

StorageTek Tape Analytics

설치 및 구성 설명서

버전 2.1.0

E60940-02

2015년 2월

StorageTek Tape Analytics

설치 및 구성 설명서

E60940-02

Copyright © 2013, 2015, Oracle and/or its affiliates. All rights reserved.

본 소프트웨어와 관련 문서는 사용 제한 및 기밀 유지 규정을 포함하는 라이선스 합의서에 의거해 제공되며, 지적 재산법에 의해 보호됩니다. 라이선스 합의서 상에 명시적으로 허용되어 있는 경우나 법규에 의해 허용된 경우를 제외하고, 어떠한 부분도 복사, 재생, 번역, 방송, 수정, 라이선스, 전송, 배포, 진열, 실행, 발행, 또는 전시될 수 없습니다. 본 소프트웨어를 리버스 엔지니어링, 디스어셈블리 또는 디컴파일하는 것은 상호 운용에 대한 법규에 의해 명시된 경우를 제외하고는 금지되어 있습니다.

이 안의 내용은 사전 공지 없이 변경될 수 있으며 오류가 존재하지 않음을 보증하지 않습니다. 만일 오류를 발견하면 서면으로 통지해 주시기 바랍니다.

만일 본 소프트웨어나 관련 문서를 미국 정부나 또는 미국 정부를 대신하여 라이선스한 개인이나 법인에게 배송하는 경우, 다음 공지 사항이 적용됩니다.

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.

본 소프트웨어 혹은 하드웨어는 다양한 정보 관리 애플리케이션의 일반적인 사용을 목적으로 개발되었습니다. 본 소프트웨어 혹은 하드웨어는 개인적인 상해를 초래할 수 있는 애플리케이션을 포함한 본질적으로 위험한 애플리케이션에서 사용할 목적으로 개발되거나 그 용도로 사용될 수 없습니다. 만일 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서 사용할 경우, 라이선스 사용자는 해당 애플리케이션의 안전한 사용을 위해 모든 적절한 비상-안전, 백업, 대비 및 기타 조치를 반드시 취해야 합니다. Oracle Corporation과 그 자회사는 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서의 사용으로 인해 발생하는 어떠한 손해에 대해서도 책임지지 않습니다.

Oracle과 Java는 Oracle Corporation 및/또는 그 자회사의 등록 상표입니다. 기타의 명칭들은 각 해당 명칭을 소유한 회사의 상표일 수 있습니다.

Intel 및 Intel Xeon은 Intel Corporation의 상표 내지는 등록 상표입니다. SPARC 상표 일체는 라이선스에 의거하여 사용되며 SPARC International, Inc.의 상표 내지는 등록 상표입니다. AMD, Opteron, AMD 로고, 및 AMD Opteron 로고는 Advanced Micro Devices의 상표 내지는 등록 상표입니다. UNIX는 The Open Group의 등록상표입니다.

본 소프트웨어 혹은 하드웨어와 관련문서(설명서)는 제3자로부터 제공되는 콘텐츠, 제품 및 서비스에 접속할 수 있거나 정보를 제공합니다. 사용자와 오라클 간의 합의서에 별도로 규정되어 있지 않는 한 Oracle Corporation과 그 자회사는 제3자의 콘텐츠, 제품 및 서비스와 관련하여 어떠한 책임도 지지 않으며 명시적으로 모든 보증에 대해서도 책임을 지지 않습니다. Oracle Corporation과 그 자회사는 제3자의 콘텐츠, 제품 및 서비스에 접속하거나 사용으로 인해 초래되는 어떠한 손실, 비용 또는 손해에 대해 어떠한 책임도 지지 않습니다. 단, 사용자와 오라클 간의 합의서에 규정되어 있는 경우는 예외입니다.

차례

머리말	19
대상	19
설명서 접근성	19
관련 문서	19
STA 응용 프로그램 사용자용	19
STA 서버 및 응용 프로그램의 설치자 및 관리자용	20
규약	20
새로운 기능	21
STA 2.1.0 2015년 1월	21
1. 사전 설치 계획	23
1.1. STA 배치 개요	23
1.2. 라이브러리를 준비하기 위한 서비스 요청 준비	23
2. Linux 설치	25
2.1. 준비 작업	25
2.1.1. 관련 설명서 검토	26
2.1.2. STA 파일 시스템 레이아웃 검토	26
2.1.3. Linux 설치 프로그램 미디어 팩 다운로드	27
2.2. 설치 작업	28
2.2.1. 필요한 정보 수집	28
2.2.2. Linux 설치	28
2.2.3. Linux 설정 에이전트 실행	30
2.3. 사후 설치 작업	31
2.3.1. SELinux 사용 안함으로 설정	31
2.3.2. Linux 방화벽 사용 안함으로 설정	32
2.3.3. 액세스 제어 사용 안함으로 설정	32
2.3.4. 네트워크 프록시 설정	33
2.3.5. yum의 올바른 설정 확인(선택 사항)	33
2.3.6. 필수 Linux 패키지 설치	35
2.3.7. SSH의 올바른 설정 확인	36
2.3.8. 올바른 DNS 설정 확인	36
2.3.9. 이름 서비스 사용 안함으로 설정	36

2.3.10. 로컬 브라우저 기능 확인(선택 사항)	37
3. STA 설치	39
3.1. STA 설치 프로그램에서 사용하는 사용자, 그룹 및 위치	39
3.2. 사용자 이름 및 암호 요구 사항	41
3.3. STA 설치 중 구성되는 계정 및 포트	41
3.3.1. STA 관리용 사용자 계정	41
3.3.1.1. WebLogic 계정	42
3.3.1.2. STA 데이터베이스 계정	42
3.3.2. STA에서 사용하는 포트	43
3.3.2.1. 구성 불가능한 외부 포트	43
3.3.2.2. 구성 가능한 외부 포트	43
3.3.2.3. 구성 가능한 내부 포트	43
3.4. STA 설치 및 제거 로그	44
3.4.1. 로그 파일 위치	44
3.5. STA 설치 프로그램 모드	45
3.6. STA 설치 작업	45
3.6.1. 설치에 필요한 정보 식별 또는 만들기	46
3.6.2. 설치 필요 조건 확인	47
3.6.3. STA 다운로드	50
3.6.4. STA 설치	51
3.6.5. 성공적인 설치 확인	52
3.6.6. STA 로그 디렉토리 재배치(선택 사항)	53
3.6.7. Oracle 중앙 인벤토리 위치 등록	55
4. STA의 라이브러리 기능 구성	57
4.1. STA 데이터에 영향을 주는 라이브러리 기능	57
4.1.1. LTO 드라이브에 대한 ADI 인터페이스	57
4.1.1.1. LTO 드라이브에서 ADI 사용으로 설정	57
4.1.1.2. 라이브러리에서 ADI를 사용으로 설정	58
4.1.2. 이중 TCP/IP 및 중복 전자 부품(SL3000 및 SL8500만 해당)	58
4.1.2.1. 이 기능을 지원하도록 STA 연결 구성	59
4.1.2.2. 이 기능에 대한 추가 고려사항	59
4.1.3. 라이브러리 컴플렉스 ID(SL8500만 해당)	60
4.1.4. 드라이브 청소 경고(SL3000 및 SL8500만 해당)	60
4.1.5. 볼륨 레이블 형식(SL500 및 SL150만 해당)	61
4.1.6. SCSI FastLoad 옵션(SL500만 해당)	61
4.1.7. 중복된 볼륨 일련 번호	61
4.2. 라이브러리 사용자 인터페이스	62

4.2.1. 라이브러리 CLI 사용법 팁	62
4.2.2. 라이브러리 구성 스크립트(선택 사항)	62
4.3. 라이브러리 기능 구성 작업	63
4.3.1. 라이브러리에 로그인	63
4.3.2. 라이브러리 펌웨어 버전 확인	64
4.3.3. 드라이브 컨트롤러 카드 버전 확인(SL3000 및 SL8500만 해당)	65
4.3.4. 라이브러리에서 ADI를 사용으로 설정(SL150을 제외한 모든 라이브러리)	65
4.3.5. 올바른 라이브러리 컴플렉스 ID 확인(SL8500만 해당)	66
4.3.6. 드라이브 청소 경고 설정(선택 사항, SL3000 및 SL8500만 해당)	67
4.3.7. SL500 볼륨 레이블 형식 설정(SL500만 해당)	68
4.3.8. SL150 볼륨 레이블 형식 및 드라이브 요소 주소 지정 모드 설정(SL150만 해당)	69
5. 라이브러리에서 SNMP 구성	71
5.1. STA에 대한 라이브러리 SNMP 구성 이해	71
5.1.1. 라이브러리에서 SNMP v3 프로토콜 구성	71
5.1.1.1. 고유한 SNMP v3 사용자	72
5.1.1.2. SNMP 엔진 ID	72
5.2. 라이브러리 SNMP 구성 작업	73
5.2.1. 라이브러리 IP 주소 검색	73
5.2.2. 라이브러리에서 SNMP 사용으로 설정	75
5.2.3. SNMP v2c 사용자 확인	76
5.2.4. SNMP v3 사용자 만들기	77
5.2.5. 라이브러리 SNMP 엔진 ID 검색(SL150을 제외한 모든 라이브러리)	79
5.2.6. STA SNMP v3 트랩 수신자 만들기	79
6. STA의 라이브러리 연결 구성	83
6.1. STA 구성 작업	83
6.1.1. STA에 로그인	83
6.1.2. 라이브러리와 SNMP 통신 확인	84
6.1.3. STA에 대한 SNMP 클라이언트 설정 구성	86
6.1.4. 라이브러리에 대한 SNMP 연결 구성	88
6.1.5. 라이브러리 SNMP 연결 테스트	90
6.1.6. 수동 데이터 수집 수행	91
7. STA 서비스 구성	93
7.1. STA 서비스 개요	93

7.2. STA 서비스 구성 작업	93
7.2.1. 시스템 경로 업데이트(선택 사항)	94
7.2.2. STA 서비스 데몬 다시 시작(선택 사항)	94
7.2.3. 라이브러리 연결 확인	95
7.2.4. STA 데이터베이스 백업 유틸리티 환경 설정 검토	95
7.2.5. 원격 데이터베이스 백업 서버 구성	95
7.2.6. STA 데이터베이스 백업 서비스 구성	97
7.2.7. STA 리소스 모니터 유틸리티 환경 설정 검토	99
7.2.8. STA 리소스 모니터 구성	100
8. STA 2.1.0으로 업그레이드	103
8.1. 업그레이드 프로세스 개요	103
8.2. 유효한 STA 2.1.0 업그레이드 경로	104
8.3. 업그레이드 방식	104
8.3.1. 단일 서버 업그레이드 방식	104
8.3.2. 두 대의 서버 업그레이드 방식	105
8.4. STA 2.1.0에 대한 환경 변경 사항	106
8.4.1. Linux 버전	106
8.4.2. 기본 WebLogic 포트 번호	107
8.4.3. STA 2.0.x 이상에 필요한 포트	107
8.4.4. 사용자 이름 및 암호 요구 사항	107
8.5. 업그레이드 준비 작업	108
8.5.1. 사이트가 업그레이드할 준비가 되었는지 확인	108
8.5.1.1. 업그레이드 필요 조건 확인	108
8.5.1.2. 현재 STA 작업 확인	109
8.5.2. 기존 로그 저장(선택 사항)	109
8.5.3. 현재 STA 사용자 및 구성 설정 기록(선택 사항)	110
8.5.3.1. MySQL 사용자 이름 기록	110
8.5.3.2. STA SNMP 클라이언트 설정 기록	110
8.5.3.3. WebLogic 사용자 이름 기록—STA 1.0.x에서 업그레이드하 는 경우만 해당	111
8.5.3.4. STA 사용자 이름 기록—STA 2.0.x에서 업그레이드하는 경우 만 해당	113
8.5.3.5. STA 전자 메일 서버 설정 기록	114
8.5.4. STA- 로 시작하는 사용자 정의 템플릿 이름 바꾸기(선택 사항)	115
8.5.5. 현재 사용자 정의 템플릿 설정 기록(선택 사항)	115
8.5.6. 실행 보고서 정책 설정 기록(선택 사항)	116
8.6. 업그레이드 작업	116
8.6.1. 작업 1: 이전 STA 데이터베이스 덤프	117
8.6.2. 작업 2: 이전 데이터베이스 덤프 전송	118

8.6.3. 작업 3a: 새 Linux 버전 설치(STA 1.0.x에서 업그레이드)	119
8.6.4. 작업 3b: 이전 STA 버전 제거(STA 2.0.x에서 업그레이드)	120
8.6.5. 작업 4: 새 STA 버전 설치	120
8.6.6. 작업 5: 새 STA 데이터베이스 덤프(선택 사항)	121
8.6.7. 작업 6: 이전 STA 데이터베이스를 STA 서버로 전송	122
8.6.8. 작업 7: 이전 STA 데이터베이스 처리 및 로드	122
8.6.9. 작업 8: 이전 데이터베이스 업그레이드	125
8.6.10. 작업 9: 새 STA 버전 구성	127
8.6.10.1. 라이브러리에서 STA 트랩 수신자 업데이트	127
8.6.10.2. STA의 SNMP 설정 구성	128
8.6.10.3. STA 서비스 및 사용자 정보 구성	128
8.6.10.4. 이전 STA 서버 구성 해제(선택 사항)	129
8.6.11. 실패한 데이터베이스 업그레이드 복구(선택 사항)	129
9. STA 제거 및 복원	131
9.1. STA 제거 개요	131
9.2. STA 제거 작업	131
9.2.1. STA 제거	132
9.2.2. 성공적인 제거 확인	132
9.2.3. STA 복원	133
A. STA 그래픽 설치 프로그램 및 제거 프로그램 화면 참조	135
A.1. 그래픽 모드 디스플레이 요구 사항	135
A.1.1. 로컬 연결	135
A.1.2. SSH(보안 셸)를 사용한 원격 연결	136
A.1.2.1. Linux 시스템에서 연결	136
A.1.2.2. Microsoft Windows PC에서 연결	136
A.1.3. 데스크탑 공유를 사용한 원격 연결	136
A.1.4. 그래픽 디스플레이 문제 해결	137
A.2. STA 그래픽 설치 프로그램 화면	138
A.2.1. Installation and Inventory Setup	139
A.2.1.1. 화면 필드	139
A.2.1.2. 화면 관련 버튼	140
A.2.2. Welcome	140
A.2.2.1. 일반 설치 프로그램 화면 레이아웃	141
A.2.3. Installation Location	142
A.2.3.1. 화면 필드	143
A.2.3.2. 화면 관련 버튼	143
A.2.4. Prerequisite Checks	145

A.2.4.1. 화면 필드	147
A.2.4.2. 화면 관련 버튼	147
A.2.5. Enter Root Password	149
A.2.5.1. 화면 필드	149
A.2.5.2. 화면 관련 버튼	149
A.2.6. Set Up DB Directories	150
A.2.6.1. 화면 필드	150
A.2.6.2. 화면 관련 버튼	151
A.2.7. Set Up Admin Accounts	151
A.2.7.1. 화면 필드	151
A.2.7.2. 화면 관련 버튼	151
A.2.8. WebLogic Administrator	152
A.2.8.1. 화면 필드	152
A.2.8.2. 화면 관련 버튼	153
A.2.9. STA Administrator	153
A.2.9.1. 화면 필드	154
A.2.9.2. 화면 관련 버튼	154
A.2.10. Set Up Database Accounts	155
A.2.10.1. 화면 필드	155
A.2.10.2. 화면 관련 버튼	155
A.2.11. Database Root User	156
A.2.11.1. 화면 필드	156
A.2.11.2. 화면 관련 버튼	157
A.2.12. Database Application User	157
A.2.12.1. 화면 필드	158
A.2.12.2. 화면 관련 버튼	158
A.2.13. Database Reports User	159
A.2.13.1. 화면 필드	159
A.2.13.2. 화면 관련 버튼	160
A.2.14. Database Administrator	160
A.2.14.1. 화면 필드	161
A.2.14.2. 화면 관련 버튼	161
A.2.15. Enter Communication Ports	162
A.2.15.1. 화면 필드	162
A.2.15.2. 화면 관련 버튼	162
A.2.16. WebLogic Admin Console	163
A.2.16.1. 화면 필드	163
A.2.16.2. 화면 관련 버튼	164
A.2.17. STA Engine	164
A.2.17.1. 화면 필드	165

A.2.17.2. 화면 관련 버튼	165
A.2.18. STA Adapter	165
A.2.18.1. 화면 필드	166
A.2.18.2. 화면 관련 버튼	166
A.2.19. STA UI	167
A.2.19.1. 화면 필드	167
A.2.19.2. 화면 관련 버튼	168
A.2.20. Diagnostic Agent	168
A.2.20.1. 화면 필드	169
A.2.20.2. 화면 관련 버튼	169
A.2.21. Installation Summary	169
A.2.21.1. 화면 필드	170
A.2.21.2. 화면 관련 버튼	170
A.2.22. Installation Progress	171
A.2.22.1. 화면 필드	171
A.2.22.2. 화면 관련 버튼	172
A.2.23. Configuration Progress	173
A.2.23.1. 화면 필드	174
A.2.23.2. 화면 관련 버튼	174
A.2.24. Installation Complete	175
A.2.24.1. 화면 필드	175
A.2.24.2. 화면 관련 버튼	175
A.3. STA 그래픽 제거 프로그램 화면	176
A.3.1. Welcome	176
A.3.1.1. 화면 필드	176
A.3.1.2. 화면 관련 버튼	177
A.3.2. Enter Root Password	177
A.3.2.1. 화면 필드	177
A.3.2.2. 화면 관련 버튼	177
A.3.3. Deinstallation Summary	178
A.3.3.1. 화면 필드	178
A.3.3.2. 화면 관련 버튼	178
A.3.4. Deinstallation Progress	179
A.3.4.1. 화면 필드	180
A.3.4.2. 화면 관련 버튼	180
A.3.5. Deinstallation Complete	181
A.3.5.1. 화면 필드	181
A.3.5.2. 화면 관련 버튼	181
B. STA 자동 모드 설치 프로그램 및 제거 프로그램	183

B.1. STA 자동 모드 설치 프로그램 및 제거 프로그램 사용	183
B.1.1. 자동 모드 요구 사항	183
B.2. 자동 모드에서 사용되는 파일 및 유틸리티	183
B.3. STA 자동 모드 설치 프로그램 작업	186
B.3.1. Oracle 중앙 인벤토리 포인터 파일 만들기	186
B.3.2. 자동 모드 설치 프로그램 응답 파일 만들기	187
B.3.3. 자동 모드 설치 프로그램 실행	189
B.4. STA 자동 모드 제거 프로그램 작업	190
B.4.1. 자동 모드 제거 프로그램 응답 파일 만들기	191
B.4.2. 자동 모드 제거 프로그램 실행	192
B.5. STA 설치 프로그램 명령 옵션	194
B.5.1. 자동 모드 옵션	194
B.5.2. 로깅 옵션	194
B.5.3. 기타 옵션	195
C. 설치 및 업그레이드 워크시트	197
C.1. 업그레이드 준비 워크시트	197
C.2. 설치 및 업그레이드 워크시트	198
C.2.1. 설치 사용자 및 위치 워크시트	198
C.2.2. 사용자 계정 워크시트	198
C.2.3. 포트 번호 워크시트	199
C.2.4. 도메인 이름 워크시트	200
C.3. 사후 설치 구성 워크시트	200
D. 보안 자격 증명 구성	201
D.1. 보안 인증서 구성 작업	201
D.1.1. 초기 HTTPS/SSL 연결 설정	201
D.1.2. 다른 보안 인증서를 사용하도록 WebLogic 재구성	202
D.1.3. Oracle 인증서 바꾸기	209
E. STA의 보안 서비스 공급자 구성	211
E.1. WebLogic OpenLDAP를 통한 STA 액세스 제어	211
E.1.1. WebLogic OpenLDAP 구성	211
E.2. IBM RACF 작업을 통한 STA 액세스 제어	215
E.2.1. 작업 1: IBM RACF 메인프레임 최소 요구 사항 검토	216
E.2.2. 작업 2: STA RACF 권한 부여를 위한 메인프레임 지원 사용으로 설 정	216
E.2.3. 작업 3: AT-TLS 구성	216
E.2.4. 작업 4: CGI 루틴에서 사용되는 RACF 프로파일 만들기	222

E.2.5. 작업 5: 인증서 파일 및 개인 키 파일 가져오기(선택 사항)	222
E.2.6. 작업 6: CGI 루틴 테스트	223
E.2.7. 작업 7: WebLogic 콘솔에 대한 RACF/SSP 설정	223
E.2.8. 작업 8: STA와 RACF 간 SSL 구성	223
E.2.9. 작업 9: WebLogic Server 구성	224
E.2.10. 작업 10: WebLogic 콘솔에 RACF/SSP 설치	224
F. SNMP v2c 모드 구성	229
F.1. SNMP v2c 구성 작업	229
F.1.1. SNMP v2c 모드 구성	229
F.1.2. 라이브러리에서 STA SNMP v2c 트랩 수신자 만들기	229
F.1.3. STA에 대해 SNMP v2c 모드 사용으로 설정	231
색인	233

그림 목록

8.1. 단일 서버 업그레이드 작업 개요	105
8.2. 두 대의 서버 업그레이드 작업 개요	106
A.1. Oracle 스토리지 홈 목록의 예	144
A.2. 기본 창에서 작업을 선택하여 표시된 작업 세부 정보	146
A.3. 확장 아이콘을 선택하여 표시된 작업 세부 정보	147
A.4. 필수 조건 확인 로그 표시의 예	148
A.5. Installation Progress 로그 표시의 예	172
A.6. Configuration Progress 세부 정보의 예	174
A.7. Deinstallation Progress 로그 표시의 예	180

표 목 록

2.1. Linux 설치 작업	25
2.2. 권장되는 파일 시스템 레이아웃	26
2.3. Linux 패키지 선택	29
3.1. 구성 불가능한 외부 포트	43
3.2. 구성 가능한 외부 포트	43
3.3. 구성 가능한 내부 포트	44
4.1. IBM LTO 드라이브에서 ADI를 사용으로 설정하는 방법	58
4.2. STA 연결에 대한 권장되는 라이브러리 IP 주소	59
4.3. 콤플렉스 ID 지정 예	60
4.4. STA에 대한 라이브러리 구성 작업	63
5.1. STA에 대한 라이브러리 구성 작업	73
7.1. STA 백업 서비스 관리 유틸리티(staservadm) 속성	95
7.2. STA 리소스 모니터(staresmonadm) 속성	99
8.1. 업그레이드 준비 작업을 수행하는 경우에 대한 지침	108
C.1. 업그레이드 준비 작업	197
C.2. 설치 사용자 및 위치 워크시트	198
C.3. 사용자 계정 워크시트	199
C.4. 구성 불가능한 외부 포트	199
C.5. 구성 가능한 내부 및 외부 포트	200
C.6. 회사 도메인 이름	200
C.7. SNMP v3 사용자 구성 정보	200

예 목 록

3.1. STA 성공적인 상태 표시	52
4.1. 독립형 SL8500 콤플렉스 ID 변경	67
5.1. SL3000 또는 SL8500에서 SNMP v3 사용자 만들기	78
5.2. SL500에서 SNMP v3 사용자 만들기	78
5.3. SL3000 또는 SL8500에서 SNMP v3 트랩 수신자 만들기	80
5.4. SL500에서 SNMP v3 트랩 수신자 만들기	80
6.1. 성공한 snmpget 명령	85
6.2. 실패한 snmpget 명령—네트워크 시간 초과	85
6.3. 실패한 snmpget 명령—잘못된 암호	85
8.1. 이전 데이터베이스 덤프	118
8.2. 백업 서버로 이전 데이터베이스 전송(단일 서버 방식)	119
8.3. 새 STA 서버로 이전 데이터베이스 전송(두 대의 서버 방식)	119
8.4. 새 데이터베이스 덤프	121
8.5. 새 STA 서버로 이전 데이터베이스 전송	122
8.6. 이전 데이터베이스 백업에서 더 이상 사용되지 않는 데이터 비우기	123
A.1. 올바르게 구성된 X11 디스플레이의 예	137
A.2. 올바르지 구성되지 않은 X11 디스플레이의 예	138
B.1. STA 자동 모드 설치 프로그램 응답 파일 템플리트	184
B.2. STA 자동 모드 제거 프로그램 응답 파일 템플리트	185
B.3. 설치 프로그램 응답 파일 작성 유틸리티 실행의 예	187
B.4. 작성 유틸리티를 사용한 후의 설치 프로그램 유틸리티 파일의 예	188
B.5. 성공적인 STA 자동 모드 설치 최종 메시지	190
B.6. 실패한 STA 자동 모드 설치 최종 메시지	190
B.7. 제거 프로그램 응답 파일 작성 유틸리티 실행의 예	191
B.8. 작성 유틸리티를 사용한 후의 제거 프로그램 응답 파일의 예	192
B.9. 성공적인 STA 자동 모드 제거 최종 메시지	193
B.10. 실패한 STA 자동 모드 제거 최종 메시지의 예	193

머리말

이 문서는 Oracle STA(StorageTek Tape Analytics) 설치 및 구성에 대한 개념 및 절차를 제공합니다.

대상

이 문서는 다음과 같은 사용자를 대상으로 합니다.

- Linux 관리자: STA 서버에서 Linux를 설치, 구성 및 관리합니다.
- STA 관리자: STA 응용 프로그램을 설치, 구성 및 관리합니다.
- 라이브러리 관리자: StorageTek 라이브러리를 구성하고 관리합니다.
- MVS 시스템 프로그래머: IBM 메인프레임 사용자의 STA에 대한 액세스를 구성하고 관리합니다.

설명서 접근성

오라클의 접근성 개선 노력에 대한 자세한 내용은 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>에서 Oracle Accessibility Program 웹 사이트를 방문하십시오.

오라클 고객지원센터 액세스

지원 서비스를 구매한 오라클 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 자세한 내용은 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>를 참조하거나, 청각 장애가 있는 경우 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>를 방문하십시오.

관련 문서

STA 설명서 세트는 다음과 같은 문서로 구성됩니다.

STA 응용 프로그램 사용자용

- *STA 빠른 시작 안내서*—이 설명서에서는 STA 응용 프로그램 및 사용자 인터페이스의 몇 가지 기능에 대해 설명합니다.
- *STA 사용 설명서*—이 설명서에서는 대시보드, 템플릿, 필터, 경보, 실행 보고서, 논리적 그룹 및 STA 매체 검증을 포함하는 모든 STA 응용 프로그램 기능 사용에 대한 지침을 제공합니다. 이 설명서에서는 STA 사용자 이름, 전자 메일 주소, 서비스 로그 및 모니터링되는 라이브러리와 SNMP 연결을 관리하는 방법도 제공합니다.
- *STA 화면 기본 사항 설명서*—이 설명서에서는 STA 사용자 인터페이스의 모든 세부 사항에 대해 설명합니다. 여기에서는 화면 탐색 및 레이아웃과 그래프 및 테이블 사용에 대해 설명합니다.

- **STA 데이터 참조 설명서**—이 설명서에서는 모든 STA 테이프 라이브러리 시스템 화면 및 데이터 속성에 대한 정의를 찾아볼 수 있습니다.

STA 서버 및 응용 프로그램의 설치자 및 관리자용

- **STA 릴리스 노트**—STA 설치 및 사용 전에 이 문서를 읽어보십시오. 이 문서에는 알려진 문제를 비롯하여 중요한 릴리스 정보가 수록되어 있습니다. 이 문서는 STA 미디어 팩 다운로드에 포함되어 있습니다.
- **STA 요구 사항 설명서**—이 설명서에서는 STA 사용을 위한 최소 및 권장 요구 사항을 확인할 수 있습니다. 이 설명서에는 라이브러리, 드라이브, 서버, 사용자 인터페이스, STA 매체 검증 및 IBM RACF 액세스 제어와 같은 요구 사항이 포함되어 있습니다.
- **STA 설치 및 구성 설명서**—이 설명서에서는 STA 설치 계획, Linux 운영 체제 설치, STA 응용 프로그램 설치 및 STA를 구성하여 라이브러리 모니터링을 시작하는 방법에 대해 설명합니다. 이 설명서에서는 새 STA 버전으로 업그레이드하는 방법에 대해서도 설명합니다.
- **STA 관리 설명서**—이 설명서에서는 STA 서비스 구성, 데이터베이스 백업 및 복원, 데이터베이스 계정에 대한 암호 관리 등 STA 서버 관리 작업에 대한 정보를 확인할 수 있습니다.
- **STA 보안 설명서**—이 설명서에서는 요구 사항, 권장 사항 및 일반 보안 원칙을 비롯하여 중요한 STA 보안 정보를 확인할 수 있습니다.
- **STA Licensing Information User Manual**—이 설명서에서는 STA 제품과 함께 배포된 타사 기술의 사용에 대한 정보를 확인할 수 있습니다.

규약

이 문서에 사용된 텍스트 규약은 다음과 같습니다.

규약	의미
굵은체	굵은체 유형은 작업과 연관된 그래픽 사용자 인터페이스 요소, 또는 텍스트나 용어집에 정의된 용어를 나타냅니다.
기울임꼴	기울임꼴 유형은 책 제목, 강조 또는 사용자가 특정 값을 제공할 위치 표시자 변수를 나타냅니다.
고정 폭	고정 폭 유형은 단락 안의 명령, URL, 예제의 코드, 화면에 나타나는 텍스트, 사용자가 입력한 텍스트를 나타냅니다.

