.gz
20130723_133755.stadb-bin.000023.gz
20130723_133755.conf.zip.gz
20130723_133755.fmwconfig.zip.gz
20130723_133755.stadb-bin.000025.gz
20130723_133755.stadb-bin.000026.gz
20130723_133755.stafullbackup.sql.gz
```

2.2.6. バックアップファイルのローカルコピーが STA サーバーに存在することの確認

`/sta_db_backup/local` ディレクトリ内のファイルを一覧表示し、最新のバックアップファイルのコピーが STA サーバーにローカルで保存されていることを確認します。例:

```
# ls -l /dbbackup/local
20130721_133755.conf.zip
20130721_133755.fmwconfig.zip
20130721_133755.stafullbackup.zip
```

一覧表示されるファイルの名前の形式は、`YYYYMMDD_HHMMSS.filename.zip` です。

2.2.7. STA バックアップサービスパスワードのリセット

[3章「パスワード管理」](#)を参照してください。

2.3. STA リソースモニターサービス

STA リソースモニターサービスは、STA サーバーリソース (データベーステーブル領域、ディスクボリューム領域、ロギングボリュームディスク領域、物理メモリーの使用率など) に関するモニターとレポート作成を行います。

各リソースに使用率の高水位標 (HWM) を設定できます。高水位標とは、警告が発行されるときのしきい値です。しきい値に到達するか、しきい値を上回ると、標準日次リソースレポートに警告が記録され、警告を 1 人以上の指定受信者に電子メールで送信する (オプション) ことも可能です。

たとえばデータベーステーブル領域の HWM を 60% に設定した場合、許可されている最大データベーステーブル領域の 60 パーセント以上を STA アプリケーションが使用すると、STA リソースモニターがこれを検知し、テーブル領域警告を有効にして、指定受信者に電子メールを送信します。また、永続モードを有効にした場合、リソースモニターは、システムのスキャンを行うたびに警告の電子メールを送信します。

- [「構成」](#)
- [「リソースモニターの現在のプリファレンス設定の問い合わせ」](#)
- [「リソースモニターのプリファレンス設定のクリア」](#)
- [「STA リソースモニターパスワードのリセット」](#)

2.3.1. 構成

STA リソースモニターサービスは、`/Oracle_storage_home/StorageTek_Tape_Analytics/common/bin`にある `staresmonadm` という管理ユーティリティを使用して構成します。STA リソースモニターサービスを構成するには、『STA インストールおよび構成ガイド』を参照してください。

2.3.2. リソースモニターの現在のプリファレンス設定の問い合わせ

現在のプリファレンス設定の状態を問い合わせるには、次のコマンドを入力します。

```
# ./staresmonadm -Q
```

Configured フィールドに「no」が表示されている場合、リソースモニターサービスは「アイドル」モードで実行されているため、リソースのモニタリングもレポートの送信も実行されていません。サーバーを構成する必要があります。詳細については、『STA インストールおよび構成ガイド』を参照してください。

構成済 STA リソースモニターサービスの出力例:

```
# ./staresmonadm -Q
```

```
Contacting daemon...connected.
Querying Preferences.
Current STA Resource Monitor Service Settings:
Configured                               [yes]
Send Reports                             -T [13:00]
Sleep Interval                           -i [600 sec]
Alert Nagging                             -n [on]
DB Username                              -U [sta_dba]
DB Password                              -P [*****]
DB Tablespace hwm                        -t [65%]
DB Backup hwm (/dbbackup)                -b [65%]
DB Data hwm (/dbdata)                   -d [65%]
Log Volume hwm (/var/log/tbi)            -l [65%]
Root Volume hwm (/)                     -z [70%]
Tmp Volume hwm (/tmp)                   -x [80%]
System Memory hwm                       -m [75%]
Email 'From:'                            -f [StaResMon@localhost]
Email 'To:'                              -r [john.doe@company.com]
Email 'Subject:'                         -s [STA Resource Monitor Report]
Output File                              -o [/var/log/tbi/db/staresmon.csv]
```

2.3.3. リソースモニターのプリファレンス設定のクリア

現在のプリファレンス設定をクリアするには、次のコマンドを入力します。

```
# ./staresmonadm -C
```

リソースモニターサービスが未構成の状態になり、アイドル状態に戻ります。新しい設定を指定できます。詳細については、『[STA インストールおよび構成ガイド](#)』を参照してください。例:

```
# ./staresmonadm -C

Contacting daemon...connected.
Clearing Preferences.
Done.
Current STA Resource Monitor Service Settings:
Configured                [no]
Send Reports               -T [00:00]
Sleep Interval            -i [300 sec]
Alert Nagging             -n [off]
DB Username               -U []
DB Password               -P []
DB Tablespace hwm         -t [-1%]
DB Backup hwm (/dbbackup) -b [-1%]
DB Data hwm (/dbdata)    -d [-1%]
Log Volume hwm (/var/log/tbi) -l [-1%]
Root Volume hwm (/)      -z [-1%]
Tmp Volume hwm (/tmp)    -x [-1%]
System Memory hwm        -m [-1%]
Email 'From:'             -f [StaResMon@localhost]
Email 'To:'               -r []
Email 'Subject:'         -s [STA Resource Monitor Report]
Output File               -o [/var/log/tbi/db/staresmon.csv]
```

2.3.4. STA リソースモニターパスワードのリセット

[3章「パスワード管理」](#)を参照してください。

2.4. リソースモニターレポート

リソースモニターレポートは、*staresmonadm* という STA リソースモニターサービス管理ユーティリティを使用して構成します。STA リソースモニターサービスを構成するには、『[STA インストールおよび構成ガイド](#)』を参照してください。

リソースモニターでは次の 2 種類のレポートを作成できます。

- 「リソースモニター標準レポート」
- 「リソース減少警告レポート」

2.4.1. リソースモニター標準レポート

リソースモニター標準レポートは 1 日 1 回、*staresmonadm -T* オプションで指定された時間付近で送信されます。時間を設定しなかった場合、午前 0 時を過ぎてから最初のスキャン時にレポートが送信されます。このサービスの構成時に指定した電子メール受信者にレポートが送信されます。

レポートには次のサーバーリソースのデータが表示されます。これらのリソースのいずれかが高水位標しきい値を超えた場合、レポートに警告が表示されます。

- データベーステーブル領域およびボリューム
- ロギング、バックアップ、およびルートボリューム
- 一時ディレクトリ
- システムメモリー使用率

注:

レポートの値はマウントポイントに依存します。複数のモニター対象項目がマウントポイントを共有している場合、これらの項目のレポート値は同一になります。

例2.1 標準レポートの例 (切り捨て後)

