

StorageTek Tape Analytics

インストールおよび構成ガイド

バージョン 2.1.0

E60939-02

2015 年 2 月

StorageTek Tape Analytics
インストールおよび構成ガイド

E60939-02

Copyright © 2013, 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さまざま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場合、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	21
対象読者	21
ドキュメントのアクセシビリティ	21
関連ドキュメント	21
STA アプリケーションのユーザー向け	21
STA サーバーと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	22
表記規則	22
新機能	25
STA 2.1.0 (2015 年 1 月)	25
1. インストール前の計画	29
1.1. STA の配備の概要	29
1.2. ライブラリを準備するためのサービスリクエストの準備	30
2. Linux のインストール	31
2.1. 準備タスク	32
2.1.1. 関連ドキュメントの確認	32
2.1.2. STA ファイルシステムレイアウトの確認	32
2.1.3. Linux インストーラメディアパックのダウンロード	35
2.2. インストールタスク	36
2.2.1. 必要な情報の収集	36
2.2.2. Linux のインストール	36
2.2.3. Linux Setup Agent の実行	39
2.3. インストール後のタスク	40
2.3.1. SELinux の無効化	40
2.3.2. Linux ファイアウォールの無効化	40
2.3.3. アクセス制御の無効化	41

2.3.4. ネットワークプロキシの設定	42
2.3.5. yum の正しい設定の確認 (オプション)	42
2.3.6. 必要な Linux パッケージのインストール	44
2.3.7. SSH の正しい設定の確認	45
2.3.8. 正しい DNS 設定の確認	46
2.3.9. ネームサービスの無効化	46
2.3.10. ローカルブラウザ機能の確認 (オプション)	47
3. STA のインストール	49
3.1. STA インストーラで使用するユーザー、グループ、場所	49
3.2. ユーザー名およびパスワードの要件	51
3.3. STA のインストール中に構成されるアカウントおよびポート	52
3.3.1. STA を管理するためのユーザーアカウント	52
3.3.1.1. WebLogic アカウント	52
3.3.1.2. STA データベースアカウント	53
3.3.2. STA が使用するポート	53
3.3.2.1. 構成不可の外部ポート	54
3.3.2.2. 構成可能な外部ポート	54
3.3.2.3. 構成可能な内部ポート	55
3.4. STA のインストールおよびアンインストールのログ	55
3.4.1. ログファイルの場所	56
3.5. STA インストーラのモード	57
3.6. STA のインストールタスク	57
3.6.1. インストールに必要な情報の特定および作成	58
3.6.2. インストールの前提条件の確認	60
3.6.3. STA のダウンロード	63
3.6.4. STA のインストール	64
3.6.5. 正常なインストールの確認	65
3.6.6. STA のログディレクトリの再配置 (オプション)	67
3.6.7. Oracle 中央インベントリの場所の登録	69
4. STA のライブラリ機能の構成	71

4.1. STA データに影響を及ぼすライブラリ機能	71
4.1.1. LTO ドライブ用の ADI インタフェース	71
4.1.1.1. LTO ドライブでの ADI の有効化	72
4.1.1.2. ライブラリでの ADI の有効化	72
4.1.2. デュアル TCP/IP および冗長電子装置 (SL3000 および SL8500 のみ)	73
4.1.2.1. これらの機能をサポートするように STA 接続を構成	73
4.1.2.2. これらの機能に関するその他の考慮事項	74
4.1.3. ライブラリコンプレックス ID (SL8500 のみ)	74
4.1.4. ドライブのクリーニング警告 (SL3000 および SL8500 のみ)	75
4.1.5. ボリュームラベル形式 (SL500 および SL150 のみ)	76
4.1.6. 「SCSI FastLoad」オプション (SL500 のみ)	76
4.1.7. 重複するボリュームシリアル番号	77
4.2. ライブラリのユーザーインタフェース	77
4.2.1. ライブラリ CLI の使用上のヒント	77
4.2.2. ライブラリ構成スクリプト (オプション)	78
4.3. ライブラリ機能構成タスク	78
4.3.1. ライブラリへのログイン	79
4.3.2. ライブラリファームウェアバージョンの確認	80
4.3.3. ドライブコントローラカードのバージョンの確認 (SL3000 および SL8500 のみ)	81
4.3.4. ライブラリでの ADI の有効化 (SL150 を除くすべてのライブラリ)	82
4.3.5. 正しいライブラリコンプレックス ID の確認 (SL8500 のみ)	83
4.3.6. ドライブのクリーニング警告の設定 (オプション、SL3000 および SL8500 のみ)	84
4.3.7. SL500 ボリュームラベル形式の設定 (SL500 のみ)	84
4.3.8. SL150 ボリュームラベル形式およびドライブ要素アドレッシングモードの設定 (SL150 のみ)	85
5. ライブラリでの SNMP の構成	87
5.1. STA のライブラリ SNMP 構成について	87
5.1.1. ライブラリでの SNMP v3 プロトコルの構成	88
5.1.1.1. 一意の SNMP v3 ユーザー	88

5.1.1.2. SNMP エンジン ID	89
5.2. ライブラリ SNMP 構成タスク	89
5.2.1. ライブラリ IP アドレスの取得	90
5.2.2. ライブラリでの SNMP の有効化	92
5.2.3. SNMP v2c ユーザーの確認	93
5.2.4. SNMP v3 ユーザーの作成	95
5.2.5. ライブラリ SNMP エンジン ID の取得 (SL150 を除くすべてのライブラリ)	97
5.2.6. STA SNMP v3 トラップ受信者の作成	97
6. STA でのライブラリ接続の構成	101
6.1. STA 構成タスク	101
6.1.1. STA へのログイン	101
6.1.2. ライブラリとのSNMP 通信の検証	102
6.1.3. STA の SNMP クライアント設定の構成	105
6.1.4. ライブラリへのSNMP 接続の構成	107
6.1.5. ライブラリへの SNMP 接続のテスト	109
6.1.6. 手動データ収集の実行	110
7. STA サービスの構成	113
7.1. STA サービスの概要	113
7.2. STA サービスの構成タスク	113
7.2.1. システムパスの更新 (オプション)	114
7.2.2. STA サービスデーモンの再起動 (オプション)	114
7.2.3. ライブラリ接続の確認	115
7.2.4. STA データベースバックアップユーティリティープリファレンスの確認	115
7.2.5. リモートデータベースバックアップサーバーの構成	116
7.2.6. STA データベースバックアップサービスの構成	118
7.2.7. STA リソースモニターユーティリティープリファレンスの確認	120
7.2.8. STA リソースモニターの構成	122
8. STA 2.1.0 へのアップグレード	125

8.1. アップグレードプロセスの概要	125
8.2. 有効な STA 2.1.0 のアップグレードパス	126
8.3. アップグレード方法	126
8.3.1. 1 台のサーバーのアップグレード方法	126
8.3.2. 2 台のサーバーのアップグレード方法	128
8.4. STA 2.1.0 の環境の変更	129
8.4.1. Linux バージョン	129
8.4.2. デフォルトの WebLogic ポート番号	130
8.4.3. STA 2.0.x 以降に必要なポート	130
8.4.4. ユーザー名およびパスワードの要件	130
8.5. アップグレード準備タスク	131
8.5.1. サイトのアップグレード準備済みの確認	131
8.5.1.1. アップグレード前提条件の確認	132
8.5.1.2. 現在の STA アクティビティの確認	132
8.5.2. 既存のログの保存 (オプション)	133
8.5.3. 現在の STA のユーザーおよび構成設定の記録 (オプション)	134
8.5.3.1. MySQL ユーザー名の記録	134
8.5.3.2. STA の SNMP クライアント設定の記録	134
8.5.3.3. WebLogic ユーザー名の記録 - STA 1.0.x からのアップグレードのみ	135
8.5.3.4. STA ユーザー名の記録 - STA 2.0.x からのアップグレードのみ	138
8.5.3.5. STA の電子メールサーバー設定の記録	138
8.5.4. 接頭辞に STA- の付くカスタムテンプレートの名前の変更 (オプション)	139
8.5.5. 現在のカスタムテンプレート設定の記録 (オプション)	140
8.5.6. エグゼクティブレポートポリシー設定の記録 (オプション)	140
8.6. アップグレードタスク	141
8.6.1. タスク 1: 古い STA データベースのダンプ	142
8.6.2. タスク 2: 古いデータベースダンプの転送	144
8.6.3. タスク 3a: 新しい Linux バージョンのインストール (STA 1.0.x からのアップグレード)	145

8.6.4. タスク 3b: 古い STA バージョンのアンインストール (STA 2.0.x からのアップグレード)	145
8.6.5. タスク 4: 新しい STA バージョンのインストール	146
8.6.6. タスク 5: 新しい STA データベースのダンプ (オプション)	147
8.6.7. タスク 6: 古い STA データベースの STA サーバーへの転送	148
8.6.8. タスク 7: 古い STA データベースの処理およびロード	149
8.6.9. タスク 8: 古いデータベースのアップグレード	151
8.6.10. タスク 9: 新しい STA バージョンの構成	154
8.6.10.1. ライブラリでの STA トラップ受信者の更新	154
8.6.10.2. STA での SNMP 設定の構成	155
8.6.10.3. STA サービスおよびユーザー情報の構成	156
8.6.10.4. 古い STA サーバーの廃止 (オプション)	157
8.6.11. 失敗したデータベースアップグレードの回復 (オプション)	157
9. STA のアンインストールと復元	159
9.1. STA のアンインストールの概要	159
9.2. STA のアンインストールタスク	160
9.2.1. STA のアンインストール	160
9.2.2. アンインストールが成功したことの確認	161
9.2.3. STA の復元	161
A. STA グラフィカルインストーラおよびアンインストーラの画面リファレンス	165
A.1. グラフィカルモードの表示要件	165
A.1.1. ローカル接続	166
A.1.2. Secure Shell (SSH) を使用したリモート接続	166
A.1.2.1. Linux マシンからの接続	166
A.1.2.2. Microsoft Windows PC からの接続	166
A.1.3. デスクトップ共有を使用したリモート接続	167
A.1.4. グラフィカル表示上の問題のトラブルシューティング	167
A.2. STA グラフィカルインストーラの画面	169
A.2.1. インストールおよびインベントリの設定	170
A.2.1.1. 画面のフィールド	170

A.2.1.2. 画面固有のボタン	171
A.2.2. ようこそ	171
A.2.2.1. インストーラの一般的な画面レイアウト	172
A.2.3. インストール場所	174
A.2.3.1. 画面のフィールド	174
A.2.3.2. 画面固有のボタン	175
A.2.4. 前提条件チェック	177
A.2.4.1. 画面のフィールド	179
A.2.4.2. 画面固有のボタン	179
A.2.5. ルートパスワードの入力	181
A.2.5.1. 画面のフィールド	181
A.2.5.2. 画面固有のボタン	181
A.2.6. DB ディレクトリの設定	182
A.2.6.1. 画面のフィールド	182
A.2.6.2. 画面固有のボタン	183
A.2.7. 管理者アカウントの設定	183
A.2.7.1. 画面のフィールド	184
A.2.7.2. 画面固有のボタン	184
A.2.8. WebLogic 管理者	184
A.2.8.1. 画面のフィールド	185
A.2.8.2. 画面固有のボタン	185
A.2.9. STA 管理者	186
A.2.9.1. 画面のフィールド	186
A.2.9.2. 画面固有のボタン	187
A.2.10. データベースアカウントの設定	188
A.2.10.1. 画面のフィールド	188
A.2.10.2. 画面固有のボタン	188
A.2.11. データベースルートユーザー	189
A.2.11.1. 画面のフィールド	190
A.2.11.2. 画面固有のボタン	190
A.2.12. データベースアプリケーションユーザー	191
A.2.12.1. 画面のフィールド	192
A.2.12.2. 画面固有のボタン	192

A.2.13. データベースレポートユーザー	193
A.2.13.1. 画面のフィールド	193
A.2.13.2. 画面固有のボタン	194
A.2.14. データベース管理者	195
A.2.14.1. 画面のフィールド	196
A.2.14.2. 画面固有のボタン	196
A.2.15. 通信ポートの入力	197
A.2.15.1. 画面のフィールド	197
A.2.15.2. 画面固有のボタン	198
A.2.16. WebLogic 管理コンソール	198
A.2.16.1. 画面のフィールド	199
A.2.16.2. 画面固有のボタン	199
A.2.17. STA エンジン	199
A.2.17.1. 画面のフィールド	200
A.2.17.2. 画面固有のボタン	200
A.2.18. STA アダプタ	201
A.2.18.1. 画面のフィールド	201
A.2.18.2. 画面固有のボタン	202
A.2.19. STA UI	202
A.2.19.1. 画面のフィールド	203
A.2.19.2. 画面固有のボタン	203
A.2.20. 診断エージェント	204
A.2.20.1. 画面のフィールド	204
A.2.20.2. 画面固有のボタン	204
A.2.21. インストールサマリー	205
A.2.21.1. 画面のフィールド	206
A.2.21.2. 画面固有のボタン	206
A.2.22. インストールの進行状況	207
A.2.22.1. 画面のフィールド	208
A.2.22.2. 画面固有のボタン	208
A.2.23. 構成の進行状況	209
A.2.23.1. 画面のフィールド	210
A.2.23.2. 画面固有のボタン	210

A.2.24. インストール完了	211
A.2.24.1. 画面のフィールド	211
A.2.24.2. 画面固有のボタン	212
A.3. STA グラフィカルアンインストーラの画面	212
A.3.1. ようこそ	212
A.3.1.1. 画面のフィールド	213
A.3.1.2. 画面固有のボタン	213
A.3.2. ルートパスワードの入力	213
A.3.2.1. 画面のフィールド	214
A.3.2.2. 画面固有のボタン	214
A.3.3. アンインストールサマリー	214
A.3.3.1. 画面のフィールド	215
A.3.3.2. 画面固有のボタン	215
A.3.4. アンインストールの進行状況	215
A.3.4.1. 画面のフィールド	216
A.3.4.2. 画面固有のボタン	216
A.3.5. アンインストール完了	218
A.3.5.1. 画面のフィールド	218
A.3.5.2. 画面固有のボタン	218
B. STA サイレントモードインストーラおよびアンインストーラ	219
B.1. STA サイレントモードインストーラおよびアンインストーラの使用	219
B.1.1. サイレントモードの要件	219
B.2. サイレントモードで使用されるファイルとユーティリティ	220
B.3. STA サイレントモードインストーラのタスク	223
B.3.1. Oracle 中央インベントリポインタファイルの作成	223
B.3.2. サイレントモードインストーラの応答ファイルの作成	224
B.3.3. サイレントモードインストーラの実行	227
B.4. STA サイレントモードアンインストーラのタスク	228
B.4.1. サイレントモードアンインストーラの応答ファイルの作成	229
B.4.2. サイレントモードアンインストーラの実行	231
B.5. STA インストーラコマンドオプション	232
B.5.1. サイレントモードオプション	233

B.5.2. ロギングオプション	233
B.5.3. その他のオプション	234
C. インストールおよびアップグレードのワークシート	235
C.1. アップグレード準備ワークシート	235
C.2. インストールおよびアップグレードのワークシート	236
C.2.1. インストールユーザーおよび場所のワークシート	236
C.2.2. ユーザーアカウントワークシート	237
C.2.3. ポート番号ワークシート	238
C.2.4. ドメイン名ワークシート	240
C.3. インストール後の構成ワークシート	240
D. セキュリティー証明書の構成	243
D.1. セキュリティー証明書の構成タスク	243
D.1.1. 初期 HTTPS/SSL 接続の確立	243
D.1.2. 別のセキュリティー証明書を使用するように WebLogic を再構成	244
D.1.3. Oracle 証明書の置換	252
E. セキュリティーサービスプロバイダの STA 用の構成	253
E.1. WebLogic OpenLDAP による STA のアクセス制御	253
E.1.1. WebLogic OpenLDAP の構成	253
E.2. IBM RACF タスクによる STA のアクセス制御	257
E.2.1. タスク 1: IBM RACF メインフレームの最小要件の確認	258
E.2.2. タスク 2: STA RACF 承認のためのメインフレームサポートの有効 化	258
E.2.3. タスク 3: AT-TLS の構成	259
E.2.4. タスク 4: CGI ルーチンによって使用される RACF プロファイルの作 成	266
E.2.5. タスク 5: 証明書ファイルと秘密鍵ファイルのインポート (オプショ ン)	266
E.2.6. タスク 6: CGI ルーチンのテスト	267
E.2.7. タスク 7: WebLogic コンソール用の RACF/SSP の設定	267
E.2.8. タスク 8: STA と RACF 間の SSL の構成	267

E.2.9. タスク 9: WebLogic Server の構成	268
E.2.10. タスク 10: WebLogic コンソールでの RACF/SSP のインストール	268
F. SNMP v2c モードの構成	273
F.1. SNMP v2c 構成タスク	273
F.1.1. SNMP v2c モードの構成	273
F.1.2. ライブラリでの STA SNMP v2c トラップ受信者の作成	274
F.1.3. STA の SNMP v2c モードの有効化	275
索引	277

図の一覧

8.1. 1 台のサーバーのアップグレードタスクの概要	127
8.2. 2 台のサーバーのアップグレードタスクの概要	129
A.1. Oracle ストレージホームのリストの例	176
A.2. メインウィンドウ内のタスクを選択することで表示されるタスクの詳細	178
A.3. 展開アイコンを選択することで表示されるタスクの詳細	179
A.4. 前提条件の検証ログの表示の例	180
A.5. インストールの進行状況ログの表示の例	208
A.6. 構成の進行状況の詳細の例	210
A.7. アンインストールの進行状況ログの表示の例	217

表の一覧

2.1. Linux インストールタスク	31
2.2. 推奨されるファイルシステムレイアウト	33
2.3. Linux パッケージの選択	37
3.1. 構成不可の外部ポート	54
3.2. 構成可能な外部ポート	54
3.3. 構成可能な内部ポート	55
4.1. IBM LTO ドライブで ADI を有効にする方法	72
4.2. STA 接続のための推奨されるライブラリ IP アドレス	74
4.3. コンプレックス ID の割り当ての例	75
4.4. STA のライブラリを構成するためのタスク	78
5.1. STA のライブラリを構成するためのタスク	89
7.1. STA バックアップサービス管理ユーティリティ (staservadm) の属性	115
7.2. STA リソースモニター (staresmonadm) の属性	120
8.1. アップグレード準備タスクを実行するタイミングのガイドライン	131
C.1. アップグレード準備アクティビティ	235
C.2. インストールユーザーおよび場所のワークシート	237
C.3. ユーザーアカウントワークシート	238
C.4. 構成不可の外部ポート	239
C.5. 構成可能な内部ポートおよび外部ポート	239
C.6. 会社のドメイン名	240
C.7. SNMP v3 ユーザーの構成情報	240

例の一覧

3.1. STA の正常なステータス表示	66
4.1. スタンドアロン SL8500 のコンプレックス ID の変更	83
5.1. SL3000 または SL8500 での SNMP v3 ユーザーの作成	95
5.2. SL500 での SNMP v3 ユーザーの作成	96
5.3. SL3000 または SL8500 での SNMP v3 トラップ受信者の作成	98
5.4. SL500 での SNMP v3 トラップ受信者の作成	98
6.1. 成功した snmpget コマンド	103
6.2. 失敗した snmpget コマンド - ネットワークタイムアウト	103
6.3. 失敗した snmpget コマンド - 無効なパスワード	103
8.1. 古いデータベースのダンプ	143
8.2. バックアップサーバーへの古いデータベースの転送 (1 台のサーバーの方法)	144
8.3. 新しい STA サーバーへの古いデータベースの転送 (2 台のサーバーの方法)	145
8.4. 新しいデータベースのダンプ	147
8.5. 新しい STA サーバーへの古いデータベースの転送	148
8.6. 古いデータベースバックアップからの廃止されたデータのパージ	150
A.1. 正しく構成された X11 ディスプレイの例	168
A.2. 正しく構成されていない X11 ディスプレイの例	168
B.1. STA サイレントモードインストーラの応答ファイルのテンプレート	221
B.2. STA サイレントモードアンインストーラの応答ファイルのテンプレート	222
B.3. インストーラの応答ファイル構築ユーティリティーの実行例	225
B.4. 構築ユーティリティーの使用後のインストーラユーティリティーファイルの例	226
B.5. 成功した STA サイレントモードインストールの最終メッセージ	228
B.6. 失敗した STA サイレントモードインストールの最終メッセージの例	228
B.7. アンインストーラの応答ファイル構築ユーティリティーの実行例	229
B.8. 構築ユーティリティーの使用後のアンインストーラの応答ファイルの例	230
B.9. 成功した STA サイレントモードアンインストールの最終メッセージ	232
B.10. 失敗した STA サイレントモードアンインストールの最終メッセージの例	232

はじめに

このドキュメントでは、Oracle の StorageTek Tape Analytics (STA) のインストールおよび構成の概念と手順について説明します。

対象読者

このドキュメントは、次の読者を対象としています。

- Linux 管理者: STA サーバーでの Linux のインストール、構成、および管理をします。
- STA 管理者: STA アプリケーションのインストール、構成、および管理をします。
- ライブラリ管理者: StorageTek ライブラリの構成および管理をします。
- MVS システムプログラマ: IBM メインフレームユーザーによる STA へのアクセスの構成および管理をします。

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 を通じ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』— このガイドでは、STA アプリケーションおよび一部のユーザーインターフェース機能の概要について学びます。
- 『STA ユーザーズガイド』— このガイドでは、ダッシュボード、テンプレート、フィルタ、アラート、Executive Report、論理グループ、STA メディア検証などの STA アプリケーション機能の使用方法について学びます。このガイドでは、STA のユーザー名、電子メールアドレス

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についても説明します。

- 『*STA 画面基本ガイド*』— このガイドでは、STA ユーザーインターフェースの詳細を学びます。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 サーバーと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 をインストールして使用する前に、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*』— このガイドでは、STA を使用するための最小要件および推奨要件について学びます。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 のインストールを計画し、Linux オペレーティングシステムをインストールし、STA アプリケーションをインストールして、ライブラリのモニタリングを開始するように STA を構成する際に使用します。このガイドでは、新バージョンの STA にアップグレードする手順についても説明します。
- 『*STA 管理ガイド*』— このガイドでは、STA サービス構成、データベースのバックアップと復元、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について学びます。
- 『*STA セキュリティーガイド*』— このドキュメントでは、要件、推奨事項、一般的なセキュリティー原則などの重要な STA セキュリティー情報を参照できます。
- 『*STA ライセンス情報ユーザーマニュアル*』— このドキュメントでは、STA 製品とともに配布されるサードパーティーテクノロジーの使用に関する情報を参照できます。

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
太字	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。
斜体	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ー変数を示します。

表記規則	意味
モノスペース	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 v2.1.0 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、次のマニュアルを参照してください。

『STA 要件ガイド』に記載

- STA 2.1.0 に対応した新しいライブラリおよびドライブ推奨の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 に対応する更新された推奨ライブラリおよびドライブ要件。
- 更新された推奨の STA サーバー構成。

『STA インストールおよび構成ガイド』に記載

- 次の新しい機能を備えた、新しい STA 2.1.0 インストーラおよびアンインストーラ
 - Oracle インストールユーザーおよびグループ — STA サーバー上での Oracle 製品のインストールおよびアップグレードに排他的に使用される 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 中央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アン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アン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アン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』に記載

- 大きな変更なし

『STA ユーザーズガイド』に記載

- 追加情報の提供およびユーザビリティの向上のため、次のテンプレートを若干更新しています。
 - 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 — 『STA 管理ガイド』から次の章を移動しました。今回の『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およびアクティビティが記載されています。
 - STA ユーザー名および電子メール
 - STA サービスログ
 - STA での SNMP 接続の管理

『STA 画面基本ガイド』に記載

- 大きな変更なし

『STA データリファレンスガイド』に記載

- ユーザビリティの向上のため、一部の画面の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**』に記載

- 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。
 - ユーザーおよび電子メール
 - ログイン
 - SNMP 管理

インストール前の計画

この章には次のセクションが含まれます。

- [STA の配備の概要](#)
- [ライブラリを準備するためのサービスリクエストの準備](#)

1.1. STA の配備の概要

STA をはじめてインストールして構成する場合は、次のアクティビティーを示された順序で実行します。このプロセスを自分で実行することも、Oracle インストールサービスを購入することもできます。

STA を以前のバージョンからアップする場合は、[8章「STA 2.1.0 へのアップグレード」](#)を参照してください。

順序	アクティビティー	詳細と手順
1	ユーザーのサイトで STA 要件を見直して確認します。	『STA 要件ガイド』
2	必要に応じて、ドライブとライブラリのサービスリクエストを準備します。	「ライブラリを準備するためのサービスリクエストの準備」
3	Linux を STA サーバーにインストールします。	2章「Linux のインストール」
4	STA を STA サーバーにインストールします。	3章「STA のインストール」
5	データを STA に送信するようにライブラリを構成します。	5章「ライブラリでの SNMP の構成」
6	データをライブラリから受け取り、モニタリングを開始するように STA を構成します。	6章「STA でのライブラリ接続の構成」
7	その他の STA ユーザー名および電子メールアドレスを構成します。	『STA ユーザーズガイド』
8	STA モニタリングサービスおよびデータベースバックアップサービスを構成します。	7章「STA サービスの構成」
9	承認済みのセキュリティー証明書を構成します (オプション)。	付録D「セキュリティー証明書の構成」
10	STA アクセス制御用に外部プロバイダを構成します (オプション)。	付録E「セキュリティーサービスプロバイダの STA 用の構成」

1.2. ライブラリを準備するためのサービスリクエストの準備

ライブラリを STA によるモニタリング用に準備するために必要な情報を Oracle サポートに提供するには、この手順と参照されるセクションを使用します。

注:

STA がライブラリコンプレックスをモニターする場合、コンプレックス内のライブラリごとにサービスリクエストを準備します。さらに、STA でサポートされる最新のドライブファームウェアをインストールするためのサービスリクエストをオープンします。

1. ライブラリファームウェアのバージョンを確認します。「[ライブラリファームウェアバージョンの確認](#)」を参照してください
2. ハイメモリー HBT カードが取り付けられていることを確認します (SL3000 および SL8500 のみ)。「[ドライブコントローラカードのバージョンの確認 \(SL3000 および SL8500 のみ\)](#)」を参照してください。
3. ライブラリと LTO ドライブで ADI を有効にします (LTO ドライブのあるライブラリの場合のみ)。「[ライブラリでの ADI の有効化 \(SL150 を除くすべてのライブラリ\)](#)」を参照してください
4. ライブラリコンプレックス ID を設定します (SL8500 のみ)。「[正しいライブラリコンプレックス ID の確認 \(SL8500 のみ\)](#)」を参照してください。
5. ライブラリの日付と時間を設定します。ライブラリデータの日付/タイムスタンプを確実に STA サーバーの日付/タイムスタンプと関連させるには、Oracle サポートによってライブラリのクロックを適切に設定する必要があります。
6. 必要なサービスリクエストを送信します。

Linux のインストール

この章には次の内容が含まれます。

- [準備タスク](#)
- [インストールタスク](#)
- [インストール後のタスク](#)

STA サーバーに Linux をインストールする前に、『[STA 要件ガイド](#)』でシステム要件を確認してください。

注:

Linux 5.x から Linux 6.x へのインプレースアップグレードは実行できません。STA 2.0.x へのアップグレードの一環として Linux 6.x をインストールする場合は、[8章「STA 2.1.0 へのアップグレード」](#)を参照してください

STA 用に Linux をインストールして構成するには、[表2.1「Linux インストールタスク」](#)のタスクを示された順序で実行します。

表2.1 Linux インストールタスク

カテゴリ	タスク
準備	<ol style="list-style-type: none">1. 32 ページの「関連ドキュメントの確認」2. 35 ページの「Linux インストーラメディアパックのダウンロード」
インストール	<ol style="list-style-type: none">1. 36 ページの「必要な情報の収集」2. 36 ページの「Linux のインストール」3. 39 ページの「Linux Setup Agent の実行」
インストール後	<ol style="list-style-type: none">1. 40 ページの「SELinux の無効化」2. 40 ページの「Linux ファイアウォールの無効化」3. 41 ページの「アクセス制御の無効化」4. 42 ページの「ネットワークプロキシの設定」5. 42 ページの「yum の正しい設定の確認 (オプション)」

カテゴリ	タスク
	6. 44 ページの「必要な Linux パッケージのインストール」
	7. 45 ページの「SSH の正しい設定の確認」
	8. 46 ページの「正しい DNS 設定の確認」
	9. 46 ページの「ネームサービスの無効化」
	10. 47 ページの「ローカルブラウザ機能の確認 (オプション)」

2.1. 準備タスク

Linux を STA サーバーにインストールする前に、次の手順を実行します。

- [「関連ドキュメントの確認」](#)
- [「STA ファイルシステムレイアウトの確認」](#)
- [「Linux インストーラメディアパックのダウンロード」](#)

2.1.1. 関連ドキュメントの確認

ネットワーク構成の要件とオプションは多岐にわたるため、ハードウェア、ソフトウェア、およびネットワークのインストールと構成のヘルプについては、次のドキュメントを参照してください。これらのドキュメントでは、IPv4 および IPv6 のネットワーク構成が詳細に説明されています。

- Oracle Linux のインストールガイド:
<http://docs.oracle.com/en/operating-systems/>
- RedHat Linux ドキュメント:
<https://access.redhat.com/home>

2.1.2. STA ファイルシステムレイアウトの確認

[表2.2「推奨されるファイルシステムレイアウト」](#)に、STA サーバーの推奨されるファイルシステムレイアウトを示します。レイアウトの構成は Linux のインストール中にします。

次の場所はユーザー定義であり、サイトの要件を満たすようにレイアウトを構成できることを意味します。

- Oracle ストレージホーム — STA インストーラで、この場所を入力するよう求められます。デフォルトはありません。詳細は、[Oracle ストレージホームの場所](#)を参照してください。
- STA データベース — STA インストーラで、この場所を入力するよう求められます。デフォルトは `/dbdata` です。

- STA データベースのローカルバックアップ — STA インストーラで、この場所を入力するよう求められます。デフォルトは `/dbbackup` です。
- STA と MySQL のログ — デフォルトは `/var/log/tbi` です。Linux のインストール完了後で STA のインストール前に、別の場所を使用することにした場合は、STA のインストールが終わったあとで、その場所から `/var/log/tbi` へのシンボリックリンクを作成する必要があります。手順については、「[STA のログディレクトリの再配置 \(オプション\)](#)」を参照してください。

Oracle では、STA のインストール前にこれらのファイルシステムをすべて作成することをお勧めします。そうしないと、STA がルート「/」ディレクトリと `/var` ディレクトリにインストールされ、これらのディレクトリへの追加の領域割り当てが必要になります。STA インストーラは必要に応じてディレクトリを作成しますが、ファイルシステムを事前に作成しておけば、ファイルシステムプロパティをうまく制御できます。

表2.2 推奨されるファイルシステムレイアウト

ファイルシステム	デフォルトのマウントポイント	サイズ	説明と推奨事項
ルート	/	最小 32G バイト	このファイルシステムに <code>/tmp</code> が含まれている場合は、最低でも 4G バイトの空き領域を確保するようにしてください。この領域は STA のインストールとアップグレード時に必要になります。
スワップ	なし。メモリーとして定義済み。	RAM サイズの 50 - 100%	スワップ領域に使用されます。
Oracle ストレージホーム	<code>/Oracle</code>	最小 30G バイト 推奨 50G バイト	STA および Oracle Middleware (WebLogic, MySQL, RDA) アプリケーションファイルの場所。 この場所はユーザー定義です。これは、別個のボリューム上の別個のファイルシステムになるようにしてください。STA のインストールとアップグレード用に最低 4G バイトの空き領域を確保します。そのほかに、WebLogic ログローテーション用に 5G バイトの空き領域を確保します。 STA では、次の Oracle Middleware サブディレクトリが自動的に作成されます。 • ローテーションされた WebLogic ログ:

ファイルシステム	デフォルトのマウントポイント	サイズ	説明と推奨事項
			<p><code>/Oracle_storage_home/Middleware/user_projects/domains/TBI/servers</code></p> <ul style="list-style-type: none"> RDA の最新の CLI スナップショット: <p><code>/Oracle_storage_home/Middleware/rda/output</code></p> <ul style="list-style-type: none"> STA GUI スナップショットログバンドル: <p><code>/Oracle_storage_home/Middleware/rda/snapshots</code></p>
STA データベースの場所	<code>/dbdata</code>	250G バイト - 2T バイト	<p>STA データベースの場所。この場所はユーザー定義です。Oracle では、このファイルをルート、スワップ、Oracle ストレージホーム、STA ログのどの場所とも異なる独自のボリュームに入れることを強くお勧めします。パフォーマンス、バックアップ、および保全性の確保のため、ミラー化またはストライプ化された単独のドライブセットを使用することが最善です。</p> <p>必要なサイズは、ライブラリ数、ドライブ数、メディア数、1 日の交換頻度、およびデータの履歴年数に応じて異なります。Oracle では、領域使用率が指定されたパーセントを超えた場合に警告するように STA サービスを構成することをお勧めします。</p>
STA データベースのローカルバックアップの場所	<code>/dbbackup</code>	<code>/dbdata</code> のサイズの 70 - 80%	<p>最新のローカルデータベースバックアップの場所。この場所はユーザー定義です。Oracle では、これを STA データベースとは異なるボリューム上にすること、そしてデータベースの破損や障害に備えてミラー化またはストライプ化されたドライブ上にすることをお勧めします。</p>
STA ログの場所	<code>/var/log/tbi</code>	最小 30G バイト 推奨 50 - 100G バイト	<p>STA および MySQL ログの場所。この場所は、別個のマウントポイントにある別個のボリュームになるようにしてください。その内容は大きくなりすいため、ログローテーションを通じて管理されます。デフォルトの場所は <code>/var/log/tbi</code> ですが、この場所は STA のインストール後にいつでも変更できます。手順については、「STA のログディレクトリの再配置 (オプション)」を参照してください。</p> <p>注: ログローテーションを除き、STA では領域管理を行いません。</p>

ファイルシステム	デフォルトのマウントポイント	サイズ	説明と推奨事項
			警告: /STA_logs/db/stadb_bin.* 内のログファイルを管理するように STA バックアップユーティリティを構成する必要があります。そうしないと、これらのファイルを手動で管理することが必要になる場合があります (詳細は『STA 管理ガイド』を参照)。

2.1.3. Linux インストーラメディアパックのダウンロード

Linux インストーラメディアパックを Oracle Software Deliver Cloud Web サイトからダウンロードするには、次の手順を使用します。このメディアパックは圧縮された ISO イメージファイルとして提供されるため、抽出して任意のポータブルメディア (フラッシュドライブや DVD など) に書き込むことができます。

このタスクを実行する前に、Oracle サポート担当者から Oracle Software Delivery Cloud のユーザー ID とパスワードを取得する必要があります。

1. Web ブラウザを起動し、Oracle Software Delivery Cloud Web サイトに移動します。

<http://edelivery.oracle.com/linux>

2. 「サインイン/登録」をクリックします。
3. Oracle サポートから提供されたユーザー ID とパスワードを入力します。
4. 「条件および規制」画面で、ライセンス契約と輸出規制への同意を示すボックスを選択し、「続行」をクリックします。
5. 「メディア・パック検索」画面で:
 - a. 「製品パックを選択」メニューで、「**Oracle Linux**」を選択します。
 - b. 「プラットフォーム」メニューで、「**x86 64 bit**」(STA では 64 ビットの Linux が必要) を選択します。
 - c. 「実行」をクリックします。
6. Linux バージョンを選択して、「続行」をクリックします。

Linux バージョンの要件については、『STA 要件ガイド』を参照してください。

7. 64 ビットオプションの「ダウンロード」をクリックします。
8. ISO ファイルを保存して、メディアに書き込みます。

2.2. インストーラタスク

次の手順では、グラフィカルインストーラと Setup Agent を使用した Oracle Enterprise Linux (OEL) 6u4 DVD のインストールを想定しています。別のバージョンの Linux をインストールするか、別のメディアを使用するか、あるいはコンソールモードを使用する場合、手順とパッケージが異なる可能性があります。

2.2.1. 必要な情報の収集

システム管理者に連絡して次の情報を取得します。

- STA サーバーのホスト名と IP アドレス
- ネットワークのゲートウェイ IP アドレスとネットマスク
- ネットワークの DNS サーバー IP アドレスと検索ドメイン
- 使用する NTP (Network Time Protocol) サーバーの IP アドレス
- ネットワークプロキシ情報 (該当する場合)

2.2.2. Linux のインストール

Linux のインストールを行うには、次の手順を使用します。

1. インストールメディアを STA サーバーに接続します。
2. メディアの README ファイルの手順を使用して、Linux インストーラを開始します。
3. 「**Install or upgrade an existing system**」を選択します。
4. DVD からインストールする場合は、「CD Found」が画面が表示されます。オプションで、メディアのテストを実行できます。テストをスキップするには、**Tab** キーを押して「**Skip**」オプションを強調表示してから、**Space** キーを押します。
5. 「Welcome」画面で、「**Next**」をクリックします。
6. 言語を選択して、「**Next**」をクリックします。
7. キーボード配列を選択して、「**Next**」をクリックします。
8. 「**Basic Storage Devices**」を選択して、「**Next**」をクリックします。
9. STA サーバーのホスト名を入力して、「**Configure Network**」をクリックします。
10. ネットワークアダプタ名を選択して、「**Edit**」をクリックします。
11. 「**Connect automatically**」と「**Available to all users**」の両方が選択されていることを確認します。
12. 残りのタブでは、ネットワーク管理者の IPv4 または IPv6 の仕様に従ってアダプタを構成します。STA サーバーの静的 IP アドレス、および少なくとも 1 つの DNS サーバーを指定する必要があります。完了したら、「**Apply**」、「**Close**」、および「**Next**」をクリックします。

13. STA サーバーのタイムゾーンを選択して、「**System clock uses UTC**」チェックボックスを選択してから、「**Next**」をクリックします。
14. サーバーの Linux root パスワードを入力して確認し、「**Next**」をクリックします。
15. サーバーで使用するパーティションレイアウトを識別します。
 - a. STA には専用のサーバーが必要なため、Oracle では、「**Use All Space**」を選択することをお勧めします。
 - b. 「**Review and modify partitioning layout**」チェックボックスを選択して、「**Next**」をクリックします。
16. デフォルトは STA の最小要件を満たしていないため、[表2.2「推奨されるファイルシステムレイアウト」](#)を使用してファイルシステムレイアウトを変更します。あるいは、Linux のインストール後に `system-config-lvm` ユーティリティーを使用してファイルシステムを変更することもできます。

完了したら、「**Next**」をクリックします。

17. 準備ができたなら、「**Write changes to disk**」を選択します。
18. ブートローダー画面で、すべてのオプションをそのままにして、「**Next**」をクリックします。
19. ソフトウェア選択画面で、「**Basic Server**」を選択して、リポジトリオプションは変更しません。次に、「**Customize now**」を選択して、「**Next**」をクリックします。
20. パッケージ選択画面で、[表2.3「Linux パッケージの選択」](#)を使用して、パッケージカテゴリごとにパッケージを構成します。
 - a. パッケージカテゴリを選択します。
 - b. 「**Select**」列でパッケージごとにボックスを選択します。
 - c. パッケージでオプションが必要な場合 (+ で示されています) は、親パッケージを強調表示して、「**Optional packages**」ボタンをクリックし、リストで子パッケージを選択してから、「**Close**」をクリックします。
 - d. 「**Deselect**」列でパッケージごとにボックスを選択解除します。
 - e. その他のチェックボックスはそのままにします。

表2.3 Linux パッケージの選択

パッケージカテゴリ	選択	選択解除
Base System	<ul style="list-style-type: none"> • Base • Compatibility libraries • Console internet tools • Java Platform 	<ul style="list-style-type: none"> • Debugging Tools • Dial-up Networking Support • Directory Client • Hardware monitoring utilities

パッケージカテゴリ	選択	選択解除
	<ul style="list-style-type: none"> Legacy UNIX compatibility + <i>ksh-xxxxxxxx-xx.e16.x86_64</i> 	<ul style="list-style-type: none"> Large Systems Performance Network file system client Performance Tools
Servers (オプション)	<ul style="list-style-type: none"> System administration tools 	なし
Web Services	なし	All packages
Databases	なし	All packages
System Management	なし	なし
Virtualization	なし	なし
Desktops (推奨) — グラ フィカル環境で特定のイン ストール後の手順を実行 するために使用されます。 詳細は「 インストール後の タスク 」を参照してくださ い。	<ul style="list-style-type: none"> Desktop Desktop Platform General Purpose Desktop Graphical Administration Tools + <i>system-config-lvm-x.x.xx-xx.e16 .noarch¹</i> Legacy X Window System compatibility X11 (X Window System, version 11) 	なし
Applications (オプション) — GUI インタフェースを 使用して STA サーバーを ローカルに構成および管 理するために使用できま す。	<ul style="list-style-type: none"> Internet Browser 	なし
Development	<ul style="list-style-type: none"> Development tools + <i>expect-x.xx.x.xx-x.e16.x86_64</i> 	なし
言語	なし	なし

¹オプション。Linux のインストールの完了後にファイルシステムを構成または再構成するために使用できます。

21. パッケージの選択が終了したら、「**Next**」をクリックします。インストールが開始されます。

すべてのパッケージを構成する前に誤って「**Next**」をクリックした場合、ソフトウェアが依存関係の検査を完了したあとで「**Back**」をクリックします。

22. 「Congratulations」画面が表示されたら、インストールメディアを取り除き、「**Reboot**」をクリックします。

インストールの完全なログは、`/root/install.log` にあります。

2.2.3. Linux Setup Agent の実行

Linux サーバーをリブートすると、Linux Setup Agent が自動的に起動します。システム環境を構成するには、次の手順を使用します。

1. 「Welcome」画面で、「**Forward**」をクリックします。
2. ライセンス契約を読み、「**Yes, I agree to the License Agreement**」を選択して、「**Forward**」をクリックします。
3. 「Software Updates」画面で、更新のためにシステムを登録する場合、「**Yes, I'd like to register now**」を選択します。それ以外の場合、「**No, I prefer to register at a later time**」を選択して、「**Forward**」をクリックします。
4. 「Finish Updates Setup」画面で、「**Forward**」をクリックします。
5. 「Create User」画面で、フィールドを空白のままにして、「**Forward**」をクリックしてから、「**Yes**」をクリックして続行します。STA サーバーでは、非管理ユーザーは不要です。
6. 「Date and Time」画面で:
 - a. 現在の日付と時間を設定します。
 - b. 「**Synchronize date and time over the network**」チェックボックスを選択します。
 - c. (IT 管理者から取得した) 希望の NTP サーバーを追加または削除して、「**Forward**」をクリックします。

注:

STA のデータおよびログファイルが正しいことを確認するには、STA サーバーの日付と時間が正しい必要があります。また、STA に接続されているすべてのライブラリも時間が正しい必要があります。

7. 「Kdump」画面では、「**Enable kdump?**」を選択しないでください。次に、「**Finish**」をクリックします。

システムがリブートします。

8. システムのリブート後、root ユーザーとしてログインします。
 - a. 「**Other...**」をクリックします。
 - b. ユーザー名 **root** を入力して、「**Log In**」をクリックします。
 - c. root パスワードを入力して、再度「**Log In**」をクリックします。

root スーパーユーザーとしてログインしているというメッセージが表示された場合、そのメッセージを無視してもかまいません。

9. Linux のリリースと更新レベルを確認します。この手順はオプションです。

```
# cat /etc/*-release
Oracle Linux Server release 6.4
Red Hat Enterprise Linux Server release 6.4 (Santiago)
Oracle Linux Server release 6.4
```

2.3. インストール後のタスク

次のタスクを実行して、確実に STA サーバーが STA インストール用に正しく構成されるようにします。

2.3.1. SELinux の無効化

Oracle では、STA サーバーで SELinux を無効にすることをお勧めします。

1. STA サーバーで端末セッションを開きます。
2. テキストエディタで SELinux 構成ファイルを開きます。

```
# vi /etc/sysconfig/selinux
```

3. そのファイルで、*SELINUX* を *disabled* に設定します。

```
SELINUX=disabled
```

4. ファイルを保存して終了します。

2.3.2. Linux ファイアウォールの無効化

Oracle では、STA サーバーでファイアウォールを無効にすることをお勧めします。ただし、サイトの要件によっては、ファイアウォールを有効にして構成することを選択してもかまいません。

ファイアウォールを無効にするには、次の手順を使用します。

1. STA サーバーで端末セッションを開きます。
2. Linux ファイアウォールの設定を確認します (次のブートのため)。

```
# chkconfig --list |grep "ip"
```


ファイアウォールが次のブート時に無効になるように設定されている場合、`iptables` と `ip6tables` の両方の出力はすべて `off` と表示されます。これ以外の場合、ファイアウォールを無効にします。

```
# chkconfig iptables off
# chkconfig ip6tables off
```

3. Linux ファイアウォールの現在のステータスを確認します。

```
# service iptables status
# service ip6tables status
```

コマンド出力は、ファイアウォールが現在実行中かどうかを示しています。ファイアウォールが実行中の場合、ファイアウォールを停止します。

```
# service iptables stop
# service ip6tables stop
```

4. 次のいずれかが当てはまる場合、サーバーをリブートする必要があります。
 - [40 ページの「SELinux の無効化」](#)で SELinux を無効にしました。
 - このセクションで (`chkconfig` を使用して) Linux ファイアウォールを無効にしました。

2.3.3. アクセス制御の無効化

特定のディレクトリのアクセス制御を無効にする必要があります。

1. Oracle ストレージホーム、STA データベース、STA データベースのローカルバックアップ、および STA ログの各場所のアクセス権を一覧表示します。例:

```
# ls -ld /Oracle /dbdata /dbbackup /var/log/tbi

drwxr-xr-x 2 oracle oinstall 4096 Jul 30 14:48 /Oracle
drwxr-xr-x 3 root    root    4096 Jul 30 14:46 /dbdata
drwxr-xr-x 3 root    root    4096 Jul 29 14:13 /dbbackup
drwxrwxrwx 4 root    root    4096 Jul 30 14:46 /var/log/tbi
```

2. 各コマンドの出力で、それらのアクセス権の最後にあるドットを探します。次の例では、`drxwr-xr-x` のあとにある「`.`」に注目してください。

```
# ls -ld /Oracle
```

```
drxwr-xr-x. 5 oracle oinstall 4096 Jul 30 18:27 /Oracle
```

3. いずれのディレクトリにも、アクセス権の記述のあとにドットが含まれていない場合、アクセス制御はすでに無効になっているため、次のタスクに進んでかまいません。

アクセス制御がディレクトリで有効になっている場合、システムの root ユーザーとして、そのディレクトリに対して次のコマンドを実行します。

```
# setfattr -h -x security.selinux directory_name
```

例:

```
# setfattr -h -x security.selinux /Oracle
```

2.3.4. ネットワークプロキシの設定

ネットワークに直接接続するか、プロキシサーバーを介して接続するように STA サーバーを構成できます。

1. Linux デスクトップの「**System**」メニューから、「**Preferences**」を選択して「**Network Proxy**」を選択します。
2. 「**Network Proxy Preferences**」ダイアログボックスで、サイトの要件に従ってプロキシ構成を指定します。
3. 「**Close**」をクリックします。

2.3.5. yum の正しい設定の確認 (オプション)

yum (Yellowdog Updater, Modified) を使用して必要な RPM (Red Hat Package Manager) Linux ソフトウェアパッケージをインストールする場合は、この手順を使用します。(必要なパッケージについては、「[必要な Linux パッケージのインストール](#)」を参照してください。)

yum をはじめ、RPM パッケージをインストールする方法はさまざまあります。yum の使用はオプションですが、これによりパッケージのインストールプロセスが非常に簡略化されるため推奨されています。yum は最新のパッケージバージョンとその依存関係を RPM パッケージリ

ポジトリで自動的に検索します。この手順では、STA サーバーで yum が正しく構成されていることを確認します。

注:

次のコマンドの例では、Oracle Linux の yum リポジトリを使用します。それらのコマンドでは、「ol6」の「l」は小文字の「L」です。

1. Oracle public-yum サーバーに対して ping を実行して、ネットワーク接続が正常であることを確認します。

```
# ping public-yum.oracle.com
```

2. yum リポジトリディレクトリに移動して、yum リポジトリファイル名を判別します。

```
# cd /etc/yum.repos.d
# ls
public-yum-ol6.repo
```

3. 既存の yum リポジトリファイルを削除します。

```
# rm public-yum-ol6.repo
```

4. 最新の yum リポジトリファイルを yum Web サイトからダウンロードします。

```
# wget http://public-yum.oracle.com/public-yum-ol6.repo
```

注:

以後このコマンドを実行すると、新しいリポジトリファイルが新しい拡張子 (たとえば、*public-yum-ol6.repo.1*) で *yum.repos.d* フォルダにコピーされます。ただし、yum は、常に拡張子なしでリポジトリファイルを使用します。

5. テキストエディタでリポジトリファイルを開きます。

```
# vi public-yum-ol6.repo
```

6. そのファイルで、Linux バージョンと一致するエントリを見つけ、*enabled=1* を設定して有効にします。*enabled=0* を設定して、その他のすべてのエントリを無効にします。

例:

```
[Linux_Version]
name=Oracle Linux $releasever Update x installation media copy ($basearch)
baseurl=http://public-yum.oracle.com/repo/OracleLinux/OL6/x/base/$basearch/
gpgkey=http://public-yum.oracle.com/RPM-GPG-KEY-oracle-ol6
gpgcheck=1
enabled=1
```

7. ファイルを保存して終了します。

2.3.6. 必要な Linux パッケージのインストール

STA のインストールと操作には、追加の RPM パッケージが必要です。STA インストーラは次のパッケージの有無を検査します。それらが存在しない場合、STA のインストールは失敗します。

注:

RPM パッケージ名では大文字と小文字が区別されます。

• <i>binutils</i>	• <i>gcc-c++</i>	• <i>libstdc++</i>
• <i>compat-libcap1</i>	• <i>glibc</i>	• <i>libstdc++-devel</i>
• <i>compat-libstdc++-33.i686</i>	• <i>glibc-devel</i>	• <i>net-snmp-utils</i>
• <i>cronie</i>	• <i>libaio</i>	• <i>rpm-build</i>
• <i>expect</i>	• <i>libaio-devel</i>	• <i>sysstat</i>
• <i>gcc</i>	• <i>libgcc</i>	• <i>xorg-x11-utils</i>

さまざまな方法を使用して、必要な RPM パッケージをインストールできます。この手順では、yum の使用方法について説明します。

yum パッケージインストールコマンドは、使用している Linux バージョンの最新バージョンのパッケージを確認して、そのパッケージとすべての依存関係をインストールします。Linux のインストールによっては、これらのパッケージの一部はすでにインストールされている可能性があります。パッケージがすでにインストールされていて、最新バージョンになっている場合は、システムによって通知されます。

1. STA サーバーで端末セッションを開きます。
2. 次のように進めます。
 - Oracle の public yum サーバー ([「yum の正しい設定の確認 \(オプション\)」](#)を参照) にアクセスできる場合は、次のいずれかの方法を使用してパッケージをインストールします。

- 。パッケージを一度に1つずつインストールします。指定されたパッケージがダウンロードおよび確認され、ユーザーはすべてのプロンプトに応答する必要があります。

```
# yum install package_name
```

- 。プロンプトなしで、一度にすべてのパッケージをインストールします。`-y` オプションは、すべてのインストールプロンプトに自動的に「yes」と応答します。

```
# yum -y install binutils compat-libcap1 compat-libstdc++-33.i686 cronie  
expect gcc gcc-c++ glibc glibc-devel libaio libaio-devel libgcc libstdc++  
libstdc++-devel net-snmp-utils rpm-build sysstat xorg-x11-utils
```

- 。ネットワークファイアウォールで外部ネットワークアクセスが禁止されている場合は、`yum` を使用して、ローカルで使用可能なパッケージを Linux メディアからインストールできます。例:

```
# cd /mnt/install_media_mount_location/packages  
# yum install ./package_name
```

2.3.7. SSH の正しい設定の確認

STA サーバーで SSH (Secure Shell) が正しく設定されていることを確認するには、次の手順を使用します。これによって、リモートホストへの STA データベースバックアップの転送が高速化されます。

1. テキストエディタで SSH 構成ファイルを開きます。

```
# vi /etc/ssh/sshd_config
```

2. `AddressFamily` エントリと `UseDNS` エントリを検索します。前にコメント文字が付かず、その値が次のようになるように変更します。

```
AddressFamily inet  
UseDNS no
```

3. ファイルを保存して終了します。
4. `sshd` デーモンを再起動します。

```
# service sshd restart
```

2.3.8. 正しい DNS 設定の確認

STA サーバーの IP アドレスがホスト名にマップされていることを確認するには、次の手順を使用します。

1. テキストエディタでホストファイルを開きます。

```
# vi /etc/hosts
```

2. ファイルの最後に、STA サーバーの IP アドレス、そのあとにタブ、次に STA サーバーのホスト名を追加します。例:

```
127.0.0.1    localhost localhost.localdomain localhost4...
::1         localhost localhost.localdomain localhost6...
192.0.2.20  sta_server
```

3. ファイルを保存して終了します。新しい設定を有効にするために STA サーバーを再起動する必要はありません。

2.3.9. ネームサービスの無効化

LDAP などのネームサービスは、STA のインストールと競合する可能性があります。これらのサービスを一時的に無効にするには、次の手順を使用します。

1. テキストエディタでネームサービススイッチ構成ファイルを開きます。

```
# vi /etc/nsswitch.conf
```

2. ネームサービスのエントリを無効にします。たとえば、LDAP を無効にするには、次に示すように次の行から「ldap」をコメントアウトします。

```
passwd:    files #ldap nis nisplus
shadow:    files #ldap nis nisplus
group:     files #ldap nis nisplus
```

3. ファイルを保存して終了します。新しい設定を有効にするために STA サーバーを再起動する必要はありません。STA のインストール後に、nsswitch.conf ファイルを変更して、ネームサービスを再度有効にできます。

2.3.10. ローカルブラウザ機能の確認 (オプション)

STA サーバーで STA をローカルで構成および管理するには、サポートされる最小のブラウザバージョンとプラグインがインストールされていることを確認します (『STA 要件ガイド』を参照)。

注:

Oracle では、STA アプリケーションへのローカルアクセスはサーバーパフォーマンスが低下するため、お勧めしません。

STA のインストール

この章では、このサーバーへの STA の新しいインストールを実行することを想定していません。

- 以前のバージョンから STA をアップグレードするには、[8章「STA 2.1.0 へのアップグレード」](#)を参照してください。Oracle では最新バージョンの STA をインストールするかアップグレードすることをお勧めします。
- STA を再インストールするか、現在のインストールを修復する場合には、[9章「STA のアンインストールと復元」](#)を参照してください。

注:

Oracle は、STA が専用のサーバー (このガイドでは STA サーバーと呼びます) にインストールされている場合のみ、サポートを提供します。

この章には次の内容が含まれます。

- [STA インストーラで使用するユーザー、グループ、場所](#)
- [STA のインストール中に構成されるアカウントおよびポート](#)
- [STA のインストールおよびアンインストールのログ](#)
- [STA インストーラのモード](#)
- [STA のインストールタスク](#)

[付録C「インストールおよびアップグレードのワークシート」](#)に、インストールアクティビティの整理および設定の記録に使用できるワークシートがあります。

3.1. STA インストーラで使用するユーザー、グループ、場所

このセクションでは、STA のインストールプロセス使用される主な概念と用語について説明します。

Oracle インストールグループ

STA サーバーに Oracle 製品をインストールおよびアップグレードする際に使用する Linux グループ。Oracle では、この目的専用独立したグループを作成することをお勧めします。

STA のインストールを実行するには、このグループのメンバーであるユーザーとしてログインする必要があります。Linux の *root* ユーザーやほかのスーパーユーザー権限を持つユーザーとして STA をインストールすることはできません。

このガイドの説明および例では、このグループに対して *oinstall* という名前を使用します。選択した名前が異なる場合には、その名前を当てはめてください。

Oracle インストールユーザー

STA サーバーに Oracle 製品をインストールおよびアップグレードする Linux ユーザー。これは Oracle インストールグループのメンバーである任意のユーザーとすることができます。

このガイドの説明および例では、このユーザーに対して *oracle* という名前を使用します。選択した名前が異なる場合には、その名前を当てはめてください。

Oracle 中央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の追跡に使用されるディレクトリ。STA のインストーラおよびアンインストーラのログが、この場所内の *logs* サブディレクトリに保持されます。

Oracle インストールユーザーは、このディレクトリを所有し、これに対するフルアクセス権を持つ必要があります。Oracle インストールグループのほかのユーザーが Oracle 製品をインストールできる適切なアクセス権を持つようにするには、Oracle インストールユーザーのホームディレクトリを使用しないでください。

この場所は、このセクションで説明するほかのディレクトリとは独立している必要があります。このガイドの説明および例では、この場所に */opt/oracle/oraInventory* を使用します。選択したディレクトリが異なる場合には、そのディレクトリを当てはめてください。

注:

Oracle では、すべての Oracle インストーラがこのサーバー上の同じ中央インベントリの場所を使用するように、STA のインストールが完了してからこの場所を登録することをお勧めします。詳細は、「[Oracle 中央インベントリの場所の登録](#)」を参照してください。

Oracle ストレージホームの場所

STA および関連する Oracle ソフトウェアがインストールされるディレクトリ。STA はこの場所内の *StorageTek_Tape_Analytics* サブディレクトリに自動的にインストールされます。[STA ホーム](#)を参照してください。

このディレクトリがすでに存在する場合、Oracle インストールユーザーは、これに対するフルアクセス権を持つ必要があります。このディレクトリが存在しない場合で、Oracle インストールユーザーが親ディレクトリにフルアクセス権を持っている場合には、STA インストーラがディレクトリを自動的に作成します。

注:

このサーバーに以前のバージョンの STA がインストールされていた場合には、このディレクトリはすでに存在している場合があります。その場合、*root* ではなく、Oracle インストールグループに所有されていることを確認する必要があります。

この場所は、このセクションで説明するほかのディレクトリとは独立している必要があります。このガイドの説明および例では、この場所に */Oracle* を使用します。選択したディレクトリが異なる場合には、そのディレクトリを当てはめてください。

STA ホーム

すべての STA ソフトウェアがインストールされるディレクトリ。このディレクトリには *StorageTek_Tape_Analytics* という名前が割り当てられ、STA インストーラがこれを [Oracle ストレージホームの場所](#)内に自動的に作成します。

このガイドの説明および例では、この場所に */Oracle/StorageTek_Tape_Analytics* を使用します。

STA インストーラの場所

STA インストーラをダウンロードするディレクトリ。

この場所は、このセクションで説明するほかのディレクトリとは独立している必要があります。このガイドの説明および例では、この場所に */Installers* を使用します。選択したディレクトリが異なる場合には、そのディレクトリを当てはめてください。

STA インストーラの作業場所

デフォルトでは、STA インストーラは */tmp* ディレクトリに展開され、約 4G バイトの領域を使用します。STA インストーラを *-J-Djava.io.tmpdir=working_directory* オプションとともに実行すると、別の作業場所を指定できます。

working_directory は絶対パスである必要があります。例:

```
$ ./sta_installer_linux64.bin -J-Djava.io.tmpdir=/Oracle/tmp
```

このオプションの使用については、[付録B「STA サイレントモードインストーラおよびアンインストーラ」](#)を参照してください。

STA ログの場所

STA および MySQL のログの場所。その内容は大きくなりすいため、ログローテーションを通じて管理されます。デフォルトの場所は */var/log/tbi* ですが、この場所は STA のインストール後にいつでも変更できます。手順については、[「STA のログディレクトリの再配置 \(オプション\)」](#)を参照してください。

領域の要件については、[「STA ファイルシステムレイアウトの確認」](#)を参照してください。

3.2. ユーザー名およびパスワードの要件

ユーザー名の要件は次のとおりです。

- 1 – 16 文字の長さにする必要があります
- すべてのユーザー名が一意である必要があります

パスワード要件は次のとおりです。

- 8 – 31 文字の長さにする必要があります
- 少なくとも 1 つの数字と 1 つの大文字を含める必要があります
- 空白を含めることはできません
- 次の特殊文字を含めることはできません

& ' () < > ? { } * / ' "

3.3. STA のインストール中に構成されるアカウントおよびポート

STA インストーラは、指定した仕様に従ってユーザーアカウントおよびポート番号を構成します。

3.3.1. STA を管理するためのユーザーアカウント

次の必須アカウントは、STA のインストール中に作成されます。これらのアカウントは STA 固有のもので、Linux のユーザー名ではありません。

- [WebLogic アカウント](#)
- [STA データベースアカウント](#)

3.3.1.1. WebLogic アカウント

次の WebLogic アカウントは、WebLogic 管理コンソールまたは STA アプリケーションへのログインに使用されます。

WebLogic の管理

WebLogic 管理コンソールにログインして、WebLogic を LDAP または RACF サーバーに接続するなどの、WebLogic 環境への変更を行う場合に使用します。

注意:

このアカウントのユーザー名およびパスワードは取得することができません。これらの資格証明を失った場合、STA を再インストールする必要があります。

STA 管理者

フルアクセス権限で STA アプリケーションにログインする際に使用します。

STA のインストールの完了後、STA アプリケーションを使用して追加の割り当て可能な役割のユーザーアカウントを作成できます。詳細は、『STA ユーザーズガイド』を参照してください。

3.3.1.2. STA データベースアカウント

次の STA データベースアカウントは、STA が STA データベースのアクセスおよび管理に使用する MySQL アカウントです。

STA データベースルートユーザー

MySQL データベースを所有し、ルートデータベースインストールを作成するために使用されます。事前定義されたユーザー名は *root* で、これを変更することはできません。