새로운 기능

이 절에서는 StorageTek Tape Analytics 2.1.0의 새로운 기능 및 향상된 기능을 요약하여 설명합니다.

STA 2.1.0 2015년 1월

새 기능과 향상된 기능에 대한 자세한 내용은 지정된 설명서를 참조하십시오.

STA 요구 사항 설명서에 설명되어 있는 항목

- STA 2.1.0을 지원하는 새 라이브러리 및 드라이브 권장 펌웨어 레벨
- Oracle의 StorageTek T10000C 및 T10000D 드라이브를 위한 TTI 5.50 프로토콜 지원
- STA 2.1.0을 지원하기 위해 권장 라이브러리 및 드라이브 요구 사항이 업데이트됨
- 권장 STA 서버 구성이 업데이트됨

STA 설치 및 구성 설명서에 설명되어 있는 항목

- 다음과 같은 새로운 기능을 제공하는 새 STA 2.1.0 설치 프로그램 및 제거 프로그램
 - Oracle 설치 사용자 및 그룹—STA 서버에서 Oracle 제품을 설치 및 업그레이드하는 데에만 사용되는 Linux 사용자 및 그룹
 - 사용자 정의 Oracle 스토리지 홈 위치—STA 응용 프로그램 및 연관된 Oracle 소프트웨어는 충분한 공간이 있는 모든 파일 시스템에 설치할 수 있습니다.
 - 사용자 정의 데이터베이스 및 로컬 백업 위치
 - Oracle 중앙 인벤토리 위치—STA 서버에 설치된 Oracle 제품에 대한 정보를 추적하기 위한 디렉토리
 - STA 설치 프로그램 및 제거 프로그램 자동 모드—그래픽 사용자 인터페이스를 건너뛰고 XML 등록 정보 파일에 설치 옵션을 제공할 수 있게 해줍니다.
 - 자세한 새 STA 설치 프로그램 및 제거 프로그램 로그
 - 모든 STA 그래픽 설치 프로그램 및 제거 프로그램 화면에 대한 상황에 맞는 도움말
- 추가 Linux RPM 패키지 요구 사항—STA 그래픽 설치 프로그램을 실행하려면 *xorg-x11-utils* 패키지를 설치해야 합니다.
- WebLogic 관리 콘솔에 대한 기본 포트가 7019(HTTP) 및 7020(HTTPS)으로 변경되었습니다. 이전 기본 지정을 사용하는 경우 새 지정으로 변경해야 합니다.
- STA 및 MySQL 사용자 이름에 대한 새 암호 요구 사항
- STA 1.0.x 및 STA 2.0.x 데이터베이스를 STA 2.1.0으로 업그레이드하는 새 프로세스

STA 빠른 시작 안내서에 설명되어 있는 항목

- 주요 변경 사항 없음

STA 사용 설명서에 설명되어 있는 항목

- 추가 정보를 제공하고 유용성을 높이기 위해 다음 템플릿이 적은 쪽으로 업데이트되었습니다.
 - STA-Complex-Configuration
 - STA-Complex-Utilization
 - STA-Lib-Configuration
 - STA-Drive-MV
 - STA-Media-All
 - STA-Media-MV-Calibration
 - Media Validation Overview 화면, STA-Default 템플릿
- 설명서 변경 사항—다음 장은 STA 관리 설명서에서 다른 위치로 이동했습니다. 이제는 STA 사용 설명서가 STA 사용자 인터페이스에서 수행할 수 있는 모든 기능 및 작업에 대해 설명합니다.
 - STA 사용자 이름 및 전자 메일
 - STA 서비스 로그
 - STA의 SNMP 연결 관리

STA 화면 기본 사항 설명서에 설명되어 있는 항목

- 주요 변경 사항 없음

STA 데이터 참조 설명서에 설명되어 있는 항목

- 유용성을 높이기 위해 일부 화면의 속성이 재구성되었습니다.
- "Last Messages" 속성을 CAP, 드라이브, 엘리베이터, 라이브러리, PTP 및 로봇의 해당 화면에서 사용할 수 있습니다.

STA 관리 설명서에 설명되어 있는 항목

- 설명서 변경 사항—다음 장은 STA 사용 설명서로 이동했습니다.
 - 사용자 및 전자 메일
 - 로깅
 - SNMP 관리

사전 설치 계획

이 장은 다음과 같은 절로 구성됩니다.

- [STA 배치 개요](#)
- [라이브러리를 준비하기 위한 서비스 요청 준비](#)

1.1. STA 배치 개요

처음으로 STA를 설치 및 구성하려면 다음 작업을 나열된 순서대로 수행합니다. 직접 프로세스를 수행하거나 Oracle 설치 서비스를 구매할 수 있습니다.

STA를 이전 버전에서 업그레이드하려면 [8장. STA 2.1.0으로 업그레이드](#)를 참조하십시오.

순서	작업	세부 정보 및 지침
1	사용자 사이트의 STA 요구 사항을 검토 및 확인합니다.	STA 요구 사항 설명서
2	필요에 따라 드라이브 및 라이브러리에 대한 서비스 요청을 준비합니다.	1.2절. "라이브러리를 준비하기 위한 서비스 요청 준비"
3	STA 서버에 Linux를 설치합니다.	2장. Linux 설치
4	STA 서버에 STA를 설치합니다.	3장. STA 설치
5	STA로 데이터를 보내도록 라이브러리를 구성합니다.	5장. 라이브러리에서 SNMP 구성
6	라이브러리에서 데이터를 받고 모니터링을 시작하도록 STA를 구성합니다.	6장. STA의 라이브러리 연결 구성
7	추가 STA 사용자 이름 및 전자 메일 주소를 구성합니다.	STA 사용 설명서
8	STA 모니터링 및 데이터베이스 백업 서비스를 구성합니다.	7장. STA 서비스 구성
9	승인된 보안 인증서를 구성합니다(선택 사항).	부록 D. 보안 자격 증명 구성
10	STA 액세스 제어에 대한 외부 공급자를 구성합니다(선택 사항).	부록 E. STA의 보안 서비스 공급자 구성

1.2. 라이브러리를 준비하기 위한 서비스 요청 준비

이 절차 및 참조 절을 사용하여 STA에서 모니터링하도록 라이브러리를 준비하는 데 필요한 정보를 Oracle 고객지원센터에 제공합니다.

주:

STA가 라이브러리 컴플렉스를 모니터링하는 경우 컴플렉스의 각 라이브러리에 대해 서비스 요청을 준비하십시오. 또한 서비스 요청을 열어 STA에서 지원하는 최신 드라이브 펌웨어를 설치하십시오.

1. 라이브러리 펌웨어 버전을 확인합니다. 4.3.2절. “라이브러리 펌웨어 버전 확인”을 참조하십시오.
2. 하이 메모리 HBT 카드가 설치되었는지 확인합니다(SL3000 및 SL8500만 해당). 4.3.3절. “드라이브 컨트롤러 카드 버전 확인(SL3000 및 SL8500만 해당)”을 참조하십시오.
3. 라이브러리 및 LTO 드라이브에서 ADI를 사용으로 설정합니다(LTO 드라이브가 있는 라이브러리만 해당). 4.3.4절. “라이브러리에서 ADI를 사용으로 설정(SL150을 제외한 모든 라이브러리)”을 참조하십시오.
4. 라이브러리 컴플렉스 ID를 설정합니다(SL8500만 해당). 4.3.5절. “올바른 라이브러리 컴플렉스 ID 확인(SL8500만 해당)”을 참조하십시오.
5. 라이브러리 날짜 및 시간을 설정합니다. 라이브러리 데이터 날짜/시간 기록이 STA 서버 날짜/시간 기록과 일치하도록 하려면 라이브러리 시계를 Oracle 고객지원센터에서 맞게 설정해야 합니다.
6. 필요한 서비스 요청을 제출합니다.

Linux 설치

이 장은 다음과 같은 항목으로 구성되어 있습니다.

- [준비 작업](#)
- [설치 작업](#)
- [사후 설치 작업](#)

STA 서버에 Linux를 설치하기 전에 STA 요구 사항 설명서의 시스템 요구 사항을 검토하십시오.

주:

Linux 5.x에서 Linux 6.x로 in-place 업그레이드를 수행할 수 없습니다. STA 2.0.x로 업그레이드하는 작업의 일부로 Linux 6.x를 설치하려는 경우 [8장. STA 2.1.0으로 업그레이드](#)를 참조하십시오.

STA에 대해 Linux를 설치 및 구성하려면 [표 2.1. “Linux 설치 작업”](#)의 작업을 표시된 순서대로 수행하십시오.

표 2.1. Linux 설치 작업

범주	작업
준비	<ol style="list-style-type: none"> 1. 2.1.1절. “관련 설명서 검토” [26] 2. 2.1.3절. “Linux 설치 프로그램 미디어 팩 다운로드” [27]
설치	<ol style="list-style-type: none"> 1. 2.2.1절. “필요한 정보 수집” [28] 2. 2.2.2절. “Linux 설치 ” [28] 3. 2.2.3절. “Linux 설정 에이전트 실행” [30]
사후 설치	<ol style="list-style-type: none"> 1. 2.3.1절. “SELinux 사용 안함으로 설정” [31] 2. 2.3.2절. “Linux 방화벽 사용 안함으로 설정” [32] 3. 2.3.3절. “액세스 제어 사용 안함으로 설정” [32] 4. 2.3.4절. “네트워크 프록시 설정” [33] 5. 2.3.5절. “yum의 올바른 설정 확인(선택 사항)” [33] 6. 2.3.6절. “필수 Linux 패키지 설치” [35] 7. 2.3.7절. “SSH의 올바른 설정 확인” [36] 8. 2.3.8절. “올바른 DNS 설정 확인” [36] 9. 2.3.9절. “이름 서비스 사용 안함으로 설정” [36] 10. 2.3.10절. “로컬 브라우저 기능 확인(선택 사항)” [37]

2.1. 준비 작업

STA 서버에 Linux를 설치하기 전에 이 절차를 수행하십시오.

- 2.1.1절. “관련 설명서 검토”
- 2.1.2절. “STA 파일 시스템 레이아웃 검토”
- 2.1.3절. “Linux 설치 프로그램 미디어 팩 다운로드”

2.1.1. 관련 설명서 검토

네트워크 구성 요구 사항 및 옵션이 매우 다양하므로 하드웨어, 소프트웨어 및 네트워크 설치 및 구성을 위해 다음 문서를 참조하십시오. IPv4 및 IPv6 네트워크 구성은 이러한 문서에서 자세히 설명됩니다.

- Oracle Linux 설치 설명서:
<http://docs.oracle.com/en/operating-systems/>
- RedHat Linux 설명서:
<https://access.redhat.com/home>

2.1.2. STA 파일 시스템 레이아웃 검토

표 2.2. “권장되는 파일 시스템 레이아웃”에서는 STA 서버에 권장되는 파일 시스템 레이아웃에 대해 설명합니다. Linux 설치 중 레이아웃을 구성합니다.

다음 위치는 사용자가 정의합니다. 즉 사이트 요구 사항에 맞도록 레이아웃을 구성할 수 있습니다.

- Oracle 스토리지 홈—STA 설치 프로그램에서 이 위치를 묻는 메시지가 표시됩니다. 기본값은 없습니다. 자세한 내용은 [Oracle 스토리지 홈 위치](#)를 참조하십시오.
- STA 데이터베이스—STA 설치 프로그램에서 이 위치를 묻는 메시지가 표시됩니다. 기본값은 `/dbdata`입니다.
- STA 데이터베이스 로컬 백업—STA 설치 프로그램에서 이 위치를 묻는 메시지가 표시됩니다. 기본값은 `/dbbackup`입니다.
- STA 및 MySQL 로그—기본값은 `/var/log/tbi`입니다. Linux 설치를 완료한 후 STA를 설치하기 전에 다른 위치를 사용하려면 STA를 설치한 후 해당 위치에서 `/var/log/tbi`로 가는 심볼릭 링크를 만들어야 합니다. 자세한 내용은 [3.6.6절. “STA 로그 디렉토리 재배치\(선택 사항\)”](#)를 참조하십시오.

Oracle은 STA를 설치하기 전에 이 모든 파일 시스템을 만들 것을 권장합니다. 그렇지 않으면 STA가 루트 `/` 및 `/var`에 설치되므로 이러한 디렉토리에 추가로 공간을 할당해야 합니다. STA 설치 프로그램은 필요에 따라 디렉토리를 만들지만, 미리 파일 시스템을 만들어 두면 파일 시스템 등록 정보에 대한 더 많은 제어 권한을 가지게 됩니다.

표 2.2. 권장되는 파일 시스템 레이아웃

파일 시스템	기본 마운트 지점	크기	설명 및 권장 사항
루트	<code>/</code>	32GB 최소	<code>/tmp</code> 가 이 파일 시스템에 포함된 경우 최소 4GB의 사용 가능 공간이 유지되어야 합니다. 이 공간은 STA 설치 및 업그레이드 중 필요합니다.

파일 시스템	기본 마운트 지점	크기	설명 및 권장 사항
스왑	없습니다. 메모리로 정의됩니다.	RAM 크기의 50~100%	스왑 공간에 사용됩니다.
Oracle 스토리지 홈	<code>/Oracle</code>	최소 30GB 50GB 권장	<p>STA 및 Oracle Middleware(WebLogic, MySQL, RDA) 응용 프로그램 파일의 위치입니다.</p> <p>이 위치는 사용자가 정의합니다. 별도 볼륨에 있는 별도의 파일 시스템이어야 합니다. STA 설치 및 업그레이드를 위해 최소 4GB의 사용 가능한 공간을 유지하십시오. WebLogic 로그 교체를 위해 추가로 5GB의 사용 가능한 공간을 유지하십시오.</p> <p>STA는 자동으로 다음 Oracle Middleware 하위 디렉토리를 만듭니다.</p> <ul style="list-style-type: none"> 교체된 WebLogic 로그: <pre><code>/Oracle_storage_home/Middleware/user_projects/domains/TBI/servers</code></pre> RDA 마지막 CLI 스냅샷: <pre><code>/Oracle_storage_home/Middleware/rda/output</code></pre> STA GUI 스냅샷 로그 번들: <pre><code>/Oracle_storage_home/Middleware/rda/snapshots</code></pre>
STA 데이터베이스 위치	<code>/dbdata</code>	250GB~2TB	<p>STA 데이터베이스의 위치입니다. 이 위치는 사용자가 정의합니다. Oracle은 이 디렉토리를 루트, 스왑, Oracle 스토리지 홈 및 STA 로그 위치와 별도의 자체 볼륨에 배치할 것을 강력하게 권장합니다. 성능, 백업 및 유지 관리를 위해 가장 좋은 방법은 미러링 또는 스트라이프된 별도의 드라이브 세트를 사용하는 것입니다.</p> <p>필요한 크기는 라이브러리 수, 드라이브 수, 매체 수, 일간 교환 횟수 및 데이터의 과거 연도 수에 따라 달라집니다. Oracle은 공간 사용률이 지정된 백분율을 초과할 경우 경보를 보내도록 STA 서비스를 구성할 것을 권장합니다.</p>
STA 데이터베이스 로컬 백업 위치	<code>/dbbackup</code>	<code>/dbdata</code> 크기의 70~80%	<p>최신 로컬 데이터베이스 백업의 위치입니다. 이 위치는 사용자가 정의합니다. Oracle은 이 위치를 STA 데이터베이스와 다른 볼륨에 두며, 데이터베이스 손상 또는 실패에 대비하여 미러링 또는 스트라이프된 드라이브에 둘 것을 권장합니다.</p>
STA 로그 위치	<code>/var/log/tbi</code>	최소 30GB 50GB~100GB 권장	<p>STA 및 MySQL 로그의 위치입니다. 이 위치는 별도 마운트 지점에 있는 별도의 볼륨이어야 합니다. 콘텐츠는 늘어나며 로그 교체를 통해 관리됩니다. 기본 위치는 <code>/var/log/tbi</code>이지만 STA 설치 후 언제든지 이 위치를 변경할 수 있습니다. 자세한 내용은 3.6.6절. “STA 로그 디렉토리 재배치(선택 사항)”를 참조하십시오.</p> <p>주: 로그 교체를 제외하고 STA는 공간 관리를 수행하지 않습니다.</p> <p>주의: <code>/STA_logs/db/stadb_bin.*</code>의 로그 파일을 관리하도록 STA 백업 유틸리티를 구성해야 합니다. 그렇지 않으면 이러한 파일에 수동 관리가 필요할 수 있습니다(자세한 내용은 STA 관리 설명서 참조).</p>

2.1.3. Linux 설치 프로그램 미디어 팩 다운로드

다음 절차에 따라 Oracle Software Delivery Cloud 웹 사이트에서 Linux 설치 프로그램 미디어 팩을 다운로드합니다. 미디어 팩은 압축된 ISO 이미지 파일로 제공되며 압축을 풀어 선택한 휴대용 매체(플래시 드라이브, DVD 등)에 저장할 수 있습니다.

이 작업을 수행하기 전에 Oracle 지원 담당자에서 Oracle Software Delivery Cloud 사용자 ID 및 암호를 확보해야 합니다.

1. 웹 브라우저를 시작하여 다음 Oracle Software Delivery Cloud 웹 사이트로 이동합니다.
<http://edelivery.oracle.com/linux>
2. **Sign In/Register**를 누릅니다.
3. Oracle 고객지원센터에서 제공한 사용자 ID 및 암호를 입력합니다.
4. Terms & Restrictions 화면에서 License Agreement and Export Restrictions에 동의한다는 확인란을 선택한 다음 **Continue**를 누릅니다.
5. Media Pack Search 화면에서 다음을 수행합니다.
 - a. Select a Product Pack 메뉴에서 **Oracle Linux**를 선택합니다.
 - b. Platform 메뉴에서 **x86 64비트**를 선택합니다(STA에는 64비트 Linux 필요).
 - c. **Go**를 누릅니다.
6. Linux 버전을 선택한 다음 **Continue**를 누릅니다.

Linux 버전 요구 사항은 STA 요구 사항 설명서를 참조하십시오.
7. 64비트 옵션에 대해 **Download**를 누릅니다.
8. ISO 파일을 저장하고 매체에 기록합니다.

2.2. 설치 작업

다음 절차에서는 그래픽 설치 프로그램 및 설정 에이전트를 사용한 Oracle Enterprise Linux(OEL) 6u4 DVD 설치를 가정합니다. 다른 버전의 Linux를 설치하거나 다른 매체를 사용하거나 콘솔 모드를 사용하는 경우 단계 및 패키지가 다를 수 있습니다.

2.2.1. 필요한 정보 수집

시스템 관리자에게 문의하여 다음 정보를 확보하십시오.

- STA 서버에 대한 호스트 이름 및 IP 주소
- 네트워크에 대한 게이트웨이 IP 주소 및 넷마스크
- 네트워크에 대한 DNS 서버 IP 주소 및 검색 도메인
- 사용할 NTP(Network Time Protocol) 서버의 IP 주소
- 네트워크 프록시 정보(해당하는 경우)

2.2.2. Linux 설치

이 절차를 따라 Linux 설치를 수행합니다.

1. 설치 매체를 STA 서버에 연결합니다.
2. 매체에 있는 README 파일의 지침에 따라 Linux 설치 프로그램을 시작합니다.
3. **Install or upgrade an existing system**을 선택합니다.
4. DVD에서 설치하는 경우 CD Found 화면이 나타납니다. 선택적으로 매체 테스트를 수행할 수 있습니다. 테스트를 건너뛰려면 **Tab** 키를 눌러 **Skip** 옵션을 강조 표시한 다음 스페이스바를 누릅니다.

5. Welcome 화면에서 **Next**를 누릅니다.
6. 언어를 선택한 다음 **Next**를 누릅니다.
7. 키보드 레이아웃을 선택한 다음 **Next**를 누릅니다.
8. **Basic Storage Devices**를 선택한 다음 **Next**를 누릅니다.
9. STA 서버에 대한 호스트 이름을 입력한 다음 **Configure Network**를 누릅니다.
10. 네트워크 어댑터 이름을 선택한 다음 **Edit**를 누릅니다.
11. **Connect automatically** 및 **Available to all users**가 둘 다 선택되었는지 확인합니다.
12. 나머지 탭에서 네트워크 관리자의 IPv4 또는 IPv6 지정에 따라 어댑터를 구성합니다. STA 서버 및 적어도 하나의 DNS 서버에 대해 정적 IP 주소를 지정해야 합니다. 작업을 마쳤으면 **Apply**, **Close** 및 **Next**를 누릅니다.
13. STA 서버의 시간대를 선택하고 **System clock uses UTC** 확인란을 선택한 다음 **Next**를 누릅니다.
14. 서버에 대한 Linux 루트 암호를 입력하고 확인한 다음 **Next**를 누릅니다.
15. 서버에서 사용할 분할 영역 레이아웃을 확인합니다.
 - a. STA에는 전용 서버가 필요하므로 Oracle은 **Use All Space**를 선택할 것을 권장합니다.
 - b. **Review and modify partitioning layout** 확인란을 선택한 다음 **Next**를 누릅니다.
16. 기본값은 STA에 대한 최소 요구 사항을 충족하지 않으므로 표 2.2. “권장되는 파일 시스템 레이아웃”를 사용하여 파일 시스템 레이아웃을 수정합니다. 또는 Linux 설치 후 *system-config-lvm* 유틸리티를 사용하여 파일 시스템을 수정할 수도 있습니다.
완료되면 **Next**를 누릅니다.
17. 준비가 되었으면 **Write changes to disk**를 선택합니다.
18. 부트 로더 화면에서 모든 옵션을 그대로 둔 다음 **Next**를 누릅니다.
19. 소프트웨어 선택 화면에서 **Basic Server**를 선택하고 저장소 옵션을 변경하지 않습니다. 그런 다음 **Customize now**를 선택하고 **Next**를 누릅니다.
20. 패키지 선택 화면에서 표 2.3. “Linux 패키지 선택”을 사용하여 각 패키지 범주에 대한 패키지를 구성합니다.
 - a. 패키지 범주를 선택합니다.
 - b. 선택 옆에 있는 각 패키지에 대한 확인란을 선택합니다.
 - c. 패키지에 옵션(+로 표시됨)이 필요한 경우 상위 패키지를 강조 표시하고 **Optional packages** 버튼을 누르고, 목록에서 하위 패키지를 선택한 다음 **Close**를 누릅니다.
 - d. 선택 해제 옆에 있는 각 패키지에 대한 확인란을 선택 해제합니다.
 - e. 다른 확인란은 그대로 둡니다.

표 2.3. Linux 패키지 선택

패키지 범주	선택	선택 해제
기본 시스템	<ul style="list-style-type: none"> • Base • Compatibility libraries • Console internet tools 	<ul style="list-style-type: none"> • Debugging Tools • Dial-up Networking Support • Directory Client

패키지 범주	선택	선택 해제
	<ul style="list-style-type: none"> • Java Platform • Legacy UNIX compatibility <p>+ <i>ksh-xxxxxxxx-xx.e16.x86_64</i></p>	<ul style="list-style-type: none"> • Hardware monitoring utilities • Large Systems Performance • Network file system client • Performance Tools
서버(선택 사항)	<ul style="list-style-type: none"> • System administration tools 	해당 사항 없음
웹 서비스	해당 사항 없음	모든 패키지
데이터베이스	해당 사항 없음	모든 패키지
시스템 관리	해당 사항 없음	해당 사항 없음
가상화	해당 사항 없음	해당 사항 없음
데스크탑(권장)— 그래픽 환경에서 특정 사후 설치 단계를 수행하는 데 사용됩니다. 자세한 내용은 2.3절. “사후 설치 작업”을 참조하십시오.	<ul style="list-style-type: none"> • Desktop • Desktop Platform • General Purpose Desktop • Graphical Administration Tools <p>+ <i>system-config-lvm-x.x.xx-xx.e16.noarch¹</i></p> <ul style="list-style-type: none"> • Legacy X Window System compatibility • X11 (X Window System, version 11) 	해당 사항 없음
응용 프로그램(선택 사항)— GUI 인터페이스를 통해 STA 서버를 로컬로 구성 및 관리하는 데 사용할 수 있습니다.	<ul style="list-style-type: none"> • Internet Browser 	해당 사항 없음
개발	<ul style="list-style-type: none"> • Development tools <p>+ <i>expect-x.xx.x.xx-x.e16.x86_64</i></p>	해당 사항 없음
언어	해당 사항 없음	해당 사항 없음

¹선택 사항입니다. Linux 설치가 완료된 후 파일 시스템을 구성하거나 재구성하는 데 사용할 수 있습니다.

21. 패키지 선택을 마쳤으면 **Next**를 누릅니다. 설치가 시작됩니다.

모든 패키지를 구성하기 전에 실수로 **Next**를 누른 경우 소프트웨어에서 종속성 검사를 완료한 후 **Back**을 누르십시오.

22. Congratulations 화면이 표시되면 설치 매체를 제거한 다음 **Reboot**를 누릅니다.

설치에 대한 전체 로그는 */root/install.log*에서 찾을 수 있습니다.

2.2.3. Linux 설정 에이전트 실행

Linux 설정 에이전트는 Linux 서버가 재부트될 때 자동으로 시작됩니다. 이 절차를 따라 시스템 환경을 구성합니다.

1. Welcome 화면에서 **Forward**를 누릅니다.
2. 라이선스 계약서를 읽고 **Yes, I agree to the License Agreement**를 선택하고 **Forward**를 누릅니다.
3. Software Updates 화면에서 업데이트를 위해 시스템을 등록하려는 경우 **Yes, I'd like to register now**를 선택합니다. 그렇지 않으면 **No, I prefer to register at a later time**를 선택하고 **Forward**를 누릅니다.

4. Finish Updates Setup 화면에서 **Forward**를 누릅니다.
5. Create User 화면에서 필드를 비워 두고 **Forward**를 누른 다음 **Yes**를 눌러 계속합니다. STA 서버에는 관리자 이외의 사용자가 필요하지 않습니다.
6. Date and Time 화면에서 다음 작업을 수행합니다.
 - a. 현재 날짜와 시간을 설정합니다.
 - b. **Synchronize date and time over the network** 확인란을 선택합니다.
 - c. 원하는 NTP 서버(IT 관리자에게 문의)를 추가하거나 제거한 다음 **Forward**를 누릅니다.

주:

STA 데이터 및 로그 파일을 정확하게 만들려면 STA 서버의 날짜 및 시간이 정확해야 합니다. 또한 STA에 연결된 모든 라이브러리의 시간이 정확해야 합니다.

7. Kdump 화면에서 **Enable kdump?**를 선택하지 않습니다. 그런 다음 **Finish**를 누릅니다.

시스템이 재부트됩니다.

8. 시스템이 재부트되면 루트 사용자로 로그인합니다.
 - a. **Other...**를 누릅니다.
 - b. 사용자 이름 **root**를 입력한 다음 **Log In**을 누릅니다.
 - c. 루트 암호를 입력한 다음 **Log In**을 다시 누릅니다.

루트 슈퍼 유저로 로그인 중과 관련된 메시지가 나타날 경우 메시지를 무시할 수 있습니다.

9. Linux 릴리스와 업데이트 레벨을 확인합니다. 이 단계는 선택 사항입니다.

```
# 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. 사후 설치 작업

다음 작업을 수행하여 STA 서버가 STA 설치에 대해 올바르게 구성되었는지 확인합니다.

2.3.1. SELinux 사용 안함으로 설정

Oracle은 STA 서버에서 SELinux를 사용 안함으로 설정할 것을 권장합니다.

1. STA 서버에서 터미널 세션을 엽니다.
2. 텍스트 편집기에서 SELinux 구성 파일을 엽니다.

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

3. 파일에서 *SELINUX*를 *disabled*로 설정합니다.

```
SELINUX=disabled
```

4. 파일을 저장하고 종료합니다.

2.3.2. Linux 방화벽 사용 안함으로 설정

Oracle은 STA 서버에서 방화벽을 사용 안함으로 설정할 것을 권장합니다. 하지만 사이트 요구 사항에 따라 방화벽을 사용으로 설정하고 구성하도록 선택할 수 있습니다.

이 절차를 사용하여 방화벽을 사용 안함으로 설정합니다.

1. STA 서버에서 터미널 세션을 엽니다.
2. (다음 부트에 대한) Linux 방화벽의 설정을 확인합니다.

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

다음 부트 시 사용 안함으로 설정되도록 방화벽이 설정된 경우 iptables 및 ip6tables에 대한 모든 출력이 *off*로 표시됩니다. 이와 같지 않은 경우 방화벽을 사용 안함으로 설정합니다.

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

3. Linux 방화벽의 현재 상태를 확인합니다.

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

명령 출력은 방화벽이 현재 실행 중인지 여부를 나타냅니다. 방화벽이 실행 중인 경우 방화벽을 중지합니다.

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

4. 다음 중 하나라도 해당하는 경우 서버를 재부트해야 합니다.
 - 2.3.1절. “SELinux 사용 안함으로 설정” [31]에서 SELinux를 사용 안함으로 설정했습니다.
 - 이 절에서 Linux 방화벽을 사용 안함으로 설정했습니다(*chkconfig* 사용).

2.3.3. 액세스 제어 사용 안함으로 설정

특정 디렉토리에 대해 액세스 제어를 사용 안함으로 설정해야 합니다.

1. Oracle 스토리지 홈, STA 데이터베이스, STA 데이터베이스 로컬 백업 및 STA 로그 위치에 대한 권한을 나열합니다. 예를 들면 다음과 같습니다.