```
STA RESOURCE MONITOR STANDARD REPORT
System: tbivb03
Scanned: 2013-10-24 11:30:14
Database Tablespace
  HWM          : 60.00%
  Used         : <0.1%
  MB Used      : 13
  MB Free      : 75763
  MB Total     : 75776
  Location     : /dbdata/mysql
Database Volume
  HWM          : 60.00%
  Used         : 6.80%
  MB Used      : 6855
  MB Free      : 93939
  MB Total     : 100794
  Directory    : /dbdata/mysql
...
```

2.4.2. リソース減少警告レポート

staresmonadm 警告の永続モード (*-n*) オプションが「on」に設定されている場合、毎スキャン後にリソース減少警告レポートが送信されます。永続モードが off の場合、警告は標準レポートにのみ表示されます。

各スキャンの間隔は *Sleep Interval (-i)* 属性によって決まり、このサービスの構成時に指定した電子メール受信者にレポートが送信されます。レポートには、報告された問題の解決に役立つ情報が表示されます。

例2.2 リソース減少警告レポートの例

```
STA RESOURCE DEPLETION REPORT
System: server01
Scanned: 2013-10-24 11:34:47
*****
```

```

*                               A L E R T S                               *
*****
=====
ALERT - Low System Physical Memory
=====
Physical memory usage has exceeded threshold value!
HWM                [1.00%]
Used               [48.24%] (!)
MB Used           [7757]
MB Free           [8324]
MB Total          [16080]
Hostname          [server01]
Recommendations:
1) Shutdown unneeded processes.
2) Under Linux, try releasing unused caches using commands:
   # free -m
   # sync
   # /sbin/sysctl -q vm.drop_caches=3
   # free -m
3) Install additional memory.

```

2.5. ファイルのタイプと場所

STA サービスは、実行可能スクリプト、サーバーおよびクライアントアプリケーションが含まれている Java jar ファイル、構成ファイル、ダンプファイル、ロギングファイル、および累積データファイルで構成されます。このセクションでは、それらの用途と場所について説明します。

- [「STA サービスデーモンの開始および停止スクリプト」](#)
- [「STA 管理ユーティリティー」](#)
- [「実行可能プログラムの場所」](#)
- [「バックアップファイルの場所」](#)
- [「リソースモニターファイルの場所」](#)

2.5.1. STA サービスデーモンの開始および停止スクリプト

STA サービスデーモンの開始および停止スクリプト *staservd* とシステム実行レベルのシンボリックリンクは次のディレクトリにあります。このスクリプトと関連するシンボリックリンクは STA インストーラによって作成されます。

/etc/init.d/staservd - メインの開始および停止スクリプト

/etc/rc0.d/K04staservd - システム停止のシンボリックリンク

/etc/rc1.d/K04staservd - システム停止のシンボリックリンク

/etc/rc2.d/S96staservd - システム開始のシンボリックリンク

/etc/rc3.d/S96staservd - システム開始のシンボリックリンク

`/etc/rc4.d/S96staservd` - システム開始のシンボリックリンク

`/etc/rc5.d/S96staservd` - システム開始のシンボリックリンク

`/etc/rc6.d/K04staservd` - システム停止のシンボリックリンク

2.5.2. STA 管理ユーティリティー

Perl スクリプトである STA バックアップサービス管理ユーティリティー `staservadm` は、`oracle.tbi.serveradm.jar` ファイルに含まれている `ServerAdm` という Java クライアントアプリケーションを呼び出します。詳細については、「[STA バックアップサービス](#)」を参照してください。

Perl スクリプトである STA リソースモニター管理ユーティリティー `staresmonadm` は、`oracle.tbi.resmonadm.jar` ファイルに含まれている `StaResMonAdm` という Java クライアントアプリケーションを呼び出します。`StaResMonAdm` は、STA サービスデーモンと通信して実行時プリファレンスの設定とリセットを行う RMI クライアントです。詳細については、「[STA リソースモニターサービス](#)」を参照してください。

2.5.3. 実行可能プログラムの場所

表2.1「[実行可能プログラムの場所](#)」は、実行可能プログラムとそれらの場所を示しています。

表2.1 実行可能プログラムの場所

プログラム	場所
STA サービスプログラム jar ファイル	<code>\$STAHOME/common/lib/oracle.tbi.server.jar</code>
STA バックアップサービス管理ユーティリティー Java アプリケーション jar ファイル	<code>\$STAHOME/common/lib/oracle.tbi.serveradm.jar</code>
STA バックアップサービス管理ユーティリティーユーザー スクリプトファイル <code>staservadm</code>	<code>\$STAHOME/common/bin/staservadm</code>
STA ResMon 管理ユーティリティー Java アプリケーション jar ファイル	<code>\$STAHOME/common/lib/oracle.tbi.resmonadm.jar</code>
STA ResMon 管理ユーティリティー Java ユーザー スクリプトファイル <code>staresmonadm</code>	<code>\$STAHOME/common/bin/staresmonadm</code>

ここでは:

`$STAHOME=/Oracle_storage_home/StorageTek_Tape_Analytics`

2.5.4. バックアップファイルの場所

STA データベースのバックアップには次の種類のファイルが含まれます。

- STA サービスデーモンおよびバックアップサービスの管理ログ
- MySQL データベースダンプファイル
- MySQL バイナリログ
- STA サービスデーモンおよび WebLogic の構成ファイル

2.5.4.1. STA サービスデーモンおよびバックアップサービスの管理ログ

これらは STA サービスデーモンサーバー、*STAServer*、およびバックアップサービス構成ユーティリティである *ServerAdm* のアクティビティのロギングを行います。管理ログは最大 10 個のログファイルで構成され、各ログファイルのサイズは最大 1.0M バイトです。ログファイル名は **.log.N* という形式で、*N* はログの番号です (*staservd.log.0*、*staservadm.log.0*、*staservd.log.1* など)。

ログは循環方式で、たとえばログファイル *staservd.log.9* がいっぱいになると、*#1* のログファイルがふたたび使用されます。アクティブなログファイルは常に *#0* (*staservd.log.0*) です。ログ *#0* がいっぱいになるとファイル名がログ *#1* に変更され、新しいログ *#0* が開始します。デフォルトでは、*STAServer* と *ServerAdm* のログは次のディレクトリにあります。

`/STA_logs/db/backups`

STA_logs のデフォルトの場所は `/var/log/tbi` です。

ログの場所と内部形式 (単純 ASCII テキストまたは XML マークアップ) は、次の場所にあるロギングプロパティファイル *staservd.log.props* および *staservadm.log.props* によって決まります。

`$STAHOME/common/conf/staservd.log.props`

`$STAHOME/common/conf/staservadm.log.props`

ここでは:

`$STAHOME=/Oracle_storage_home/StorageTek_Tape_Analytics`

2.5.4.2. MySQL データベースダンプファイル

MySQL データベースダンプファイルは、データベーススキーマとデータ内容の瞬間のスナップショットです。STA バックアップサービスは次のアクションを実行します。

1. 24 時間に 1 回、このセクションで説明するファイルタイプの高速ダンプ (ホットバックアップとも呼ばれています) を実行します。
2. 指定されたバックアップホストに最新のダンプファイルを転送します。
3. 前日の完全ダンプファイルをローカルバックアップディレクトリから削除します。
4. 現在日のダンプファイルのコピーをローカルバックアップディレクトリに書き込みます。

デフォルトで STA バックアップサービスは、ローカルダンプファイルと増分 binlog ファイルを `/sta_db_backup/local` ディレクトリに `YYYYMMDD_HHMMSS.filename.sql` の形式で保存します。

2.5.4.3. MySQL バイナリログ

増分ダンプとは、データベース変更の原因となったすべてのトランザクションを記録する MySQL バイナリログ (binlog) のことです。STA バックアップサービスは binlog をメインのデータベースダンプに続く増分バックアップとして扱います。

STA 増分ダンプは、最後の完全ダンプ以降に生成されたすべてのバイナリログで構成されます。binlog を再生することで、ログに記録されている最後のトランザクション時の状態までデータベースを復元できます。復元では、最新のダンプファイルのロード後、最後のデータベースダンプ以降に生成されたすべての MySQL binlog が順番に再生されます。

binlog のバックアップでは、最後の完全ダンプ後に作成されたすべての binlog のリストが作成され、それらの各ログがバックアップサーバーに転送されます (現行ログはオープン状態のため転送されません)。

バックアップバイナリログの命名形式は、`YYYYMMDD_HHMMSS.stadb-bin.log_sequence_number` です。

MySQL バイナリログの場所は MySQL 設定ファイル `/etc/my.cnf` で定義されます。これは現在次のように設定されています。