注意:

このアカウントのパスワードは取得することができません。

STA データベースアプリケーションユーザー

STA がデータベースに接続するために使用するユーザー定義の MySQL ユーザー名 (たとえば、*stadb*)。データ表で特権を作成、更新、削除、および読み取るために必要です。

STA データベースレポートユーザー

STA 以外のアプリケーションおよびサードパーティーのアプリケーションがデータベースへの接続に使用できるユーザー定義の MySQL ユーザー名 (たとえば、*starpt*)。これには、特定のデータベース表に対する読み取り専用アクセス権があります。

STA データベース管理ユーザー

STA 管理者とモニタリングユーティリティが、データベースに接続して、主にスケジュールされたバックアップを構成および実行するために使用するユーザー定義の MySQL ユーザー名 (たとえば、*stadb*)。「付与オプション」を除く、すべてのデータベース表に対するすべての DBA 権限を持ちます。

3.3.2. STA が使用するポート

STA は、次のポートを使用して、データを取得および受信します。これらは専用ポートで、STA が使用できる状態である必要があります。STA インストーラは、ポートがネットワークでまだ使用されていないことを確認します。

注意:

STA のインストール中にこれらのポートが構成されると、STA をアンインストールして再インストールしないかぎり変更することはできません。

3.3.2.1. 構成不可の外部ポート

表3.1「構成不可の外部ポート」で説明されているポートは、STA サーバーとほかのネットワークエンティティー間の通信に使用される外部ポートです。ポートの値は固定され、STA のインストール中に変更することはできません。

ファイアウォール/ルーター構成: STA サーバーとバックアップサーバー (SSH の場合) 間、および STA サーバーとモニター対象ライブラリ (SNMP および SNMPTRAP の場合) の間で到達可能である必要があります。

表3.1 構成不可の外部ポート

ポート	プロトコル	説明および目的
22	SSH	セキュアシェル。STA データベースバックアップ。ライブラリログイン。
161	SNMP	Simple Network Management Protocol (SNMP)。SNMP 要求の送信用。
162	SNMPTRAP	SNMP 通知 (トラップ) の受信用。

3.3.2.2. 構成可能な外部ポート

表3.2「構成可能な外部ポート」で説明されているポートは、STA サーバーとほかのネットワークエンティティー間の通信に使用される外部ポートです。これらのポートは、標準ポート 80 と 8080 (HTTP) および 443 (HTTPS) と同等の構成可能ポートであり、ネットワーク上のその他の HTTP および HTTPS ポートとは異なる必要があります。値を選択するには、ネットワーク管理者に相談してください。

ファイアウォール/ルーター構成: STA サーバーと、STA GUI が実行されているクライアントの間で到達可能である必要があります。

表3.2 構成可能な外部ポート

デフォルトポート	プロトコル	説明および目的
7019	HTTP	WebLogic 管理コンソールへのアクセス。セキュリティー保護されていません
7020	HTTPS	WebLogic 管理コンソールへのアクセス。セキュリティー保護されています

デフォルトポート	プロトコル	説明および目的
7021	HTTP	staUi 管理対象サーバー。STA GUI へのアクセス。セキュリティ保護されていません。
7022	HTTPS	staUi 管理対象サーバー。STA GUI へのアクセス。セキュリティ保護されています。

3.3.2.3. 構成可能な内部ポート

表3.3「構成可能な内部ポート」で説明されているポートは、内部の STA 通信に使用されます。これらのポート値は一意である必要があります。

ファイアウォール/ルーター構成: 該当なし

表3.3 構成可能な内部ポート

デフォルトポート	プロトコル	説明および目的
7023	HTTP	staEngine 管理対象サーバー。基本的な STA 内部。セキュリティ保護されていません。
7024	HTTPS	staEngine 管理対象サーバー。基本的な STA 内部。セキュリティ保護されています。
7025	HTTP	staAdapter 管理対象サーバー。SNMP 通信。セキュリティ保護されていません。
7026	HTTPS	staAdapter 管理対象サーバー。SNMP 通信。セキュリティ保護されています。

3.4. STA のインストールおよびアンインストールのログ

STA のインストールおよびアンインストールのログを使用して、問題のトラブルシューティングに役立てることができます。ログファイル名の多くは、インストールまたはアンインストールのインスタンスを特定できるよう、タイムスタンプが含まれています。タイムスタンプとは、インストールまたはアンインストールが開始した日付と時間のことです。

特に次のログでは、インストールまたはアンインストールが失敗した場合に、価値のある情報が提供されます。これらの場所については、[/STA_logs/install](#)を参照してください。

- `installtimestamp.log`
- `sta_installtimestamp.log`
- `deinstalltimestamp.log`
- `sta_deinstalltimestamp.log`

3.4.1. ログファイルの場所

STA のインストールおよびアンインストールのログの場所は、インストールまたはアンインストールのステータスにより異なります。ログは、次のディレクトリにあります。これらのディレクトリの詳細は、「[STA ファイルシステムレイアウトの確認](#)」を参照してください。

`/tmp/OraInstalltimestamp`

このディレクトリには、進行中のインストールまたはアンインストールのログが含まれます。このディレクトリに表示される可能性のあるログのサンプルのリストは次のとおりです。

```
install2014-09-24_04-14-04PM.log
installProfile2014-09-24_04-14-04PM.log
launcher2014-09-24_04-14-04PM.log
```

`/Oracle_storage_home/oraInventory/logs`

ここで `Oracle_storage_home` は、STA のインストール中に定義された Oracle ストレージホームの場所です。

このディレクトリには、正常に完了したインストールおよびアンインストールのログが含まれます。エラーまたはパッチのログなど、一部のログは該当する場合のみ含まれます。

このディレクトリに表示される可能性のあるログのサンプルのリストは次のとおりです。

```
2014-09-24_02-57-41PM.log
install2014-09-24_02-57-41PM.log
install2014-09-24_02-57-41PM.out
installActions2014-09-24_02-57-41PM.log
installProfile2014-09-24_02-57-41PM.log
installSummary2014-09-24_02-57-41PM.txt
launcher2014-09-24_02-57-41PM.log1
OPatch2014-09-24_02-58-47-PM.log
oraInstall2014-09-24_02-57-41PM.err
oraInstall2014-09-24_02-57-41PM.out
```

`/STA_logs/install`

デフォルトで、`STA_logs` は `/var/log/tbi` に配置されています。オプションで、このディレクトリを、STA のインストール後はいつでも、任意の場所に再配置できます。手順については、「[STA のログディレクトリの再配置 \(オプション\)](#)」を参照してください。

このディレクトリには、正常に完了した、または失敗したインストールおよびアンインストールのログが含まれます。これには、WebLogic サーバーおよび MySQL データベースのインストールに関連するログのほか、STA アプリケーションのインストールおよび構成についてのログも含まれます。

このディレクトリに表示される可能性のあるログのサンプルのリストは次のとおりです。

```
dbinstall.log
dbinstall.mysqlld.err
dbinstall.stadb-slow.log
install2014-09-24_02-52-09PM.log
install_weblogic.log
sta_install2014-09-24_02-53-22PM.log
```

3.5. STA インストーラのモード

次のいずれかのモードを使用して STA をインストールできます。

グラフィカルモード

これは推奨のインストールモードです。このモードでは、STA のインストール用のグラフィカルユーザーインターフェースが用意されており、X11 ディスプレイが必要になります。詳細は、[付録A「STA グラフィカルインストーラおよびアンインストーラの画面リファレンス」](#)を参照してください。

サイレントモード

このモードでは、グラフィカルユーザーインターフェースを省略し、インストールオプションを応答ファイルと呼ばれる XML プロパティファイルで指定します。詳細は、[付録B「STA サイレントモードインストーラおよびアンインストーラ」](#)を参照してください。

このモードは、無人インストールや複数のマシンに STA をインストールする際に役立ちます。応答ファイルを使用することで、1 組のパラメータを指定して、インストールを自動化できます。サイレントモードのインストーラは、スクリプトから実行することも、Linux コマンド行から実行することもできます。

3.6. STA のインストールタスク

STA をインストールするには、次のすべてのタスクを示された順に実行します。

- [「インストールに必要な情報の特定および作成」](#)
- [「インストールの前提条件の確認」](#)
- [「STA のダウンロード」](#)
- [「STA のインストール」](#)
- [「正常なインストールの確認」](#)

- 「[STA のログディレクトリの再配置 \(オプション\)](#)」
- 「[Oracle 中央インベントリの場所の登録](#)」

3.6.1. インストールに必要な情報の特定および作成

この手順を使用して、STA インストーラを実行するユーザーおよび場所を特定し、必要に応じてそれらを作成します。この情報を記録するには、[表C.2「インストールユーザーおよび場所のワークシート」](#)を使用できます。これらの項目の詳細については、「[STA インストーラで使用するユーザー、グループ、場所](#)」を参照してください。

1. Linux の root ユーザーとしてログインします。
2. STA サーバーに Oracle 中央インベントリのポインタファイル `/etc/oraInst.loc` があるかどうかを判断します。Oracle 中央インベントリが以前に登録されている場合には、ファイルは存在します。詳細は、[Oracle 中央インベントリの場所](#)を参照してください。

- ファイルが存在する場合には、その内容を記録します。例:

```
# cat /etc/oraInst.loc
inventory_loc=/opt/oracle/oraInventory
inst_group=oinstall
```

`inventory_loc` エントリは Oracle 中央インベントリの場所を特定し、`inst_group` エントリは Oracle インストールグループを特定します。

- ファイルが存在しない場合、手順 3 に進み、必要なユーザーと場所を作成します。例:

```
# cat /etc/oraInst.loc
cat: /etc/oraInst.loc: No such file or directory
```

3. 手順 2 で Oracle 中央インベントリのポインタファイルがなかった場合は、Oracle インストールグループを作成します。詳細は、[Oracle インストールグループ](#)を参照してください。例:

```
# groupadd oinstall
```

4. Oracle インストールユーザーのユーザー名およびパスワードを取得するか、必要に応じて新しく作成します。このユーザーは、Oracle インストールグループに属している必要があります。詳細は、[Oracle インストールユーザー](#)を参照してください。例:

```
# useradd -g oinstall -d /home/oracle oracle
```

```
# passwd oracle
Changing password for user oracle.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

- 手順 2 で Oracle 中央インベントリのポインタファイルがなかった場合は、Oracle 中央インベントリの場所を作成します。このディレクトリは、Oracle インストールユーザーが所有している必要があります。詳細は、[Oracle 中央インベントリの場所](#)を参照してください。例:

```
# mkdir /opt/oracle/oraInventory
# chown oracle /opt/oracle/oraInventory
# ls -la /opt/oracle/oraInventory
total 8
drwxr-xr-x 2 oracle oinstall 4096 Feb 11 10:49 .
drwxr-xr-x 3 root   root      4096 Feb 11 10:49 ..
```

- Oracle ストレージホームの場所を特定するか、存在しない場合にはディレクトリを作成します。このディレクトリは、Oracle インストールユーザーが所有している必要があります。詳細は、[Oracle ストレージホームの場所](#)を参照してください。例:

```
# mkdir /Oracle
# chown oracle /Oracle
# ls -la /Oracle
total 8
drwxr-xr-x 2 oracle oinstall 4096 Feb 11 10:49 .
drwxr-xr-x 3 root   root      4096 Feb 11 10:49 ..
```

- STA インストーラの場所を特定するか、存在しない場合にはディレクトリを作成します。詳細は、[STA インストーラの場所](#)を参照してください。例:

```
# mkdir /Installers
```

- Linux の root ユーザーのパスワードを指定します。STA インストーラでは、特定のタスクの実行にルートアクセスが必要で、パスワードが要求されます。

9. インストール中に作成される WebLogic 管理者、STA 管理者、および MySQL アカウントのユーザー名を選択します。詳細は、「[STA を管理するためのユーザーアカウント](#)」を参照してください。
10. STA の動作に必要な、構成可能な内部ポートおよび外部ポートのポート番号を選択します。外部ポートが必要なネットワーク上で開いていることを確認します。詳細は、「[STA が使用するポート](#)」を参照してください。
11. Oracle の Remote Diagnostics Agent (RDA) を構成するための、サイトのドメイン名を取得します。詳細は、『[STA ユーザーズガイド](#)』を参照してください。

3.6.2. インストールの前提条件の確認

STA インストーラを実行する前に、この手順を使用して前提条件を確認します。この手順はオプションですが、これらの前提条件のいずれも一致しない場合、STA のインストールは失敗します。インストールの前提条件の完全なリストについては、『[STA 要件ガイド](#)』を参照してください。

これらすべての手順は、STA サーバーで実行されます。支援が必要な場合には、Linux 管理者に相談してください。

注:

STA のインストールでは、64 ビット Linux が [2章「Linux のインストール」](#) で指定された Linux RPM パッケージとともにインストールされていることを想定しています。必要なパッケージがインストールされていない場合、STA のインストールは失敗します。詳細は、次のドキュメントを参照してください。

- サポートされている Linux のバージョンについては、『[STA 要件ガイド](#)』。
- 必要なパッケージのリストは、[44 ページの「必要な Linux パッケージのインストール」](#)

注意:

既存のソフトウェアを永久に削除または置換することを選択する前に、必要に応じてファイルをバックアップしてください。

1. STA がサーバーにインストールされていないことを確認します。STA インストーラは、新しいインストール用にのみ使用します。ほかの説明については、該当する場合、次のセクションを参照してください。
 - STA を以前のバージョンからアップグレードする場合には、[8章「STA 2.1.0 へのアップグレード」](#)を参照してください。
 - STA を再インストールするか、現在のインストールを修復する場合には、[9章「STA のアンインストールと復元」](#)を参照してください。

次の例は、STA がインストールされていない場合を示しています。

```
$ ls /etc/init.d/sta*
ls: cannot access /etc/init.d/sta*: No such file or directory$ ls /usr/bin/STA
ls: cannot access /usr/bin/STA: No such file or directory
$
```

- MySQL が STA サーバーにインストールされていないことを確認します。MySQL がインストールされている場合、インストーラはそれを削除して再インストールし、既存の MySQL データベースはすべて削除されます。
- `/tmp` ディレクトリに少なくとも 4G バイトの空き領域があることを確認します。これがデフォルトの STA インストーラの作業場所になります。

```
$ df /tmp
Filesystem          1K-blocks      Used Available Use% Mounted on
/dev/mapper/vg_sta_server-lv_root
                    51606140  42896756   6087944   88% /
```

注:

STA インストーラの起動時に、オプションで別の作業ディレクトリを指定できます。詳細は、[STA インストーラの作業場所](#)を参照してください。

- SELinux が無効になっていることを確認します。「[インストール後のタスク](#)」の指示に従った場合、SELinux はすでに無効にされているはずですが、詳細は、[40 ページの「SELinux の無効化」](#)を参照してください。

```
$ sestatus
SELinux status:      disabled
```

- Linux ファイアウォール (IPTables) が停止されていることを確認します。「[インストール後のタスク](#)」の指示に従った場合、IPTables はすでに停止されているはずですが、詳細は、[40 ページの「Linux ファイアウォールの無効化」](#)を参照してください。

```
$ service iptables status
iptables: Firewall is not running.
```

注:

サイトで IPTables サービスが実行していることが必要な場合、STA をインストールし、ライブラリを構成し、STA がライブラリをモニターしていることを確認してから、サービスを開始できます。IPTables の開始後、STA がライブラリをモニターしていることを再確認する必要があります。

6. SNMP サービスを停止し、構成解除します。

ネットワークポートの衝突とその他の問題を回避するために、STA サーバーではその他の SNMP サービスを実行してはいけません。STA インストーラは、次のいずれかの状況で終了します。

- `snmpd` および `snmptrapd` デーモンサービスが実行している。
- UDP ポート 161 (SNMP) および 162 (SNMPTRAP) を利用できない。

必要に応じて次の手順を実行します。

- a. SNMP の `snmpd` サービスおよび `snmptrapd` サービスの現在のステータスを表示します。

```
# service snmpd status
snmpd is stopped
# service snmptrapd status
snmptrapd is stopped
```

- b. 必要に応じて SNMP サービスをただちに停止します。

```
# service snmpd stop
# service snmptrapd stop
```

注:

これらのコマンドのいずれかで「FAILED」エラーが表示された場合、サービスはすでに停止している可能性があります。

- c. Linux サービス構成ファイルに次のように入力して、Linux のリブート時に自動的に起動しないように、SNMP サービスを無効にします。

```
# chkconfig snmpd off
# chkconfig --list snmpd
snmpd          0:off  1:off  2:off  3:off  4:off  5:off  6:off
# chkconfig snmptrapd off
# chkconfig --list snmptrapd
snmptrapd     0:off  1:off  2:off  3:off  4:off  5:off  6:off
```

7. 該当するモード固有の要件を次のように再確認します。

- STA のグラフィカルインストーラについては、「[グラフィカルモードの表示要件](#)」を参照してください。
- STA のサイレントモードインストーラについては、「[サイレントモードの要件](#)」を参照してください。

3.6.3. STA のダウンロード

STA インストーラのダウンロードには、次のファイルが含まれています。*version* は STA のインストールのバージョン番号です。

- *sta_install_version_linux64.bin*— すべてのインストールに必要です。
 - *sta_install_version_linux64-2.zip*— すべてのインストールに必要です。
 - *silentInstallUtility_version.jar*— 応答ファイル構築ユーティリティ。STA のサイレントモードインストーラまたはアンインストーラを使用する場合のみ必要です。詳細は、[付録B「STA サイレントモードインストーラおよびアンインストーラ](#)」を参照してください。
1. ブラウザウィンドウで、次の URL にある Oracle Software Delivery Cloud Web サイトにアクセスします。

<http://edelivery.oracle.com/>
 2. 「サインイン/登録」をクリックします。
 3. Oracle サポートから提供されたユーザー ID とパスワードを入力するか、新しいアカウントを作成します。
 4. 「Terms & Restrictions」画面で、ライセンス契約と輸出規制への同意を示すチェックボックスを選択し、「**Continue**」をクリックします。
 5. 「Media Pack Search」画面で次の段階を実行します。
 - a. 「**Select a Product Pack**」メニューで、「Oracle StorageTek Products」を選択します。
 - b. 「**Platform**」メニューで、「Linux x86-64」を選択します。
 - c. 「実行」をクリックします。
 6. 「Results」表で「**Oracle StorageTek Tape Analytics 2.1.0**」を選択し、「**Continue**」をクリックします。
 7. 各メディアパック zip ファイルごとに「**Download**」をクリックして、少なくとも 4G バイトの空き領域がある場所にそれらのファイルを保存します。
 8. 解凍ツールを使用して、zip ファイルの内容を「[インストールに必要な情報の特定および作成](#)」で選択した STA インストーラの場所に抽出します (たとえば、*/Installers*)。

- Oracle インストールユーザーに `sta_install_version_linux64.bin` ファイルの実行権と、`sta_install_version_linux64-2.zip` ファイルの読み取りアクセス権があることを確認します。例:

```
# cd /Installers
# ls -la
-rw-r--r-- 1 oracle oinstall      5964 Oct 23 16:14 silentInstallUtility.jar
-rw-r--r-- 1 oracle oinstall 1275158996 Oct 23 13:35 sta_install_2.1.0.64.124_linux64-2.zip
-rw-r--r-- 1 oracle oinstall 1599220560 Oct 23 13:01 sta_install_2.1.0.64.124_linux64.bin

# chmod u+x sta_install*.bin
# chmod u+r sta_install*.zip
# ls -la
-rw-r--r-- 1 oracle oinstall      5964 Oct 23 16:14 silentInstallUtility.jar
-rw-r--r-- 1 oracle oinstall 1275158996 Oct 23 13:35 sta_install_2.1.0.64.124_linux64-2.zip
-rwxr--r-- 1 oracle oinstall 1599220560 Oct 23 13:01 sta_install_2.1.0.64.124_linux64.bin
```

- インストーラのダウンロードパッケージに含まれる『*STA* リリースノート』を確認します。

3.6.4. STA のインストール

STA インストーラを実行するには、この手順を使用します。グラフィカルモードまたはサイレントモードを使用して STA をインストールできます。詳細は、「[STA インストーラのモード](#)」を参照してください。

- 端末ウィンドウで STA サーバーに接続し、Oracle インストールユーザーとしてログインします。詳細は、[Oracle インストールユーザー](#)を参照してください。
- STA インストーラの場所に変更します。詳細は、[STA インストーラの場所](#)を参照してください。例:

```
$ cd /Installers
```

- 次のいずれかのコマンドを使用して、STA インストーラを起動します。
 - STA グラフィカルインストーラを使用する場合

```
$ ./sta_install_version_linux64.bin
```

ここで *version* は、ダウンロードした STA インストーラのバージョンです。例:


```
$ ./sta_install_2.1.0.64.124_linux64.bin
```

このモードには X11 ディスプレイが必要です。手順については、[付録A「STA グラフィカルインストーラおよびアンインストーラの画面リファレンス」](#)を参照してください。

- STA サイレントインストーラを使用する場合

```
$ ../sta_install_version_linux64.bin -silent -responseFile response_file
```

ここでは:

- *version* は、ダウンロードした STA インストーラのバージョンです。
- *response_file* は、以前に作成した応答ファイルの絶対パスです。

例:

```
$ ./sta_install_2.1.0.64.124_linux64.bin -silent -responseFile /Installers/  
SilentInstall.rsp
```

このモードを使用する前に、*silentInstallUtility.jar* ファイルをダウンロードし、インストールオプションを指定する応答ファイルを作成する必要があります。手順については、[付録B「STA サイレントモードインストーラおよびアンインストーラ」](#)を参照してください。

3.6.5. 正常なインストールの確認

STA が実行していることを確認するには、この手順を使用します。

1. 次の手順を使用して、STA bin ディレクトリが、システムの root ユーザーの *PATH* 変数に含まれていることを確認します。
 - a. 現在の STA サーバーで端末セッションを開き、システムの root ユーザーとしてログインします。
 - b. テキストエディタを使用してユーザープロファイルを開きます。例:

```
# vi /root/.bash_profile
```

- c. STA bin ディレクトリを *PATH* 定義に追加します。たとえば、次の行をファイルに追加します。

```
PATH=$PATH:Oracle_storage_home/StorageTek_Tape_Analytics/common/bin
```

ここで `Oracle_storage_home` は、STA のインストール中に指定された Oracle ストレージホームの場所です。

- d. ファイルを保存して終了します。
- e. ログアウトしてから、再度システムの root ユーザーとしてログインします。
- f. `PATH` 変数が正しく更新されていることを確認します。

```
# echo $PATH
/usr/lib64/qt-3.3/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin:/Oracle/StorageTek_Tape_Analytics/common/bin
```

2. STA コマンドを使用して、すべての STA サービスが実行中でアクティブであることを確認します。[例3.1「STA の正常なステータス表示」](#) は正常なステータスの表示例です。詳細は、『[STA 管理ガイド](#)』を参照してください。

例3.1 STA の正常なステータス表示

```
$ STA status all
mysql is running
staservd service is running
weblogic service is runningstaengine 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
stai service is running
.... and the deployed application for stai is in an ACTIVE state
```

3. 次のように進めます。
 - STA サービスが実行中でアクティブの場合、ライブラリおよび STA の構成を開始できます。手順については、[5章「ライブラリでの SNMP の構成」](#)および[6章「STA でのライブラリ接続の構成」](#)を参照してください。
 - STA サービスに問題がある場合、インストールおよび STA のログで詳細を確認できます。これらの場所については、[「STA のインストールおよびアンインストールのログ」](#)を参照してください。

3.6.6. STA のログディレクトリの再配置 (オプション)

この手順は、STA および MySQL のログをデフォルトの `/var/log/tbi` とは異なる場所に再配置する場合にのみ実行します。この手順の完了後、新しいログは指定した場所へ書き込まれます。この手順は、STA のインストール後いつでも実行できます。場所の要件については、「[STA ファイルシステムレイアウトの確認](#)」を参照してください。

1. システムの root ユーザーとしてログインします。
2. すべての STA サービスを停止します。

```
# STA stop all
Stopping the stau service.....
Successfully stopped the stau 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
#
```

3. STA および MySQL のログに使用する新しい STA ログディレクトリを作成します。例:

```
# mkdir -p /LOGS_DIR/log/
# ls -ld /LOGS_DIR/log
drwxr-xr-x 2 root root 4096 Jan 20 14:17 /LOGS_DIR/log
```

4. ディレクトリへのアクセス権を STA および MySQL が書き込めるように変更します。例:

```
# chmod 777 /LOGS_DIR/log
# ls -ld /LOGS_DIR/log
drwxrwxrwx 2 root root 4096 Jan 20 14:17 /LOGS_DIR/log
```

5. 現在の `/var/log/tbi` ディレクトリを今作成した STA ログディレクトリに移動します。

```
# mv /var/log/tbi /LOGS_DIR/log/
# ls -l /LOGS_DIR/log/tbi
total 20
drwxrwxrwx 2 mysql mysql 4096 Jan  7 10:45 backups
drwxrwxrwx 3 mysql mysql 4096 Jan  7 10:45 db
drwxrwxrwx 2 mysql mysql 4096 Jan  7 11:30 install
-rwxrwxrwx 1 root  root  1191 Jan 20 13:04 monitor_staserver.log
drwxrwxrwx 2 root  root  4096 Jan  7 11:03 uidumps
```

6. 新しい STA ログディレクトリからデフォルトの場所へのシンボリックリンクを作成します。
例:

```
# ln -s /LOGS_DIR/log/tbi /var/log/tbi
# ls -l /var/log/tbi
lrwxrwxrwx 1 root  root           15 Jan 20 14:22 /var/log/tbi -> /LOGS_DIR/log/
tbi
#
```

7. STA を再起動します。

```
# 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 stau Service.....
stau service was successfully started
#
```

3.6.7. Oracle 中央インベントリの場所の登録

STA のインストール完了後にこの手順を使用して、Oracle 中央インベントリの場所を STA サーバーに登録します。この手順は、このサーバーで一度だけ使用する必要があります。

この手順では、Oracle 中央インベントリのポインタファイル `/etc/oraInst.loc` を作成し、Oracle 中央インベントリの場所および Oracle インストールグループを、サーバーで使用されているすべての Oracle インストーラがわかるようにします。

1. Linux の `root` ユーザーとしてログインします。
2. Oracle 中央インベントリのディレクトリに変更します。例:

```
# cd /opt/oracle/oraInventory
```

3. そのディレクトリ内にある登録スクリプトを実行します。

```
# ./createCentralInventory.sh
Setting the inventory to /opt/oracle/oraInventory
Setting the group name to oinstall
Creating the Oracle inventory pointer file (/etc/oraInst.loc)
Changing permissions of /opt/oracle/oraInventory to 770.
Changing groupname of /opt/oracle/oraInventory to oinstall.
The execution of the script is complete
#
```

これで、Oracle 中央インベントリの場所および Oracle インストールグループが Oracle 中央インベントリのポインタファイル `/etc/oraInst.loc` で特定されました。

STA のライブラリ機能の構成

ライブラリで高品質の SNMP データを STA に送信するためには、選択された機能を適切に構成する必要があります。これらの機能はライブラリモデルによって異なります。5章「[ライブラリでの SNMP の構成](#)」に進む前に、この章のアクティビティを完了するようにしてください。

この章には次のセクションが含まれます。

- [STA データに影響を及ぼすライブラリ機能](#)
- [ライブラリのユーザーインターフェース](#)
- [ライブラリ機能構成タスク](#)

4.1. STA データに影響を及ぼすライブラリ機能

- [「LTO ドライブ用の ADI インタフェース」](#)
- [「デュアル TCP/IP および冗長電子装置 \(SL3000 および SL8500 のみ\)」](#)
- [「ライブラリコンプレックス ID \(SL8500 のみ\)」](#)
- [「ドライブのクリーニング警告 \(SL3000 および SL8500 のみ\)」](#)
- [「ボリュームラベル形式 \(SL500 および SL150 のみ\)」](#)
- [「SCSI FastLoad」オプション \(SL500 のみ\)」](#)
- [「重複するボリュームシリアル番号」](#)

4.1.1. LTO ドライブ用の ADI インタフェース

StorageTek モジュラーライブラリは、HP および IBM 製の Linear Tape Open (LTO) ドライブをサポートしています。Automation/Drive Interface (ADI) をサポートしている LTO ドライブは、ドライブの構成やファームウェアレベルに応じて、豊富なデータ (たとえば、ドライブのパフォーマンスや使用率) をライブラリに提供できます。

ライブラリで豊富な LTO ドライブデータを STA に送信するためには、そのライブラリと LTO ドライブの両方で ADI を有効にする必要があります。両方で ADI が有効になっていないと、ライブラリは LTO ドライブに関する基本データしか送信できません。

必要なドライブファームウェアレベルの詳細は、『STA 要件ガイド』を参照してください。

4.1.1.1. LTO ドライブでの ADI の有効化

ADI を有効にする方法は、ドライブの製造元およびモデルによって異なります。

- **HP LTO-3、LTO-4、LTO-5、および LTO-6:** これらのドライブは、ライブラリで ADI が有効になり、ライブラリがリブートし、ドライブがリブートすると、自動的に ADI モードに切り替わります。(ドライブは SL コンソールを使用してリブートできます。)
- **IBM LTO-3、LTO-4、LTO-5、および LTO-6:** これらのドライブは、ADI モード用に明示的に構成する必要があり、ライブラリで ADI が有効になり、ライブラリがリブートするまで認識されません。表4.1「IBM LTO ドライブで ADI を有効にする方法」に詳細が記載されています。

注:

Belisarius アダプタカードは、Oracle Key Manager (OKM) テープ暗号化ソリューションへのインタフェースを提供します。ドライブファームウェアと Belisarius カードファームウェアの両方が STA の最小要件を満たしている必要があります。

表4.1 IBM LTO ドライブで ADI を有効にする方法

IBM LTO ドライブ	LTO - 3	LTO - 4	LTO - 5、LTO-6
Belisarius アダプタカードを搭載しない IBM	Oracle サポートがドライブハードウェアを ADI モード用に構成します。	Oracle サポートがドライブハードウェアを ADI モード用に構成します。	なし
Belisarius アダプタカードを搭載した IBM	なし	Oracle サポートがドライブハードウェアを ADI モード用に構成します。	Virtual Operator Panel (VOP) を使用してドライブファームウェアを ADI モード用に構成する必要があります。Oracle サポートに連絡してください。

4.1.1.2. ライブラリでの ADI の有効化

デフォルトで ADI は SL500、SL3000、および SL8500 ライブラリで有効ではなく、ユーザーまたは Oracle サポートが手動で有効にする必要があります。ADI を有効にするにはライブラリをリブートする必要があるため、LTO ドライブの取り付けを計画している場合は、事前に有効にする必要があります。

SL3000 および SL8500 ライブラリでは、ライブラリにハイメモリードライブコントローラ (HBT) カードが搭載されている場合にのみ ADI を有効にできます。HBT カードの詳細は、『STA 要件ガイド』を参照してください。

4.1.2. デュアル TCP/IP および冗長電子装置 (SL3000 および SL8500 のみ)

冗長電子装置およびデュアル TCP/IP は SL3000 および SL8500 ライブラリのオプション機能です。

デュアル TCP/IP は、2 つのライブラリ TCP/IP ポートを提供することで、ライブラリやホストの操作をネットワーク障害から保護します。これは通常、個々のサブネット上で構成されます。一方のサブネット上でネットワークの切断または障害が発生した場合、ライブラリまたはホスト接続は自動的にもう一方のポートにフェイルオーバーします。

冗長電子装置は、2 つの別個の完全に機能的なライブラリコントローラカード (つまりアクティブでスタンバイ状態にあるもの) を提供することで、ライブラリコントローラのハードウェア障害から保護します。アクティブなコントローラで重大なエラーが検出された場合は、ライブラリ制御をスタンバイカードに切り替えて、ライブラリやホストの操作の中断を最小限に抑えることができます。

これらの機能の詳細は、ライブラリのユーザーズガイドを参照してください。

4.1.2.1. これらの機能をサポートするように STA 接続を構成

これらの機能 (デュアル TCP/IP、冗長電子装置、その両方) のどれがアクティブ化されているかに応じて、SL3000 または SL8500 ライブラリは 1 つ、2 つ、または 4 つの IP アドレスを持つことができます。ただし、STA は、同時に最大 2 つのライブラリ IP アドレスとの連続した接続しか保持できません。そのため、特定のライブラリでは、デュアル TCP/IP または冗長電子装置のいずれか (両方ではない) をサポートするように STA を構成できます。

ライブラリへの STA 接続を構成するときは、必ずプライマリライブラリ IP アドレスを指定する必要があります。ライブラリの機能構成や STA でサポートする機能に応じて、オプションでセカンダリ IP アドレスを指定することもできます。

注:

両方の機能を備えたライブラリの場合、Oracle では、冗長電子装置をサポートするよう STA を構成することをお勧めします。連続したライブラリ操作を保持するために、この機能がより不可欠であるためです。

STA がデュアル TCP/IP をサポートするように構成されている場合、ポートのフェイルオーバーの発生時にライブラリとの接続が保持されます。

STA が冗長電子装置をサポートするように構成されている場合、コントローラカードの切り替え時に、セカンダリライブラリ IP アドレスとして指定されたポートを介してライブラリとの接続が保持されます。

これらの機能の詳細は、ライブラリのユーザーズガイドを参照してください。

表4.2「[STA 接続のための推奨されるライブラリ IP アドレス](#)」に、ライブラリへの STA 接続の構成時に使用する、推奨されるライブラリ IP アドレスをまとめて示します。

表4.2 STA 接続のための推奨されるライブラリ IP アドレス

アクティブ化された機能	プライマリライブラリ IP	セカンダリライブラリ IP
いずれもなし	2B ポート	なし
デュアル TCP/IP のみ	2B ポート	アクティブなカードの 2A ポート
冗長電子装置のみ	アクティブなカードの 2B ポート	スタンバイカードの 2B ポート
両方	アクティブなカードの 2B ポート	スタンバイカードの 2B ポート

4.1.2.2. これらの機能に関するその他の考慮事項

- SL3000 または SL8500 ライブラリでデュアル TCP/IP をサポートするように STA を構成するには、ポリシールーティングを使用する必要がある場合があります。詳細は、SL3000 または SL8500 の『[ホスト接続ガイド](#)』を参照してください。デュアル TCP/IP 構成の支援が必要な場合は、Oracle サポートに連絡してください。
- ライブラリに冗長電子装置とデュアル TCP/IP の両方がある場合、STA サーバーのサブネットは、STA 用に構成されていないライブラリポートのサブネットとは異なる必要があります（[「ライブラリへの SNMP 接続の構成」](#)を参照）。そうしない場合、ライブラリはそれらのポート（STA にとっては不明）を通じてデータを送信しようとし、そのデータは STA によって拒否されることになります。
- デフォルトゲートウェイは必ず 2B インタフェースにしてください。

4.1.3. ライブラリコンプレックス ID (SL8500 のみ)

STA がライブラリコンプレックスのデータを正しくロールアップできるようにするため、サイトの各ライブラリコンプレックスには、一意のコンプレックス ID が必要です。SL8500 ライブラリでは、コンプレックス ID を手動で設定します。ほかのすべてのライブラリモデルでは、コンプレックス ID は自動的に設定されるため、手動での介入や検証は必要ありません。

各スタンドアロン SL8500 は、別個のコンプレックスであるとみなされ、そのため一意のコンプレックス ID が必要です。また、各マルチライブラリコンプレックスにも一意のコンプレックス ID が必要であり、コンプレックス内のすべてのライブラリが同じ ID を共有する必要があります。有効なコンプレックス ID の値は、1-127 です。

表4.3「[コンプレックス ID の割り当ての例](#)」に、SL8500 の有効なコンプレックス ID 割り当ての例をいくつか示します。

表4.3 コンプレックス ID の割り当ての例

コンプレックスのタイプ	ライブラリ	割り当てられたコンプレックス ID
マルチライブラリコンプレックス	SL8500-1	1
	SL8500-2	1
	SL8500-3	1
スタンドアロンライブラリ	SL8500-4	2
	SL8500-5	3

注意:

Oracle Service Delivery Platform (SDP) も、ライブラリデータを追跡するために一意のコンプレックス ID を使用します。サイトで SDP を使用する場合は、コンプレックス ID を変更する前に Oracle サポートに連絡してください。コンプレックス ID を変更すると、SDP で障害が発生する可能性があります。ほとんどの場合、SDP が接続されていればコンプレックス ID は正しく設定されています。

手順については、「[正しいライブラリコンプレックス ID の確認 \(SL8500 のみ\)](#)」を参照してください。

4.1.4. ドライブのクリーニング警告 (SL3000 および SL8500 のみ)

ドライブのクリーニング警告フラグは、ドライブのクリーニングが必要などときには常にドライブの警告を発行するべきかどうかを示します。このフラグは、ライブラリレベルで設定されるため、同じ設定がライブラリ内のすべてのドライブに適用されます。

- フラグが「on」に設定されているときは、各ドライブでクリーニングが必要などときには常に、警告のヘルスステータスが表示されます。また、これによって、ライブラリの最上位レベルのヘルスステータスが STA モニターで低下します。
- フラグが「off」に設定されているときは、各ドライブのステータスはクリーニングの必要性の影響を受けないため、STA におけるライブラリの最上位レベルのステータスは低下しません。

ライブラリ内に多数のドライブがある場合、ドライブでクリーニングが必要になるたびにライブラリの最上位レベルの状態が低下しないように、このフラグを「off」に設定することをお勧めします。

手順については、「[ドライブのクリーニング警告の設定 \(オプション、SL3000 および SL8500 のみ\)](#)」を参照してください。

4.1.5. ボリュームラベル形式 (SL500 および SL150 のみ)

STA がライブラリ交換データを正しく処理するために、SNMP データ内のボリュームシリアル番号 (volser) が正しい形式になっている必要があります。メディアの volser には、メディアタイプを示す 2 文字の接尾辞が含まれています。たとえば、カートリッジの volser が ABC123L4 だとすると、「L4」はメディアタイプが LTO4であることを示します。STA が適切に報告するには、volser の接尾辞が除外される必要があります。

形式設定が正しく行われるようにするには、次のパラメータを設定する必要があります。

- STA によってモニターされるすべての SL500 ライブラリでは、ホストのラベルの向きが *left6* に設定され、STA モード (*staConfig* フラグで制御される) が *on* に設定される必要があります。STA モードは、SNMP を介して STA サーバーに送信される volser の形式にのみ影響し、SL500 ライブラリ自体で使用される形式には影響しません。
- STA によってモニターされるすべての SL150 ライブラリでは、「Volume Label Format」が「*Trim last two characters*」に設定される必要があります。

注意:

これらのパラメータが適切に設定されない場合、volser の形式が正しくないため、交換処理がブロックされたり、最新のメディアデータを無用に取得しようとしたり、「Show Removed Media」設定が設定されているときには常に) 取り消しできない 8 文字の volser レコードが「Media - Overview」画面に表示されたりします。

手順については、「[SL500 ボリュームラベル形式の設定 \(SL500 のみ\)](#)」および「[SL150 ボリュームラベル形式およびドライブ要素アドレッシングモードの設定 \(SL150 のみ\)](#)」を参照してください。

4.1.6. 「SCSI FastLoad」オプション (SL500 のみ)

「SCSI FastLoad」オプションは、SL500 ライブラリでは無効にするべきです。「SCSI FastLoad」が有効になっていると、カートリッジマウントトラップが STA に適切に送信されません。「FastLoad」はデフォルトで無効になっています。このオプションのステータスが不明な場合は、Oracle サポートに連絡してください。

4.1.7. 重複するボリュームシリアル番号

STA データストアでは、メディアの履歴はボリュームシリアル番号 (volser) によって保持されます。メディアの特定の部分の履歴はすべてその volser に関連付けられるため、Oracle では、volser の重複を避けることをお勧めします。volser は、モニターされるすべてのライブラリ間で一意であるべきです。volser が重複していると、メディアのさまざまな部分のデータが混在します。

重複する volser の詳細は、『STA ユーザーズガイド』を参照してください。

4.2. ライブラリのユーザーインターフェース

SL500、SL3000、および SL8500 ライブラリには、コマンド行インターフェース (CLI) と、グラフィカルユーザーインターフェースである StorageTek ライブラリコンソール (SL コンソール) があります。SL150 ライブラリは、ブラウザベースのユーザーインターフェースを排他的に使用します。この章に記載された手順の実行には、これらのインターフェースを使用します。

4.2.1. ライブラリ CLI の使用上のヒント

ほとんどの CLI コマンドでは、構文は SL500、SL3000、および SL8500 ライブラリモデル間で同じです。構文がライブラリモデルによって異なるいくつかのコマンドについては、例が示されています。大部分の CLI の例は SL500 ライブラリを使用します。SL3000 または SL8500 ライブラリを構成している場合、各コマンドによって返される詳細は、表示されているものとわずかに異なることがあります。ライブラリ CLI を使用した場合のいくつかのヒントは次のとおりです。

- ライブラリ CLI への SSH (セキュアシェル) 接続を確立するには、PuTTY などの端末エミュレータを使用します。
- エラーのトラブルシューティングが必要な場合は、アクティビティーを確認できるようにロギングを有効にします。
- 一部のファームウェアバージョンでは、CLI は 6 時間後にタイムアウトになります。
- 任意の CLI コマンドのヘルプを表示するには、*help* とコマンド名を入力します (たとえば、*help snmp*)。
- SL500 ライブラリコマンドでは大文字と小文字が区別されます。SL3000 と SL8500 コマンドでは区別されません。
- 入力エラーを回避するために、最初にテキストファイルにコマンドを入力してから、CLI にコピー&ペーストできます。CLI コマンドのヘルプについては、*help snmp* と入力します。
- 次の CLI 機能を使用することで、キーストローク数を減らせます。

- コマンドの自動補完には、**Tab** キーを押します。
- コマンド履歴をスクロールするには、上矢印および下矢印キーを押します。以前に入力したコマンドを変更してから、**Enter** を押して実行できます。
- **Enter** を押して実行する前にコマンドを訂正するには、左矢印および右矢印キーを使用してエラーの場所にカーソルを移動してから、訂正内容を入力します。そのカーソル位置に新しい文字が挿入されます。その文字を削除するには、**Back Space** キーを使用します。

4.2.2. ライブラリ構成スクリプト (オプション)

STA には、ライブラリに関する構成プロセスを実行する際に役立つライブラリ構成スクリプトが用意されています。このスクリプトはライブラリ構成設定の入力を求め、入力された値に基づいて、ライブラリ CLI にコピー&ペーストできる完全なコマンドを表示します。

注:

スクリプトを開始する前に、この章のライブラリ構成手順を確認して理解することをお勧めします。

スクリプトを開始するには、STA サーバーで端末セッションを開き、次のコマンドを発行します。

```
# sh /Oracle_storage_home/StorageTek_Tape_Analytics/common/bin/STA-lib-config-steps.sh
```

ここで、*Oracle_storage_home* は STA とそれに関連する Oracle ソフトウェアがインストールされているディレクトリです。詳細は、「[STA インストーラで使用するユーザー、グループ、場所](#)」を参照してください。

スクリプトの追加情報および使用例については、次のコマンドを発行してください。

```
# sh /Oracle_storage_home/StorageTek_Tape_Analytics/common/bin/STA-lib-config-steps.sh
-? | more
```

4.3. ライブラリ機能構成タスク

サイトのライブラリモデルに適用するタスクを判断するには、[表4.4「STA のライブラリを構成するためのタスク」](#)を使用します。STA でモニターするライブラリごとに適切なタスクを実行する必要があります。

表4.4 STA のライブラリを構成するためのタスク

タスク	SL150	SL500	SL3000	SL8500
「ライブラリへのログイン」	はい	はい	はい	はい

タスク	SL150	SL500	SL3000	SL8500
「ライブラリファームウェアバージョンの確認」	はい	はい	はい	はい
「ドライブコントローラカードのバージョンの確認 (SL3000 および SL8500 のみ)」	–	–	はい	はい
「ライブラリでの ADI の有効化 (SL150 を除くすべてのライブラリ)」	–	はい	はい	はい
「正しいライブラリコンプレックス ID の確認 (SL8500 のみ)」	–	–	–	はい
「ドライブのクリーニング警告の設定 (オプション、SL3000 および SL8500 のみ)」	–	–	はい	はい
「SL500 ポリウムラベル形式の設定 (SL500 のみ)」	–	はい	–	–
「SL150 ポリウムラベル形式およびドライブ要素アドレッシングモードの設定 (SL150 のみ)」	はい	–	–	–

注:

SL500、SL3000、および SL8500 ライブラリの場合、多数のタスクで、使用するインタフェースとして CLI または SL コンソールを選択できます。SL150 ライブラリの場合、ブラウザベースのユーザーインタフェースを排他的に使用する必要があります。

4.3.1. ライブラリへのログイン

ライブラリ CLI の使用 (SL150 を除くすべてのライブラリ)

1. IP アドレスまたは DNS 別名を使用してライブラリへの SSH 接続を確立します。
2. *admin* のユーザー名とパスワードを使用して CLI にログインします。

SL コンソールの使用 (SL150 を除くすべてのライブラリ)

1. SL コンソールアプリケーションを起動します。
2. 「**About**」ボタンをクリックして現在の SL コンソールのバージョンを表示し、ライブラリファームウェアの最小要件を満たしていることを確認します。
3. 「**Close**」をクリックして、「**Login**」画面に戻ります。
4. *admin* のユーザー名、パスワード、およびライブラリ IP アドレスまたは DNS 別名を使用してログインします。

冗長電子装置機能を備えた SL3000 および SL8500 ライブラリでは、アクティブコントローラにのみログインできます。

SL150 ユーザーインタフェースの使用

1. SL150 ライブラリのホスト名または IP アドレスを参照します。

2. ユーザー ID とパスワードを使用してログインします。ユーザー ID は、管理者の役割を持っている必要があります。

4.3.2. ライブラリファームウェアバージョンの確認

ライブラリファームウェアが『STA 要件ガイド』に記載されている最小要件を満たしているかこれを超えていることを確認するには、次の手順を使用します。それ以外の場合は、Oracle サポートにサービスリクエストを送信してファームウェアをアップグレードします。

SL8500 ライブラリの場合、アップグレード後にネットワーク接続設定の再入力または更新が必要になることがあるため、Oracle サポートではファームウェアのアップグレードを実行する前にこれらの設定を記録する必要があります。

ライブラリ CLI の使用 (SL150 を除くすべてのライブラリ。ただし、FRS 4.x より下の SL3000 ライブラリには適用されない)

1. 次のコマンドを実行します。

```
SL500> version print
Library Hardware Information
Library Vendor: STK
...
Firmware Version: xxxx (x.xx.xx)
```

注:

画面に「SYNTAX ERROR!!」が表示される場合、ライブラリファームウェアは下位レベルです。Oracle サポートに連絡してファームウェアをアップグレードしてください。

SL コンソールの使用 (SL150 を除くすべてのライブラリ)

1. 「Tools」メニューで、「System Detail」を選択します。
2. ナビゲーションツリーで、「Library」を選択します。
3. 「Properties」タブを選択してから、「Library Controller」タブを選択します。

ファームウェアバージョンが「Code Version」セクションの下に表示されます。

SL150 ユーザーインターフェースの使用

1. ナビゲーションツリーで、「Firmware」を選択します。

ファームウェアバージョンが「Library Firmware」セクションの下に表示されます。または、ステータスバーの「**About**」ボタンをクリックして、ファームウェアバージョンを取得することもできます。

4.3.3. ドライブコントローラカードのバージョンの確認 (SL3000 および SL8500 のみ)

SL3000 および SL8500 ライブラリで豊富なドライブデータを STA に送信するためには、ライブラリにハイメモリードライブコントローラ (HBT) カードが搭載されている必要があります。新しいユニットにはハイメモリーカードが標準装備されているため、これは主に古いライブラリ (2006 年半ば以前に出荷されたもの) に関することです。ファームウェアレベルの詳しい要件については、『*STA 要件ガイド*』を参照してください。

ハイメモリー HBT カードがライブラリに取り付けられていることを確認するには、次の手順を使用します。ライブラリにハイメモリー HBT カードが搭載されていない場合は、Oracle サポートにサービスリクエストを送信してそれを取り付けてもらいます。

この手順は SL コンソールを使用して実行します。SL8500 FRS 8.x および SL3000 FRS 4.x の場合、CLI `config print` コマンドを使用して HBT カード情報を表示することもできます。

この手順は SL コンソールを使用して実行します。

1. 「**Tools**」メニューで、「**System Detail**」を選択します。
2. ナビゲーションツリーで、「**Library**」を選択します。
3. 「**Properties**」タブを選択してから、「**Drive Controller**」タブを選択します。

画面に、アクティブなドライブコントローラ (HBT) カードに関する詳細が表示されます。

4. 「High Memory HBT」に「*true*」と示されていることを確認します。
5. 冗長電子装置を備えた SL3000 (FRS 4.x) または SL8500 (FRS 8.x) ライブラリがある場合、「Redundant Electronics」フォルダを展開して、それぞれの HBT カード (hbta, hbtb) を選択します。両方の「High Memory HBT」に「*True*」が示されるはずですが。

注:

アクティブとスタンバイの両方の HBT カードが取り付けられていて通信中である必要があり、両方にハイメモリーがある必要があります。

4.3.4. ライブラリでの ADI の有効化 (SL150 を除くすべてのライブラリ)

ライブラリに LTO ドライブが含まれる場合、豊富なドライブデータを受信するためには、そのドライブと STA のライブラリの両方で ADI プロトコルを有効にする必要があります。ADI ドライブインタフェースがライブラリで有効になっていることを確認するには、次の手順を使用します。詳細は、「[LTO ドライブ用の ADI インタフェース](#)」を参照してください。

この手順はライブラリ CLI を使用して実行します。

SL3000 または SL8500 ライブラリの場合

1. ADI インタフェースのステータスを表示します。

```
drive adiEnable print
```

2. 「Attributes Adi Status」が *true* の場合、このタスクを終了できます。*false* の場合、次の手順に進みます。
3. ADI インタフェースを有効にします。

```
drive adiEnable on
```

4. ライブラリをリブートして、変更をアクティブ化します。

SL500 ライブラリの場合

1. ADI インタフェースのステータスを表示します。

```
enableADI print
```

2. 「enableADI set to」が *on* の場合、このタスクを終了できます。*off* に設定されている場合、次の手順に進みます。
3. ADI インタフェースを有効にします。

```
enableADI on
```

4. ライブラリをリブートして、変更をアクティブ化します。

4.3.5. 正しいライブラリコンプレックス ID の確認 (SL8500 のみ)

STA がライブラリコンプレックスのデータを正しくロールアップできるようにするため、サイトの各ライブラリコンプレックスには、一意のコンプレックス ID が必要です。各 SL8500 ライブラリの正しいライブラリコンプレックス ID を確認するには、次の手順を使用します。詳細は、「[ライブラリコンプレックス ID \(SL8500 のみ\)](#)」を参照してください。

この手順はライブラリ CLI を使用して実行します。

1. STA でモニターされる SL8500 ライブラリごとに、現在割り当てられているコンプレックス ID を表示します。

```
SL8500> config complexId print
```

```
...  
Complex Id 3  
...
```

2. 各スタンドアロンライブラリと各ライブラリコンプレックスに一意のコンプレックス ID があること、各ライブラリコンプレックス内のすべてのライブラリが同じコンプレックス ID を共有していることを確認します。

スタンドアロンライブラリのコンプレックス ID を変更する必要がある場合、この手順を続行します。

注意:

ライブラリコンプレックス内のライブラリのコンプレックス ID を変更する必要がある場合、Oracle サポートに連絡してください。この手順を続行しないでください。

3. ライブラリをオフラインにしてから、すべてのトランザクションが完了するのを待機します。
4. スタンドアロンライブラリのコンプレックス ID を変更します。*complex_ID* は 1 – 127 の数値です。

```
config complexId set complex_ID
```

例4.1 スタンドアロン SL8500 のコンプレックス ID の変更

```
SL8500> config complexId set 5
```

```
...  
Complex Id 5  
Success true  
Done
```

...

Note: TCP/IP stack reset may take a few seconds after command completion.

注:

このコマンドを実行すると、すべての TCP/IP 接続が終了します。ライブラリへの再度のログインが必要になる場合があります。

4.3.6. ドライブのクリーニング警告の設定 (オプション、SL3000 および SL8500 のみ)

ライブラリにおけるドライブのクリーニング警告フラグの現在の設定を確認して、必要に応じて変更するには、このオプションの手順を使用します。詳細は、「[ドライブのクリーニング警告 \(SL3000 および SL8500 のみ\)](#)」を参照してください。

この手順はライブラリ CLI を使用して実行します。

1. ドライブのクリーニング警告フラグの現在の設定を表示します。

```
SL3000> cleaning driveWarning get
...
Object Drive Cleaning Warning true
...
```

2. このフラグを *false* (off) に設定する場合、次のコマンドを使用します。

```
cleaning driveWarning set off
```

4.3.7. SL500 ボリュームラベル形式の設定 (SL500 のみ)

STA に送信される SNMP データでボリュームシリアル番号 (volser) が正しく形式設定されていることを確認するには、次の手順を使用します。詳細は、「[ボリュームラベル形式 \(SL500 および SL150 のみ\)](#)」を参照してください。

この手順は SL500 CLI を使用して実行します。

注:

Oracle では、これらのパラメータを変更する前にライブラリに対するすべてのアクティビティを休止することをお勧めします。テープアプリケーションとホスト、またはそのいずれかでは、これらのパラメータの変更後に構成の変更が必要になる場合があります。

1. *orientlabel* フラグの現在の設定を表示します。

```
SL500> orientlabel print
Host: (left8) Window left-justified with 6 character label
Op Panel: (left8) Window left-justified with 8 character label
```

2. *host* フラグを *left6* に設定する必要があります。これには、次のコマンドを使用します。

```
SL500> orientlabel host left6
New settings were accepted...Setting are now in effect.
```

3. 設定を再度表示して、正しく更新されたことを確認します。

```
SL500> orientlabel print
Host: (left6) Window left-justified with 6 character label
Op Panel: (left8) Window left-justified with 8 character label
```

4. *staConfig* フラグの現在の設定を表示します。

```
SL500> staConfig print
STA mode is disabled
```

5. *staConfig* フラグを *on* に設定する必要があります。これには、次のコマンドを使用します。

```
SL500> staConfig on
```

6. 設定を再度表示して、正しく更新されたことを確認します。

```
SL500> staConfig print
STA mode is enabled
```

4.3.8. SL150 ボリュームラベル形式およびドライブ要素アドレッシングモードの設定 (SL150 のみ)

STA に送信される SNMP データでボリュームシリアル番号 (*volser*) が正しく形式設定されていることを確認するには、次の手順を使用します。

また、SL150 ファームウェア 2.xx 以上では、この手順を使用して、STA に送信されるデータに空のドライブベイが含まれるようにドライブ要素アドレッシングモードを設定します。

詳細は、「[ボリュームラベル形式 \(SL500 および SL150 のみ\)](#)」を参照してください。

注:

Oracle では、これらのパラメータを変更する前にライブラリに対するすべてのアクティビティを休止することをお勧めします。テープアプリケーションとホストでは、これらのパラメータの変更後に構成の変更が必要になる場合があります。

この手順は SL150 ブラウザベースインタフェースを使用して実行します。

1. ナビゲーションツリーで、「**Configuration**」を選択します。
2. 「**Configure**」ボタンを選択します。
3. 構成ウィザードのウィンドウで、「**Configure Library Settings**」チェックボックスを選択して、「**Next**」をクリックします。
4. 次のパラメータをそのように設定します。
 - 「Drive Element Addressing Mode」: 「**Address All Drive Slots (Recommended)**」
 - 「Library Volume Label Format」: 「**Trim last two characters (Default)**」

注:

「Drive Element Addressing Mode」の変更後、STA で SNMP を構成する前に少なくとも 10 分待つようにしてください。

5. 「**Next**」をクリックします。
6. 「Summary of Configuration Changes」画面で、「**Accept all changes**」チェックボックスを選択して、「**Apply**」をクリックします。
7. 「Apply Configuration Changes」画面で、「**Set the Library back Online after applying the changes**」チェックボックスを選択して、「**OK**」をクリックします。
8. 「**All configuration changes have been applied successfully**」が表示されたら、「**Close**」をクリックします。

ライブラリでの SNMP の構成

STA でサイトでのライブラリのモニターを行うには、ライブラリと STA サーバーのそれぞれでいくつかの構成アクティビティーを実行する必要があります。この章では、ライブラリに対して実行されるアクティビティーについて説明します。[6章「STA でのライブラリ接続の構成」](#)に進む前に、この章のアクティビティーを完了するようにしてください。

この章には次のセクションが含まれます。

- [STA のライブラリ SNMP 構成について](#)
- [ライブラリ SNMP 構成タスク](#)

StorageTek ライブラリへの SNMP の実装に関する一般情報については、*StorageTek モジューラーライブラリの SNMP リファレンスガイド*を参照してください。

5.1. STA のライブラリ SNMP 構成について

STA とそれによってモニターされるライブラリとの通信は、Simple Network Management Protocol (SNMP) を介して行われます。ライブラリは SNMP トラップおよびインフォームを通じてデータを STA に送信し、STA は SNMP の `get` 関数を使用してライブラリ構成データを取得します。SNMP の観点から見ると、STA は クライアントエージェント、各ライブラリはサーバーエージェントになります。

SNMP v3 は、STA とライブラリとの SNMP 通信に推奨されるプロトコルです。SNMP v3 の認証、暗号化、およびメッセージ整合性機能では、ライブラリデータの送信にセキュアなメカニズムを提供します。SNMP v3 は STA メディア検証機能にも必要です (STA メディア検証はサポートされているライブラリにのみ使用可能。詳細は『*STA 要件ガイド*』を参照)。

この章では、推奨される SNMP v3 構成について説明します。ただし、サイトの要件に応じて、1 つ以上のライブラリに SNMP v2c を使用することを選択してもかまいません。SNMP v2c の構成手順については、[付録 F「SNMP v2c モードの構成」](#)を参照してください。

注:

SNMP v3 プロトコルは SNMP トラップおよび get 関数に使用されますが、ライブラリと STA との初期通信ハンドシェイクは常に SNMP v2c プロトコルを介して行われます。

5.1.1.1. ライブラリでの SNMP v3 プロトコルの構成

各ライブラリで、STA と各ライブラリとの SNMP v3 通信を設定するには、ライブラリを SNMP v3 ユーザーとして定義し、STA サーバーを SNMP v3 トラップ受信者として定義します。さらに、承認メカニズム、プライバシメカニズム、およびパスワードを指定する必要があります。STA では、承認方式は常に SHA (Secure Hash Algorithm) で、プライバシ方式は常に DES (Data Encryption Standard) です。

5.1.1.1.1. 一意の SNMP v3 ユーザー

STA では 1 つの SNMP v3 ユーザーのみがサポートされます。単一の STA インスタンスによってモニターされるすべてのライブラリで同じユーザーを定義する必要があります。使用する値を記録するためのワークシートについては、[付録C「インストールおよびアップグレードのワークシート」](#)を参照してください。

注:

ライブラリには 1 つ以上の SNMP v3 ユーザーがすでに存在する場合があります、STA 通信にはそれらのいずれかを使用できます。ただし Oracle では、この目的のために新しい一意の SNMP v3 ユーザーを設定することを強くお勧めします。

SNMP v3 ユーザーを定義するために指定する必要のある値は次のとおりです。

SNMP v3 ユーザー名

STA サーバーは、このユーザーによって送信されたトラップを待機します。これは、トラップ受信者の作成時に使用される SNMP v3 受信者名でもあります。すべてのライブラリで同じである必要があります。

SNMP v3 承認パスワード

SNMP v3 ユーザーに割り当てる承認パスワード。

少なくとも 8 文字の長さにする必要があります、コンマ、セミコロン、または等号を含めることはできません。

SNMP v3 プライバシ暗号化パスワード

SNMP v3 ユーザーに割り当てるプライバシパスワード。

少なくとも 8 文字の長さにする必要があります、コンマ、セミコロン、または等号を含めることはできません。

SNMP v2c ユーザーコミュニティ

通常は *public* に設定される SNMP v2c ユーザーコミュニティ文字列。SNMP v3 プロトコルを使用するときでも、ライブラリと STA サーバーの間の初期ハンドシェイクにはこの文字列が必要です。

英数字 (a-z、A-Z、0-9) のみ含めることができます。特殊文字は許可されません。

SNMP v2c トラップコミュニティ

ライブラリとの通信に SNMP v2c が使用される場合にのみ用いられる SNMP v2c トラップコミュニティ名。SNMP v3 を使用している場合は、この値をデフォルト (*public*) に設定されたまましておきます。

英数字 (a-z、A-Z、0-9) のみ含めることができます。特殊文字は許可されません。

5.1.1.2. SNMP エンジン ID

SNMP v3 プロトコルでは各 SNMP デバイスでグローバルに一意的なエンジン ID が必要となるため、STA サーバーとライブラリにはそれぞれ独自のエンジン ID があります。SL8500 ライブラリコンプレックスの場合、コンプレックス内の各ライブラリにも独自の SNMP エージェントがあるため、独自の一意のエンジン ID があります。エンジン ID には、最大 31 文字の 16 進数文字列が含まれています。

SNMP トラップは送信者のエンジン ID を使用します。そのため、STA を SNMP v3 トラップ受信者として定義する際に、ライブラリエンジン ID を指定する必要があります。

5.2. ライブラリ SNMP 構成タスク

表5.1「STA のライブラリを構成するためのタスク」に、適切な SNMP データを STA に送信するようにライブラリを構成するプロセスをまとめます。STA でモニターするライブラリごとに、それらのタスクを示された順に実行する必要があります。

表5.1 STA のライブラリを構成するためのタスク

タスク	SL150	SL500	SL3000	SL8500
「ライブラリ IP アドレスの取得」	はい	はい	はい	はい
「ライブラリでの SNMP の有効化」	はい	はい	はい	はい
「SNMP v2c ユーザーの確認」	はい	はい	はい	はい
「SNMP v3 ユーザーの作成」	はい	はい	はい	はい
「ライブラリ SNMP エンジン ID の取得 (SL150 を除くすべてのライブラリ)」	–	はい	はい	はい

タスク	SL150	SL500	SL3000	SL8500
「STA SNMP v3 トラップ受信者の作成」	はい	はい	はい	はい

注:

これらの手順では、STA とライブラリとの通信に推奨される SNMP v3 プロトコルを使用するものと想定します。詳細は、「[STA のライブラリ SNMP 構成について](#)」を参照してください。

注:

SL500、SL3000、および SL8500 ライブラリの場合、一部のタスクで、使用するインターフェースとして CLI または SL コンソールを選択できます。SL150 ライブラリの場合、常にブラウザベースのユーザーインターフェースを使用する必要があります。

5.2.1. ライブラリ IP アドレスの取得

ライブラリとの接続を構成するために使用するライブラリ IP アドレスを取得して記録するには、次の手順を使用します。

SL3000 および SL8500 ライブラリの場合、冗長電子装置またはデュアル TCP/IP のどちらかをサポートするか、どちらもサポートしない方法を選択します。詳細は、「[デュアル TCP/IP および冗長電子装置 \(SL3000 および SL8500 のみ\)](#)」を参照してください。

この手順は SL コンソールまたは SL150 ブラウザベースインターフェースを使用して実行します。

SL500 の IP アドレス

1. 「**Tools**」メニューから、「**System Detail**」を選択します。
2. ナビゲーションツリーで、「**Library**」を選択します。
3. 「**Properties**」タブを選択してから、「**General**」タブを選択します。

ライブラリ IP アドレスが「Library Interface TCP/IP」セクションの下に一覧表示されます。

4. ライブラリ IP アドレスをプライマリライブラリ IP アドレスとして記録します。(このアドレスは 1B ポートに対応します。)

SL3000 または SL8500 の IP アドレス — 冗長電子装置サポート

- a. 「**Tools**」メニューから、「**System Detail**」を選択します。
- b. ナビゲーションツリーで、「**Redundant Electronics**」フォルダを選択します。

このフォルダが一覧表示されない場合、冗長電子装置機能はこのライブラリでは使用できません。

- c. 「Device State」フィールドで、1つのライブラリコントローラに「*Duplex: software ready, switch possible*」(これがアクティブカード)が表示され、もう1つに「*Standby: software ready*」(これがスタンバイカード)が表示されることを確認します。

これらのステータスは、コントローラカードが正常に機能していることを示しています。これらのステータスが表示されない場合、Oracle サポートに連絡してください。

- d. 「**Redundant Electronics**」フォルダを展開して、アクティブコントローラカードを選択します。
- e. 2B ポートの IP アドレスを記録します。
- f. 代替 (スタンバイ) コントローラカードについて、手順 d と手順 e を繰り返します。

SL3000 または SL8500 の IP アドレス — デュアル TCP/IP サポート

- a. 「**Tools**」メニューから、「**System Detail**」を選択します。
- b. ナビゲーションツリーで、「**Library**」を選択します。
- c. 「**Properties**」タブを選択してから、「**General**」タブを選択します。

IP アドレス情報は、「Host Interface TCP/IP 2B」セクションと「Host Interface TCP/IP 2A」セクションに表示されます。

注:

ライブラリに冗長電子装置機能も組み込まれている場合、アクティブコントローラカードのみの IP アドレスが表示されます。

- d. プライマリ IP アドレス (2B セクション) とセカンダリ IP アドレス (2A セクション) を記録します。

SL3000 または SL8500 の IP アドレス — デュアル TCP/IP も冗長電子装置もなし

- a. 「**Tools**」メニューから、「**System Detail**」を選択します。
- b. ナビゲーションツリーで、「**Library**」を選択します。
- c. 「**Properties**」タブを選択してから、「**General**」タブを選択します。

IP アドレス情報は、「Host Interface TCP/IP 2B」セクションに表示されます。2A セクションには IP アドレス情報はありません。

- d. IP アドレスをプライマリライブラリ IP アドレスとして記録します。

SL150 の IP アドレス

1. ナビゲーションツリーで、「**Configuration**」を選択します。

「**Settings**」を選択してから、「**Network**」を選択します。ライブラリ IP アドレスが「**Network Port 1 Settings**」セクションに表示されます。(「**Network Port 2 Settings**」セクションはサービスの使用のために予約されています。)

注:

「**Configure IPxx**」フィールド値は「*Static*」である必要があります。そうではない場合、「**Configure**」ボタンをクリックしてから、「**Configure Network Settings**」を選択して静的 IP アドレスを指定します。

5.2.2. ライブラリでの SNMP の有効化

ライブラリのパブリックポートで SNMP を有効にするには、次の手順を使用します。

ライブラリ CLI の使用

1. ライブラリモデルに応じて、次のいずれかのコマンドを使用します。
 - SL3000 および SL8500 ライブラリの場合、ポート 2B で SNMP を有効にします。ライブラリにデュアル TCP/IP 機能が組み込まれている場合、このコマンドによってポート 2A でも SNMP が有効になります。