```
# 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. 각 명령에 대한 출력에서 권한의 끝에 있는 점을 찾습니다. 다음 예에서 `drwxr-xr-x` 뒤에 "."이 있음을 알 수 있습니다.

```
# ls -ld /Oracle

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

3. 권한 명령문 뒤에 점이 있는 디렉토리가 없는 경우 액세스 제어가 이미 사용 안함으로 설정된 것이며 다음 작업으로 진행할 수 있습니다.

디렉토리에 대한 액세스 제어가 사용으로 설정된 경우 해당 디렉토리에 대해 시스템 루트 사용자로 다음 명령을 실행합니다.

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

예를 들면 다음과 같습니다.

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

2.3.4. 네트워크 프록시 설정

STA 서버가 네트워크에 직접 또는 프록시 서버를 통해 연결하도록 구성할 수 있습니다.

1. Linux 데스크탑 **System** 메뉴에서 **Preferences, Network Proxy**를 차례로 선택합니다.
2. Network Proxy Preferences 대화 상자에서 사이트 요구 사항에 따라 프록시 구성을 지정합니다.
3. **Close**를 누릅니다.

2.3.5. yum의 올바른 설정 확인(선택 사항)

yum(Yellowdog Updater, Modified)을 사용하여 필수 RPM(Red Hat Package Manager) Linux 소프트웨어 패키지를 설치하려는 경우에만 이 절차를 사용하십시오. (필수 패키지는 [2.3.6절. "필수 Linux 패키지 설치"](#)를 참조하십시오.)

RPM 패키지를 설치하는 방법에는 yum을 비롯한 다양한 방법이 있습니다. yum은 패키지 설치 프로세스를 크게 간소화하므로 yum 사용은 선택 사항이지만 권장됩니다. yum은 RPM

패키지 저장소에서 최신 패키지 버전 및 해당 종속 항목을 자동으로 검색합니다. 이 절차를 사용하여 yum이 STA 서버에서 올바르게 구성되었는지 확인하십시오.

주:

다음 명령 예에서는 Oracle Linux용 yum 저장소를 사용합니다. 명령에서 "ol6"의 "l"은 "L"의 소문자입니다.

1. Oracle 공용 yum 서버에 대해 ping을 수행하여 네트워크 연결이 작동 중인지 확인합니다.

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

2. yum 저장소 디렉토리로 변경하고 yum 저장소 파일 이름을 확인합니다.

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

3. 기존 yum 저장소 파일을 제거합니다.

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

4. yum 웹 사이트에서 최신 yum 저장소 파일을 다운로드합니다.

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

주:

이 명령의 다음 실행 시 새 저장소 파일이 새로운 확장자(예: *public-yum-ol6.repo.1*)로 *yum.repos.d* 폴더에 복사됩니다. 하지만 yum은 항상 확장자 없이 저장소 파일을 사용합니다.

5. 텍스트 편집기에서 저장소 파일을 엽니다.

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

6. 파일에서 해당 Linux 버전과 일치하는 항목을 찾고 *enabled=1*을 설정하여 사용으로 설정합니다. 기타 모든 항목은 *enabled=0*으로 설정하여 사용 안함으로 설정합니다.

예를 들면 다음과 같습니다.

```
[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. 파일을 저장하고 종료합니다.

2.3.6. 필수 Linux 패키지 설치

STA 설치 및 작업을 위해서는 추가 RPM 패키지가 필요합니다. STA 설치 프로그램에서는 다음 패키지를 확인하며, 존재하지 않을 경우 STA 설치가 실패합니다.

주:

RPM 패키지 이름은 대소문자를 구분합니다.

• <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>

다양한 방법으로 필수 RPM 패키지를 설치할 수 있습니다. 이 절차에서는 yum을 사용하는 방법에 대해 설명합니다.

yum 패키지 설치 명령은 사용자의 Linux 버전에 해당하는 최신 버전을 확인한 후 해당 패키지 및 모든 종속 항목을 설치합니다. Linux 설치에 따라 이러한 패키지 중 일부는 이미 설치되었을 수 있습니다. 패키지가 이미 설치되어 있고 최신 버전이면 시스템이 이러한 사실을 사용자에게 알립니다.

1. STA 서버에서 터미널 세션을 엽니다.
2. 다음과 같이 진행합니다.
 - Oracle의 공용 yum 서버(2.3.5절. “yum의 올바른 설정 확인(선택 사항)” 참조)에 연결할 수 있는 경우 다음 방법 중 하나를 사용하여 패키지를 설치합니다.
 - 한 번에 하나씩 패키지를 설치합니다. 지정된 패키지는 다운로드되어 확인되며 사용자는 표시되는 모든 메시지에 답해야 합니다.

```
# yum install package_name
```

- 메시지 표시 없이 한 번에 모든 패키지를 설치합니다. `-y` 옵션을 지정하면 모든 설치 프롬프트에 자동으로 "yes"가 응답됩니다.

```
# 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
```

- 네트워크 방화벽에서 외부 네트워크 액세스를 금지하는 경우, yum을 사용하여 Linux 매체에서 로컬로 사용 가능한 패키지를 설치할 수 있습니다. 예를 들면 다음과 같습니다.

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

2.3.7. SSH의 올바른 설정 확인

이 절차를 사용하여 SSH(보안 셸)가 STA 서버에서 올바르게 설정되었는지 확인하십시오. 이렇게 하면 원격 호스트로 STA 데이터베이스 백업을 전송하는 속도가 빨라집니다.

1. 텍스트 편집기에서 SSH 구성 파일을 엽니다.

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

2. *AddressFamily* 및 *UseDNS* 항목을 검색합니다. 앞에 주석 문자가 붙지 않고 값이 다음과 같도록 수정합니다.

```
AddressFamily inet
UseDNS no
```

3. 파일을 저장하고 종료합니다.
4. sshd 데몬을 다시 시작합니다.

```
# service sshd restart
```

2.3.8. 올바른 DNS 설정 확인

이 절차를 사용하여 STA 서버의 IP 주소가 해당 호스트 이름으로 매핑되는지 확인하십시오.

1. 텍스트 편집기에서 hosts 파일을 엽니다.

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

2. 파일의 끝에 STA 서버의 IP 주소를 추가하고 탭 문자를 추가한 다음 STA 서버의 호스트 이름을 추가합니다. 예를 들면 다음과 같습니다.

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

3. 파일을 저장하고 종료합니다. 새로운 설정을 적용하기 위해 STA 서버를 다시 시작할 필요는 없습니다.

2.3.9. 이름 서비스 사용 안함으로 설정

LDAP와 같은 이름 서비스는 STA 설치와 충돌할 수 있습니다. 이 절차를 사용하여 이러한 서비스를 일시적으로 사용 안함으로 설정하십시오.

1. 텍스트 편집기에서 Name Service Switch 구성 파일을 엽니다.

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

2. 모든 이름 서비스 항목을 사용 안함으로 설정합니다. 예를 들어, LDAP를 사용 안함으로 설정하려면 다음과 같이 다음 라인에서 "ldap"를 주석 처리합니다.

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

3. 파일을 저장하고 종료합니다. 새로운 설정을 적용하기 위해 STA 서버를 다시 시작할 필요는 없습니다. STA 설치 후 nsswitch.conf 파일을 수정하여 이름 서비스를 다시 사용으로 설정할 수 있습니다.

2.3.10. 로컬 브라우저 기능 확인(선택 사항)

STA 서버에서 STA를 로컬로 구성하고 관리하려면 지원되는 최소 브라우저 버전 및 플러그인이 설치되어 있는지 확인하십시오(STA 요구 사항 설명서 참조).

주:

Oracle은 서버 성능 저하 문제로 인해 STA 응용 프로그램에 대한 로컬 액세스를 권장하지 않습니다.

STA 설치

이 장에서는 이 서버에 STA를 새로 설치한다고 가정합니다.

- 이전 버전에서 STA를 업그레이드 하는 경우 [8장. STA 2.1.0으로 업그레이드](#)를 참조하십시오. Oracle에서는 최신 버전의 STA를 설치하거나 최신 버전으로 업그레이드할 것을 권장합니다.
- STA를 재설치하거나 현재 설치를 복구해야 하는 경우 [9장. STA 제거 및 복원](#)을 참조하십시오.

주:

Oracle은 STA가 전용 서버(이 설명서에서는 STA 서버라 함)에 설치된 경우에만 지원을 제공합니다.

이 장은 다음과 같은 항목으로 구성되어 있습니다.

- [STA 설치 프로그램에서 사용하는 사용자, 그룹 및 위치](#)
- [STA 설치 중 구성되는 계정 및 포트](#)
- [STA 설치 및 제거 로그](#)
- [STA 설치 프로그램 모드](#)
- [STA 설치 작업](#)

[부록 C. 설치 및 업그레이드 워크시트](#)에는 설치 작업을 구성하고 설정을 기록하는 데 사용할 수 있는 워크시트가 포함되어 있습니다.

3.1. STA 설치 프로그램에서 사용하는 사용자, 그룹 및 위치

이 절에서는 STA 설치 프로세스에 사용되는 핵심 개념 및 용어에 대해 설명합니다.

Oracle 설치 그룹

STA 서버에 Oracle 제품을 설치 및 업그레이드하는 데 사용되는 Linux 그룹입니다. Oracle은 이 용도로만 사용되는 별도의 그룹을 만들 것을 권장합니다.

STA 설치를 수행하려면 이 그룹의 구성원인 사용자로 로그인해야 합니다. Linux *root* 사용자나 슈퍼유저 권한이 있는 다른 사용자로는 STA를 설치할 수 없습니다.

이 설명서의 지침 및 예에서는 이 그룹을 *oinstall*이라고 합니다. 이름이 다른 경우 선택한 이름으로 이 이름을 대체하십시오.

Oracle 설치 사용자

STA 서버에 Oracle 제품을 설치 및 업그레이드하는 데 사용되는 Linux 사용자입니다. Oracle 설치 그룹의 구성원인 어떤 사용자도 가능합니다.

이 설명서의 지침 및 예에서는 이 사용자를 *oracle*이라고 합니다. 이름이 다른 경우 선택한 이름으로 이 이름을 대체하십시오.

Oracle 중앙 인벤토리 위치

STA 서버에 설치된 Oracle 제품에 대한 정보를 추적하는 데 사용되는 디렉토리입니다. STA 설치 프로그램 및 제거 프로그램 로그는 이 위치의 *logs* 하위 디렉토리에 보관됩니다.

Oracle 설치 사용자는 이 디렉토리를 소유해야 하며 이 디렉토리에 대한 전체 권한을 가지고 있어야 합니다. Oracle 설치 그룹의 다른 사용자가 적절할 액세스 권한을 가지고 Oracle 제품을 설치할 수 있도록, Oracle 설치 사용자의 홈 디렉토리를 사용해서는 안 됩니다.

이 위치는 이 절에 설명된 다른 디렉토리와 별도의 위치여야 합니다. 이 설명서의 지침 및 예에서는 이 위치로 */opt/oracle/oraInventory*를 사용합니다. 디렉토리가 다른 경우 선택한 디렉토리로 이 디렉토리를 대체하십시오.

주:

Oracle은 모든 Oracle 설치 프로그램이 이 서버에서 동일한 중앙 인벤토리 위치를 사용하도록, STA 설치가 완료된 후 이 위치를 등록할 것을 권장합니다. 자세한 내용은 [3.6.7절. "Oracle 중앙 인벤토리 위치 등록"](#)을 참조하십시오.

Oracle 스토리지 홈 위치

STA 및 이와 연관된 Oracle 소프트웨어가 설치된 디렉토리입니다. STA는 자동으로 이 위치의 *StorageTek_Tape_Analytics* 하위 디렉토리에 설치됩니다. [STA 홈](#)을 참조하십시오.

이 디렉토리가 이미 존재하는 경우 Oracle 설치 사용자에게 해당 디렉토리에 대한 전체 권한이 있어야 합니다. 이 디렉토리가 존재하지 않는 경우 Oracle 설치 사용자에게 상위 디렉토리에 대한 전체 권한이 있다면 STA 설치 프로그램이 이 디렉토리를 자동으로 만듭니다.

주:

이 서버에 이전 버전의 STA가 설치되어 있는 경우 이 디렉토리는 이미 존재할 수 있습니다. 이런 경우 이 디렉토리를 *root*가 아니라 Oracle 설치 그룹이 소유하고 있는지 확인해야 합니다.

이 위치는 이 절에 설명된 다른 디렉토리와 별도의 위치여야 합니다. 이 설명서의 지침 및 예에서는 이 위치로 */oracle*을 사용합니다. 디렉토리가 다른 경우 선택한 디렉토리로 이 디렉토리를 대체하십시오.

STA 홈

모든 STA 소프트웨어가 설치된 디렉토리입니다. 이 디렉토리는 이름이 *StorageTek_Tape_Analytics*로 지정되며 STA 설치 프로그램은 [Oracle 스토리지 홈 위치](#) 내에 이 디렉토리를 자동으로 만듭니다.

이 설명서의 지침 및 예에서는 이 위치로 */oracle/StorageTek_Tape_Analytics*를 사용합니다.

STA 설치 프로그램 위치

STA 설치 프로그램을 다운로드하는 디렉토리입니다.

이 위치는 이 절에 설명된 다른 디렉토리와 별도의 위치여야 합니다. 이 설명서의 지침 및 예에서는 이 위치로 `/Installers`를 사용합니다. 디렉토리가 다른 경우 선택한 디렉토리로 이 디렉토리를 대체하십시오.

STA 설치 프로그램 작업 위치

기본적으로 STA 설치 프로그램은 `/tmp` 디렉토리에 압축이 풀리며 약 4GB의 공간을 소비합니다. 다음과 같이 옵션을 지정하여 STA 설치 프로그램을 실행하면 다른 작업 위치를 지정할 수 있습니다. `-J-Djava.io.tmpdir=working_directory`

`working_directory`는 절대 경로여야 합니다. 예를 들면 다음과 같습니다.

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

이 옵션 사용에 대한 자세한 내용은 [부록 B. STA 자동 모드 설치 프로그램 및 제거 프로그램](#)을 참조하십시오.

STA 로그 위치

STA 및 MySQL 로그의 위치입니다. 콘텐츠는 늘어나며 로그 교체를 통해 관리됩니다. 기본 위치는 `/var/log/tbi`이지만 STA 설치 후 언제든지 이 위치를 변경할 수 있습니다. 자세한 내용은 [3.6.6절. "STA 로그 디렉토리 재배치\(선택 사항\)"](#)를 참조하십시오.

공간 요구 사항은 [2.1.2절. "STA 파일 시스템 레이아웃 검토"](#)를 참조하십시오.

3.2. 사용자 이름 및 암호 요구 사항

사용자 이름 요구 사항은 다음과 같습니다.

- 길이가 1~16자여야 합니다.
- 모든 사용자 이름은 고유해야 합니다.

암호 요구 사항은 다음과 같습니다.

- 길이가 8~31자여야 합니다.
- 최소한 숫자 1개와 대문자 1개를 포함해야 합니다.
- 공백을 포함할 수 없습니다.
- 다음 특수 문자를 포함할 수 없습니다.

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

3.3. STA 설치 중 구성되는 계정 및 포트

STA 설치 프로그램은 사용자가 제공하는 사양에 따라 사용자 계정 및 포트 번호를 구성합니다.

3.3.1. STA 관리용 사용자 계정

STA 설치 중 다음과 같은 필수 계정이 만들어집니다. 이러한 계정은 STA에 특정된 것으로, Linux 사용자 이름이 아닙니다.

- [WebLogic 계정](#)
- [STA 데이터베이스 계정](#)

3.3.1.1. WebLogic 계정

다음 WebLogic 계정은 WebLogic 관리 콘솔 또는 STA 응용 프로그램에 로그인하는 데 사용됩니다.

WebLogic 관리

WebLogic 환경을 변경하기 위해(예: WebLogic을 LDAP 또는 RACF 서버에 연결) WebLogic 관리 콘솔에 로그인하는 데 사용됩니다.

주의:

이 계정의 사용자 이름 및 암호는 검색할 수 없습니다. 이 자격 증명을 분실하면 STA를 재설치해야 합니다.

STA 관리자

전체 액세스 권한으로 STA 응용 프로그램에 로그인하는 데 사용됩니다.

STA 설치가 완료되면 STA 응용 프로그램을 사용하여 지정 가능한 역할을 가진 추가 사용자 계정을 만들 수 있습니다. 자세한 내용은 STA 사용 설명서를 참조하십시오.

3.3.1.2. STA 데이터베이스 계정

다음 STA 데이터베이스 계정은 STA가 STA 데이터베이스를 액세스 및 관리하기 위해 사용하는 MySQL 계정입니다.

STA 데이터베이스 루트 사용자

MySQL 데이터베이스를 소유하며 루트 데이터베이스 설치를 만드는 데 사용됩니다. 사전 정의된 사용자 이름은 *root*이며 변경할 수 없습니다.

주의:

이 계정의 암호는 검색할 수 없습니다.

STA 데이터베이스 응용 프로그램 사용자

STA가 데이터베이스에 연결하는 데 사용하는 사용자 정의된 MySQL 사용자 이름(예: *stadb*)입니다. 데이터 테이블에서 권한 만들기, 업데이트, 삭제 및 읽기에 필요합니다.

STA 데이터베이스 보고서 사용자

STA 이외의 프로그램 및 타사 응용 프로그램이 데이터베이스에 연결하는 데 사용할 수 있는 사용자 정의된 MySQL 사용자 이름(예: *starpt*)입니다. 특정 데이터베이스 테이블에 대한 읽기 전용 액세스 권한을 가집니다.

STA 데이터베이스 관리자 사용자

STA 관리 및 모니터링 유틸리티가 주로 예약된 백업을 구성하거나 실행하기 위해 데이터베이스에 연결하는 데 사용하는 사용자 정의된 MySQL 사용자 이름(예: *stadb*)입니다. 모든 데이터베이스 테이블에서 "grant option"을 제외한 모든 DBA 권한을 가집니다.

3.3.2. STA에서 사용하는 포트

STA는 다음 포트를 사용하여 데이터를 검색하고 수신합니다. 이 포트는 전용 포트이며 STA에서 계속 사용할 수 있어야 합니다. STA 설치 프로그램은 이 포트가 네트워크에서 이미 사용 중이 아닌지 확인합니다.

주의:

STA 설치 중 이 포트를 구성하면 STA를 제거 및 재설치하지 않고는 변경할 수 없습니다.

3.3.2.1. 구성 불가능한 외부 포트

표 3.1. "구성 불가능한 외부 포트"에 설명된 포트는 STA 서버와 다른 네트워크 엔티티 간 통신을 위해 사용되는 외부 포트입니다. 포트 값은 고정되어 있으며 STA 설치 중 변경할 수 없습니다.

방화벽/라우터 구성: STA 서버와 백업 서버 사이(SSH의 경우) 및 STA 서버와 모니터링 라이브러리 사이(SNMP 및 SNMPTRAP의 경우)에서 도달할 수 있어야 합니다.

표 3.1. 구성 불가능한 외부 포트

포트	프로토콜	설명/용도
22	SSH	보안 셸. STA 데이터베이스 백업 및 라이브러리 로그인용입니다.
161	SNMP	SNMP(Simple Network Management Protocol). SNMP 요청 전송용입니다.
162	SNMPTRAP	SNMP 통지(트랩) 수신용입니다.

3.3.2.2. 구성 가능한 외부 포트

표 3.2. "구성 가능한 외부 포트"에 설명된 포트는 STA 서버와 다른 네트워크 엔티티 간 통신을 위해 사용되는 외부 포트입니다. 이러한 포트는 표준 포트 80과 8080(HTTP) 및 443(HTTPS)에 해당하는 구성 가능 포트이며, 네트워크의 다른 HTTP 및 HTTPS 포트와 달라야 합니다. 해당 값을 선택하는 데 도움이 필요하다면 네트워크 관리자에게 문의하십시오.

방화벽/라우터 구성: STA 서버와 STA GUI를 실행 중인 클라이언트 사이에서 도달할 수 있어야 합니다.

표 3.2. 구성 가능한 외부 포트

기본 포트	프로토콜	설명/용도
7019	HTTP	WebLogic 관리 콘솔에 액세스, 비보안
7020	HTTPS	WebLogic 관리 콘솔에 액세스, 보안
7021	HTTP	staUi 관리 서버. STA GUI에 액세스, 비보안
7022	HTTPS	staUi 관리 서버. STA GUI에 액세스, 보안

3.3.2.3. 구성 가능한 내부 포트

표 3.3. "구성 가능한 내부 포트"에 설명된 포트는 내부 STA 통신용으로 사용됩니다. 이 포트 값은 고유해야 합니다.

방화벽/라우터 구성: 해당 사항 없음

표 3.3. 구성 가능한 내부 포트

기본 포트	프로토콜	설명/용도
7023	HTTP	staEngine 관리 서버. 기본 STA 내부, 비보안
7024	HTTPS	staEngine 관리 서버. 기본 STA 내부, 보안
7025	HTTP	staAdapter 관리 서버. SNMP 통신, 비보안
7026	HTTPS	staAdapter 관리 서버. SNMP 통신, 보안

3.4. STA 설치 및 제거 로그

문제를 해결하기 위해 STA 설치 및 제거 로그를 사용할 수 있습니다. 대부분의 로그 파일 이름에는 설치 또는 제거 인스턴스를 식별할 수 있도록 시간 기록이 포함됩니다. 시간 기록은 설치 또는 제거가 시작된 날짜 및 시간입니다.

특히 다음 로그는 설치 또는 제거가 실패했을 때 유용한 정보를 제공합니다. 해당 위치에 대한 자세한 내용은 [/STA_logs/install](#)을 참조하십시오.

- *installtimestamp.log*
- *sta_installtimestamp.log*
- *deinstalltimestamp.log*
- *sta_deinstalltimestamp.log*

3.4.1. 로그 파일 위치

STA 설치 및 제거 로그의 위치는 설치 또는 제거 상태에 따라 다릅니다. 로그는 다음 디렉토리에서 찾을 수 있습니다. 이러한 디렉토리에 대한 자세한 내용은 [2.1.2절. "STA 파일 시스템 레이아웃 검토"](#)를 참조하십시오.

/tmp/OracleInstalltimestamp

이 디렉토리는 진행 중인 설치 또는 제거 로그를 포함합니다. 다음은 이 디렉토리에서 볼 수 있는 로그 목록의 예입니다.

```
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

여기서 *Oracle_storage_home*은 STA 설치 중 정의된 Oracle 스토리지 홈 위치입니다.

이 디렉토리는 성공적으로 완료된 설치 및 제거 로그를 포함합니다. 오류 또는 패치 로그와 같은 일부 로그는 해당하는 경우에만 포함됩니다.

다음은 이 디렉토리에서 볼 수 있는 로그 목록의 예입니다.

```
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

기본적으로 *STA_logs*는 `/var/log/tbi`에 있습니다. 원하는 경우 STA 설치 후 언제든지 선택한 위치로 이 디렉토리를 재배치할 수 있습니다. 자세한 내용은 [3.6.6절. “STA 로그 디렉토리 재배치\(선택 사항\)”](#)를 참조하십시오.

이 디렉토리는 성공 또는 실패로 완료된 설치 및 제거 로그를 포함합니다. 이 디렉토리에는 WebLogic Server 및 MySQL 데이터베이스 설치와 관련된 로그 및 STA 응용 프로그램의 설치 및 구성 로그가 포함됩니다.

다음은 이 디렉토리에서 볼 수 있는 로그 목록의 예입니다.

```
dbinstall.log
dbinstall.mysqlfd.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 설치 프로그램 모드

다음 모드 중 하나를 사용하여 STA를 설치할 수 있습니다.

그래픽 모드

권장되는 설치 모드입니다. 이 모드에는 STA를 설치하기 위한 그래픽 사용자 인터페이스가 제공되며, X11 디스플레이가 필요합니다. 자세한 내용은 [부록 A. STA 그래픽 설치 프로그램 및 제거 프로그램 화면 참조](#)를 참조하십시오.

자동 모드

이 모드를 사용하면 그래픽 사용자 인터페이스를 건너뛰고 응답 파일이라는 XML 등록 정보 파일에 설치 옵션을 제공할 수 있습니다. 자세한 내용은 [부록 B. STA 자동 모드 설치 프로그램 및 제거 프로그램](#)을 참조하십시오.

이 모드는 무인 설치 및 여러 시스템에 STA를 설치하는 경우에 유용합니다. 응답 파일을 사용하면 단일 매개변수 세트를 제공하여 설치를 자동화할 수 있습니다. 자동 모드 설치 프로그램은 스크립트 또는 Linux 명령줄에서 실행할 수 있습니다.

3.6. STA 설치 작업

STA를 설치하려면 다음 작업을 모두 나열된 순서대로 수행하십시오.

- [3.6.1절. “설치에 필요한 정보 식별 또는 만들기”](#)
- [3.6.2절. “설치 필요 조건 확인”](#)
- [3.6.3절. “STA 다운로드”](#)
- [3.6.4절. “STA 설치”](#)

- 3.6.5절. “성공적인 설치 확인”
- 3.6.6절. “STA 로그 디렉토리 재배치(선택 사항)”
- 3.6.7절. “Oracle 중앙 인벤토리 위치 등록”

3.6.1. 설치에 필요한 정보 식별 또는 만들기

이 절차를 사용하여 STA 설치 프로그램을 실행하는 데 필요한 사용자 및 위치를 식별하고, 필요한 경우 만듭니다. 표 C.2. “설치 사용자 및 위치 워크시트”를 사용하여 이 정보를 기록할 수 있습니다. 이 항목에 대한 자세한 내용은 3.1절. “STA 설치 프로그램에서 사용하는 사용자, 그룹 및 위치”를 참조하십시오.

1. Linux 루트 사용자로 로그인합니다.
2. STA 서버에 Oracle 중앙 인벤토리 포인터 파일 `/etc/oraInst.loc`가 있는지 확인합니다. 이전에 Oracle 중앙 인벤토리를 등록했다면 이 파일이 있어야 합니다. 자세한 내용은 [Oracle 중앙 인벤토리 위치](#)를 참조하십시오.
 - 파일이 존재하면 해당 내용을 기록합니다. 예를 들면 다음과 같습니다.

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

`inventory_loc` 항목은 Oracle 중앙 인벤토리 위치를 식별하고, `inst_group` 항목은 Oracle 설치 그룹을 식별합니다.

- 파일이 없는 경우 3 단계로 이동하여 필요한 사용자 및 위치를 만듭니다. 예를 들면 다음과 같습니다.

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

3. 2 단계에서 Oracle 중앙 인벤토리 포인터 파일이 없었다면 Oracle 설치 그룹을 만듭니다. 자세한 내용은 [Oracle 설치 그룹](#)를 참조하십시오. 예를 들면 다음과 같습니다.

```
# groupadd oinstall
```

4. Oracle 설치 사용자의 사용자 이름 및 암호를 확보하거나 필요한 경우 새로 만듭니다. 이 사용자는 Oracle 설치 그룹에 속해야 합니다. 자세한 내용은 [Oracle 설치 사용자](#)를 참조하십시오. 예를 들면 다음과 같습니다.

```
# 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.
```

5. 2 단계에서 Oracle 중앙 인벤토리 포인터 파일이 없었다면 Oracle 중앙 인벤토리 위치를 만듭니다. 이 디렉토리는 Oracle 설치 사용자가 소유해야 합니다. 자세한 내용은 [Oracle 중앙 인벤토리 위치](#)를 참조하십시오. 예를 들면 다음과 같습니다.

```
# 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 ..
```

6. Oracle 스토리지 홈 위치를 찾거나, 이 위치가 존재하지 않으면 해당 디렉토리를 만듭니다. 이 디렉토리는 Oracle 설치 사용자가 소유해야 합니다. 자세한 내용은 [Oracle 스토리지 홈 위치](#)를 참조하십시오. 예를 들면 다음과 같습니다.

```
# 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 ..
```

7. STA 설치 프로그램 위치를 찾거나, 이 위치가 존재하지 않으면 해당 디렉토리를 만듭니다. 자세한 내용은 [STA 설치 프로그램 위치](#)를 참조하십시오. 예를 들면 다음과 같습니다.