```
/STA_logs/db
```

バックアップ binlog ファイルのローカルコピーは次の場所にあります。

```
/sta_db_backup/local
```

バックアップサーバーに正常に転送されたすべての binlog (最新の binlog を除く) は、MySQL コマンド `PURGE BINARY LOGS BEFORE NOW()` を使用してパージできます。そのため、現行の binlog と現在日の完全バックアップファイルはサーバー上に残ります。

注意:

binlog ファイルは絶対に手動で削除しないでください。

2.5.4.4. STA サービスデーモンおよび WebLogic の構成ファイル

STA アプリケーションデータベースの復元に必要なファイルに加え、STA バックアップサービスは自身の STA サービスデーモン構成ファイルと、STA の WebLogic 構成ファイルもバックアップします。このバックアップでは、それぞれの構成ディレクトリ内のすべてのファイルとディレクトリが繰り返しバックアップされます。

構成ファイルのバックアップは 24 時間ごとに 1 回、完全 STA データベースダンプが実行されたときに実行されます。バックアップファイルの名前形式は、`YYYYMMDD_HHMMSS.filename.zip.gz` です。

これらのバックアップのソースとターゲットの場所は、[表2.2「バックアップソース/ターゲットの場所」](#)のとおりです。

表2.2 バックアップソース/ターゲットの場所

ソースの場所	ローカルコピー	リモートコピー
<code>\$STAHOME/common/conf/*</code>	<code>\$BACKUPS/YYYYMMDD_HHMMSS.conf.zip</code>	<code>\$RHOST:\$RDIR/YYYYMMDD_HHMMSS.conf.zip.gz</code>
<code>\$WLHOME/config/fmconfig/*</code>	<code>\$BACKUPS/YYYYMMDD_HHMMSS.fmconfig.zip</code>	<code>\$RHOST:\$RDIR/YYYYMMDD_HHMMSS.fmconfig.zip.gz</code>

ここでは:

`$STAHOME = /Oracle_storage_home/StorageTek_Tape_Analytics`

`$WLHOME = /Oracle_storage_home/Middleware/user_projects/domains/TBI`

`$BACKUPS = /dbdata/mysql/backups`

`$RHOST` = バックアップサーバーの IP アドレスまたは名前

`$RDIR` = バックアップサーバー上のディレクトリ

2.5.5. リソースモニターファイルの場所

モニタリング操作に関連する 2 種類のファイルがあります。

- [STA サービスデーモンおよび ResMonAdm のログ](#)
- [STA リソースモニターの CSV ファイル](#)

2.5.5.1. STA サービスデーモンおよび ResMonAdm のログ

これらは STA サービスデーモンとリソースモニター管理ユーティリティーである `staresmonadm` のアクティビティーのロギングを行います。これらのログは最大 10 個のログファイルで構成され、各ログファイルのサイズは最大 1.0M バイトです。ログファイル名は `*.log.N` という形式で、`N` はログの番号です (`staservd.log.0`、`staservadm.log.0`、`staservd.log.1` など)。

ログは循環方式で、たとえばログファイル `staservd.log.9` がいっぱいになると、`#1` のログファイルがふたたび使用されます。アクティブなログファイルは常に `#0` (`staservd.log.0`) です。ログ `#0` がいっぱいになるとファイル名がログ `#1` に変更され、新しいログ `#0` が開始します。デフォルトでは STA サービス、STA ResMon、および STA ResMonAdm のログはすべて次の場所にあります。

```
/STA_logs/db/backups
```

ログの場所と内部形式 (単純 ASCII テキストまたは XML マークアップ) は、次の場所にあるロギングプロパティファイル `staservd.log.props` および `staresmonadm.log.props` によって決まります。