```
snmp enable port2b
```

- SL500 ライブラリの場合、ポート 1B で SNMP を有効にします。

```
snmp enable port1B
```

SL コンソールの使用 (SL500 のみ)

1. 「**Tools**」メニューから、「**System Detail**」を選択します。
2. ナビゲーションツリーで、「**Library**」を選択します。
3. 「**SNMP**」タブを選択してから、「**Port Control**」タブを選択します。
4. 次のように「**Port Control**」セクションに入力します。

「**Port**」: 「*Public (1B)*」を選択します。

「**Command**」: 「*Enable*」を選択します。

5. 「**Apply**」をクリックします。

SL150 ユーザーインターフェースの使用

1. ナビゲーションツリーで、「**SNMP**」を選択します。
2. SNMP が無効と示される場合、「**Enable SNMP**」を選択します。
3. 確認ウィンドウで、「**OK**」をクリックします。

5.2.3. SNMP v2c ユーザーの確認

SNMP v2c ユーザーは、ライブラリと STA サーバーの間の初期ハンドシェイクに必要です。また、STA 通信に SNMP v2c を使用する場合にも必要です。詳細は、「[STA のライブラリ SNMP 構成について](#)」を参照してください。

次の構成要件に注意してください。

- ライブラリには SNMP v2c ユーザーが 1 つだけ必要です。
- SNMP v2c コミュニティー文字列には英数字 (a - z, A - Z, 0 - 9) のみを含めることができます。特殊文字は許可されません。
- 既存の SNMP v2c ユーザーは一般に *public* コミュニティーに設定されますが、別のコミュニティ名で定義してもかまいません。
- Oracle サービスに連絡せずに既存の SNMP v2c *public* ユーザーを削除しないようにしてください。場合によっては、SNMP v2c *public* ユーザーは Oracle Service Delivery Platform (SDP) に必要です。

ライブラリ CLI の使用 (SL150 を除くすべてのライブラリ)

1. SNMP v2c ユーザーがすでに存在するかどうかを確認します。

```
snmp listUsers
```

2. 次の例に示すように SNMP v2c ユーザーがすでに定義されている場合、このタスクを終了できます。それ以外の場合は、次の手順に進みます。

```
SL500> snmp listUsers
...
Attributes Community public
Index 1
Version v2c
Object Snmp snmp
...
```

3. SNMP v2c ユーザーを追加します。

```
snmp addUser version v2c community community_name
```

ここで、*community_name* は、*public* または別の名前です。例:

```
SL3000> snmp addUser version v2c community public
```

4. SNMP ユーザーを再度一覧表示して、SNMP v2c ユーザーが正しく追加されていることを確認します。

```
snmp listUsers
```

SL コンソールの使用 (SL500 のみ)

1. 「**Tools**」メニューから、「**System Detail**」を選択します。
2. ナビゲーションツリーで、「**Library**」を選択します。
3. 「**SNMP**」タブを選択してから、「**Add Users**」タブを選択します。
4. SNMP v2c ユーザーが「**Users**」セクションにすでに存在する場合、このタスクを終了できます。それ以外の場合は、次の手順に進みます。
5. SNMP v2c ユーザーを追加するには、次のように「**Add Users**」タブに入力します。
 - 「*Version*」: 「*v2c*」を選択します。
 - 「*Community*」: コミュニティー文字列 (たとえば、*public*) を指定します。
6. 「**Apply**」をクリックします。

デフォルトでは、SL150 は SNMP v2c ユーザーが定義されていない状態で出荷されます。STA 通信に SNMP v2c を使用する予定がある場合は、次のように SNMP v2c ユーザーを作成します。

SL150 ユーザーインターフェースの使用

1. ナビゲーションツリーで、「**SNMP**」を選択します。
2. 「**SNMP Users**」セクション (またはタブ) で、「**Add SNMP User**」を選択します。
3. 「**Add SNMP User**」画面で、次のように情報を入力します。

「*Version*」: 「*v2c*」を選択します。

「*Community Name*」: コミュニティー文字列 (たとえば、*public*) を指定します。

4. 「OK」をクリックします。

5.2.4. SNMP v3 ユーザーの作成

すべての SNMP トラップおよび MIB (管理情報ベース) データは、SNMP v3 ユーザーを介して STA サーバーに送信されます。指定するユーザー名とパスワードは書き留めておきます。この情報は、SNMP v3 トラップ受信者を定義するときに使用します。

次の構成要件に注意してください。

- 承認方式は *SHA* (Secure Hash Algorithm) で、プライバシ方式は *DES* (Data Encryption Standard) である必要があります。
- 単一の STA インスタンスによってモニターされるすべてライブラリに同じ SNMP v3 ユーザー名を割り当てる必要があります。このために、新しい一意のユーザーを作成する必要があります。
- 承認パスワードとプライバシパスワードは、少なくとも 8 文字の長さにする必要があります、コンマ、セミコロン、または等号を含めることはできません。

ライブラリ CLI の使用 (SL150 を除くすべてのライブラリ)

1. SNMP v3 ユーザーを作成します。

```
snmp addUser version v3 name name auth SHA authPass auth_password priv DES
privPass priv_password
```

ここでは:

- *name* は SNMP v3 ユーザー名です。
- *auth_password* および *priv_password* は承認パスワードとプライバシパスワードです。

注:

SL3000 および SL8500 ライブラリの場合、すべての変数を単一引用符で囲みます (例5.1「SL3000 または SL8500 での SNMP v3 ユーザーの作成」)。

例5.1 SL3000 または SL8500 での SNMP v3 ユーザーの作成

```
SL3000> snmp addUser version v3 name 'STAsnmp' auth SHA authPass 'authpwd1' priv
DES privPass 'privpwd1'
```

例5.2 SL500 での SNMP v3 ユーザーの作成

```
SL500> snmp addUser version v3 name STAsnmp auth SHA authPass authpwd1 priv DES  
privPass privpwd1
```

2. SNMP ユーザーを一覧表示して、SNMP v3 ユーザーが正しく追加されていることを確認します。

```
snmp listUsers
```

SL コンソールの使用 (SL500 ライブラリのみ)

1. 「**Tools**」メニューから、「**System Detail**」を選択します。
2. ナビゲーションツリーで、「**Library**」を選択します。
3. 「**SNMP**」タブを選択してから、「**Add Users**」タブを選択します。
4. 次のように「**Add Users**」タブに入力します。
 - 「*Version*」: 「v3」を選択します。
 - 「*UserName*」: SNMP v3 ユーザーの名前。
 - 「*Auth*」: 「SHA」を選択します。
 - 「*AuthPass*」: 承認パスワードを指定します。
 - 「*Priv*」: 「DES」を選択します。
 - 「*PrivPass*」: プライバシパスワードを指定します。
5. 「**Apply**」をクリックします。

SL150 ユーザーインターフェースの使用

1. ナビゲーションツリーで、「**SNMP**」を選択します。
2. 「SNMP Users」セクションで、「**Add SNMP User**」を選択します。
3. 「Version」では「v3」を選択して、次のように情報を入力します。
 - 「*User Name*」: SNMP v3 ユーザーの名前。
 - 「*Authentication Protocol*」: 「SHA」を選択します。
 - 「*Authentication Passphrase*」: 承認パスワードを指定します。
 - 「*Privacy Protocol*」: 「DES」を選択します。
 - 「*Privacy Passphrase*」: プライバシパスワードを指定します。
4. 「**OK**」をクリックします。

5.2.5. ライブラリ SNMP エンジン ID の取得 (SL150 を除くすべてのライブラリ)

ライブラリの SNMP エンジン ID (たとえば、0x81031f88804b7e542f49701753) を表示するには、次の手順を使用します。

この手順はライブラリ CLI を使用して実行します。

1. ライブラリモデルに応じて、次のいずれかのコマンドを使用します。

- SL3000 および SL8500 ライブラリの場合:

```
snmp engineId print
```

- SL500 ライブラリの場合:

```
snmp engineId
```

2. 残りの SNMP 構成タスクで使用するために、エンジン ID をテキストファイルに保存します。

5.2.6. STA SNMP v3 トラップ受信者の作成

STA サーバーを SNMP トラップの承認済みユーザーとして定義して、ライブラリが送信するトラップを定義するには、次の手順を使用します。

次の構成要件に注意してください。

- 重複したレコードを回避するために、複数のインスタンスで STA サーバーをトラップ受信者として定義しないでください。たとえば、STA サーバーに対して SNMP v3 と SNMP v2c の両方のトラップ受信者定義を作成しないでください。
- トラップレベル 13 (テストトラップ) と 14 (ヘルストラップ) は STA 2.0.x の新機能です。トラップレベル 4 は、古いライブラリファームウェアバージョンではサポートされない場合がありますが、トラップ受信者の作成時にはいつでも指定可能です。

ライブラリ CLI の使用 (SL150 を除くすべてのライブラリ)

1. SNMP v3 トラップ受信者を作成します。トラップレベルはコンマで区切ります。

```
snmp addTrapRecipient trapLevel 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
host STA_server_IP version v3 name recipient_name auth SHA authPass auth_password
priv DES privPass priv_password engineId library_engineID
```

ここでは:

- *STA_server_IP* は、STA サーバーの IP アドレスです。
- *recipient_name* は、95 ページの「SNMP v3 ユーザーの作成」で作成した SNMP ユーザー名です。
- *auth_password* および *priv_password* は、95 ページの「SNMP v3 ユーザーの作成」で作成した承認パスワードとプライバシパスワードです。
- *library_engineID* は、0x 接頭辞を含む、97 ページの「ライブラリ SNMP エンジン ID の取得 (SL150 を除くすべてのライブラリ)」で表示したライブラリエンジン ID です。

注:

SL3000 および SL8500 ライブラリの場合、*recipient_name*、*auth_password*、および *priv_password* を単一引用符で囲みます (例5.3「SL3000 または SL8500 での SNMP v3 トラップ受信者の作成」)。

例5.3 SL3000 または SL8500 での SNMP v3 トラップ受信者の作成

```
SL3000> snmp addTrapRecipient trapLevel
1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host 192.0.2.20 version v3
name 'STAsnmp' auth SHA authPass 'authpwd1' priv DES privPass 'privpwd1' engineId
0x00abcdef0000000000000000000000
```

例5.4 SL500 での SNMP v3 トラップ受信者の作成

```
SL500> snmp addTrapRecipient trapLevel
1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100 host 192.0.2.20 version v3
name STAsnmp auth SHA authPass authpwd1 priv DES privPass privpwd1 engineId
0x00abcdef0000000000000000000000
```

2. トラップ受信者を一覧表示して、受信者が正しく追加されていることを確認します。

```
snmp listTrapRecipients
```

SL コンソールの使用 (SL500 ライブラリのみ)

1. 「Tools」メニューから、「System Detail」を選択します。

2. ナビゲーションツリーで、「**Library**」を選択します。
3. 「**SNMP**」タブを選択してから、「**Add Trap Recipients**」タブを選択します。
4. 次のように「Trap Recipients」画面のフィールドに入力します。
 - *Host*: STA サーバーの IP アドレス。
 - 「*TrapLevel*」 - ライブラリが STA に送信するべきトラップレベルのコンマ区切りのリスト: 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100。
 - 「*Version*」 - 「v3」を選択します。
 - *TrapUserName*: 95 ページの「[SNMP v3 ユーザーの作成](#)」で作成した SNMP ユーザー名。
 - 「*Auth*」 - 「SHA」を選択します。
 - 「*AuthPass*」 - 95 ページの「[SNMP v3 ユーザーの作成](#)」で作成した承認パスワード。
 - 「*Priv*」 - 「DES」を選択します。
 - 「*PrivPass*」 - 95 ページの「[SNMP v3 ユーザーの作成](#)」で作成したプライバシパスワード。
 - 「*EngineID*」 - 97 ページの「[ライブラリ SNMP エンジン ID の取得 \(SL150 を除くすべてのライブラリ\)](#)」で表示したライブラリエンジン ID。0x 接頭辞は入力しないでください。
5. 「**Apply**」をクリックします。

SL150 ユーザーインタフェースの使用

1. ナビゲーションツリーで、「**SNMP**」を選択します。
2. 「SNMP Trap Recipients」セクションで、「**Add Trap Recipient**」を選択します。
3. 次のようにフィールドに入力します。
 - 「*Host Address*」 - STA サーバーの IP アドレス。
 - 「*Trap Level*」 - ライブラリが STA に送信するべきトラップレベルのコンマ区切りのリスト: 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100。
 - 「*Version*」 - 「v3」を選択します。
 - 「*Trap User Name*」 - 95 ページの「[SNMP v3 ユーザーの作成](#)」で作成した SNMP ユーザー名。
 - 「*Authentication Protocol*」 - 「SHA」を選択します。
 - 「*Authentication Passphrase*」 - 95 ページの「[SNMP v3 ユーザーの作成](#)」で作成した承認パスワード。

- 「*Privacy Protocol*」 - 「*DES*」を選択します。
 - 「*Privacy Passphrase*」 - 95 ページの「SNMP v3 ユーザーの作成」で作成したプライバシパスワード。
 - 「*Engine ID*」 - このフィールドは自動的に入力されます。値は変更しないでください。
4. 「**OK**」をクリックします。

STA でのライブラリ接続の構成

STA でサイトでのライブラリのモニターを行うには、ライブラリと STA サーバーのそれぞれでいくつかの構成アクティビティーを実行する必要があります。この章では、STA サーバーで実行されるアクティビティーについて説明します。

この章には次のセクションが含まれます。

- [STA 構成タスク](#)

6.1. STA 構成タスク

次に示すリストの順番どおりに手順を完了する必要があります。このプロセスを完了すると、STA はライブラリのモニタリングと分析の実行を開始できるようになります。

- [「STA へのログイン」](#)
- [「ライブラリとのSNMP 通信の検証」](#)
- [「STA の SNMP クライアント設定の構成」](#)
- [「ライブラリへのSNMP 接続の構成」](#)
- [「ライブラリへの SNMP 接続のテスト」](#)
- [「手動データ収集の実行」](#)

6.1.1. STA へのログイン

この手順を使用して、STA にログインし、このセクションのその他の手順を実行します。詳細な手順については、*STA ユーザーズガイド*を参照してください。

1. 使用しているコンピュータでサポートされている Web ブラウザを起動し、STA アプリケーションの URL を入力します。

`http(s)://STA_host_name:port_number/STA/`

ここでは:

- `host_name` は STA サーバーのホスト名です。
- `port_number` はインストール中に指定した STA ポート番号です。デフォルトの HTTP ポートは 7021 であり、デフォルトの HTTPS ポートは 7022 です。
- `STA` は大文字にする必要があります。

例:

```
https://staserver.example.com:7022/STA/
```

2. ログイン画面で STA 管理者ユーザー名とパスワードを入力します。

6.1.2. ライブラリ との SNMP 通信の検証

STA サーバーとライブラリ間の SNMP 接続が良好であることを確認するには、次の手順を使用します。

この手順では、UDP ポート 161 と 162 が STA サーバーとライブラリ間のすべてのネットワークノードで有効化されているかどうかを検証します。SNMP v3 トラップ受信者が正しく指定されているかどうかは検証できません。

モニター対象のライブラリごとに次の手順を実行します。冗長電子装置またはデュアル TCP/IP を使用する SL3000 または SL8500 ライブラリに対し、この手順を 2 回 (プライマリライブラリ IP アドレスとセカンダリ IP アドレスについて 1 回ずつ) 実行します。

注:

この手順は、STA サーバーのシステムコマンド行から実行されます。

1. STA サーバーでターミナルウィンドウを開き、システムルートユーザーとしてログインします。
2. SNMP v3 接続をテストします。指定する値は、ライブラリ内の対応する値と一致する必要があります。

```
# snmpget -v3 -u SNMP_user -a SHA -A auth_pwd -x DES -X priv_pwd -l  
authPriv library_IP_addr 1.3.6.1.4.1.1211.1.15.3.1.0
```

ここでは:

- `v3` は、SNMP v3 を示します。

- *SNMP_user* は、SNMP v3 のユーザー名です。
- *SHA* は、認証プロトコルを示します。
- *auth_pwd* は認証パスワードです。
- *DES* は、プライバシープロトコルです。
- *priv_pwd* はプライバシーパスワードです。
- *authPriv* は、コマンドでプライバシー実行が行われることを示します。
- *library_IP_addr* は、ライブラリのパブリックポートの IP アドレスです。
 - SL150 ライブラリの場合、これはネットワークポート 1 です。
 - SL500 ライブラリの場合、これはポート 1B です。
 - SL3000 および SL8500 ライブラリの場合、デュアル TCP/IP または冗長電子装置がライブラリでアクティブ化されているかどうかに応じて、テストするポートが複数存在する可能性があります。複数のポートがある場合、IP アドレスごとにこのコマンドを実行します。
- *1.3.6.1.4.1.1211.1.15.3.1.0* は、ライブラリの SNMP オブジェクト識別子 (OID) で、すべてのライブラリモデルに対して同一です。

コマンド出力にライブラリモデルが表示されると、テストは成功です。次にコマンドの例をいくつか挙げます。

例6.1 成功した snmpget コマンド

```
# snmpget -v3 -u STAsnmp -a SHA -A authpwd1 -x DES -X privpwd1 -l authPriv 192.0.2.20 1
.3.6.1.4.1.1211.1.15.3.1.0
SNMPv2-SMI::enterprises.1211.1.15.3.1.0 =STRING: "SL8500"
```

例6.2 失敗した snmpget コマンド - ネットワークタイムアウト

```
# snmpget -v3 -u STAsnmp -a SHA -A authpwd1 -x DES -X privpwd1 -l authPriv 192.0.2.20 1
.3.6.1.4.1.1211.1.15.3.1.0
Timeout: No Response from 192.0.2.20.
```

例6.3 失敗した snmpget コマンド - 無効なパスワード

```
# snmpget -v3 -u WrongUsr -a SHA -A authpwd1 -x DES -X WrongPwd -l authPriv 192.0.2.20
1.3.6.1.4.1.1211.1.15.3.1.0
snmpget: Authentication failure (incorrect password, community or key)
```

3. SNMP v2c 接続をテストします。

```
# snmpget -v2c -c public -l authPriv library_IP_addr
```

ここでは:

- `v2c` は、SNMP v2c を示します。
 - `public` は、コミュニティ文字列を示します。
 - `authPriv` は、コマンドでプライバシー実行が行われることを示します。
 - `library_IP_addr` は、ライブラリのパブリックポートの IP アドレスです。
4. どちらの SNMP 接続テストも成功している場合は、この手順を終了できます。いずれかのテストが失敗した場合は、次のステップに進み、必要に応じてネットワークの問題がある箇所のトラブルシューティングをします。
 5. STA サーバーからライブラリへのパケットルーティングを確認します。

```
# traceroute -I library_IP_addr
```

ここでは:

- `-I` (大文字の "I") は、ユーザーデータグラムプロトコル (UDP) のデータグラムではなく、インターネットコントロールメッセージプロトコル (ICMP) のエコーリクエストパケットを使用することを示します。
- `library_IP_addr` は、ライブラリのパブリックポートの IP アドレスです。

出力に、ホップ数と各ホップに到達するための往復時間が示されます。往復時間 (コマンド出力の最後の行) は、1 秒未満であるべきです。これを満たさない場合、ネットワークのパフォーマンスをネットワーク管理者と確認してください。

6. STA サーバーとライブラリ間で送信される TCP/IP パケットをモニターします。

```
# tcpdump -v host library_IP_addr > /var/tmp/file_name &
```

ここでは:

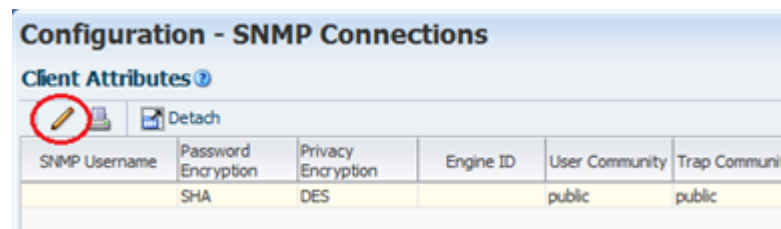
- `-v` は詳細出力を示します。
- `host` は指定したホスト (この場合、ライブラリ) で送受信されるパケットのみを収集することを示しています。
- `library_IP_addr` は、ライブラリのパブリックポートの IP アドレスです。
- `file_name` は出力の保存先のファイル名です。

6.1.3. STA の SNMP クライアント設定の構成

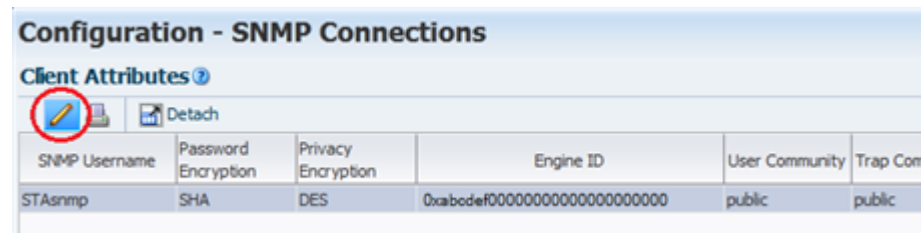
STA の SNMP クライアント設定を追加または修正するには、次の手順を使用します。1 つ以上のライブラリから SNMP データを受信するように STA を構成するには、次の設定を使用します。

SNMP クライアントは、ユーザーサイトの STA インスタンスごとに 1 つだけエントリがあります。

1. 「**Setup & Administration**」タブから、「**Configuration**」を選択し、「**SNMP Connection**」を選択します。
2. 次のように進めます。
 - はじめてクライアント設定を構成するには、「**Client Attributes**」表で空の表行を選択し、「**Edit**」をクリックします。



- 既存のクライアント設定を変更するには、「**Client Attributes**」表のエントリを選択し、「**Edit**」をクリックします。



「**Define SNMP Client Settings**」ダイアログボックスが表示されます。これが新しい構成の場合、フィールドは空白です。

3. 次の手順でダイアログボックスの操作を完了します。指定する値は、ライブラリ内の対応する値と一致する必要があります。

注:

STA が SNMP v2c 通信のために構成されたライブラリをモニタリングするだけの場合でも、SNMP v3 に該当するものを含め、すべてのフィールドに入力する必要があります。フィールドを空白のままにすることはできません。

- STA SNMP 接続ユーザー名 (Auth)—SNMP v3 ユーザー名を入力します。
- STA SNMP 接続 (承認) パスワードを入力— 接続承認パスワードを入力します。
- プライバシ暗号化パスワードを入力 (プライバシ) —プライバシ暗号化パスワードを入力します。
- ユーザーコミュニティ—このフィールドは、ライブラリとのSNMP ハンドシェイクに必要です。または、SNMP v2c を使用している場合は、ライブラリとの STA 通信のために必要です。ライブラリに指定されている通信名を入力します。デフォルト値は *public* です。
- トラップコミュニティ—ライブラリとの通信に SNMP v2c が使用されている場合にのみ使用します。SNMP v3 を使用している場合は、この値をデフォルト (*public*) に設定されたまましておきます。SNMP v2c を使用している場合、ライブラリに指定されているトラップコミュニティ名を入力します。

Define SNMP Client Settings

STA SNMP Connection Username (Auth) * sta1

Enter STA SNMP Connection Password (Auth) *

Verify STA SNMP Connection Password (Auth) *

Connection Password Encryption (Auth) SHA

Enter Privacy Encryption Password (Privacy) *

Verify Privacy Encryption Password (Privacy) *

Privacy Encryption Protocol (Privacy) DES

STA Engine ID 0x8000002a050000014817ec1dc1

Trap Levels 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100

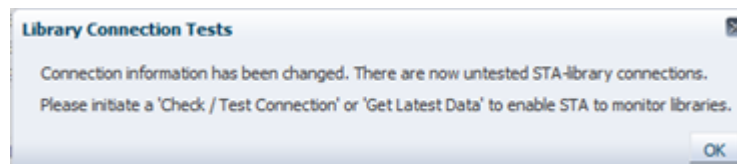
User Community * public

Trap Community * public

Save Cancel

4. 「保存」をクリックします。

構成レコードが更新され、メッセージボックスが表示されます。これは、ライブラリとの SNMP 通信ハンドシェイクを確立または再確立するためのライブラリ接続テストを実行すべきであることを示します。



5. 「OK」をクリックすると、そのメッセージが閉じます。

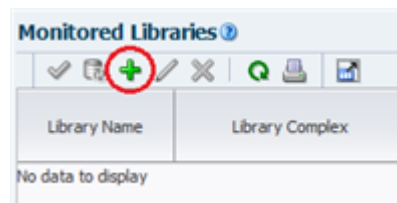
6.1.4. ライブラリへのSNMP 接続の構成

SNMP 接続を構成するか、または既存の接続を変更するには、STA でモニターするライブラリごとに次の手順を使用します。既存の接続の場合は、ライブラリ IP アドレスの変更など、モニター対象ライブラリの SNMP 構成の設定に何らかの変更がある場合、この手順を実行する必要があります。

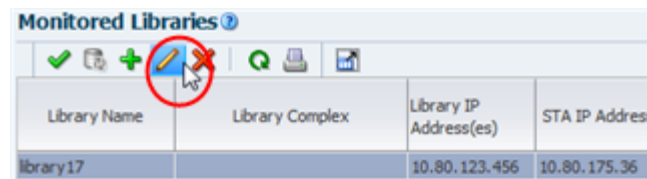
注:

複数のライブラリ接続を一度に構成している場合は、ライブラリの障害を最小化するために、すべてのライブラリについてこの手順を完了してから SNMP 接続をテストします。

1. 「**Setup & Administration**」タブから、「**Configuration**」を選択し、「**SNMP Connection**」を選択します。
2. 次のように進めます。
 - はじめてライブラリへの接続を構成するには、「**Monitored Libraries**」ツールバーで「**Add**」をクリックします。



- 既存のライブラリ接続を変更するには、「**Monitored Libraries**」表のライブラリを選択し、「**Edit**」をクリックします。



「**Define Library Connection Details**」ダイアログボックスが表示されます。これが新しいライブラリ接続の場合、フィールドは空白です。

3. 次の手順でダイアログボックスの操作を完了します。指定する値は、ライブラリ内の対応する値と一致する必要があります。
 - *Library Name*— STA ユーザーインターフェース画面全体でライブラリを識別する名前を入力します (たとえば、ライブラリホスト名)。
 - *Library Primary IP Address*— ライブラリのプライマリパブリックポートの IP アドレスを入力します。別のモニター対象ライブラリの IP アドレスを指定することはできません。

- **ライブラリセカンダリ IP アドレス** — デュアル TCP/IP または冗長電子装置を使用する SL3000 および SL8500 ライブラリにのみ適用します。ライブラリ内でセカンダリパブリックポートの IP アドレスを指定します。別のモニター対象ライブラリの IP アドレスを指定することはできません。その他すべてのライブラリについては、SL500 および SL150 の全ライブラリを含めフィールドを空白のままにします。
- **STA IP アドレス** — STA サーバーの IP アドレスを選択します。
- **ライブラリエンジン ID** — このフィールドは変更しないでください。これは、STA とライブラリ間の初期接続の確立時に自動的に指定される、ライブラリの一意の SNMP エンジン ID です。これは、新規接続の場合は空白です。
- **日次データの自動リフレッシュ** — STA でライブラリからの最新構成データ収集を実行する時間を指定します。データは、その時間に 24 時間ごとに自動的に収集されます。通常、ライブラリの使用率が低くなる時間を選択するべきです。デフォルトは 00:00 (深夜 12:00) です。24 時間制を使用してください。

注意:

このフィールドを空白のままにすると、スケジュールされた自動ライブラリデータ収集は無効になります。この場合、STA ライブラリ構成データがライブラリと同期しなくなります。

- **ライブラリのタイムゾーン** — ライブラリのローカルタイムゾーンを選択します。

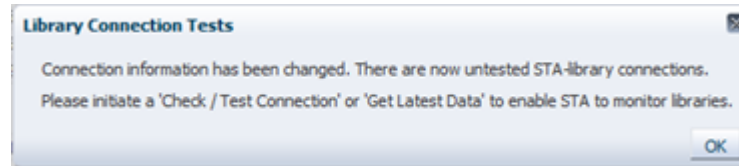
The screenshot shows a dialog box titled "Define Library Connection Details". It contains the following fields and values:

- Library Complex: SL8500_1
- Library Name: library17
- Library Primary IP Address: 10.80.123.456
- Library Secondary IP Address: (empty)
- STA IP Address: 10.80.175.36
- Library Engine ID: 0x80001f880436303030313030323237
- Automated Daily Data Refresh: 00:00
- Library Time Zone: UTC

Buttons for "Save" and "Cancel" are located at the bottom right of the dialog.

4. 「保存」をクリックします。

構成レコードが更新され、メッセージボックスが表示されます。これは、ライブラリとの SNMP 通信ハンドシェイクを確立または再確立するためのライブラリ接続テストを実行すべきであることを示します。



5. 「OK」をクリックすると、そのメッセージが閉じます。

既存のライブラリ接続を変更すると、「Monitored Libraries」表の「Library Engine ID」フィールドがクリアされ、SNMP 接続が切れたことを示します。

6.1.5. ライブラリへの SNMP 接続のテスト

STA とライブラリ間の SNMP 接続をテストして、通信ハンドシェイクを確立または再確立するには、次の手順を使用します。接続の切断やSNMPトラップの損失を回避するには、モニター対象のライブラリごとに、ライブラリまたは STA クライアントの SNMP 構成の設定を追加したり変更したりするときは常に、次の手順を実行することをお勧めします。

- 1 回につき 1 つのライブラリ接続のみテストできます。

注:

接続テストによって受信 SNMP パケットが一瞬失われる可能性があるため、この手順は必要などきのみ行うようにしてください。

注:

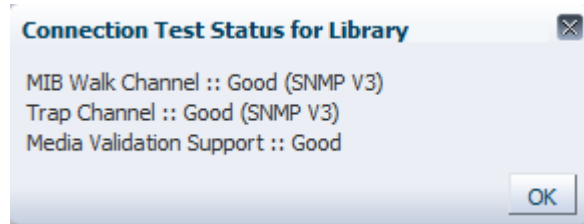
この手順を実行する前に、ライブラリが操作可能であることを確認する場合があります。

1. 「Setup & Administration」タブで、「Configuration」を選択して、「SNMP 接続」を選択します。
2. 「Monitored Libraries」表でライブラリを選択して、「Check / Test Connection」をクリックします。

A screenshot of the "Monitored Libraries" table in a software interface. The table has columns: Library Name, Library Complex, Library IP Address(es), STA IP Address, Library Engine ID, Recent SNMP Trap Communication Status, Automated Daily Data Refresh Time, Library Time Zone, and Last Suc Connect. The table contains several rows, with the row for "Crimson14" highlighted in red. A red circle highlights the "Check / Test Connection" icon in the top left corner of the table area.

Library Name	Library Complex	Library IP Address(es)	STA IP Address	Library Engine ID	Recent SNMP Trap Communication Status	Automated Daily Data Refresh Time	Library Time Zone	Last Suc Connect
Crimson11	SL3000_571000200060	10.80.104.51	10.80.175.36	0x80001f880431303030323030303630	GOOD	00:00:00	UTC	2014-05
Crimson14	SL3000_571000000001	10.80.104.54	10.80.175.36		NO RECENT TRAPS	00:00:00	UTC	2014-05
Crimson13	SL3000_571000200007	10.80.87.13	10.80.175.36	0x80001f88043537313030303230303030	GOOD	00:00:00	UTC	2014-05
elb18	SL8500_2	10.80.104.98	10.80.175.36	0x80001f880436303030313030343337	GOOD	00:15:00	US/Mountain	2014-05

「Connection Test Status」メッセージボックスが表示され、MIB Walk Channel、トラップチャンネル、および Media Validation Support テストの結果が表示されます。



- 「OK」をクリックしてメッセージボックスを閉じます。

「Monitored Libraries」表は、テスト結果に基づいて更新されています。

Library Name	Library Complex	Library IP Address(es)	STA IP Address	Library Engine ID	Recent SNMP Trap Communication Status	Automated Daily Data Refresh Time	Library Time Zone	Last Suc Connect
crimson14	SL3000_571000000001	10.80.104.54	10.80.175.36	0x80001f8804313030303030303031	GOOD	00:00:00	UTC	2014-05-05
crimson19	SL3000_571000200007	10.80.87.13	10.80.175.36	0x80001f8804353731303030323030303030	GOOD	00:00:00	UTC	2014-05-05
elb18	SL8500_2	10.80.104.98	10.80.175.36	0x80001f880436303030313030343337	GOOD	00:15:00	US/Mountain	2014-05-05

- 「Library Complex」フィールドが空白の場合は、手動データ収集の実行後に供給されます。
- Library Engine ID は、ライブラリの一意的な SNMP エンジン ID を示します。
- Last Connection Attempt は、接続テストが開始された日時を示します。
- Last Successful Connection は、テストが成功した場合、テストが完了した日時を示します。
- Last Connection Status は、テストの結果を示します。テストが失敗した場合、STA は情報を「Last Connection Failure Detail」フィールドに提供します。(値全体を表示するには、列幅の拡大が必要になることがあります。)

注:

タイムアウトが原因でテストが失敗する場合は、ライブラリのアクティビティが少ない期間にこの手順を繰り返してください。テストが完了したら、タイムスタンプを比較して、ライブラリが最新情報を提供しているかどうか検証できます。

6.1.6. 手動データ収集の実行

この手順を使用してライブラリの手動データ収集を開始し、最新のライブラリ構成データを取得します。この手順が正常に完了すると、STA はライブラリのモニタリングとデータ分析の実行を開始します。

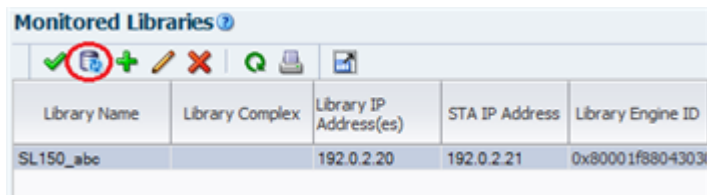
STA は、スケジュールされた時間に24時間ごとに自動的にデータ収集を実行しますが、ライブラリまたは STA クライアントの SNMP 構成設定を追加または変更する場合は必ず、モニター対象のライブラリごとに手動データ収集を実行する必要があります。

データ収集には、ライブラリサイズに応じて数分から 1 時間かかる場合があります。

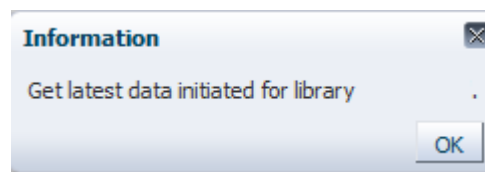
注:

複数のデータ収集を同時に実行できますが、1 回につき 1 つ開始してください。この手順を必要なだけ繰り返し、そのつど、別のライブラリを選択します。

1. 「**Setup & Administration**」タブで、「**Configuration**」を選択して、「**SNMP 接続**」を選択します。
2. 「**Monitored Libraries**」表でライブラリを選択して、「**Get latest data**」をクリックします。1 回につき 1 つのライブラリのみ選択できます。



「確認」メッセージボックスが表示されます。



3. 「**OK**」をクリックしてメッセージボックスを閉じます。

データ収集が開始され、「**Monitored Libraries**」表で結果が更新されます。

- *Library Complex* は、ライブラリコンプレックス ID を示します。
- *Library Engine ID* は、ライブラリの一意的 SNMP エンジン ID を示します。
- *Last Connection Attempt* は、データ収集が開始された日時を示します。
- *Last Successful Connection* は、データ収集が成功した場合、テストが完了した日時を示します。
- *Last Connection Status* が次のように更新されます。
 - *IN PROGRESS*: データの収集プロセスが進行中です。
 - *SUCCESS*: データの収集に成功しました。STA は、ライブラリから交換データの受信を開始します。
 - *FAILED*: データ収集は成功しませんでした。可能な場合、STA によって「*Last Connection Failure Detail*」フィールドに情報が提供されます。(値全体を表示するには、列幅の拡大が必要になることがあります。)

注:

ステータスは 4 分ごとに更新され、デフォルトの画面リフレッシュ間隔は 480 秒です。ただし、いつでも「**Refresh Table**」ボタンをクリックして、表のリフレッシュを強制的に行うことができます。



- 「Recent SNMP Trap Communication Status」が断続的に、「MISSED HEARTBEAT」と示されることがあります。これは正常な状態です。

STA サービスの構成

STA バックアップサービスユーティリティと STA リソースモニターサービスユーティリティを構成するには、次の手順を使用します。

この章には次のセクションが含まれます。

- [STA サービスの概要](#)
- [STA サービスの構成タスク](#)

7.1. STA サービスの概要

- STA データベースバックアップサービス — STA バックアップサービスの構成にはその管理ユーティリティ `staservadm` を使用します。このユーティリティのコマンドオプションの完全なリストを表示するには、`staservadm -h` と入力します。詳細は、『[STA 管理ガイド](#)』を参照してください。
- 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の構成にはその管理ユーティリティ `staresmonadm` を使用します。このユーティリティのコマンドオプションの完全なリストを表示するには、コマンド行で `staresmonadm -h` と入力します。詳細は、『[STA 管理ガイド](#)』を参照してください。

これらのサービスユーティリティは、`/Oracle_storage_home/StorageTek_Tape_Analytics/common/bin` ディレクトリにあります。Oracle ストレージホームの詳細は、『[STA インストーラで使用するユーザー、グループ、場所](#)』を参照してください。

7.2. STA サービスの構成タスク

一般的なタスク

- 「[システムパスの更新 \(オプション\)](#)」
- 「[STA サービスデーモンの再起動 \(オプション\)](#)」
- 「[ライブラリ接続の確認](#)」

STA データベースバックアップの構成タスク

- 「[STA データベースバックアップユーティリティプリファレンスの確認](#)」

- 「リモートデータベースバックアップサーバーの構成」
- 「STA データベースバックアップサービスの構成」

STA リソースモニターの構成タスク

- 「STA リソースモニターユーティリティープリファレンスの確認」
- 「STA リソースモニターの構成」

7.2.1. システムパスの更新 (オプション)

STA bin ディレクトリがシステムの root ユーザーの *PATH* 変数に確実に含まれるようにするには、次の手順を使用します。bin ディレクトリには、STA サービスユーティリティーである *staservadm* と *staresmonadm* が含まれています。

- 現在の STA サーバーで端末セッションを開き、システムの root ユーザーとしてログインします。
- テキストエディタを使用してユーザープロファイルを開きます。例:

```
# vi /root/.bash_profile
```

- STA bin ディレクトリを *PATH* 定義に追加します。たとえば、次の行をファイルに追加します。

```
PATH=$PATH:Oracle_storage_home/StorageTek_Tape_Analytics/common/bin
```

ここで *Oracle_storage_home* は、STA のインストール中に指定された Oracle ストレージホームの場所です。

- ファイルを保存して終了します。
- ログアウトしてから、再度システムの root ユーザーとしてログインします。
- PATH* 変数が正しく更新されていることを確認します。

```
# echo $PATH
```

```
/usr/lib64/qt-3.3/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin:/Oracle/StorageTek_Tape_Analytics/common/bin
```

7.2.2. STA サービスデーモンの再起動 (オプション)

STA サービスデーモン *staservd* を再起動するには、次の手順を使用します。

STA バックアップサービスまたは STA リソースモニターサービスの構成設定を変更して、新しい設定を即時に有効にする場合に、この手順が役に立ちます。この手順を使用しない場合、サービスがスリープ間隔から復帰して新しい設定を処理するとすぐに、新しい設定が有効になります。

1. STA サービスデーモンを停止します。

```
# STA stop staservd
```

2. STA サービスデーモンを起動します。

```
# STA start staservd
```

3. デーモンのステータスを表示して、実行中であることを確認します。

```
# STA status staservd
```

7.2.3. ライブラリ接続の確認

サービスの構成が終了したら、構成済みのすべてのライブラリが「最新データの取得」リクエストを完了したことを確認します（「Last Connection Status」には「*SUCCESS*」と示され、STA はライブラリから交換データを受信しているはずです）。詳細は、『*STA ユーザーズガイド*』を参照してください。

7.2.4. STA データベースバックアップユーティリティープリファレンスの確認

使用可能なプリファレンス設定の説明および設定の定義については、[表7.1「STA バックアップサービス管理ユーティリティー \(staservadm\) の属性」](#)を確認してください。

表7.1 STA バックアップサービス管理ユーティリティー (staservadm) の属性

オプション	属性	説明	デフォルト値	使用する値
-S、--scp -F、--ftp	File transfer type	バックアップファイルを STA サーバーからバックアップホストにコピーするために使用されるファイル転送の方法。オプションは、「SCP」(推奨) または「FTP」です。	SCP	
-T、--time	Full backup dump time	STA がデータベース全体のバックアップダンプを実行する時間。ダンプは、この時間	00:00	

オプション	属性	説明	デフォルト	使用する値
		前後に 24 時間ごとに自動的に実行されま す。実際の時間は、この時間よりあとの「ス リープ間隔」秒内です。形式は、24 時間制の <i>hh:mm</i> です。		
<code>-i, --int</code>	Sleep interval	STA サービスデーモンが新しい増分バック アップファイルを調べるまでに待機する秒 数。	300	
<code>-s, --server</code>	Backup host name	STA サーバーがバックアップファイルをコ ピーする先となるサーバーホストの IPv4 ア ドレス、IPv6 アドレス、または完全修飾 DNS ホスト名。	なし	
<code>-u, --usr</code>	Backup user ID	バックアップホストへの SCP ファイルの転送 の実行が許可されているシステムユーザー ID。	なし	
<code>-p, --pwd</code>	Backup password	バックアップユーザーに割り当てられている パスワード。	なし	
<code>-d, --dir</code>	Backup directory	バックアップファイルがコピーされるバック アップホストにあるディレクトリ。	なし	
<code>-U, --dbusr</code>	Database username	<i>mysqldump</i> コマンドの実行が許可されて いるデータベースユーザー名。STA データ ベースの DBA アカウントユーザー名を指定 する必要があります。	なし	
<code>-P, --dbpwd</code>	Database password	データベースユーザー名のパスワード。	なし	

7.2.5. リモートデータベースバックアップサーバーの構成

STA データベースバックアップサービスによって生成された圧縮済みバックアップファイルを受信するようにリモートバックアップサーバー (または同等のもの) を構成するには、次の手順を使用します。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ます。

必要な領域は不定です。サイズは、保持するコピーの数に応じて、STA データベースのローカルバックアップに使用されるサイズの倍数であるべきです。バックアップサーバーストレージは、ミラー化またはストライプ化されているべきです。

1. バックアップサーバーで、システムの root ユーザーとしてログインします。
2. STA バックアップユーザーの新しいグループを作成します。例:

```
# groupadd -g 54321 stabckgr
```

この例では、グループ ID は「stabckgr」で、数値 GID を指定するために `-g` オプションが使用されています。

3. STA バックアップユーザーを作成します。例:

```
# adduser stabck -c "STA database backup user" -m -d /home/stabck -g stabckgr -s /bin/bash -u 98765
```

この例では、ユーザー ID は「stabck」で、次のオプションが使用されています。

- `-c` – コメント。
- `-m` – ユーザーのホームディレクトリを作成します。
- `-d` – ホームディレクトリの絶対パス。
- `-g` – ユーザーを指定のグループに割り当てます。
- `-s` – 指定のログインシェルをユーザーに割り当てます。
- `-u` – 指定の数値 UID をユーザーに割り当てます。

4. STA バックアップユーザーにパスワードを割り当てます。例:

```
# passwd stabck
Changing password for user stabck.
New UNIX password: bckpwd1
Retype new UNIX password: bckpwd1
passwd: all authentication tokens updated successfully.
```

5. STA バックアップがコピーされるディレクトリを作成します。例:

```
# cd /home/stabck
# pwd
/home/stabck
# mkdir -p STAbackups
# ls
STAbackups
```

この例では、「STABackups」ディレクトリは STA バックアップユーザーのホームディレクトリに作成され、必要に応じて親ディレクトリを作成するために `-p` オプションが使用されています。

- すべての情報が正しく入力されていることを確認するために、ユーザー属性を表示します。例:

```
# cat /etc/passwd |grep sta
stabck:x:98765:54321:STA database backup user:/home/stabck:/bin/bash
```

- ディレクトリの排他的所有権とアクセス権を STA バックアップユーザーとグループに割り当てます。例:

```
# chown -R stabck:stabckgr STABackups
# chmod -R 700 STABackups
# chmod 755 /home/stabck
```

この例では、再帰的に属性をディレクトリとそのファイルに割り当てるために `-R` オプションが使用されています。

- すべての情報が正しく入力されていることを確認するために、ディレクトリを一覧表示します。例:

```
# ls -la |grep STA
drw----- 2 stabck stabckgr 4096 Oct 19 14:20 STABackups
```

7.2.6. STA データベースバックアップサービスの構成

STA データベースバックアップサービスを構成するには、次の手順を使用します。バックアップファイルがコピーされるディレクトリを指定できます。Oracle では、このディレクトリをリモートバックアップサーバーに置くことをお勧めします。

サービスが現在のスリープ間隔から復帰して新しい設定を処理するか、ユーザーが STA サービスデーモンを手動で再起動する (**「STA サービスデーモンの再起動 (オプション)」**) とすぐに、構成設定が有効になります。

- STA サーバーで、システムの root ユーザーとしてログインします。
- `staservadm -q` コマンドを使用して現在の STA バックアップサービス設定を表示します。

この例は、サービスがまだ構成されていないため、バックアップを実行していないことを示しています。

```
# ./staservadm -Q
Contacting daemon...connected.
Querying Preferences.
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 []
```

3. 表7.1「[STA バックアップサービス管理ユーティリティ \(staservadm\) の属性](#)」を参照として使用して、`staservadm` コマンドで属性値を設定します。

属性を別のコマンドで送信することも、1つのコマンドに結合することもできます。例:

```
# ./staservadm -S -T 11:00 -i 350 -s stabaksvr -u stabck -p bckpwd1 -d /home/
stabck/STAbckups -U sta_dba -P password1
```

このユーティリティは、コマンドに含まれているそれぞれの値を設定してから、現在のすべての設定を表示します。例:

```
Contacting daemon...connected.
Setting File Transfer Type... SCP
Setting Sleep Interval..... 350
Setting Backup Hostname..... stabaksvr
Setting Backup Username..... stabck
Setting Backup Password..... *****
Setting Backup Directory..... /home/stabck/STAbckups
```

```

Setting Full Backup Time..... 11:00
Setting Database Username.... sta_dba
Setting Database Password.... *****
Done.

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 [sta_dba]
Database Password    -P [*****]
    
```

4. コマンド出力を調べて、値が正しく設定されていることを確認します。

7.2.7. STA リソースモニターユーティリティープリファレンスの確認

表7.2「[STA リソースモニター \(staresmonadm\) の属性](#)」のオプションの説明を確認して、設定を定義します。デフォルト値「-1」は、属性が構成されていないことを示しています。

表7.2 STA リソースモニター (staresmonadm) の属性

オプション	属性	説明	デフォルト値	使用する値
-T, --time	Daily report time	STA が標準の日次レポートを送信する時間。レポートは、この時間前後に 24 時間ごとに自動的に送信されます。実際の時間は、この時間よりあとの「スリープ間隔」秒内です。形式は、24 時間制の <i>hh:mm</i> です。	00:00	
-i, interval	Sleep interval	STA リソースモニターがスキャンの間に待機する秒数。	300	
-n, --nag	Nag mode	最高水位標に達した場合に STA がアラートを出す頻度を示します。「on」に設定した場合、システムがスキャンされる	Off	

オプション	属性	説明	デフォルト値	使用する値
		たびに STA はアラート電子メールを送信します。「off」に設定した場合、アラートは単に標準の日次レポートに記録されます。		
<code>-U</code> 、 <code>--dbusr</code>	Database username	「information_schema」表および MySQL なしサーバーの内部システムグローバル変数に対して問合せを実行することが許可されているデータベースユーザー名。STA データベースの DBA アカウントユーザー名または STA データベースのルートアカウントユーザー名 (<i>root</i>) のいずれかを指定する必要があります。		
<code>-P</code> 、 <code>--dbpwd</code>	Database password	データベースユーザー名に割り当てられているパスワード。		
<code>-t</code> 、 <code>--tblsphwm</code>	Database tablespace HWM	使用可能な最大の割合として入力する、データベース表領域の最高水位標。	-1	
<code>-b</code> 、 <code>--backvolhwm</code>	Local backup HWM	使用可能な最大の割合として入力する、STA データベースローカルバックアップボリューム (<i>/sta_db_backup</i>) の最高水位標。	-1	
<code>-d</code> 、 <code>--dbvolhwm</code>	Database disk volume HWM	使用可能な最大の割合として入力する、STA データベースボリューム (<i>/sta_db/mysql</i>) の最高水位標。	-1	
<code>-l</code> 、 <code>--logvolhwm</code>	Logging disk volume HWM	使用可能な最大の割合として入力する、STA データベースログ (<i>/STA_logs/db</i>) の最高水位標。	-1	
<code>-z</code> 、 <code>--rootvolhwm</code>	Root volume HWM	使用可能な最大の割合として入力する、ルートボリューム (<i>/</i>) の最高水位標。	-1	
<code>-x</code> 、 <code>--tmpvolhwm</code>	Tmp volume HWM	使用可能な最大の割合として入力する、一時ディレクトリボリューム (<i>/tmp</i>) の最高水位標。	-1	

オプション	属性	説明	デフォルト値	使用する値
<code>-m</code> , <code>--memhwm</code>	Physical memory (RAM) HWM	使用可能な最大の割合として入力する、合計システムメモリー (仮想メモリーを除く) の最高水位標。	<code>-1</code>	
<code>-f</code> , <code>--from</code>	Email from	標準の日次レポート電子メールの「From」フィールドに表示される名前または電子メールアドレス。	<code>StaResMon@localhost</code>	
<code>-r</code> , <code>--recips</code>	Email recipients	コロン区切りのリストとして入力する、受信者の電子メールアドレス。	なし	
<code>-s</code> , <code>--subject</code>	Email subject	標準の日次レポート電子メールの「Subject」フィールドに表示される、最大 128 文字のエントリ。空白が含まれる場合は引用符で囲みます。電子メールの送信時に、 <code>yyyy-mm-dd hh:mm:ss</code> 形式のタイムスタンプがエントリに追加されます。	<code>STA Resource Monitor Report</code>	
<code>-o</code> , <code>--outfile</code>	Output data file	コンマ区切り (CSV) の出力データファイルの絶対パス。	<code>/STA_logs/db/staresmon.csv</code>	例: <code>/var/log/tbi/db/staresmon.csv</code>

7.2.8. STA リソースモニターの構成

STA リソースモニターサービスを構成するには、次の手順を使用します。サービスが現在のスリープ間隔から復帰して新しい設定を処理するか、ユーザーが STA サービスデーモンを手動で再起動する ([「STA サービスデーモンの再起動 \(オプション\)」](#)) とすぐに、構成設定が有効になります。

1. STA サーバーで、システムの root ユーザーとしてログインします。
2. `staresmonadm -q` コマンドを使用して現在の STA リソースモニター設定を表示します。

この例は、サービスがまだ構成されていないため、スキャンを実行していないことを示しています。

```
# ./staresmonadm -Q
Contacting daemon...connected.
Querying Preferences.
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]
```

3. [表7.2「STA リソースモニター \(staresmonadm\) の属性」](#)を参照として使用して、*staresmonadm* コマンドで属性値を設定します。

属性を別のコマンドで送信することも、1つのコマンドに結合することもできます。例:

```
# ./staresmonadm -T 13:00 -i 600 -n on -U sta_dba -P password1 -t 65 -b 65 -d 65 -l 65 -z 70 -x 80 -m 75 -r john.doe@company.com
```

このユーティリティーは、コマンドに含まれているそれぞれの値を設定してから、現在のすべての設定を表示します。例:

```
Contacting daemon...connected.
Setting DB Tablespace HWM..... 65
Setting DB Disk Volume HWM.... 65
```

```

Setting Logging Volume HWM.... 65
Setting Backup Volume HWM..... 65
Setting Root Volume HWM..... 70
Setting Temp Volume HWM..... 80
Setting System Memory HWM..... 75
Setting 'To:' addresses..... john.doe@company.com
Setting Send Time..... 13:00
Setting Sleep Interval..... 600
Setting Alert Nag Mode..... ON
Setting DB Username..... sta_dba
Setting DB Password..... *****
Done.

```

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]

```

4. コマンド出力を調べて、値が正しく設定されていることを確認します。

STA 2.1.0 へのアップグレード

この章では、以前にリリースされたバージョンの STA から STA 2.1.0 にアップグレードする手順を説明します。次のセクションがあります。

- [アップグレードプロセスの概要](#)
- [有効な STA 2.1.0 のアップグレードパス](#)
- [アップグレード方法](#)
- [STA 2.1.0 の環境の変更](#)
- [アップグレード準備タスク](#)
- [アップグレードタスク](#)

STA をはじめてインストールする場合には、新しい基本インストールを実行する必要があります。手順については、[3章「STA のインストール」](#)を参照してください。

[付録C「インストールおよびアップグレードのワークシート」](#)に、アップグレードアクティビティの整理および設定の記録に使用できるワークシートがあります。

8.1. アップグレードプロセスの概要

アップグレード中、既存の STA データが現在の STA バージョンから新しいものに変換されます。これらの変換が完了するまでは、STA データベースは新しいバージョンの STA で有効になりません。アップグレード後に、STA は、新しい STA スキーマと分析ルールに従って新しいデータを処理します。履歴データは再処理されません。

アップグレードを開始する前に、この章のすべての手順を読み、必ずプロセス全体に十分な時間を配分してください。アップグレード準備タスクの一部において、ネットワーク管理などの、サイトでのほかのグループとの調整が必要となる場合があります。アップグレード自体をできるかぎり少ない時間で終了するには、事前にすべての準備タスクを完了させておく必要があります。

プロセス自体のアップグレードを開始すると、STA を実行できないため、モニター対象のライブラリからの交換情報を受けなくなります。また、新しいバージョンの STA は、アップグレード

のすべての手順を完了し、各モニター対象ライブラリへの SNMP 接続をテストするまでは、ライブラリからの情報の受け取りを開始しません。

注:

一部のアップグレード手順には時間の推定が含まれていますが、これは単に計画の目的のために用意されているものです。サーバーの機能 (CPU 数、CPU 速度、ディスク速度、メモリー、および使用可能なスワップ領域など) に応じて、実際の時間は異なる場合があります。

8.2. 有効な STA 2.1.0 のアップグレードパス

次のリリース済みの STA バージョンのいずれかから STA 2.1.0 にアップグレードできます。

- STA 2.0.x:
 - STA 2.0.0.83
 - STA 2.0.1.4
- STA 1.0.x:
 - STA 1.0.0.99
 - STA 1.0.1.133
 - STA 1.0.2.24

注:

STA 1.0.x からアップグレードする場合、STA 2.1.0 をインストールする前に新しいバージョンの Linux もインストールする必要があります。詳細は、『STA 要件ガイド』を参照してください。

8.3. アップグレード方法

目的および使用可能なリソースに応じて、1 台または 2 台のサーバーを使用して STA のアップグレードを実行できます。2 つの方法のアップグレードタスクは大部分が同じですが、異なる順序でタスクが実行されます。2 つの方法は次のセクションで説明します。

- [「1 台のサーバーのアップグレード方法」](#)
- [「2 台のサーバーのアップグレード方法」](#)