```
# mkdir /Installers
```

8. Linux 루트 사용자의 암호를 확보합니다. STA 설치 프로그램은 일부 작업을 수행하기 위해 루트로 액세스해야 하므로 해당 암호를 묻는 메시지를 표시합니다.
9. WebLogic 관리자, STA 관리자 및 설치 중 만들어질 MySQL 계정의 사용자 이름을 선택합니다. 자세한 내용은 [3.3.1절. "STA 관리용 사용자 계정"](#)을 참조하십시오.
10. STA 작업에 필요한 구성 가능한 내부 및 외부 포트의 포트 번호를 선택합니다. 필요한 네트워크에서 외부 포트가 열려 있는지 확인합니다. 자세한 내용은 [3.3.2절. "STA에서 사용하는 포트"](#)를 참조하십시오.
11. Oracle의 RDA(원격 진단 에이전트)를 구성하는 데 사용할 사이트의 도메인 이름을 확보합니다. 자세한 내용은 [STA 사용 설명서](#)를 참조하십시오.

3.6.2. 설치 필요 조건 확인

다음 절차에 따라 STA 설치 프로그램을 실행하기 전에 필수 조건을 확인합니다. 이 절차는 선택 사항이지만 이 필수 조건이 하나라도 충족되지 않으면 STA 설치가 실패합니다. 설치 요구 사항의 전체 목록은 [STA 요구 사항 설명서](#)를 참조하십시오.

이 단계는 모두 STA 서버에서 수행됩니다. 도움이 필요하면 Linux 관리자에게 문의하십시오.

주:

STA 설치에서는 [2장. Linux 설치](#)에 지정된 Linux RPM 패키지가 포함된 64비트 Linux가 설치되어 있다고 가정합니다. 필요한 패키지가 설치되지 않은 경우 STA 설치가 실패합니다. 자세한 내용은 다음 문서를 참조하십시오.

- 지원되는 Linux 버전은 STA 요구 사항 설명서를 참조합니다.
- 필요한 패키지 목록은 [2.3.6절. "필수 Linux 패키지 설치" \[35\]](#)를 참조합니다.

주의:

기존 소프트웨어를 영구적으로 제거하거나 바꾸도록 선택하기 전에 필요에 따라 파일을 백업하십시오.

1. STA가 서버에 설치되지 않았는지 확인합니다. STA 설치 프로그램은 새 설치에만 사용 됩니다. 다른 지침은 다음 절을 참조하십시오(해당하는 경우).
 - STA를 이전 버전에서 업그레이드하려면 [8장. STA 2.1.0으로 업그레이드](#)를 참조합니다.
 - STA를 재설치하거나 현재 설치를 복구하려면 [9장. STA 제거 및 복원](#)을 참조합니다.

다음 예에서는 STA가 설치되지 않았음을 보여 줍니다.

```
$ 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
$
```

2. MySQL이 STA 서버에 설치되지 않았는지 확인합니다. MySQL이 설치된 경우 설치 프로그램이 해당 설치를 제거하고 재설치하므로 기존의 모든 MySQL 데이터베이스가 삭제됩니다.
3. `/tmp` 디렉토리의 사용 가능 공간이 4GB 이상인지 확인합니다. 이 디렉토리는 기본 STA 설치 프로그램 작업 위치입니다.

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

주:

원하는 경우 STA 설치 프로그램을 시작할 때 다른 작업 디렉토리를 지정할 수 있습니다. 자세한 내용은 [STA 설치 프로그램 작업 위치](#)를 참조하십시오.

4. SELinux가 사용 안함으로 설정되었는지 확인합니다. "[사후 설치 작업](#)"의 지침을 따르면 SELinux는 이미 사용 안함으로 설정되어 있어야 합니다. 자세한 내용은 [2.3.1절. "SELinux 사용 안함으로 설정" \[31\]](#)을 참조하십시오.

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

5. Linux 방화벽(IPTables)이 중지되었는지 확인합니다. "사후 설치 작업"의 지침을 따랐다면 IPTables는 이미 중지되었어야 합니다. 자세한 내용은 2.3.2절. "Linux 방화벽 사용 안함으로 설정" [32]을 참조하십시오.

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

주:

사용자의 사이트에서 IPTables 서비스를 실행해야 하는 경우 STA를 설치하고, 라이브러리를 구성하고, STA가 라이브러리를 모니터링하고 있는지 확인한 후 이 서비스를 시작할 수 있습니다. IPTables를 시작한 후 STA가 라이브러리를 모니터링하고 있는지 다시 확인해야 합니다.

6. SNMP 서비스를 중지하고 구성을 해제합니다.

네트워크 포트 충돌 및 기타 문제를 피하기 위해 STA 서버는 다른 SNMP 서비스를 실행해서는 안됩니다. 다음 조건 중 하나에 해당하면 STA 설치 프로그램이 종료됩니다.

- snmpd 및 snmptrapd 데몬 서비스가 실행 중입니다.
- UDP 포트 161(SNMP) 및 162(SNMPTRAP)를 사용할 수 없습니다.

필요에 따라 다음 단계를 수행합니다.

- a. SNMP *snmpd* 및 *snmptrapd* 서비스의 현재 상태를 표시합니다.

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

- b. 필요한 경우 SNMP 서비스를 즉시 중지합니다.

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

주:

이 명령 중 하나를 실행할 때 "FAILED" 오류가 발생하는 경우 서비스가 이미 중지되었을 수 있습니다.

- c. Linux가 재부트될 때 SNMP 서비스가 자동으로 시작되지 않도록 다음을 입력하여 Linux 서비스 구성 파일에서 해당 서비스를 사용 안함으로 설정합니다.

```
# 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. 다음과 같이 해당 모드 관련 요구 사항을 검토 및 확인합니다.
 - STA 그래픽 설치 프로그램의 경우 [A.1절. “그래픽 모드 디스플레이 요구 사항”](#)을 참조합니다.
 - STA 자동 모드 설치 프로그램의 경우 [B.1.1절. “자동 모드 요구 사항”](#)을 참조합니다.

3.6.3. STA 다운로드

STA 설치 프로그램 다운로드에는 다음 파일이 포함됩니다. *version*은 STA 설치 버전 번호입니다.

- *sta_install_version_linux64.bin*—모든 설치에 필요합니다.
- *sta_install_version_linux64-2.zip*—모든 설치에 필요합니다.
- *silentInstallUtility_version.jar*—응답 파일 작성 유틸리티입니다. STA 자동 모드 설치 프로그램 또는 제거 프로그램을 사용할 때만 필요합니다. 자세한 내용은 [부록 B. STA 자동 모드 설치 프로그램 및 제거 프로그램](#)을 참조하십시오.

1. 브라우저 창에서 다음 URL의 Oracle Software Delivery Cloud 웹사이트에 액세스합니다.

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

2. **Sign In/Register**를 누릅니다.
3. Oracle 고객지원센터에서 제공한 사용자 ID 및 암호를 입력하거나 새 계정을 만듭니다.
4. Terms & Restrictions 화면에서 License Agreement and Export Restrictions에 동의한다는 확인란을 선택한 다음 **Continue**를 누릅니다.
5. Media Pack Search 화면에서 다음 단계를 수행합니다.
 - a. **Select a Product Pack** 메뉴에서 Oracle StorageTek Products를 선택합니다.
 - b. **Platform** 메뉴에서 Linux x86-64를 선택합니다.
 - c. **Go**를 누릅니다.
6. Results 테이블에서 **Oracle StorageTek Tape Analytics 2.1.0**을 선택하고 **Continue**를 누릅니다.
7. 각 미디어 팩 ZIP 파일에 대해 **Download**를 누른 다음 해당 파일을 4GB 이상의 사용 가능한 공간이 있는 위치에 저장합니다.
8. 압축 풀기 도구를 사용하여 zip 파일의 내용을 [3.6.1절. “설치에 필요한 정보 식별 또는 만들기”](#)에서 선택한 STA 설치 프로그램 위치(예: */Installers*)에 풉니다.
9. Oracle 설치 사용자에게 *sta_install_version_linux64.bin* 파일에 대한 실행 권한이 있고 *sta_install_version_linux64-2.zip* 파일에 대한 읽기 권한이 있는지 확인합니다. 예를 들면 다음과 같습니다.

```
# 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
```

10. 설치 프로그램 다운로드 패키지에 포함되어 있는 STA 릴리스 노트를 검토합니다.

3.6.4. STA 설치

다음 절차에 따라 STA 설치 프로그램을 실행합니다. 그래픽 모드 또는 자동 모드 중 하나를 사용하여 STA를 설치할 수 있습니다. 자세한 내용은 [3.5절. "STA 설치 프로그램 모드"](#)를 참조하십시오.

1. 터미널 창에서 STA 서버에서 연결한 다음 Oracle 설치 사용자로 로그인합니다. 자세한 내용은 [Oracle 설치 사용자](#)를 참조하십시오.
2. STA 설치 프로그램 위치로 변경합니다. 자세한 내용은 [STA 설치 프로그램 위치](#)를 참조하십시오. 예를 들면 다음과 같습니다.

```
$ cd /Installers
```

3. 다음 명령 중 하나를 사용하여 STA 설치 프로그램을 실행합니다.
 - STA 그래픽 설치 프로그램을 사용하는 경우:

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

여기서 *version*은 다운로드한 STA 설치 프로그램의 버전입니다. 예를 들면 다음과 같습니다.

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

이 모드를 사용하려면 X11 디스플레이가 필요합니다. 자세한 내용은 [부록 A. STA 그래픽 설치 프로그램 및 제거 프로그램 화면 참조](#)를 참조하십시오.

- STA 자동 설치 프로그램을 사용하는 경우:

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

여기서 각 항목은 다음과 같습니다.

- *version*은 다운로드한 STA 설치 프로그램의 버전입니다.
- *response_file*은 이전에 만든 응답 파일의 절대 경로입니다.

예를 들면 다음과 같습니다.

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

이 모드를 사용하려면 먼저 *silentInstallUtility.jar* 파일을 다운로드하고 설치 옵션을 지정하는 응답 파일을 만들어야 합니다. 자세한 내용은 [부록 B. STA 자동 모드 설치 프로그램 및 제거 프로그램](#)을 참조하십시오.

3.6.5. 성공적인 설치 확인

다음 절차에 따라 STA가 실행 중인지 확인합니다.

1. 다음 단계를 사용하여 STA bin 디렉토리가 시스템 루트 사용자에게 대한 *PATH* 변수에 포함되어 있는지 확인합니다.
 - a. 현재 STA 서버에서 터미널 세션을 열고 시스템 루트 사용자로 로그인합니다.
 - b. 텍스트 편집기를 사용하여 사용자 프로파일을 엽니다. 예를 들면 다음과 같습니다.

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

- c. STA bin 디렉토리를 *PATH* 정의에 추가합니다. 예를 들어 다음 라인을 파일에 추가합니다.

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

여기서 *Oracle_storage_home*은 STA 설치 중 지정된 Oracle 스토리지 홈 위치입니다.

- d. 파일을 저장하고 종료합니다.
 - e. 로그아웃 후 시스템 루트 사용자로 다시 로그인합니다.
 - f. *PATH* 변수가 올바르게 업데이트되었는지 확인합니다.

```
# 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 명령을 사용하여 모든 STA 서비스가 실행 중이고 활성 상태인지 확인합니다. [예 3.1. "STA 성공적인 상태 표시"](#)은 성공적인 상태 표시의 예입니다. 자세한 내용은 STA 관리 설명서를 참조하십시오.

예 3.1. STA 성공적인 상태 표시

```
$ 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
stau service is running
.... and the deployed application for stau is in an ACTIVE state

```

3. 다음과 같이 진행합니다.

- STA 서비스가 실행 중이고 활성 상태이면 라이브러리 및 STA 구성을 시작할 수 있습니다. 자세한 내용은 [5장. 라이브러리에서 SNMP 구성](#) 및 [6장. STA의 라이브러리 연결 구성](#)을 참조하십시오.
- STA 서비스에 문제가 있으면 설치 및 STA 로그에서 자세한 정보를 검토할 수 있습니다. 로그의 위치는 [3.4절. "STA 설치 및 제거 로그"](#)를 참조하십시오.

3.6.6. STA 로그 디렉토리 재배포(선택 사항)

STA 및 MySQL 로그를 기본값인 `/var/log/tbi`가 아닌 위치로 재배포하려는 경우에만 이 절차를 사용하십시오. 이 절차를 완료하면 새 로그가 사용자가 지정한 위치에 기록됩니다. 이 절차는 STA가 설치된 후 언제든지 수행할 수 있습니다. 위치 요구 사항은 [2.1.2절. "STA 파일 시스템 레이아웃 검토"](#)를 참조하십시오.

1. 시스템 루트 사용자로 로그인합니다.
2. 모든 STA 서비스를 중지합니다.

```

# 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 및 MySQL 로그에 사용할 새 STA 로그 디렉토리를 만듭니다. 예를 들면 다음과 같습니다.

```

# 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. STA 및 MySQL이 쓸 수 있도록 디렉토리에 대한 액세스 권한을 변경합니다. 예를 들면 다음과 같습니다.

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

5. 현재 `/var/log/tbi` 디렉토리를 방금 만든 STA 로그 디렉토리로 이동합니다.

```
# 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. 새 STA 로그 디렉토리에서 기본 위치로의 심볼릭 링크를 만듭니다. 예를 들면 다음과 같습니다.

```
# 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. STA를 다시 시작합니다.

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

3.6.7. Oracle 중앙 인벤토리 위치 등록

STA 설치가 완료된 후 이 절차를 사용하여 STA 서버의 Oracle 중앙 인벤토리 위치를 등록합니다. 이 절차는 이 서버에서 한 번만 수행하면 됩니다.

이 절차는 Oracle 중앙 인벤토리 포인터 파일 `/etc/oraInst.loc`를 만드는데 이 파일을 통해 Oracle 중앙 인벤토리 위치 및 Oracle 설치 그룹이 서버에서 사용되는 모든 Oracle 설치 프로그램에 알려집니다.

1. Linux `root` 사용자로 로그인합니다.
2. Oracle 중앙 인벤토리 디렉토리로 변경합니다. 예를 들면 다음과 같습니다.

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

3. 해당 디렉토리에 있는 등록 스크립트를 실행합니다.

```
# ./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
#
```

Oracle 중앙 인벤토리 위치 및 Oracle 설치 그룹이 이제 Oracle 중앙 인벤토리 포인터 파일 `/etc/oraInst.loc`에서 식별됩니다.

STA의 라이브러리 기능 구성

라이브러리가 고품질 SNMP 데이터를 STA에 보내려면 선택한 기능이 적절하게 구성되어야 합니다. 이러한 기능은 라이브러리 모델에 따라 다릅니다. [5장. 라이브러리에서 SNMP 구성](#)으로 진행하기 전에 이 장의 작업을 완료해야 합니다.

이 장은 다음과 같은 절로 구성됩니다.

- [STA 데이터에 영향을 주는 라이브러리 기능](#)
- [라이브러리 사용자 인터페이스](#)
- [라이브러리 기능 구성 작업](#)

4.1. STA 데이터에 영향을 주는 라이브러리 기능

- [4.1.1절. "LTO 드라이브에 대한 ADI 인터페이스"](#)
- [4.1.2절. "이중 TCP/IP 및 중복 전자 부품\(SL3000 및 SL8500만 해당\)"](#)
- [4.1.3절. "라이브러리 컴플렉스 ID\(SL8500만 해당\)"](#)
- [4.1.4절. "드라이브 청소 경고\(SL3000 및 SL8500만 해당\)"](#)
- [4.1.5절. "볼륨 레이블 형식\(SL500 및 SL150만 해당\)"](#)
- [4.1.6절. "SCSI FastLoad 옵션\(SL500만 해당\)"](#)
- [4.1.7절. "중복된 볼륨 일련 번호 "](#)

4.1.1. LTO 드라이브에 대한 ADI 인터페이스

StorageTek 모듈식 라이브러리는 HP와 IBM의 LTO(Linear Tape Open) 드라이브를 지원합니다. ADI(Automation/Drive 인터페이스)를 지원하는 LTO 드라이브는 드라이브 구성 및 펌웨어 레벨에 따라 다양한 데이터(예: 드라이브 성능 및 사용률)를 라이브러리에 제공할 수 있습니다.

라이브러리가 다양한 LTO 드라이브 데이터를 STA에 보내려면 라이브러리와 LTO 드라이브 모두에서 ADI가 사용으로 설정되어야 합니다. 둘 중 하나라도 ADI가 사용으로 설정되지 않은 경우 라이브러리는 LTO 드라이브에 대한 기본 데이터만 전송합니다.

필요한 드라이브 펌웨어 레벨에 대한 자세한 내용은 STA 요구 사항 설명서를 참조하십시오.

4.1.1.1. LTO 드라이브에서 ADI 사용으로 설정

ADI를 사용으로 설정하는 방법은 드라이브 제조업체 및 모델에 따라 다릅니다.

- **HP LTO - 3, LTO - 4, LTO - 5 및 LTO-6:** 이러한 드라이브는 라이브러리에서 ADI가 사용으로 설정되고 라이브러리 및 드라이브가 재부트되면 자동으로 ADI 모드로 전환됩니다. (드라이브는 SL Console에서 재부트할 수 있습니다.)
- **IBM LTO - 3, LTO - 4, LTO - 5 및 LTO-6:** 이러한 드라이브는 ADI 모드에 대해 명시적으로 구성되어야 하며 라이브러리에서 ADI가 사용으로 설정되고 라이브러리가 재부트될 때까지 인식되지 않습니다. 자세한 내용은 표 4.1. “IBM LTO 드라이브에서 ADI를 사용으로 설정하는 방법”을 참조하십시오.

주:

Belisarius 어댑터 카드는 Oracle OKM(Oracle Key Manager) 테이프 암호화 솔루션에 대한 인터페이스를 제공합니다. 드라이브 및 Belisarius 카드 펌웨어는 모두 STA에 대한 최소 요구 사항을 충족해야 합니다.

표 4.1. IBM LTO 드라이브에서 ADI를 사용으로 설정하는 방법

IBM LTO 드라이브	LTO - 3	LTO - 4	LTO - 5, LTO-6
Belisarius 어댑터 카드가 없는 IBM	Oracle 고객지원센터에서 ADI 모드에 대해 드라이브 하드웨어를 구성합니다.	Oracle 고객지원센터에서 ADI 모드에 대해 드라이브 하드웨어를 구성합니다.	해당 사항 없음
Belisarius 어댑터 카드가 있는 IBM	해당 사항 없음	Oracle 고객지원센터에서 ADI 모드에 대해 드라이브 하드웨어를 구성합니다.	드라이브 펌웨어는 VOP(Virtual Operator Panel)에서 ADI 모드에 대해 구성해야 합니다. 지원이 필요하면 Oracle 고객지원센터에 문의하십시오.

4.1.1.2. 라이브러리에서 ADI를 사용으로 설정

기본적으로 ADI는 SL500, SL3000 및 SL8500 라이브러리에서 사용으로 설정되지 않으며 관리자나 Oracle 고객지원센터에서 수동으로 사용으로 설정해야 합니다. ADI를 사용으로 설정하려면 라이브러리 재부트가 필요하므로 LTO 드라이브를 설치할 계획이 있는 경우 미리 사용으로 설정해야 합니다.

SL3000 및 SL8500 라이브러리의 경우 라이브러리에 하이 메모리 드라이브 컨트롤러 (HBT) 카드가 있는 경우에만 ADI를 사용으로 설정할 수 있습니다. HBT 카드에 대한 자세한 내용은 STA 요구 사항 설명서를 참조하십시오.

4.1.2. 이중 TCP/IP 및 중복 전자 부품(SL3000 및 SL8500만 해당)

중복 전자 부품 및 이중 TCP/IP는 SL3000 및 SL8500 라이브러리의 선택적 기능입니다.

이중 TCP/IP는 대개 별도의 서브넷에 구성된 두 개의 라이브러리 TCP/IP 라이브러리 포트를 제공하여 네트워크 실패로부터 라이브러리/호스트 작업을 보호합니다. 한 서브넷에서 네트워크 중단 또는 실패가 발생하면 라이브러리/호스트 연결이 자동으로 다른 포트로 페일오버됩니다.

중복 전자 부품은 두 개의 완벽히 기능하는 별도의 라이브러리 컨트롤러 카드(활성과 대기)를 제공하여 라이브러리 컨트롤러를 하드웨어 실패로부터 보호합니다. 활성 컨트롤러에 심

각한 오류가 발생하면 라이브러리 및 호스트 작업의 종단을 최소화하면서 대기 카드로 라이브러리 제어권이 넘어갑니다.

이 기능에 대한 자세한 내용은 라이브러리 사용 설명서를 참조하십시오.

4.1.2.1. 이 기능을 지원하도록 STA 연결 구성

이중 TCP/IP와 중복 전자 부품 중 어느 기능이 활성화되었는지, 또는 둘 다 활성화되었는지에 따라 SL3000 또는 SL8500 라이브러리는 1개, 2개 또는 4개의 IP 주소를 가질 수 있습니다. 하지만 STA는 한 번에 최대 2개의 라이브러리 IP 주소에 대해서만 무종단 연결을 유지할 수 있습니다. 따라서 주어진 라이브러리에서 STA가 이중 TCP/IP 또는 중복 전자 부품 중 하나를 지원하도록 구성할 수는 있지만 둘 다를 지원하도록 구성할 수는 없습니다.

라이브러리에 대한 STA 연결을 구성할 때는 항상 기본 라이브러리 IP 주소를 지정해야 합니다. 라이브러리의 기능 구성 및 STA가 지원하게 될 기능에 따라 선택적으로 보조 IP 주소를 지정할 수 있습니다.

주:

두 가지 기능이 모두 있는 라이브러리의 경우, 중복 전자 부품 기능이 연속적인 라이브러리 작업을 유지하는 데 더 중요하므로 Oracle은 STA가 이 기능을 지원하도록 구성할 것을 권장합니다.

STA가 이중 TCP/IP를 지원하도록 구성되면 STA는 포트 페일오버 발생 시 라이브러리와 연결을 유지합니다.

STA가 중복 전자 부품을 지원하도록 구성된 경우 컨트롤러 카드 전환이 발생하면 STA는 보조 라이브러리 IP 주소로 지정된 포트를 통해 라이브러리와 연결을 유지합니다.

이러한 기능에 대한 자세한 내용은 라이브러리 사용 설명서를 참조하십시오.

표 4.2. “STA 연결에 대한 권장되는 라이브러리 IP 주소”는 라이브러리에 대한 STA 연결을 구성할 때 사용할 권장되는 라이브러리 IP 주소를 요약한 것입니다.

표 4.2. STA 연결에 대한 권장되는 라이브러리 IP 주소

활성화된 기능	기본 라이브러리 IP	보조 라이브러리 IP
둘 다 아님	2B 포트	해당 사항 없음
이중 TCP/IP만	2B 포트	2A 포트, 활성 카드
중복 전자 부품만	2B 포트, 활성 카드	2B 포트, 대기 카드
둘 다	2B 포트, 활성 카드	2B 포트, 대기 카드

4.1.2.2. 이 기능에 대한 추가 고려사항

- SL3000 또는 SL8500 라이브러리에서 STA가 이중 TCP/IP를 지원하도록 구성하려면 정책 경로 지정을 사용해야 할 수 있습니다. 자세한 내용은 SL3000 또는 SL8500 호스트 연결 설명서를 참조하십시오. 이중 TCP/IP 구성에 도움이 필요한 경우 Oracle 고객지원센터로 문의하십시오.
- 라이브러리에 중복 전자 부품과 이중 TCP/IP가 모두 있는 경우, STA 서버의 서브넷은 STA에 대해 구성되지 않은 라이브러리 포트의 서브넷과 달라야 합니다([6.1.4절. “라이브](#)

러리에 대한 [SNMP 연결 구성](#) 참조). 그렇지 않으면 라이브러리가 이러한 포트(STA에 알려지지 않음)를 통해 데이터를 보내려고 시도하고 해당 데이터는 STA에 의해 거부됩니다.

- 기본 게이트웨이가 2B 인터페이스인지 확인합니다.

4.1.3. 라이브러리 컴플렉스 ID(SL8500만 해당)

STA가 라이브러리 컴플렉스 데이터를 올바르게 롤업하려면 사이트의 각 라이브러리 컴플렉스에 고유한 컴플렉스 ID가 있어야 합니다. SL8500 라이브러리에서 컴플렉스 ID는 수동으로 설정됩니다. 다른 모든 라이브러리 모델에서 컴플렉스 ID는 자동으로 설정되므로 수동 개입 또는 확인이 필요하지 않습니다.

각 독립형 SL8500은 별도의 컴플렉스로 간주되므로 고유한 컴플렉스 ID가 있어야 합니다. 또한 각 다중 라이브러리 컴플렉스에는 고유한 컴플렉스 ID가 있어야 하고, 컴플렉스 내의 모든 라이브러리는 동일한 ID를 공유해야 합니다. 유효한 컴플렉스 ID 값은 1-127입니다.

[표 4.3. "컴플렉스 ID 지정 예"](#)은 유효한 SL8500 컴플렉스 ID 지정의 몇 가지 예를 보여줍니다.

표 4.3. 컴플렉스 ID 지정 예

컴플렉스 유형	라이브러리	지정된 컴플렉스 ID
다중 라이브러리 컴플렉스	SL8500-1	1
	SL8500-2	1
	SL8500-3	1
독립형 라이브러리	SL8500 - 4	2
	SL8500-5	3

주의:

Oracle SDP(Service Delivery Platform)에서도 라이브러리 데이터 추적을 위해 고유한 컴플렉스 ID를 사용합니다. 사이트에서 SDP를 사용하는 경우 컴플렉스 ID를 변경하기 전에 Oracle 고객센터로 문의하십시오. 컴플렉스 ID를 변경하면 SDP가 실패할 수 있습니다. 대부분의 경우 SDP가 연결되면 컴플렉스 ID는 올바르게 설정됩니다.

자세한 내용은 [4.3.5절. "올바른 라이브러리 컴플렉스 ID 확인\(SL8500만 해당\)"](#)을 참조하십시오.

4.1.4. 드라이브 청소 경고(SL3000 및 SL8500만 해당)

드라이브 청소 경고 플래그는 드라이브 청소가 필요할 때마다 드라이브 경고가 표시되어야 하는지 여부를 나타냅니다. 이 플래그는 라이브러리 레벨에서 설정되므로 라이브러리의 모든 드라이브에 동일한 설정이 적용됩니다.

- 플래그가 "on"으로 설정되면 청소가 필요할 때마다 각 드라이브가 경고 상태를 표시합니다. 이로 인해 STA 모니터에서 라이브러리의 최상위 레벨 상태가 저하될 수도 있습니다.

- 플래그가 "off"로 설정된 경우 각 드라이브의 상태는 청소의 필요성에 의해 영향을 받지 않습니다. 따라서 STA의 라이브러리 최상위 레벨 상태는 저하되지 않습니다.

라이브러리에 많은 수의 드라이브가 있는 경우, 드라이브에 청소가 필요할 때마다 라이브러리 최상위 레벨 조건이 저하되지 않도록 이 플래그를 "off"로 설정할 수 있습니다.

자세한 내용은 4.3.6절. "드라이브 청소 경고 설정(선택 사항, SL3000 및 SL8500만 해당)"을 참조하십시오.

4.1.5. 볼륨 레이블 형식(SL500 및 SL150만 해당)

STA가 라이브러리 교환 데이터를 올바르게 처리하려면 SNMP 데이터의 볼륨 일련 번호(volser)가 제대로 형식 지정되어야 합니다. 매체 volser에는 매체 유형을 나타내는 2자리 문자의 접미어가 포함됩니다. 예를 들어, 카트리지 volser가 ABC123L4인 경우 "L4"는 매체 유형이 LTO4임을 나타냅니다. 올바른 STA 보고를 위해서는 volser 접미어를 제외해야 합니다.

적절한 형식 지정을 위해서는 다음 매개변수를 설정해야 합니다.

- STA가 모니터하는 모든 SL500 라이브러리의 경우 호스트에 대한 레이블 방향은 *left6*으로, STA 모드(*staConfig* 플래그에 의해 제어됨)는 *on*으로 설정되어야 합니다. STA 모드는 SNMP를 통해 STA 서버로 전송되는 volser의 형식에만 영향을 미치고 SL500 라이브러리 자체에 사용되는 형식에는 영향을 미치지 않습니다.
- STA에 의해 모니터되는 모든 SL150 라이브러리의 경우, Volume Label Format은 *Trim last two characters*로 설정되어야 합니다.

주의:

이러한 매개변수가 제대로 설정되지 않을 경우 volser가 올바르게 형식 지정되어 교환 처리가 차단되며 최신 매체 데이터를 가져오려는 불필요한 시도가 발생하고, "Show Removed Media" 환경 설정이 설정될 때마다 되돌릴 수 없는 8자리 문자의 volser 레코드가 Media – Overview 화면에 나타납니다.

자세한 내용은 4.3.7절. "SL500 볼륨 레이블 형식 설정(SL500만 해당)" 및 4.3.8절. "SL150 볼륨 레이블 형식 및 드라이브 요소 주소 지정 모드 설정(SL150만 해당)"을 참조하십시오.

4.1.6. SCSI FastLoad 옵션(SL500만 해당)

SCSI FastLoad가 사용으로 설정되면 카트리지 마운트 트랩이 STA로 제대로 보내지지 않으므로 SL500 라이브러리에서 SCSI FastLoad 옵션은 사용 안함으로 설정되어야 합니다. FastLoad는 기본적으로 사용 안함으로 설정됩니다. 이 옵션의 상태를 확인할 수 없는 경우 Oracle 고객지원센터로 문의하십시오.

4.1.7. 중복된 볼륨 일련 번호

STA 데이터 저장소에서 매체 내역은 볼륨 일련 번호(volser)로 보존됩니다. 특정 매체에 대한 모든 내역은 volser에 연결되므로 Oracle은 중복된 volser를 피할 것을 권장합니다.

volser는 모니터링되는 모든 라이브러리에서 고유해야 합니다. volser가 중복되면 서로 다른 매체에 대한 데이터가 섞이게 됩니다.

중복된 volser에 대한 자세한 내용은 STA 사용 설명서를 참조하십시오.

4.2. 라이브러리 사용자 인터페이스

SL500, SL3000 및 SL8500 라이브러리에는 CLI(명령줄 인터페이스) 및 그래픽 사용자 인터페이스인 SL Console(StorageTek Library Console)이 있습니다. SL150 라이브러리는 브라우저 기반 사용자 인터페이스만 사용합니다. 이 장의 절차는 이러한 인터페이스를 사용하여 수행됩니다.

4.2.1. 라이브러리 CLI 사용법 팁

대부분 CLI 명령의 경우, 구문은 SL500, SL3000 및 SL8500 라이브러리 모델에서 동일합니다. 구문이 라이브러리 모델에 따라 달라지는 일부 명령의 경우 예가 제공됩니다. 대부분의 CLI 예에서는 SL500 라이브러리를 사용합니다. SL3000 또는 SL8500 라이브러리를 구성하는 경우, 각 명령에서 반환되는 세부 정보는 표시된 것과 약간 다를 수 있습니다. 다음은 라이브러리 CLI 사용에 대한 몇 가지 팁입니다.

- PuTTY와 같은 터미널 에뮬레이터를 사용하여 라이브러리 CLI에 대한 SSH(보안 셸) 연결을 설정합니다.
- 오류 문제를 해결해야 하는 경우를 대비하여 작업을 검토할 수 있도록 로깅을 사용으로 설정합니다.
- 일부 펌웨어 버전에서는 6시간 후 CLI 시간 초과가 발생합니다.
- CLI 명령에 대한 도움말을 표시하려면 *help*와 명령 이름을 입력합니다(예: *help snmp*).
- SL500 라이브러리 명령은 대소문자를 구분합니다. SL3000 및 SL8500 명령은 대소문자를 구분하지 않습니다.
- 입력 오류를 피하기 위해 먼저 텍스트 파일에 명령을 입력한 다음 복사하여 CLI에 붙여 넣을 수 있습니다. CLI 명령에 대한 도움말을 보려면 *help snmp*를 입력하십시오.
- 다음 CLI 기능을 사용하면 키보드 입력을 줄일 수 있습니다.
 - 자동 명령 완성을 사용하려면 **Tab** 키를 누릅니다.
 - 명령 내역을 스크롤하려면 **위쪽 화살표** 및 **아래쪽 화살표** 키를 누릅니다. 이전에 입력한 명령을 수정한 다음 **Enter**를 눌러 실행할 수 있습니다.
 - **Enter**를 눌러 실행하기 전에 명령을 수정하려면 **왼쪽 화살표** 및 **오른쪽 화살표** 키를 사용하여 커서를 오류가 발생한 위치로 이동한 후 수정 사항을 입력합니다. 새 문자는 커서 위치에 삽입됩니다. 문자를 삭제하려면 **백스페이스** 키를 사용하십시오.

4.2.2. 라이브러리 구성 스크립트(선택 사항)

STA는 라이브러리에 대한 구성 프로세스를 완료하는 데 도움이 되는 라이브러리 구성 스크립트를 제공합니다. 이 스크립트는 라이브러리 구성 설정에 대해 묻는 메시지를 표시한 후 사용자가 입력하는 값에 따라 전체 명령을 표시합니다. 사용자는 이 명령을 복사하여 라이브러리 CLI에 붙여 넣을 수 있습니다.

주:

스크립트를 시작하기 전에 이 장에 나와 있는 라이브러리 구성 단계를 검토하여 이해하는 것이 좋습니다.

스크립트를 시작하려면 STA 서버에서 터미널 세션을 열고 다음 명령을 실행합니다.

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

여기서 `Oracle_storage_home`은 STA 및 이와 연관된 Oracle 소프트웨어가 설치된 디렉토리입니다. 자세한 내용은 3.1절. “STA 설치 프로그램에서 사용하는 사용자, 그룹 및 위치”를 참조하십시오.

스크립트에 대한 추가 정보 및 사용법 예를 보려면 다음 명령을 실행하십시오.

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

4.3. 라이브러리 기능 구성 작업

표 4.4. “STA에 대한 라이브러리 구성 작업”를 사용하여 사용자 사이트의 라이브러리 모델에 적용되는 작업을 확인하십시오. STA가 모니터링할 각 라이브러리에 대해 해당 작업을 수행해야 합니다.

표 4.4. STA에 대한 라이브러리 구성 작업

작업	SL150	SL500	SL3000	SL8500
4.3.1절. “라이브러리에 로그인”	예	예	예	예
4.3.2절. “라이브러리 펌웨어 버전 확인”	예	예	예	예
4.3.3절. “드라이브 컨트롤러 카드 버전 확인(SL3000 및 SL8500만 해당)”	–	–	예	예
4.3.4절. “라이브러리에서 ADI를 사용으로 설정(SL150을 제외한 모든 라이브러리)”	–	예	예	예
4.3.5절. “올바른 라이브러리 컴플렉스 ID 확인(SL8500만 해당)”	–	–	–	예
4.3.6절. “드라이브 청소 경고 설정(선택 사항, SL3000 및 SL8500만 해당)”	–	–	예	예
4.3.7절. “SL500 볼륨 레이블 형식 설정(SL500만 해당)”	–	예	–	–
4.3.8절. “SL150 볼륨 레이블 형식 및 드라이브 요소 주소 지정 모드 설정(SL150만 해당)”	예	–	–	–

주:

SL500, SL3000 및 SL8500 라이브러리의 경우 많은 작업에서 CLI 또는 SL Console 중에서 사용할 인터페이스를 선택할 수 있습니다. SL150 라이브러리의 경우 브라우저 기반 사용자 인터페이스만 사용해야 합니다.

4.3.1. 라이브러리에 로그인

라이브러리 CLI 사용(SL150을 제외한 모든 라이브러리)

1. IP 주소 또는 DNS 별칭을 사용하여 라이브러리에 대한 SSH 연결을 설정합니다.
2. `admin` 사용자 이름과 암호를 사용하여 CLI에 로그인합니다.

SL Console 사용(SL150을 제외한 모든 라이브러리)

1. SL Console 응용 프로그램을 시작합니다.
2. **About** 버튼을 눌러 현재 SL Console 버전을 표시하고 라이브러리 펌웨어 최소 요구 사항을 충족하는지 확인합니다.
3. **Close**를 눌러 Login 화면으로 돌아갑니다.
4. *admin* 사용자 이름, 암호 및 라이브러리 IP 주소 또는 DNS 별칭을 사용하여 로그인합니다.

중복 전자 부품 기능이 있는 SL3000 및 SL8500 라이브러리의 경우, 활성 컨트롤러에만 로그인할 수 있습니다.

SL150 사용자 인터페이스 사용

1. SL150 라이브러리의 호스트 이름 또는 IP 주소로 이동합니다.
2. 사용자 ID와 암호를 사용하여 로그인합니다. 사용자 ID에는 관리자의 역할이 있어야 합니다.

4.3.2. 라이브러리 펌웨어 버전 확인

이 절차를 사용하여 라이브러리 펌웨어가 STA 요구 사항 설명서에 나와 있는 최소 요구 사항 이상인지 확인하십시오. 그렇지 않은 경우 Oracle 고객지원센터에 펌웨어 업그레이드에 대한 서비스 요청을 제출하십시오.

SL8500 라이브러리의 경우, 펌웨어 업그레이드 후 네트워크 연결 설정을 다시 입력하거나 업데이트해야 할 수 있으므로 Oracle 고객지원센터에서는 펌웨어 업그레이드를 수행하기 전에 이러한 설정을 기록해 두어야 합니다.

라이브러리 CLI 사용(SL150을 제외한 모든 라이브러리, FRS 4.x 미만의 SL3000 라이브러리에는 적용되지 않음)

1. 다음 명령을 실행합니다.

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

주:

화면에 *SYNTAX ERROR!!*가 표시되는 경우 라이브러리 펌웨어가 낮은 레벨입니다. Oracle 고객지원센터로 문의하여 펌웨어를 업그레이드하십시오.

SL Console 사용(SL150을 제외한 모든 라이브러리)

1. **Tools** 메뉴에서 **System Detail**을 선택합니다.
2. 탐색 트리에서 **Library**를 선택합니다.

3. **Properties** 탭을 선택한 다음 **Library Controller** 탭을 선택합니다.

Code Version 섹션 아래에 펌웨어 버전이 표시됩니다.

SL150 사용자 인터페이스 사용

1. 탐색 트리에서 **Firmware**를 선택합니다.

Library Firmware 섹션 아래에 펌웨어 버전이 표시됩니다. 또는 상태 표시줄에 있는 **About** 버튼을 눌러 펌웨어 버전을 확인할 수도 있습니다.

4.3.3. 드라이브 컨트롤러 카드 버전 확인(SL3000 및 SL8500만 해당)

SL3000 및 SL8500 라이브러리가 다양한 드라이브 데이터를 STA로 보내려면 라이브러리에 하이 메모리 드라이브 컨트롤러(HBT) 카드가 포함되어 있어야 합니다. 최신 장치에는 하이 메모리 카드가 포함되어 있으므로 주로 2006년 중반 이전에 출시된 이전 라이브러리에서 문제가 있을 수 있습니다. 펌웨어 레벨 요구 사항에 대한 자세한 내용은 STA 요구 사항 설명서를 참조하십시오.

이 절차를 수행하여 하이 메모리 HBT 카드가 라이브러리에 설치되었는지 확인합니다. 라이브러리에 하이 메모리 HBT 카드가 없으면 Oracle 고객지원센터에 해당 카드 설치에 대한 서비스 요청을 제출하십시오.

이 절차는 SL Console을 사용하여 수행됩니다. SL8500 FRS 8.x 및 SL3000 FRS 4.x의 경우, CLI `config print` 명령을 사용하여 HBT 카드 정보를 표시할 수도 있습니다.

이 절차는 SL Console을 사용하여 수행됩니다.

1. **Tools** 메뉴에서 **System Detail**을 선택합니다.
2. 탐색 트리에서 **Library**를 선택합니다.
3. **Properties** 탭을 선택한 다음 **Drive Controller** 탭을 선택합니다.

화면에 활성 드라이브 컨트롤러(HBT) 카드에 대한 세부 정보가 표시됩니다.

4. High Memory HBT가 `true`인지 확인합니다.
5. 중복 전자 부품 기능이 있는 SL3000(FRS 4.x) 또는 SL8500(FRS 8.x) 라이브러리인 경우 Redundant Electronics 폴더를 확장한 다음 각 HBT 카드(hbta, hbta)를 선택합니다. 둘 다 High Memory HBT에 대해 `True`로 나타나야 합니다.

주:

활성 및 대기 HBT 카드가 모두 설치되고 통신 중이며, 둘 다 하이 메모리가 있어야 합니다.

4.3.4. 라이브러리에서 **ADI**를 사용으로 설정(SL150을 제외한 모든 라이브러리)

라이브러리에 LTO 드라이브가 포함되어 있는 경우 STA가 다양한 드라이브 데이터를 받을 수 있도록 드라이브와 라이브러리 모두에서 ADI를 사용으로 설정해야 합니다. 이 절차를 사

용하여 ADI 드라이브 인터페이스가 라이브러리에서 사용으로 설정되었는지 확인합니다. 자세한 내용은 [4.1.1절. "LTO 드라이브에 대한 ADI 인터페이스"](#)를 참조하십시오.

이 절차는 라이브러리 CLI를 사용하여 수행됩니다.

SL3000 또는 SL8500 라이브러리의 경우

1. ADI 인터페이스의 상태를 표시합니다.