```
$STAHOME/common/conf/staservd.log.props
```

```
$STAHOME/common/conf/staresmonadm.log.props
```

ここでは:

```
$STAHOME=/Oracle_storage_home/StorageTek_Tape_Analytics
```

2.5.5.2. STA リソースモニターの CSV ファイル

ResMon はシステムをスキャンするたびに収集した値をカンマ区切り値 (CSV) ファイルとして、デフォルトの次の場所へ書き込みます。

```
/STA_logs/db/staresmon.csv
```

このデータファイルは Excel や MySQL などのプログラムにロードできるので、時間ベースの値を元に各種の分析を行ったり、グラフを作成したりできます (リソースの減少傾向の分析など)。

注:

ResMon CSV ファイルを STA バックアップサービスを使用してページ、ロール、またはバックアップすることはできません。

staresmon.csv 内の各レコードはシステムの 1 回のスキャンを表しています。21 列レコードの形式を、[表2.3「リソースモニターの CSV ファイル形式」](#)に示します。

表2.3 リソースモニターの CSV ファイル形式

列	ヘッダー	説明	形式
1	TIMESTAMP	スキャンの日時	"YYYY-MM-DD HH:MM:SS"
2	TS_MB_MAX	最大テーブル領域	123
3	TS_MB_USED	使用されているデータベース領域合計	123
4	TS_MB_AVAIL	残っているデータベース領域	123
5	TS_PCT_USED	使用されているデータベーステーブル領域 (最大に占めるパーセンテージとして)	12.34%
6	TS_PCT_HWM	データベーステーブル領域の高水位標 (最大に占めるパーセンテージとして)	12.34%
7	DBVOL_MB_MAX	データベースが含まれているボリューム上の最大使用可能領域	123
8	DBVOL_MB_USED	使用されているデータベースディスクボリューム領域合計	123
9	DBVOL_MB_AVAIL	残っているデータベースボリュームディスク領域	123
10	DBVOL_PCT_USED	使用されているデータベースボリュームディスク領域 (最大に占めるパーセンテージとして)	12.34%
11	DBVOL_PCT_HWM	データベースボリューム高水位標 (最大に占めるパーセンテージとして)	12.34%

列	ヘッダー	説明	形式
12	LOGVOL_MB_MAX	ログが含まれているボリューム上の最大使用可能領域	123
13	LOGVOL_MB_USED	使用されているロギングディスクボリューム領域合計	123
14	LOGVOL_MB_AVAIL	残っているロギングボリュームディスク領域	123
15	LOGVOL_PCT_USED	使用されているロギングボリュームディスク領域 (最大に占めるパーセンテージとして)	12.34%
16	LOGVOL_PCT_HWM	ロギングボリューム高水位標 (最大に占めるパーセンテージとして)	12.34%
17	MEM_MB_MAX	インストールされている最大物理 RAM	123
18	MEM_MB_USED	使用されている物理メモリーの合計	123
19	MEM_MB_AVAIL	残っている物理メモリー領域	123
20	MEM_PCT_USED	使用されている物理メモリー領域 (最大に占めるパーセンテージとして)	12.34%
21	MEM_PCT_HWM	物理メモリー高水位標 (最大に占めるパーセンテージとして)	12.34%

2.6. ロギング構成ファイル

STA サービスデーモン、バックアップサービス、バックアップサービス管理ユーティリティー、および STA リソースモニターユーティリティーのロギングは、次のロギング構成ファイルで制御されます。

```
$STAHOME/common/conf/staservd.log.props
```

```
$STAHOME/common/conf/staservadm.log.props
```

```
$STAHOME/common/conf/staresmonadm.log.props
```

ここで、`$STA_HOME` は STA のインストール時に指定された STA のホーム位置です。詳細については、『[STA インストールおよび構成ガイド](#)』を参照してください。

ロギングファイルの内容と形式は、これらのファイル内の Java Log Manage プロパティーによって制御されます。[表2.4「Java ロギングプロパティー」](#)に、これらのプロパティーの概要を

示します。詳細については、次のサイトにある Oracle Java SE ドキュメントを参照してください。

<http://docs.oracle.com/en/java/>

表2.4 Java ロギングプロパティ

プロパティ	説明	STA の設定
<code>java.util.logging</code> <code>.FileHandler.append</code>	ファイルハンドラが既存のファイルに付加するかどうかを指定します。デフォルトは <code>false</code> です。	<code>true</code>
<code>java.util.logging</code> <code>.FileHandler.count</code>	循環させる出力ファイルの数を指定します。デフォルトは <code>1</code> です。	<code>10</code>
<code>java.util.logging</code> <code>.FileHandler.formatter</code>	Formatter クラスの名前を指定します。デフォルトは <code>java.util.logging.XMLFormatter</code> です。	<code>Java.util.logging</code> <code>.SimpleFormatter</code> (可読性を得るため)。 <code>java.util.logging</code> <code>.XMLFormatter</code> はコメント化されており、使用可能です
<code>java.util.logging</code> <code>.FileHandler.level</code>	ハンドラのデフォルトレベルを指定します。デフォルトは <code>Level.ALL</code> です。	<code>CONFIG</code>
<code>java.util.logging</code> <code>.FileHandler.limit</code>	1つのファイルに書き込むおおよその最大バイト数を指定します。これがゼロの場合は、制限がないことを示します。デフォルトは制限なしです。	<code>500000</code> (.5M バイト)
<code>java.util.logging</code> <code>.FileHandler.pattern</code>	出力ファイル名のパターンを指定します。デフォルトは <code>"%h/java%u.log"</code> です。	<code>/STA_logs/db/backups/staservd.log.%g</code> <code>/STA_logs/db/backups/staservadm.log.%g</code> ここで、 <code>STA_logs</code> は Linux のインストール時に確立されたログの場所です。詳細については、『STA インストールおよび構成ガイド』を参照してください。

ログレベルは、これらのファイル内の STA ロギングプロパティによって制御されます。表 2.5「STA サービスのロギングプロパティ」に、これらのプロパティの概要を示します。

表2.5 STA サービスのロギングプロパティ

プロパティ	説明	STA の設定
<code>oracle.tbi.server.level</code>	サーバーのログレベルを指定します。	<code>CONFIG</code>
<code>oracle.tbi.serveradm.level</code>	サーバー管理機能のログレベルを指定します。	<code>CONFIG</code>
<code>oracle.tbi.resmonadm.level</code>	リソースモニター管理機能のログレベルを指定します。	<code>CONFIG</code>

2.7. STA データベースの復元

STA データベースの復元手順では、データベースの最新の完全ダンプをロードし、そのダンプ後のすべてのバイナリログを再生します。

バックアップサーバーディレクトリ上にあるバックアップファイルのセットは状況によって異なります。例:

```
# cd /data/stabackups

# ls -l

20130721_133755.conf.zip.gz
20130721_133755.fmwconfig.zip.gz
20130721_133755.stadb-bin.000024.gz
20130721_133755.stafullbackup.sql.gz
20130722_133755.conf.zip.gz
20130722_133755.fmwconfig.zip.gz
20130722_133755.stadb-bin.000024.gz
20130722_133755.stafullbackup.sql.gz
20130723_133755.conf.zip.gz
20130723_133755.fmwconfig.zip.gz
20130723_133755.stadb-bin.000021.gz
20130723_133755.stadb-bin.000022.gz
20130723_133755.stadb-bin.000023.gz
20130723_133755.stadb-bin.000024.gz
20130723_133755.stafullbackup.sql.gz
```

ファイル名のタイムスタンプの形式は `YYYYMMDD_HHMMSS` です。同じ日付のタグが付いたバイナリログはすべて、完全ダンプのロード後にデータベースで再生されます。

ここでは、次の管理タスクについて説明します。

- [「バックアップファイルのサーバーへのコピー」](#)
- [「構成ディレクトリファイルの復元」](#)
- [「データベースの復元」](#)

- 「特定時点の復元」

2.7.1. バックアップファイルのサーバーへのコピー

バックアップファイルを STA サーバーにコピーするには、この手順を使用します。

1. 1 日分のファイルをすべてコピーして STA サーバーに戻します。

Oracle では、`/tmp` ディレクトリにすべてをコピーすることをお勧めしています。たとえば、STA がサーバー `sta.server.com` にインストールされていて、現在バックアップサーバーにログオンしているとします。

```
# scp 20130723*.* sta.server.com:/tmp/.
```

```
Password:
```

2. STA サーバーに root としてログインします。
3. *.gz ファイルを解凍します。例:

```
# cd /tmp
```

```
# gunzip 20130723*.*.gz
```

2.7.2. 構成ディレクトリファイルの復元

構成ディレクトリファイルを復元するには、この手順を使用します。

1. すべての STA プロセスを停止します。次に、MySQL サーバーのみを再起動します。

```
# STA stop all
```

```
# STA start mysql
```

2. STAServer および STA サービスデーモンの構成ディレクトリを解凍します。

zip ファイルは完全ディレクトリパスで作成されており、既存ファイルの復元または上書きが可能です。`unzip` コマンドでは、`-d` オプションを使用して復元パスのルートを先頭に付け直すことができます。その他のオプションを使用して、選択的な置換など、操作を細かく制御できます。

全面的な復元の場合、既存の構成ディレクトリを完全に置換する必要がありますが、最初にオリジナルをバックアップしておいてください。例:

```
# cd $WLSHOME
```



```
# zip -vr fmwconfig.orig.zip fmwconfig

# rm -rf fmwconfig

# cd /tmp

# unzip -X -d/ 20130723_133755.fmwconfig.zip

# cd $STAHOME/common

# zip -vr conf.orig.zip conf

# rm -rf conf

# cd /tmp

# unzip -X -d/ 20130723_133755.conf.zip
```

ここでは:

```
$WLSHOME =/Oracle_storage_home/Middleware/user_projects/domains/TBI/
config
```

```
$STAHOME =/Oracle_storage_home/StorageTek_Tape_Analytics
```

2.7.3. データベースの復元

MySQL のルートユーザーとして、次のコマンドを実行します。

2.7.3.1. データベースのリロード

データベースをリロードするには:

1. stadb データベースが残っている場合は、削除します。例:

```
# mysql -uroot -p -e 'drop database stadb;'
```

Password:

2. 最新の完全ダンプをロードします。スキーマが作成されすべてのデータがインストールされます。例:

```
# mysql -uroot -p -e 'source 20130723_133755.stafullbackup.sql;'
```

Password:

2.7.3.2. Binlog の再生

binlog を再生するには:

1. 各増分ダンプ (binlog) を新しいものから順番に実行します。

MySQL サーバーで複数のバイナリログを実行する場合のもっとも安全な方法は、すべてのバイナリログを 1 つのサーバー接続で処理し、すべてのバイナリログの内容を 1 つの MySQL プロセスで実行することです。

例:

```
# mysqlbinlog 20130723_133755.sta-binlog.000021 /
> 20130723_133755.sta-binlog.000022 /
> 20130723_133755.sta-binlog.000023 /
> 20130723_133755.sta-binlog.000024 |mysql -u root -p
```

別の方法として、すべてのログを 1 つのファイルに連結し、そのファイルを処理する方法もあります。

```
# mysqlbinlog 20130723_133755.sta-binlog.000021 > /tmp/recoversta.sql
# mysqlbinlog 20130723_133755.sta-binlog.000022 >> /tmp/recoversta.sql
# mysqlbinlog 20130723_133755.sta-binlog.000023 >> /tmp/recoversta.sql
# mysqlbinlog 20130723_133755.sta-binlog.000024 >> /tmp/recoversta.sql
# mysql -u root -p -e 'source /tmp/recoversta.sql'
```

注:

コマンド行でパスワードを指定しなかった場合、処理前に MySQL からパスワードの入力を求められます。

2.7.3.2.1. 複数のサーバー接続の回避

次の例のようなバイナリログの処理では、複数のサーバー接続が作成される場合があります。複数の接続を使用すると、最初のログファイルに CREATE TEMPORARY TABLE 文が含まれていて、次のログにその一時テーブルを使用する文が含まれていた場合に問題が発生します。最初の MySQL プロセスが終了したときに、サーバーは一時テーブルを削除します。2 つ目の MySQL プロセスがそのテーブルを使用しようとしたときに、サーバーが「不明テーブル」を報告します。

```
# mysqlbinlog binlog.000001 |mysql -u root -p #<=== DANGER!!  
# mysqlbinlog binlog.000002 |mysql -u root -p #<=== DANGER!!
```

2.7.3.3. すべてのサービスの再起動

Linux システムのルートユーザーとして、次のコマンドを入力します。