8.3.1. 1 台のサーバーのアップグレード方法

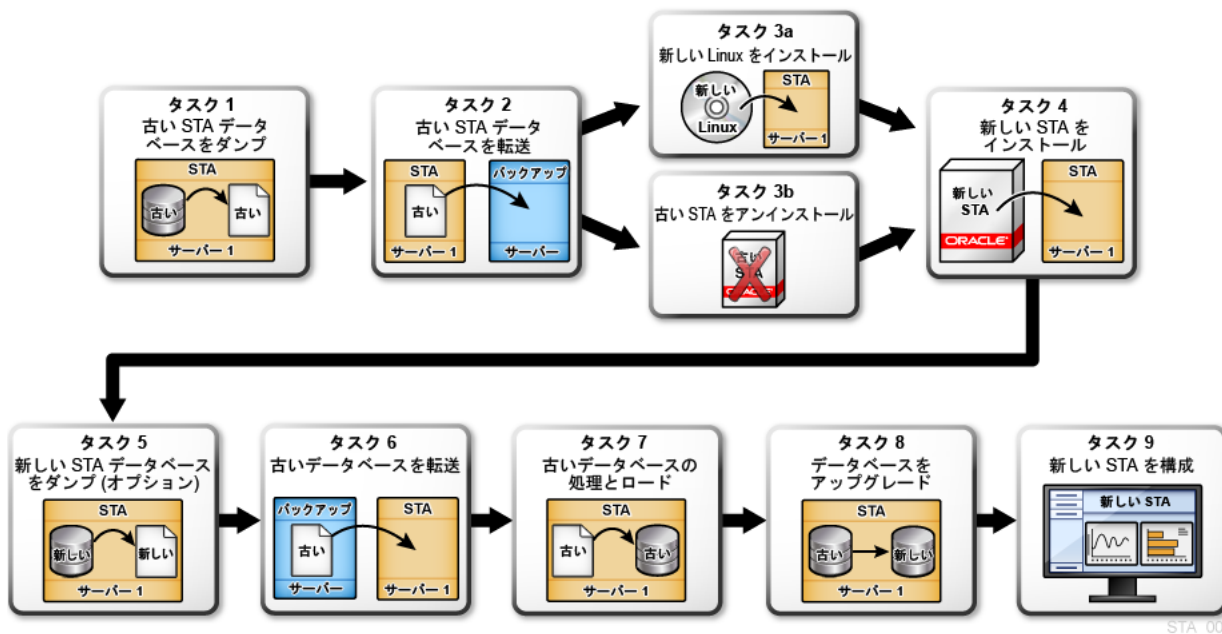
1 台のサーバーの方法を使用する場合、新しいバージョンをインストールして同じサーバーのデータベースをアップグレードする前に、STA をアンインストールする必要があります。この処理の実行中は、STA はライブラリをモニターしていません。

この方法には、アップグレードにおいて追加の専用サーバーが不要という利点があります。STA 2.0.x からアップグレードする場合、新しいバージョンの Linux をインストールする必要がないため、この方法はニーズを十分満たしている可能性があります。

図8.1「1 台のサーバーのアップグレードタスクの概要」に、1 台のサーバーの方法を示します。タスク 1 からタスク 9 まで連続した順に実行します。まとめると次のようになります。

- 現在のデータベースをダンプし、保護のためそれをバックアップサーバーに転送します (タスク 1 およびタスク 2)。
- STA の現在のバージョンに応じて、Linux 6.x (タスク 3a) をインストールするか、STA 2.0.x をアンインストール (タスク 3b) します。
- STA 2.1.0 をインストールし、予防策として新しいデータベースをダンプします (タスク 4 およびタスク 5)。
- バックアップサーバーから古いデータベースのダンプを転送し、それを新しい STA のバージョンにロードおよびアップグレードします (タスク 6 からタスク 8)。
- モニター対象ライブラリへの接続を再確立し、必要な手動の構成タスクを実行します (タスク 9)。STA 2.1.0 をインストールする前に古いバージョンの STA をアンインストールする必要があるため、一部のユーザー構成データを手動で再入力する必要があります。

図8.1.1 1 台のサーバーのアップグレードタスクの概要



STA_006

8.3.2. 2 台のサーバーのアップグレード方法

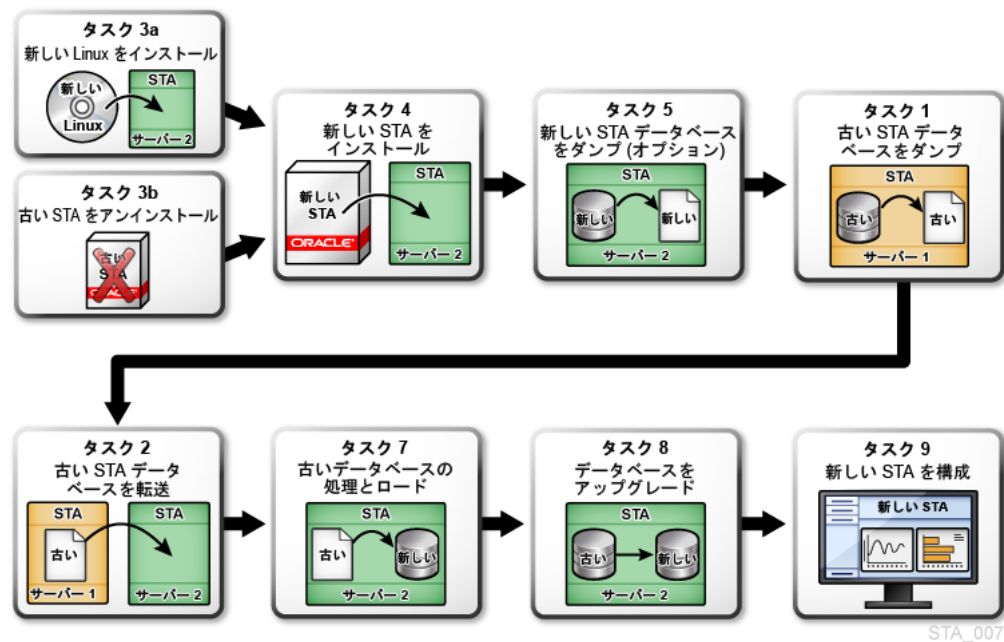
2 台のサーバーのアップグレード方法では、2 台目の専用 STA サーバーが必要になりますが、STA アプリケーションのダウンタイムが削減されるという利点が得られます。この方法は、STA 1.0.x からアップグレードする場合、古いバージョンの STA が古いサーバーでライブラリのモニターを継続でき、Linux および新しいバージョンの STA の両方が新しいサーバーにインストールされるため、特に便利です。

ただし、この方法であっても、現在のデータベースを新しい STA のバージョンにアップグレードしている間は、STA はライブラリをモニターしていません。ダウンタイムの長さは、現在のデータベースのサイズにより異なります。

図8.2「2 台のサーバーのアップグレードタスクの概要」に、2 台のサーバーの方法を示します。タスクは示された順に実行する必要があります (これらは連続の順では行われず、タスク 6 は省略されます)。新しいバージョンの STA を新しいサーバーにインストールするまでは、現在の STA データベースをダンプしないでください。まとめると次のようになります。

- 2 台目のサーバーが現在 STA のバージョンを実行しているかどうかに応じて、Linux 6.x (タスク 3a) をインストールするか、STA 2.0.x をアンインストール (タスク 3b) します。
- 新しいサーバーに STA 2.1.0 をインストールし、予防策として新しいデータベースをダンプします (タスク 4 およびタスク 5)。
- 現在のデータベースを古いサーバーでダンプし、それを新しいサーバーに転送します (タスク 1 およびタスク 2)。
- 現在のデータベースを新しい STA バージョンにロードおよびアップグレードします (タスク 7 およびタスク 8)。
- モニター対象ライブラリへの接続を再確立し、必要な手動の構成タスクを実行します (タスク 9)。

図8.2 2 台のサーバーのアップグレードタスクの概要



8.4. STA 2.1.0 の環境の変更

次に、STA 2.1.0 へのアップグレードの計画時に考慮する必要がある環境の変更をまとめます。

8.4.1. Linux バージョン

STA 2.1.0 では Linux 6.3 以降が必要です (詳細は『STA 要件ガイド』を参照してください)。現在の STA のバージョンに応じて、STA のアップグレードプロセスの一環として、新しいバージョンの Linux をインストールする必要がある場合があります。

- STA 1.0.x からアップグレードする場合、STA 2.1.0 をインストールする前に Linux 6.3 以降をインストールする必要があります。Linux では、Linux 5.x から Linux 6.x へのインプレースアップグレードはサポートしておらず、代わりに、STA サーバーに新しい Linux 6.x のインストールを行う必要があります。
- STA 2.0.x からアップグレードする場合、すでに Linux 6.3 以降を実行していますが、STA 2.1.0 をインストールする前に、現在のバージョンの STA をアンインストールする必要があります。また、必要な Linux RPM パッケージをインストールまたは更新する必要がある場合があります。アップグレード準備の一環として、すべての必要な RPM パッケージレベルがインストールされていることを確認し、最終チェックとして、不足しているパッケージがある場合には STA インストーラによっても通知されます。

8.4.2. デフォルトの WebLogic ポート番号

デフォルトの WebLogic 管理コンソールのポート番号は、STA 2.1.0 では変わりました。現在、古いデフォルトのポート番号を使用している場合、新しいデフォルト値に変更します。新旧のデフォルトのポート番号は次のとおりです。

- STA 2.1.0 の新しいデフォルト - 7019 (HTTP) および 7020 (HTTPS)
- 古いデフォルト (STA 1.0.x および STA 2.0.x) - 7001 (HTTP) および 7002 (HTTPS)

注:

WebLogic 管理コンソールのポートは外部にあります。ネットワーク管理者は、STA サーバーと、WebLogic 管理インターフェースにアクセスするクライアントとの間の通信を開くように、ファイアウォールおよびルーターを構成する必要がある場合があります。

8.4.3. STA 2.0.x 以降で必要なポート

注:

この変更は STA 2.0.x で導入されたため、STA 1.0.x からアップグレードする場合にのみ関係します。

STA 2.0.x では、STA ポートが StaUi および StaEngine 管理対象サーバー用に追加されています。STA 2.0.x および STA 2.1.0 のデフォルトの STA 管理対象サーバーのポート番号は次のとおりです。

- StaUi - 7021 (HTTP) および 7022 (HTTPS)
- StaEngine - 7023 (HTTP) および 7024 (HTTPS)
- StaAdapter - 7025 (HTTP) および 7026 (HTTPS)

注:

StaUi ポートは外部にあります。ネットワーク管理者は、STA サーバーと STA ユーザーインターフェースにアクセスするクライアントとの間の通信を開くように、ファイアウォールおよびルーターを構成する必要がある場合があります。

8.4.4. ユーザー名およびパスワードの要件

STA 2.1.0 では、STA および MySQL のユーザー名およびパスワードの要件が変更されています。これらの要件をサイトの内部要件に合わせて調整する必要がある場合があります。

ユーザー名の要件は次のとおりです。

- 1 - 16 文字の長さにする必要があります

- すべてのユーザー名が一意である必要があります

パスワード要件は次のとおりです。

- 8 – 31 文字の長さにする必要があります
- 少なくとも 1 つの数字と 1 つの大文字を含める必要があります
- 空白を含めることはできません
- 次の特殊文字を含めることはできません

& ' () < > ? { } * / ' "

8.5. アップグレード準備タスク

STA のアップグレードを開始する前に、次のタスクを実行します。これらのタスクの多くはオプションで、表8.1「アップグレード準備タスクを実行するタイミングのガイドライン」はそれぞれを使用するタイミングのガイドラインを示しています。

表8.1 アップグレード準備タスクを実行するタイミングのガイドライン

タスク	実行するタイミング
「サイトのアップグレード準備済みの確認」	すべてのアップグレード
「既存のログの保存 (オプション)」	現在のバージョンの STA からサービスログを保持するとき。
「現在の STA のユーザーおよび構成設定の記録 (オプション)」	現在の STA ユーザー名および構成設定を保持するとき。
「接頭辞に STA- の付くカスタムテンプレートの名前の変更 (オプション)」	接頭辞に「STA-」の付く名前のカスタムテンプレートがあるとき。
「現在のカスタムテンプレート設定の記録 (オプション)」	既存のカスタムテンプレートの所有権と可視性の設定を保持するとき。
「エグゼクティブレポートポリシー設定の記録 (オプション)」	既存のエグゼクティブレポートポリシーの所有権の設定を保持するとき。

8.5.1. サイトのアップグレード準備済みの確認

アップグレード要件を再確認し、サイトが準備できていることを確認するには、この手順を使用します。

8.5.1.1. アップグレード前提条件の確認

使用している環境がすべての STA 2.1.0 前提条件を満たしていることを確認するには、この手順を使用します。

1. 現在の STA のバージョンを表示します。一部のアップグレードタスクは、STA 1.0.x からアップグレードするか、STA 2.0.x からアップグレードするかによって異なります。
 - a. STA 管理者のユーザー名を使用して STA にログインします。
 - b. ステータスバーの「**About**」をクリックします。
 - c. 現在リリースされているバージョンの STA を実行していることを確認します。詳細は、「[有効な STA 2.1.0 のアップグレードパス](#)」を参照してください。
2. 1 台のサーバーのアップグレード方法を使用するか、2 台のサーバーのアップグレード方法を使用するかを選択します。詳細は、「[アップグレードプロセスの概要](#)」を参照してください。
3. サイトおよびターゲットサーバーが STA 2.1.0 の要件を満たしていることを確認します。詳細は、『[STA 要件ガイド](#)』を参照してください。
4. ターゲットの STA サーバーの `/tmp` ファイルシステムにアップグレードに十分な容量があることを確認します。`/tmp` のサイズは、少なくとも既存の非圧縮の STA データベースのサイズと同等の大きさで最低 4G バイト必要で、大きいデータベースに対しては、Oracle は `/tmp` のサイズを最低でも 32G バイトに増加することをお勧めします。

`/tmp` のサイズを増加させる必要があると判断する場合、アップグレードスクリプトを実行する直前にこれを実行できます。手順については、「[タスク 8: 古いデータベースのアップグレード](#)」を参照してください。

5. アップグレードパスに関連する環境の変更点を確認し、プランや環境に合わせて必要な調整をします。詳細は、「[STA 2.1.0 の環境の変更](#)」を参照してください。
6. STA 2.0.x からアップグレードする場合、すべての必要な RPM パッケージが STA サーバーにインストールされていることを確認します。詳細は、「[必要な Linux パッケージのインストール](#)」を参照してください。最終チェックとして、不足しているパッケージがある場合には、STA インストーラによっても通知されます。

8.5.1.2. 現在の STA アクティビティの確認

現在の STA 環境が正常に機能していることを確認するには、この手順を使用します。

1. 次の手順を使用して、現在のバージョンの STA が最近、各モニター対象ライブラリと正常に通信したことを確認します。
 - a. STA の管理者ユーザーとして STA にログインします。

- b. 「**Setup & Administration**」タブから、「**SNMP Connections**」を選択します。
 - c. 「**Monitored Libraries**」表で次の値を確認します。
 - 「Recent SNMP Trap Communication Status」 - 「GOOD」
 - 「Last Connection Status」 - 「SUCCESS」
2. 次の手順を使用して、STA がすべてのライブラリにわたって交換を処理していることを確認します。
- a. 「**Tape System Activity**」タブから「**Exchanges – Overview**」を選択します。
 - b. 「**Filter**」アイコンを選択し、「Exchange End (No. Days) Less Than 1」のフィルタ処理をします。
 - c. 表のツールバーで、「**View**」、「**Sort**」、「**Advanced**」の順に選択します。「Drive Library Name」、「Drive Serial Number」でソートします。
 - d. すべてのライブラリに交換アクティビティがあることを確認します。

8.5.2. 既存のログの保存 (オプション)

STA 2.1.0 をインストールする前に、現在のバージョンの STA をアンインストールするか、新しいバージョンの Linux をインストールする必要があるため、既存のアプリケーションおよびサービスログはアップグレード後に保持されません。保持する必要のあるログを保存するには、この手順を使用します。

1. 保持する必要のあるインストールログおよびデータベースログを特定し、それらを安全な場所に移動します。対象となり得るログは、インストール用に定義した STA ログの場所にあります。詳細は、「[STA ファイルシステムレイアウトの確認](#)」を参照してください。
2. 次の手順を使用して、現在の STA インストールでサービスログスナップショットを実行します。この手順はオプションですが、Oracle Support がこのログを使用して、アップグレード前に存在していた可能性のある問題をトラブルシューティングできるため、お勧めします。
 - a. STA の管理者ユーザーとして STA にログインします。
 - b. 「**Setup & Administration**」タブから、「**Logs**」を選択します。
 - c. 「Service – Logs」画面で、「**Create New Log Bundle**」アイコンをクリックします。
 - d. 「Create New Log Bundle」ダイアログボックスでバンドル名を割り当て、「**Save**」をクリックします。プロセスが完了するには、数分かかる場合があります。
3. 次の手順を使用して、今作成したサービスログバンドルと、保持する必要のあるほかのものをダウンロードします。バンドルは一度に 1 つずつダウンロードする必要があります。
 - a. 「Service – Logs」画面で、ダウンロードするバンドルを選択します。

- b. 「**Download Selected Log Bundle**」アイコンをクリックします。
- c. ダイアログボックスで、保存先の場所を指定し、ログバンドルを保存します。

8.5.3. 現在の STA のユーザーおよび構成設定の記録 (オプション)

このセクションは、STA 2.1.0 に現在の STA のユーザー名および構成の設定を保持する場合のみ適用されます。これらの手順を使用して、現在の値を STA 2.1.0 で再入力できるよう、表示および記録します。これらの値の多くは、アップグレード後に再入力することになります。詳細は、「[タスク 9: 新しい STA バージョンの構成](#)」を参照してください。

8.5.3.1. MySQL ユーザー名の記録

STA データベースへのアクセスに使用する既存の MySQL ユーザー名を表示および記録するには、この手順を使用します。STA インストーラによりこれらの値がプロンプト表示されます。パスワードは取得できません。

- a. 現在の STA サーバーで端末セッションを開き、システムの root ユーザーとしてログインします。
- b. 次の問合せを発行して、STA データベースのすべてのユーザー名を表示します。入力を求められたら、データベースの root ユーザーパスワードを入力します。例:

```
$ mysql -uroot -p -e "select distinct(user) from user order by user ;" mysql
Enter password: password
+-----+
| user   |
+-----+
| root   |
| staapp |
| stadba |
| starpt |
+-----+
```

- c. ユーザー名を記録します。

8.5.3.2. STA の SNMP クライアント設定の記録

STA の SNMP クライアント設定を表示および記録するには、この手順を使用します。これらの値は、アップグレード後に再入力することになります。

注:

新しいバージョンの STA で、SNMP 値がモニター対象ライブラリで指定されたものと一致している必要があります。

- a. STA 管理者のユーザー名を使用して STA にログインします。
- b. 「**Setup & Administration**」タブから、「**SNMP Connections**」を選択します。

「Client Attributes」表に、STA SNMP クライアントの構成設定が表示されます。

SNMP Username	Password Encryption	Privacy Encryption	Engine ID	User Community	Trap Community	SNMP Trap Le
sta1	SHA	DES	0x8000002a050000148c730df28	public	public	1,2,3,4,11,13,14,21,25,27,41,4

- c. 次の列の値を記録します。
 - 「SNMP Username」
 - 「User Community」
 - 「Trap Community」

8.5.3.3. WebLogic ユーザー名の記録 - STA 1.0.x からのアップグレードのみ

STA 1.0.x からのアップグレードの場合、この手順を使用して STA へのログインに使用した既存の WebLogic ユーザー名を表示および記録します。これらの値は、アップグレード後に再入力することになります。パスワードは取得できません。

注:

STA 2.0.x からは、ユーザー名は STA ユーザーインターフェースを介して作成および管理します。手順については、「[STA ユーザー名の記録 - STA 2.0.x からのアップグレードのみ](#)」を参照してください。

- a. コンピュータ上のサポートされている Web ブラウザを起動し、WebLogic 管理コンソールの URL を入力します。

`http(s)://STA_host_name:port_number/console/`

ここでは:

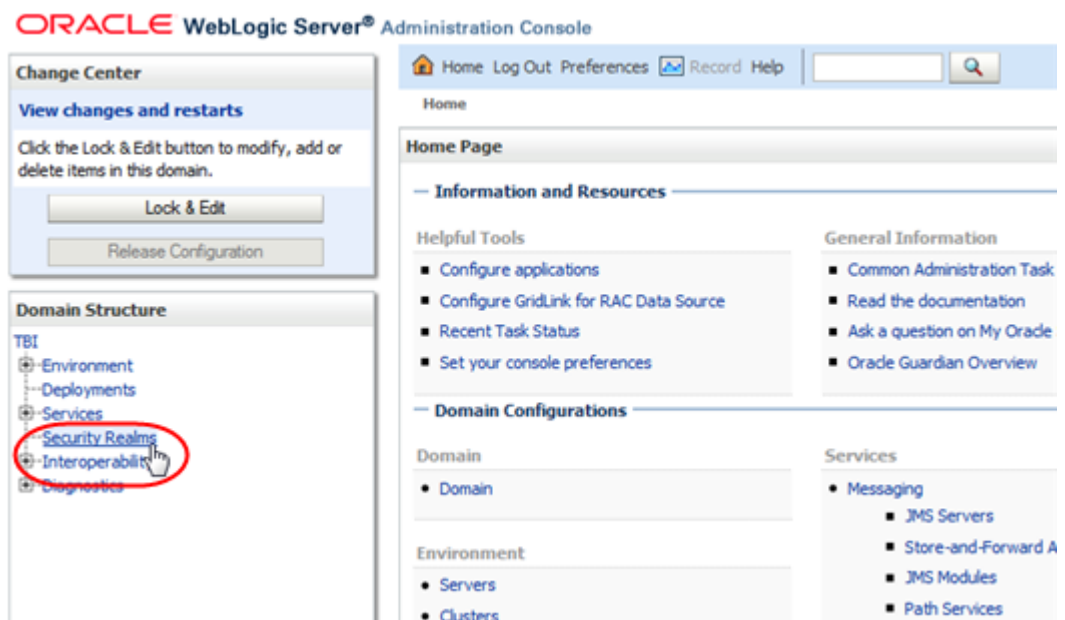
- `host_name` は STA サーバーのホスト名です。

- `port_number` は、現在の STA のバージョンでの WebLogic 管理コンソールの STA ポート番号です。
- `STA` は大文字にする必要があります。

例:

`https://staserver.example.com:7002/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。
- 「Domain Structure」ナビゲーションツリーで、「**Security Realms**」をクリックします。



「Summary of Security Realms」画面が表示されます。

- 「Name」列で、「**myrealm**」アクティブリンクを選択します (チェックボックスは選択しません)。

Summary of Security Realms

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

Customize this table

Realms (Filtered - More Columns Exist)

Click the *Lock & Edit* button in the Change Center to activate all the buttons on this page.

New Delete Showing 1 to 1 of 1 Previous | Next

<input type="checkbox"/>	Name ↕	Default Realm
<input type="checkbox"/>	myrealm	true

New Delete Showing 1 to 1 of 1 Previous | Next

「Settings for myrealm」画面が表示されます。

- e. 「Users and Groups」タブを選択します。

Settings for myrealm

Configuration **Users and Groups** Roles and Policies Credential Mappings Providers Migration

General RDBMS Security Store User Lockout Performance

Click the *Lock & Edit* button in the Change Center to modify the settings on this page.

Save

Use this page to configure the general behavior of this security realm.

「Users」表に使用可能なユーザー名が一覧表示されます。

Settings for myrealm

Configuration **Users and Groups** Roles and Policies Credential Mappings Providers Migration

Users Groups

This page displays information about each user that has been configured in this security realm.

Customize this table

Users (Filtered - More Columns Exist)

New Delete Showing 1 to 2 of 2 Previous | Next

<input type="checkbox"/>	Name ↕	Description	Provider
<input type="checkbox"/>	sta_admin	STA administrator	DefaultAuthenticator
<input type="checkbox"/>	weblogic	This user is the default administrator.	DefaultAuthenticator

New Delete Showing 1 to 2 of 2 Previous | Next

- f. 保持するユーザー名を記録します。

8.5.3.4. STA ユーザー名の記録 - STA 2.0.x からのアップグレードのみ

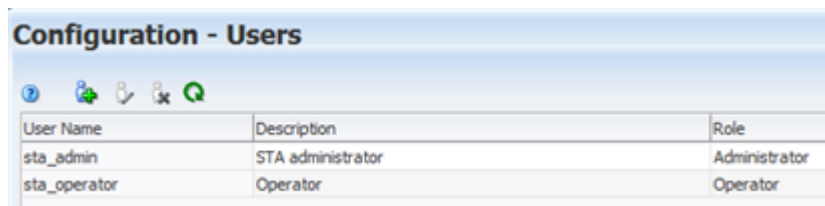
STA 2.0.x からのアップグレードの場合、この手順を使用して STA へのログインに使用したユーザー名を表示および記録します。この情報は、アップグレード後に再入力することになります。パスワードは取得できません。

注:

STA 1.0.x では、ユーザー名は WebLogic 管理コンソールを介して作成および管理されていました。手順については、「[WebLogic ユーザー名の記録 - STA 1.0.x からのアップグレードのみ](#)」を参照してください。

- a. STA 管理者のユーザー名を使用して STA にログインします。
- b. 「**Setup & Administration**」タブから、「**Users**」を選択します。

「Configuration - Users」画面にすべての STA のユーザー名とその役割が表示されます。



User Name	Description	Role
sta_admin	STA administrator	Administrator
sta_operator	Operator	Operator

- c. 保持するユーザー名および役割を記録します。

8.5.3.5. STA の電子メールサーバー設定の記録

STA の電子メールプロトコル、およびアカウントのユーザー名 (電子メールサーバーが認証を必要とする場合) を表示および記録するには、この手順を使用します。これらの値は、アップグレード後に再入力することになります。パスワードは表示できません。

- a. STA 管理者のユーザー名を使用して STA にログインします。
- b. 「**Setup & Administration**」タブから、「**Email**」を選択します。
- c. 「SMTP Server Settings」表で、「StorageTek Tape Analytics Alerts」レコードを選択して、「**Edit Selected SMTP Server**」アイコンをクリックします。

「Define SMTP Server Details」ダイアログボックスが表示されます。

- d. 次のフィールドの値を記録します。
- 「Use Secure Connection Protocol」
 - 「Username」

8.5.4. 接頭辞に STA- の付くカスタムテンプレートの名前の変更 (オプション)

この手順は、接頭辞に「STA-」の付く名前のカスタムテンプレートがある場合のみ適用されます。STA 2.1.0 のインストール中、「STA-」の接頭辞の付いたすべてのテンプレートが削除され、事前定義済みの新しい STA テンプレートに置き換えられます。

アップグレード中にテンプレートが保存されるように、テンプレートに新しい名前を割り当てるには、この手順を使用します。

注:

STA の事前定義済みテンプレートは、接頭辞「STA-」が付けられています。そのため、Oracle では、カスタムテンプレートに名前を付ける際にこの接頭辞を使用しないことをお勧めします。

- a. 管理者ユーザー名を使用して STA にログインします。
- b. 「**Setup & Administration**」タブから、「**Templates Management**」を選択します。
- c. 「Created/Updated」日で表をソートし、STA のインストール日以降に変更されたテンプレートに焦点を置きます。
- d. 接頭辞に「STA-」の付いた名前のカスタムテンプレートのテキストリンクを選択します。

選択したテンプレートが適用された画面になります。

- e. テンプレートツールバーの「**Save Template**」をクリックします。

「Save Template」ダイアログボックスが表示されます。

- f. 「**Template Name**」フィールドに接頭辞「STA-」を付けない新しい名前を割り当てます。エントリは一意である必要があります。
- g. 「保存」をクリックします。

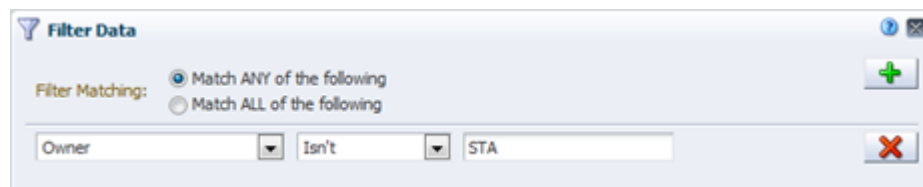
テンプレートが保存されます。

8.5.5. 現在のカスタムテンプレート設定の記録 (オプション)

このセクションは、カスタムテンプレートがある場合のみ適用されます。アップグレードではカスタムテンプレートが保存されますが、アップグレード後、すべてのカスタムテンプレートはパブリックの可視性ととも STA に所有されます。

すべてのカスタムテンプレートの現在の所有権および可視性の設定を、必要に応じてアップグレード後に復元できるように記録するには、この手順を使用します。使用している実装でテンプレートの所有権および可視性が重要でない場合には、この手順を省略できます。

- a. 管理者ユーザー名を使用して STA にログインします。
- b. 「**Setup & Administration**」タブから、「**Templates Management**」を選択します。
- c. 「**Filter**」アイコンを選択して画面をフィルタし、STA に所有されていないテンプレートのみを表示します (カスタムテンプレートのみが表示されます)。



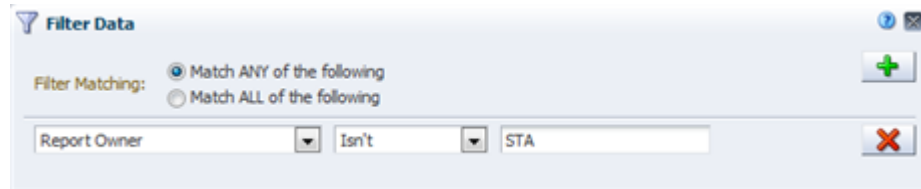
- d. 各カスタムテンプレートの現在の「Owner」および「Public Visibility」の設定を記録します。テンプレートが多い場合には、スクリーンショットを撮ることもできます。

8.5.6. エグゼクティブレポートポリシー設定の記録 (オプション)

このセクションは、プライベートでエグゼクティブレポートポリシーを所有していた場合のみ適用されます。アップグレードではすべてのエグゼクティブレポートポリシーを保存しますが、アップグレード後、すべてのプライベートポリシーは、パブリックの所有権に割り当てられます。

すべてのプライベートポリシーの現在の所有権の設定を、必要に応じてアップグレード後に復元できるように記録するには、この手順を使用します。使用している実装でエグゼクティブレポートポリシーの所有権が重要でない場合には、この手順を省略できます。

- a. STA 管理者のユーザー名を使用して STA にログインします。
- b. 「**Setup & Administration**」タブから、「**Executive Reports Policies**」を選択します。
- c. 「**Filter**」アイコンを選択して画面をフィルタし、STA に所有されていないポリシーのみを表示します (プライベートポリシーのみが表示されます)。



- d. 各ポリシーに対する現在の「Report Owner」の設定を記録します。ポリシーが多い場合には、スクリーンショットを撮ることもできます。

8.6. アップグレードタスク

注意:

Linux 管理者と STA 管理者のみが、アップグレードを実行するべきです。すべてのタスクが必要で、記載されたとおり正確に指定された順で実行する必要があり、そうしないとデータが失われる可能性があります。

1 台のサーバーのアップグレード方法を使用する場合、連続した順にタスクを実行します。詳細は、[図8.1「1 台のサーバーのアップグレードタスクの概要」](#)を参照してください。

2 台のサーバーのアップグレード方法を使用する場合、タスクを連続した順には実行せず、タスク 6が省略されます。タスクの順については、[図8.2「2 台のサーバーのアップグレードタスクの概要」](#)を参照してください。

- 「タスク 1: 古い STA データベースのダンプ」
- 「タスク 2: 古いデータベースダンプの転送」
- 「タスク 3a: 新しい Linux バージョンのインストール (STA 1.0.x からのアップグレード)」
- 「タスク 3b: 古い STA バージョンのアンインストール (STA 2.0.x からのアップグレード)」
- 「タスク 4: 新しい STA バージョンのインストール」
- 「タスク 5: 新しい STA データベースのダンプ (オプション)」
- 「タスク 6: 古い STA データベースの STA サーバーへの転送」

- 「タスク 7: 古い STA データベースの処理およびロード」
- 「タスク 8: 古いデータベースのアップグレード」
- 「タスク 9: 新しい STA バージョンの構成」
- 「失敗したデータベースアップグレードの回復 (オプション)」

8.6.1. タスク 1: 古い STA データベースのダンプ

古い (現在の) STA データベースの完全ダンプを実行するには、この手順を使用します。

1. 次の手順を使用して、現在の STA データベースのサイズを表示します。
 - a. STA 管理者のユーザー名を使用して STA にログインします。
 - b. ステータスバーの「**About**」をクリックします。
 - c. 「About」ダイアログボックスで、「Database Current Size」が表示されているところまでスクロールダウンし、その値を記録します。
2. 次の手順を使用して、データベースをダンプする場所に十分な容量があることを確認します。
 1. STA サーバーで端末セッションを開き、システムの root ユーザーとしてログインします。
 2. データベースのダンプ先で使用可能な容量を表示し、ダンプファイルに十分であることを確認します。例:

```
# df -h /dbdumpfiles
Filesystem          Size  Used Avail Use% Mounted on
/dev/mapper/sta_server-STA_DbVol
                    200G   53G   243G   27% /dbdumpfiles
```

3. すべての STA サービスを停止します。

```
# STA stop all
```

4. MySQL サービスを起動します。

```
# service mysql start
```

5. STA データベースを単一のファイルにダンプします。入力を求められたら、データベースの root ユーザーパスワードを入力します。

```
# mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert --
dump-date --events --flush-logs --routines --single-transaction --triggers --
databases stadb > /dumpfile_path/dumpfile_name.sql
Enter password: mysql_root_password
```

注:

オプションの `-v` パラメータ (詳細出力用) は、端末ウィンドウに多数のメッセージが表示され、大規模データベースのコマンド処理の速度を大幅に低下させる可能性があるため、推奨しません。

例8.1「古いデータベースのダンプ」では、STA 1.0.x データベースが STA サーバーの `/dbdumpfiles` フォルダに `Dec14_dump.sql` というファイル名でダンプされます。

例8.1 古いデータベースのダンプ

```
# mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert --
dump-date --events --flush-logs --routines --single-transaction --triggers --
databases stadb > /dbdumpfiles/Dec14_dump.sql
```

```
Enter password: mysql_root_password
```

```
...
-- Retrieving view structure for table v_library_complex_io...
...
-- Retrieving view structure for table v_library_summary_averages...
-- It's base table, skipped
...
-- Retrieving table structure for table v_mdv_status_codes...-- It's a view,
create dummy table for view
...
-- Disconnecting from localhost...
```

6. ダンプファイルサイズを約 50% 縮小するには、ファイルを gzip します。

```
# cd /path_to_dump_file/
# gzip dump_file_name.sql
```

8.6.2. タスク 2: 古いデータベースダンプの転送

古い STA データベースの圧縮済みダンプをプラットフォーム外のバックアップサーバー (1 台のサーバーの方法) または新しい STA 2.1.0 サーバー (2 台のサーバーの方法) のいずれかに転送するには、この手順を使用します。

注意:

1 台のサーバーの方法で STA 1.0.x からアップグレードする場合、STA データベースを別のサーバーにバックアップする必要があります。[145 ページの「タスク 3a: 新しい Linux バージョンのインストール \(STA 1.0.x からのアップグレード\)」](#) の Linux 6.x のインストールによって、現在の STA サーバー上のデータがすべて破棄されるため、このサーバー上のファイルシステムにはデータベースをバックアップしないでください。

1. まだ停止していない場合には、すべての STA サービスを停止します。

```
# STA stop all
```

2. ファイルをバックアップサーバーに転送する前に、チェックサムを実行します。

```
# cksum dump_file_name.sql.gz
```

出力には、チェックサム値とバイト数が含まれています。チェックサム値を記録します。ファイルをバックアップサーバーに転送したあとで、これを使用してファイルの整合性を検証します。

3. SCP などの転送ユーティリティーを使用して、ファイルをターゲットサーバーに転送します。-p オプションは、タイムスタンプ値を保存します。

```
# scp -p dump_file_name.sql.gz target_host:/path/
```

例8.2「バックアップサーバーへの古いデータベースの転送 (1 台のサーバーの方法)」

では、SCP を使用して、圧縮済みのデータベースダンプファイル `Dec14_dump.sql.gz` がバックアップホスト `backup1` 上の `/dbdumpfiles` フォルダに転送されます。`/dbdumpfiles` フォルダはすでにバックアップホストに存在しています。

例8.2 バックアップサーバーへの古いデータベースの転送 (1 台のサーバーの方法)

```
# cd /dbdumpfiles
```

```
# scp -p Dec14_dump.sql.gz backup1:/dbdumpfiles
```


例8.3「新しい STA サーバーへの古いデータベースの転送 (2 台のサーバーの方法)」では、SCP を使用して、圧縮済みのデータベースダンプファイル `Dec14_dump.sql.gz` が STA 2.1.0 ホスト `sta_new` 上の `/dbdumpfiles` フォルダに転送されます。

例8.3 新しい STA サーバーへの古いデータベースの転送 (2 台のサーバーの方法)

```
# cd /dbdumpfiles
# scp -p Dec14_dump.sql.gz sta_new:/dbdumpfiles
```

4. ターゲットサーバーで、転送されたファイルのチェックサムを実行します。チェックサム値が一致することを確認します。

```
# cd /path_to_dump_file/
# cksum dump_file_name.sql.gz
```

8.6.3. タスク 3a: 新しい Linux バージョンのインストール (STA 1.0.x からのアップグレード)

この手順は、STA 1.0.x からのアップグレードのみに適用されます。Linux 6.3 以降を STA サーバーにインストールします。手順については、2章「[Linux のインストール](#)」を参照してください。

注意:

このアクティビティにより、サーバー上のすべてのデータが破棄されます。1 台のサーバーのアップグレード方法を使用する場合、この手順は、「[タスク 1: 古い STA データベースのダンプ](#)」および「[タスク 2: 古いデータベースダンプの転送](#)」の実行後にのみ使用します。

8.6.4. タスク 3b: 古い STA バージョンのアンインストール (STA 2.0.x からのアップグレード)

この手順は、STA 2.0.x からのアップグレードのみに適用されます。現在のバージョンの STA をアンインストールします。手順については、「[STA のアンインストール](#)」および「[アンインストールが成功したことの確認](#)」を参照してください。

注意:

このアクティビティにより、サーバー上のすべての STA データが破棄されます。1 台のサーバーのアップグレード方法を使用する場合、この手順は、「[タスク 1: 古い STA データベースのダンプ](#)」および「[タスク 2: 古いデータベースダンプの転送](#)」の実行後にのみ使用します。

8.6.5. タスク 4: 新しい STA バージョンのインストール

STA 2.1.0 をインストールするには、この手順を使用します。

1. STA 2.1.0 をインストールします。手順については、3章「[STA のインストール](#)」を参照してください。
2. STA が正常に動作していることを確認し、WebLogic での STA 管理者設定を完了させるには、STA アプリケーションにログインします。

「Dashboard」が表示されます。

注:

アップグレード処理がまだ完了していないため、「Dashboard」ポートレットに「No data to display」のメッセージが表示されます。これは正常です。ライブラリデータは、データベースをアップグレードし、新しい STA のバージョンを構成したあとに、正常に表示されます。

3. STA からログアウトします。
4. STA サーバーで端末セッションを開き、システムの root ユーザーとしてログインします。
5. すべての STA サービスを停止します。

STA stop all

6. この手順は、SNMP v2c を使用して STA にライブラリをモニターさせる場合にのみ適用されます (詳細は、[付録F「SNMP v2c モードの構成」](#)を参照してください)。STA 2.0.x からは、SNMP v2c はデフォルトで有効にされます。次の手順を使用して、これが有効になっていることを確認します。
 - a. STA 構成ファイルのディレクトリに移動します。

```
# cd /Oracle_storage_home/Middleware/user_projects/domains/TBI
```

- b. SNMP バージョンプロパティファイル表示し、v2c パラメータが true に設定されていることを確認します。

```
# cat TbiSnmpVersionSupport.properties
```

```
V2c=true
```

```
Verbal=false
```

- c. パラメータが true に設定されていない場合、変更する方法の手順は、「[STA の SNMP v2c モードの有効化](#)」を参照してください。

8.6.6. タスク 5: 新しい STA データベースのダンプ (オプション)

この手順はオプションですが、推奨されます。予防策として空の STA 2.1.0 データベースをダンプするには、この手順を使用します。データベースのアップグレード(「[タスク 8: 古いデータベースのアップグレード](#)」)を完了できない場合、空のデータベースを復元して STA 2.1.0 をデータなしで新しくインストールされたかのように実行するよう構成できる状態に回復することができます。復元処理の詳細は、「[失敗したデータベースアップグレードの回復 \(オプション\)](#)」を参照してください。

1. STA サーバーで端末セッションを開き、システムの root ユーザーとしてログインします。
2. まだ停止していない場合には、すべての STA サービスを停止します。

```
# STA stop all
```

3. MySQL サービスを起動します。

```
# STA start mysql
```

4. データベースバックアップファイルを作成します。入力を求められたら、データベースの root ユーザーパスワードを入力します。

```
# mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert --
dump-date --events --flush-logs --routines --single-transaction --triggers --
databases stadb > /dumpfile_path/dumpfile_name.sql
```

注:

オプションの `-v` パラメータ (詳細出力用) は、端末ウィンドウに多数のメッセージが表示され、大規模データベースのコマンド処理の速度を大幅に低下させる可能性があるため、推奨しません。

[例8.4「新しいデータベースのダンプ](#)」では、STA 2.1.0 データベースが STA サーバーの `/dbdumpfiles` フォルダに `/dbdumpfiles` というファイル名でダンプされます。

例8.4 新しいデータベースのダンプ

```
# mysqldump -uroot -p --opt --add-drop-database --comments --complete-insert --
dump-date --events --flush-logs --routines --single-transaction --triggers --
databases stadb > /dbdumpfiles/STA_FRESH_INSTALL_BACKUP.sql
```

```
Enter password: mysql_root_password
```

```
...
```

```
-- Retrieving view structure for table v_mdv_request_states...
-- Retrieving view structure for table version_info...
...
-- Disconnecting from localhost...
```

注:

「Can't connect to local MySQL server」のメッセージが表示された場合には、MySQL サーバーは動作していません。MySQL が起動されていることを確認します (手順 3)。

8.6.7. タスク 6: 古い STA データベースの STA サーバーへの転送

注:

この手順は、1 台のサーバーの方法にのみ適用されます。

STA 1.0.x または STA 2.0.x のデータベースバックアップを STA 2.1.0 サーバーに転送するには、この手順を使用します。

1. まだ停止していない場合には、すべての STA サービスを停止します。

```
# STA stop all
```

2. データベースを転送します。SCP 用の `-p` オプションは、タイムスタンプ値を保存します。

```
# scp -p backup_host:/path_to_dump_file/dump_file_name.sql.gz /local_path
```

例8.5「新しい STA サーバーへの古いデータベースの転送」では、SCP を使用して、圧縮済みのデータベースダンプファイル `Dec14_dump.sql.gz` がホスト `backup1` の `/dbdumpfiles` から STA 2.1.0 サーバー上の `/dbdumpfiles` フォルダに転送されます。

例8.5 新しい STA サーバーへの古いデータベースの転送

```
# scp -p backup1:/dbdumpfiles/Dec14_dump.sql.gz /dbdumpfiles
```

3. 転送されたファイルのチェックサムを実行します。チェックサム値が、[142 ページの「タスク 1: 古い STA データベースのダンプ」](#)で受け取った値と一致することを確認します。

```
# cd /path_to_dump_file/
```

```
# cksum dump_file_name.sql.gz
```

8.6.8. タスク 7: 古い STA データベースの処理およびロード

STA 1.0.x または STA 2.0.x のデータベースを圧縮解除し、それを STA 2.1.0 サーバーに回復するには、この手順を使用します。圧縮解除されたデータベースは、圧縮されたデータベースの 10 - 15 倍の容量を必要とする場合があります。

1. まだ停止していない場合には、すべての STA サービスを停止します。

```
# STA stop all
```

2. バックアップファイルを圧縮解除します。

```
# gunzip dump_file_name.sql.gz
```

3. 次の手順を使用して、SNMP レコードや空の分析レコードなどの廃止されたデータの STA データベースをパージします。

推定時間: STA 1.0.x および STA 2.0.x では、1G バイトの非圧縮のデータベーススナップショットサイズにつき最大 1 分です。

注:

purgerecs コマンドアクティビティの永続レコードは、STA データベースに保存されます。STA 2.0.x からは、データベースのパージも実行時に自動的に行われます。MySQL イベントスケジューラがさまざまなテーブルからのレコードを定期的にパージして、データベースの拡張を緩和します。

- a. STA データベースの更新ディレクトリに変更します。

```
# cd /Oracle_storage_home/StorageTek_Tape_Analytics/db/updates
```

- b. パージを開始します。

```
# ./purgerecs /path_to_dump_file/dump_file_name.sql /path_to_dump_file/dump_file_name_PURGED.sql
```

注:

purgerecs コマンドのヘルプについては、次のコマンドを入力します。

```
# ./purgerecs -h
```

例8.6「古いデータベースバックアップからの廃止されたデータのパーズ」では、`purgerecs` ユーティリティーが `/dbdumpfiles` の MySQL ダンプファイル `Dec14_dump.sql` を処理します。出力は、`/dbdumpfiles` の `Dec14_dump_PURGED.sql` という名前の新しいファイルに送られます。200 個のレコードが処理されるたびに、進捗を示すドットが 1 つ表示されます。

例8.6 古いデータベースバックアップからの廃止されたデータのパーズ

```
# cd /Oracle/StorageTek_Tape_Analytics/db/updates
# ./purgerecs /dbdumpfiles/Dec14_dump.sql /dbdumpfiles/Dec14_dump_PURGED.sql
.....
          STA v1.0.2, Schema 33.02
Processed 11,689 lines from '20130711_dump.sql':
-----
snmp_storage_cells.....1,614,255
snmp_media.....110,205
...
media_summaries.....254
transform_logs.....0
=====
Records Processed:.....13,143,283
Records Purged:.....2,857,623
Records Remaining:.....10,285,660
Elapsed Time:.....00:00:11
```

4. この手順はオプションです。データベースファイルサイズを特定し、ロード処理時間を推定します。

推定時間: STA 1.0.x および STA 2.0.x では、1G バイトの非圧縮のデータベーススナップショットサイズにつき最大 3 - 10 分です。

```
# ls -s -h dump_file_name_PURGED.sql
```

5. MySQL サーバーを起動します。

```
# STA start mysql
```

6. STA 1.0.x データベースまたは STA 2.0.x データベースをロードします。入力を求められたら、データベースの root ユーザーパスワードを入力します。`-v` (詳細) オプション (推奨されません) を指定した場合を除き、プロセスの実行中にコマンド出力は表示されません。

注:

オプションの `-v` パラメータ (詳細出力用) は、端末ウィンドウに多数のメッセージが表示され、大規模データベースのコマンド処理の速度を大幅に低下させる可能性があるため、推奨しません。

```
# mysql -uroot -p -e "SET SESSION SQL_LOG_BIN=0; SOURCE /path_to_dump_file/dump_file_name_PURGED.sql;"
Password: mysql_root_password
```

ここでは:

- `-p` - STA のインストール中に設定したデータベースの root パスワードを要求します。
- `-e` - 次の引用符で囲まれた文を実行します。
 - `SET SESSION SQL_LOG_BIN=0;` - 不要なバイナリロギングをオフにし、ロードの速度を上げます。
 - `SOURCE /path_to_dump_file/dump_file_name_PURGED.sql` - ダンプファイルを DB にロードします。

コマンドが成功した場合は、プロセスの完了後にコマンドプロンプトに戻ります。

8.6.9. タスク 8: 古いデータベースのアップグレード

STA 1.0.x または STA 2.0.x のデータベースを新しい STA 2.1.0 スキーマにアップグレードするには、この手順を使用します。

推定時間: 1G バイトの非圧縮のデータベーススナップショットサイズごとの概算時間。

- STA 1.0.x - 1G バイトにつき最大 5 分
- STA 2.0.x - 1G バイトにつき最大 30 分

1. まだ停止していない場合には、すべての STA サービスを停止します。

```
# STA stop all
```

2. 「アップグレード前提条件の確認」で `/tmp` のサイズがアップグレードに不十分であることが判明した場合、必要に応じて `/tmp` のサイズを増やします。

これができない場合には、次の手順を使用して MySQL の環境変数を代替の一時的な場所を使用するように設定します。

- a. 代替の一時的場所を作成し、それにオープン権限を割り当てます。例:

```
# mkdir /dbbackup/tmp
# chmod 777 /dbbackup/tmp
```

- b. MySQL を停止します。

```
# STA stop mysql
```

- c. MySQL 構成ファイルを編集します。例:

```
# vi /etc/my.cnf
```

- d. ファイルの `mysqld` セクションで、`tmpdir` 変数で特定される、代替の一時的場所を定義する行を追加します。この行の追加後のファイルの例を次に示します。

```
[mysqld]
#----- mysqld MySQL Server Options -----

tmpdir                                = /dbbackup/tmp
server-id                              = 1
...
```

- e. MySQL を再起動します。

```
# STA start mysql
```

3. データベースの更新ディレクトリに変更します。

```
# cd /Oracle_storage_home/StorageTek_Tape_Analytics/db/updates
```

4. アップグレードスクリプトを開始し、入力を求められたら、データベースの `root` ユーザーパスワードを入力します。セキュリティー保護のため、パスワードは画面に表示されません。


```
# ./upgradedb.sh
```

注:

この手順は、システムの root ユーザーまたは Oracle インストールユーザーのいずれかとして実行できます。

次に、画面の表示例を示します。

```
# ./upgradedb.sh
```

```
DB Root Password:
```

```
+-----+
| STA DATABASE UPGRADE                               |
| Upgrading DB schema from 58.00r0 to 59.00r0        |
| Started: 2014-12-12 15:14:45                        |
+-----+
STA database is 5.15 GB and contains approximately 12,636,002 records.
Checking if current database v58.00 is a valid upgrade candidate...
...DB v58.00 is a valid upgrade candidate...
+-----+
==> You may ABORT using CTRL-C within 7 seconds
==> .....6.....5.....4.....3.....2.....1
==> CTRL-C disabled!
+-----+
Starting upgrade...
```

処理が完了すると、次のようなバナーが表示されます。

注意:

このバナーが表示されるまで待機してから次に進みます。

```
+-----+
| Started.....2014-12-12 15:14:45                    |
| Finished.....2014-12-12 17:07:11                   |
| Elapsed Time.....01:52:26                          |
| Starting Version.....58.00r0                       |
+-----+
```

```

| Final Schema Version....59.00r0          |
| Schema Release Date.....2014-12-12 11:00:00 |
| Records (approximate)...12,636,002      |
+-----+

```

5. 「[タスク 8: 古いデータベースのアップグレード](#)」で `/tmp` のサイズを増やしたか、代替の一時的場所を作成した場合、それを通常のサイズおよび場所に戻します。
6. すべての STA サービスを開始します。

```
# STA start all
```

7. この手順はオプションです。`STA_FRESH_INSTALL_BACKUP.sql` ファイルを削除して、STA データベースのバックアップボリュームのディスク領域を解放します。

8.6.10. タスク 9: 新しい STA バージョンの構成

STA がライブラリアクティビティのモニタリングを開始できるよう、ライブラリおよび STA 2.1.0 を構成するには、これらの手順を使用します。

8.6.10.1. ライブラリでの STA トラップ受信者の更新

STA 2.0.x では、13 (テストトラップ) および 14 (ヘルストラップ) の新しい 2 つのトラップレベルが導入されました。各モニター対象ライブラリで次の手順を実行して、これらのトラップレベルが STA トラップ受信者の定義に含まれていることを確認します。

1. アップグレードパスに応じて、次のように進みます。
 - STA 2.0.x からのアップグレードに 1 台のサーバーの方法を使用する場合、[155 ページの「STA での SNMP 設定の構成」](#)に進みます。
 - STA 1.0.x からのアップグレードに 1 台のサーバーの方法を使用する場合、[手順 2](#)に進み、各モニター対象ライブラリの既存の STA トラップ受信者に新しいトラップレベルを追加します。
 - 2 台のサーバーのアップグレード方法を使用する場合、[手順 3](#)に進み、各モニター対象ライブラリに新しい STA トラップ受信者を追加します。
2. STA 1.0.x からのアップグレードに 1 台のサーバーの方法を使用する場合、ライブラリモデルに適した手順を使用し、STA トラップ受信者に新しいトラップレベルを追加します。

SL150 以外のすべてのライブラリモデルにおいて、トラップ受信者を変更するには、既存の定義を削除してから新しい定義を追加する必要があります。

SL150 以外のすべてのライブラリ

- a. ライブラリ CLI にログインします。
- b. 既存のすべてのトラップ受信者を表示し、STA 受信者のインデックス番号をメモします。

```
snmp listTrapRecipients
```

- c. STA トラップ受信者を削除します。

```
snmp deleteTrapRecipient id index
```

ここでは:

- *index* は、STA トラップ受信者のインデックス番号です。

- d. STA トラップ受信者を再度追加し、トラップレベルリストに新しいトラップレベルを含めます。手順については、「[STA SNMP v3 トラップ受信者の作成](#)」または「[ライブラリでの STA SNMP v2c トラップ受信者の作成](#)」を参照してください。

SL150 ライブラリ

- a. ブラウザベースのユーザーインターフェースにログインします。
 - b. 「SNMP」メニューから「SNMP Trap Recipients」を選択します。
 - c. リストから STA トラップ受信者を選択します。
 - d. 「Modify Trap Recipient」を選択します。
 - e. トラップレベルリストに新しいトラップレベルを追加し、「Save」をクリックします。
3. 2 台のサーバーのアップグレード方法を使用する場合、各モニター対象ライブラリで新しい STA 2.1.0 サーバーをトラップ受信者として追加します。[97 ページの「STA SNMP v3 トラップ受信者の作成」](#)または「[ライブラリでの STA SNMP v2c トラップ受信者の作成](#)」を参照してください。

8.6.10.2. STA での SNMP 設定の構成

すべてのアップグレードに対して次の手順を実行します。これらの手順は、STA で実行されます。

1. STA の管理者ユーザーとして STA にログインします。

- アップグレード前に記録した値を使用して、STA SNMP クライアントの構成設定を再入力します。「現在の STA のユーザーおよび構成設定の記録 (オプション)」を参照してください。これらの値は、モニター対象ライブラリで構成されたものと一致している必要があります。手順については、「STA の SNMP クライアント設定の構成」を参照してください。
- STA とライブラリ間の SNMP 通信を復元するため、各モニター対象ライブラリへの接続をテストします。手順については、「ライブラリへの SNMP 接続のテスト」を参照してください。

注:

この手順が正常に完了すると、STA は各モニター対象ライブラリからデータの受信および処理を開始します。

STA が停止されたとき、またはライブラリ接続が復元されたときに、「Exchanges Overview」画面で進行中の交換からの不完全な交換に気づくことがあります。不完全な交換の詳細については、『STA ユーザーズガイド』を参照してください。

- 各ライブラリからの最新の SNMP 構成データを取得します。手順については、「手動データ収集の実行」を参照してください。

8.6.10.3. STA サービスおよびユーザー情報の構成

すべてのアップグレードに対してこれらの手順を実行します。これらの手順は、STA サーバーで実行されます。

以前の STA バージョンから設定を維持する場合には、アップグレード前に記録した値を使用します。「現在の STA のユーザーおよび構成設定の記録 (オプション)」を参照してください。

注:

アップグレード後、すべての論理グループが STA に所有されます。論理グループの所有権は STA の機能には重大ではなく、オペレータ権限または管理者権限を持つ STA ユーザーは論理グループを変更できます。

- STA バックアップサービスユーティリティおよび STA リソースモニターサービスユーティリティを構成します。詳細は、7章「STA サービスの構成」を参照してください。
- STA のユーザー名およびパスワードを作成します。手順については、『STA ユーザーズガイド』を参照してください。また、次のこともします。
 - STA 2.1.0 の新しいパスワード要件についてユーザーに通知します。
 - 該当する場合、ユーザーにカスタムユーザープリファレンスを再入力させます。

3. STA 電子メールサーバーで認証が必要な場合、電子メールアカウントのユーザー名およびパスワードを入力する必要があります。手順については、『STA ユーザーズガイド』を参照してください。
4. 該当する場合は、元の所有権をカスタムテンプレートに復元します。手順については、『STA ユーザーズガイド』を参照してください。
5. 該当する場合は、元の所有権をプライベートエグゼクティブレポートポリシーに復元します。手順については、『STA ユーザーズガイド』を参照してください。

8.6.10.4. 古い STA サーバーの廃止 (オプション)

この手順は、2 台のサーバーのアップグレード方法を使用した場合のみ適用されます。この手順は、新しい STA サーバーが期待どおりに機能していることを確認したあと、使用できません。

1. 各ライブラリの SNMP 構成から、トラップ受信者として古い STA 1.0.x サーバーまたは STA 2.0.x サーバーを削除します。手順については、『STA ユーザーズガイド』を参照してください。
2. 古い STA 1.0.x サーバーまたは STA 2.0.x サーバーを廃止します。

8.6.11. 失敗したデータベースアップグレードの回復 (オプション)

注意:

この手順は Oracle サポート担当者 の指導に従ってのみ実行してください。

この手順は、151 ページの「[タスク 8: 古いデータベースのアップグレード](#)」でのデータベースのアップグレードが正常に完了せず、アップグレードの繰り返しの試行も失敗した場合のみ使用します。

1. [149 ページの「タスク 7: 古い STA データベースの処理およびロード](#)」、手順 6 から [151 ページの「タスク 8: 古いデータベースのアップグレード](#)」を繰り返します。

アップグレードが再度失敗した場合、データベースは不明な破損状態になっている可能性があるため、データベースを元の新しくインストールされた状態に復元する必要があります。次の手順に進みます。

2. 破損したアップグレード済みデータベースを削除します。

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

3. STA データベースのバックアップ場所に変更し、[147 ページの「タスク 5: 新しい STA データベースのダンプ \(オプション\)」](#)で作成した新しいインストールデータベースダンプファイルをロードします。

例:

```
# cd /dbbackup
# mysql -uroot -p -e < /home/oracle/STA_FRESH_INSTALL_BACKUP.sql
```

4. [151 ページの「タスク 8: 古いデータベースのアップグレード」](#)を実行します。
5. STA を新しいインストールとして構成します。詳細は、次のセクションを参照してください。
 - [6章「STA でのライブラリ接続の構成」](#)
 - [7章「STA サービスの構成」](#)

STA のアンインストールと復元

この章には次のセクションが含まれます。

- [STA のアンインストールの概要](#)
- [STA のアンインストールタスク](#)

注意:

Oracle では、STA の前のバージョンへのダウングレードはサポートしていません。古いバージョンの STA をインストールすると、新しいバージョンの STA で作成されたデータベースデータは失われます。

9.1. STA のアンインストールの概要

STA アンインストーラは、STA アプリケーションとそれに関連するすべてのデータおよび Oracle ソフトウェアを削除します。次の更新が行われます。

- Oracle ストレージホームの場所にある *StorageTek_Tape_Analytics* サブディレクトリが完全に削除されます。Oracle ストレージホームの場所にあるほかのディレクトリは影響を受けません。
- STA と MySQL のすべてのログがログの場所から削除されます。この場所の詳細は、「[STA ファイルシステムレイアウトの確認](#)」を参照してください。
- STA サービスログがすべて削除されます。
- STA データベースとすべてのローカルバックアップが削除されます。データベースディレクトリまたはローカルバックアップディレクトリがマウントポイントであるか、その中にユーザー定義ファイルが含まれている場合、それらのディレクトリは保持されます。それ以外の場合、それらは削除されます。

Oracle 中央インベントリの場所は、STA のアンインストールによって削除されません。STA のすべてのインストールログとアンインストールログや、Oracle ソフトウェアインベントリ情報など、このディレクトリ内のデータはすべて保持されます。詳細は、[Oracle 中央インベントリの場所](#)を参照してください。

STA アンインストーラは、グラフィカルモードとサイレントモードの両方で使用できます。詳細は、「[STA インストーラのモード](#)」を参照してください。

STA のアンインストールログの詳細は、「[STA のインストールおよびアンインストールのログ](#)」を参照してください。

9.2. STA のアンインストールタスク

次の各セクションでは、STA アンインストーラの使用方法について説明します。

- 「[STA のアンインストール](#)」
- 「[アンインストールが成功したことの確認](#)」
- 「[STA の復元](#)」

9.2.1. STA のアンインストール

STA をアンインストールするには、次の手順を使用します。

注意:

アンインストールでは、すべての STA データベースデータが削除されます。この手順を開始する前に、完全なデータベースダンプを実行するようにしてください。手順については、「[タスク 1: 古い STA データベースのダンプ](#)」を参照してください。

注:

STA をアンインストールするには、Oracle インストールグループのメンバーであるユーザーとしてログインする必要があります。Linux *root* ユーザーとしても、スーパーユーザー権限を持つほかのユーザーとしても STA をアンインストールすることはできません。詳細は、「[Oracle インストールグループ](#)」を参照してください。

1. Oracle インストールユーザーとしてログインします。
2. Oracle ストレージホームディレクトリに移動します。例:

```
$ cd /Oracle
```

3. STA インストーラバイナリディレクトリに移動します。

```
$ cd StorageTek_Tape_Analytics/oui/bin
```

4. 次のいずれかのコマンドを使用して、STA アンインストーラを起動します。

- STA グラフィカルアンインストーラを使用するには:

```
$ ./deinstall.sh
```


このモードには X11 ディスプレイが必要です。手順については、[付録A「STA グラフィカルインストーラおよびアンインストーラの画面リファレンス」](#)を参照してください。

- STA サイレントアンインストーラを使用するには:

```
$ ./deinstall.sh -silent -responseFile response_file
```

ここで、*response_file* はあらかじめ作成した応答ファイルの絶対パスです。

このモードを使用する前に、*silentInstallUtility.jar* ファイルをダウンロードし、インストールオプションを指定する応答ファイルを作成する必要があります。手順については、[付録B「STA サイレントモードインストーラおよびアンインストーラ」](#)を参照してください。

9.2.2. アンインストールが成功したことの確認

アンインストール後にすべての STA コンポーネントが STA サーバーから削除されていることを確認するには、次の手順を使用します。

1. Oracle インストールユーザーとしてログインします。
2. Oracle ストレージホームディレクトリの内容を一覧表示します。空になっているはずですが。
例:

```
$ ls -la /Oracle
total 8
drwxr-xr-x  2 oracle oinstall 4096 Sep 23 14:55 .
dr-xr-xr-x. 31 root   root    4096 Sep 23 16:41 ..
$
```

9.2.3. STA の復元

アンインストールしたあとで、たとえば、現在のインストールを修復するために STA を再インストールするには、次の手順を使用します。STA インストーラを使用して、現在のインストールを再インストールしたり上書きしたりすることはできません。