```
drive adiEnable print
```

2. "Attributes Adi Status"가 *true*인 경우 이 작업을 끝내도 됩니다. *false*인 경우 다음 단계를 진행합니다.
3. ADI 인터페이스를 사용으로 설정합니다.

```
drive adiEnable on
```

4. 라이브러리를 재부트하여 변경 사항을 활성화합니다.

SL500 라이브러리의 경우

1. ADI 인터페이스의 상태를 표시합니다.

```
enableADI print
```

2. "enableADI set to"가 *on*인 경우 이 작업을 끝내도 됩니다. *off*로 설정된 경우 다음 단계를 진행합니다.
3. ADI 인터페이스를 사용으로 설정합니다.

```
enableADI on
```

4. 라이브러리를 재부트하여 변경 사항을 활성화합니다.

4.3.5. 올바른 라이브러리 콤플렉스 ID 확인(SL8500만 해당)

STA가 라이브러리 콤플렉스 데이터를 올바르게 롤업하려면 사이트의 각 라이브러리 콤플렉스에 고유한 콤플렉스 ID가 있어야 합니다. 이 절차를 사용하여 각 SL8500 라이브러리에 대한 올바른 라이브러리 콤플렉스 ID를 확인합니다. 자세한 내용은 [4.1.3절. "라이브러리 콤플렉스 ID\(SL8500만 해당\)"](#)를 참조하십시오.

이 절차는 라이브러리 CLI를 사용하여 수행됩니다.

1. STA가 모니터할 각 SL8500 라이브러리에 대해 다음과 같이 현재 지정된 콤플렉스 ID를 표시합니다.

```
SL8500> config complexId print
```

```
...
```

```
Complex Id 3
```

```
...
```

2. 각 독립형 라이브러리 및 각 라이브러리 컴플렉스에 고유한 컴플렉스 ID가 있고, 각 라이브러리 컴플렉스의 모든 라이브러리가 동일한 컴플렉스 ID를 공유하는지 확인합니다.

독립형 라이브러리의 컴플렉스 ID를 변경해야 하는 경우 이 절차를 계속합니다.

주의:

라이브러리 컴플렉스에서 라이브러리의 컴플렉스 ID를 변경해야 하는 경우 Oracle 고객지원센터로 문의하십시오. 이 절차를 계속하지 마십시오.

3. 라이브러리를 오프라인으로 전환한 다음 모든 트랜잭션이 완료될 때까지 기다립니다.
4. 독립형 라이브러리의 컴플렉스 ID를 변경합니다. *complex_ID*는 1–127 사이의 숫자입니다.

```
config complexId set complex_ID
```

예 4.1. 독립형 SL8500 컴플렉스 ID 변경

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

```
...
```

```
Complex Id 5
```

```
Success true
```

```
Done
```

```
...
```

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

주:

이 명령을 실행하면 모든 TCP/IP 연결이 종료됩니다. 라이브러리에 다시 로그인해야 할 수 있습니다.

4.3.6. 드라이브 청소 경고 설정(선택 사항, SL3000 및 SL8500만 해당)

다음 선택적 절차를 사용하여 라이브러리에서 드라이브 청소 경고 플래그의 현재 설정을 확인하고 필요한 경우 변경하십시오. 자세한 내용은 4.1.4절. “드라이브 청소 경고(SL3000 및 SL8500만 해당)”를 참조하십시오.

이 절차는 라이브러리 CLI를 사용하여 수행됩니다.

1. 드라이브 청소 경고 플래그의 현재 설정을 표시합니다.

```
SL3000> cleaning drivewarning get
```

```
...
```

```
Object Drive Cleaning Warning true
```

```
...
```

2. 플래그를 *false*(off)로 설정하려는 경우 다음 명령을 사용합니다.

```
cleaning driveWarning set off
```

4.3.7. SL500 볼륨 레이블 형식 설정(SL500만 해당)

이 절차를 사용하여 STA로 전송되는 SNMP 데이터에서 볼륨 일련 번호(volser)의 형식이 올바르게 지정되었는지 확인하십시오. 자세한 내용은 [4.1.5절. "볼륨 레이블 형식\(SL500 및 SL150만 해당\)"](#)을 참조하십시오.

이 절차는 SL500 CLI를 사용하여 수행됩니다.

주:

Oracle은 이러한 매개변수를 변경하기 전에 라이브러리에 대한 모든 작업을 중지할 것을 권장합니다. 이러한 매개변수를 변경한 후 테이프 응용 프로그램 및/또는 호스트에 구성 변경이 필요할 수 있습니다.

1. *orientlabel* 플래그의 현재 설정을 표시합니다.

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

2. *host* 플래그는 *left6*으로 설정되어야 합니다. 이렇게 하려면 다음 명령을 사용하십시오.

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

3. 설정을 다시 표시하여 올바르게 업데이트되었는지 확인합니다.

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

4. *staConfig* 플래그의 현재 설정을 표시합니다.

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

5. *staConfig* 플래그는 *on*으로 설정되어야 합니다. 이렇게 하려면 다음 명령을 사용하십시오.

```
SL500> staConfig on
```

6. 설정을 다시 표시하여 올바르게 업데이트되었는지 확인합니다.

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

4.3.8. SL150 볼륨 레이블 형식 및 드라이브 요소 주소 지정 모드 설정 (SL150만 해당)

이 절차를 사용하여 STA로 전송되는 SNMP 데이터에서 볼륨 일련 번호(volser)의 형식이 올바르게 지정되었는지 확인하십시오.

또한 SL150 펌웨어 2.xx 이상의 경우 이 절차를 사용하여 빈 드라이브 베이가 STA로 전송되는 데이터에 포함되도록 드라이브 요소 주소 지정 모드를 설정할 수 있습니다.

자세한 내용은 4.1.5절. “볼륨 레이블 형식(SL500 및 SL150만 해당)”을 참조하십시오.

주:

Oracle은 이러한 매개변수를 변경하기 전에 라이브러리에 대한 모든 작업을 중지할 것을 권장합니다. 이러한 매개변수를 변경한 후 테이프 응용 프로그램 및 호스트에 구성 변경이 필요할 수 있습니다.

이 절차는 SL150 브라우저 기반 인터페이스를 사용하여 수행됩니다.

1. 탐색 트리에서 **Configuration**을 선택합니다.
2. **Configure** 버튼을 선택합니다.
3. Configuration Wizard 창에서 **Configure Library Settings** 확인란을 선택한 후 **Next**를 누릅니다.
4. 다음 매개변수를 알맞게 설정합니다.
 - 드라이브 요소 주소 지정 모드: **Address All Drive Slots(권장)**
 - 라이브러리 볼륨 레이블 형식: **Trim last two characters(기본값)**

주:

드라이브 요소 주소 지정 모드를 변경한 후 STA에서 SNMP를 구성하기 전에 적어도 10분을 기다려야 합니다.

5. **Next**를 누릅니다.
6. Summary of Configuration Changes 화면에서 **Accept all changes** 확인란을 선택한 다음 **Apply**를 누릅니다.
7. Apply Configuration Changes 화면에서 **Set the Library back Online after applying the changes** 확인란을 선택한 다음 **OK**를 누릅니다.
8. **All configuration changes have been applied successfully**가 표시되면 **Close**를 누릅니다.

라이브러리에서 SNMP 구성

STA가 사이트에서 라이브러리를 모니터하려면 라이브러리와 STA 서버에서 몇 가지 구성 작업을 수행해야 합니다. 이 장에서는 라이브러리에서 수행되는 작업에 대해 설명합니다. [6 장. STA의 라이브러리 연결 구성](#)으로 진행하기 전에 이 장의 작업을 완료해야 합니다.

이 장은 다음과 같은 절로 구성됩니다.

- [STA에 대한 라이브러리 SNMP 구성 이해](#)
- [라이브러리 SNMP 구성 작업](#)

StorageTek 라이브러리의 SNMP 구현에 대한 일반적인 내용은 *StorageTek Modular Libraries SNMP Reference Guide*를 참조하십시오.

5.1. STA에 대한 라이브러리 SNMP 구성 이해

STA와 모니터되는 라이브러리 사이의 통신은 SNMP(Simple Network Management Protocol)를 통해 수행됩니다. 라이브러리는 SNMP 트랩 및 정보를 통해 데이터를 STA로 보내고, STA는 SNMP get 함수를 통해 라이브러리 구성 데이터를 검색합니다. SNMP 용어로 STA는 클라이언트 에이전트이고 각 라이브러리는 서버 에이전트입니다.

SNMP v3은 STA와 라이브러리 간 SNMP 통신에 권장되는 프로토콜입니다. SNMP v3의 인증, 암호화, 메시지 무결성 기능을 통해 라이브러리 데이터를 전송할 수 있는 보안 메커니즘을 제공합니다. SNMP v3은 STA 매체 검증 기능에도 필요합니다. (STA 매체 검증은 지원되는 라이브러리에 대해서만 사용할 수 있습니다. 자세한 내용은 STA 요구 사항 설명서를 참조하십시오.)

이 장에서는 권장되는 SNMP v3 구성에 대해 설명합니다. 하지만 사이트 요구 사항에 따라 하나 이상의 라이브러리에 대해 SNMP v2c를 사용하도록 선택할 수 있습니다. SNMP v2c 구성 지침은 [부록 F. SNMP v2c 모드 구성](#)을 참조하십시오.

주:

SNMP 트랩 및 get 함수에는 SNMP v3 프로토콜이 사용되지만 라이브러리와 STA 간 초기 통신 핸드셰이킹은 항상 SNMP v2c 프로토콜을 통해 수행됩니다.

5.1.1. 라이브러리에서 SNMP v3 프로토콜 구성

각 라이브러리에서 라이브러리를 SNMP v3 사용자로 정의하고 STA 서버를 SNMP v3 트랩 수신자로 정의하여 STA와 각 라이브러리 사이의 SNMP v3 통신을 설정합니다. 또한 권

한 부여 및 프라이버시 메커니즘과 암호를 지정해야 합니다. STA의 경우, 권한 부여 방식은 항상 SHA(Secure Hash Algorithm)이고, 프라이버시 방식은 항상 DES(Data Encryption Standard)입니다.

5.1.1.1. 고유한 SNMP v3 사용자

STA는 하나의 SNMP v3 사용자만 지원합니다. 단일 STA 인스턴스가 모니터링하는 모든 라이브러리에 동일한 사용자를 정의해야 합니다. 사용할 값을 기록하는 데 사용할 워크시트는 [부록 C. 설치 및 업그레이드 워크시트](#)를 참조하십시오.

주:

라이브러리에 이미 하나 이상의 SNMP v3 사용자가 있는 경우 이중 하나를 STA 통신에 사용할 수 있지만 Oracle은 이 용도를 위해 고유한 SNMP v3 사용자를 새로 설정할 것을 강력히 권장합니다.

다음은 SNMP v3 사용자를 정의하기 위해 사용자가 제공해야 하는 값입니다.

SNMP v3 사용자 이름

STA 서버는 이 사용자가 보내는 트랩을 수신합니다. 이 이름은 트랩 수신자를 만들 때 사용되는 SNMP v3 수신자 이름이기도 합니다. 모든 라이브러리에서 동일해야 합니다.

SNMP v3 권한 부여 암호

SNMP v3 사용자에게 지정하는 권한 부여 암호입니다.

길이는 8자 이상이어야 하며 콤마, 세미콜론 또는 등호가 포함될 수 없습니다.

SNMP v3 프라이버시 암호화 암호

SNMP v3 사용자에게 지정하는 프라이버시 암호입니다.

길이는 8자 이상이어야 하며 콤마, 세미콜론 또는 등호가 포함될 수 없습니다.

SNMP v2c 사용자 커뮤니티

SNMP v2c 사용자 커뮤니티 문자열이며, 일반적으로 *public*으로 설정됩니다. 이 문자열은 SNMP v3 프로토콜을 사용할 때도 라이브러리와 STA 서버 사이의 초기 핸드셰이크에 필요합니다.

영숫자(a-z, A-Z, 0-9)만 포함할 수 있습니다. 특수 문자는 허용되지 않습니다.

SNMP v2c 트랩 커뮤니티

라이브러리와 통신에 SNMP v2c가 사용되는 경우에만 사용되는 SNMP v2c 트랩 커뮤니티 이름입니다. SNMP v3을 사용하는 경우 기본값인 *public*으로 설정된 상태로 두십시오.

영숫자(a-z, A-Z, 0-9)만 포함할 수 있습니다. 특수 문자는 허용되지 않습니다.

5.1.1.2. SNMP 엔진 ID

SNMP v3 프로토콜에서는 각 SNMP 장치에 전역으로 고유한 엔진 ID가 있어야 하므로 STA 서버와 라이브러리는 각각 자체 엔진 ID를 보유합니다. SL8500 라이브러리 컴플렉스의 경우, 컴플렉스의 각 라이브러리가 자체 SNMP 에이전트를 가지고 있으므로 각각 고유한 엔진 ID도 가지고 있습니다. 엔진 ID에는 최대 31자의 16진수 문자가 포함됩니다.

SNMP 트랩에서는 송신자의 엔진 ID를 사용하므로 STA를 SNMP v3 트랩 수신자로 정의할 때 라이브러리 엔진 ID를 지정해야 합니다.

5.2. 라이브러리 SNMP 구성 작업

표 5.1. “STA에 대한 라이브러리 구성 작업”은 올바른 SNMP 데이터를 STA로 보내도록 라이브러리를 구성하는 프로세스를 요약하여 보여 줍니다. STA가 모니터할 각 라이브러리에 대해, 나열된 순서대로 작업을 수행해야 합니다.

표 5.1. STA에 대한 라이브러리 구성 작업

작업	SL150	SL500	SL3000	SL8500
5.2.1절. “라이브러리 IP 주소 검색”	예	예	예	예
5.2.2절. “라이브러리에서 SNMP 사용으로 설정”	예	예	예	예
5.2.3절. “SNMP v2c 사용자 확인”	예	예	예	예
5.2.4절. “SNMP v3 사용자 만들기”	예	예	예	예
5.2.5절. “라이브러리 SNMP 엔진 ID 검색(SL150을 제외한 모든 라이브러리)”	–	예	예	예
5.2.6절. “STA SNMP v3 트랩 수신자 만들기”	예	예	예	예

주:

이 절차에서는 STA와 라이브러리 간 통신에 권장되는 SNMP v3 프로토콜을 사용한다고 가정합니다. 자세한 내용은 5.1절. “STA에 대한 라이브러리 SNMP 구성 이해”를 참조하십시오.

주:

SL500, SL3000 및 SL8500 라이브러리의 경우 일부 작업에서 CLI 또는 SL Console 중에서 사용할 인터페이스를 선택할 수 있습니다. SL150 라이브러리의 경우 항상 브라우저 기반 사용자 인터페이스를 사용해야 합니다.

5.2.1. 라이브러리 IP 주소 검색

이 절차를 사용하여 라이브러리와 연결을 구성하는 데 사용할 라이브러리 IP 주소를 검색하고 기록하십시오.

SL3000 또는 SL8500 라이브러리의 경우, 중복 전자 부품 또는 이중 TCP/IP 중 하나를 지원하거나 둘 다 지원하지 않는 방법을 선택합니다. 자세한 내용은 4.1.2절. “이중 TCP/IP 및 중복 전자 부품(SL3000 및 SL8500만 해당)”을 참조하십시오.

이 절차는 SL Console 또는 SL150 브라우저 기반 인터페이스를 사용하여 수행됩니다.

SL500 IP 주소

1. **Tools** 메뉴에서 **System Detail**을 선택합니다.
2. 탐색 트리에서 **Library**를 선택합니다.
3. **Properties** 탭을 선택한 다음 **General** 탭을 선택합니다.

Library Interface TCP/IP 섹션 아래에 라이브러리 IP 주소가 나열됩니다.

4. 라이브러리 IP 주소를 기본 라이브러리 IP 주소로 기록합니다. (이 주소는 1B 포트에 해당합니다.)

SL3000 또는 SL8500 IP 주소 — 중복 전자 부품 지원

- a. **Tools** 메뉴에서 **System Detail**을 선택합니다.
- b. 탐색 트리에서 **Redundant Electronics** 폴더를 선택합니다.

이 폴더가 나열되지 않은 경우 중복 전자 부품 기능을 라이브러리에서 사용할 수 없습니다.

- c. Device State 필드에서 한 라이브러리 컨트롤러가 *Duplex: software ready, switch possible*(활성 카드)을 표시하고, 다른 라이브러리 컨트롤러가 *Standby: software ready*(대기 카드)를 표시하는지 확인합니다.

이러한 상태는 컨트롤러 카드가 정상적으로 작동 중임을 나타냅니다. 이러한 상태를 볼 수 없는 경우 Oracle 고객지원센터로 문의하십시오.

- d. **Redundant Electronics** 폴더를 확장한 다음 활성 컨트롤러 카드를 선택합니다.
- e. 2B 포트의 IP 주소를 기록합니다.
- f. 대체(대기) 컨트롤러 카드에 대해 d단계 및 e단계를 반복합니다.

SL3000 또는 SL8500 IP 주소 — 이중 TCP/IP 지원

- a. **Tools** 메뉴에서 **System Detail**을 선택합니다.
- b. 탐색 트리에서 **Library**를 선택합니다.
- c. **Properties** 탭을 선택한 다음 **General** 탭을 선택합니다.

Host Interface TCP/IP 2B 및 Host Interface TCP/IP 2A 섹션 아래에 IP 주소 정보가 표시됩니다.

주:

라이브러리에 중복 전자 부품 기능도 포함되어 있는 경우 표시된 IP 주소는 활성 컨트롤러 카드 전용입니다.

- d. 기본 IP 주소(2B 섹션) 및 보조 IP 주소(2A 섹션)를 기록합니다.

SL3000 또는 SL8500 IP 주소—이중 TCP/IP와 중복 전자 부품을 둘 다 지원하지 않음

- a. **Tools** 메뉴에서 **System Detail**을 선택합니다.
- b. 탐색 트리에서 **Library**를 선택합니다.
- c. **Properties** 탭을 선택한 다음 **General** 탭을 선택합니다.

Host Interface TCP/IP 2B 섹션 아래에 IP 주소 정보가 표시됩니다. 2A 섹션에는 IP 주소 정보가 없습니다.

- d. IP 주소를 기본 라이브러리 IP 주소로 기록합니다.

SL150 IP 주소

1. 탐색 트리에서 **Configuration**을 선택합니다.

Settings, Network를 차례로 선택합니다. **Network Port 1 Settings** 섹션에 라이브러리 IP 주소가 표시됩니다. (Network Port 2 Settings 섹션은 서비스용으로 예약되어 있습니다.)

주:

Configure IPxx 필드 값은 *Static*이어야 합니다. 그렇지 않은 경우 **Configure** 버튼을 누른 다음 **Configure Network Settings**를 선택하여 정적 IP 주소를 지정하십시오.

5.2.2. 라이브러리에서 SNMP 사용으로 설정

이 절차를 사용하여 라이브러리 공용 포트에서 SNMP를 사용으로 설정합니다.

라이브러리 CLI 사용

1. 라이브러리 모델에 따라 다음 명령 중 하나를 실행합니다.
 - SL3000 및 SL8500 라이브러리의 경우, 포트 2B에서 SNMP를 사용으로 설정합니다. 라이브러리에 이중 TCP/IP 기능이 포함된 경우 이 명령은 포트 2A에서도 SNMP를 사용으로 설정합니다.