```
# STA start all
```

2.7.4. 特定時点の復元

別の復元方法である特定時点の復元では、開始時点と終了時点を指定してバイナリログを再生できます。

たとえば、バイナリログの内容を調査した結果、ログエントリ #6817916 の直後に不正な操作によりいくつかのテーブルが削除されたことが判明した場合などです。前日の完全ダンプからデータベースを復元したあと、すべての STA サービスを再起動する前に、この手順で説明したコマンドを使用して、最新のバイナリログの最初のログエントリ番号 "176" からエントリ番号 "6817916" までを再生します。

2.7.4.1. ログ番号の範囲からの復元

STA データベースをログ番号の範囲から復元するには、この手順を使用します。

1. すべての STA プロセスが停止していて、MySQL サービスのみが実行していることを確認します。

```
# STA stop all
```

```
# STA start mysql
```

2. MySQL ルートユーザーとして、有効な操作を抽出します。例:

```
# mysqlbinlog --start-position=176 --stop-position=6817916
```

```
/var/log/tbi/db/stadb-bin.000007 > ./recover.sql
```

3. それらをデータベースに適用します。例:

```
# mysql -uroot -p -e 'source ./recover.sql'
```

```
Password:
```

4. Linux システムルートユーザーとして、STA アプリケーションと STA サービスデーモンを再起動します。

STA start all

特定時点の復元または増分復元の方法の詳細は、次のサイトにある MySQL のドキュメントを参照してください。

<http://docs.oracle.com/en/database/>

パスワード管理

この章では、STA データベースおよびサービスの各種パスワードの変更方法について説明します。STA ユーザー名のパスワードを変更するには、『STA インストールおよび構成ガイド』を参照してください。

注意:

WebLogic 管理コンソールのログインパスワードは変更しないでください。このパスワードを変更した場合、STA の再インストールが必要になります。

この章は次のセクションで構成されています。

- [STA データベースアカウントパスワードの変更](#)
- [STA バックアップサービスおよびリソースモニターのパスワードの変更](#)

3.1. STA データベースアカウントパスワードの変更

次の手順を実行し、STA データベースルートアカウント、アプリケーションアカウント、レポートアカウント、または DBA アカウントのパスワードを変更します。

注:

STA データベースルートアカウントのパスワードの変更は MySQL データベース管理者だけが行うようにしてください。

1. 次のように開始します。

- STA データベースルートアカウント、レポートアカウント、または DBA アカウントのパスワードを変更する場合は、段階 11 に進みます。
- STA アプリケーションアカウントのパスワードを変更する場合は、次の段階に進み、まずは WebLogic でパスワードを変更します。

注意:

STA アプリケーションアカウントのパスワードを変更する場合は、WebLogic と MySQL データベース間でのパスワードの同期と、すべての STA プロセスの停止および再開が必要になります。一部のライブラリのトランザクションが失われることがあります。Oracle では、この手順を実行する前に STA データベースをバックアップすることをお勧めしています。

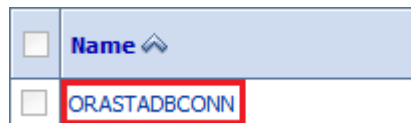
- STA のインストール中に選択した HTTP (デフォルトは 7001) または HTTPS (デフォルトは 7002) のポート番号を使用して、WebLogic コンソールのログイン画面に移動します。
例:

https://yourHostName:PortNumber/console

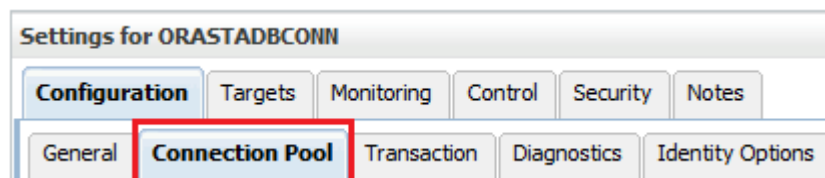
- WebLogic 管理コンソールのユーザー名とパスワードを使用してログインします。
- 「ドメイン構造」メニューから「サービス」を選択し、「データ・ソース」を選択します。



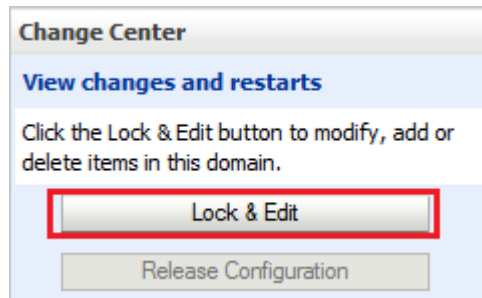
- 「データ・ソース」表の「名前」列で、**ORASTADBCONN** を選択します (チェックボックスではなく名前自体を選択します)。



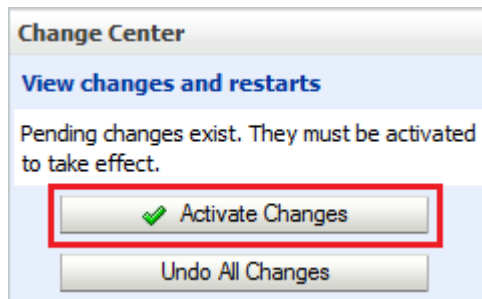
- 「接続プール」タブをクリックします。



- 「チェンジ・センター」セクションで、「ロックして編集」をクリックします。



8. 新しいパスワードを入力して確認し、「保存」をクリックします。
9. 「チェンジ・センター」セクションで、「変更のアクティブ化」をクリックします。



10. WebLogic 管理コンソールからログアウトします。
11. Linux ルートユーザーとして MySQL クライアントにログインします。

```
# mysql -uroot -p  
  
Password: root_password
```

12. 次のコマンドを入力します。

```
mysql> use mysql;
```

13. STA データベースユーザー名のリストを取得します。

```
mysql> select distinct(user) from user order by user;
```

14. パスワードを変更するアカウントユーザー名をメモします。このユーザー名は次の段階で使用します。
15. 次のコマンドを入力して、パスワードを変更します。*new_password* および *username* 変数は引用符で囲みます。

```
mysql> update user set password=PASSWORD('new_password') where user='username';  
  
mysql> commit;  
  
mysql> flush privileges;
```

16. MySQL クライアントを終了します。

```
mysql> quit;
```

17. 新しいログインパスを設定します。この段階は、前の段階でどのデータベースユーザーのパスワードを変更したかによって異なります。

- STA データベースルートアカウントのパスワードを変更した場合:

a. ルートユーザー情報のリストを取得します。