1. 現在の STA インストールに対してサービスログスナップショットを実行します。Oracle サポートでは、生成されたサービスログを使用して、アップグレード前に存在していた可能性のある問題をトラブルシューティングできます。詳しい手順については、『[STA ユーザーズガイド](#)』を参照してください。
2. すべての STA サービスを停止します。

```
# STA stop all
```

3. データベーススナップショットを実行します。
 - a. MySQL サービスを起動します。

```
# STA start mysql
```

- b. バックアップファイルを作成します。

```
# /usr/bin/mysqldump -uroot -p --opt --routines --triggers --events --flush-logs --single-transaction --complete-insert --comments --dump-date --add-drop-database --databases stadb -v > /sta_db_backup/backup_filename.sql
Enter password: mysql_root_password
```

出力は、次のようになります。

```
...
-- Retrieving view structure for table v_mdv_request_states...
-- Retrieving view structure for table version_info...
...
-- Disconnecting from localhost...
```

注:

「Can't connect to local MySQL server」が表示される場合、MySQL サーバーは実行中ではありません。手順 a に戻り、MySQL が起動していることを確認してください。

4. 次の手順ですべての STA ファイルが削除されるため、サービスログスナップショットとデータベーススナップショットを別のサーバーに移動します。これらのスナップショットは、次のディレクトリに格納されています。
 - サービスログスナップショットは `/Oracle_storage_home/Middleware/rda/snapshots` にあります。たとえば、`/Oracle/Middleware/rda/snapshots` です
 - データベーススナップショットは、STA のインストール中に指定されたデータベースの場所にあります。たとえば、`/dbbackup` です
5. 必要に応じて、ほかのファイルをバックアップします。
6. STA をアンインストールします。手順については、[「STA のアンインストール」](#)を参照してください。

7. STA を再インストールします。手順については、[3章「STA のインストール」](#)を参照してください。
8. すべての STA サービスを停止します。

STA stop all

9. データベースを復元します。手順については、『[STA 管理ガイド](#)』を参照してください。
10. すべての STA サービスを起動します。

STA start all

11. STA を構成します。手順については、[「STA での SNMP 設定の構成」](#)を参照してください。

STA グラフィカルインストーラおよびアンインストーラの画面リファレンス

この章には次のセクションが含まれます。

- [グラフィカルモードの表示要件](#)
- [STA グラフィカルインストーラの画面](#)
- [STA グラフィカルアンインストーラの画面](#)

A.1. グラフィカルモードの表示要件

STA のグラフィカルモードのインストーラとアンインストーラには、X Window System, version 11 (X11) が必要です。X11 の構成はこのガイドでは扱っていませんが、次の一般的なガイドラインが適用されます。詳細は、システム管理者にお問い合わせください。

グラフィカルモードのインストーラとアンインストーラを実行する場合は、X11 サービスが STA サーバーで実行され、X11 転送を許可するように構成されている必要があります。[2章「Linux のインストール」](#)の指示に従って Linux をインストールした場合、これらの条件はすでに満たされているはずです。

また、X11 承認およびディスプレイを Oracle インストールユーザー用に正しく設定する必要があります。この処理方法は、ユーザーがローカル接続とリモート接続のどちらでログインしているかによって異なります。

詳細は、次の各セクションを参照してください。

- [「ローカル接続」](#)
- [「Secure Shell \(SSH\) を使用したリモート接続」](#)
- [「デスクトップ共有を使用したリモート接続」](#)
- [「グラフィカル表示上の問題のトラブルシューティング」](#)

注:

リモート接続のレスポンス時間は、ネットワークと VPN の構成やパフォーマンスによって異なります。

A.1.1. ローカル接続

STA サーバーへの直接接続では、Oracle インストールユーザーとしてログインしてから、手動で `DISPLAY` 変数を設定する必要があります。例:

```
# export DISPLAY=hostname:0.0
```

また、場合により、Oracle インストールユーザーに適切な X11 承認があることを確認する必要があります。これについては、Linux 管理者に問い合わせてください。

A.1.2. Secure Shell (SSH) を使用したリモート接続

X11 転送を有効にして Secure Shell (SSH) を使用する場合、ログインユーザーの X11 承認およびディスプレイは自動的に処理されます。たとえば、この方法で `oracle` ユーザーとしてログインすると、STA サーバーの SSH サービスによって、`oracle` ユーザーに適した X11 承認およびディスプレイが自動的に設定されます。`DISPLAY` 変数を手動で設定しないようにしてください。

ただし、別のユーザー (`root` など) としてログインしたあと、`su` コマンドで `oracle` に切り替えた場合、`oracle` ユーザーの X11 承認およびディスプレイは正しく設定されないため、手動で設定する必要があります。この操作手順については、このガイドでは扱っていないため、Linux 管理者に問い合わせてください。

A.1.2.1. Linux マシンからの接続

Linux マシンで X11 転送を有効にするには、`ssh` コマンドを `-X` または `-Y` オプション付きで使用します。例:

```
$ ssh -X oracle@sta_server
```

A.1.2.2. Microsoft Windows PC からの接続

使用している PC では、X11 サーバー (Xming や Cygwin/X など) と SSH クライアント (PuTTY や WinSCP など) が動作している必要があります。PuTTY を使用した接続手順の例を次に示します。

1. 使用している PC で X11 サーバーが動作していることを確認します。必要に応じて、システム管理者に連絡してください。
2. PuTTY を起動し、次のように進みます。
 - a. メインの「セッション」ウィンドウで、次の入力を行います。

- 「ホスト名」フィールドで、STA サーバーの名前または IP アドレスを入力します。
 - 「接続タイプ」フィールドで、「SSH」を選択します。
- b. 「カテゴリ」メニューツリーで、「接続」を展開してから、「SSH」を展開して、「X11」を選択します。このウィンドウで、次の選択をします。
- 「X11 フォワーディング」フィールドで、「X11 フォワーディングを有効にする」チェックボックスを選択します。
 - 「リモート X11 認証プロトコル」フィールドで、「MIT-Magic-Cookie-1」を選択します。
 - その他のフィールドは空白のままにします。

A.1.3. デスクトップ共有を使用したリモート接続

デスクトップ共有を通じて STA インストーラを実行するには、STA サーバーとローカルコンピュータの両方でデスクトップ共有アプリケーションを実行する必要があります (たとえば、STA サーバーで VNC Server を実行し、ローカルコンピュータで VNC Viewer を実行する)。また、ローカルコンピュータが仮想プライベートネットワーク (VPN) などのプライベートネットワーク経由で STA サーバーに接続できる必要もあります。

VNC を使用した接続プロセスの例を次に示します。

1. VNC Server を STA サーバーにインストールして構成します。
2. VNC Viewer をローカルコンピュータにインストールして構成します。
3. プライベートネットワーク経由で STA サーバーに接続します。手順については、IT 管理者に問い合わせてください。

A.1.4. グラフィカル表示上の問題のトラブルシューティング

STA インストーラおよびアンインストーラは、X11 が Oracle インストールユーザー用に正しく構成されているかどうかを検証します。これらの前提条件チェックに失敗する場合は、Linux システム管理者に連絡してください。次の手順は、問題のトラブルシューティングに役立ちます。

1. Oracle インストールユーザーとして STA サーバーにログインし、現在インストールされている RPM パッケージを表示します。

```
# yum list installed
```

表示されたリストの中に `xorg - x11 - util` エントリが含まれているはずです。例:

```
xorg-x11-utils.x86_64
```

```
7.5-6.el6
```

- Oracle インストールユーザーの現在のディスプレイ設定を表示します。例:

```
$ echo $DISPLAY
:0.0
```

- ディスプレイに正しい X11 構成が含まれていることを確認します。例:

```
$ xdpinfo -display :0.0
```

[例A.1「正しく構成された X11 ディスプレイの例」](#)は、正しく構成されたディスプレイを示すコマンド出力の最初の部分の例です。

例A.1 正しく構成された X11 ディスプレイの例

```
$ xdpinfo
name of display:      :0.0
version number:      11.0
vendor string:       The X.Org Foundation
vendor release number:  11300000
X.Org version: 1.13.0
maximum request size: 16777212 bytes
motion buffer size:  256
...
```

[例A.2「正しく構成されていない X11 ディスプレイの例」](#)は、正しく構成されていないディスプレイからのコマンド出力の一部の例を示しています。

例A.2 正しく構成されていない X11 ディスプレイの例

```
$ xdpinfo
xdpinfo: unable to open display ":0.0".
```

```
$ xdpinfo
PuTTY X11 proxy: MIT-MAGIC-COOKIE-1 data did not matchxdpinfo: unable to open
display ":0.0".
```


A.2. STA グラフィカルインストーラの画面

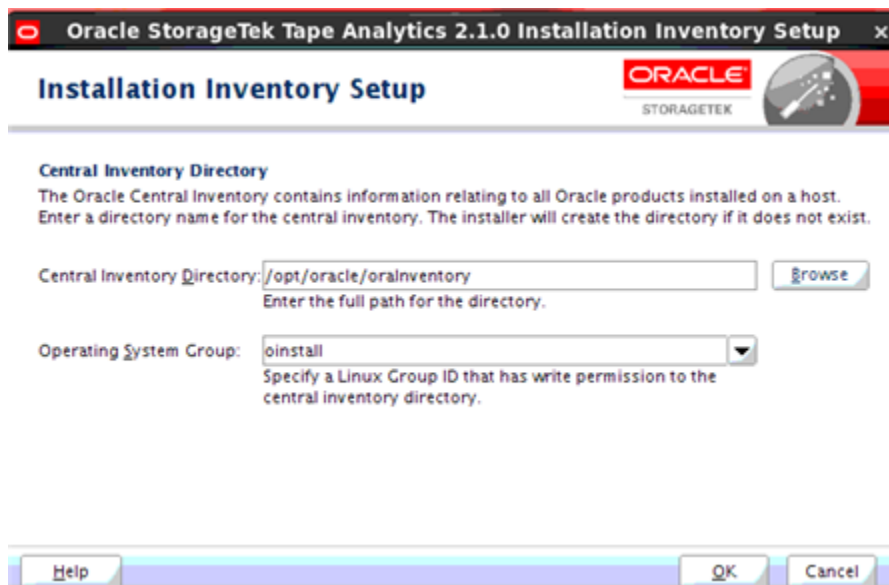
このセクションでは、STA グラフィカルインストーラの各画面について詳しく見ていきます。

- 「ようこそ」
- 「インストール場所」
- 「前提条件チェック」
- 「ルートパスワードの入力」
- 「DB ディレクトリの設定」
- 「管理者アカウントの設定」
 - 「WebLogic 管理者」
 - 「STA 管理者」
- 「データベースアカウントの設定」
 - 「データベースルートユーザー」
 - 「データベースアプリケーションユーザー」
 - 「データベースレポートユーザー」
 - 「データベース管理者」
- 「通信ポートの入力」
 - 「WebLogic 管理コンソール」
 - 「STA エンジン」
 - 「STA アダプタ」
 - 「STA UI」
- 「診断エージェント」
- 「インストールサマリー」
- 「インストールの進行状況」
- 「構成の進行状況」
- 「インストール完了」

注:

STA グラフィカルインストーラを起動すると、Oracle Universal Installer でいくつかの基本的な環境チェックが行われるときにメッセージが端末ウィンドウに表示されます。STA グラフィカルインストーラを実行するための要件がこれらの最小チェックを上回ることがあります。

A.2.1. インストールおよびインベントリの設定



Oracle 中央インベントリディレクトリは、このサーバーにインストールされているすべての Oracle ソフトウェアの名前と場所を把握しておくために使用されます。STA のインストールログとアンインストールログはすべてこの場所に自動的に保存されます。

Oracle インストールグループのほかのユーザーがこのディレクトリにアクセスできるようにするために、それを Oracle インストールユーザーのホームディレクトリと区別することをお勧めします。ホームディレクトリには、Oracle インストールグループに対する適切なアクセス権がない場合があります。

この画面は Oracle Universal Installer の一部です。Oracle 中央インベントリの場所を登録するための推奨方法に従えば、この画面は STA をこのサーバーにはじめてインストールするときのみ表示されます。それ以降のインストールでは、ユーザーに入力を求めることなくその場所を自動的に検出します。詳細は、「[Oracle 中央インベントリの場所の登録](#)」を参照してください。

A.2.1.1. 画面のフィールド

Inventory Directory

Oracle 中央インベントリディレクトリに指定するディレクトリの名前を入力します。

デフォルトは `$USER_HOME/oraInventory` です。絶対パスを指定するか、「**Browse**」ボタンをクリックして既存のディレクトリに移動します。

- 既存のディレクトリを指定する場合、Oracle インストールユーザーにはそのディレクトリへのフルアクセス権が必要です。

- 存在しないディレクトリを指定した場合、インストーラは Oracle インストールユーザーにその親ディレクトリへのフルアクセス権があれば、それを自動的に作成します。

Operating System Group

Oracle インストールグループに指定する Linux グループを選択します。このグループのメンバーはすべて、Oracle ソフトウェアをこのサーバーにインストールできます。

このメニューには、Oracle インストールユーザーが属しているすべてのグループが一覧表示されます。デフォルトは、Oracle インストールユーザーのプライマリグループです。

A.2.1.2. 画面固有のボタン

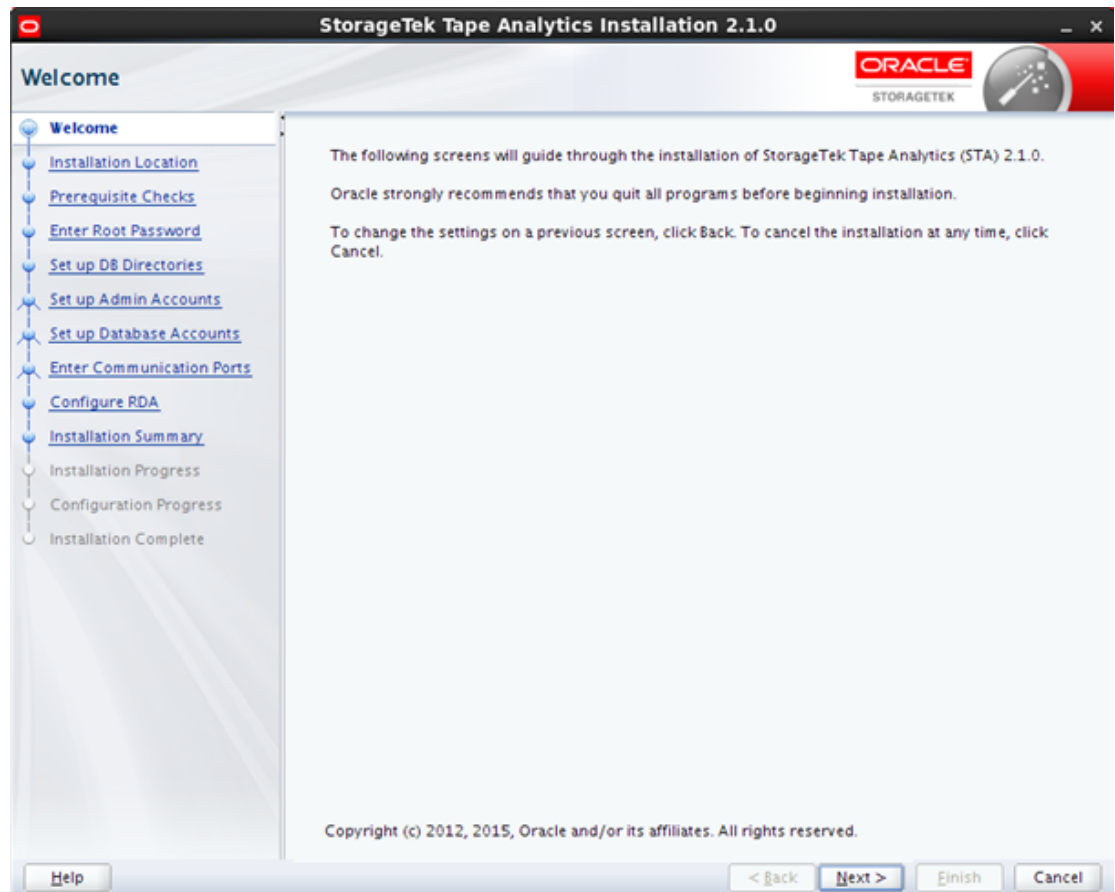
Browse

これをクリックすると、指定するディレクトリに移動できます。

OK

これをクリックすると、STA インストーラが開始されます。「Installation Inventory Setup」ウィンドウが閉じてから、STA インストーラのスプラッシュ画面が表示されるまでわずかな遅れが生じることがあります。

A.2.2. ようこそ



この画面には、STA インストーラを実行するための一般情報が表示されます。テキストを読んだら、「Next」をクリックしてインストールを開始します。

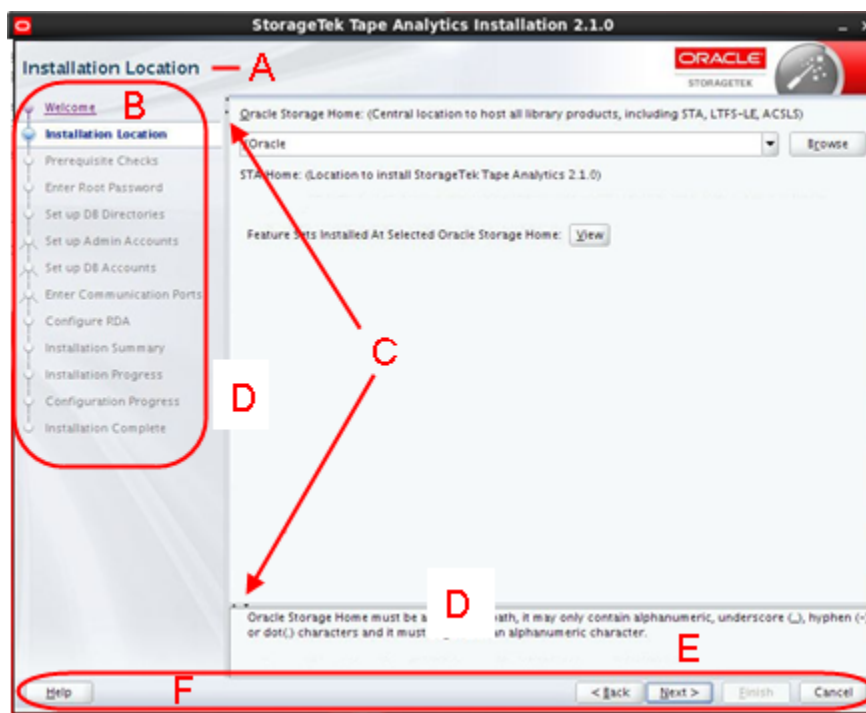
注:

STA インストーラのすべての入力画面を完了し、「インストールサマリー」で「Install」をクリックするまで、システムの変更は行われません。それ以前であればいつでも、前の画面に戻って入力内容を変更できます。

STA インストーラの画面の詳細は、「インストーラの一般的な画面レイアウト」を参照してください。

A.2.2.1. インストーラの一般的な画面レイアウト

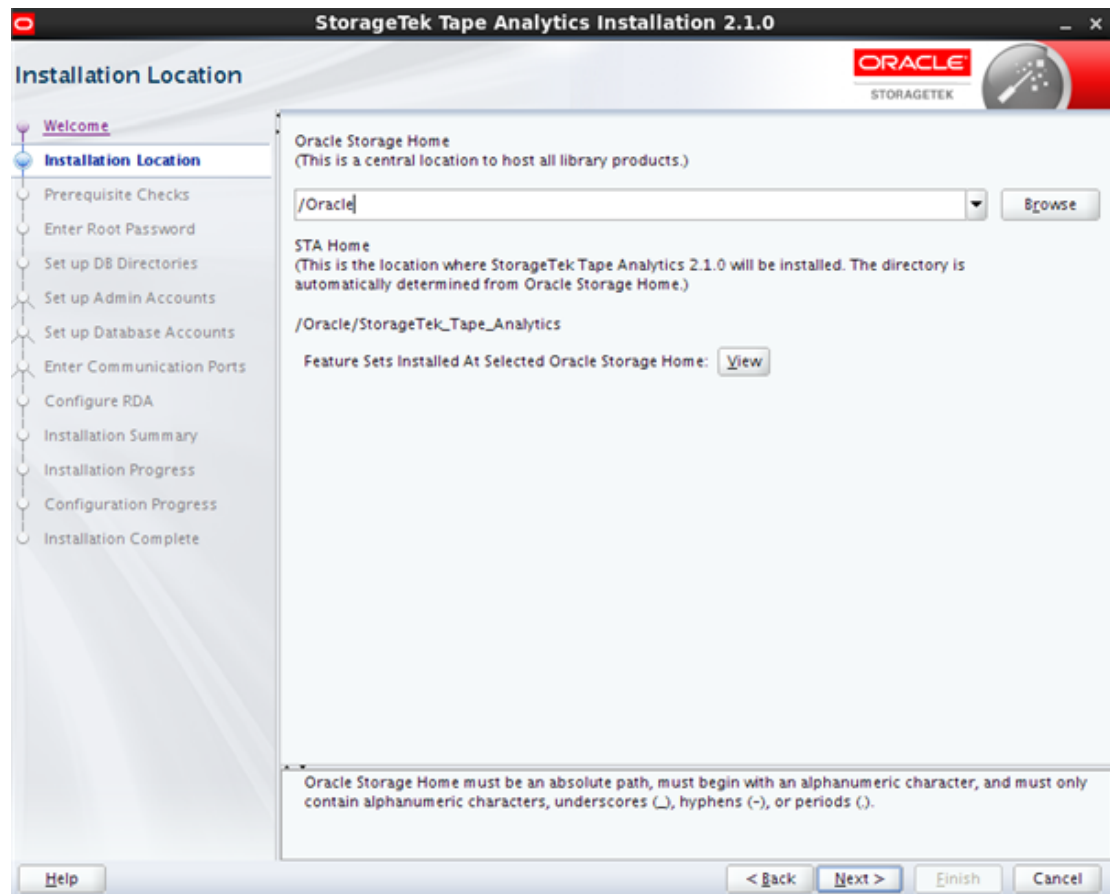
STA インストーラのすべての画面は、同一の基本レイアウトに従っています。主な部分について、次に図示および説明します。



項目	名前	説明
A	画面のタイトル	STA インストーラ画面のタイトル
B	ナビゲーションツリー	インストールシーケンスにおける現在の位置を表示します。各画面を完了すると、画面タイトルがアクティブリンクになります。任意のアクティブリンクをクリックすると、その画面に直接戻り、入力内容を確認または変更できます。
C	展開および縮小アイコン	これをクリックすると、ナビゲーションツリーやメッセージペインを非表示または表示できます。

項目	名前	説明
D	サイズ変更コントロールバー	これをクリックしてドラッグすると、ナビゲーションツリーやメッセージペインのサイズを変更できます。
D	メッセージペイン	選択した画面の中に含まれています。その画面で実行されるプロセスに関連したステータスメッセージを表示します。
E	共通のボタン	次のボタンは、STA インストーラのすべての画面に共通しています。 <ul style="list-style-type: none">• Help - これをクリックすると、その画面のコンテキスト依存ヘルプが表示されます。• Back - これをクリックすると、前の画面に戻って入力内容を確認または変更できます。インストールの先頭まで一度に 1 画面ずつ戻ることができます。• Next - 必要な入力を行なったあとで、これをクリックすると、次の画面に進めます。• Finish - これをクリックすると、インストールを完了できます。このボタンは最終画面でのみアクティブになります。• Cancel - これをクリックすると、いつでもインストールを取り消せます。インストールの一部が完了している場合、インストーラはインストールをロールバックして、サーバーを元の状態に戻します。取り消しを確認するよう求められます。

A.2.3. インストール場所



この画面を使用すると、STA とそれに関連する Oracle ソフトウェアがインストールされるサーバー上の場所を指定できます。

以前にインストールされた STA バージョン上にインストールすることはできません。STA が特定の場所にまだインストールされていないことを確認するには、「**Oracle Storage Home**」フィールドにディレクトリを入力して、「**View**」ボタンをクリックします。

- その場所にソフトウェアがインストールされていない場合、リストは空白になります。
- ソフトウェアがインストールされている場合、[図A.1「Oracle ストレージホームのリストの例」](#)に示すように一覧表示されます。

A.2.3.1. 画面のフィールド

Oracle Storage Home

STA とそれに関連する Oracle ソフトウェアがインストールされるディレクトリを入力します。各ソフトウェアパッケージは、このディレクトリ内の独自のサブディレクトリにインス

トールされます。STA がすでにインストールされているディレクトリを指定することはできません。

このディレクトリに関する技術的な推奨事項は、[表2.2「推奨されるファイルシステムレイアウト」](#)を参照してください。

このディレクトリがすでに存在するかどうかによって、Oracle インストールユーザーとグループには次のアクセス権が必要になります。

- ディレクトリが存在する場合は、そのディレクトリへのフルアクセス権が必要です。
- ディレクトリが存在しない場合は、STA インストーラが Oracle ストレージホームディレクトリを作成できるように、親ディレクトリへのフルアクセス権が必要です。

絶対パスを指定するか、「**Browse**」ボタンをクリックして指定するディレクトリに移動します。

STA Home

表示専用。これは、STA がインストールされる Oracle ストレージホーム内のサブディレクトリです。このディレクトリには *StorageTek_Tape_Analytics* という名前が割り当てられ、インストール中に自動的に作成されます。

A.2.3.2. 画面固有のボタン

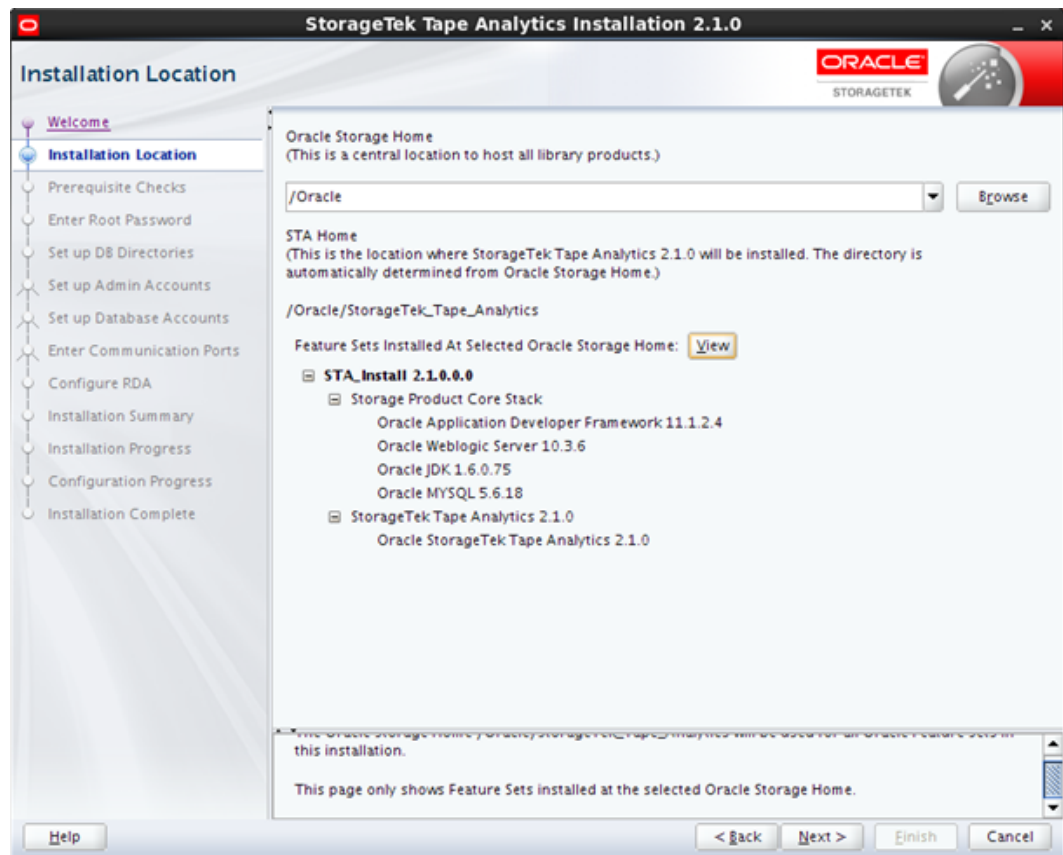
Browse

これをクリックすると、指定するディレクトリに移動できます。

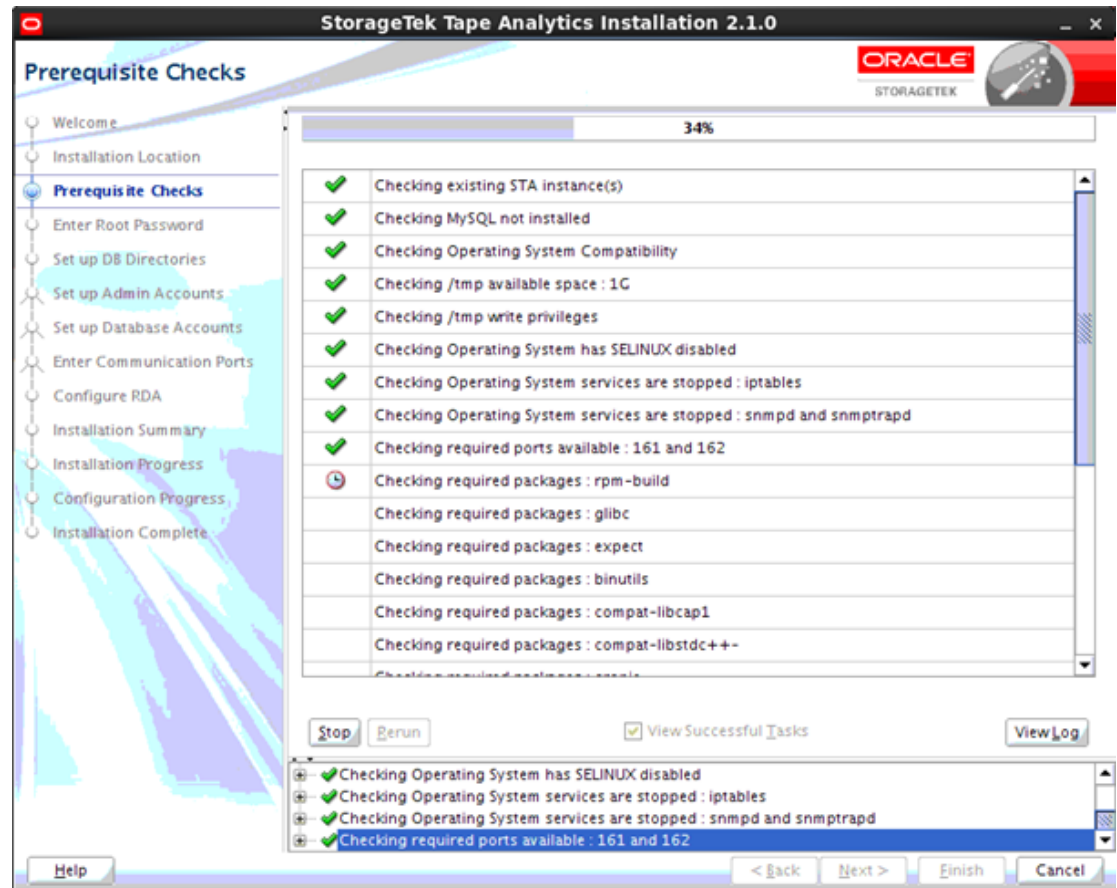
View

これをクリックすると、指定した Oracle ストレージホームディレクトリに現在インストールされているすべてのソフトウェアのリストが表示されます。新規インストールの場合、このリストは空白です。[図A.1「Oracle ストレージホームのリストの例」](#)は、STA をインストールしたあとの表示の例です。

図A.1 Oracle ストレージホームのリストの例



A.2.4. 前提条件チェック



インストーラは、サーバー環境が必須および推奨される前提条件をすべて満たしているかどうかを検証するための一連のタスクを実行します。このプロセスには数分かかる場合があります。

各検証タスクの考えられる結果は次のとおりです。

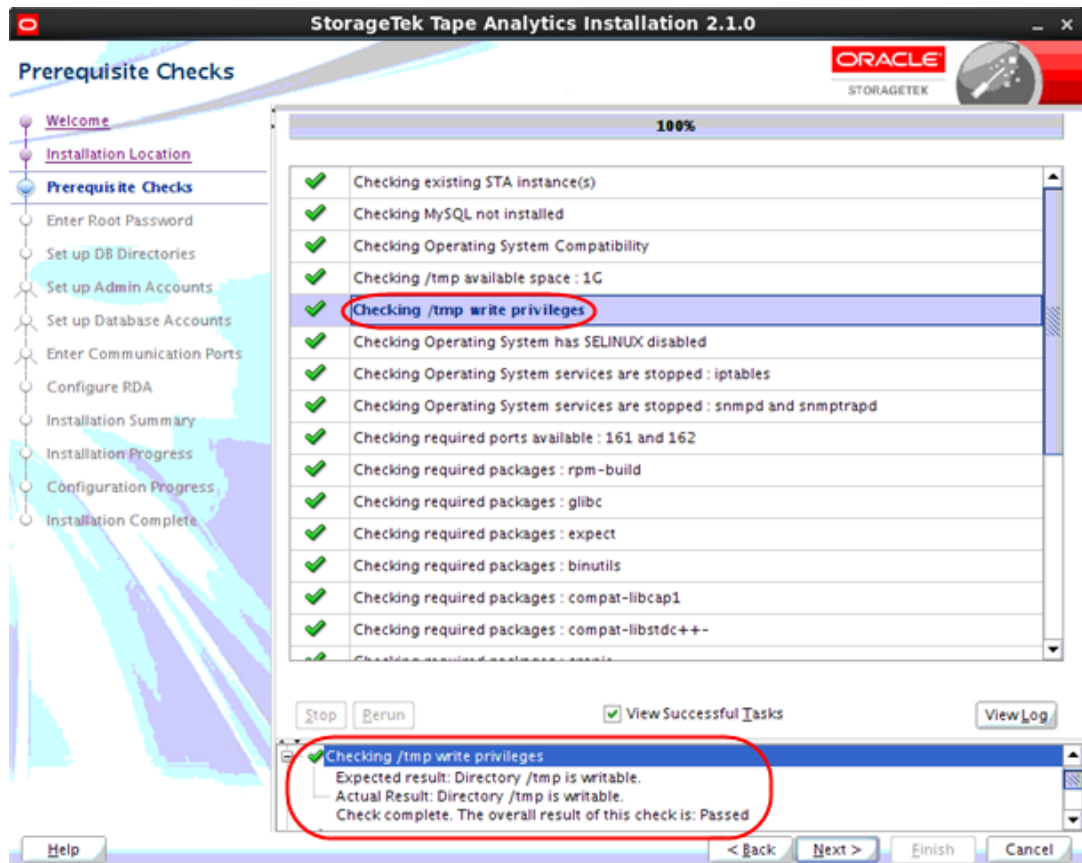
- 成功 - 前提条件のチェックに正常に合格しました。
- 警告 - 推奨される前提条件のチェックに合格しませんでした。
- 失敗 - 必須の前提条件のチェックに合格しませんでした。

いずれかの結果が失敗である場合は、インストールを続行できません。また、続行する前に、警告の結果をすべて解決することをお勧めします。問題を解決している間もインストーラをこの画面で起動しておき、その後復帰し、「**Rerun**」をクリックして検証プロセスを再度実行することができます。

前提条件の性質によっては、問題を解決するためにサービスの停止、ユーザー権限の変更、または yum パッケージのインストールが必要になる場合があります。次のどちらかの方法を使用すると、問題のトラブルシューティングや対処方法の判断に役立つ、展開された詳細を表示できます。

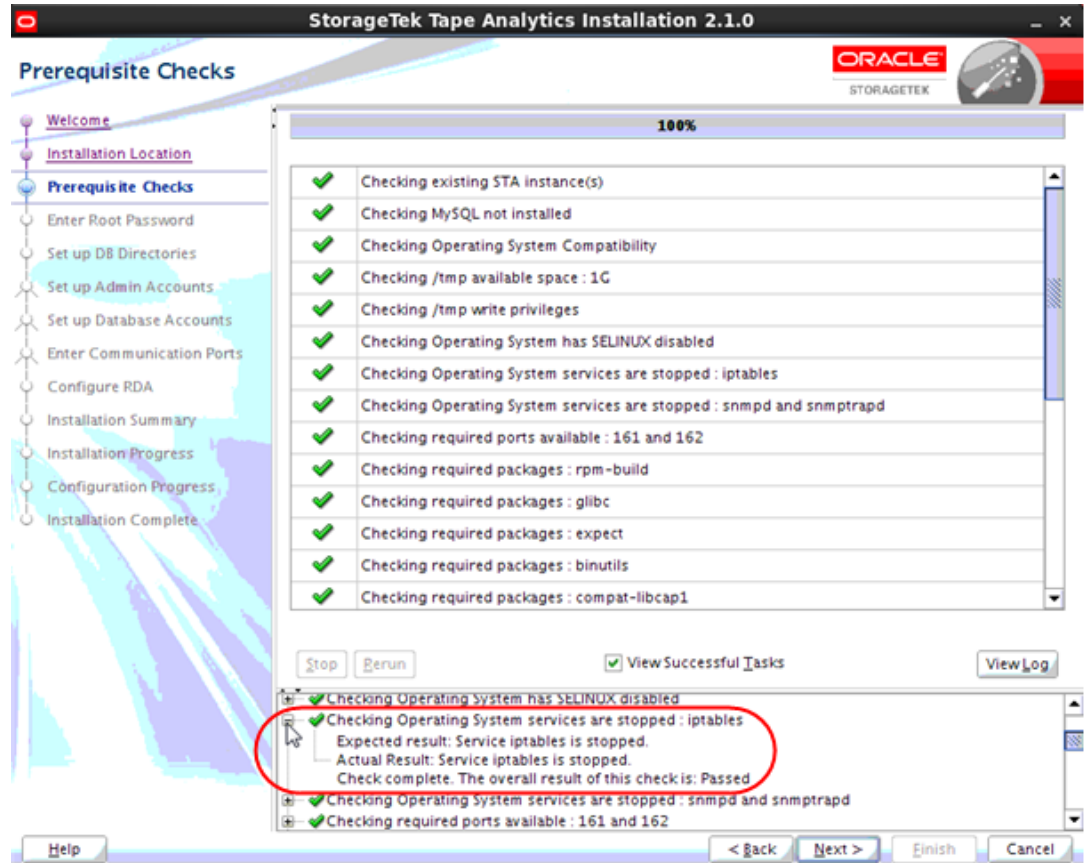
- メインウィンドウ内のタスクを選択します。そのタスクがメッセージペインで強調表示され、展開された詳細が表示されます。図A.2「メインウィンドウ内のタスクを選択することで表示されるタスクの詳細」に例を示します。

図A.2 メインウィンドウ内のタスクを選択することで表示されるタスクの詳細



- メッセージペインで、詳細を表示するタスクの横にある展開 (+) アイコンをクリックします。図A.3「展開アイコンを選択することで表示されるタスクの詳細」に例を示します。縮小 (-) アイコンをクリックすると、再度詳細が非表示になります。

図A.3 展開アイコンを選択することで表示されるタスクの詳細



A.2.4.1. 画面のフィールド

なし

A.2.4.2. 画面固有のボタン

Stop

これをクリックすると、現在のタスクで検証プロセスが停止します。すでに完了している選択されたタスクの詳細を表示できるように、この操作が必要になる場合があります。

Rerun

これをクリックすると、検証プロセスがもう一度最初から実行されます。これにより、STA インストーラを終了したり再起動したりすることなく、失敗または警告の結果を解決できます。

View Successful Tasks

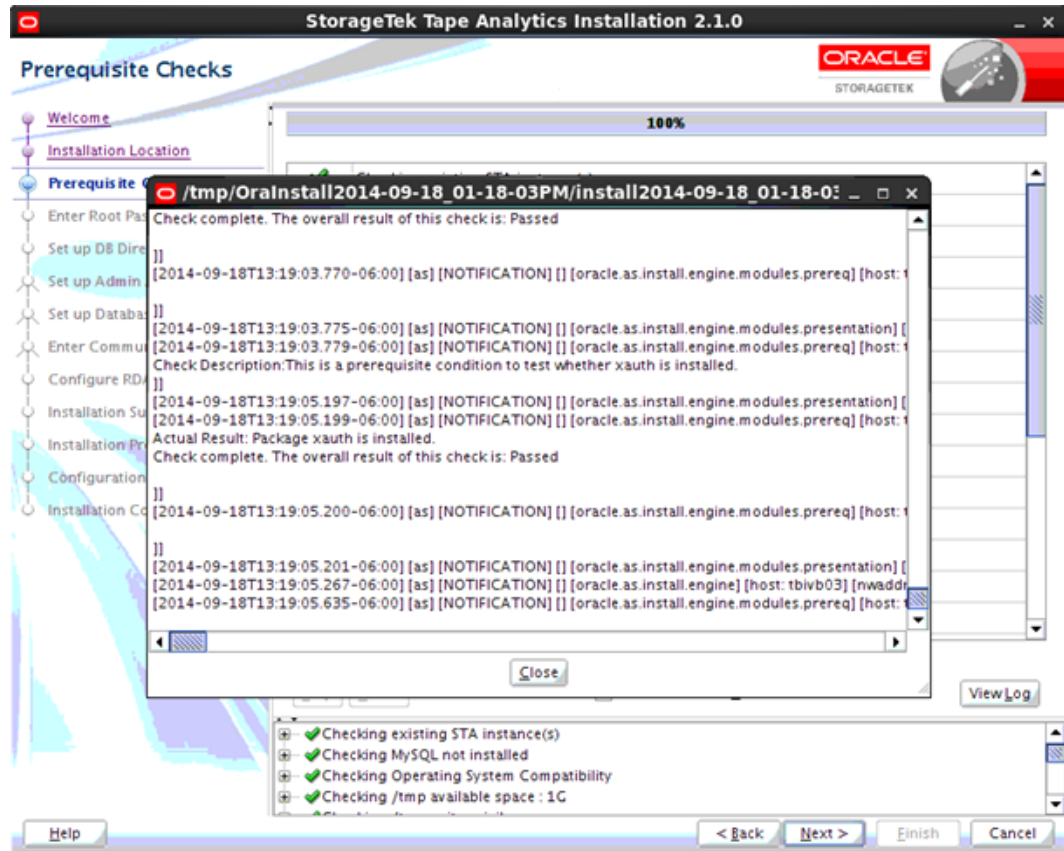
このチェックボックスを選択すると、表示に成功の結果を含めることができます。これはデフォルトです。

このチェックボックスをクリアすると、失敗または警告の結果のみが表示されます。これにより、正常なタスクを除外できるため、注意が必要なタスクに重点的に取り組みます。

View Log

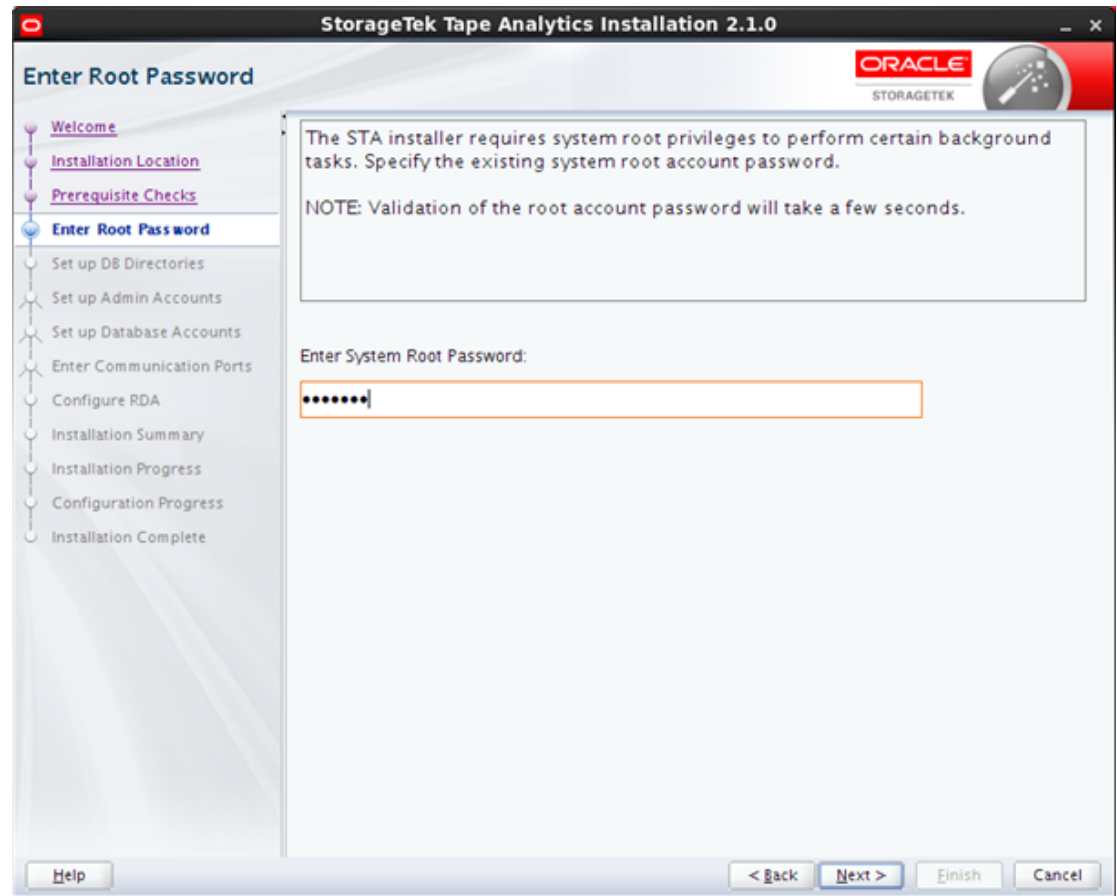
これをクリックすると、前提条件の検証ログが別のウィンドウに表示されます。図A.4「前提条件の検証ログの表示の例」に例を示します。「Close」をクリックすると、そのログウィンドウが閉じます。

図A.4 前提条件の検証ログの表示の例



Linux コマンド行からログを表示することもできます。インストーラの実行中は、`/tmp` 内のサブディレクトリにログが保存されます。詳細は、「[STA のインストールおよびアンインストールのログ](#)」を参照してください。

A.2.5. ルートパスワードの入力



STA インストーラでインストールを実行するためには Linux root アクセス権が必要です。

A.2.5.1. 画面のフィールド

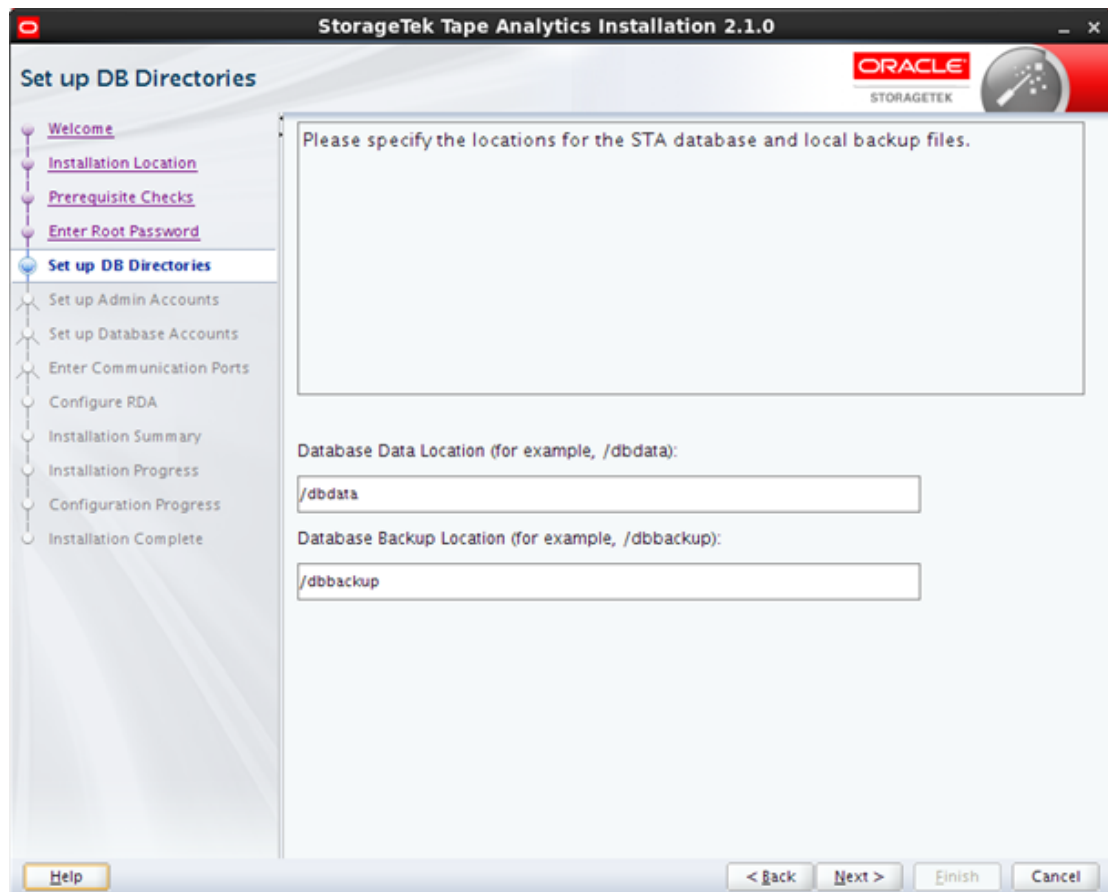
Enter Root Password

Linux root ユーザーのパスワードを入力します。入力中にエントリがマスクされます。パスワードの検証に数秒かかる場合があります。

A.2.5.2. 画面固有のボタン

なし

A.2.6. DB ディレクトリの設定



この画面では、STA データベースとローカルの STA データベースバックアップの場所を指定できます。STA インストーラでは、これらのディレクトリが存在しない場合は作成します。

データベースサービスおよびバックアップの管理については、『STA 管理ガイド』を参照してください。

A.2.6.1. 画面のフィールド

Database Data Location

STA データベースが置かれるディレクトリを入力します。このディレクトリを「**Database Backup Location**」と同じにすることはできません。絶対パスを指定する必要があります。

指定したディレクトリにすでにデータベース用サブディレクトリ (*mysql*) が含まれている場合は、警告メッセージが表示されます。別のデータベースの場所を指定することも、現在のエントリを受け入れることもできます。後者の場合、STA のインストール中にデータベース用サブディレクトリが削除されます。

Database Backup Location

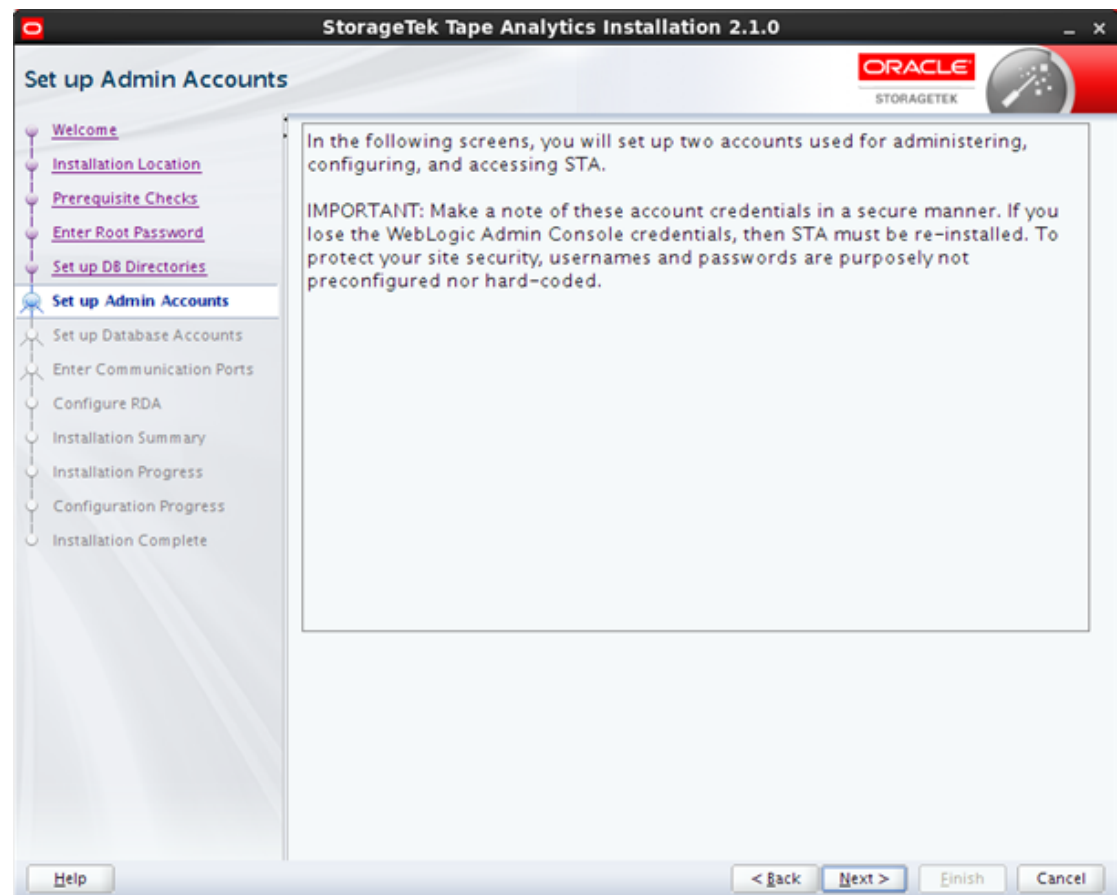
STA データベースバックアップが置かれるサーバー上のディレクトリを入力します。このディレクトリを「**Database Data Location**」と同じにすることはできません。絶対パスを指定する必要があります。

指定したディレクトリにすでにデータベースバックアップ用サブディレクトリ (*local*) が含まれている場合は、警告メッセージが表示されます。別のバックアップの場所を指定することも、現在のエントリを受け入れることもできます。後者の場合、STA のインストール中にバックアップ用サブディレクトリが削除されます。

A.2.6.2. 画面固有のボタン

なし

A.2.7. 管理者アカウントの設定



この画面は、次の2つの画面で定義する情報の種類について説明しています。テキストを読んだら、「**Next**」をクリックして続行します。

A.2.7.1. 画面のフィールド

なし

A.2.7.2. 画面固有のボタン

なし

A.2.8. WebLogic 管理者

StorageTek Tape Analytics Installation 2.1.0

ORACLE
STORAGETEK

WebLogic Administrator

Welcome
Installation Location
Prerequisite Checks
Enter Root Password
Set up DB Directories
Set up Admin Accounts
-WebLogic Administrator
-STA Administrator
Set up Database Accounts
Enter Communication Ports
Configure RDA
Installation Summary
Installation Progress
Configuration Progress
Installation Complete

Enter a username and password for the WebLogic Admin Console login. This account is limited to administration tasks for WebLogic (the application server that hosts STA) and is infrequently used.