```
snmp enable port2b
```

- SL500 라이브러리의 경우, 포트 1B에서 SNMP를 사용으로 설정합니다.

```
snmp enable port1B
```

SL Console 사용(SL500만 해당)

1. **Tools** 메뉴에서 **System Detail**을 선택합니다.
2. 탐색 트리에서 **Library**를 선택합니다.
3. **SNMP** 탭을 선택한 다음 **Port Control** 탭을 선택합니다.
4. Port Control 섹션을 다음과 같이 입력합니다.

*Port: Public (1B)*을 선택합니다.

*Command: Enable*을 선택합니다.

5. **Apply**를 누릅니다.

SL150 사용자 인터페이스 사용

1. 탐색 트리에서 **SNMP**를 선택합니다.
2. SNMP가 disabled로 표시된 경우 **Enable SNMP**를 선택합니다.
3. 확인 창에서 **OK**를 누릅니다.

5.2.3. SNMP v2c 사용자 확인

SNMP v2c 사용자는 라이브러리와 STA 서버 사이의 초기 핸드셰이크에 필요합니다. 또한 STA 통신을 위해 SNMP v2c를 사용하려는 경우에도 필요합니다. 자세한 내용은 [5.1절. "STA에 대한 라이브러리 SNMP 구성 이해"](#)를 참조하십시오.

다음 구성 요구 사항을 확인합니다.

- 라이브러리에는 하나의 SNMP v2c 사용자만 있어야 합니다.
- SNMP v2c 커뮤니티 문자열은 영숫자(a-z, A-Z, 0-9)만 포함할 수 있습니다. 특수 문자는 허용되지 않습니다.
- 기존 SNMP v2c 사용자는 일반적으로 *public* 커뮤니티로 설정되지만, 다른 커뮤니티 이름으로 정의할 수도 있습니다.
- Oracle 고객지원센터와 상의 없이 기존 SNMP v2c *public* 사용자를 제거해서는 안됩니다. 경우에 따라 SNMP v2c *public* 사용자는 Oracle SDP(Service Delivery Platform)에 필요합니다.

라이브러리 CLI 사용(SL150을 제외한 모든 라이브러리)

1. SNMP v2c 사용자가 존재하는지 확인합니다.

```
snmp listUsers
```

2. 다음 예와 같이 SNMP v2c 사용자가 이미 정의된 경우 이 작업을 끝내도 됩니다. 그렇지 않은 경우 다음 단계를 진행합니다.

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

3. SNMP v2c 사용자를 추가합니다.

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

여기서 *community_name*은 *public* 또는 다른 이름입니다. 예를 들면 다음과 같습니다.

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

4. SNMP 사용자를 다시 나열하여 SNMP v2c 사용자가 올바르게 추가되었는지 확인합니다.

```
snmp listUsers
```

SL Console 사용(SL500만 해당)

1. **Tools** 메뉴에서 **System Detail**을 선택합니다.
2. 탐색 트리에서 **Library**를 선택합니다.
3. **SNMP** 탭을 선택한 다음 **Add Users** 탭을 선택합니다.
4. SNMP v2c 사용자가 Users 섹션에 존재하는 경우 이 작업을 끝내도 됩니다. 그렇지 않은 경우 다음 단계를 진행합니다.
5. SNMP v2c 사용자를 추가하려면 **Add Users** 탭을 다음과 같이 입력합니다.
 - *Version: v2c*를 선택합니다.
 - *Community: 커뮤니티 문자열(예: public)*을 지정합니다.
6. **Apply**를 누릅니다.

기본적으로 SL150은 정의된 SNMP v2c 사용자 없이 출고됩니다. STA 통신을 위해 SNMP v2c를 사용하려는 경우 다음과 같이 SNMP v2c 사용자를 만드십시오.

SL150 사용자 인터페이스 사용

1. 탐색 트리에서 **SNMP**를 선택합니다.
2. SNMP Users 섹션(또는 탭)에서 **Add SNMP User**를 선택합니다.
3. Add SNMP User 화면에서 다음과 같이 정보를 입력합니다.

*Version: v2c*를 선택합니다.

*Community Name: 커뮤니티 문자열(예: public)*을 지정합니다.
4. **OK**를 누릅니다.

5.2.4. SNMP v3 사용자 만들기

모든 SNMP 트랩 및 MIB(Management Information Base) 데이터는 SNMP v3 사용자를 통해 STA 서버로 보내집니다. 사용자 이름과 암호는 SNMP v3 트랩 수신자를 정의할 때 사용되므로 지정하는 사용자 이름과 암호를 메모해 두십시오.

다음 구성 요구 사항을 확인합니다.

- 권한 부여 방식은 *SHA*(Secure Hash Algorithm)이고, 프라이버시 방식은 *DES*(Data Encryption Standard)이어야 합니다.
- 단일 STA 인스턴스에서 모니터되는 모든 라이브러리는 동일한 SNMP v3 사용자 이름을 가져야 합니다. 이 목적에 맞는 고유한 사용자를 새로 만들어야 합니다.
- 권한 부여 및 프라이버시 암호의 길이는 8자 이상이어야 하며 콤마, 세미콜론 또는 등호가 포함될 수 없습니다.

라이브러리 CLI 사용(SL150을 제외한 모든 라이브러리)

1. 다음과 같이 SNMP v3 사용자를 만듭니다.

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

여기서 각 항목은 다음과 같습니다.

- *name*은 SNMP v3 사용자 이름입니다.
- *auth_password* 및 *priv_password*는 권한 부여 암호 및 프라이버시 암호입니다.

주:

SL3000 및 SL8500 라이브러리의 경우, 모든 변수를 작은 따옴표로 묶으십시오(예 5.1. “SL3000 또는 SL8500에서 SNMP v3 사용자 만들기”).

예 5.1. SL3000 또는 SL8500에서 SNMP v3 사용자 만들기

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

예 5.2. SL500에서 SNMP v3 사용자 만들기

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

2. SNMP 사용자를 나열하여 SNMP v3 사용자가 올바르게 추가되었는지 확인합니다.

```
snmp listUsers
```

SL Console 사용(SL500 라이브러리만 해당)

1. **Tools** 메뉴에서 **System Detail**을 선택합니다.
2. 탐색 트리에서 **Library**를 선택합니다.
3. **SNMP** 탭을 선택한 다음 **Add Users** 탭을 선택합니다.
4. **Add Users** 탭을 다음과 같이 입력합니다.
 - *Version*: v3을 선택합니다.
 - *UserName*: SNMP v3 사용자의 이름입니다.
 - *Auth*: SHA를 선택합니다.
 - *AuthPass*: 권한 부여 암호를 지정합니다.
 - *Priv*: DES를 선택합니다.
 - *PrivPass*: 프라이버시 암호를 지정합니다.
5. **Apply**를 누릅니다.

SL150 사용자 인터페이스 사용

1. 탐색 트리에서 **SNMP**를 선택합니다.

2. SNMP Users 섹션에서 **Add SNMP User**를 선택합니다.
3. Version에 대해 v3을 선택하고 다음과 같이 정보를 입력합니다.
 - *User Name*: SNMP v3 사용자의 이름입니다.
 - *Authentication Protocol*: SHA를 선택합니다.
 - *Authentication Passphrase*: 권한 부여 암호를 지정합니다.
 - *Privacy Protocol*: DES를 선택합니다.
 - *Privacy Passphrase*: 프라이버시 암호를 지정합니다.
4. **OK**를 누릅니다.

5.2.5. 라이브러리 SNMP 엔진 ID 검색(SL150을 제외한 모든 라이브러리)

이 절차를 사용하여 라이브러리의 SNMP 엔진 ID(예: 0x81031f88804b7e542f49701753)를 표시합니다.

이 절차는 라이브러리 CLI를 사용하여 수행됩니다.

1. 라이브러리 모델에 따라 다음 명령 중 하나를 실행합니다.
 - SL3000 및 SL8500 라이브러리:

```
snmp engineId print
```

- SL500 라이브러리:

```
snmp engineId
```

2. 남은 SNMP 구성 작업에서 사용할 수 있도록 엔진 ID를 텍스트 파일로 저장합니다.

5.2.6. STA SNMP v3 트랩 수신자 만들기

이 절차를 사용하여 STA 서버를 SNMP 트랩의 권한이 부여된 수신자로 정의하고 라이브러리에서 보낼 트랩을 정의하십시오.

다음 구성 요구 사항을 확인합니다.

- 중복 레코드를 피하기 위해 STA 서버를 여러 인스턴스에서 트랩 수신자로 정의하지 마십시오. 예를 들어, STA 서버에 대해 SNMP v3 및 SNMP v2c 트랩 수신자 정의를 둘 다 만들지는 마십시오.
- 트랩 레벨 13(테스트 트랩) 및 14(상태 트랩)는 STA 2.0.x의 새로운 기능입니다. 트랩 레벨 4는 이전 라이브러리 펌웨어 버전에서 지원되지 않을 수 있지만, 트랩 수신자를 만들 때는 항상 지정할 수 있습니다.

라이브러리 CLI 사용(SL150을 제외한 모든 라이브러리)

1. SNMP v3 트랩 수신자를 만듭니다. 트랩 레벨은 콤마로 구분하십시오.

```
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
```

여기서 각 항목은 다음과 같습니다.

- *STA_server_IP*는 STA 서버의 IP 주소입니다.
- *recipient_name*은 5.2.4절. “SNMP v3 사용자 만들기” [77]에서 만든 SNMP 사용자 이름입니다.
- *auth_password* 및 *priv_password*는 5.2.4절. “SNMP v3 사용자 만들기” [77]에서 만든 권한 부여 및 프라이버시 암호입니다.
- *library_engineID*는 5.2.5절. “라이브러리 SNMP 엔진 ID 검색(SL150을 제외한 모든 라이브러리)” [79]에서 표시한 라이브러리 엔진 ID(0x 접두어 포함)입니다.

주:

SL3000 및 SL8500 라이브러리의 경우, *recipient_name*, *auth_password* 및 *priv_password*를 작은 따옴표로 묶으십시오(예 5.3. “SL3000 또는 SL8500에서 SNMP v3 트랩 수신자 만들기”).

예 5.3. SL3000 또는 SL8500에서 SNMP v3 트랩 수신자 만들기

```
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
0x00abcdef00000000000000000000
```

예 5.4. SL500에서 SNMP v3 트랩 수신자 만들기

```
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
0x00abcdef00000000000000000000
```

2. 트랩 수신자를 나열하고 수신자가 올바르게 추가되었는지 확인합니다.

```
snmp listTrapRecipients
```

SL Console 사용(SL500 라이브러리만 해당)

1. **Tools** 메뉴에서 **System Detail**을 선택합니다.
2. 탐색 트리에서 **Library**를 선택합니다.
3. **SNMP** 탭을 선택한 다음 **Add Trap Recipients** 탭을 선택합니다.
4. Trap Recipients 화면 필드를 다음과 같이 입력합니다.
 - *Host*: STA 서버의 IP 주소입니다.

- *TrapLevel*—라이브러리에서 STA로 보내야 하는 콤마로 구분된 트랩 레벨 목록입니다(1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100).
- *Version*—v3을 선택합니다.
- *TrapUserName*: 5.2.4절. “SNMP v3 사용자 만들기” [77]에서 만든 SNMP 사용자 이름입니다.
- *Auth*—SHA를 선택합니다.
- *AuthPass*—5.2.4절. “SNMP v3 사용자 만들기” [77]에서 만든 권한 부여 암호입니다.
- *Priv*—DES를 선택합니다.
- *PrivPass*—5.2.4절. “SNMP v3 사용자 만들기” [77]에서 만든 프라이버시 암호입니다.
- *EngineID*—5.2.5절. “라이브러리 SNMP 엔진 ID 검색(SL150을 제외한 모든 라이브러리)” [79]에서 표시한 라이브러리 엔진 ID입니다. 0x 접두어는 입력하지 마십시오.

5. **Apply**를 누릅니다.

SL150 사용자 인터페이스 사용

1. 탐색 트리에서 **SNMP**를 선택합니다.
2. SNMP Trap Recipients 섹션에서 **Add Trap Recipient**를 선택합니다.
3. 필드를 다음과 같이 입력합니다.
 - *Host Address*—STA 서버의 IP 주소입니다.
 - *Trap Level*—라이브러리에서 STA로 보내야 하는 콤마로 구분된 트랩 레벨 목록입니다(1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100).
 - *Version*—v3을 선택합니다.
 - *Trap User Name*—5.2.4절. “SNMP v3 사용자 만들기” [77]에서 만든 SNMP 사용자 이름입니다.
 - *Authentication Protocol*—SHA를 선택합니다.
 - *Authentication Passphrase*—5.2.4절. “SNMP v3 사용자 만들기” [77]에서 만든 권한 부여 암호입니다.
 - *Privacy Protocol*—DES를 선택합니다.
 - *Privacy Passphrase*—5.2.4절. “SNMP v3 사용자 만들기” [77]에서 만든 프라이버시 암호입니다.
 - *Engine ID*—이 필드는 자동으로 제공됩니다. 값을 수정하지 마십시오.
4. **OK**를 누릅니다.

STA의 라이브러리 연결 구성

STA가 사이트에서 라이브러리를 모니터하려면 라이브러리와 STA 서버에서 몇 가지 구성 작업을 수행해야 합니다. 이 장에서는 STA 서버에서 수행되는 작업에 대해 설명합니다.

이 장은 다음과 같은 절로 구성됩니다.

- [STA 구성 작업](#)

6.1. STA 구성 작업

나열된 순서로 절차를 수행해야 합니다. 이 프로세스를 완료하면 STA가 라이브러리 모니터링 및 분석 수행을 시작할 수 있습니다.

- [6.1.1절. “STA에 로그인 ”](#)
- [6.1.2절. “라이브러리와 SNMP 통신 확인”](#)
- [6.1.3절. “STA에 대한 SNMP 클라이언트 설정 구성”](#)
- [6.1.4절. “라이브러리에 대한 SNMP 연결 구성”](#)
- [6.1.5절. “라이브러리 SNMP 연결 테스트”](#)
- [6.1.6절. “수동 데이터 수집 수행”](#)

6.1.1. STA에 로그인

이 절차를 사용하여 STA에 로그인하여 이 절의 다른 절차를 수행합니다. 전체 지침은 *STA* 사용 설명서를 참조하십시오.

1. 컴퓨터에서 지원되는 웹 브라우저를 시작하고 STA 응용 프로그램의 URL을 입력합니다.

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

여기서 각 항목은 다음과 같습니다.

- *host_name*은 STA 서버의 호스트 이름입니다.
- *port_number*는 설치 중 지정한 STA 포트 번호입니다. 기본 HTTP 포트는 7021이고, 기본 HTTPS 포트는 7022입니다.
- *STA*는 대문자여야 합니다.

예를 들면 다음과 같습니다.

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

2. Login 화면에서 STA 관리자의 사용자 이름 및 암호를 입력합니다.

6.1.2. 라이브러리와 SNMP 통신 확인

이 절차를 사용하여 STA 서버와 라이브러리 사이의 SNMP 연결이 올바른지 확인합니다.

이 절차에서는 STA 서버와 라이브러리 사이의 모든 네트워크 노드에서 UDP 포트 161 및 162가 사용으로 설정되었는지 확인합니다. SNMP v3 트랩 수신자가 올바르게 지정되었는지 검증할 수는 없습니다.

모니터되는 각 라이브러리에 대해 이 절차를 수행합니다. 중복 전자 부품 또는 이중 TCP/IP 중 하나를 지원하는 SL3000 또는 SL8500 라이브러리의 경우, 라이브러리에 대해 이 절차를 기본 라이브러리 IP 주소에 한 번, 보조 IP 주소에 한 번, 이렇게 두 번 수행합니다.

주:

이 절차는 STA 서버의 시스템 명령줄에서 수행됩니다.

1. STA 서버에서 터미널 창을 열고 시스템 루트 사용자로 로그인합니다.
2. SNMP v3 연결을 테스트합니다. 지정한 값은 라이브러리의 해당 값과 일치해야 합니다.

```
# snmpget -v3 -u SNMP_user -a SHA -A auth_pwd -x DES -X priv_pwd -1
authPriv library_IP_addr 1.3.6.1.4.1.1211.1.15.3.1.0
```

여기서 각 항목은 다음과 같습니다.

- v3은 SNMP v3을 나타냅니다.
- SNMP_user는 SNMP v3 사용자 이름입니다.
- SHA는 인증 프로토콜을 나타냅니다.
- auth_pwd는 권한 부여 암호입니다.
- DES는 프라이버시 프로토콜을 나타냅니다.
- priv_pwd는 프라이버시 암호입니다.
- authPriv는 프라이버시가 명령에서 수행됨을 의미합니다.
- library_IP_addr은 라이브러리의 공용 포트의 IP 주소입니다.
 - SL150 라이브러리의 경우, 네트워크 포트 1입니다.
 - SL500 라이브러리의 경우, 포트 1B입니다.
 - SL3000 및 SL8500 라이브러리의 경우, 이중 TCP/IP 또는 중복 전자 부품이 라이브러리에서 활성화되었는지 여부에 따라 테스트할 여러 포트가 있을 수 있습니다. 여러 포트가 있을 경우 각 IP 주소에 대해 이 명령을 실행합니다.
- 1.3.6.1.4.1.1211.1.15.3.1.0은 라이브러리에 대한 SNMP 객체 식별자(OID)이며, 모든 라이브러리 모델에 대해 동일합니다.

명령 출력에 라이브러리 모델이 표시되는 경우 테스트는 성공입니다. 다음은 몇 가지 명령 예입니다.

예 6.1. 성공한 snmpget 명령

```
# 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"
```

예 6.2. 실패한 snmpget 명령—네트워크 시간 초과

```
# 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.
```

예 6.3. 실패한 snmpget 명령—잘못된 암호

```
# 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 연결을 테스트합니다.

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

여기서 각 항목은 다음과 같습니다.

- *v2c*는 SNMP v2c를 나타냅니다.
 - *public*은 커뮤니티 문자열을 나타냅니다.
 - *authPriv*는 프라이버시가 명령에서 수행됨을 의미합니다.
 - *library_IP_addr*은 라이브러리의 공용 포트의 IP 주소입니다.
4. 두 SNMP 연결 테스트가 모두 성공하면 이 절차를 끝낼 수 있습니다. 테스트 중 하나라도 실패하면 다음 단계로 진행하여 필요에 따라 의심스러운 네트워크 문제를 해결하십시오.
 5. STA 서버에서 라이브러리로의 패킷 경로 지정을 확인합니다.

```
# traceroute -I library_IP_addr
```

여기서 각 항목은 다음과 같습니다.

- *-I*(대문자 "I")는 UDP(사용자 데이터그램 프로토콜) 데이터그램 대신 ICMP(Internet Control Message Protocol) 에코 요청 패킷을 사용함을 나타냅니다.
- *library_IP_addr*은 라이브러리의 공용 포트의 IP 주소입니다.

출력은 홉의 수 및 각 홉에 도달하는 데 걸린 왕복 시간을 표시합니다. 왕복 시간(명령 출력의 마지막 라인)은 1초 미만이어야 합니다. 그렇지 않은 경우 네트워크 관리자에게 네트워크의 성능을 확인하십시오.

6. STA 서버와 라이브러리 간에 전송되는 TCP/IP 패킷을 모니터합니다.

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

여기서 각 항목은 다음과 같습니다.

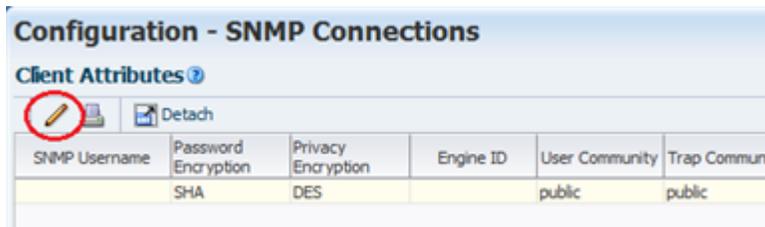
- -v는 상세 정보 표시 출력을 나타냅니다.
- host는 표시된 호스트(이 경우에는 라이브러리)에 대해서만 패킷을 수집함을 나타냅니다.
- library_IP_addr은 라이브러리의 공용 포트의 IP 주소입니다.
- file_name은 출력을 저장할 파일의 이름입니다.

6.1.3. STA에 대한 SNMP 클라이언트 설정 구성

이 절차를 사용하여 STA에 대한 SNMP 클라이언트 설정을 추가 또는 수정합니다. 이 설정은 하나 이상의 라이브러리에서 SNMP 데이터를 수신하도록 STA를 구성합니다.

사이트의 각 STA 인스턴스에 대해 단 한 개씩의 SNMP 클라이언트 항목이 있습니다.

1. **Setup & Administration** 탭에서 **Configuration, SNMP Connections**를 차례로 선택합니다.
2. 다음과 같이 진행합니다.
 - 처음으로 클라이언트 설정을 구성하는 경우 Client Attributes 테이블에서 빈 테이블 행을 선택한 다음 **Edit**를 누릅니다.



- 기존 클라이언트 설정을 수정하려면 Client Attributes 테이블에서 항목을 선택한 다음 **Edit**를 누릅니다.



Define SNMP Client Settings 대화 상자가 표시됩니다. 새 구성인 경우 필드가 비어 있습니다.

3. 다음과 같이 대화 상자를 채웁니다. 지정하는 값은 라이브러리의 해당 값과 일치해야 합니다.

주:

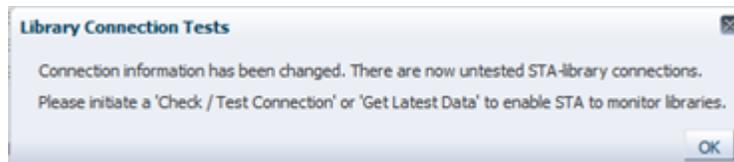
STA가 SNMP v2c 통신을 위해 구성된 라이브러리만 모니터링하더라도 SNMP v3에 해당하는 항목을 포함한 모든 필드를 채워야 합니다. 어떤 필드도 비워 둘 수 없습니다.

- *STA SNMP Connection Username (Auth)*—SNMP v3 사용자 이름을 입력합니다.
- *Enter STA SNMP Connection Password (Auth)*—연결 권한 부여 암호를 입력합니다.
- *Enter Privacy Encryption Password (Privacy)*—프라이버시 암호화 암호를 입력합니다.
- *User Community*—이 필드는 라이브러리와 SNMP 핸드셰이크에 필요하거나, SNMP v2c를 사용하는 경우 라이브러리와 STA 통신에 필요합니다. 라이브러리에 지정된 커뮤니티 이름을 입력합니다. 기본값은 *public*입니다.
- *Trap Community* —라이브러리와 통신에 SNMP v2c가 사용되는 경우에만 사용됩니다. SNMP v3을 사용하는 경우 기본값인 *public*으로 설정된 상태로 두십시오. SNMP v2c를 사용하는 경우 라이브러리에 지정된 트랩 커뮤니티 이름을 입력합니다.



4. **Save**를 누릅니다.

구성 레코드가 업데이트되고 라이브러리와 SNMP 통신 핸드셰이크를 설정 또는 재설정하기 위해 라이브러리 연결 테스트를 수행해야 함을 알리는 메시지 상자가 표시됩니다.



5. **OK**를 눌러 메시지를 없앱니다.

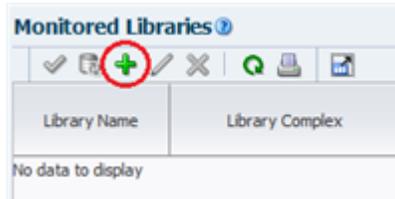
6.1.4. 라이브러리에 대한 SNMP 연결 구성

이 절차를 사용하여 STA가 모니터할 각 라이브러리에 대한 SNMP 연결을 구성하거나 기존 연결을 수정합니다. 기존 연결의 경우 모니터되는 라이브러리에서 SNMP 구성 설정이 하나라도 변경된 경우(예: 라이브러리 IP 주소 변경) 이 절차를 반드시 수행해야 합니다.

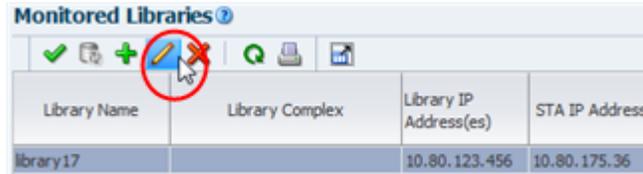
주:

한 번에 여러 라이브러리 연결을 구성하는 경우 라이브러리 중단을 최소화하기 위해 SNMP 연결을 테스트하기 전에 모든 라이브러리에 대해 이 절차를 완료하십시오.

1. **Setup & Administration** 탭에서 **Configuration, SNMP Connections**를 차례로 선택합니다.
2. 다음과 같이 진행합니다.
 - 처음으로 라이브러리에 대한 연결을 구성하는 경우 Monitored Libraries 도구 모음에서 **Add**를 누릅니다.



- 기존 라이브러리 연결을 수정하려면 Monitored Libraries 테이블에서 라이브러리를 선택한 다음 **Edit**를 누릅니다.



Define Library Connection Details 대화 상자가 표시됩니다. 새 라이브러리 연결인 경우 필드는 비어 있습니다.

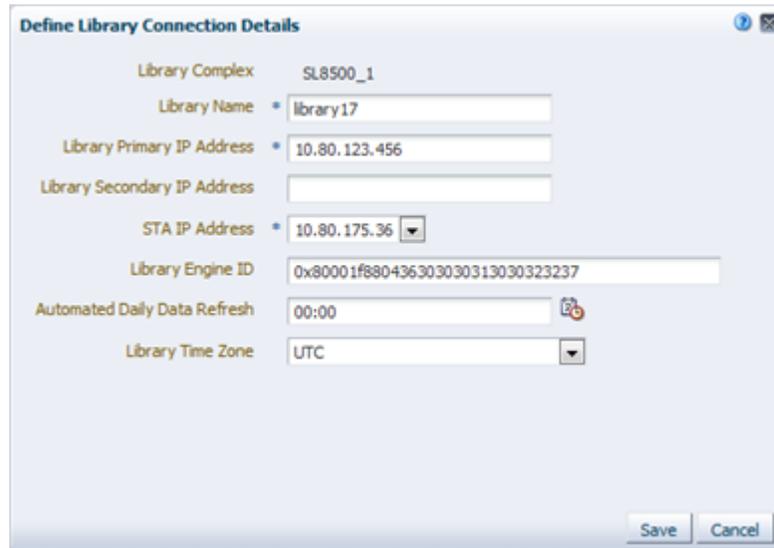
3. 다음과 같이 대화 상자를 채웁니다. 지정한 값은 라이브러리의 해당 값과 일치해야 합니다.
 - *Library Name*—STA 사용자 인터페이스 화면에서 라이브러리를 식별하는 데 사용할 이름을 입력합니다(예: 라이브러리 호스트 이름).
 - *Library Primary IP Address*—라이브러리의 기본 공용 포트의 IP 주소를 입력합니다. 모니터되는 다른 라이브러리의 IP 주소를 지정할 수 없습니다.
 - *Library Secondary IP Address*—이중 TCP/IP 또는 중복 전자 부품을 사용하는 SL3000 및 SL8500 라이브러리에만 적용됩니다. 라이브러리의 보조 공용 포트의 IP 주소를 지정합니다. 모니터되는 다른 라이브러리의 IP 주소를 지정할 수 없습니다. 모든 SL500 및 SL150 라이브러리를 비롯하여 다른 모든 라이브러리에 대해 이 필드를 비워 둡니다.
 - *STA IP Address*—STA 서버의 IP 주소를 선택합니다.

- *Library Engine ID*—이 필드는 변경하지 않습니다. STA와 라이브러리 사이에 초기 연결이 이루어질 때 자동으로 제공되는 라이브러리의 고유한 SNMP 엔진 ID입니다. 새 연결인 경우 비어 있습니다.
- *Automated Daily Data Refresh*—STA가 라이브러리에서 최신 구성 데이터를 수집할 하루 중 시간을 지정합니다. 데이터는 24시간마다 이 시간에 자동으로 수집됩니다. 일반적으로 라이브러리 사용이 많지 않은 시간을 선택해야 합니다. 기본값은 00:00(12:00 am)입니다. 24시간제 형식을 사용합니다.