```
# mysql -u root -p -e "select user, host, password from mysql.user where  
user='root'"
```

```
Enter password: new_mysql_root_password
```

出力例:

```
+-----+-----+-----+  
| user | host      | password |  
+-----+-----+-----+  
| root | localhost | *ABCDEF123456789ABCDEF123456789ABCDEF1234 |  
| root | server1   | *ABCDEF123456789ABCDEF123456789ABCDEF1234 |  
| root | 127.0.0.1 | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |  
| root | ::1       | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |  
| root | %         | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |  
+-----+-----+-----+
```

b. 新規ログインパスのパスワードを設定するには、一覧表示された各ホストについて次のコマンドを実行します。たとえば、ホストのリストが前述の出力例に似ている場合、このコマンドを 5 回、*host* の部分を *localhost*、*server1*、*127.0.0.1*、*::1*、*%* に置き換えて実行します。

```
# mysql_config_editor set --login-path=root_path --host=host --user=root --  
password
```

```
Enter password: new_mysql_root_password
```

```
WARNING : 'root_path' path already exists and will be overwritten.
```

```
Continue?(Press y|Y for Yes, any other key for No) : y
```

c. 新規ログインパスをテストするには、一覧表示された各ホストについて次のコマンドを実行します。


```
# mysql --login-path=root_path --host=host
```

```
Welcome to the MySQL monitor. Commands end with ; or \g.
```

```
Your MySQL connection id is 1234
```

```
Server version: 5.6.15-enterprise-commercial-advanced-log MySQL Enterprise
Server - Advanced Edition (Commercial)
```

```
Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.
```

```
Oracle is a registered trademark of Oracle Corporation and/or its affiliates
.Other names may be trademarks of their respective owners.
```

```
Type 'help;' or '/h' for help. Type '/c' to clear the current input
statement.
```

```
mysql> quit
```

```
Bye
```

- STA データベースアプリケーションアカウント、レポートアカウント、または DBA アカウ
ントのパスワードを変更した場合:
 - a. データベースユーザーのリストを取得します。

```
# mysql -u root -p -e "select user, host, password from mysql.user where
user <> 'root'"
```

```
Enter password: mysql_root_password
```

出力例:

```
+-----+-----+-----+
| user   | host   | password                                     |
+-----+-----+-----+
| stadba | localhost | *ABCDEF123456789ABCDEF123456789ABCDEF1234 |
| stadba | %       | *ABCDEF123456789ABCDEF123456789ABCDEF1234 |
| staapp | localhost | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |
| staapp | %       | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |
| staur  | localhost | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |
| staur  | %       | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |
+-----+-----+-----+
```

- b. 新規ログインパスのパスワードを設定するには、一覧表示された各ユーザーおよび関連付けられているホストについて次のコマンドを実行します。たとえば、ユーザーのリストが前述の出力例に似ている場合、このコマンドを 6 回、*user* の部分を各ユーザー名 (*stadba*、*staapp*、または *stausr*) に置き換え、さらに *host* の部分を各ユーザーの各ホスト名 (*localhost* または *%*) に置き換えて実行します。

```
# mysql_config_editor set --login-path=user_path --host=host --user=root --password
```

```
Enter password: new_user_password
```

```
WARNING : 'root_path' path already exists and will be overwritten.
```

```
Continue?(Press y|Y for Yes, any other key for No) : y
```

- c. 新規ログインパスをテストするには、一覧表示された各ユーザーおよび関連付けられているホストについて次のコマンドを実行します。

```
# mysql --login-path=user_path --host=host
```

```
Welcome to the MySQL monitor.  Commands end with ; or /g.
```

```
Your MySQL connection id is 1234
```

```
Server version: 5.6.15-enterprise-commercial-advanced-log MySQL Enterprise Server - Advanced Edition (Commercial)
```

```
Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
```

```
Type 'help;' or '/h' for help. Type '/c' to clear the current input statement.
```

```
mysql> quit
```

```
Bye
```

18. 次のように進めます。

- STA データベースの DBA アカウントパスワードを変更した場合は、「[STA バックアップサービスおよびリソースモニターのパスワードの変更](#)」を参照し、これらのサービスのパスワードを同期します。
- STA データベースアプリケーションアカウントのパスワードを変更した場合は、次の段階に進みます。

- STA データベースルートアカウントまたはレポートアカウントを変更した場合は、ここで終了です。
19. STA サーバーのルートとして、次のコマンドを発行してすべての STA プロセスを停止してから開始します。

```
# STA stop all
```

```
# STA start all
```

STA コマンドの使用方法の詳細は、1章「[サーバー管理](#)」を参照してください。

20. STA セッションの接続を検証します。
 - a. STA のインストール中に選択した HTTP (デフォルトは 7021) または HTTPS (デフォルトは 7022) ポート番号を使用して、STA GUI ログイン画面に移動します。STA は大文字にしてください。例:

```
https://yourHostName:PortNumber/STA
```

- b. STA GUI のログインユーザー名とパスワードを使用してログインします。
 - ダッシュボード画面がすべて入力された状態で表示された場合は、WebLogic サーバーと MySQL データベースの両方で、STA データベースアプリケーションアカウントのパスワードのリセットが成功しています。
 - アプリケーションエラーが表示された場合は、WebLogic で定義したパスワードと MySQL 内の STA データベースアプリケーションアカウントのパスワードが一致していません。パスワードが一致していることを確認してください。

3.2. STA バックアップサービスおよびリソースモニターのパスワードの変更

「[STA データベースアカウントパスワードの変更](#)」で STA データベースの DBA アカウントのパスワードを変更した場合は、このパスワードを STA バックアップサービスとリソースモニター内で更新する必要があります。

1. ディレクトリを変更します。

```
# cd /Oracle_storage_home/StorageTek_Tape_Analytics/common/bin
```

2. STA バックアップサービスとリソースモニターがオンラインになっていることを確認します。
 - バックアップサービス:

```
# ./staservadm -Q
```

```
Contacting daemon...connected.
```

```
...
```

- リソースモニター:

```
# ./staresmonadm -Q
```

```
Contacting daemon...connected.
```

```
...
```

3. システムルートユーザーとして、STA バックアップサービスとリソースモニターのパスワードを次のコマンドを発行してリセットします。ここで、*dba_user* は STA データベースの DBA アカウントのユーザー名、*dba_password* は現在の STA データベースの DBA アカウントのパスワードです。

- バックアップサービス:

```
# ./staservadm -U dba_user -P
```

```
Enter database password: dba_password
```

- リソースモニター:

```
# ./staresmonadm -U dba_user -P
```

```
Enter database password: dba_password
```

注:

コマンド行で **-P** の後ろにパスワードを入力する方法もありますが、セキュアな方法ではないため、お勧めしません。

サービス拒否攻撃の防止

この付録では、STA サーバーに対する Denial of Service (DoS) 攻撃の防止方法について説明します。ライブラリの初期構成が終了してから、これらの手順を実行します。IPTables の構成後、STA が正常にライブラリのモニターを続けていることを確認する必要があります。

この付録は次のセクションで構成されています。

- [概要](#)
- [iptables ルールの構成](#)
- [iptables サンプルスクリプト](#)

注:

この付録の手順はオプションで、情報提供のために記載されています。サイトのセキュリティーはお客様の責任で確保してください。

A.1. 概要

サーバーを DoS 攻撃から防御するため、Linux の *iptables* ソフトウェアを構成し、ポートまたは IP アドレス (あるいはその両方) をフィルタするルールを作成します。STA の構成に基づいて、Oracle ではルールを UDP 162 と STA 管理対象サーバーを実行しているポート値に適用することをお勧めしています。

注:

STA で使用されているデフォルトポート値など、ポート情報については、『*STA インストールおよび構成ガイド*』を参照してください。

[iptables サンプルスクリプト](#)を使用して、サーバーの入力ルールを定義し、接続を試みるホストを次の条件に基づいてブロックできます。

- 特定の Ethernet インタフェース
- 特定のポート
- 特定のプロトコル
- 指定された時間内のリクエスト数。

時間内でホストの接続数が超過すると、残りの時間内のそのホストによる以降の接続がブロックされます。

A.2. iptables ルールの構成

iptables ルールを構成するには:

1. [iptables サンプルスクリプト](#)のソースをテキストエディタにコピーします。
2. 環境に合わせて次の変数を変更します。
 - *INTERFACE* — 攻撃を監視する Ethernet インタフェースを定義します
 - *PORT* — 攻撃を監視するポート番号を定義します
 - *PROTO* — プロトコルを定義します (TCP または UDP)
 - *HITS* および *TIME* — サーバーをブロックするのに妥当と考えられる一定時間内のリクエスト数 (*HITS*) と秒数 (*TIME*) を指定します。
3. スクリプトをシステムに保存して実行します。

新しいルールが iptables に追加され、すぐに有効になります。

A.3. iptables サンプルスクリプト

次は iptables サンプルスクリプトです。

```
# The name of the iptable chain
CHAIN=INPUT

# The ethernet interface to watch for attacks
INTERFACE=eth0

# The port number to watch for attacks
PORT=80

# The protocol (tcp or udp)
PROTO=tcp

# A server that sends HITS number of requests within TIME seconds will be blocked
HITS=8
TIME=60

# Log filtered IPs to file
touch /var/log/iptables.log
grep iptables /etc/syslog.conf 1>/dev/null 2>&1

if [ $? -ne 0 ]; then
    echo kern.warning /var/log/iptables.log >>
```

```
/etc/syslog.conf
echo touch /var/log/iptables.log >> /etc/syslog.conf
/etc/init.d/syslog restart
fi
# Undo any previous chaining for this combination of chain, proto, hits, and time
/sbin/iptables -L $CHAIN |grep $PROTO |grep $HITS |grep $TIME 1>/dev/null 2>&1
if [ $? -eq 0 ]; then
    R=0
    while [ $R -eq 0 ]; do
        /sbin/iptables -D $CHAIN 1 1>/dev/null 2>&1
        R=$?
    done
fi
# Logging rule
/sbin/iptables --append $CHAIN --jump LOG --log-level 4
# Interface rule
/sbin/iptables --insert $CHAIN --proto $PROTO --dport $PORT --in-interface $INTERFACE
--match state --state NEW --match recent --set
# Blocking rule
/sbin/iptables --insert $CHAIN --proto $PROTO --dport $PORT --in-interface $INTERFACE
--match state --state NEW --match recent --update --seconds $TIME --hitcount $HITS --
jump DROP
```


索引

さ

サービス拒否攻撃、防止、
サービスコマンド, 19
サービスデーモン
 開始および停止スクリプト, 30
 概要, 21
 管理ログ, 32
 構成ファイル, 34
 バックアップファイルの場所, 32
 ログ, 35

た

データベースサービス
 管理の概要,
 実行可能プログラムの場所, 31
データベースの復元, 39

は

パスワード
 データベースアカウントの変更, 45
 バックアップサービスの変更, 51
 変更,
 リソースモニターの変更, 51
パスワードの変更,
バックアップサービス
 概要, 22
 管理ユーティリティー, 31
 構成, 22
 ターゲットサーバーにファイルが送信されたことの
 確認, 24
 ダンプファイル, 33
 バイナリログ, 33
 ファイルの場所, 32
 プリファレンス設定のクリア, 24
 プリファレンス設定の表示, 23
 プロセス, 23
 ローカルバックアップファイルの確認, 26
 ログ, 32
 ファイルのタイプと場所, 30
復元、データベース, 39

ら

リソースモニターサービス

CSV ファイル, 35
概要, 26
管理ユーティリティー, 31
構成, 27
標準レポート, 28
ファイルの場所, 35
プリファレンス設定のクリア, 27
プリファレンス設定の問い合わせ, 27
リソース減少警告レポート, 29
レポートの概要, 28
レポート
 概要, 28
 標準レポート, 28
 リソース減少警告レポート, 29
ログ
 MySQL バイナリ, 33
 ResMonAdm, 35
 構成ファイル, 37
 サービスデーモン管理, 32, 35
 バックアップ, 32

S

STA コマンド, 18
STA サーバー
 管理,
 管理コマンド, 18
 管理対象サーバー, 17
 サービスコマンド, 19
 メモリー使用要件, 18
STA プロセスの開始, 18
STA プロセスの確認, 18
STA プロセスの停止, 18

W

WebLogic 構成ファイル, 34