Username Requirements:
- 1 to 16 characters in length
- All usernames must be unique

Password Requirements:
- 8 to 31 characters in length with no spaces
- Must contain at least one capital letter and one number, except:
&'(<>?){}*\'`"

Enter WebLogic Administrator Username:
weblogic

Enter WebLogic Administrator Password:

Confirm WebLogic Administrator Password:

Help < Back Next > Finish Cancel

WebLogic は、STA をホストするアプリケーションサーバーです。WebLogic 管理コンソールにログインし、WebLogic サーバーを構成および管理するには、WebLogic 管理者アカウントを使用します。このアカウントを使用することはまれです。

このアカウントは、指定された資格証明を使ってインストール中に作成されます。

注意:

これらのアカウント資格証明のセキュアな記録を取ってください。それらを紛失すると、WebLogic 管理コンソールにログインできなくなり、STA の再インストールが必要になります。

サイトのセキュリティーを守るため、ユーザー名やパスワードが意図的に再構成されたり、ハードコードされたりすることはありません。

A.2.8.1. 画面のフィールド

Enter Username

WebLogic 管理者アカウントに割り当てる名前を入力します。

ユーザー名の要件は次のとおりです。

- 1–16 文字の長さにする必要があります
- すべてのユーザー名が一意である必要があります

Enter Password

このアカウントに割り当てるパスワードを入力します。入力中にエントリがマスクされます。

パスワード要件は次のとおりです。

- 8–31 文字の長さにする必要があります
- 少なくとも 1 つの数字と 1 つの大文字を含める必要があります
- 空白を含めることはできません
- 次の特殊文字を含めることはできません

& ' () < > ? { } * / ' "

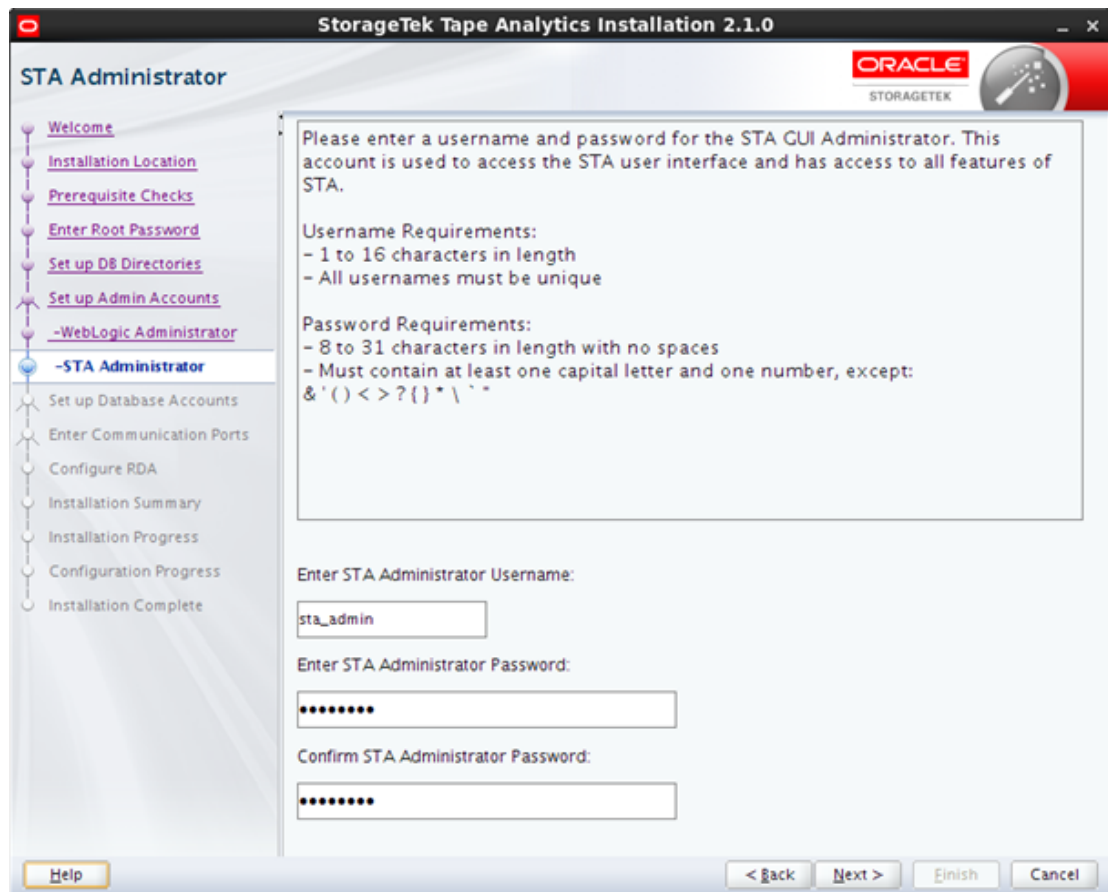
Confirm Password

パスワードを再度入力して、正しく入力したことを確認します。

A.2.8.2. 画面固有のボタン

なし

A.2.9. STA 管理者



STA ユーザーインタフェースにログインするには、STA 管理者アカウントを使用します。このユーザーは STA アプリケーションに対する管理者権限を持っているため、すべての STA 画面にアクセスできます。

このアカウントは、指定された資格証明を使ってインストール中に作成されます。

注意:

これらのアカウント資格証明のセキュアな記録を取ってください。それらを紛失すると、STA ユーザーインタフェースにログインできなくなります。

サイトのセキュリティーを守るため、ユーザー名やパスワードが意図的に再構成されたり、ハードコードされたりすることはありません。

A.2.9.1. 画面のフィールド

Enter Username

STA 管理者に割り当てるユーザー名を入力します。

ユーザー名の要件は次のとおりです。

- 1–16 文字の長さにする必要があります
- すべてのユーザー名が一意である必要があります

Enter Password

このアカウントに割り当てるパスワードを入力します。入力中にエントリがマスクされます。

パスワード要件は次のとおりです。

- 8–31 文字の長さにする必要があります
- 少なくとも 1 つの数字と 1 つの大文字を含める必要があります
- 空白を含めることはできません
- 次の特殊文字を含めることはできません

& ' () < > ? { } * / ' "

Confirm Password

パスワードを再度入力して、正しく入力したことを確認します。

A.2.9.2. 画面固有のボタン

なし

A.2.10. データベースアカウントの設定



この画面は、次の 4 つの画面で定義する情報の種類について説明しています。テキストを読んだら、「Next」をクリックして続行します。

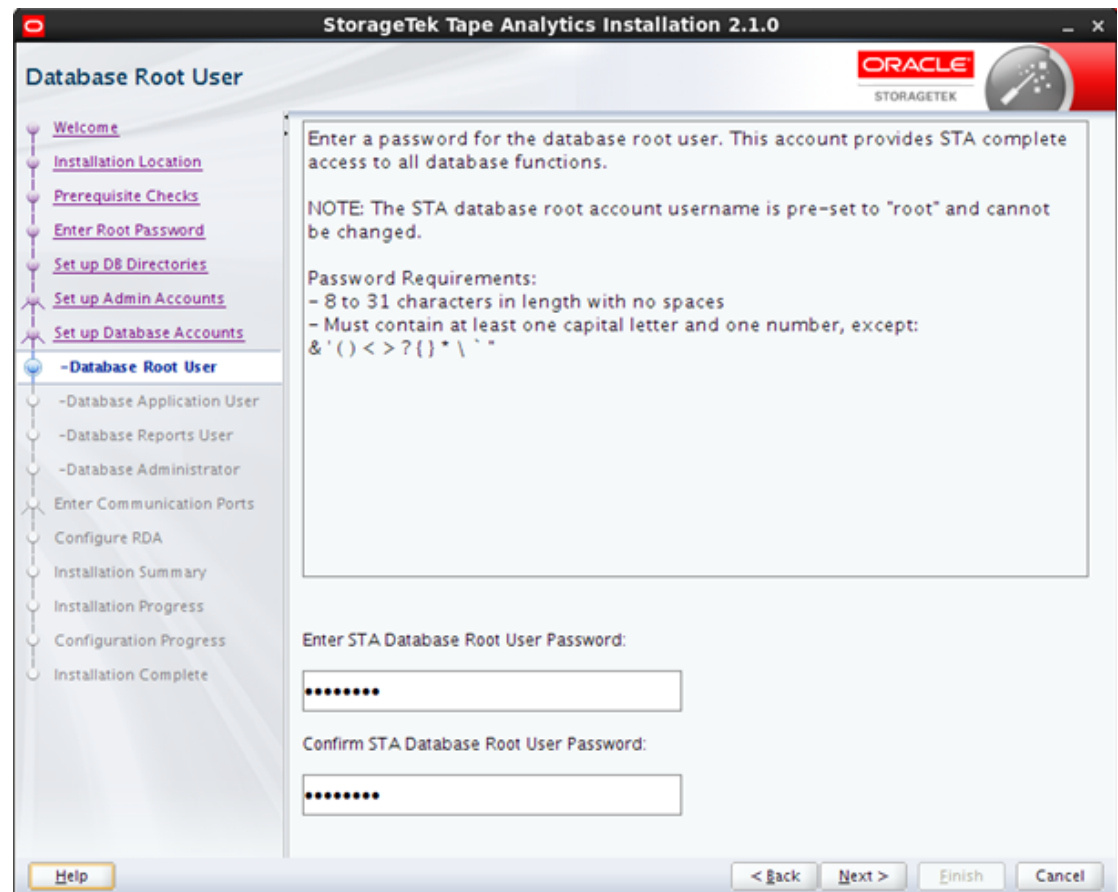
A.2.10.1. 画面のフィールド

なし

A.2.10.2. 画面固有のボタン

なし

A.2.11. データベースルートユーザー



STA データベースルートユーザーは STA データベースを所有します。このアカウントは、STA アプリケーションでデータベースを作成するために内部的に使用され、すべてのデータベーステーブルへのフルアクセス権を提供します。通常の STA 操作では、このアカウントを使用しません。

このアカウントのユーザー名は *root* に自動的に設定され、変更できません。これは MySQL アカウントであり、Linux ルートユーザーとは区別されます。このアカウントは、指定された資格証明を使ってインストール中に作成されます。

注:

これらのアカウント資格証明のセキュアな記録を取ってください。

サイトのセキュリティを守るため、ユーザー名やパスワードが意図的に再構成されたり、ハードコードされたりすることはありません。

A.2.11.1. 画面のフィールド

Enter Password

STA データベースルートユーザーに割り当てるパスワードを入力します。入力中にエンタリがマスクされます。

パスワード要件は次のとおりです。

- 8 – 31 文字の長さにする必要があります
- 少なくとも 1 つの数字と 1 つの大文字を含める必要があります
- 空白を含めることはできません
- 次の特殊文字を含めることはできません

& ' () < > ? { } * / ' "

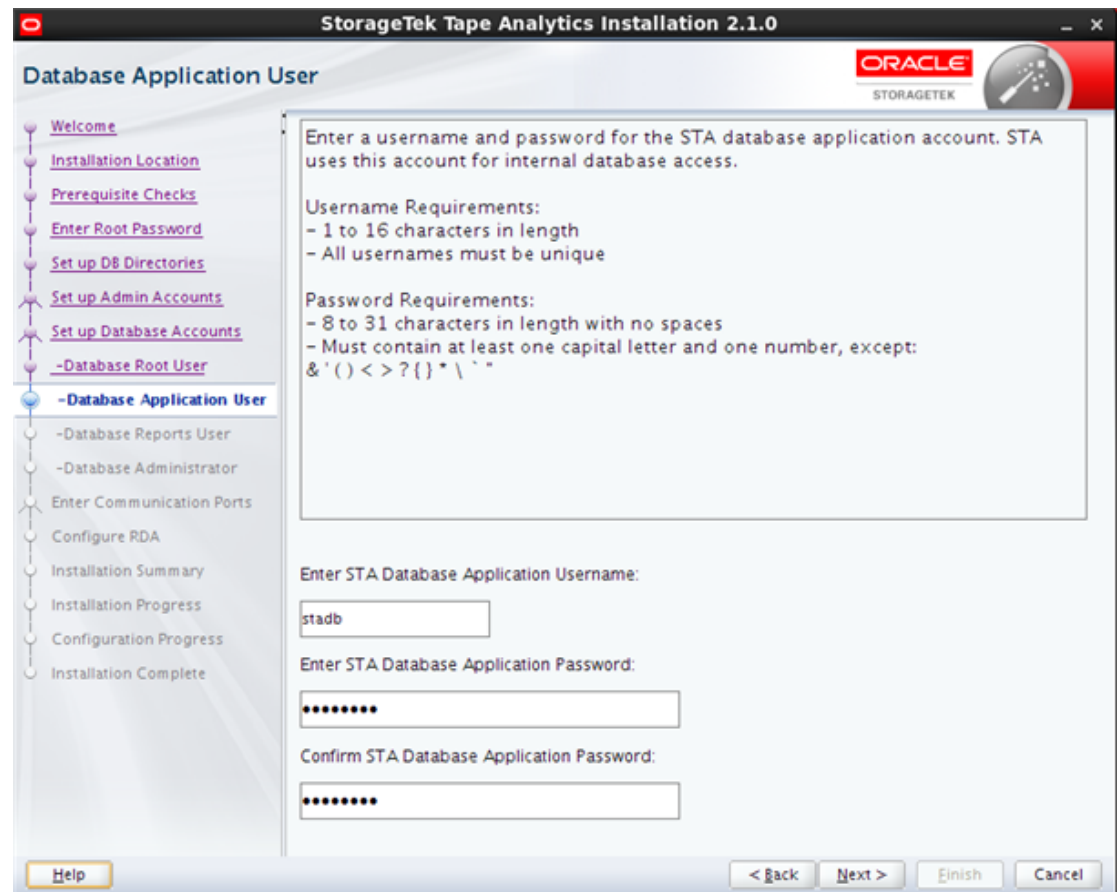
Confirm Password

パスワードを再度入力して、正しく入力したことを確認します。

A.2.11.2. 画面固有のボタン

なし

A.2.12. データベースアプリケーションユーザー



データベースアプリケーションアカウントとは、STA アプリケーションで STA データベースに接続したり、それを更新したりするために内部的に使用される MySQL アカウントです。このアカウントは、すべてのデータベーステーブルへの作成、更新、削除、および読み取りアクセス権を提供します。通常の STA 操作では、このアカウントを使用しません。

このアカウントは、指定された資格証明を使ってインストール中に作成されます。

注:

これらのアカウント資格証明のセキュアな記録を取ってください。

サイトのセキュリティを守るため、ユーザー名やパスワードが意図的に再構成されたり、ハードコードされたりすることはありません。

A.2.12.1. 画面のフィールド

Enter Username

STA データベースアプリケーションアカウントに割り当てる名前を入力します (例: *stadb*)。

ユーザー名の要件は次のとおりです。

- 1–16 文字の長さにする必要があります
- すべてのユーザー名が一意である必要があります

Enter Password

STA データベースアプリケーションアカウントに割り当てるパスワードを入力します。入力中にエントリがマスクされます。

パスワード要件は次のとおりです。

- 8–31 文字の長さにする必要があります
- 少なくとも 1 つの数字と 1 つの大文字を含める必要があります
- 空白を含めることはできません
- 次の特殊文字を含めることはできません

& ' () < > ? { } * / ' "

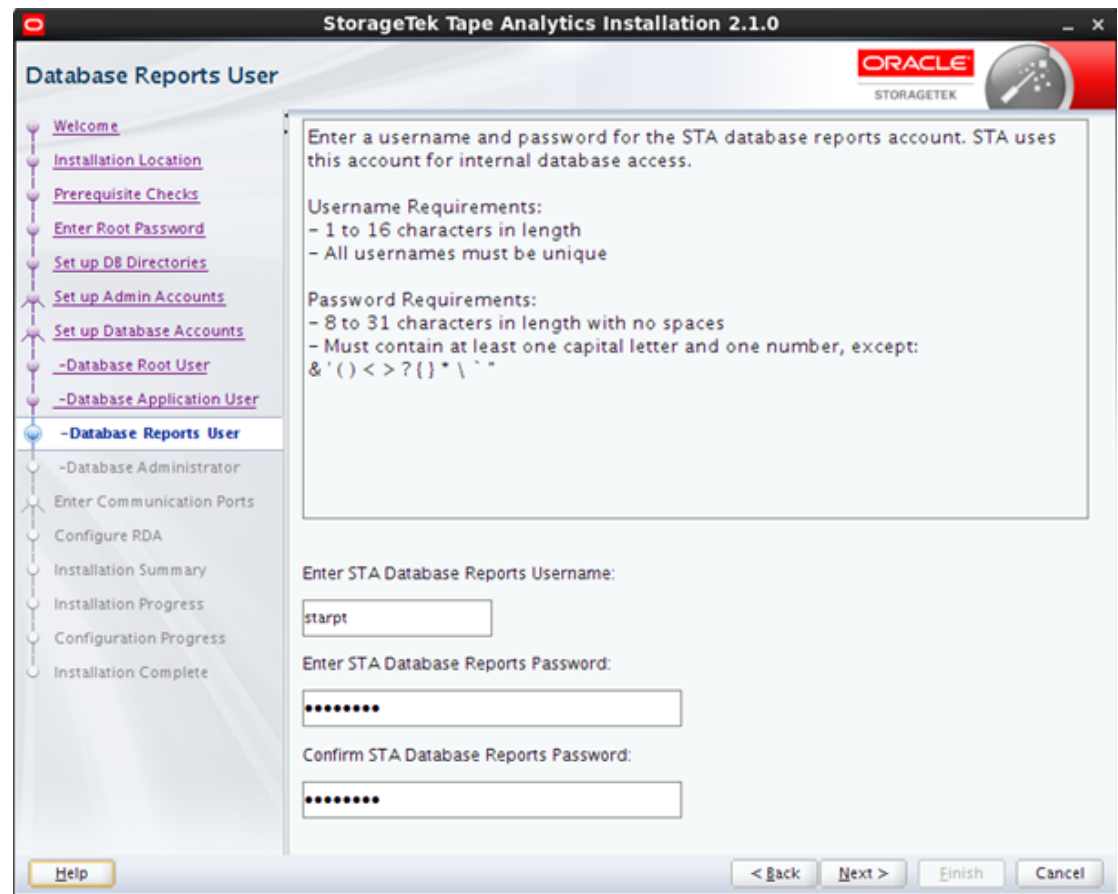
Confirm Password

パスワードを再度入力して、正しく入力したことを確認します。

A.2.12.2. 画面固有のボタン

なし

A.2.13. データベースレポートユーザー



STA データベースレポートアカウントとは、STA 以外のアプリケーションやサードパーティーアプリケーションで STA データベースに接続するために内部的に使用される MySQL アカウントです。このアカウントは、選択されたデータベーステーブルへの読み取り専用アクセス権を提供します。通常の STA 操作では、このアカウントを使用しません。

このアカウントは、指定された資格証明を使ってインストール中に作成されます。

注:

これらのアカウント資格証明のセキュアな記録を取ってください。

サイトのセキュリティを守るため、ユーザー名やパスワードが意図的に再構成されたり、ハードコードされたりすることはありません。

A.2.13.1. 画面のフィールド

Enter Username

STA データベースレポートアカウントに割り当てる名前を入力します (例: *starpt*)。

ユーザー名の要件は次のとおりです。

- 1–16 文字の長さにする必要があります
- すべてのユーザー名が一意である必要があります

Enter Password

このアカウントに割り当てるパスワードを入力します。入力中にエントリがマスクされます。

パスワード要件は次のとおりです。

- 8–31 文字の長さにする必要があります
- 少なくとも 1 つの数字と 1 つの大文字を含める必要があります
- 空白を含めることはできません
- 次の特殊文字を含めることはできません

& ' () < > ? { } * / ' "

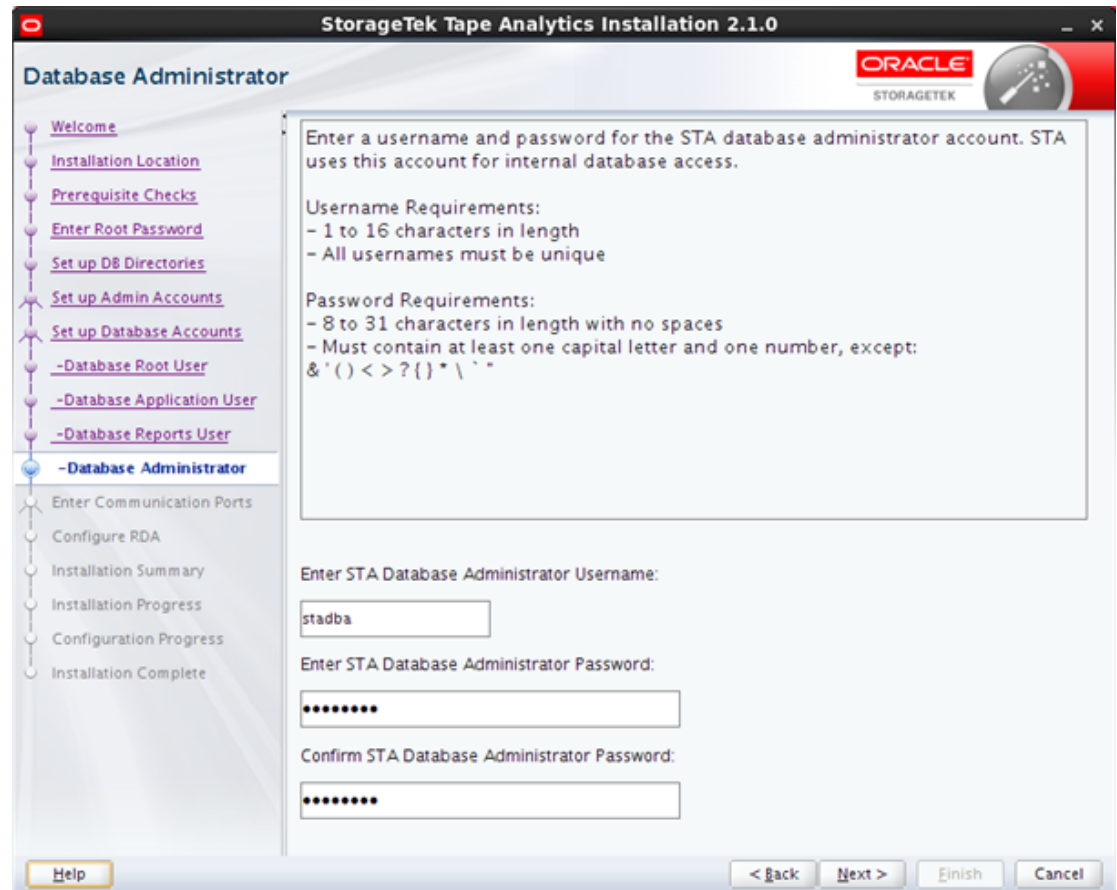
Confirm Password

パスワードを再度入力して、正しく入力したことを確認します。

A.2.13.2. 画面固有のボタン

なし

A.2.14. データベース管理者



STA データベース管理者アカウントとは、STA 管理ユーティリティーやモニタリングユーティリティーで STA データベースに接続したり、スケジュールされたバックアップを構成および実行したりするために内部的に使用される MySQL アカウントです。このアカウントは、すべてのデータベーステーブルへのフルアクセス権（「grant」オプションを除く）を提供します。通常の STA 操作では、このアカウントを使用しません。

このアカウントは、指定された資格証明を使ってインストール中に作成されます。

注:

これらのアカウント資格証明のセキュアな記録を取ってください。

サイトのセキュリティを守るため、ユーザー名やパスワードが意図的に再構成されたり、ハードコードされたりすることはありません。

A.2.14.1. 画面のフィールド

Enter Username

STA データベース管理者アカウントに割り当てる名前を入力します (例: *stadba*)。

ユーザー名の要件は次のとおりです。

- 1–16 文字の長さにする必要があります
- すべてのユーザー名が一意である必要があります

Enter Password

このアカウントに割り当てるパスワードを入力します。入力中にエントリがマスクされます。

パスワード要件は次のとおりです。

- 8–31 文字の長さにする必要があります
- 少なくとも 1 つの数字と 1 つの大文字を含める必要があります
- 空白を含めることはできません
- 次の特殊文字を含めることはできません

& ' () < > ? { } * / ' "

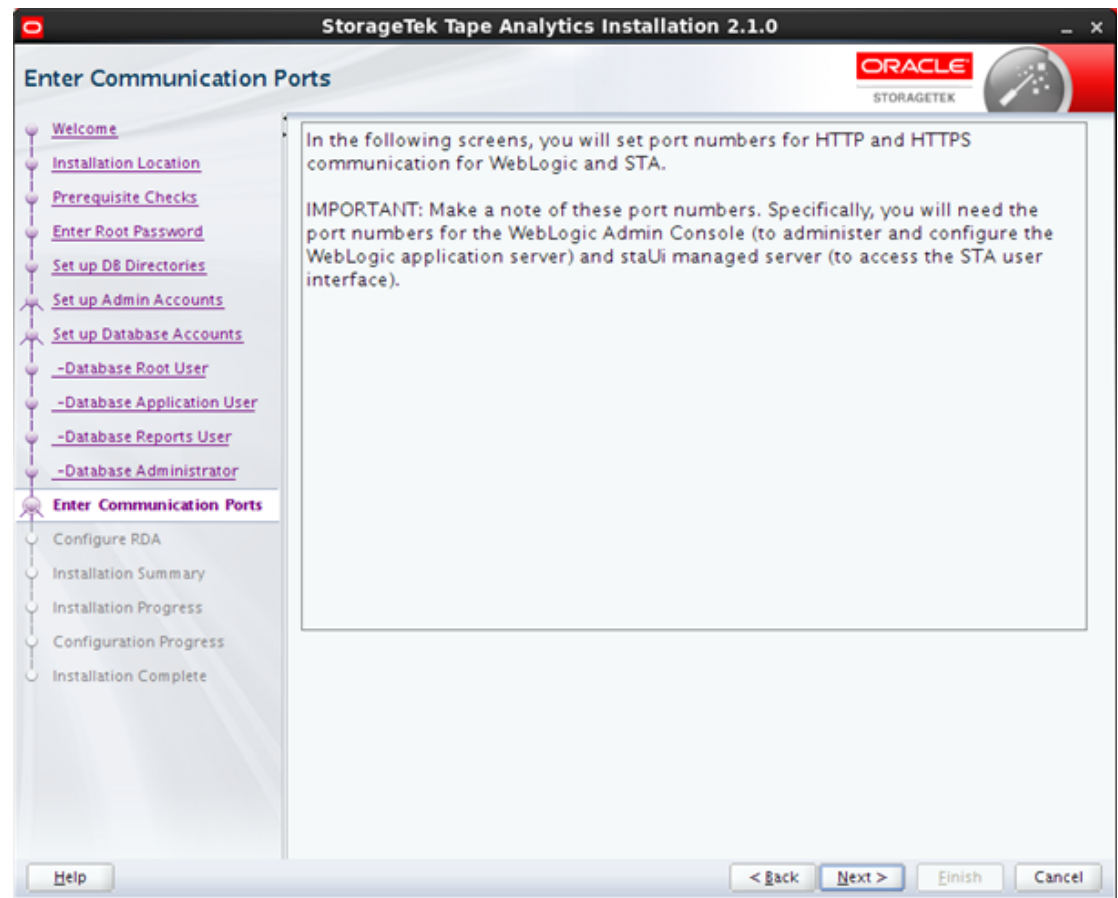
Confirm Password

パスワードを再度入力して、正しく入力したことを確認します。

A.2.14.2. 画面固有のボタン

なし

A.2.15. 通信ポートの入力



この画面は、次の4つの画面で定義する情報の種類について説明しています。テキストを読んだら、「Next」をクリックして続行します。

構成可能な内部および外部の WebLogic ポートと STA ポートの値を指定します。これらのポートは、指定された値を使ってインストール中に構成および有効化されます。指定するポート番号は一意であり、STA で使い続けることができる専用のものである必要があります。

注:

これらの画面の入力を完了する前に、正しいポート番号をネットワーク管理者に確認してください。STA のインストールが完了すると、STA のアンインストールと再インストールを行わずにポート番号を変更することはできません。

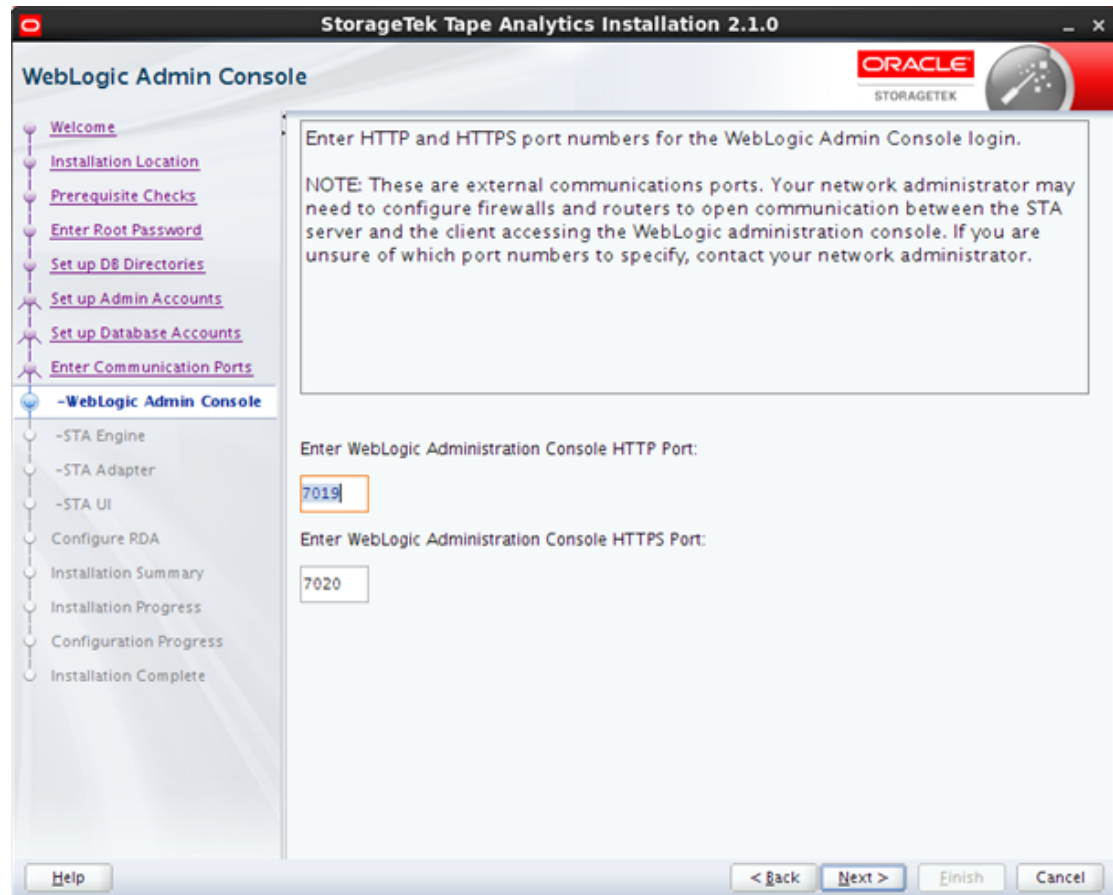
A.2.15.1. 画面のフィールド

なし

A.2.15.2. 画面固有のボタン

なし

A.2.16. WebLogic 管理コンソール



WebLogic アプリケーションサーバーの管理および構成に使用される WebLogic 管理コンソールへのログイン時は、WebLogic 管理コンソールのポート番号を指定します。

注:

これらは外部通信ポートです。ネットワーク管理者は、STA サーバーと、WebLogic 管理コンソールにアクセスするクライアントとの通信を開始するようにファイアウォールやルーターを構成する必要がある場合があります。

注:

これらのポート番号のセキュアな記録を取ってください。STA のインストール後は変更できません。

サイトのセキュリティを守るため、これらの番号が意図的に再構成されたり、ハードコードされたりすることはありません。

A.2.16.1. 画面のフィールド

Enter HTTP Port

WebLogic 管理コンソールログインへのセキュアでないアクセス用の HTTP ポート番号を入力します。通常、このポート番号は 7019 です。

ポート番号は一意で使用可能である必要があります。

Enter HTTPS Port

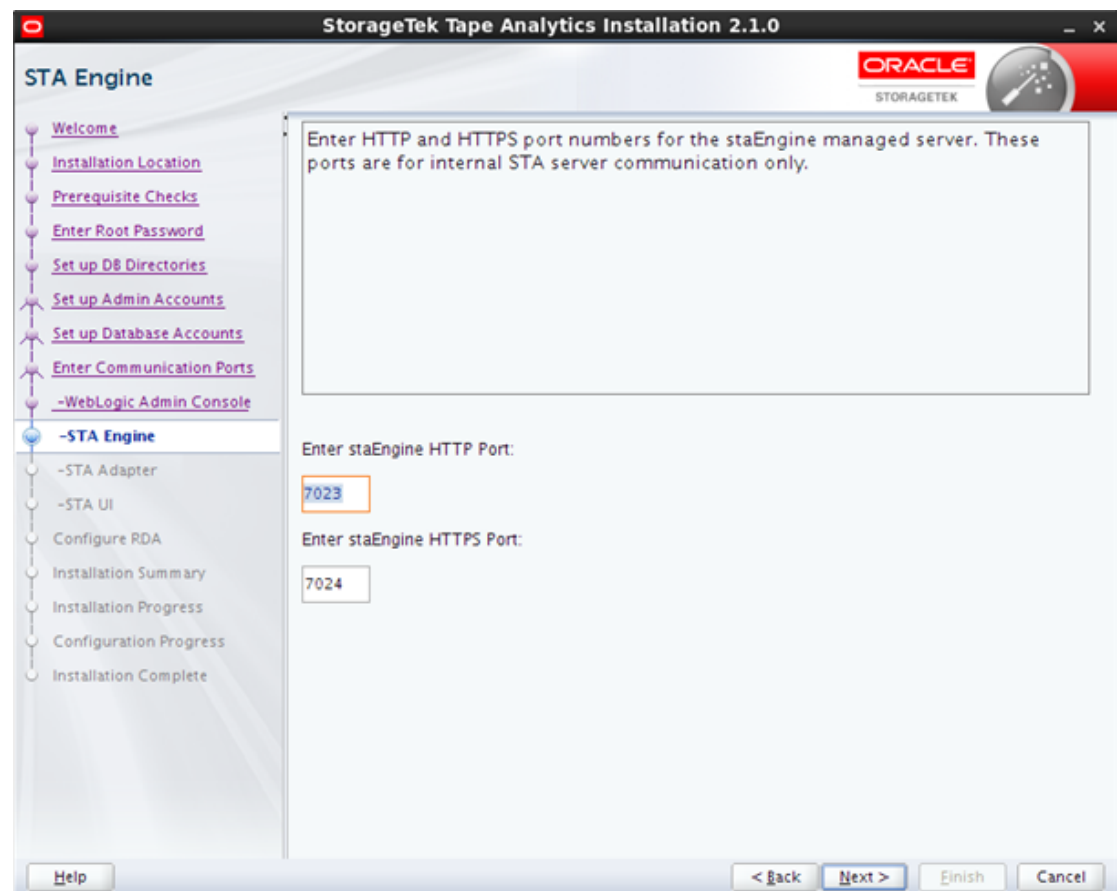
WebLogic 管理コンソールログインへのセキュアなアクセス用の HTTPS ポート番号を入力します。通常、このポート番号は 7020 です。

ポート番号は一意で使用可能である必要があります。

A.2.16.2. 画面固有のボタン

なし

A.2.17. STA エンジン



staEngine 管理対象サーバーのポートは、内部の STA サーバー通信にのみ使用されます。

注:

これらのポート番号のセキュアな記録を取ってください。STA のインストール後は変更できません。

サイトのセキュリティーを守るため、これらの番号が意図的に再構成されたり、ハードコードされたりすることはありません。

A.2.17.1. 画面のフィールド

Enter HTTP Port

staEngine 管理対象サーバーへのセキュアでないアクセス用の HTTP ポート番号を入力します。通常、このポート番号は 7023 です。

ポート番号は一意で使用可能である必要があります。

Enter HTTPS Port

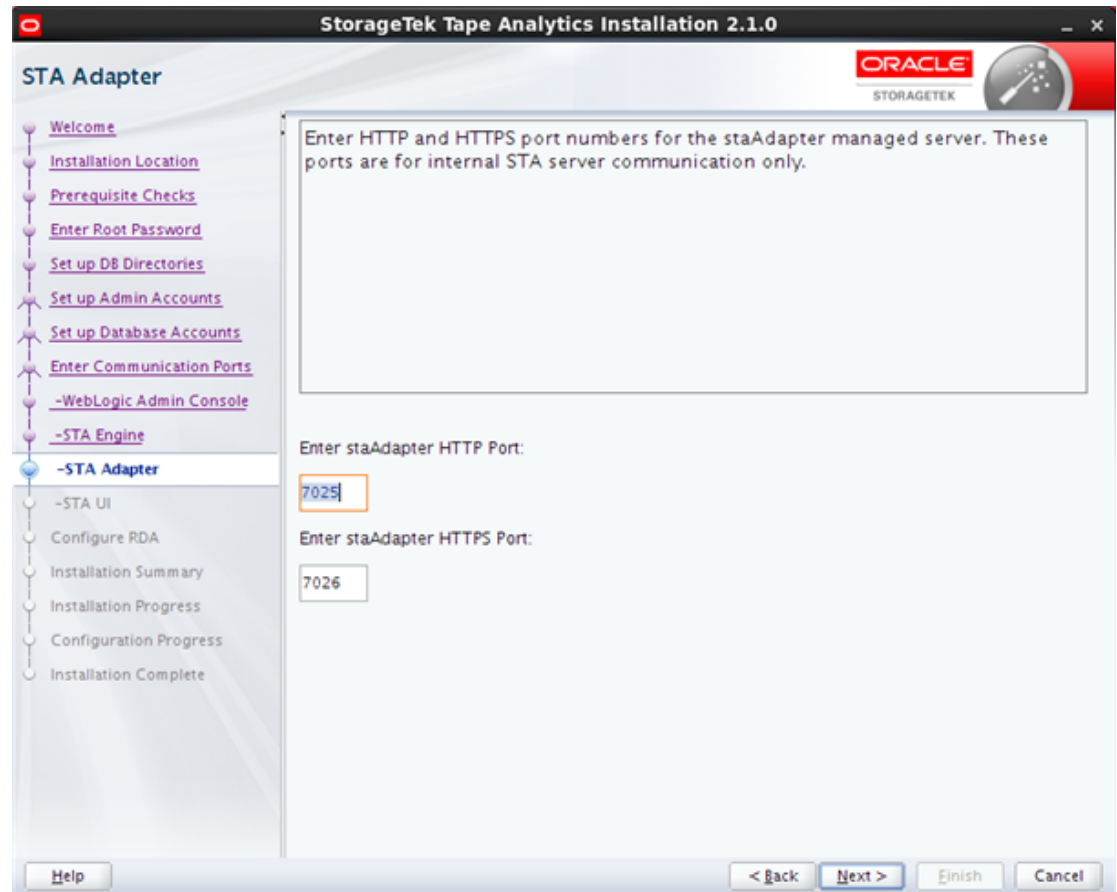
staEngine 管理対象サーバーへのセキュアなアクセス用の HTTPS ポート番号を入力します。通常、このポート番号は 7024 です。

ポート番号は一意で使用可能である必要があります。

A.2.17.2. 画面固有のボタン

なし

A.2.18. STA アダプタ



staAdapter 管理対象サーバーのポートは、内部の SNMP 通信にのみ使用されます。

注:

これらのポート番号のセキュアな記録を取ってください。STA のインストール後は変更できません。

サイトのセキュリティを守るため、これらの番号が意図的に再構成されたり、ハードコードされたりすることはありません。

A.2.18.1. 画面のフィールド

Enter HTTP Port

staEngine 管理対象サーバーへのセキュアでないアクセス用の HTTP ポート番号を入力します。通常、このポート番号は 7025 です。

ポート番号は一意で使用可能である必要があります。

Enter HTTPS Port

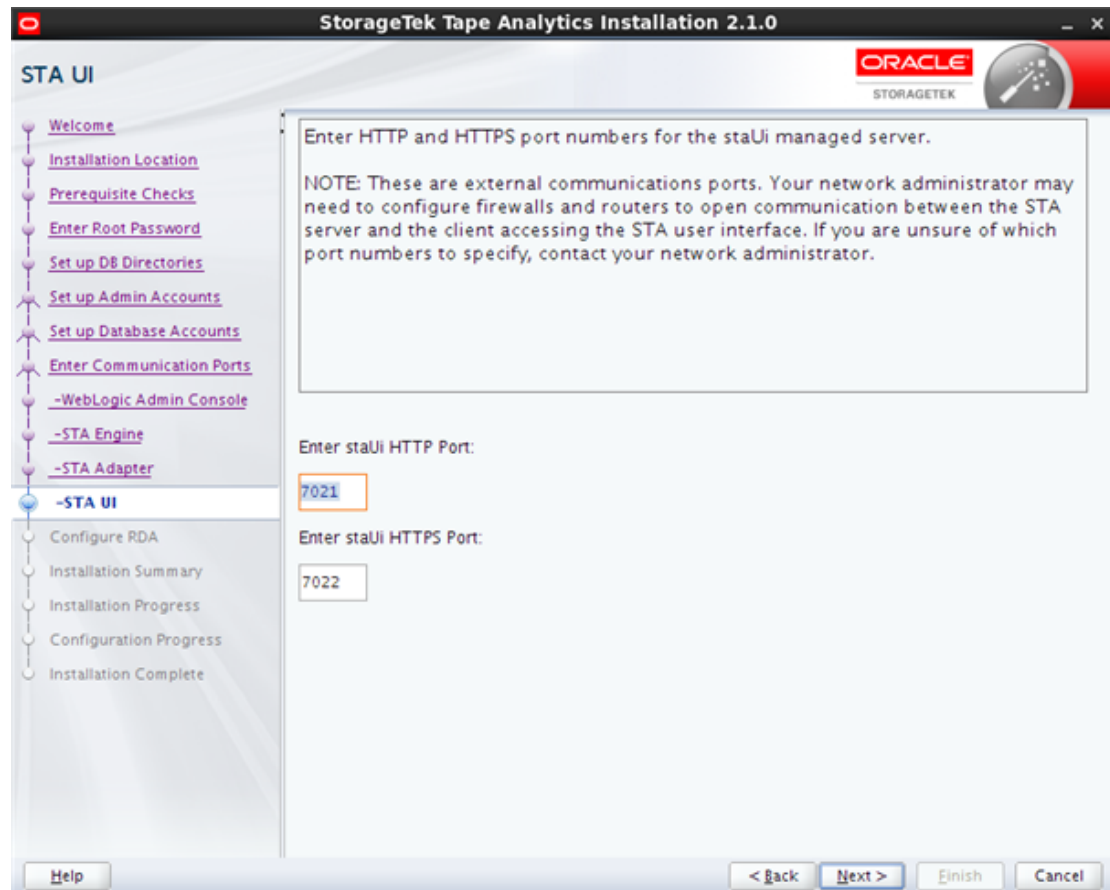
staEngine 管理対象サーバーへのセキュアなアクセス用の HTTPS ポート番号を入力します。通常、このポート番号は 7026 です。

ポート番号は一意で使用可能である必要があります。

A.2.18.2. 画面固有のボタン

なし

A.2.19. STA UI



STA アプリケーションユーザーインターフェースへのログイン時は、staUi 管理対象サーバーのポート番号を指定します。

注:

これらは外部通信ポートです。ネットワーク管理者は、STA サーバーと、WebLogic 管理コンソールにアクセスするクライアントとの通信を開始するようにファイアウォールやルーターを構成する必要がある場合があります。

注:

これらのポート番号のセキュアな記録を取ってください。STA のインストール後は変更できません。

サイトのセキュリティを守るため、これらの番号が意図的に再構成されたり、ハードコードされたりすることはありません。

A.2.19.1. 画面のフィールド

Enter HTTP Port

staUi 管理対象サーバーへのセキュアでないアクセス用の HTTP ポート番号を入力します。通常、このポート番号は 7021 です。

ポート番号は一意で使用可能である必要があります。

Enter HTTPS Port

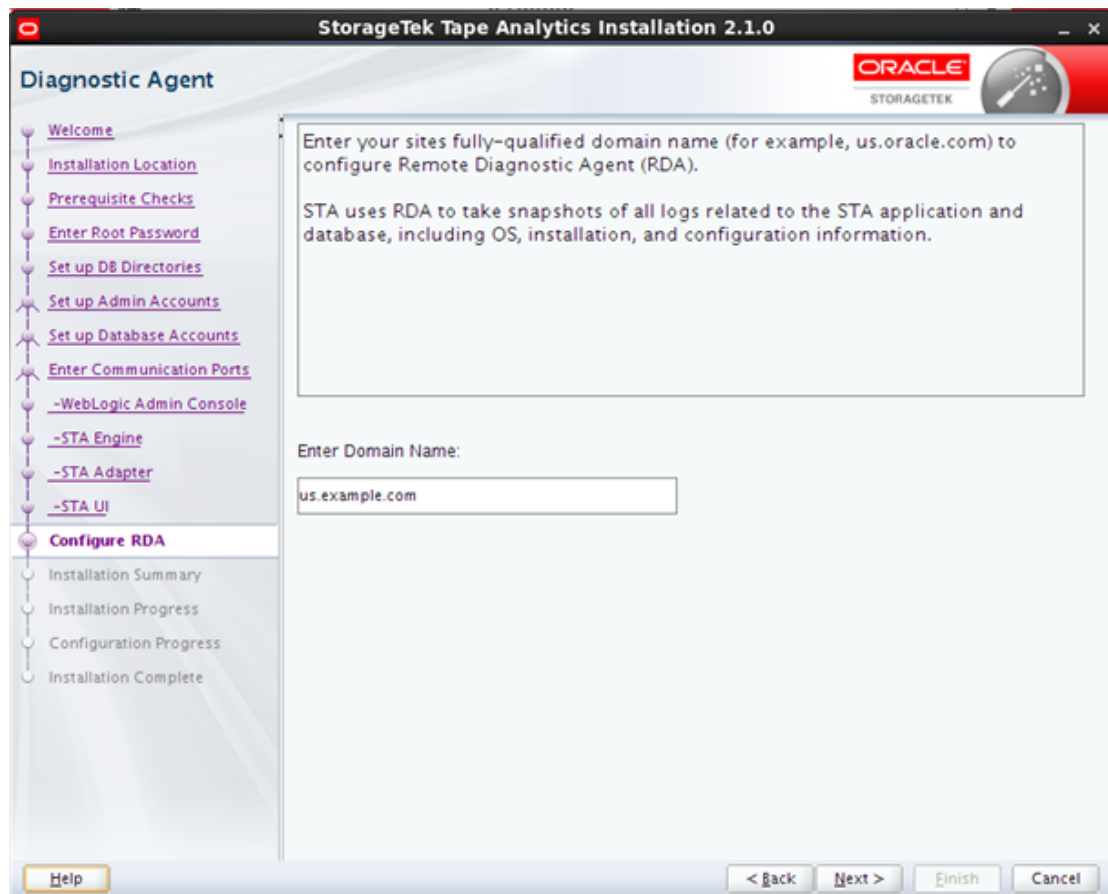
staUi 管理対象サーバーへのセキュアなアクセス用の HTTPS ポート番号を入力します。通常、このポート番号は 7022 です。

ポート番号は一意で使用可能である必要があります。

A.2.19.2. 画面固有のボタン

なし

A.2.20. 診断エージェント



STA インストーラは、サイトの完全修飾ドメイン名を使用して Oracle のリモート診断エージェント (RDA) を構成します。

STA は RDA を使用して、オペレーティングシステム、インストール、構成の情報を含む、STA アプリケーションおよびデータベースに関連するすべてのログのスナップショットを取得します。詳細は、『STA ユーザーズガイド』を参照してください。

A.2.20.1. 画面のフィールド

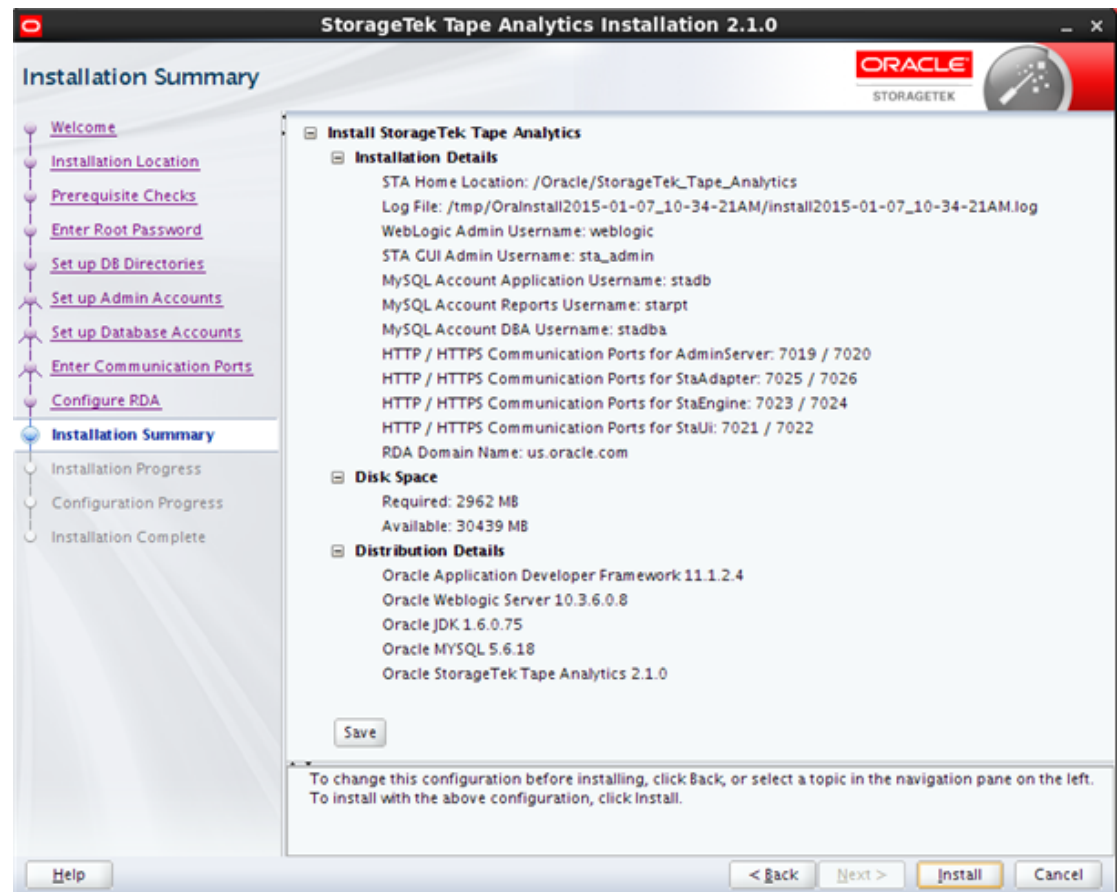
Enter Domain Name

サイトの完全修飾ドメイン名を入力します (例: *us.example.com*)。

A.2.20.2. 画面固有のボタン

なし

A.2.21. インストールサマリー



この画面には、インストールに関する次の詳細が表示されます。この情報は、控えとしてテキストファイルに保存できます。

- インストールの詳細 - インストーラ画面で入力された情報。
- ディスク領域 - 必要なディスク領域と使用可能なディスク領域 (M バイト)。
- ディストリビューションの詳細 - インストールされるソフトウェアパッケージの名前とバージョン番号。

次のように続行します。

- インストールの詳細のいずれかを変更するには、「**Back**」をクリックして該当する画面まで戻るか、ナビゲーションペインの画面リンクを選択してその画面に直接移動します。
- 表示された詳細をテキストファイルに保存するには、「**Save**」をクリックします。
- 表示された値を使用してインストールするには、「**Install**」をクリックします。
- インストールを取り消すには、「**Cancel**」をクリックします。

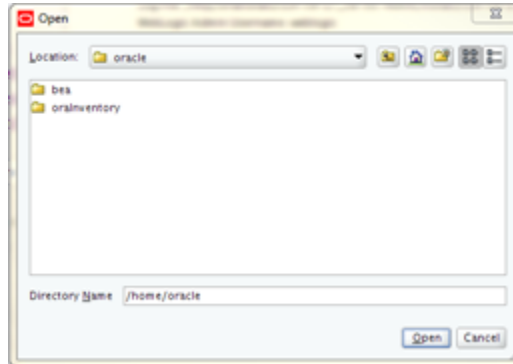
A.2.21.1. 画面のフィールド

なし

A.2.21.2. 画面固有のボタン

Save

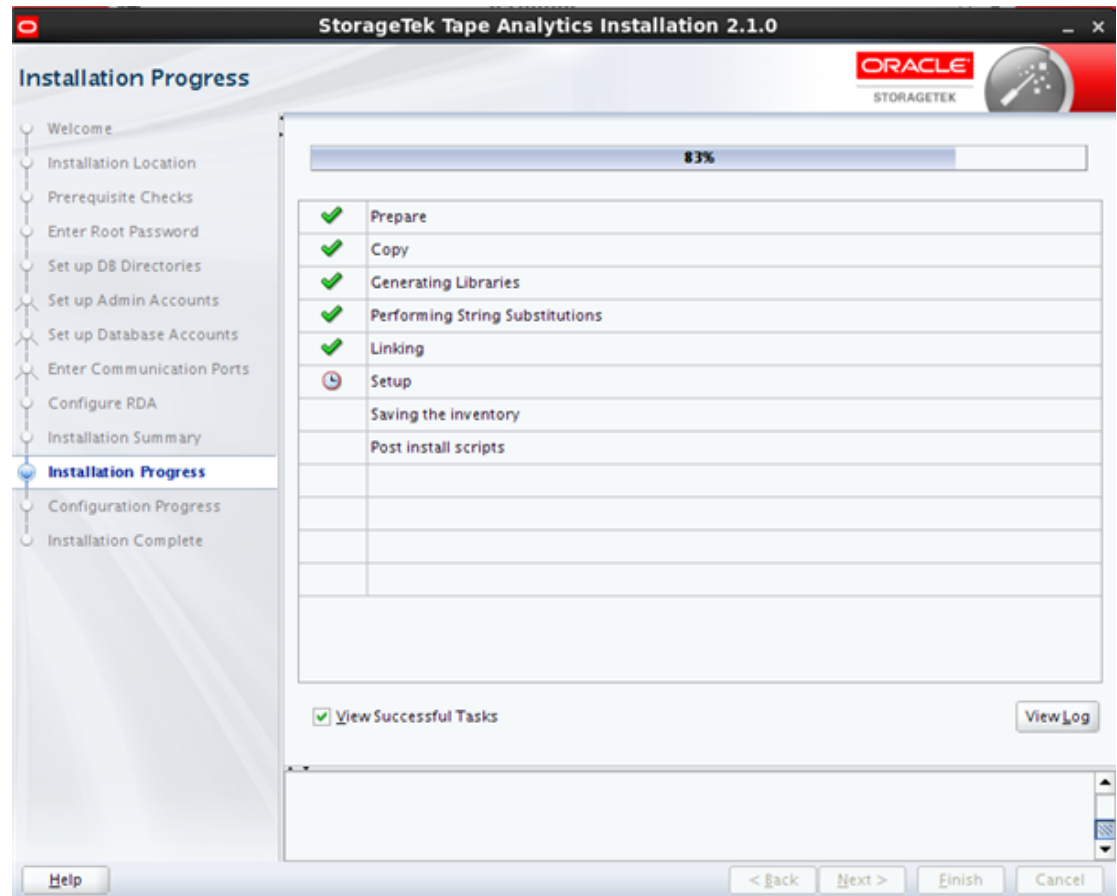
これをクリックすると、表示された情報が、*STA_Installation_Profile_timestamp.txt* という名前でテキストファイルに保存されます。「Open」ダイアログボックスで、ファイルの保存先のディレクトリを指定します。



Install

これをクリックすると、インストールが開始します。一度このボタンをクリックしたら、インストールを一時停止したり取り消したりすることはできません。

A.2.22. インストールの進行状況



STA のインストールが開始すると、この画面に各タスクのステータスが表示されます。

注意:

インストールの進行中は、このウィンドウを閉じたり、別の方法でインストールを中断したりしないでください。サーバー上に不完全なインストールコンポーネントが残る可能性があるからです。

タスクが失敗すると、インストールが停止するため、「**Cancel**」をクリックしてインストーラを終了する必要があります。インストーラはインストールをロールバックして、サーバーを元の状態に戻します。

終了する前に、メッセージペインに追加の詳細を表示して、問題のトラブルシューティングや対処方法の判断に役立てることができます。詳細情報に関するインストールログを表示することもできます。

A.2.22.1. 画面のフィールド

なし

A.2.22.2. 画面固有のボタン

View Successful Tasks

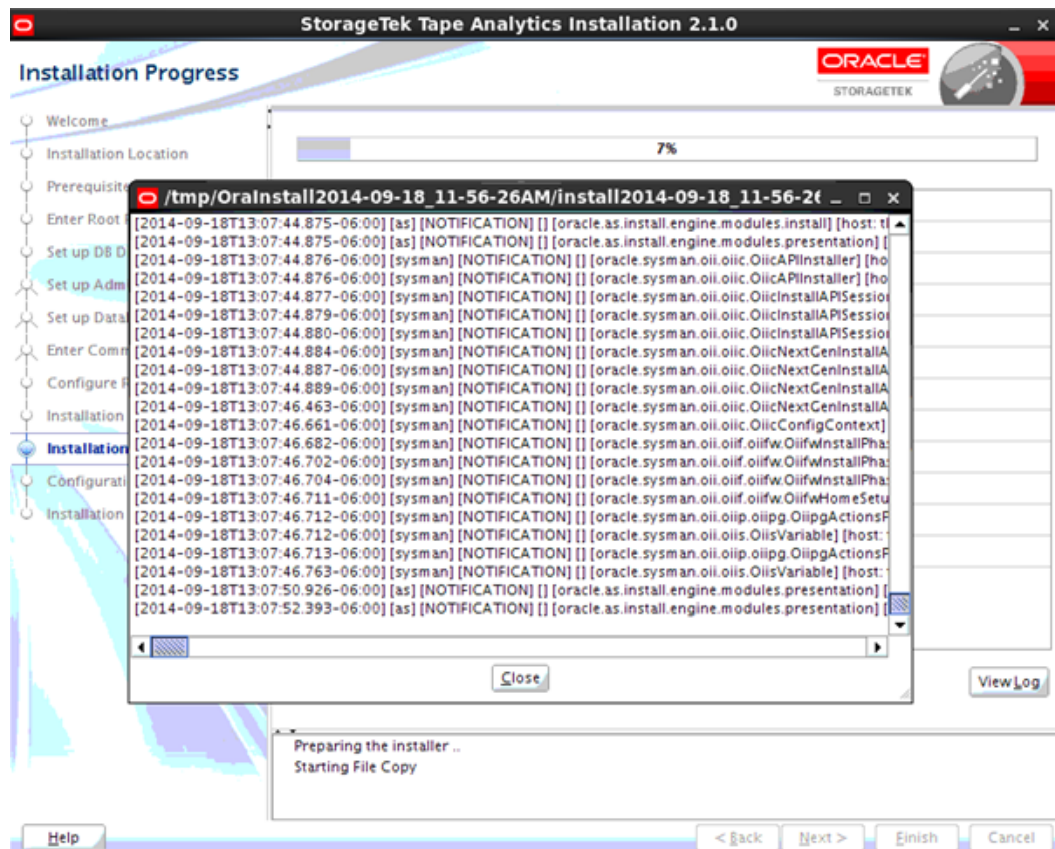
このチェックボックスを選択すると、表示に成功の結果を含めることができます。これはデフォルトです。

このチェックボックスをクリアすると、失敗の結果のみが表示されます。これにより、正常なタスクを除外できるため、注意が必要なタスクに重点的に取り組みます。

View Log

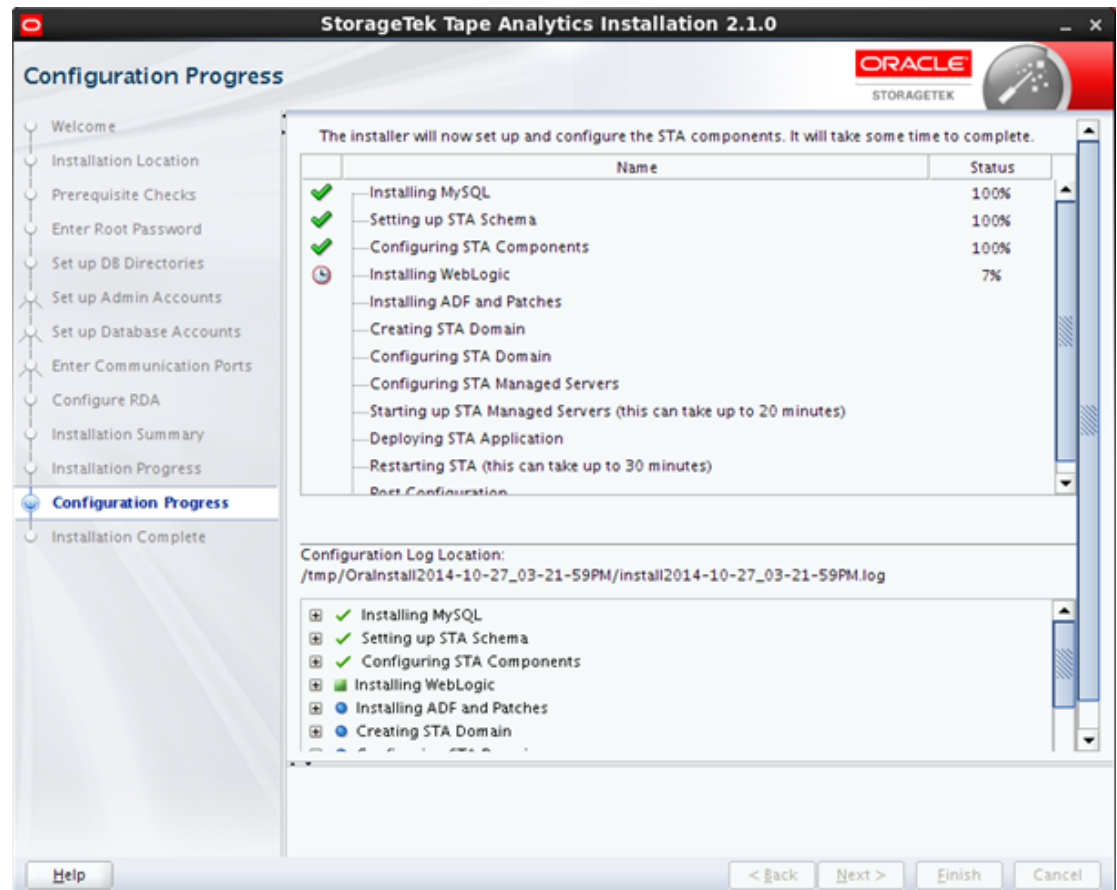
これをクリックすると、インストールログが別のウィンドウに表示されます。図A.5「インストールの進行状況ログの表示の例」に例を示します。「Close」をクリックすると、そのログウィンドウが閉じます。

図A.5 インストールの進行状況ログの表示の例



Linux コマンド行からログを表示することもできます。インストーラの実行中は、`/tmp` 内のサブディレクトリにログが保存されます。詳細は、「[STA のインストールおよびアンインストールのログ](#)」を参照してください。

A.2.23. 構成の進行状況



STA の構成および配備が開始すると、この画面に各タスクのステータスが表示されます。

注意:

構成の進行中は、このウィンドウを閉じたり、別の方法で構成を中断したりしないでください。サーバー上に不完全なインストールコンポーネントが残る可能性があるからです。

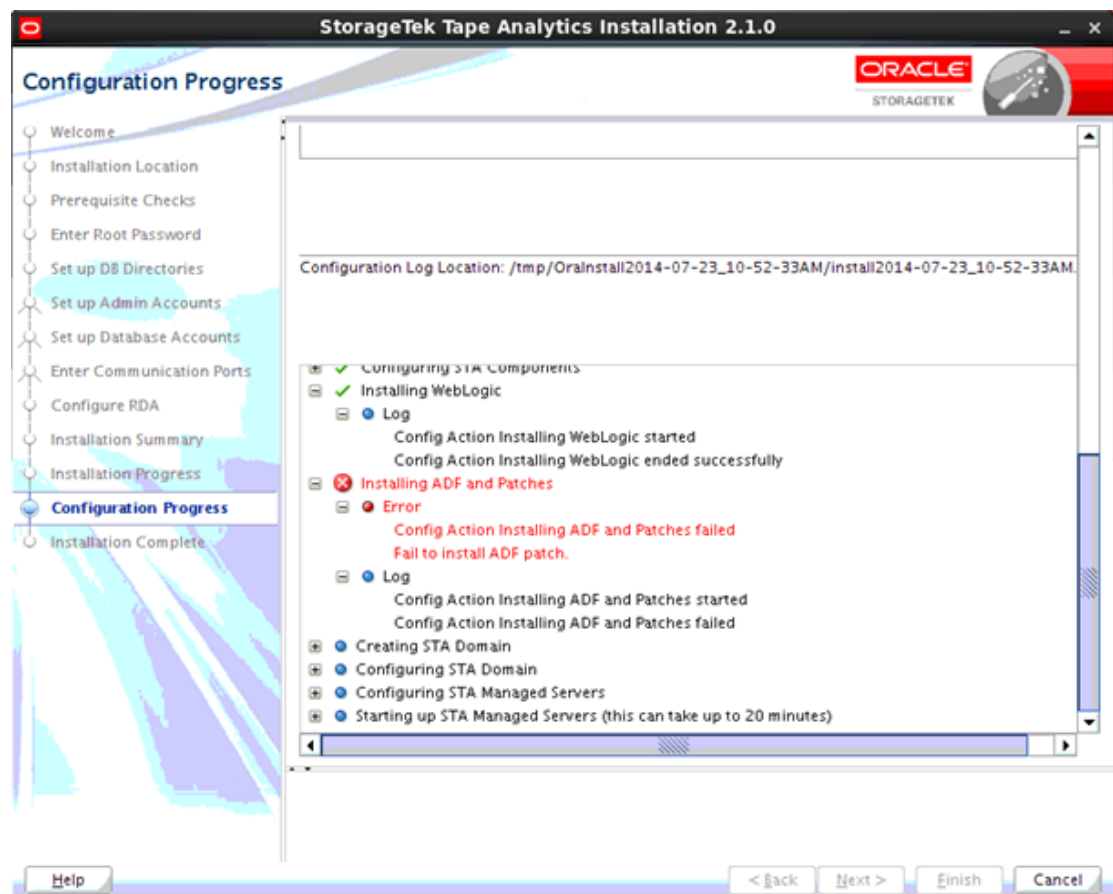
このプロセスの実行中に、WebLogic サーバー、STA 管理対象サーバー、および STA アプリケーションが構成され、起動されます。これが完了するまで 30 - 60 分かかる場合があります。

完了したタスクまたは進行中のどのタスクについても、展開された詳細を表示できます。メッセージペインで、詳細を表示するタスクの横にある展開 (+) アイコンをクリックします。「縮小

(-) アイコンをクリックすると、再度詳細が非表示になります。図A.6「構成の進行状況の詳細の例」は、正常なタスクと失敗したタスクに関する展開された詳細を示す例です。

タスクが失敗すると、STA インストーラは処理を中止し、インストールをロールバックして、サーバーを元の状態に戻します。インストールログを表示して問題のトラブルシューティングを行うことができます。詳細は、「STA のインストールおよびアンインストールのログ」を参照してください。