주의:

이 필드를 비워 둘 경우 예약된 자동 라이브러리 데이터 수집이 사용 안함으로 설정됩니다. 그 결과 STA 라이브러리 구성 데이터가 라이브러리와 동기화되지 않은 상태가 될 수 있습니다.

- *Library Time Zone*—라이브러리의 로컬 시간대를 선택합니다.



4. **Save**를 누릅니다.

구성 레코드가 업데이트되고 라이브러리와 SNMP 통신 핸드셰이크를 설정 또는 재설정하기 위해 라이브러리 연결 테스트를 수행해야 함을 알리는 메시지 상자가 표시됩니다.



5. **OK**를 눌러 메시지를 없앱니다.

기존 라이브러리 연결을 수정한 경우 Monitored Libraries 테이블의 Library Engine ID 필드가 지워져 SNMP 연결이 끊어졌음을 나타냅니다.

6.1.5. 라이브러리 SNMP 연결 테스트

이 절차를 사용하여 STA와 라이브러리 간 SNMP 연결을 테스트하고 통신 핸드셰이크를 설정 또는 재설정합니다. 연결이 끊어지거나 SNMP 트랩이 손실되지 않도록 하기 위해, STA 클라이언트 또는 라이브러리에 대해 SNMP 구성 설정을 추가 또는 변경할 때마다, 모니터링되는 각 라이브러리에 대해 이 절차를 수행해야 합니다.

한 번에 하나의 라이브러리 연결만 테스트할 수 있습니다.

주:

연결 테스트를 수행하면 수신 SNMP 패킷이 일시적으로 손실될 수 있으므로 필요할 때만 이 절차를 수행해야 합니다.

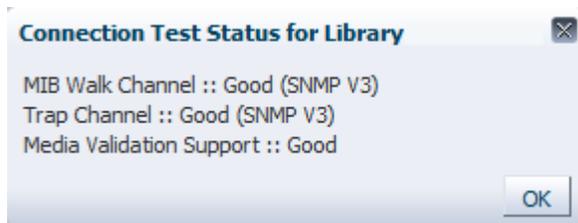
주:

이 절차를 수행하기 전에 라이브러리가 작동하는지 확인하십시오.

1. **Setup & Administration** 탭에서 **Configuration, SNMP Connections**를 차례로 선택합니다.
2. **Monitored Libraries** 테이블에서 라이브러리를 선택한 다음 **Check / Test Connection**을 누릅니다.

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	0x80001f8804313030303030303031	NO RECENT TRAPS	00:00:00	UTC	2014-05
Crimson19	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

MIB Walk Channel, Trap Channel 및 Media Validation Support 테스트 결과를 보여주는 Connection Test Status 메시지 상자가 표시됩니다.



3. **OK**를 눌러 메시지 상자를 닫습니다.

Monitored Libraries 테이블이 테스트 결과로 업데이트됩니다.

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
Crimson19	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

- *Library Complex* 필드가 비어 있는 경우 이 값은 사용자가 수동 데이터 수집을 수행한 후에 제공됩니다.

- *Library Engine ID*는 라이브러리에 대한 고유 SNMP 엔진 ID를 나타냅니다.
- *Last Connection Attempt*는 연결 테스트가 시작된 날짜 및 시간을 나타냅니다.
- *Last Successful Connection*은 테스트가 완료된 날짜 및 시간을 나타냅니다(성공한 경우).
- *Last Connection Status*는 테스트 결과를 나타냅니다. 테스트가 실패한 경우 STA는 *Last Connection Failure Detail* 필드에 정보를 제공합니다. (전체 값을 보려면 열 너비를 늘려야 할 수 있습니다.)

주:

시간 초과로 인해 테스트를 실패하는 경우 라이브러리 작업이 많지 않은 시간에 이 절차를 반복하십시오. 테스트가 완료되면 시간 기록을 비교하여 라이브러리가 현재 정보를 제공하는지 확인할 수 있습니다.

6.1.6. 수동 데이터 수집 수행

이 절차를 수행하여 라이브러리에 대한 수동 데이터 수집을 시작하고 최신 라이브러리 구성 데이터를 가져옵니다. 이 절차가 성공적으로 완료되면 STA가 라이브러리 모니터링 및 데이터에 대한 분석 수행을 시작합니다.

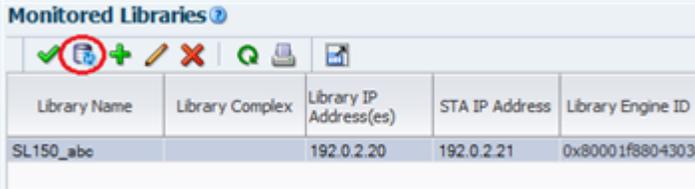
STA는 예약한 시간에 24시간마다 자동으로 데이터 수집을 수행하지만, 사용자는 STA 클라이언트 또는 라이브러리의 SNMP 구성 설정을 추가 또는 변경할 때마다, 모니터링되는 각 라이브러리에 대해 수동 데이터 수집을 수행해야 합니다.

데이터 수집은 라이브러리 크기에 따라 수 분에서 한 시간이 소요될 수 있습니다.

주:

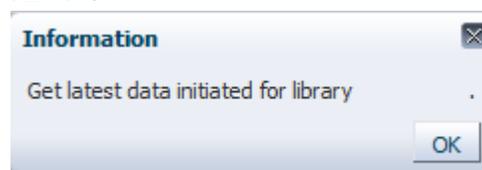
여러 데이터 수집을 동시에 실행할 수는 있지만 데이터 수집 시작은 한 번에 하나씩 해야 합니다. 매번 다른 라이브러리를 선택하여 필요한 만큼 이 절차를 반복하십시오.

1. **Setup & Administration** 탭에서 **Configuration, SNMP Connections**를 차례로 선택합니다.
2. **Monitored Libraries** 테이블에서 라이브러리를 선택한 다음 **Get latest data**를 누릅니다. 한 번에 하나의 라이브러리만 선택할 수 있습니다.



Library Name	Library Complex	Library IP Address(es)	STA IP Address	Library Engine ID
SL150_abc		192.0.2.20	192.0.2.21	0x80001f8804303

확인 메시지 상자가 나타납니다.



3. **OK**를 눌러 메시지 상자를 닫습니다.

데이터 수집이 계속되고 Monitored Libraries 테이블이 해당 결과로 업데이트됩니다.

- *Library Complex*는 라이브러리 컴플렉스 ID를 나타냅니다.
- *Library Engine ID*는 라이브러리에 대한 고유 SNMP 엔진 ID를 나타냅니다.
- *Last Connection Attempt*는 데이터 수집이 시작된 날짜 및 시간을 나타냅니다.
- *Last Successful Connection*은 데이터 수집이 완료된 날짜 및 시간을 나타냅니다(성공한 경우).
- *Last Connection Status*는 다음과 같이 업데이트됩니다.
 - *IN PROGRESS*: 데이터 수집 프로세스가 진행 중입니다.
 - *SUCCESS*: 데이터 수집을 성공했습니다. STA가 라이브러리에서 교환 데이터를 수신하기 시작합니다.
 - *FAILED*: 데이터 수집을 실패했습니다. 가능한 경우 STA는 *Last Connection Failure Detail* 필드에 정보를 제공합니다. (전체 값을 보려면 열 너비를 늘려야 할 수 있습니다.)

주:

상태는 4분마다 업데이트되고, 기본 화면 새로 고침 간격은 480초입니다. 하지만 **Refresh Table** 버튼을 눌러 언제든지 수동으로 테이블을 새로 고칠 수 있습니다.



- *Recent SNMP Trap Communication Status*에 가끔씩 *MISSED HEARTBEAT*가 나타날 수 있습니다. 이것은 정상적인 동작입니다.

STA 서비스 구성

이 절차를 사용하여 STA 백업 서비스 및 STA 리소스 모니터 서비스 유틸리티를 구성합니다.

이 장은 다음과 같은 절로 구성됩니다.

- [STA 서비스 개요](#)
- [STA 서비스 구성 작업](#)

7.1. STA 서비스 개요

- STA 데이터베이스 백업 서비스—STA 백업 서비스는 관리 유틸리티인 *staservadm*을 사용하여 구성합니다. 이 유틸리티에 대한 명령 옵션의 전체 목록을 표시하려면 *staservadm -h*를 입력하십시오. 자세한 내용은 *STA 관리 설명서*를 참조하십시오.
- STA 리소스 모니터 서비스—STA 리소스 모니터 서비스는 관리 유틸리티인 *staresmonadm*을 사용하여 구성합니다. 이 유틸리티에 대한 명령 옵션의 전체 목록을 표시하려면 명령줄에 *staresmonadm -h*를 입력하십시오. 자세한 내용은 *STA 관리 설명서*를 참조하십시오.

이러한 서비스 유틸리티는 */Oracle_storage_home/StorageTek_Tape_Analytics/common/bin* 디렉토리에 있습니다. Oracle 스토리지 홈에 대한 자세한 내용은 [3.1절. “STA 설치 프로그램에서 사용하는 사용자, 그룹 및 위치”](#)를 참조하십시오.

7.2. STA 서비스 구성 작업

일반 작업

- [7.2.1절. “시스템 경로 업데이트\(선택 사항\)”](#)
- [7.2.2절. “STA 서비스 데몬 다시 시작\(선택 사항\)”](#)
- [7.2.3절. “라이브러리 연결 확인”](#)

STA 데이터베이스 백업 구성 작업

- [7.2.4절. “STA 데이터베이스 백업 유틸리티 환경 설정 검토”](#)
- [7.2.5절. “원격 데이터베이스 백업 서버 구성”](#)
- [7.2.6절. “STA 데이터베이스 백업 서비스 구성”](#)

STA 리소스 모니터 구성 작업

- 7.2.7절. “STA 리소스 모니터 유틸리티 환경 설정 검토”
- 7.2.8절. “STA 리소스 모니터 구성”

7.2.1. 시스템 경로 업데이트(선택 사항)

이 절차를 사용하여 STA bin 디렉토리가 시스템 루트 사용자에게 대한 *PATH* 변수에 포함되어 있는지 확인합니다. bin 디렉토리는 STA 서비스 유틸리티, *staservadm* 및 *staresmonadm*을 포함합니다.

- 현재 STA 서버에서 터미널 세션을 열고 시스템 루트 사용자로 로그인합니다.
- 텍스트 편집기를 사용하여 사용자 프로파일을 엽니다. 예를 들면 다음과 같습니다.

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

- STA bin 디렉토리를 *PATH* 정의에 추가합니다. 예를 들어 다음 라인을 파일에 추가합니다.

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

여기서 *Oracle_storage_home*은 STA 설치 중 지정된 Oracle 스토리지 홈 위치입니다.

- 파일을 저장하고 종료합니다.
- 로그아웃 후 시스템 루트 사용자로 다시 로그인합니다.
- PATH* 변수가 올바르게 업데이트되었는지 확인합니다.

```
# 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 서비스 데몬 다시 시작(선택 사항)

이 절차를 사용하여 STA 서비스 데몬인 *staservd*를 다시 시작합니다.

이 절차는 STA 백업 또는 STA 리소스 모니터 서비스의 구성 설정을 변경하고 새로운 설정을 즉시 적용하려는 경우 유용합니다. 이 절차를 사용하지 않을 경우 새로운 설정은 서비스가 일시 정지 간격에서 깨어나고 새로운 설정을 처리하는 즉시 적용됩니다.

1. STA 서비스 데몬을 중지합니다.

```
# STA stop staservd
```

2. STA 서비스 데몬을 시작합니다.

```
# STA start staservd
```

3. 데몬의 상태를 표시하여 실행 중임을 확인합니다.

```
# STA status staservd
```

7.2.3. 라이브러리 연결 확인

서비스 구성을 마쳤으면 모든 구성된 라이브러리가 "Get latest data" 요청을 완료했는지 확인합니다(Last Connection Status가 *SUCCESS*를 나타내고, STA가 라이브러리로부터 교환 데이터를 수신해야 함). 자세한 내용은 STA 사용 설명서를 참조하십시오.

7.2.4. STA 데이터베이스 백업 유틸리티 환경 설정 검토

표 7.1. "STA 백업 서비스 관리 유틸리티(staservadm) 속성"에서 사용 가능한 환경 설정에 대한 설명을 검토하고 원하는 설정을 정의하십시오.

표 7.1. STA 백업 서비스 관리 유틸리티(staservadm) 속성

옵션	속성	설명	기본값	원하는 값
-S, --scp -F, --ftp	File transfer type	STA 서버에서 백업 호스트로 백업 파일을 복사하는 데 사용되는 파일 전송 방식입니다. 옵션은 SCP(권장) 또는 FTP입니다.	SCP	
-T, --time	Full backup dump time	STA가 전체 데이터베이스 백업 덤프를 수행하는 하루 중 시간입니다. 덤프는 24시간마다 대략 이 시간에 자동으로 수행됩니다. 실제 시간은 이 시간 이후 "sleep interval"초 이내입니다. 형식은 hh:mm이며, 24시간제를 사용합니다.	00:00	
-i, --int	Sleep interval	STA 서비스 데몬이 새로운 증분 백업 파일을 확인하기 전 대기 시간(초)입니다.	300	
-s, --server	Backup host name	STA 서버가 백업 파일을 복사하는 서버 호스트의 IPv4/IPv6 주소 또는 정규화된 DNS 호스트 이름입니다.	해당 사항 없음	
-u, --usr	Backup user ID	백업 호스트로 SCP 파일 전송을 수행할 수 있는 권한이 부여된 시스템 사용자 ID입니다.	해당 사항 없음	
-p, --pwd	Backup password	백업 사용자에게 지정된 암호입니다.	해당 사항 없음	
-d, --dir	Backup directory	백업 파일이 복사될 백업 호스트의 디렉토리입니다.	해당 사항 없음	
-U, --dbusr	Database username	mysqldump 명령을 수행할 수 있는 권한이 부여된 데이터베이스 사용자 이름입니다. STA 데이터베이스 DBA 계정 사용자 이름을 지정해야 합니다.	해당 사항 없음	
-P, --dbpwd	Database password	데이터베이스 사용자 이름의 암호입니다.	해당 사항 없음	

7.2.5. 원격 데이터베이스 백업 서버 구성

이 절차를 사용하여 원격 백업 서버(또는 동등 서버)가 STA 데이터베이스 백업 서비스로 생성된 압축 백업 파일을 수신하도록 구성하십시오. Oracle은 원격 백업 서버를 구성할 것을 권장합니다.

필요한 공간은 가변적입니다. 크기는 보존할 복사본 수에 따라 STA 데이터베이스 로컬 백업에 사용되는 크기의 배수여야 합니다. 백업 서버 스토리지는 미러링되거나 스트라이프되어야 합니다.

1. 백업 서버에서 시스템 루트 사용자로 로그인합니다.
2. STA 백업 사용자에게 대한 새로운 그룹을 만듭니다. 예를 들면 다음과 같습니다.

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

이 예에서 그룹 ID는 "stabckgr"이고, 숫자 GID를 지정하기 위해 `-g` 옵션이 사용되었습니다.

3. STA 백업 사용자를 만듭니다. 예를 들면 다음과 같습니다.

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

이 예에서 사용자 ID는 "stabck"이고, 다음 옵션이 사용되었습니다.

- `-c` – 주석입니다.
- `-m` – 사용자에게 대한 홈 디렉토리를 만듭니다.
- `-d` – 홈 디렉토리의 절대 경로입니다.
- `-g` – 지정된 그룹에 사용자를 지정합니다.
- `-s` – 지정된 로그인 셸을 사용자에게 지정합니다.
- `-u` – 지정된 숫자 UID를 사용자에게 지정합니다.

4. STA 백업 사용자에게 암호를 지정합니다. 예를 들면 다음과 같습니다.

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

5. STA 백업이 복사될 디렉토리를 만듭니다. 예를 들면 다음과 같습니다.

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

이 예에서 "STAbackups" 디렉토리가 STA 백업 사용자의 홈 디렉토리에 만들어지고, 필요에 따라 상위 디렉토리를 만들기 위해 `-p` 옵션이 사용되었습니다.

6. 사용자 속성을 표시하여 모든 정보가 올바르게 입력되었는지 확인합니다. 예를 들면 다음과 같습니다.

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

7. 디렉토리에 대한 배타적 소유권 및 액세스 권한을 STA 백업 사용자 및 그룹에 지정합니다. 예를 들면 다음과 같습니다.

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

이 예에서는 속성을 디렉토리 및 해당 파일에 순환적으로 지정하기 위해 `-R` 옵션이 사용되었습니다.

8. 디렉토리를 나열하여 모든 정보가 올바르게 입력되었는지 확인합니다. 예를 들면 다음과 같습니다.

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

7.2.6. STA 데이터베이스 백업 서비스 구성

이 절차를 사용하여 STA 데이터베이스 백업 서비스를 구성합니다. 백업 파일을 복사할 디렉토리를 지정할 수 있습니다. Oracle은 이 디렉토리를 원격 백업 서버에 배치할 것을 권장합니다.

구성 설정은 서비스가 현재 일시 정지 간격에서 깨어나고 새로운 설정을 처리하거나 STA 서비스 데몬을 수동으로 다시 시작(7.2.2절. “STA 서비스 데몬 다시 시작(선택 사항)”)하는 즉시 적용됩니다.

1. STA 서버에서 시스템 루트 사용자로 로그인합니다.
2. `staservadm -q` 명령을 사용하여 현재 STA 백업 서비스 설정을 표시합니다.

이 예는 서비스가 아직 구성되지 않고 이에 따라 백업을 수행하고 있지 않음을 보여줍니다.

```
# ./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. 표 7.1. “STA 백업 서비스 관리 유틸리티(staservadm) 속성”을 참조로 사용하여 *staservadm* 명령으로 속성 값을 설정합니다.

속성은 별도의 명령으로 제출하거나 하나로 결합할 수 있습니다. 예를 들면 다음과 같습니다.

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

유틸리티는 명령에 포함된 각 값을 설정한 다음 모든 현재 설정을 표시합니다. 예를 들면 다음과 같습니다.

```
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/STAbckups]
Database Username    -U [sta_dba]
Database Password    -P [*****]
```

4. 명령 출력을 검토하여 값이 올바르게 설정되었는지 확인합니다.

7.2.7. STA 리소스 모니터 유틸리티 환경 설정 검토

표 7.2. "STA 리소스 모니터(staresmonadm) 속성"에서 옵션 설명을 검토하고 원하는 설정을 정의하십시오. 기본값 "-1"은 속성이 구성되지 않았음을 나타냅니다.

표 7.2. STA 리소스 모니터(staresmonadm) 속성

옵션	속성	설명	기본값	원하는 값
-T, --time	Daily report time	STA가 표준 일간 보고서를 보내는 하루 중 시간입니다. 보고서는 24시간마다 대략 이 시간에 자동으로 보내집니다. 실제 시간은 이 시간 이후 "sleep interval"초 이내입니다. 형식은 hh:mm이며, 24시간제를 사용합니다.	00:00	
-i, interval	Sleep interval	STA 리소스 모니터가 검사 사이에 대기하는 시간(초)입니다.	300	
-n, --nag	Nag mode	상위 워터마크에 도달할 경우 STA가 경보를 보내는 빈도를 나타냅니다. "on"으로 설정되면 시스템이 검사될 때마다 STA가 경고 전자 메일을 보냅니다. "off"로 설정되면 경보가 표준 일간 보고서에 기록되기만 합니다.	Off	
-U, --dbusr	Database username	"information_schema" 테이블 및 MySQL 서버 내부 시스템 전역 변수에 대해 질의를 수행할 수 있는 권한이 부여된 데이터베이스 사용자 이름입니다. STA 데이터베이스 DBA 계정 사용자 이름 또는 STA 데이터베이스 루트 계정 사용자 이름 (root)을 지정해야 합니다.	해당 사항 없음	
-P, --dbpwd	Database password	데이터베이스 사용자 이름에 지정된 암호입니다.	해당 사항 없음	
-t, --tblsphwm	Database tablespace HWM	데이터베이스 테이블스페이스에 대한 상위 워터마크이며, 사용 가능한 최대값의 백분율로 입력됩니다.	-1	
-b, --backvolhwm	Local backup HWM	STA 데이터베이스 로컬 백업 볼륨(/sta_db_backup)에 대한 상위 워터마크이며, 가능한 최대값의 백분율로 입력됩니다.	-1	
-d, --dbvolhwm	Database disk volume HWM	STA 데이터베이스 볼륨(/sta_db/mysql)에 대한 상위 워터마크이며, 사용 가능한 최대값의 백분율로 입력됩니다.	-1	
-l, --logvolhwm	Logging disk volume HWM	STA 데이터베이스 로그(/STA_logs/db)에 대한 상위 워터마크이며, 사용 가능한 최대값의 백분율로 입력됩니다.	-1	
-z, --rootvolhwm	Root volume HWM	루트 볼륨(/)에 대한 상위 워터마크이며, 사용 가능한 최대값의 백분율로 입력됩니다.	-1	
-x, --tmpvolhwm	Tmp volume HWM	임시 디렉토리 볼륨(/tmp)에 대한 상위 워터마크이며, 사용 가능한 최대값의 백분율로 입력됩니다.	-1	
-m, --memhwm	Physical memory (RAM) HWM	총 시스템 메모리(가상 메모리 제외)에 대한 상위 워터마크이며, 사용 가능한 최대값의 백분율로 입력됩니다.	-1	
-f, --from	Email from	표준 일간 보고서 전자 메일의 "From" 필드에 나타나는 이름 또는 전자 메일 주소입니다.	StaResMon@localhost	

옵션	속성	설명	기본값	원하는 값
-r, --recips	Email recipients	수신자 전자 메일 주소이며, 콜론으로 구분된 목록으로 입력됩니다.		해당 사항 없음
-s, --subject	Email subject	표준 일간 보고서 전자 메일의 "Subject" 필드에 나타나는 항목이며, 최대 128자입니다. 공백이 포함된 경우 따옴표를 사용하십시오. 전자 메일을 보낼 때 yyyy-mm-dd hh:mm:ss 형식의 시간 기록이 항목에 추가됩니다.	STA Resource Monitor Report	
-o, --outfile	Output data file	콤마로 구분된(CSV) 출력 데이터 파일의 절대 경로입니다.	/STA_logs/db/staresmon.csv	예를 들면 다음과 같습니다. /var/log/tbi/db/staresmon.csv

7.2.8. STA 리소스 모니터 구성

이 절차를 사용하여 STA 리소스 모니터 서비스를 구성하십시오. 구성 설정은 서비스가 현재 일시 정지 간격에서 깨어나고 새로운 설정을 처리하거나 STA 서비스 데몬을 수동으로 다시 시작(7.2.2절. "STA 서비스 데몬 다시 시작(선택 사항)")하는 즉시 적용됩니다.

1. STA 서버에서 시스템 루트 사용자로 로그인합니다.
2. `staresmonadm -Q` 명령을 사용하여 현재 STA 리소스 모니터 설정을 표시합니다.

이 예는 서비스가 아직 구성되지 않고 이에 따라 검사를 수행하고 있지 않음을 보여줍니다.

```
# ./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. 표 7.2. “STA 리소스 모니터(staresmonadm) 속성”를 참조로 사용하여 *staresmonadm* 명령으로 속성값을 설정합니다.

속성은 별도의 명령으로 제출하거나 하나로 결합할 수 있습니다. 예를 들면 다음과 같습니다.

```
# ./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
```

유틸리티는 명령에 포함된 각 값을 설정한 다음 모든 현재 설정을 표시합니다. 예를 들면 다음과 같습니다.

```
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. 명령 출력을 검토하여 값이 올바르게 설정되었는지 확인합니다.

STA 2.1.0으로 업그레이드

이 장에서는 이전에 릴리스된 모든 STA 버전을 STA 2.1.0으로 업그레이드하는 방법에 대한 지침을 제공합니다. 다음과 같은 절로 구성됩니다.

- [업그레이드 프로세스 개요](#)
- [유효한 STA 2.1.0 업그레이드 경로](#)
- [업그레이드 방식](#)
- [STA 2.1.0에 대한 환경 변경 사항](#)
- [업그레이드 준비 작업](#)
- [업그레이드 작업](#)

처음으로 STA를 설치하는 경우 새로운 기본 설치를 수행해야 합니다. 자세한 내용은 [3장. STA 설치](#)를 참조하십시오.

[부록 C. 설치 및 업그레이드 워크시트](#)에는 업그레이드 작업을 구성하고 설정을 기록하는 데 사용할 수 있는 워크시트가 포함되어 있습니다.

8.1. 업그레이드 프로세스 개요

업그레이드 중 기존 STA 데이터는 현재 STA 버전에서 새로운 버전으로 변환됩니다. 이 변환이 완료되어야 사용자의 STA 데이터베이스를 새 STA 버전에서 유효하게 사용할 수 있습니다. 업그레이드 후 STA는 새로운 STA 스키마 및 분석 규칙에 따라 새 데이터를 처리합니다(과거 데이터는 다시 처리되지 않음).

업그레이드를 시작하기 전에 이 장의 모든 지침을 읽고 전체 프로세스에 충분한 시간을 할당하십시오. 일부 업그레이드 준비 작업에서는 네트워크 관리 등의 영역에서 사이트의 다른 그룹과 협력해야 할 수 있습니다. 가능한 한 짧은 시간에 업그레이드 자체를 완료할 수 있도록 미리 모든 준비 작업을 완료해야 합니다.

업그레이드 프로세스 자체가 시작되면 STA가 실행될 수 없으므로 모니터링되는 라이브러리로 부터 교환 정보가 수신되지 않습니다. 또한 새 STA 버전은 업그레이드의 모든 단계를 완료하고 모니터링되는 각 라이브러리에 대한 SNMP 연결을 테스트할 때까지 라이브러리에서 정보를 수신하지 않습니다.

주:

일부 업그레이드 단계에는 계획 용도로만 제공되는 시간 예측이 포함됩니다. 실제 시간은 CPU 수, CPU 속도, 디스크 속도, 메모리, 사용 가능한 스왑 공간 등의 서버 용량에 따라 달라질 수 있습니다.

8.2. 유효한 STA 2.1.0 업그레이드 경로

릴리스된 다음 STA 버전에서 STA 2.1.0으로 업그레이드할 수 있습니다.

- 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

주:

STA 1.0.x에서 업그레이드하는 경우 STA 2.1.0을 설치하기 전에 새 Linux 버전도 설치해야 합니다. 자세한 내용은 STA 요구 사항 설명서를 참조하십시오.

8.3. 업그레이드 방식

사용자의 목표 및 사용 가능한 리소스에 따라 단일 서버 또는 두 대의 서버를 사용하여 STA 업그레이드를 수행할 수 있습니다. 이 두 방식에서 수행되는 업그레이드 작업은 대략 비슷하지만 작업이 다른 순서로 수행됩니다. 이 두 방식은 다음 절에서 설명합니다.

- [8.3.1절. “단일 서버 업그레이드 방식”](#)
- [8.3.2절. “두 대의 서버 업그레이드 방식”](#)

8.3.1. 단일 서버 업그레이드 방식

단일 서버 방식을 사용하는 경우 STA를 제거한 후에 새 버전을 설치하고 같은 서버에서 데이터베이스를 업그레이드해야 합니다. 이 프로세스를 수행하는 동안 STA는 라이브러리를 모니터하지 않습니다.

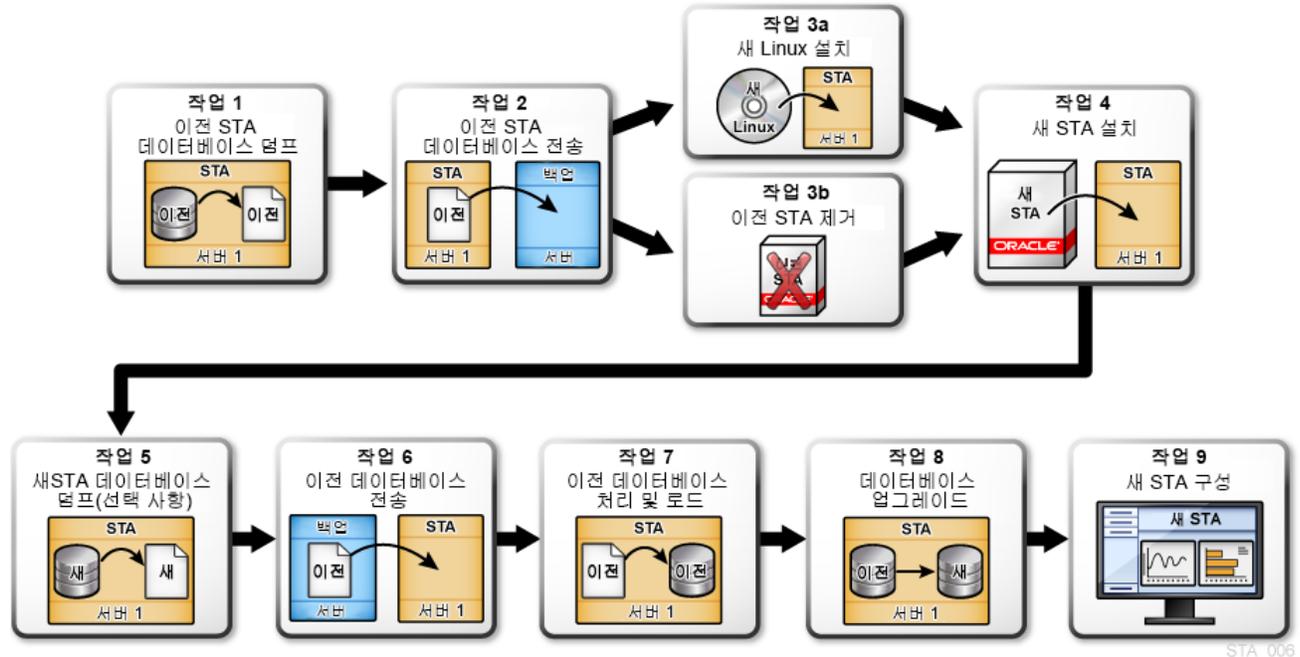
이 방식에서는 업그레이드를 위해 추가로 전용 서버가 필요하지 않다는 이점이 있습니다. STA 2.0.x에서 업그레이드하는 경우 새 Linux 버전을 설치할 필요가 없으므로 이 방식으로 충분합니다.