図A.6 構成の進行状況の詳細の例



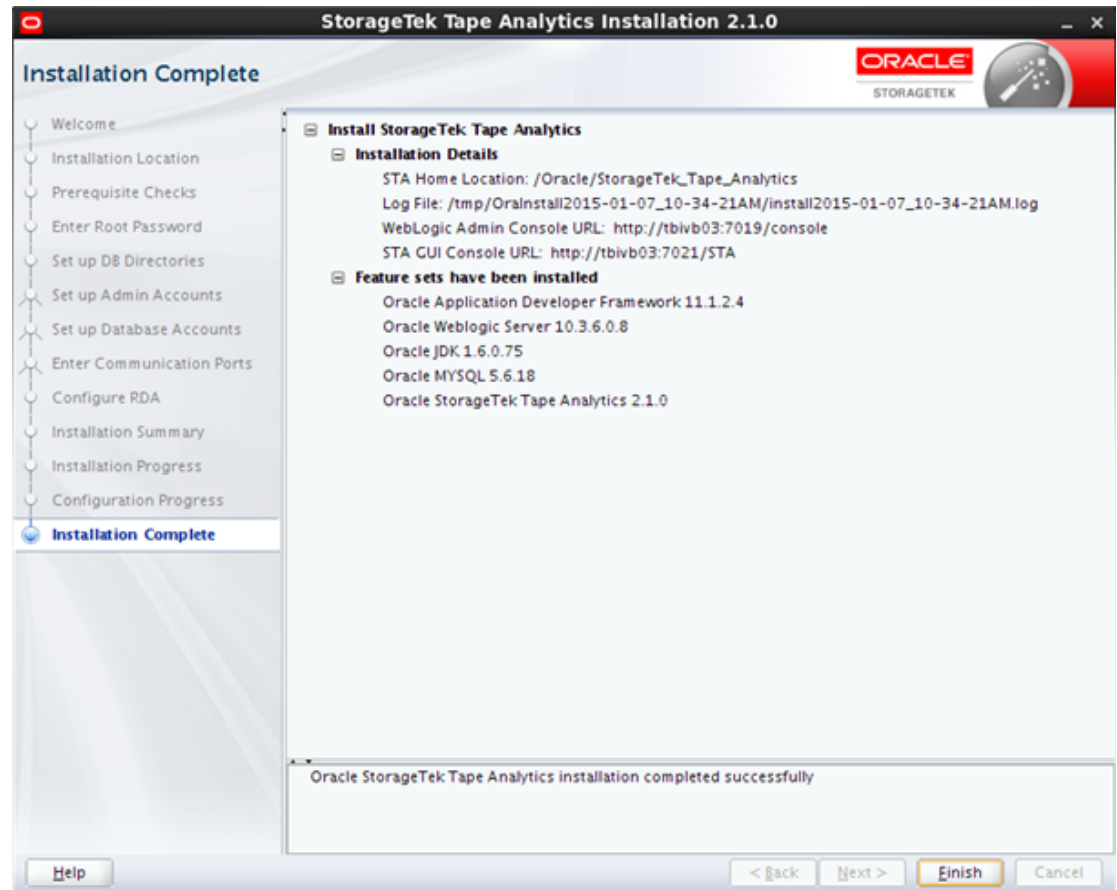
A.2.23.1. 画面のフィールド

なし

A.2.23.2. 画面固有のボタン

なし

A.2.24. インストール完了



この画面には、完了したインストールに関する次の詳細が表示されます。

- インストールの詳細 - インストールされた STA アプリケーションとインストーラログファイルの場所、および WebLogic と STA アプリケーションユーザーインタフェースの接続の詳細。
- インストールされている機能セット - インストールされているソフトウェアパッケージの名前とバージョン番号。

控え用にこの情報のスクリーンショットを保存することをお勧めします。インストーラを終了するには、「**Finish**」をクリックします。

A.2.24.1. 画面のフィールド

なし

A.2.24.2. 画面固有のボタン

Finish

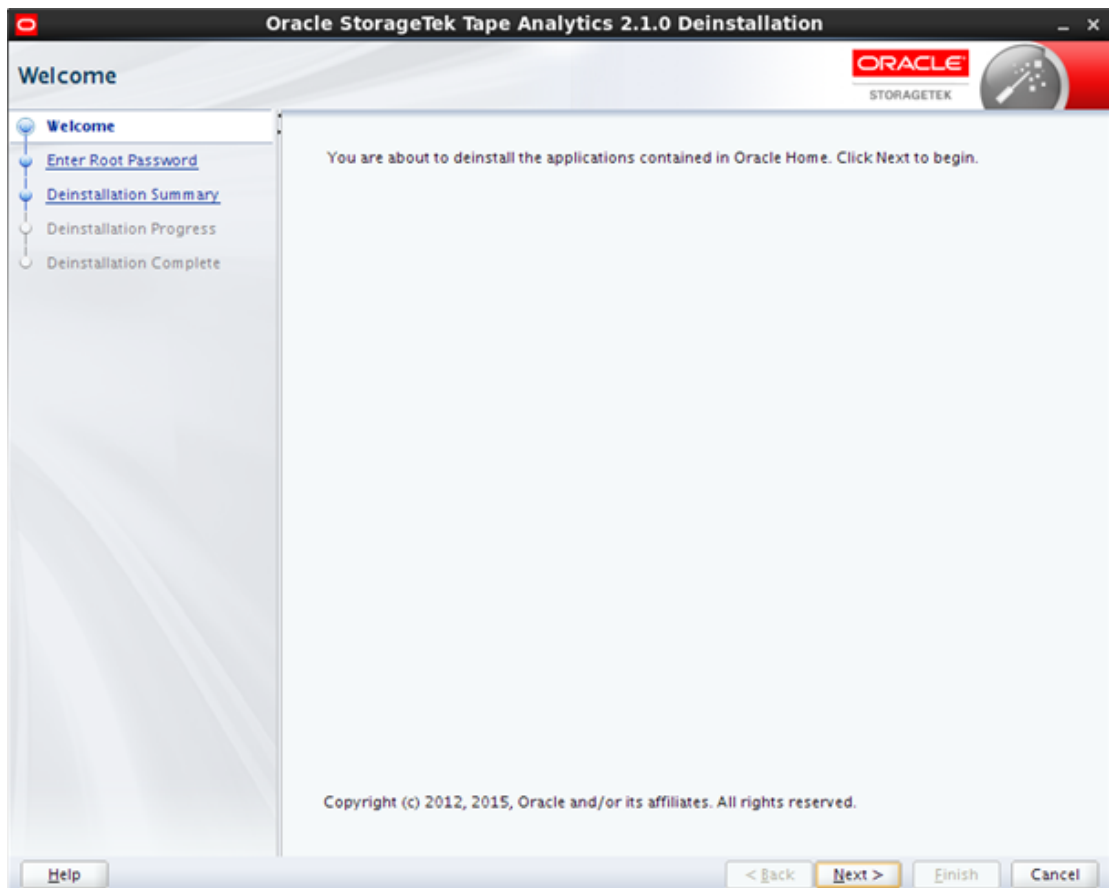
これをクリックすると、STA インストーラが終了します。

A.3. STA グラフィカルアンインストーラの画面

このセクションでは、STA グラフィカルアンインストーラの各画面について詳しく見ていきます。

- 「ようこそ」
- 「ルートパスワードの入力」
- 「アンインストールサマリー」
- 「アンインストールの進行状況」
- 「アンインストール完了」

A.3.1. ようこそ



この画面は、ユーザーが実行しようとしているアクションについて説明しています。テキストを読み、「Next」をクリックして処理を進めます。

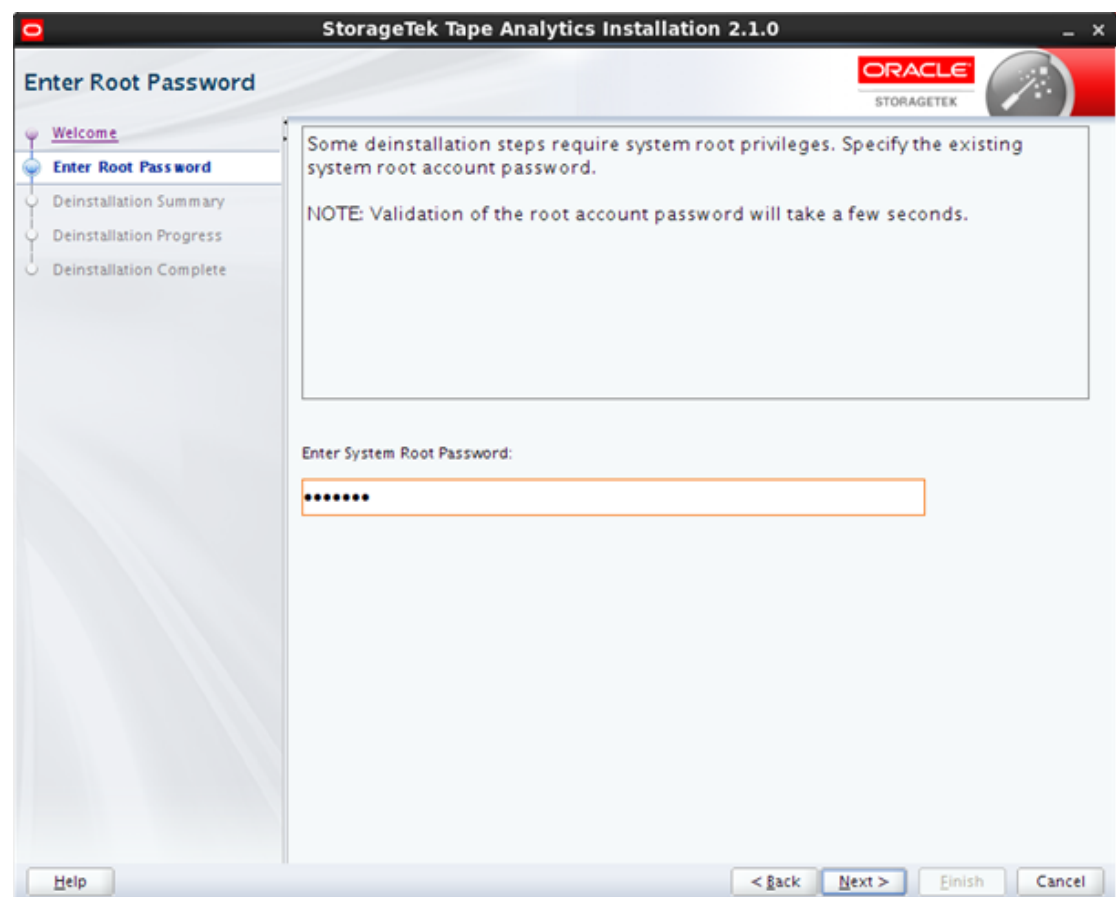
A.3.1.1. 画面のフィールド

なし

A.3.1.2. 画面固有のボタン

なし

A.3.2. ルートパスワードの入力



STA アンインストーラでアンインストールタスクを実行するためには Linux root アクセス権が必要です。

A.3.2.1. 画面のフィールド

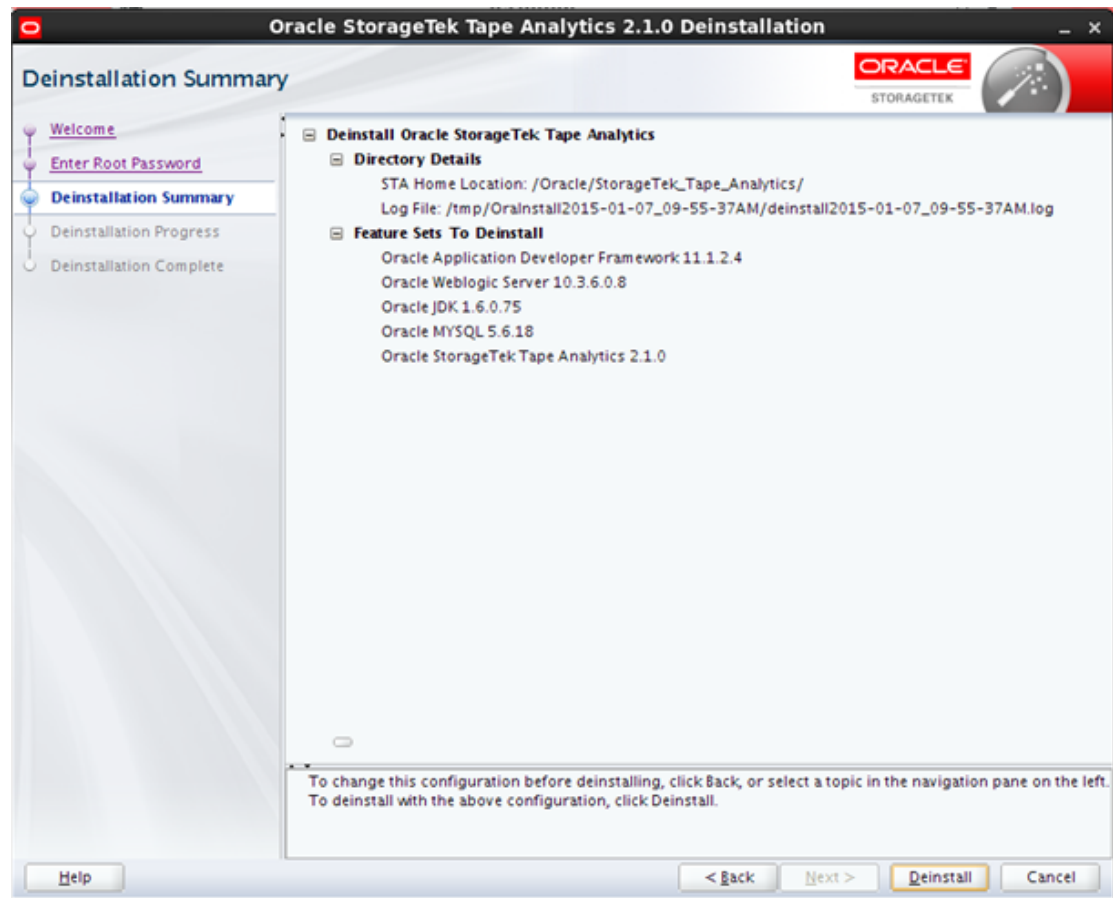
Enter Root Password

Linux root ユーザーのパスワードを入力します。入力中にエントリがマスクされます。パスワードの検証に数秒かかる場合があります。

A.3.2.2. 画面固有のボタン

なし

A.3.3. アンインストールサマリー



この画面には、アンインストールされるソフトウェアに関する次の詳細が表示されます。

- ディレクトリの詳細 - STA アプリケーションソフトウェアとアンインストールバグの場所。
- アンインストールする機能セット - アンインストールされるソフトウェアパッケージの名前とバージョン番号。

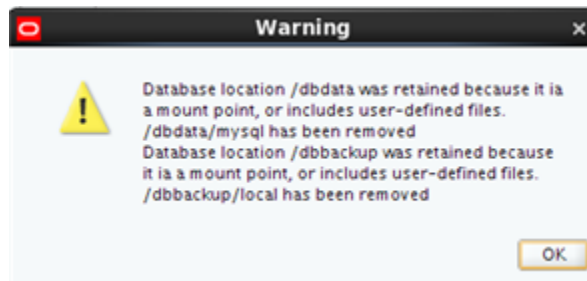
この情報を確認したら、次のように続行します。

注意:

アンインストールの進行中は、このウィンドウを閉じたり、別の方法でアンインストールを中断したりしないでください。サーバー上に不完全な STA コンポーネントが残る可能性があるからです。

注:

どちらかのデータベースの場所が STA サーバー上のマウントポイントである場合は、次のメッセージが表示され、そのマウントポイントが保持されていることが通知されます。「OK」をクリックすると、そのメッセージが閉じます。



アンインストールが完了すると、「Deinstallation Successful」というメッセージがメッセージペインに表示されます。「Next」または「Finish」をクリックして、最終画面に進みます。

タスクが失敗すると、STA アンインストーラは処理を中止し、アンインストールをロールバックして、サーバーを元の状態に戻します。アンインストールログを表示して問題のトラブルシューティングを行うことができます。詳細は、「[STA のインストールおよびアンインストールのログ](#)」を参照してください。

A.3.4.1. 画面のフィールド

なし

A.3.4.2. 画面固有のボタン

View Successful Tasks

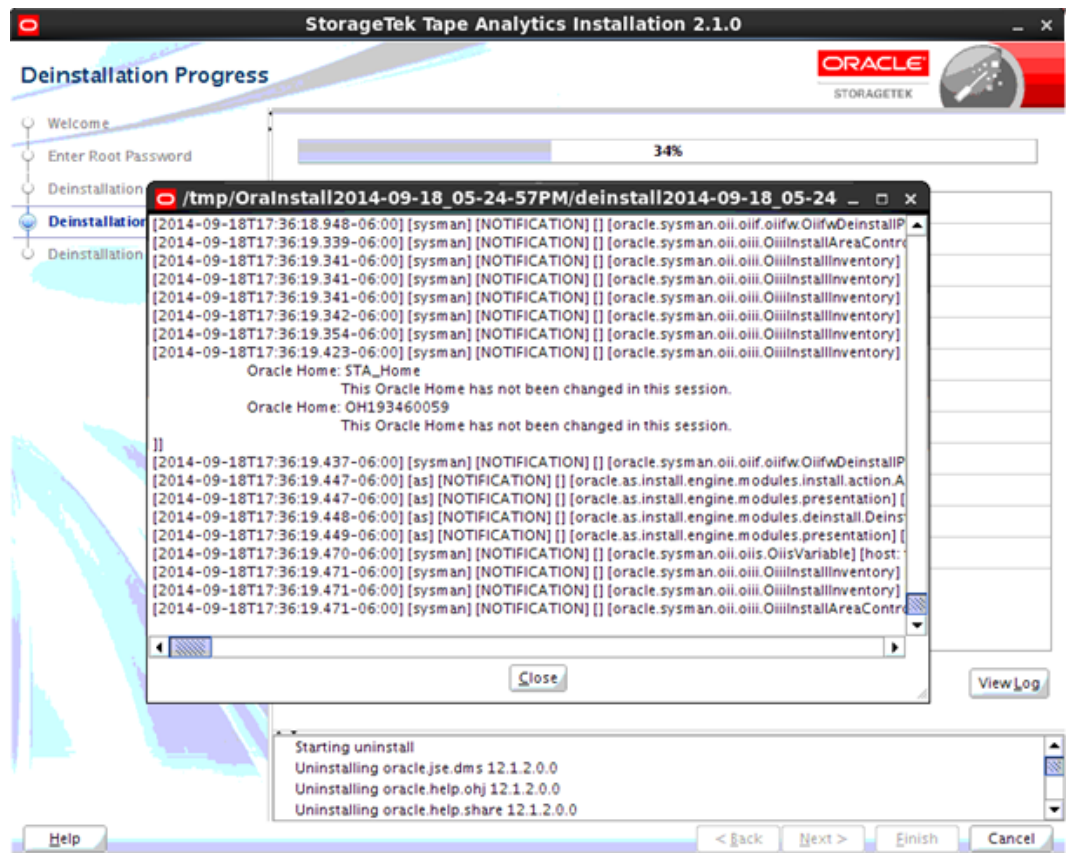
このチェックボックスを選択すると、表示に成功の結果を含めることができます。これはデフォルトです。

このチェックボックスをクリアすると、失敗の結果のみが表示されます。これにより、正常なタスクを除外できるため、注意が必要なタスクに重点的に取り組めます。

View Log

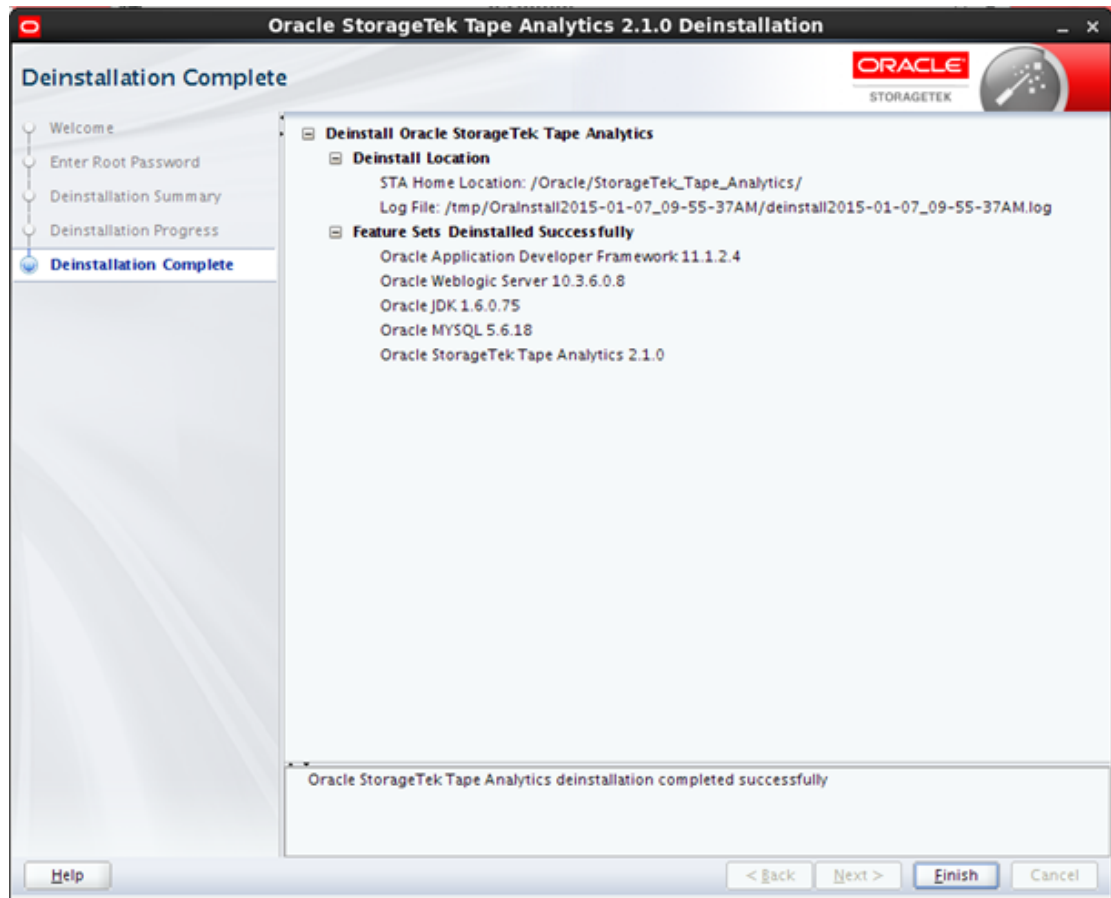
これをクリックすると、アンインストールログが別のウィンドウに表示されます。[図A.5「インストールの進行状況ログの表示の例」](#)に例を示します。「Close」をクリックすると、そのログウィンドウが閉じます。

図A.7 アンインストールの進行状況ログの表示の例



Linux コマンド行からログを表示することもできます。アンインストーラの実行中は、`/tmp` 内のサブディレクトリにログが保存されます。詳細は、「[STA のインストールおよびアンインストールのログ](#)」を参照してください。

A.3.5. アンインストール完了



この画面には、アンインストールされたソフトウェアパッケージに関する詳細が表示されます。

A.3.5.1. 画面のフィールド

なし

A.3.5.2. 画面固有のボタン

Finish

これをクリックすると、STA アンインストーラが終了します。

STA サイレントモードインストーラおよびアンインストーラ

この付録には次のセクションが含まれます。

- [STA サイレントモードインストーラおよびアンインストーラの使用](#)
- サイレントモードで使用されるファイルとユーティリティ
- STA サイレントモードインストーラのタスク
- STA サイレントモードアンインストーラのタスク
- STA インストーラコマンドオプション

B.1. STA サイレントモードインストーラおよびアンインストーラの使用

サイレントモードでは、グラフィカルユーザーインターフェースを迂回し、応答ファイルと呼ばれる XML プロパティファイル内に STA インストールまたはアンインストールオプションを指定できます。応答ファイルの作成には、`silentInstallUtility_version.jar` (`version` はダウンロードしたユーティリティのバージョン) という応答ファイル構築ユーティリティを使用します。

このモードは、無人インストールや複数のマシンに STA をインストールする際に役立ちます。応答ファイルを使用することで、1 組のパラメータを指定して、インストールを自動化できます。サイレントモードのインストーラは、スクリプトから実行することも、Linux コマンド行から実行することもできます。

B.1.1. サイレントモードの要件

一般的な STA インストール要件については、「[インストールの前提条件の確認](#)」を参照してください。それに加えて、STA サイレントモードインストーラおよびアンインストーラには次のモード固有の要件もあります。

- PuTTY など、X11 プロトコルを使用しない telnet クライアントからサイレントモードを使用できます。ただし、`xorg-x11-utils` RPM パッケージを STA サーバーにインストールする必要があります。

- サイレントモードをインストールする前に、Oracle Software Delivery Cloud Web サイトから `silentInstallUtility_version.jar` ファイルをダウンロードし、それを使って暗号化パスワードを含む応答ファイルを作成する必要があります。手順については、「[サイレントモードインストーラの応答ファイルの作成](#)」を参照してください。
- サイレントモードには、Oracle 中央インベントリディレクトリの場所と Oracle インストールグループを指定する、中央インベントリポインタファイルも必要です。このファイルが存在しない場合は手動で作成する必要があります。詳細は、「[Oracle 中央インベントリポインタファイル](#)」を参照してください。

B.2. サイレントモードで使用されるファイルとユーティリティ

このセクションでは、サイレントモードのインストールとアンインストールに関する重要な概念と用語について説明します。

Oracle 中央インベントリポインタファイル

STA サイレントモードインストーラおよびアンインストーラでは、中央インベントリポインタファイル内に指定されている Oracle 中央インベントリの場所と Oracle インストールグループを使用します。詳細は、「[STA インストーラで使用するユーザー、グループ、場所](#)」を参照してください。

デフォルトでは、サイレントモードのインストーラとアンインストーラは `/etc/oraInst.loc` というポインタファイルを使用します。Oracle 中央インベントリを登録すると、この名前と場所でそのファイルが自動的に作成されます。詳細は、「[Oracle 中央インベントリの場所の登録](#)」を参照してください。

Oracle 中央インベントリの場所が登録されていない場合は、ポインタファイルを手動で作成して、`oraInst.loc` というファイル名を付ける必要があります。詳細は、「[Oracle 中央インベントリポインタファイルの作成](#)」を参照してください。ポインタファイルは任意のディレクトリに格納できますが、それが `/etc` 以外にある場合は、サイレントモードインストーラまたはアンインストーラを実行するときに、`-invPtrLoc` パラメータを使ってそのファイルの場所を指定する必要があります。このパラメータの詳細は、「[-invPtrLoc pointer_file](#)」を参照してください。

サイレントインストーラおよびアンインストーラの応答ファイル

オペレータの介在なしで実行するには、STA サイレントモードインストーラおよびアンインストーラで、作成された応答ファイルに含まれている構成設定を使用します。`-responseFile` パラメータを使ってこのファイルの名前と場所を指定する必要があります。

インストーラとアンインストーラにはそれぞれ独自の応答ファイルがあります。[例 B.1「STA サイレントモードインストーラの応答ファイルのテンプレート」](#)と[例 B.2「STA サ](#)

「サイレントモードアンインストーラの応答ファイルのテンプレート」にそれぞれのファイルの内容と必要なエントリを示します。独自の応答ファイルを作成するには、各テンプレートをテキストファイルにコピー&ペーストし、サイトに合わせて適切な変更をします。

パスワードのセキュリティを確保するために、クリアテキストのパスワードを応答ファイルに入力しないでください。ほかのすべての構成設定を入力し、ファイルを保存したら、応答ファイル構築ユーティリティを使って暗号化パスワードをファイルに挿入する必要があります。詳細は、[STA インストーラの応答ファイル構築ユーティリティ](#)を参照してください。

例B.1 STA サイレントモードインストーラの応答ファイルのテンプレート

```
[ENGINE]
#DO NOT CHANGE THIS. Response File Version=1.0.0.0.0
[GENERIC]
#The oracle storage home location. This can be an existing Oracle Storage Home or
#a new Oracle Storage Home
STORAGE_HOME=required
#Root access password var.
ROOT ACCESS PASSWORD=
RESPONSEFILE_LOC=
KEYFILE_LOC=
#DBDATA LOC
DBDATA LOC=required
#DBBACKUP LOC
DBBACKUP LOC=required
#Weblogic Admin Name Var
WEBLOGIC ADMIN NAME=required
#Weblogic Admin Password Var
WEBLOGIC ADMIN PASSWORD=
#Weblogic Admin ConfirmPassword Var
WEBLOGIC ADMIN CONFIRMPASSWORD=
#STAGUI Admin Name Var
STAGUI ADMIN NAME=required
#STAGUI Admin Password Var
STAGUI ADMIN PASSWORD=
#STAGUI Admin ConfirmPassword Var
STAGUI ADMIN CONFIRMPASSWORD=
#MySQL root password var.
MYSQL ROOT PASSWORD=
#MySQL root confirm password var.
MYSQL ROOT CONFIRM PASSWORD=
#MySQL App Name Var
MYSQL APP NAME=required
#MySQL App Password Var
MYSQL APP PASSWORD=
#MySQL App ConfirmPassword Var
MYSQL APP CONFIRMPASSWORD=
#MySQL RPTS Name Var
MYSQL RPTS NAME=required
#MySQL RPTS Password Var
MYSQL RPTS PASSWORD=
#MySQL RPTS ConfirmPassword Var
MYSQL RPTS CONFIRMPASSWORD=
#MySQL DBA Name Var
MYSQL DBA NAME=required
#MySQL DBA Password Var
```

```

MYSQL DBA PASSWORD=
#MySQL DBA ConfirmPassword Var
MYSQL DBA CONFIRMPASSWORD=
#ADMINSERVER HTTP Port Var
ADMINSERVER HTTP PORT=7019
#ADMINSERVER HTTPS Port Var
ADMINSERVER HTTPS PORT=7020
#staEngine HTTP Port Var
STAENGINE HTTP PORT=7023
#staEngine HTTPS Port Var
STAENGINE HTTPS PORT=7024
#staAdapter HTTP Port Var
STAADAPTER HTTP PORT=7025
#staAdapter HTTPS Port Var
STAADAPTER HTTPS PORT=7026
#staUi HTTP Port Var
STAUI HTTP PORT=7021
#staUi HTTPS Port Var
STAUI HTTPS PORT=7022
#Domain name var.
DOMAIN NAME=required
    
```

例B.2 STA サイレントモードアンインストーラの応答ファイルのテンプレート

```

[ENGINE]
#DO NOT CHANGE THIS. Response File Version=1.0.0.0.0
[GENERIC]
#This will be blank when there is nothing to be de-installed in distribution level
SELECTED_DISTRIBUTION=STA_Install~2.1.0.0.0
#Root access password var.
DEINSTALL ROOT ACCESS PASSWORD=
RESPONSEFILE_LOC=
KEYFILE_LOC=
    
```

STA インストーラの応答ファイル構築ユーティリティ

インストーラの応答ファイル構築ユーティリティを使用すると、暗号化パスワードをサイレントモードインストーラおよびアンインストーラの応答ファイルに挿入できます。このユーティリティは、ユーザーにパスワードの入力を求め、それらを指定されたファイルに暗号化形式で追加します。また、暗号鍵ファイルを任意のディレクトリに保存します。

応答ファイル構築ユーティリティのダウンロードは、STA インストーラのダウンロード時に行えます。ユーティリティ名は、*silentInstallUtility_version.jar* (*version* はダウンロードしたユーティリティのバージョン) です。

STA が正常にインストールまたはアンインストールされると、暗号化パスワードがそれぞれの応答ファイルから削除されます。サイレントモードインストーラまたはアンインストーラをもう一度実行するには、構築ユーティリティを再実行して暗号化パスワードを再度指定します。

構築ユーティリティでは応答ファイルの場所をファイルの内容に書き込むため、このユーティリティを使って応答ファイルを更新したあとでそれを移動することはできません。

手順については、「[サイレントモードインストーラの応答ファイルの作成](#)」を参照してください。

B.3. STA サイレントモードインストーラのタスク

これらのタスクを使用する前に、必要なインストール情報を取得し、前提条件を確認して、STA インストーラをダウンロードするようにしてください。手順については、「[STA のインストールタスク](#)」を参照してください。

その後、サイレントモードインストーラを使って STA をインストールするには、次のタスクを示された順序で実行します。

- 「[Oracle 中央インベントリポインタファイルの作成](#)」
- 「[サイレントモードインストーラの応答ファイルの作成](#)」
- 「[サイレントモードインストーラの実行](#)」

B.3.1. Oracle 中央インベントリポインタファイルの作成

Oracle 中央インベントリポインタファイルが存在しない場合にそれを作成するには、次の手順を使用します。

1. Oracle インストールユーザーとしてログインします。
2. 次のコマンドを発行して、Oracle 中央インベントリポインタファイルが存在するかどうかを確認します。

```
$ cat /etc/oraInst.loc
```

ファイルが存在するかどうかに応じて、表示の例は次のようになります。

- ファイルが存在しない場合:

```
cat: /etc/oraInst.loc: No such file or directory
```

- ファイルが存在する場合:

```
inventory_loc=/opt/oracle/oraInventory  
inst_group=oinstall
```

3. ファイルが存在する場合は、この手順を終了してかまいません。それ以外の場合は、次の手順に進みます。

4. テキストエディタを使用してインベントリポインタファイルを作成します。ファイル名は `oraInst.loc` にする必要があります。このファイルの内容については、[-invPtrLoc pointer_file](#)を参照してください。
5. そのファイルを任意のディレクトリに保存します。そのファイルを `/etc` ディレクトリに保存した場合、STA サイレントモードインストーラおよびアンインストーラは自動的にそれを見つけます。それ以外の場合は、これらのユーティリティを実行するときにその場所を指定する必要があります。

B.3.2. サイレントモードインストーラの応答ファイルの作成

サイレントモードインストーラの応答ファイルを作成し、暗号化パスワードをそれに追加するには、次の手順を使用します。

1. Oracle インストールユーザーとしてログインします。
2. テキストエディタを使用して、任意の名前で応答ファイルを作成します。ファイルテンプレートについては、[例B.1「STA サイレントモードインストーラの応答ファイルのテンプレート」](#)を参照してください。

テンプレートをテキストファイルにコピー&ペーストし、サイトに合わせて適切な変更をします。「required」とマークされたすべて変数に値を指定する必要があります、必要に応じてサイトのポート番号を変更できます。

- `RESPONSEFILE_LOC`
- `KEYFILE_LOC`
- すべての `PASSWORD` 変数

3. そのファイルを任意の名前と場所で保存します。
4. 応答ファイル構築ユーティリティがダウンロードされているディレクトリに移動します。このユーティリティの名前は `silentInstallUtility_version.jar` です。例:

```
$ cd /Installers
```

5. 応答ファイル構築ユーティリティを実行します。

```
$ java -jar silentInstallUtility_2.1.0.64.124.jar response_file
```

ここで、`response_file` は作成した応答ファイルの絶対パスです。

- 各プロンプトに適切な情報で応答します。入力したパスワード値は画面に表示されません。パスワード要件については、「[STA を管理するためのユーザーアカウント](#)」を参照してください。

例B.3「インストーラの応答ファイル構築ユーティリティーの実行例」は、応答ファイル構築ユーティリティーの実行例です。

例B.3 インストーラの応答ファイル構築ユーティリティーの実行例

```
$ java -jar silentInstallUtility_2.1.0.64.124.jar /Installers/SilentInstall.rsp
Oracle StorageTek Tape Analytics Silent Installation Utility
```

```
-----
```

```
This utility is used to assist users with the password fields in the Silent
Installation response file. The silent installation process requires the
password fields in the response file requires the password fields to be
encrypted. The utility will ask the users for the required passwords, and encrypt
these values, then update the values into the supplied response file.
```

```
Please enter the location to save the key file : /Installers
What is the response file used for? ('i' for Install, 'd' for Deinstall) : i
Enter system root password:
Confirm system root password:
Enter mySQL DB root password:
Confirm mySQL DB root password:
Enter STA user password:
Confirm STA user password:
Enter Weblogic console password:
Confirm Weblogic console password:
Enter STA DB Application password:
Confirm STA DB Application password:
Enter STA DB Report password:
Confirm STA DB Report password:
Enter STA DBA password:
Confirm STA DBA password:
```

7. ユーティリティーが完了したら、応答ファイルのあるディレクトリに暗号鍵ファイルが作成されていることを確認します。これは、「sk」で始まるランダムに生成された名前を持つ隠しファイルです。次に例を示します。

```
$ ls -la /Installers/.sk*
-r----- 1 oracle oinstall          17 Sep 22 12:00 .sk1414440339833
```

8. 応答ファイルを表示し、次の値を確認します。
 - `RESPONSEFILE_LOC` が正しい応答ファイルの場所で更新されています。
 - `KEYFILE_LOC` が正しい暗号鍵ファイルの場所で更新されています。
 - すべてのパスワードが暗号化された値で更新されています。

例B.4「構築ユーティリティーの使用後のインストーラユーティリティーファイルの例」は、適切な値を示す、ファイルの最初の部分の例です。

例B.4 構築ユーティリティーの使用後のインストーラユーティリティーファイルの例

```
$ view /Installers/SilentInstall.rsp
[ENGINE]
#DO NOT CHANGE THIS. Response File Version=1.0.0.0.0
[GENERIC]
#The oracle storage home location. This can be an existing Oracle Storage Home or
  a new Oracle Storage Home
STORAGE_HOME=/Oracle
#Root access password var.
ROOT ACCESS PASSWORD=JvPABRzrtVP7LZT1Vin0Qg==
RESPONSEFILE_LOC=/Installers/SilentInstall.rsp
KEYFILE_LOC=/Installers/.sk1414705403180
#DBDATA LOC
DBDATA LOC=/dbdata
#DBBACKUP LOC
DBBACKUP LOC=/dbbackup
#Weblogic Admin Name Var
WEBLOGIC ADMIN NAME=weblogic
#Weblogic Admin Password Var
WEBLOGIC ADMIN PASSWORD=k5/c60q1KGwQdUje6CfCgA==
```

```
#Weblogic Admin ConfirmPassword Var
WEBLOGIC ADMIN CONFIRMPASSWORD=k5/c60q1KGwQdUje6CfCgA==
...
```

B.3.3. サイレントモードインストーラの実行

サイレントモードインストーラを使用して STA をインストールするには、次の手順を使用します。

1. STA インストーラの場所に移動します。例:

```
$ cd /Installers
```

2. STA サイレントモードインストーラを起動します。これらのパラメータの完全な定義については、「[STA インストーラコマンドオプション](#)」を参照してください。

```
$ ./sta_installer_linux64_version.bin -silent -responseFile response_file -
invPtrLoc pointer_file
```

ここでは:

- *version* はダウンロードした STA インストーラのバージョンです。
- *-silent* はサイレントモードを示します。このパラメータは必須です。
- *-responseFile response_file* はサイレントモードインストーラの応答ファイルの絶対パスを示します。このパラメータは必須です。
- *-invPtrLoc pointer_file* は Oracle 中央インベントリポインタファイルの絶対パスを示します。このパラメータは、そのファイルが */etc* ディレクトリに存在しない場合またはユーザーが別のファイルを使用する場合にのみ必須です。

例:

```
$ ./sta_install_2.1.0.64.124_linux64.bin -silent -responseFile /Installers/
SilentInstall.rsp -invPtrLoc /opt/oracle/oraInst.loc
```

3. インストーラが次のインストール手順を実行すると、ステータスメッセージが端末ウィンドウに表示されます。このプロセスは、完了するまでに 30 - 60 分かかる場合があります。
 - STA サーバー環境の前提条件チェックを実行します。

- MySQL、WebLogic、および STA アプリケーションなど、含まれているソフトウェアパッケージをインストールします。
- 応答ファイル内に指定されている設定を使って STA 環境を構成します。
- STA アプリケーションを起動します。

例B.5「成功した STA サイレントモードインストールの最終メッセージ」に、成功したインストールの最後に表示されるメッセージを示します。例B.6「失敗した STA サイレントモードインストールの最終メッセージの例」に、失敗したインストールの最後に表示される可能性のあるいくつかのメッセージを示します。

例B.5 成功した STA サイレントモードインストールの最終メッセージ

```
...
Started Configuration:Deploying STA Application
Configuration:Deploying STA Application completed successfully
Started Configuration:Restarting STA (this can take up to 30 minutes)
Configuration:Restarting STA (this can take up to 30 minutes) completed
successfully
Started Configuration:Post Configuration
Successfully moved logs to /var/log/tbi/install.
Configuration:Post Configuration completed successfully
The installation of STA_Install 2.1.0.0.0 completed successfully.
Logs successfully copied to /home/oracle/oraInventory/logs.
$
```

例B.6 失敗した STA サイレントモードインストールの最終メッセージの例

```
[ERROR] Rule_CalculateFreeSpace_Error. Aborting Install
Logs are located here: /tmp/OraInstall2014-09-24_09-29-29AM.
** Error during execution, error code = 256.
$
```

4. インストーラが正常に完了したら、STA が動作していることを確認します。手順については、「[正常なインストールの確認](#)」を参照してください。

B.4. STA サイレントモードアンインストーラのタスク

- 「[サイレントモードアンインストーラの応答ファイルの作成](#)」
- 「[サイレントモードアンインストーラの実行](#)」

B.4.1. サイレントモードアンインストーラの応答ファイルの作成

サイレントモードアンインストーラの応答ファイルを作成し、暗号化パスワードをそれに追加するには、次の手順を使用します。

1. Oracle インストールユーザーとしてログインします。
2. テキストエディタを使用して、任意の名前でアンインストーラの応答ファイルを作成します。ファイルテンプレートについては、[例B.2「STA サイレントモードアンインストーラの応答ファイルのテンプレート」](#)を参照してください。

テンプレートをテキストファイルにコピー&ペーストし、すべての変数を空白のままにします。

3. そのファイルを任意の名前と場所で保存します。
4. 応答ファイル構築ユーティリティがダウンロードされているディレクトリに移動します。このユーティリティの名前は `silentInstallUtility_version.jar` です。例:

```
$ cd /Installers
```

5. 応答ファイル構築ユーティリティを実行します。

```
$ java -jar silentInstallUtility_2.1.0.64.124.jar response_file
```

ここで、`response_file` は作成した応答ファイルの絶対パスです。

6. 各プロンプトに適切な情報で応答します。入力したパスワード値は画面に表示されません。

[例B.7「アンインストーラの応答ファイル構築ユーティリティの実行例」](#)は、ユーティリティの実行例です。

例B.7 アンインストーラの応答ファイル構築ユーティリティの実行例

```
$ java -jar silentInstallUtility_2.1.0.64.124.jar /Installers/SilentIDeinstall.rsp
Oracle StorageTek Tape Analytics Silent Installation Utility
```

```
-----
```

```
This utility is used to assist users with the password fields in the Silent
Installation response file. The silent installation process requires the
password fields in the response file requires the password fields to be
```

encrypted. The utility will ask the users for the required passwords, and encrypt these values, then update the values into the supplied response file.

```
Please enter the location to save the key file : /Installers
What is the response file used for? ('i' for Install, 'd' for Deinstall) : d
Enter system root password:
Confirm system root password:
```

7. ユーティリティーが完了したら、暗号鍵ファイルが作成されていることを確認します。これは、ランダムに生成された名前を持つ隠しファイルです。次に例を示します。

```
$ ls -la /Installers/.sk*
-r----- 1 oracle oinstall 17 Sep 22 12:00 .sk1414437879829
```

8. 応答ファイルを表示し、次の値を確認します。
 - システムの root パスワードが暗号化された値で更新されています。
 - `RESPONSEFILE_LOC` が正しい応答ファイルの場所で更新されています。
 - `KEYFILE_LOC` が暗号鍵ファイルの場所で更新されています。

例B.8「構築ユーティリティーの使用後のアンインストーラの応答ファイルの例」は、適切な値を示すファイル例です。

例B.8 構築ユーティリティーの使用後のアンインストーラの応答ファイルの例

```
$ view /Installers/SilentDeinst.rsp
[ENGINE]
#DO NOT CHANGE THIS. Response File Version=1.0.0.0.0
[GENERIC]
#This will be blank when there is nothing to be de-installed in distribution level
SELECTED_DISTRIBUTION=STA_Install~2.1.0.0.0
#Root access passsword var.
DEINSTALL ROOT ACCESS PASSWORD=zMZJYDbrhiRZUQL35r7uEg==
RESPONSEFILE_LOC=/Installers/silentdeinstall.rsp
KEYFILE_LOC=/Installers/.sk1414700056981
```

B.4.2. サイレントモードアンインストーラの実行

サイレントモードアンインストーラを使用して STA をアンインストールするには、次の手順を使用します。

1. Oracle インストールユーザーとしてログインします。
2. STA ホームディレクトリに移動します。例:

```
$ cd /Oracle/StorageTek_Tape_Analytics
```

3. STA ユーティリティーディレクトリに移動します。

```
$ cd oui/bin
```

4. STA サイレントモードアンインストーラを起動します。これらのパラメータの完全な定義については、「[STA インストーラコマンドオプション](#)」を参照してください。

```
$ ./deinstall.sh -silent -responseFile response_file -invPtrLoc pointer_file
```

ここでは:

- `-silent` はサイレントモードを示します。このパラメータは必須です。
- `-responseFile response_file` は STA アンインストーラの応答ファイルの絶対パスを示します。このパラメータは必須です。
- `-invPtrLoc pointer_file` は Oracle 中央インベントリポインタファイルの絶対パスを示します。このパラメータは、そのファイルが `/etc` ディレクトリに存在しない場合またはユーザーが別のファイルを使用する場合にのみ必須です。

例:

```
$ ./deinstall.sh -silent -responseFile /Installers/SilentDeinst.rsp -invPtrLoc /opt/oracle/oraInst.loc
```

5. アンインストーラが次のアンインストール手順を実行すると、ステータスメッセージが端末ウィンドウに表示されます。このプロセスは、完了するまでに最大 30 分かかります。

[例B.9「成功した STA サイレントモードアンインストールの最終メッセージ」](#)に、成功したアンインストールの最後に表示されるメッセージを示します。[例B.10「失敗した STA サイ](#)

「[レントモードアンインストールの最終メッセージの例](#)」に、失敗したアンインストールの最後の表示される可能性のあるいくつかのメッセージを示します。

例B.9 成功した STA サイレントモードアンインストールの最終メッセージ

```
...
Reading response file..
Starting silent deinstallation...
-----20%-----40%-----60%-----80%-----Successfully moved
logs to /var/log/tbi/install.
s/common/bin/uninstall.sh/mysql was removed, with s/common/bin/uninstall.sh left,
because there are user defined files in s/common/bin/uninstall.sh or it is a
mount point.
/dbdata/local was removed, with /dbdata left, because there are user defined files
in /dbdata or it is a mount point.
100%

The uninstall of STA_Install 2.1.0.0.0 completed successfully.
Logs successfully copied to /home/oracle/oraInventory/logs.
```

例B.10 失敗した STA サイレントモードアンインストールの最終メッセージの例

```
...
Reading response file..
Starting silent deinstallation...
-----20%-----40%-----60%-----80%-----Internal Error: File
Copy failed. Aborting Install
Logs are located here: /tmp/OraInstall2014-09-25_10-07-18AM.
```

- アンインストーラが完了したら、STA ディレクトリが削除されていることを確認します。手順については、「[アンインストールが成功したことの確認](#)」を参照してください。

B.5. STA インストーラコマンドオプション

このセクションでは、STA インストーラオプションの参照情報を示します。サイレントモードオプションは、サイレントモードのインストーラとアンインストーラで排他的に使用されます。ロギングやその他のオプションは、インストールとアンインストールの両方のモードで使用できます。

B.5.1. サイレントモードオプション

次のオプションは、サイレントモードのインストーラとアンインストーラで使用されます。

-force

空でないディレクトリへのサイレントモードインストールを可能にします。

-invPtrLoc *pointer_file*

`/etc/oraInst.loc`にあるものではなく、指定された Oracle 中央インベントリポインタファイルを使用します。`pointer_file` は絶対パスにする必要があります。

Oracle 中央インベントリファイルの内容は次のとおりです。

```
inventory_loc=Oracle_central_inventory_location
inst_group=Oracle_install_group
```

ここでは:

- `Oracle_central_inventory_location` は Oracle 中央インベントリの絶対パスです。
- `Oracle_install_group` は Oracle インストールグループの名前です。

-response、-responseFile *response_file*

サイレントモードに必須です。STA サイレントモードインストーラまたはアンインストーラの入力を含む応答ファイルの場所。`response_file` は絶対パスにする必要があります。

インストーラとアンインストーラの応答ファイルの内容については、[例B.1「STA サイレントモードインストーラの応答ファイルのテンプレート」](#)と[例B.2「STA サイレントモードアンインストーラの応答ファイルのテンプレート」](#)を参照してください。

-silent

サイレントモードに必須です。サイレントモードを使用することを示します。指定された応答ファイルから入力取得されます。

B.5.2. ロギングオプション

次のオプションを使用すると、インストーラおよびアンインストーラログで提供される情報の種類を制御できます。それらは、グラフィカルモードとサイレントモードの両方で使用できます。

-debug

デバッグ情報を記録します。一部のデバッグ情報はコンソールウィンドウにも表示されます。

-logLevel *level*

優先度レベルが指定されたレベルよりも低いログメッセージを省略します。`level` の値は次のとおりです。

- severe
- warning
- info
- config
- fine
- finer
- finest

-printdiskusage

ディスク使用量に関するデバッグ情報を記録します。

-printmemory

メモリー使用量に関するデバッグ情報を記録します。

-printtime

経過時間に関するデバッグ情報を記録します。

B.5.3. その他のオプション

次のコマンドオプションは一般的に使用されるものです。それらは、グラフィカルモードとサイレントモードの両方で使用できます。

-compatibilityFile *compatibility_file*

機能セットの依存関係の変更を指定するファイルの場所。

-executeSysPrereqs

インストーラの実行に備えてシステム環境の前提条件チェックを実行し、その後インストールを行わずに終了します。

-help

ヘルプを表示します。

-i, -install

グラフィカルモードを使用します。これはデフォルトです。

-J-Djava.io.tmpdir=*working_directory*

/tmp ではなく指定された作業ディレクトリに STA インストーラを展開します。*working_directory* は絶対パスにする必要があります。

-paramFile *initialization_file*

STA_home/oui/oraparam.ini にあるものではなく、指定された初期化ファイルを使用します。*initialization_file* は絶対パスにする必要があります。

STA インストーラは、前提条件チェックを含むすべての操作に、ユーザーが指定するファイルを使用します。デフォルトの場所は、*STA_home/oui* ディレクトリにあります。

インストールおよびアップグレードのワークシート

この付録のワークシートは、STA のインストールまたはアップグレードを実行するために、収集する必要がある情報やアクティビティを整理するうえで役立つ計画ツールとなっています。この付録には次のセクションが含まれます。

- [アップグレード準備ワークシート](#)
- [インストールおよびアップグレードのワークシート](#)
- [インストール後の構成ワークシート](#)

C.1. アップグレード準備ワークシート

以前のバージョンの STA からのアップグレードでは、[表C.1「アップグレード準備アクティビティ」](#)のみを使用します。これは、アップグレードの準備のために実行する、必須およびオプションのアクティビティの追跡に使用します。特別な計画情報を記録するには、「コメント」列を使用してください。これらのアクティビティの詳細は、[「アップグレード準備タスク」](#)を参照してください。

表C.1 アップグレード準備アクティビティ

アクティビティ	コメント	完了
現在の STA のバージョンがリリースされたバージョンであることを確認します。		
注: STA 1.0.x からアップグレードする場合、STA 2.1.0 をインストールする前に、新しいバージョンの Linux もインストールする必要があります。		
1 台のサーバーのアップグレード方法または 2 台のサーバーのアップグレード方法を選択します。		
サイトおよびターゲットが STA 2.1.0 の要件を満たしていることを確認します。		
/tmp ファイルシステムのサイズをアップグレード用に一時的に増やす必要があるかどうかを判断します。		

アクティビティ	コメント	完了
STA 2.1.0 に対する環境の変更がアップグレード計画に影響があるかどうかを確認します。		
すべての必要な RPM パッケージがインストールされていることを確認します (STA 2.0.x からのアップグレードのみ)。		
現在のバージョンの STA が最近、モニター対象ライブラリと正常に通信したことを確認します。		
STA がすべてのモニター対象ライブラリにわたって交換を処理していることを確認します。		
保持する必要があるインストールログおよびデータベースログを安全な場所に移動します (オプション)。		
現在の STA インストールでサービスログスナップショットを実行します (オプション)。		
保持する必要があるサービスログバンドルをダウンロードします (オプション)。		
接頭辞に「STA-」の付いたカスタムテンプレートの名前を変更します (オプション)。		
保持する必要がある現在のカスタムテンプレート設定を記録します (オプション)。		
保持する必要があるエグゼクティブレポートポリシー設定を記録します (オプション)。		

C.2. インストールおよびアップグレードのワークシート

これらのワークシートには、STA インストーラで必要な情報が含まれます。要求される情報の詳細は、「[STA のインストール中に構成されるアカウントおよびポート](#)」を参照してください。

以前のバージョンの STA からアップグレードする場合、ワークシートの「現在の値」列を使用して現在のインストールで使用されている値を記録します。STA 2.1.0 に使用する値を記録するには、「STA 2.1.0 の値」の列を使用します。

C.2.1. インストールユーザーおよび場所のワークシート

表C.2「[インストールユーザーおよび場所のワークシート](#)」には、STA インストーラの実行に必要なユーザーアカウントおよび場所が含まれます。

表C.2 インストールユーザーおよび場所のワークシート

項目	説明	現在の値	STA 2.1.0 の値
Oracle インストールグループ	STA サーバーへの Oracle 製品のインストールおよびアップグレードに使用する Linux グループ。STA 2.1.0 で新しくなっています。	-	
Oracle インストールユーザー	STA サーバーに Oracle 製品をインストールおよびアップグレードする Linux ユーザー。STA 2.1.0 で新しくなっています。	-	
Oracle 中央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 2.1.0 で新しくなっています。	-	
Oracle ストレージホームの場所	STA および関連する Oracle ソフトウェアがインストールされるディレクトリ。STA 2.1.0 で新しくなっています。	-	
STA インストーラの場所	STA インストーラがダウンロードされる場所。		
STA データベースデータの場所	STA データベースの場所。		
STA データベースのバックアップ場所	STA サーバー上の STA データベースのバックアップ場所。		

C.2.2. ユーザーアカウントワークシート

表C.3「ユーザーアカウントワークシート」には、STA の管理アクティビティを行うために使用するユーザーアカウント、および STA データベースをアクセスおよび管理するために STA アプリケーションによって内部的に使用される MySQL アカウントが含まれます。

注:

STA 2.1.0 では、パスワード要件が変更されています。詳細は、「[ユーザー名およびパスワードの要件](#)」を参照してください。

表C.3 ユーザーアカウントワークシート

アカウント	説明	現在のユーザー名 およびパスワード	STA 2.1.0 のユーザー名 およびパスワード
WebLogic の管理	WebLogic 管理コンソールへのログインに使用します。 警告: このアカウントのユーザー名およびパスワードは取得することができません。これらの資格証明を失った場合、STA を再インストールする必要があります。		
STA の管理者	フルアクセス権限で STA アプリケーションにログインする際に使用します。		
STA データベースルートユーザー	MySQL データベースを所有します。事前定義されたユーザー名 <i>root</i> は変更することができません。 警告: このアカウントのパスワードは取得することができません。	ユーザー名 = <i>root</i>	ユーザー名 = <i>root</i>
STA データベースアプリケーションユーザー	STA はこのアカウントを使用してデータベースに接続します。		
STA データベースレポートユーザー	STA 以外およびサードパーティーのアプリケーションは、このアカウントを使用してデータベースに接続します。		
STA データベース管理ユーザー	STA の管理およびモニタリングユーティリティは、このアカウントを使用してデータベースに接続し、主にスケジュールされたバックアップを実行します。		

C.2.3. ポート番号ワークシート

表C.4「構成不可の外部ポート」には STA アプリケーションで使用する外部ポートが含まれます。これらのポート番号は事前定義されているため、変更できません。ネットワーク管理者とともにこれらのポートが開かれ、使用可能であることを確認したことを記録するには、「確認済み」列を使用します。

表C.4 構成不可の外部ポート

ポートの説明	プロトコル	STA 2.1.0 確認済み ポート
セキュアシェル。STA サーバーから STA データベースバックアップ およびモニター対象ライブラリにログインする際に使用します。	SSH	22
モニター対象ライブラリへの Simple Network Management Protocol (SNMP) 要求の送信に使用します。	SNMP	161
モニター対象ライブラリからの SNMP 通知 (トラップ) の受信に使 用します。	SNMPTRAP	162

表C.5「構成可能な内部ポートおよび外部ポート」には、STA アプリケーションで使用する構成可能な外部ポートおよび内部ポートが含まれます。ネットワーク管理者とともにこれらのポートが開かれ、使用可能であることを確認したことを記録するには、「確認済み」列を使用します。

注:

デフォルトの WebLogic 管理コンソールのポートは、STA 2.1.0 では変更されています。

表C.5 構成可能な内部ポートおよび外部ポート

ポートの説明	タイプ	プロトコ ル	STA 2.1 .0 のデ フォルト ポート	現在の ポート	STA 2.1 .0 のポー ト	確認済 み
WebLogic 管理コンソール用の非セキュア なポート (STA 1.0.x および 2.0.x のデフォ ルトは 7001 でした)	外部	HTTP	7019			
WebLogic 管理コンソール用のセキュアな ポート (STA 1.0.x および 2.0.x のデフォルト は 7002 でした)	外部	HTTPS	7020			
STA GUI を管理する staUi 管理対象サー バーの非セキュアなポート	外部	HTTP	7021			
staUi 管理対象サーバーのセキュアなポート	外部	HTTPS	7022			
基本的な STA 内部を管理する staEngine 管理対象サーバーの非セキュアなポート	内部	HTTP	7023			

ポートの説明	タイプ	プロトコル	STA 2.1 .0 のデフォルトポート	現在のポート	STA 2.1 .0 のポート	確認済み
staEngine 管理対象サーバーのセキュアなポート	内部	HTTPS	7024			
モニター対象ライブラリとの SNMP 通信を管理する staAdapter 管理対象サーバーの非セキュアなポート	内部	HTTP	7025			
staAdapter 管理対象サーバーのセキュアなポート	内部	HTTPS	7026			

C.2.4. ドメイン名ワークシート

表C.6「会社のドメイン名」には、STA サービスログの生成時に、Oracle の Remote Diagnostic Agent (RDA) に使用されるサイトの完全修飾ドメイン名が含まれます。

表C.6 会社のドメイン名

必要な情報	現在の値	STA 2.1.0 の値
会社のドメイン名 (たとえば, us.example.com)		

C.3. インストール後の構成ワークシート

表C.7「SNMP v3 ユーザーの構成情報」には STA とモニター対象ライブラリとの間の SNMP 通信の構成に使用する情報が含まれます。各モニター対象ライブラリおよび STA インスタンスでは、同じ SNMP v3 ユーザーが構成される必要があります。要求される情報の詳細は、「一意の SNMP v3 ユーザー」を参照してください。

表C.7 SNMP v3 ユーザーの構成情報

必要な情報	以前の値	STA 2.1.0 の値
SNMP v3 ユーザー名		
SNMP v3 承認パスワード (承認)		
SNMP v3 プライバシ暗号化パスワード (プライバシー)		
SNMP v2c ユーザーコミュニティ		

必要な情報	以前の値	STA 2.1.0 の値
SNMP v2c トラップコミュニティ		

セキュリティ証明書の構成

Oracle は、HTTPS/SSL ポートで使用する自己生成セキュリティ証明書を提供します。インストール中に、STA は Java keytool を使用して、サーバーホスト名で STA サーバー上に証明書を生成します。オプションで、Oracle 証明書を、選択した認証局 (たとえば、VeriSign) からの独自の承認済み証明書に置き換えることができます。

この章には次のセクションが含まれます。

- [セキュリティ証明書の構成タスク](#)

D.1. セキュリティ証明書の構成タスク

デフォルトとは異なるセキュリティ証明書を使用する場合は、次の手順を示された順序で実行します。

- 「[初期 HTTPS/SSL 接続の確立](#)」
- 「[別のセキュリティ証明書を使用するように WebLogic を再構成](#)」
- 「[Oracle 証明書の置換](#)」

注:

これらの手順では、Windows プラットフォームで実行されている Mozilla Firefox を使用します。

D.1.1. 初期 HTTPS/SSL 接続の確立

1. 使用しているコンピュータでサポートされている Web ブラウザを起動し、STA アプリケーションの HTTPS/SSL バージョンの URL を入力します。

`https://STA_host_name:port_number/STA/`

ここでは:

- `host_name` は STA サーバーのホスト名です。
- `port_number` はインストール中に指定した STA ポート番号です。デフォルトの HTTP ポートは 7021 であり、デフォルトの HTTPS ポートは 7022 です。

- STA は大文字にする必要があります。

例:

`https://staserver.example.com:7022/STA/`

「接続の安全性を確認できません」画面が表示されます。

2. 「危険性を理解した上で接続するには」を選択してから、「例外を追加」をクリックします。

「セキュリティ例外の追加」画面が表示されます。

3. 「表示」をクリックします。

「証明書ビューア」画面が表示されます。証明書は認証局のものではないため、検証済みとして表示されません。

4. 証明書を調べるには、「詳細」タブをクリックします。
5. 「証明書のフィールド」パネルで、「**Issuer**」を選択します。表示の例を次に示します。「CN」は、証明書が生成されたサーバー名を示します。

CN = staserver.example.com

OU = Tape Systems

O = Oracle America Inc

L = Redwood City

ST = California

C = USA

6. 「閉じる」をクリックして「セキュリティ例外の追加」画面に戻ります。
7. 「セキュリティ例外を承認」を選択します。

証明書が STA サーバーに追加され、HTTPS を証明書とともに使用できるようになります。

D.1.2. 別のセキュリティ証明書を使用するように WebLogic を再構成

1. ブラウザウィンドウを開き、WebLogic 管理コンソールの URL を入力します。デフォルトの HTTP ポートは 7019 であり、デフォルトの HTTPS ポートは 7020 です。

`https://your_hostname:port number/console/`

例:

<https://staserver.company.com:7019/console/>

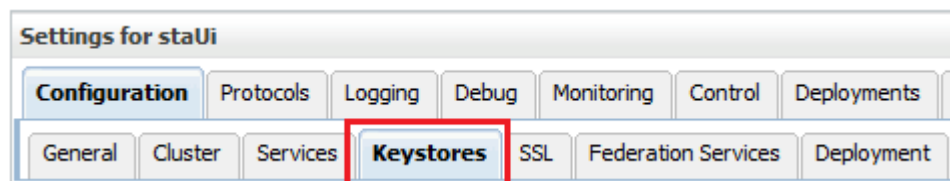
2. STA のインストール中に定義した WebLogic 管理コンソールのユーザー名とパスワードを使用してログインします。
3. 「ドメイン構造」セクションで、「環境」を選択してから、「サーバー」を選択します。



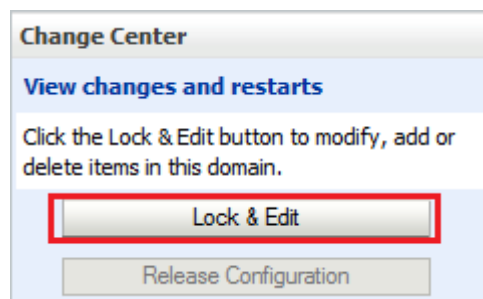
4. 「サーバー」テーブルで、「staUi」アクティブリンクを選択します (チェックボックスではなく、名前自体を選択します)。

<input type="checkbox"/>	Name ^	Cluster	Machine
<input type="checkbox"/>	AdminServer(admin)		
<input type="checkbox"/>	staAdapter	STA_Cluster1	
<input type="checkbox"/>	staEngine	STA_Cluster1	
<input type="checkbox"/>	staUi	STA_Cluster1	

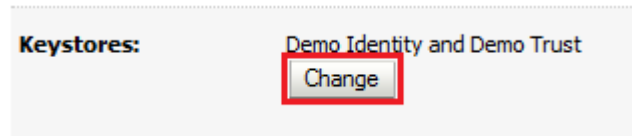
5. 「キーストア」タブを選択します。



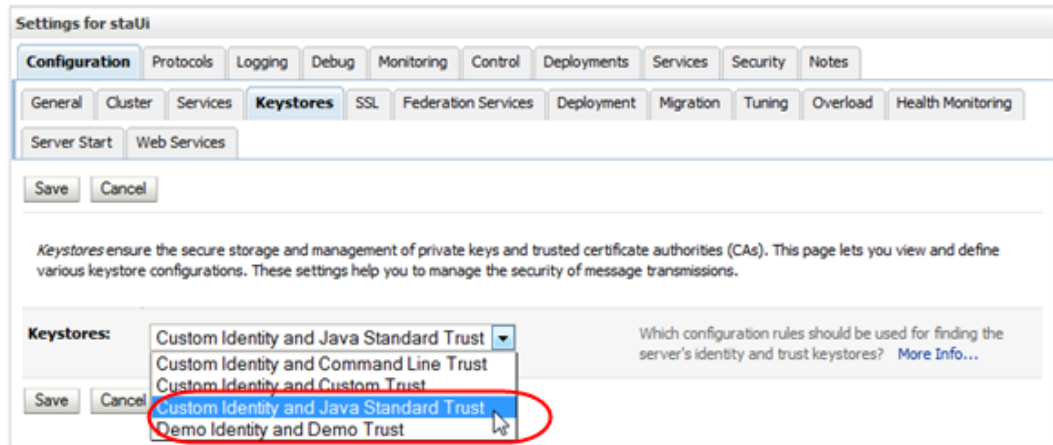
6. 「チェンジ・センター」セクションで、「ロックして編集」をクリックします。



7. 「キーストア」セクションで、「変更」をクリックします。



8. 「キーストア」メニューで、「カスタム・アイデンティティとJava標準信頼」を選択します。



9. 「保存」をクリックします。
10. 「キーストア」画面に次のように入力します。
- 「カスタム・アイデンティティ・キーストア」: 秘密鍵ファイルのパスとファイル。
 - 「カスタム・アイデンティティ・キーストアのタイプ」: キーストアのタイプ。RACF 認証用に構成する場合、PKCS12 と入力します。
 - 「カスタム・アイデンティティ・キーストアのパスフレーズ」: MVS システム管理者が指定したパスワード。
 - 「Java標準信頼キーストアのパスフレーズ」: Java 標準信頼キーストアファイルの新しいパスワード。

注意:

これらのパスワードを忘れた場合は、STA を再インストールする必要があります。

11. 「保存」をクリックします。
12. 「SSL」タブを選択します。

13. 秘密鍵の別名、および MVS システムプログラマが指定した秘密鍵のパスフレーズを入力します。

注:

秘密鍵の別名を決定するには、*keytool* コマンドを使用します。例:

```
# keytool -list -keystore CLTBI.PKCS12DR.D080411 -storetype PKCS12
```

```
Enter keystore password: (password from the MVS sysadmin)
```

```
Keystore type: PKCS12
```

```
Keystore provider: SunJSSE
```

```
Your keystore contains 1 entry
```

```
tbiclient, Aug 17, 2011, PrivateKeyEntry,
```

```
Certificate fingerprint (MD5):
```

```
9A:F7:D1:13:AE:9E:9C:47:55:83:75:3F:11:0C:BB:46
```

Settings for staUI

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores **SSL** Federation Services Deployment Migration Tuning Overload Health Monitoring

Server Start Web Services

Save

This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instance. These settings help you to manage the security of message transmissions.

Identity and Trust Locations: Keystores [Change](#) Indicates where SSL should find the server's identity (certificate and private key) as well as the server's trust (trusted CAs). [More Info...](#)

— Identity —

Private Key Location: from Custom Identity Keystore The keystore attribute that defines the location of the private key file. [More Info...](#)

Private Key Alias: The keystore attribute that defines the string alias used to store and retrieve the server's private key. [More Info...](#)

Private Key Passphrase: The keystore attribute that defines the passphrase used to retrieve the server's private key. [More Info...](#)

Confirm Private Key Passphrase:

Certificate Location: from Custom Identity Keystore The keystore attribute that defines the location of the trusted certificate. [More Info...](#)

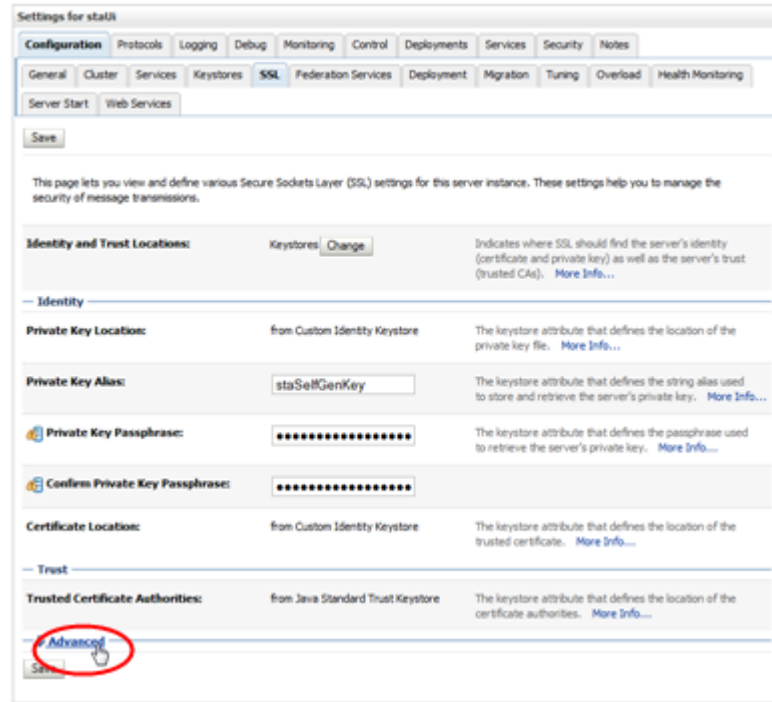
— Trust —

Trusted Certificate Authorities: from Java Standard Trust Keystore The keystore attribute that defines the location of the certificate authorities. [More Info...](#)

— Advanced —

Save

14. 「保存」をクリックします。
15. 「信頼性のある認証局」セクションで、「詳細」をクリックします。



16. 「SSL」画面の「詳細」セクションに次のように入力します。
 - a. 「サーバーの証明書を使用」チェックボックスを選択します。
 - b. 「相互クライアント証明書の動作」メニューから、「クライアント証明書をリクエスト (強制しない)」を選択します。
 - c. 「インバウンド証明書の検証」と「アウトバウンド証明書の検証」メニューで、「組み込みSSLの検証のみ」を選択します。

▼ Advanced

Hostname Verification: BEA Hostname Verifier ▼
Specifies whether to ignore the installed implementation of the `weblogic.security.SSL.HostnameVerifier` interface (when this server is acting as a client to another application server). [More Info...](#)

Custom Hostname Verifier:
The name of the class that implements the `weblogic.security.SSL.HostnameVerifier` interface. [More Info...](#)

Export Key Lifespan: 500
Indicates the number of times WebLogic Server can use an exportable key between a domestic server and an exportable client before generating a new key. The more secure you want WebLogic Server to be, the fewer times the key should be used before generating a new key. [More Info...](#)

Use Server Certs
Sets whether the client should use the server certificates/key as the client identity when initiating an outbound connection over https. [More Info...](#)

Two Way Client Cert Behavior: Client Certs Requested But Not Enforced ▼
The form of SSL that should be used. [More Info...](#)

Cert Authenticator:
The name of the Java class that implements the `weblogic.security.ad.CertAuthenticator` class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. [More Info...](#)

SSLRejection Logging Enabled
Indicates whether warning messages are logged in the server log when SSL connections are rejected. [More Info...](#)

Allow Unencrypted Null Cipher
Test if the `AllowUnencryptedNullCipher` is enabled. [More Info...](#)

Inbound Certificate Validation: Builtin SSL Validation Only ▼
Indicates the client certificate validation rules for inbound SSL. [More Info...](#)

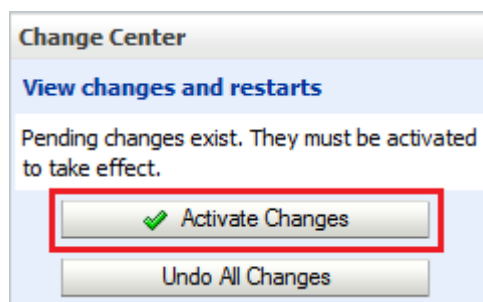
Outbound Certificate Validation: Builtin SSL Validation Only ▼
Indicates the server certificate validation rules for outbound SSL. [More Info...](#)

Use JSSE SSL
Select the JSSE SSL implementation to be used in Weblogic. [More Info...](#)

Save

17. 「保存」をクリックします。

18. 「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。



19. WebLogic からログアウトします。
20. STA コマンドを使用して STA を停止して再起動します。コマンドの使用の詳細は、『STA 管理ガイド』を参照してください。

```
# STA stop all
# STA start all
```

D.1.3. Oracle 証明書の置換

1. 使用しているコンピュータでサポートされている Web ブラウザを起動し、STA アプリケーションの HTTPS/SSL バージョンの URL を入力します。

```
https://STA_host_name:port_number/STA/
```

ここでは:

- *host_name* は STA サーバーのホスト名です。
- *port_number* はインストール中に指定した STA ポート番号です。デフォルトの HTTP ポートは 7021 であり、デフォルトの HTTPS ポートは 7022 です。
- STA は大文字にする必要があります。

例:

```
https://staserver.example.com:7022/STA/
```

2. 「接続の安全性を確認できません」画面で「危険性を理解した上で接続するには」を選択します。
3. 「例外を追加」をクリックします。
4. 組織の証明書を指定するには、「セキュリティ例外の追加」画面で「証明書を取得」をクリックして、適切なファイルを選択します。
5. 「セキュリティ例外を承認」をクリックします。

セキュリティサービスプロバイダの STA 用の構成

ユーザーの STA へのアクセスを許可する前に、ユーザーを認証する必要があります。STA 内でローカルにユーザーを作成するか、外部のセキュリティサービスプロバイダ (SSP) を使用して STA へのアクセス制御を提供できます。

この付録では、WebLogic OpenLDAP (Lightweight Directory Access Protocol) および IBM RACF (Resource Access Control Facility) の STA アクセス制御用の使用方法について説明します。次のセクションがあります。

- [WebLogic OpenLDAP による STA のアクセス制御](#)
- [IBM RACF タスクによる STA のアクセス制御](#)

STA アプリケーションを使用してユーザーを作成するには、『[STA ユーザーズガイド](#)』を参照してください。

E.1. WebLogic OpenLDAP による STA のアクセス制御

OpenLDAP を STA 用に構成するには、この手順を使用します。

E.1.1. WebLogic OpenLDAP の構成

1. STA のインストール中に選択した HTTP (STA 2.1.0 のデフォルトは 7019) または HTTPS (STA 2.1.0 のデフォルトは 7020) 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。

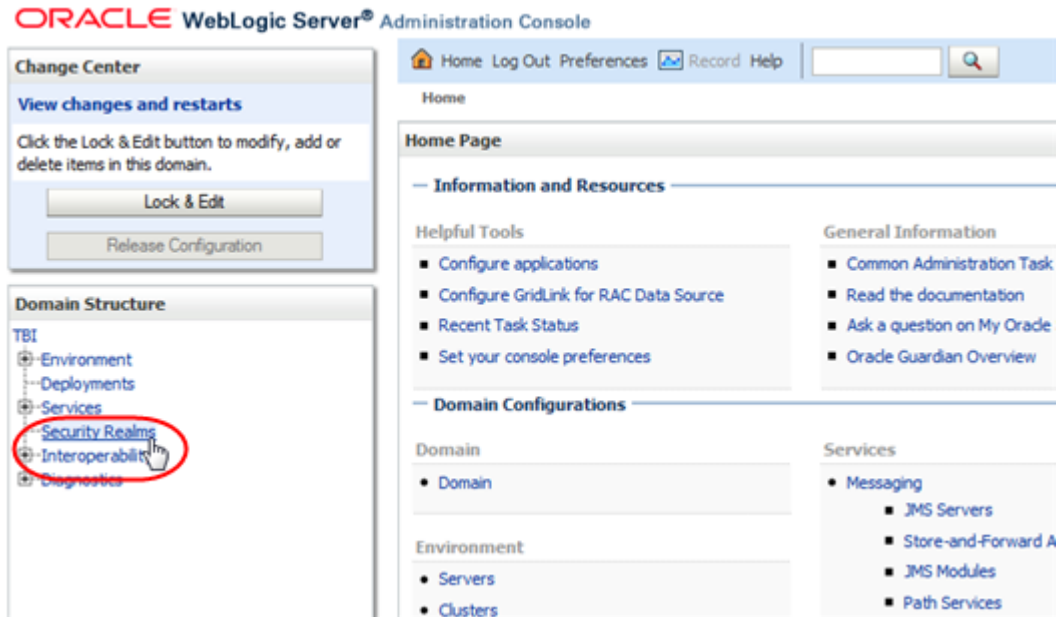
```
https://yourHostName:PortNumber/console/
```

例:

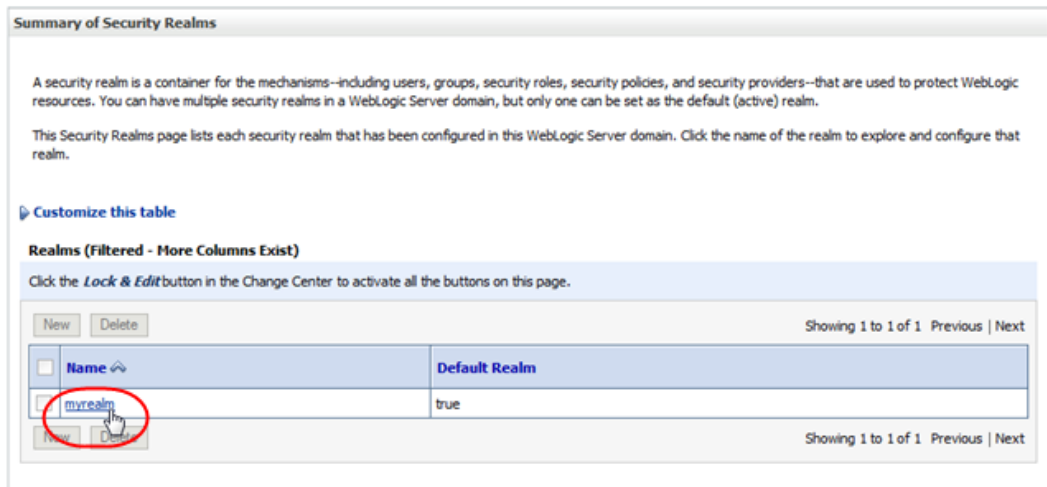
```
https://sta_server:7020/console
```

2. STA のインストール中に定義した 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。

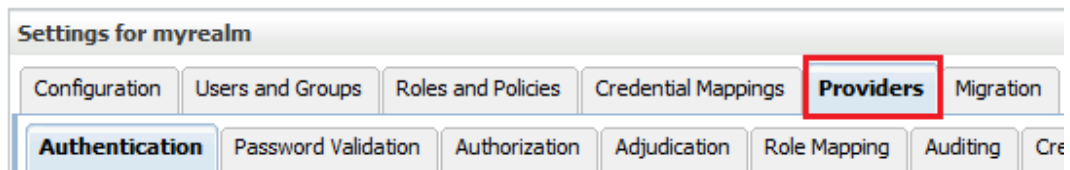
- 「Domain Structure」セクションで、「Security Realms」をクリックします。



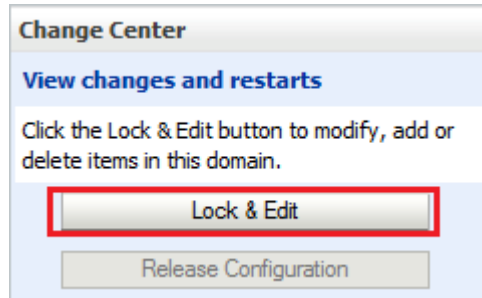
- 「Realms」の表で、「myrealm」アクティブリンクを選択します (チェックボックスではなく、リンク自体を選択します)。



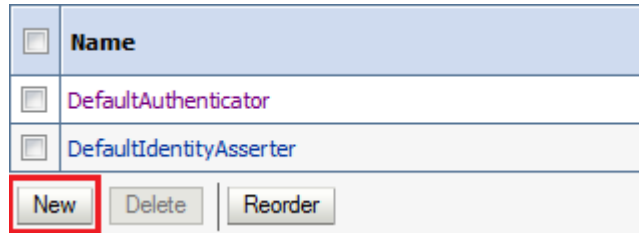
- 「Providers」タブをクリックします。



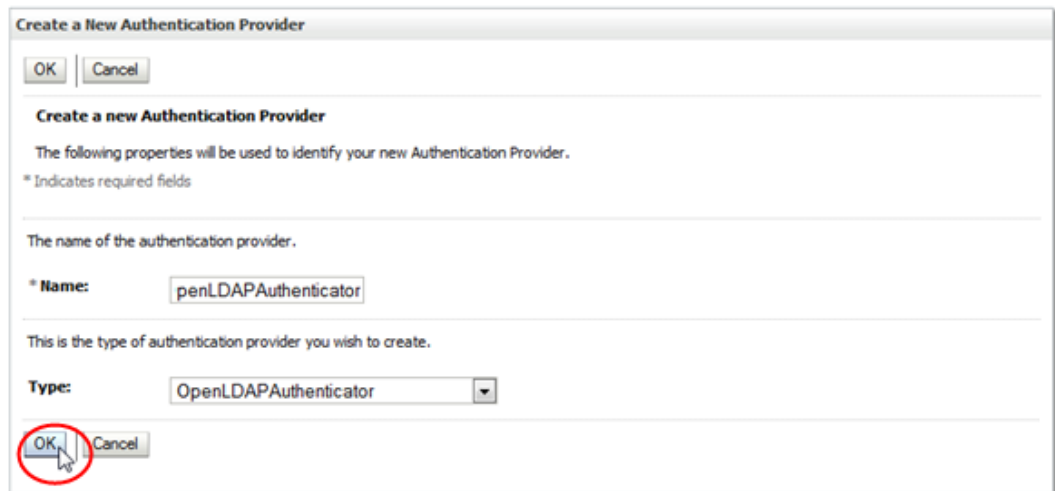
- 「チェンジ・センター」セクションで、「ロックして編集」をクリックします。



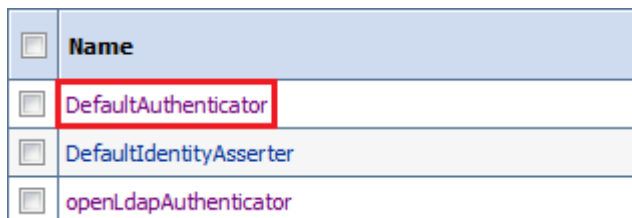
7. 「Authentication Providers」セクションで、「New」をクリックします。



8. 作成する認証プロバイダの名前 (たとえば、OpenLdapAuthenticator) を入力して、「Type」メニューで「OpenLDAPAuthenticator」を選択します。「OK」をクリックします。



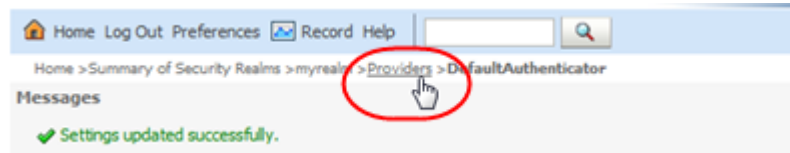
9. 「DefaultAuthenticator」アクティブリンクを選択します (チェックボックスではなく、リンク自体を選択します)。



10. 「Control Flag」メニューで、「Sufficient」を選択し、「Save」をクリックします。



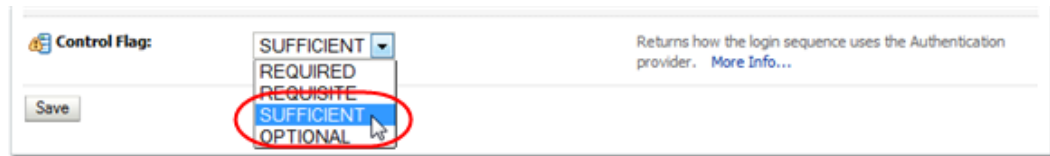
11. 「Providers」ロケータリンクを選択して、「Authentication Providers」画面に戻ります。



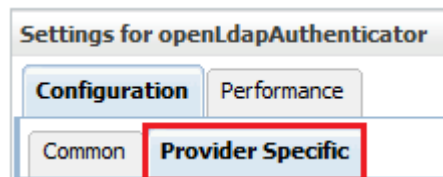
12. 「Authentication Providers」の表で、手順 8 で作成した OpenLDAP オーセンティケータ名を選択します (チェックボックスではなく、名前自体を選択します)。

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider
<input type="checkbox"/>	openLdapAuthenticator	Provider that performs LDAP authentication

13. 「Control Flag」メニューで、「Sufficient」を選択し、「Save」をクリックします。



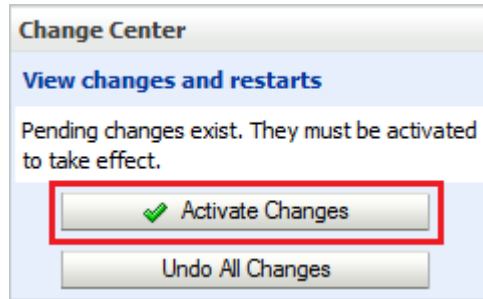
14. 「Provider Specific」タブをクリックします。



15. サイトの要件に従って、画面のフィールドに入力します。次の例は、*1ses-1dap1* サーバーに適用され、各カスタマ環境固有のものです。

- 「Host」 = *1ses-1dap1*
- 「Port」 = *389*
- 「Principal」 = 空白のまま
- 「Credential」 = 空白のまま
- 「User Base DN」 = *ou=people,o=STA,dc=oracle,dc=com*
- 「User From Name Filter」 = *(&(cn=%u)(objectclass=inetOrgPerson))*

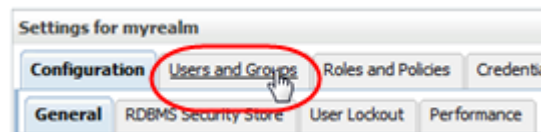
- 「User Object Class」 = *inetOrgPerson*
 - 「Group Base DN」 = *ou=groups,o=STA,dc=oracle,dc=com*
 - 「Group From Name Filter」 = *(&(cn=%g)(objectclass=groupofnames))*
16. 「保存」をクリックします。
17. 「チェンジ・センター」セクションで、「変更のアクティブ化」をクリックします。



18. 次の手順を実行して構成をテストします。
- WebLogic 管理コンソールからログアウトします。
 - STA コマンドを使用して STA を停止して再起動します。コマンドの使用方法の詳細は、『STA 管理ガイド』を参照してください。

```
# STA stop all
# STA start all
```

- WebLogic コンソールにログインします。
- 「Domain Structure」セクションで、「Security Realms」を選択します。
- 「Realms」の表で、「myrealm」アクティブリンクを選択します (チェックボックスではなく、リンク自体を選択します)。
- 「Users and Groups」タブをクリックします。



- 「Users」タブと「Groups」タブ内で、OpenLDAP プロバイダの「Provider」列にエントリが存在することを確認します。

E.2. IBM RACF タスクによる STA のアクセス制御

IBM RACF (Resource Access Control Facility) 認証を STA 用に構成するには、次の手順を使用します。示された順に手順を実行する必要があります。

- 「タスク 1: IBM RACF メインフレームの最小要件の確認」
- 「タスク 2: STA RACF 承認のためのメインフレームサポートの有効化」
- 「タスク 3: AT-TLS の構成」
- 「タスク 4: CGI ルーチンによって使用される RACF プロファイルの作成」
- 「タスク 5: 証明書ファイルと秘密鍵ファイルのインポート (オプション)」
- 「タスク 6: CGI ルーチンのテスト」
- 「タスク 7: WebLogic コンソール用の RACF/SSP の設定」
- 「タスク 8: STA と RACF 間の SSL の構成」
- 「タスク 9: WebLogic Server の構成」
- 「タスク 10: WebLogic コンソールでの RACF/SSP のインストール」

注:

STA では、CA の ACF-2 や Top Secret など、IBM RACF との互換性があるサードパーティーの製品がサポートされます。インストールされているセキュリティ製品に適したコマンドを発行するかどうかは、STA をインストールするユーザーまたはセキュリティ管理者が決定します。

E.2.1. タスク 1: IBM RACF メインフレームの最小要件の確認

完全な RACF 要件については、『STA 要件ガイド』を参照してください。

E.2.2. タスク 2: STA RACF 承認のためのメインフレームサポートの有効化

STA の RACF サービスのメインフレーム側は、ELS 7.0 および 7.1 用の SMC コンポーネントの一部である CGI ルーチンによって提供されます。この CGI ルーチンは SMC HTTP サーバーによって呼び出され、FACILITY クラスで定義された RACF プロファイルを使用します。

STA が RACF をアクセス認証の手段として使用するためには、HTTP サーバーを実行する SMC 開始タスクをメインフレームで設定する必要があります。これを行う方法の詳細は、ELS ドキュメントの「SMC の構成と管理」にあります。

注:

SMC 開始タスクは、定義されている AT-TLS ルールと一致する必要があります。または、AT-TLS 定義で汎用ジョブ名 (たとえば、SMCW) を使用できます。

値が指定された STC 識別子 (たとえば、JOBNAME.JOB) を使用する場合、これによって CGI ルーチンの接続が失敗します。

HTTP サーバーに使用するポート番号は、WebLogic Console で定義されているポート番号と一致する必要があり、ホストは、SMC タスクが実行されるホストの IP 名と一致する必要があります。

注:

既存の SMC は、RACF 承認が実行されるホスト上に存在する場合に使用できます。この場合、WebLogic 構成の実行時に既存の HTTP サーバーのポート番号を使用してください。

E.2.3. タスク 3: AT-TLS の構成

AT-TLS は、アプリケーションサーバーとクライアントに対して透過的な TCP/IP アプリケーションの暗号化ソリューションです。パケットの暗号化および復号化は、z/OS TCPIP アドレス空間で TCP プロトコルレベルで行われます。RACF 承認のための AT-TLS の要件は、『STA 要件ガイド』に記載されています。

次の RACF コマンドは、構成プロセスで定義するさまざまな RACF オブジェクトのステータスを一覧表示します。

- *RLIST STARTED PAGENT.* STDATA ALL*
- *RLIST DIGTRING *ALL*
- *RLIST FACILITY IRR.DIGTCERT.LISTRING ALL*
- *RLIST FACILITY IRR.DIGCERT.LST ALL*
- *RLIST FACILITY IRR.DIGCERT.GENCERT ALL*
- *RACDCERT ID(stcuser) LIST*
- *RACDCERT ID(stcuser) LISTRING(keyringname)*
- *RACDCERT CERTAUTH LIST*

AT-TLS を構成するには、次をします。

1. TCPIP プロファイルデータセットで次のパラメータを指定して、AT-TLS をアクティブ化します。

TCPCONFIG TTLS

この文は、TCP OBEY ファイル内に配置してもかまいません。

2. ポリシーエージェントの構成 (PAGENT)

ポリシーエージェントアドレス空間は、暗号化される TCP/IP トラフィックを制御します。

- a. **PAGENT** 開始タスク JCL を入力します。

例:

```
//PAGENT PROC
//*
//PAGENT EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
// PARM='POSIX(ON) ALL31(ON) ENVAR("_CEE_ENVFILE=DD:STDENV")/-d1'
//*
//STDENV DD DSN=pagentdataset,DISP=SHR//SYSPRINT DD SYSOUT=*
//SYSOUT DD SYSOUT=*
//*
//CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
```

- b. **PAGENT** 環境変数を入力します。*pagentdataset* データセットには、**PAGENT** 環境変数が含まれます。

例:

```
LIBPATH=/lib:/usr/lib:/usr/lpp/ldapclient/lib:.
PAGENT_CONFIG_FILE=/etc/pagent.conf
PAGENT_LOG_FILE=/tmp/pagent.log
PAGENT_LOG_FILE_CONTROL=3000,2
_BPXK_SETIBMOPT_TRANSPORT=TCPIP
TZ=MST7MDT
```

この例では、*/etc/pagent.conf* に **PAGENT** 構成パラメータが含まれています。*TZ* パラメータには独自のタイムゾーンを使用してください。

- c. **PAGENT** を構成します。

例:

```
TTLRule TBI-T0-ZOS
{
  LocalAddr localtcpipaddress
  RemoteAddr remotetcpipaddress
  LocalPortRange localportrange
}
```

```
RemotePortRange remoteportrange
Jobname HTTPserverJobname
Direction Inbound
Priority 255
TTLSTLSGroupActionRef gAct1~TBI_ICSF
TTLSEnvironmentActionRef eAct1~TBI_ICSF
TTLSTLSConnectionActionRef cAct1~TBI_ICSF
}
TTLSTLSGroupAction gAct1~TBI_ICSF
{
  TTLSEnvironmentAction eAct1~TBI_ICSF
  {
    HandshakeRole Server
    EnvironmentUserInstance 0
    TTLSTLSKeyringParmsRef keyR~ZOS
  }
  TTLSTLSConnectionAction cAct1~TBI_ICSF
  {
    HandshakeRole ServerWithClientAuth
    TTLSTLSCipherParmsRef cipher1~AT-TLS__Gold
    TTLSTLSConnectionAdvancedParmsRef cAdv1~TBI_ICSF
    CtraceClearText Off
    Trace 2
  }
  TTLSTLSConnectionAdvancedParms cAdv1~TBI_ICSF
  {
    ApplicationControlled Off
    HandshakeTimeout 10
    ResetCipherTimer 0
    CertificateLabel certificatelabel
    SecondaryMap Off
  }
  TTLSTLSKeyringParms keyR~ZOS
  {
```

```

Keyring keyringname
}
TTLSCipherParms cipher1~AT-TLS__Gold
{
V3CipherSuites TLS_RSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites TLS_RSA_WITH_AES_128_CBC_SHA
}

```

ここでは:

- *localtcpipaddress*: HTTP サーバーのローカル TCP/IP アドレス
 - *remotetcpipaddress*: STA クライアントのリモート TCP/IP アドレス。これは、すべての TCP/IP アドレスで ALL にできます
 - *localportrange*: HTTP サーバーのローカルポート (HTTP または SMC の起動で指定されます)
 - *remoteportrange*: リモートポートの範囲 (すべてのエフェメラルポートで 1024-65535)
 - *HTTPserverJobname*: HTTP サーバーのジョブ名
 - *certificateLabel*: 認証定義からのラベル
 - *keyringname*: RACF 鍵リング定義からの名前
3. RACF クラスをアクティブ化します。RACF パネルまたは CLI のいずれかを使用できます。

RACF クラスには、次のものが含まれます。

- *DIGTCERT*
- *DIGTNMAP*
- *DIGTRING*

PORTMAP および *RXSERV* が異常終了しないようにするには、*SERVAUTH* クラスを *RACLIST* する必要があります。

```

SETROPTS RACLIST(SERVAUTH)
RDEFINE SERVAUTH **UACC(ALTER) OWNER (RACFADM)
RDEFINE STARTED PAGENT*.* OWNER(RACFADM) STDATA(USER(TCPIP) GROUP(STCGROUP)
RDEFINE FACILITY IRR.DIGTCERT.LISTRING UACC(NONE) OWNER(RACFADM)
RDEFINE FACILITY IRR.DIGTCERT.LIST UACC(NONE) OWNER(RACFADM)

```

```
RDEFINE FACILITY IRR.DIGTCERT.GENCERT UACC(NONE) OWNER (RACFADM)
```

4. RACF 鍵リングと証明書の定義

- a. 鍵リングと証明書を作成するには、次の RACF コマンドを入力します。

```
RACDCERT ID(stcuser) ADDRING(keyringname)
```

ここでは:

- *stcuser*: TCPIP アドレス領域に関連付けられた RACF ユーザー ID
- *keyringname*: 鍵リングの名前で、PAGENT 構成で指定した鍵リングと一致する必要があります

```
RACDCERT ID(stcuser) GENCERT CERTAUTH SUBJECTSDN(CN('serverdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('calabel') TRUST
SIZE(1024) KEYUSAGE(HANDSHAKE, DATAENCRYPT, CERTSIGN)
```

注:

これは、STA システムの CA 証明書です。

ここでは:

- *stcuser*: TCPIP アドレス領域に関連付けられた RACF ユーザー ID
- *serverdomainname*: z/OS サーバーのドメイン名 (たとえば、*MVSA* .*COMPANY.COM*)
- *companyname*: 組織名
- *unitname*: 組織単位名
- *country*: 国
- *calabel*: 認証局のラベル (たとえば、*CATBISERVER*)

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('serverdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('serverlabel') TRUST
SIZE(1024) SIGNWITH(CERTAUTH LABEL('calabel'))
```

注:

これは、サーバー証明書です。

ここでは:

- *stcuser*: TCPIP アドレス領域に関連付けられた RACF ユーザー ID
- *serverdomainname*: z/OS サーバーのドメイン名 (たとえば、MVSA .COMPANY.COM)
- *companyname*: 組織名
- *unitname*: 組織単位名
- *country*: 国
- *serverlabel*: サーバー証明書のラベル (たとえば、TBISERVER)
- *calabel*: CA 証明書定義で指定した認証局のラベル

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('clientdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('clientlabel') TRUST
SIZE(1024) SIGNWITH(CERTAUTH LABEL('calabel'))
```

注:

これは、クライアント証明書です。

ここでは:

- *stcuser*: TCPIP アドレス領域に関連付けられた RACF ユーザー ID
- *clientdomainname*: STA クライアントのドメイン名 (たとえば、TBIA .COMPANY.COM)
- *companyname*: 組織名
- *unitname*: 組織単位名
- *country*: 国
- *clientlabel*: サーバー証明書のラベル – TBICLIENT
- *calabel*: CA 証明書定義で指定した認証局のラベル。

- b. PAGENT 構成で指定された鍵リングに CA、サーバー、およびクライアント証明書を接続します。

```
RACDCERT ID(stcuser) CONNECT(CERTAUTH LABEL('calabel') RING('keyringname')
USAGE(CERTAUTH))
```

ここでは:

- *stcuser*: TCPIP アドレス領域に関連付けられた RACF ユーザー ID
- *calabel*: CA 証明書定義で指定した認証局のラベル

- *keyringname*: 鍵リングの名前で、PAGENT 構成で指定した鍵リングと一致する必要があります

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('serverlabel')
RING('keyringname') DEFAULT USEAGE(PERSONAL)
```

ここでは:

- *stcuser*: TCPIP アドレス領域に関連付けられた RACF ユーザー ID
- *serverlabel*: サーバー証明書のラベル
- *keyringname*: 鍵リングの名前で、PAGENT 構成で指定した鍵リングと一致する必要があります

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('clientlabel')
RING('keyringname') USEAGE(PERSONAL)
```

ここでは:

- *stcuser*: TCPIP アドレス領域に関連付けられた RACF ユーザー ID
- *clientlabel*: クライアント証明書のラベル
- *keyringname*: 鍵リングの名前で、PAGENT 構成で指定した鍵リングと一致する必要があります

- c. STA に送信される CA およびクライアント証明書をエクスポートします。

```
RACDCERT EXPORT (LABEL('calabel')) CERTAUTH DSN('datasetname') FORMAT(CERTB64)
```

ここでは:

- *calabel*: CA 証明書定義で指定した認証局のラベル
- *datasetname*: エクスポートされる証明書を受け取るデータセット

```
RACDCERT EXPORT (LABEL('clientlabel')) ID(stcuser) DSN('datasetname')
FORMAT(PKCS12DER) PASSWORD(' password ')
```

ここでは:

- *clientlabel*: クライアント証明書のラベル

- *stcuser*: TCPIP アドレス領域に関連付けられた RACF ユーザー ID
- *datasetname*: エクスポートされる証明書を受け取るデータセット
- *password*: データ暗号化のパスワード。STA で証明書が受け取られるときに必要です。パスワードは、8 文字以上である必要があります。

これで、エクスポートされたデータセットは STA に転送され、FTP を使用できます。CA 証明書は、EBCDIC から ASCII に変換されて送信されます。CLIENT 証明書はバイナリファイルとして送信され、クライアント証明書とその秘密鍵の両方を含んでいます。

E.2.4. タスク 4: CGI ルーチンによって使用される RACF プロファイルの作成

プロファイルは、FACILITY クラスで定義されます。最初のプロファイルは *SMC.ACCESS.STA* と呼ばれ、ユーザーが STA アプリケーションにアクセスできるかどうかを決定します。

STA へのアクセスを要求するユーザーは、このプロファイルに対する READ アクセス権を持っている必要があります。ほかのプロファイルはすべて、*SMC.ROLE.nnn* として表示され、ユーザーがログオン後に持つ役割を決定するために使用されます。

注:

STA に対して定義されている役割は *StorageTapeAnalyticsUser* のみです。この役割を取得するには、READ アクセス権を持つ *SMC.ROLE.STORAGETAPEANALYTICSUSER* プロファイルに追加するユーザー ID を要求する必要があります。

E.2.5. タスク 5: 証明書ファイルと秘密鍵ファイルのインポート (オプション)

公開鍵と秘密鍵が正常に生成されたことと、適切な権限を持つユーザー ID とパスワードが正しく定義されていることをテストするために、この手順が役に立つことがあります。

テストは、任意のブラウザを使用して行うことができますが、ここでは Firefox が例として使用されています。

1. Firefox の「ツール」メニューで、「オプション」を選択します。
2. 「詳細」タブ、「証明書」タブの順に選択します。
3. 「証明書を表示」をクリックします。
4. 「証明書マネージャー」ダイアログボックスで「認証局証明書」タブをクリックして、インポートする証明書ファイルを選択します。
5. 「インポート」をクリックします。

6. 「あなたの証明書」タブを選択して、インポートする秘密鍵ファイルを入力します。
7. 「インポート」をクリックします。
8. 「OK」をクリックして、保存してダイアログボックスを閉じます。

E.2.6. タスク 6: CGI ルーチンのテスト

CGI ルーチンをブラウザからテストするには、次の URL を入力します。*host*、*port*、*userid*、および *password* は適切な値に設定されています。

```
https://host:port/smcgsaf?  
type=authentication&userid=userid&password=password&roles=StorageTapeAnalyticsUser
```

結果として表示される出力は、ユーザーが STA および *StorageTapeAnalyticsUser* 役割へのアクセスを承認されているかどうかを示します。

注:

STA RACF 承認機能では、メインフレームユーザー ID のパスワードの変更はサポートされません。ユーザー ID のパスワードが期限切れになった場合、STA はこれを示します。STA へのログインを再試行する前に、通常のメインフレームチャネルからパスワードをリセットする必要があります。

E.2.7. タスク 7: WebLogic コンソール用の RACF/SSP の設定

RACF セキュリティーサービスプロバイダ (または RACF SSP) は、プラグインとして WebLogic にインストールされている必要があります。

RACF SSP がインストールされている場合、STA インストーラは RACF SSP を WebLogic 内の適切な場所に配置するはずですが、インストールされていない場合、次のようにディレクトリに RACF セキュリティー *jar* ファイルを配置してください。

```
/Oracle_storage_home/Middleware/wlserver_10.3/server/lib/mbeantypes/staRACF.jar
```

ここで *Oracle_storage_home* は、STA のインストール中に指定された Oracle ストレージホームの場所です。

E.2.8. タスク 8: STA と RACF 間の SSL の構成

1. 必要な PTF を MVS システムにインストールします。これらの PTF により、STA へのログイン時に、RACF またはその他のサードパーティーのセキュリティソフトウェアでの認証が可能になります。PTF 要件については、『STA 要件ガイド』を参照してください。

Application Transparent TLS (AT-TLS) は、SMC HTTP サーバーおよび WebLogic に対して定義されたポート番号がサーバーに暗号化されるように、MVS 上に構成されています。

続行する前に、MVS サーバー証明書 (ASCII 形式) と STA クライアント秘密鍵 (バイナリ PKCS12 形式) の 2 つのファイルを所有していることを確認してください。MVS システム管理者により、PKCS12 ファイルへのパスワードが提供されています。

2. 証明書を `/Oracle_storage_home/Middleware/user_projects/domains/tbi/cert` に配置します。

ここで `Oracle_storage_home` は、STA のインストール中に指定された Oracle ストレージホームの場所です。

3. 証明書を DER 形式から PEM 形式に変換します。

```
openssl pkcs12 -clcerts -in PKCS12DR.xxxxxx -out mycert.pem
```

インポートパスワード (証明書とともに提供されます)、新しい PEM パスワード、およびパスワードの確認を入力するよう求められます。

4. Java keytool コマンドを使用して、証明書ファイルを `/Oracle_storage_home/Middleware/jdk1.6.0_xx/jre/lib/security/cacerts` ファイルにインポートします。

```
# /Oracle_storage_home/Middleware/jdk1.6.0_xx/jre/bin/keytool -importcert -alias  
tbiServer -file certificate -keystore /Oracle/Middleware/jdk1.6.0_xx/jre/lib/  
security/cacerts -storetype jks
```

E.2.9. タスク 9: WebLogic Server の構成

RACF 認証のために WebLogic を構成するには、「[別のセキュリティー証明書を使用するよ
うに WebLogic を再構成](#)」の手順に従います

E.2.10. タスク 10: WebLogic コンソールでの RACF/SSP のインストール

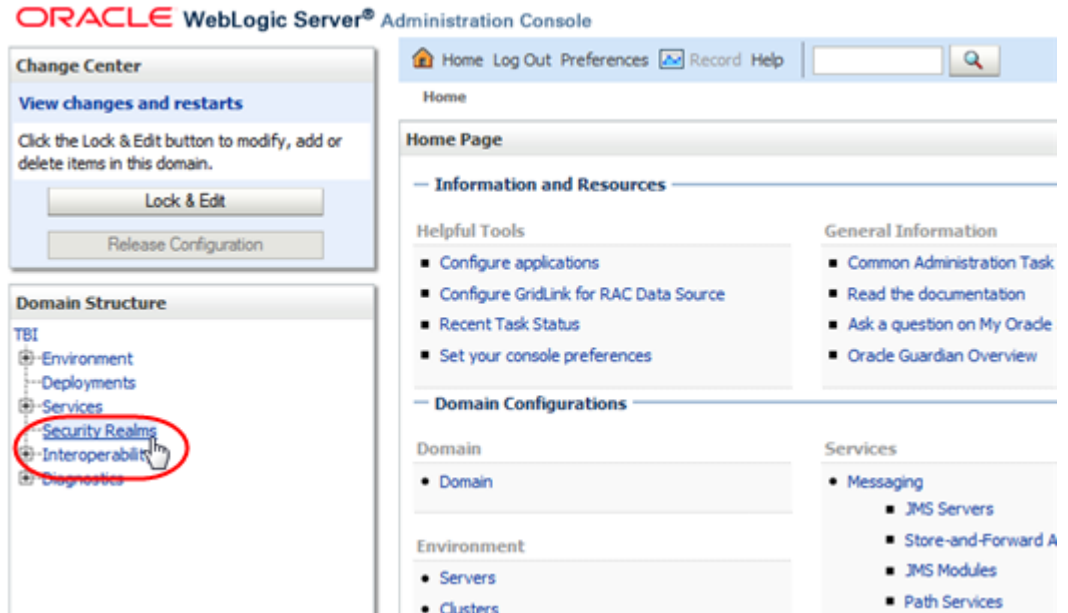
1. STA のインストール中に選択した HTTP (STA 2.1.0 のデフォルトは 7019) または HTTPS (STA 2.1.0 のデフォルトは 7020) のポート番号を使用して、WebLogic コンソールのログイン画面に移動します。

```
https://yourHostName:PortNumber/console/
```

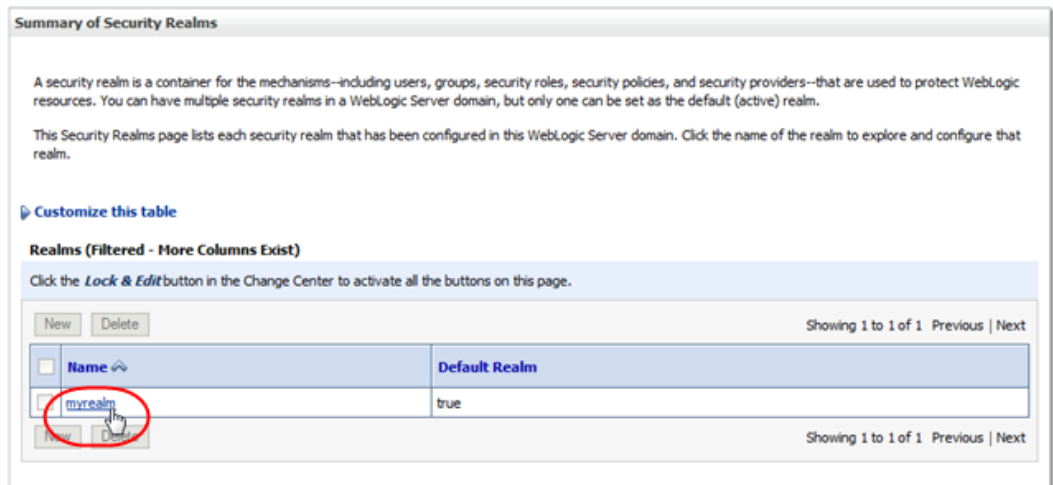
例:

https://sta_server:7020/console/

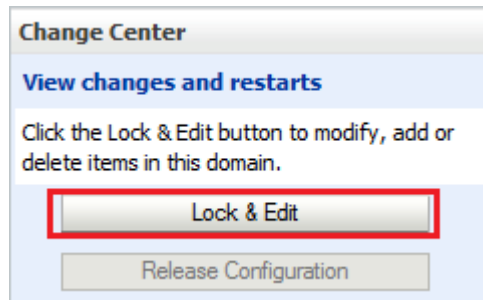
2. STA のインストール中に定義した WebLogic 管理コンソールのユーザー名とパスワードを使用してログインします。
3. 「Domain Structure」セクションで、「**Security Realms**」を選択します。



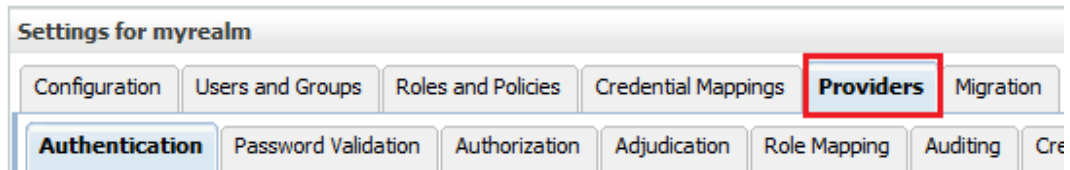
4. 「Realms」のセクションで、「**myrealm**」アクティブリンクを選択します (チェックボックスではなく、名前自体を選択します)。



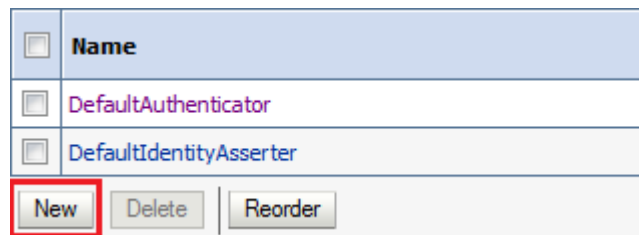
5. 「Change Center」セクションで「**Lock & Edit**」をクリックします。



6. 「Providers」タブを選択します。



7. 「Authentication Providers」セクションで、「New」をクリックします。



8. 追加する認証プロバイダの名前 (たとえば、*STA RacfAuthenticator*) を入力して、「Type」メニューの「*RacfAuthenticator*」を選択します。「OK」をクリックします。

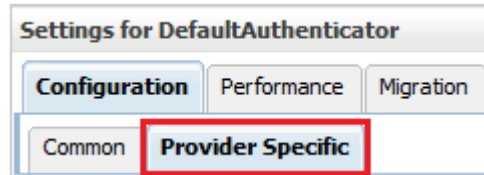
注:

RACF jar ファイルが「Type」メニューに表示されるはずですが、そうではない場合、*STA* コマンドを使用して *STA* を停止して再起動します。コマンドの使用の詳細は、『*STA 管理ガイド*』を参照してください。

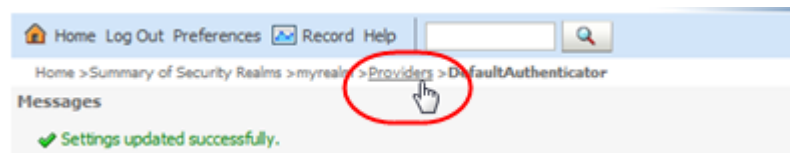
9. RACF プロバイダが「Authentication Providers」表に含められたことを確認します。*DefaultAuthenticator* および *DefaultIdentityAsserter* が常にリストの最初の 2 つのプロバイダでなければなりません。
10. 「DefaultAuthenticator」アクティブリンクを選択します (チェックボックスではなく、名前自体を選択します)。

<input type="checkbox"/>	Name
<input type="checkbox"/>	DefaultAuthenticator
<input type="checkbox"/>	DefaultIdentityAsserter
<input type="checkbox"/>	RacfAuthenticator

11. 「**Control Flag**」メニューで、「Sufficient」を選択し、「Save」をクリックします。
12. 「**Provider Specific**」タブをクリックして、「Save」をクリックします。



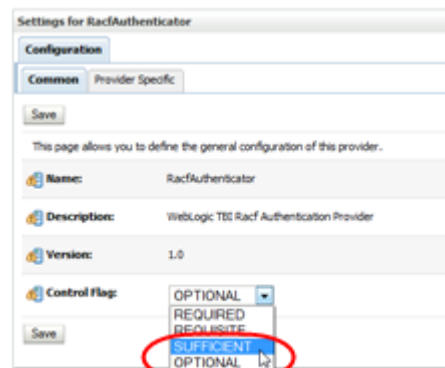
13. 「**Providers**」ロケータリンクをクリックして、「Authentication Providers」画面に戻ります。



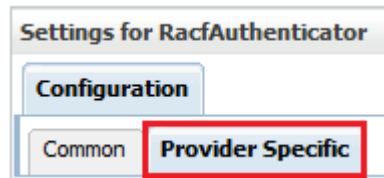
14. 「Authentication Providers」の表で、手順 8 で作成した RACF オーセンティケータ名を選択します (チェックボックスではなく、名前自体を選択します)。

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider
<input type="checkbox"/>	RacfAuthenticator	WebLogic TBI Racf Authentication Provider

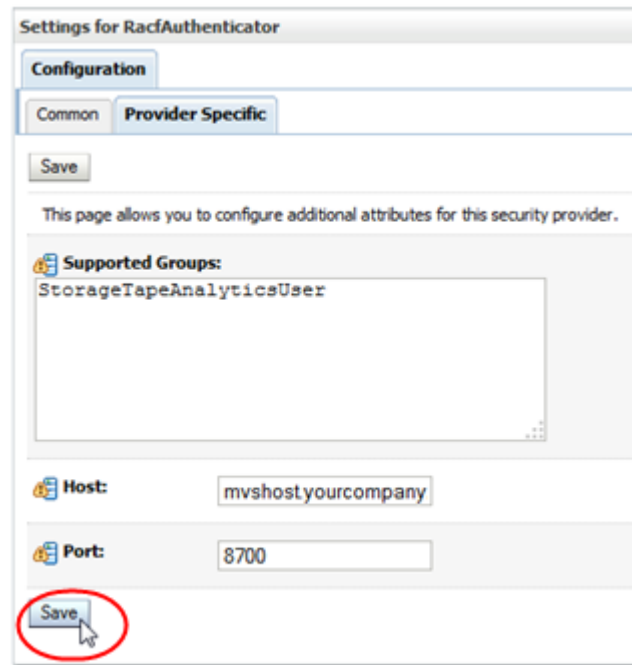
15. 「**Control Flag**」メニューで、「Sufficient」を選択し、「Save」をクリックします。



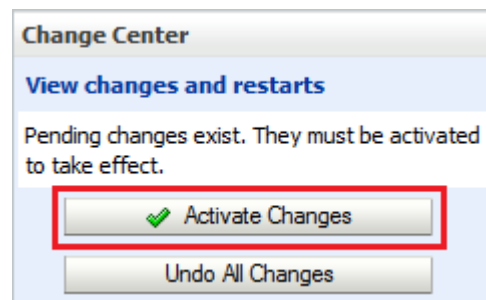
16. 「**Provider Specific**」タブをクリックします。



17. MVS システムが実行されているホスト名 (たとえば、*mvshost.yourcompany.com*) とポート番号 (たとえば、*8700*) を入力して、「Save」をクリックします。



18. 「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。



19. WebLogic 管理コンソールからログアウトします。
20. STA コマンドを使用して STA を停止して再起動します。コマンドの使用の詳細は、『STA 管理ガイド』を参照してください。

```
# STA stop all  
# STA start all
```


SNMP v2c モードの構成

SNMP v2c 用に構成されたライブラリを STA がモニターする場合は、SNMP v2c モードを構成することをお勧めします。

STA は常に、推奨される SNMP v3 プロトコルを使用してライブラリとの通信を試行します。SNMP v3 通信が可能でない場合 (たとえば、ライブラリで SNMP v3 が構成されていない場合)、この付録の手順に従って有効化されていれば STA は SNMP v2c を使用します。

SNMP v3 の構成プロセスは、5章「[ライブラリでの SNMP の構成](#)」および6章「[STA でのライブラリ接続の構成](#)」で説明されています。この付録では、SNMP v2c 構成によって異なる手順について説明します。

この付録には、次のセクションが含まれます。

- [SNMP v2c 構成タスク](#)

F.1. SNMP v2c 構成タスク

- [「SNMP v2c モードの構成」](#)
- [「ライブラリでの STA SNMP v2c トラップ受信者の作成」](#)
- [「STA の SNMP v2c モードの有効化」](#)

F.1.1. SNMP v2c モードの構成

SNMP 通信に SNMP v2c を使用するように STA とライブラリを構成するには、次の手順を使用します。

1. 5章「[ライブラリでの SNMP の構成](#)」では、次の点を除き、表5.1「[STA のライブラリを構成するためのタスク](#)」に示されているすべての手順に従います。
 - 97 ページの「[STA SNMP v3 トラップ受信者の作成](#)」を「[ライブラリでの STA SNMP v2c トラップ受信者の作成](#)」で置き換えます。
 - 表5.1「[STA のライブラリを構成するためのタスク](#)」のプロセスを完了したあと、「[STA の SNMP v2c モードの有効化](#)」を実行します。
2. STA での SNMP v2c の構成手順については、101 ページの6章「[STA でのライブラリ接続の構成](#)」を参照してください。

F.1.2. ライブラリでの STA SNMP v2c トラップ受信者の作成

STA サーバーを SNMP v2c トラップの認証済み受信者として定義して、ライブラリが送信するトラップを定義するには、次の手順を使用します。ライブラリモデルに応じて、ライブラリ CLI、SL コンソール、または SL150 ブラウザインタフェースを使用できます。次の点に注意してください。

- トラップレベルはコンマで区切ります。
- 重複したレコードを回避するために、複数のインスタンスで STA サーバーをトラップ受信者として定義しないでください。たとえば、STA サーバーに対して SNMP v3 と SNMP v2c の両方のトラップ受信者定義を作成しないでください。
- トラップレベル 4 は、古いライブラリファームウェアバージョンではサポートされない場合がありますが、トラップ受信者の作成時にはいつでも指定可能です。
- CLI での入力エラーを回避するために、最初にテキストファイルにコマンドを入力してから、CLI にコピー&ペーストできます。CLI コマンドのヘルプについては、`help snmp` と入力します。

ライブラリ CLI の使用 (SL150 を除くすべてのライブラリ)

1. SNMP v2c トラップ受信者の作成

```
snmp addTrapRecipient trapLevel 1,2,3,4,11,13,14,21,25,27,41,45,  
61,63,65,81,85,100 host STA_server_IP version v2c community community_name
```

ここでは:

- `STA_server_IP`: STA サーバーの IP アドレス。
- `community_name`: SNMP v2c トラップコミュニティ。これは、`public` または別の名前にできます。

例:

```
SL3000> snmp addTrapRecipient trapLevel 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100  
host 192.0.2.20 version v2c community public
```

- #### 2. トラップ受信者を一覧表示して、STA サーバーが正しく追加されていることを確認します。

```
snmp listTrapRecipients
```

SL コンソールの使用 (SL500 ライブラリのみ)

1. 「**Tools**」メニューから、「**System Detail**」を選択します。
2. ナビゲーションツリーで、「**Library**」を選択します。
3. 「**SNMP**」タブを選択してから、「**Add Trap Recipients**」タブを選択します。
4. 次の情報を入力します。
 - *Host*: STA サーバーの IP アドレス。
 - *TrapLevel*: ライブラリが STA に送信すべきトラップレベルのコンマ区切りのリスト:
1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
 - 「*Version*」: 「v2c」を選択します。
 - *Community* – これは、*public* または別の名前にできます。
5. 「**Apply**」をクリックして、トラップ受信者を追加します。

SL150 ユーザーインターフェースの使用

1. ナビゲーションツリーで、「**SNMP**」を選択します。
2. 「SNMP Trap Recipients」セクション (またはタブ) で、「**Add Trap Recipient**」を選択します。
3. 次のように「Add Trap Recipient」フィールドに入力します。
 - *Host Address*: STA サーバーの IP アドレス
 - *Trap Level*: ライブラリが STA に送信すべきトラップレベルのコンマ区切りのリスト:
1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
 - 「*Version*」: 「v2c」を選択します。
 - *Community Name*: *public* または別の名前にできます。
4. 「**OK**」をクリックして、トラップ受信者を追加します。

F.1.3. STA の SNMP v2c モードの有効化

1. STA サーバーとのターミナルセッションを確立し、システムルートユーザーとしてログインします。
2. STA 構成ファイルのディレクトリに移動します。

```
# cd /Oracle_storage_home/Middleware/user_projects/domains/TBI
```

3. SNMP バージョンプロパティファイルを編集します。

```
# vi TbiSmpVersionSupport.properties
```

4. SNMP v2c パラメータの値が *true* に設定されていることを確認します。

```
V2c=true
```

5. ファイルを保存して終了します。
6. ステップ 4 で SNMP v2c パラメータの値を変更した場合、すべての STA プロセスを停止して再起動します。

```
# STA stop all
```

```
# STA start all
```

索引

あ

アンインストール, 159

か

クライアント属性, 105
コンプレックス ID, 74

さ

サービスリクエスト, 30
再インストール, 161

た

トラップ受信者
追加, 155

は

ファイアウォールポート構成, 53
ボリュームシリアル番号、重複, 77
ボリュームラベル形式, 76

や

ユーザーアカウント
MySQL の要件, 52
WebLogic の要件, 52

ら

ライブラリ構成,
SL500 の高速ロード, 76
SNMP 構成, 88
SNMP ワークシート, 240
オプションの構成スクリプト, 78
コンプレックス ID, 74
冗長電子装置, 73
タスク, 78
デュアル TCP/IP, 73
ボリュームラベル形式, 76
ユーザーインタフェース, 77

L

LDAP 構成, 253
Linux PATH 設定, 114
Linux のインストール

インストール後のタスク, 40
概要,
準備タスク, 32
タスク, 36

R

RACF 構成, 257

S

SNMP

管理

クライアント属性の変更, 105
トラップ受信者の追加, 155
接続の確認, 102

SNMP クライアント属性の変更, 105

SSP

RACF の構成, 257
WebLogic Open LDAP の構成, 253
構成,

STA

ダウンロード, 63

STA 構成

SNMP,

STA データベースバックアップサービス, 113
サービス,

Linux PATH 設定の更新, 114
サービスデーモンの再起動, 114
ライブラリ接続の確認, 115
リソースモニター, 113

証明書,

Oracle 証明書の置換, 252
WebLogic の再構成, 244
初期接続の確立, 243

タスク, 101

STA サーバー

ポートの構成, 53

STA のアップグレード,

STA のインストール

一般的な前提条件, 60
インストールの手順, 64
概要,
グラフィカルインストーラ, 64
コンソールインストーラ, 64

V

v2c モード

概要,
構成プロセス, 273
トラップ受信者の作成, 274
有効化, 275