[그림 8.1. “단일 서버 업그레이드 작업 개요”](#)은 단일 서버 방식을 보여 줍니다. 작업 1~작업 9를 순번대로 수행합니다. 요약하면 다음과 같습니다.

- 현재 데이터베이스를 덤프한 다음 안전하게 보관하기 위해 백업 서버로 전송합니다(작업 1 및 작업 2).
- 현재 STA 버전에 따라 Linux 6.x를 설치하거나(작업 3a) STA 2.0.x를 제거합니다(작업 3b).
- STA 2.1.0을 설치하고 예방 조치로 새 데이터베이스를 덤프합니다(작업 4 및 작업 5).
- 이전 데이터베이스 덤프를 백업 서버에서 전송한 다음 이를 새 STA 버전으로 로드하고 업그레이드합니다(작업 6~작업 8).

- 모니터되는 라이브러리의 연결을 재설정하고 필요한 수동 구성 작업을 수행합니다(작업 9). STA 2.1.0을 설치하기 전에 이전 STA 버전을 제거해야 하기 때문에 일부 사용자 구성 데이터를 수동으로 다시 입력해야 합니다.

그림 8.1. 단일 서버 업그레이드 작업 개요



8.3.2. 두 대의 서버 업그레이드 방식

두 대의 서버 업그레이드 방식에는 두번째 전용 STA 서버가 필요하지만 STA 응용 프로그램 작동 중지 시간이 줄어든다는 이점이 있습니다. 이 방식은 STA 1.0.x에서 업그레이드하는 경우 특히 유용한데, 그 이유는 새 서버에 Linux와 새 STA 버전을 설치하는 동안 이전 STA 버전이 이전 서버에서 라이브러리를 계속 모니터할 수 있기 때문입니다.

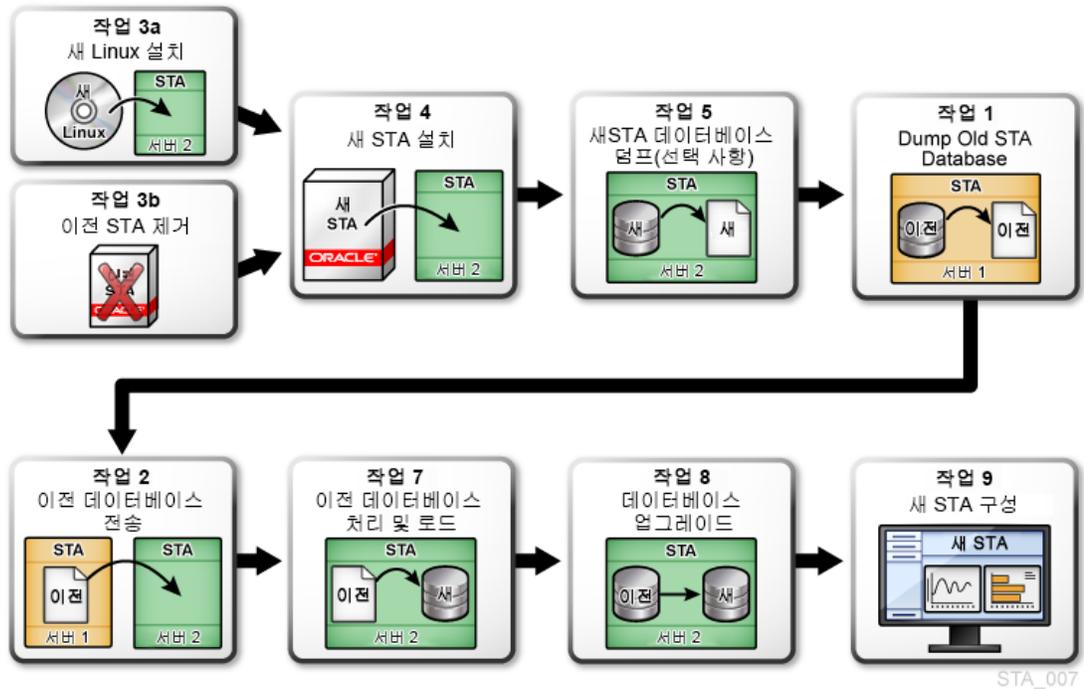
하지만 이 방식에서도 현재 데이터베이스를 새 STA 버전으로 업그레이드하는 동안에는 STA가 라이브러리를 모니터하지 않습니다. 작동 중지 시간의 길이는 현재 데이터베이스의 크기에 따라 다릅니다.

그림 8.2. “두 대의 서버 업그레이드 작업 개요”는 두 서버 방식을 보여 줍니다. 표시된 순서대로 작업을 완료해야 합니다. 작업은 순번대로 수행되지 않으며 작업 6은 생략됩니다. 새 서버에 새 STA 버전을 설치할 때까지 현재 STA 데이터베이스를 덤프하지 않는다는 점을 유의하십시오. 요약하면 다음과 같습니다.

- 두번째 서버가 현재 STA 버전을 실행 중인지 여부에 따라 Linux 6.x를 설치하거나(작업 3a) STA 2.0.x를 제거합니다(작업 3b).
- 새 서버에 STA 2.1.0을 설치하고 예방 조치로 새 데이터베이스를 덤프합니다(작업 4 및 작업 5).
- 이전 서버에서 현재 데이터베이스를 덤프하여 새 서버로 전송합니다(작업 1 및 작업 2).

- 현재 데이터베이스를 새 STA 버전으로 로드하고 업그레이드합니다(작업 7 및 작업 8).
- 모니터되는 라이브러리의 연결을 재설정하고 필요한 수동 구성 작업을 수행합니다(작업 9).

그림 8.2. 두 대의 서버 업그레이드 작업 개요



8.4. STA 2.1.0에 대한 환경 변경 사항

다음은 STA 2.1.0으로의 업그레이드를 계획할 때 고려해야 하는 환경 변경 사항을 요약한 것입니다.

8.4.1. Linux 버전

STA 2.1.0에는 Linux 6.3 이상이 필요합니다(자세한 내용은 STA 요구 사항 설명서 참조). 현재 STA 버전에 따라 STA 업그레이드 프로세스의 일환으로 새 버전의 Linux를 설치해야 할 수 있습니다.

- STA 1.0.x에서 업그레이드하는 경우 STA 2.1.0을 설치하기 전에 Linux 6.3 이상을 설치해야 합니다. Linux는 Linux 5.x에서 Linux 6.x로의 in-place 업그레이드를 지원하지 않습니다. 따라서 STA 서버에 Linux 6.x를 새로 설치해야 합니다.
- STA 2.0.x에서 업그레이드하는 경우 이미 Linux 6.3 이상을 실행하고 있습니다. 하지만 STA 2.1.0을 설치하기 전에 현재 STA 버전을 제거해야 합니다. 필요한 Linux RPM 패키지를 설치 또는 업데이트해야 할 수도 있습니다. 업그레이드 준비의 일환으로, 필요한 모든 RPM 패키지 레벨이 설치되었는지 확인합니다. 최종 확인으로 STA 설치 프로그램은 누락된 패키지가 있는 경우 사용자에게 이를 알립니다.

8.4.2. 기본 WebLogic 포트 번호

STA 2.1.0에서는 기본 WebLogic 관리 콘솔 포트 번호가 변경되었습니다. 현재 이전 기본 포트 번호를 사용하고 있다면 새 기본값으로 변경해야 합니다. 새 기본 포트 번호와 이전 기본 포트 번호는 다음과 같습니다.

- STA 2.1.0의 새 기본값—7019(HTTP) 및 7020(HTTPS)
- 이전 기본값(STA 1.0.x 및 STA 2.0.x)—7001(HTTP) 및 7002(HTTPS)

주:

WebLogic 관리 콘솔 포트는 외부 포트입니다. 네트워크 관리자는 STA 서버와 WebLogic 관리 인터페이스에 액세스하는 클라이언트 사이의 통신을 열기 위해 방화벽 및 라우터를 구성해야 할 수 있습니다.

8.4.3. STA 2.0.x 이상에 필요한 포트

주:

이 내용은 STA 2.0.x에서 변경되었으므로 STA 1.0.x에서 업그레이드하는 경우에만 관련이 있습니다.

STA 2.0.x에서 StaUi 및 StaEngine 관리 서버에 대해 STA 포트가 추가되었습니다. STA 2.0.x 및 STA 2.1.0에 대한 기본 STA 관리 서버 포트 번호는 다음과 같습니다.

- StaUi—7021(HTTP) 및 7022(HTTPS)
- StaEngine—7023(HTTP) 및 7024(HTTPS)
- StaAdapter—7025(HTTP) 및 7026(HTTPS)

주:

StaUi 포트는 외부 포트입니다. 네트워크 관리자는 STA 서버와 STA 사용자 인터페이스에 액세스하는 클라이언트 사이의 통신을 열기 위해 방화벽 및 라우터를 구성해야 할 수 있습니다.

8.4.4. 사용자 이름 및 암호 요구 사항

STA 2.1.0에서는 STA 및 MySQL에 대한 사용자 이름 및 암호 요구 사항이 변경되었습니다. 이러한 요구 사항을 사용자 사이트의 내부 요구 사항과 조정해야 합니다.

사용자 이름 요구 사항은 다음과 같습니다.

- 길이가 1~16자여야 합니다.
- 모든 사용자 이름은 고유해야 합니다.

암호 요구 사항은 다음과 같습니다.

- 길이가 8~31자여야 합니다.
- 최소한 숫자 1개와 대문자 1개를 포함해야 합니다.

- 공백을 포함할 수 없습니다.
- 다음 특수 문자를 포함할 수 없습니다.

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

8.5. 업그레이드 준비 작업

STA 업그레이드를 시작하기 전에 다음 작업을 수행합니다. 이 작업의 대부분은 선택 사항이며 표 8.1. "업그레이드 준비 작업을 수행하는 경우에 대한 지침"은 각 작업을 수행하는 경우에 대한 지침을 제공합니다.

표 8.1. 업그레이드 준비 작업을 수행하는 경우에 대한 지침

작업	수행하는 경우
8.5.1절. "사이트가 업그레이드할 준비가 되었는지 확인"	모든 업그레이드
8.5.2절. "기존 로그 저장(선택 사항)"	현재 STA 버전의 서비스 로그를 보존하려는 경우
8.5.3절. "현재 STA 사용자 및 구성 설정 기록(선택 사항)"	STA 사용자 이름 및 구성 설정을 보존하려는 경우
8.5.4절. "STA- 로 시작하는 사용자 정의 템플릿 이름 바꾸기(선택 사항)"	이름이 "STA-"로 시작하는 사용자 정의 템플릿이 있는 경우
8.5.5절. "현재 사용자 정의 템플릿 설정 기록(선택 사항)"	기존 사용자 정의 템플릿의 소유권 및 가시성 설정을 보존하려는 경우
8.5.6절. "실행 보고서 정책 설정 기록(선택 사항)"	기존 실행 보고서 정책의 소유권 설정을 보존하려는 경우

8.5.1. 사이트가 업그레이드할 준비가 되었는지 확인

이 절차를 사용하여 업그레이드 요구 사항을 검토하고 사이트가 준비되었는지 확인합니다.

8.5.1.1. 업그레이드 필요 조건 확인

이 절차에 따라 사용자 환경이 모든 STA 2.1.0 필요 조건을 충족하는지 확인합니다.

1. 현재 STA 버전을 표시합니다. 일부 업그레이드 작업은 STA 1.0.x에서 업그레이드하는지 STA 2.0.x에서 업그레이드하는지에 따라 달라집니다.
 - a. STA 관리자의 사용자 이름을 사용하여 STA에 로그인합니다.
 - b. 상태 표시줄에서 **About**를 누릅니다.
 - c. 현재 릴리스된 STA 버전을 실행 중인지 확인합니다. 자세한 내용은 8.2절. "유효한 STA 2.1.0 업그레이드 경로"를 참조하십시오.
2. 단일 서버 업그레이드 방식을 사용할지 두 대의 서버 업그레이드 방식을 사용할지 선택합니다. 자세한 내용은 8.1절. "업그레이드 프로세스 개요"를 참조하십시오.
3. 사용자 사이트 및 대상 서버가 STA 2.1.0 요구 사항을 충족하는지 확인합니다. 자세한 내용은 STA 요구 사항 설명서를 참조하십시오.
4. 대상 STA 서버의 `/tmp` 파일 시스템에 업그레이드를 위한 충분한 공간이 있는지 확인합니다. `/tmp`의 크기는 압축되지 않은 기존 STA 데이터베이스 크기 이상이어야 합니다.

최소 4GB가 필요하며 큰 데이터베이스의 경우 Oracle은 `/tmp`의 크기를 최소 32GB로 늘릴 것을 권장합니다.

`/tmp`의 크기를 늘리기로 결정하는 경우 업그레이드 스크립트를 실행하기 직전에 해당 크기를 늘릴 수 있습니다. 자세한 내용은 8.6.9절. “[작업 8: 이전 데이터베이스 업그레이드](#)”를 참조하십시오.

5. 업그레이드 경로와 관련된 환경 변경 사항을 검토하고 필요한 경우 계획 또는 환경을 조정하십시오. 자세한 내용은 8.4절. “[STA 2.1.0에 대한 환경 변경 사항](#)”을 참조하십시오.
6. STA 2.0.x에서 업그레이드하는 경우 필요한 모든 RPM 패키지가 STA 서버에 설치되어 있는지 확인합니다. 자세한 내용은 2.3.6절. “[필수 Linux 패키지 설치](#)”를 참조하십시오. 최종 점검으로 STA 설치 프로그램은 누락된 패키지가 있는 경우 사용자에게 이를 알립니다.

8.5.1.2. 현재 STA 작업 확인

이 절차를 사용하여 STA 환경이 정상적으로 작동 중인지 확인합니다.

1. 다음 단계를 사용하여 현재 STA 버전이 모니터되는 각 라이브러리와 최근에 통신을 성공했는지 확인합니다.
 - a. STA 관리자인 사용자로 STA에 로그인합니다.
 - b. **Setup & Administration** 탭에서 **SNMP Connections**를 선택합니다.
 - c. Monitored Libraries 테이블에서 다음 값을 확인합니다.
 - Recent SNMP Trap Communication Status—GOOD
 - Last Connection Status—SUCCESS
2. 다음 단계를 사용하여 STA가 모든 라이브러리에서 교환을 처리 중인지 확인합니다.
 - a. **Tape System Activity** 탭에서 **Exchanges – Overview**를 선택합니다.
 - b. **Filter** 아이콘을 선택하고 Exchange End (No. Days) Less Than 1로 필터링합니다.
 - c. Table 도구 모음에서 **View, Sort, Advanced**를 차례로 선택합니다. Drive Library Name, Drive Serial Number 기준으로 정렬합니다.
 - d. 모든 라이브러리에 교환 작업이 있는지 확인합니다.

8.5.2. 기존 로그 저장(선택 사항)

STA 2.1.0을 설치하기 전에 현재 STA 버전을 제거하거나 새 Linux 버전을 설치해야 하므로 업그레이드 후 기존 응용 프로그램 및 서비스 로그는 보존되지 않습니다. 이 절차를 사용하여 보존할 모든 로그를 저장할 수 있습니다.

1. 보존할 모든 설치 및 데이터베이스 로그를 찾아 안전한 장소로 이동합니다. 관련된 로그는 사용자가 설치에 대해 정의한 STA 로그 위치에 있습니다. 자세한 내용은 2.1.2절. “[STA 파일 시스템 레이아웃 검토](#)”를 참조하십시오.
2. 다음 단계를 사용하여 현재 STA 설치에서 서비스 로그 스냅샷을 만듭니다. 이 단계는 선택 사항이지만 Oracle 고객지원센터가 이 로그를 사용하여 업그레이드 전에 존재했던 문제를 해결할 수 있기 때문에 이 단계를 수행하는 것이 권장됩니다.

- a. STA 관리자인 사용자로 STA에 로그인합니다.
 - b. **Setup & Administration** 탭에서 **Logs**를 선택합니다.
 - c. Service – Logs 화면에서 **Create New Log Bundle** 아이콘을 누릅니다.
 - d. Create New Log Bundle 대화 상자에서 번들 이름을 지정하고 **Save**를 누릅니다. 프로세스를 완료하는 데 몇 분이 걸릴 수 있습니다.
3. 다음 단계를 사용하여 방금 만든 서비스 로그 번들 및 보존하려는 기타 모든 번들을 다운로드합니다. 번들은 한 번에 하나씩 다운로드해야 합니다.
 - a. Service – Logs 화면에서 다운로드할 번들을 선택합니다.
 - b. **Download Selected Log Bundle** 아이콘을 누릅니다.
 - c. 대화 상자에서 대상 위치를 지정하고 로그 번들을 저장합니다.

8.5.3. 현재 STA 사용자 및 구성 설정 기록(선택 사항)

이 절은 STA 2.1.0의 현재 STA 사용자 이름 및 구성 설정을 보존하려는 경우에만 적용됩니다. 이 절차를 사용하여 STA 2.1.0에 다시 입력할 수 있도록 현재 값을 표시 및 기록합니다. 업그레이드 후 이 값 중 대부분을 다시 입력합니다. 자세한 내용은 [8.6.10절. "작업 9: 새 STA 버전 구성"](#)을 참조하십시오.

8.5.3.1. MySQL 사용자 이름 기록

이 절차를 사용하여 STA 데이터베이스에 액세스하는 데 사용되는 MySQL 사용자 이름을 표시 및 기록합니다. STA 설치 프로그램은 이 값을 묻는 메시지를 표시합니다. 암호는 검색할 수 없습니다.

- a. 현재 STA 서버에서 터미널 세션을 열고 시스템 루트 사용자로 로그인합니다.
- b. 다음 질의를 실행하여 모든 STA 데이터베이스 사용자 이름을 표시합니다. 메시지가 표시되면 데이터베이스 루트 사용자 암호를 입력합니다. 예를 들면 다음과 같습니다.

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

- c. 사용자 이름을 기록합니다.

8.5.3.2. STA SNMP 클라이언트 설정 기록

이 절차를 사용하여 STA에 대한 SNMP 클라이언트 설정을 표시 및 기록합니다. 업그레이드 후 이 값을 다시 입력합니다.

주:

새 STA 버전에서 SNMP 값은 모니터링되는 라이브러리에 지정된 값과 일치해야 합니다.

- a. STA 관리자의 사용자 이름을 사용하여 STA에 로그인합니다.
- b. **Setup & Administration** 탭에서 **SNMP Connections**를 선택합니다.

Client Attributes 테이블에 STA SNMP 클라이언트에 대한 구성 설정이 표시됩니다.

Configuration - SNMP Connections						
Client Attributes						
SNMP Username	Password Encryption	Privacy Encryption	Engine ID	User Community	Trap Community	SNMP Trap Le
sta1	SHA	DES	0x8000002a0500000148c730df28	public	public	1,2,3,4,11,13,14,21,25,27,41,4

- c. 다음 열의 값을 기록합니다.
 - SNMP Username
 - User Community
 - Trap Community

8.5.3.3. WebLogic 사용자 이름 기록—STA 1.0.x에서 업그레이드하는 경우만 해당

STA 1.0.x에서 업그레이드하는 경우 이 절차를 사용하여 STA에 로그인하는 데 사용되는 기존 WebLogic 사용자 이름을 표시 및 기록합니다. 업그레이드 후 이 값을 다시 입력합니다. 암호는 검색할 수 없습니다.

주:

STA 2.0.x부터 사용자 이름은 STA 사용자 인터페이스를 통해 만들어지고 유지 관리됩니다. 자세한 내용은 8.5.3.4절. “STA 사용자 이름 기록—STA 2.0.x에서 업그레이드하는 경우만 해당”을 참조하십시오.

- a. 컴퓨터에서 지원되는 웹 브라우저를 시작한 다음 WebLogic 관리 콘솔의 URL을 입력합니다.

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

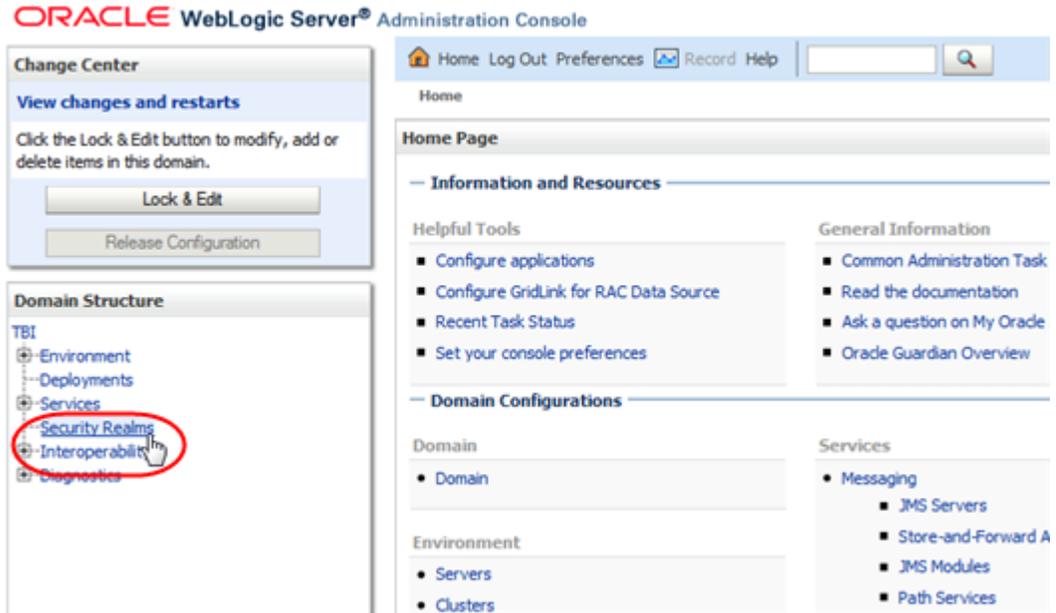
여기서 각 항목은 다음과 같습니다.

- *host_name*은 STA 서버의 호스트 이름입니다.
- *port_number*는 현재 STA 버전의 WebLogic 관리 콘솔의 STA 포트 번호입니다.
- *STA*는 대문자여야 합니다.

예를 들면 다음과 같습니다.

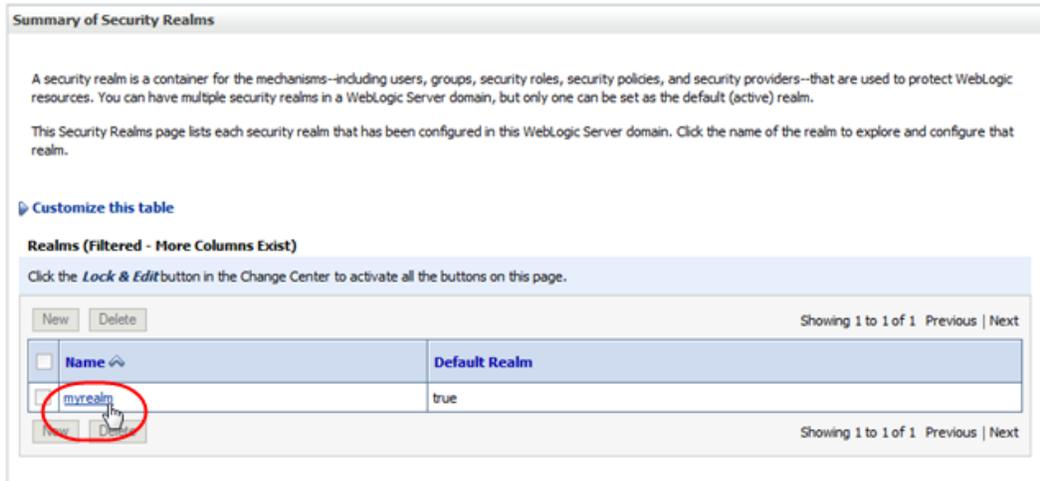
`https://staserver.example.com:7002/console/`

- b. WebLogic 관리 콘솔 사용자 이름과 암호를 사용하여 로그인합니다.
- c. Domain Structure 탐색 트리에서 **Security Realms**를 누릅니다.



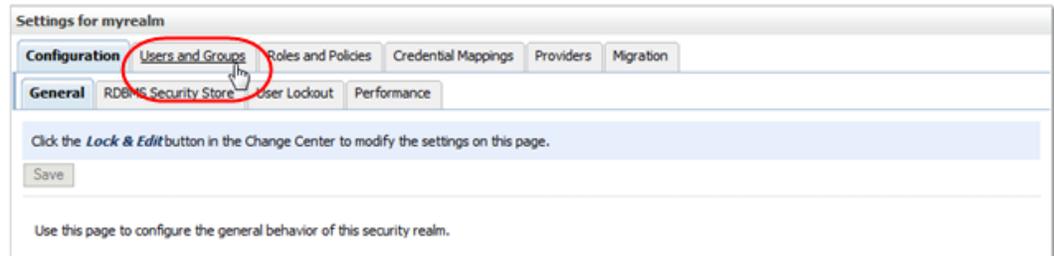
Summary of Security Realms 화면이 표시됩니다.

- d. Name 열에서 **myrealm** 활성 링크를 선택합니다(확인란 선택 안함).

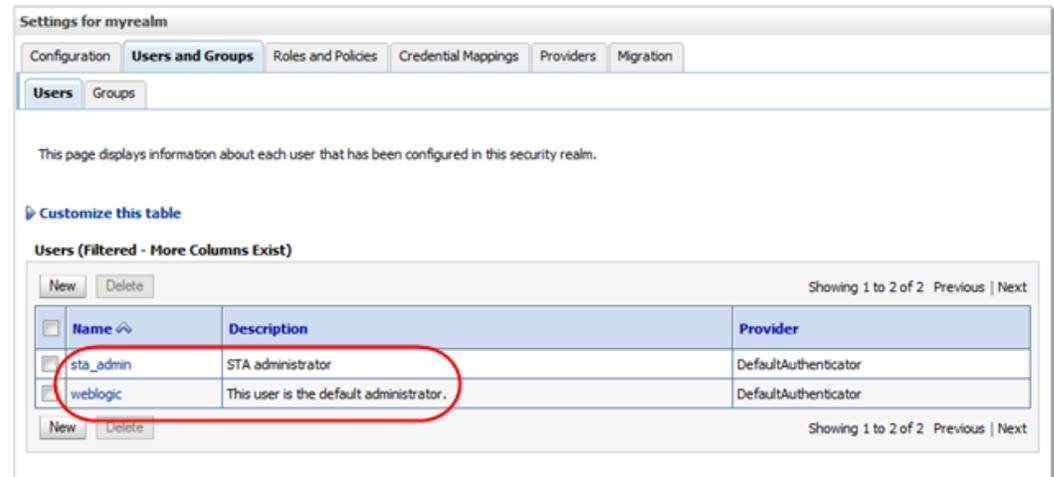


Settings for myrealm 화면이 나타납니다.

- e. **Users and Groups** 탭을 선택합니다.



Users 테이블에 사용 가능한 사용자 이름이 나열됩니다.



f. 보관할 사용자 이름을 기록합니다.

8.5.3.4. STA 사용자 이름 기록—STA 2.0.x에서 업그레이드하는 경우만 해당

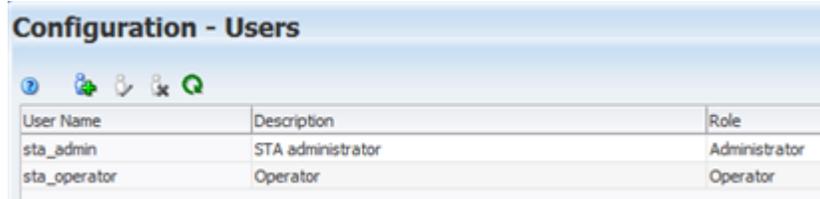
STA 2.0.x에서 업그레이드하는 경우 이 절차를 사용하여 STA에 로그인하는 데 사용되는 사용자 이름을 표시 및 기록합니다. 업그레이드 후 이 정보를 다시 입력합니다. 암호는 검색할 수 없습니다.

주:

STA 1.0.x의 경우 사용자 이름은 WebLogic 관리 콘솔을 통해 만들어지고 유지 관리됩니다. 자세한 내용은 8.5.3.3절. "WebLogic 사용자 이름 기록—STA 1.0.x에서 업그레이드하는 경우만 해당"을 참조하십시오.

- STA 관리자의 사용자 이름을 사용하여 STA에 로그인합니다.
- Setup & Administration** 탭에서 **Users**를 선택합니다.

Configuration – Users 화면에 모든 STA 사용자 이름 및 해당 역할이 표시됩니다.



User Name	Description	Role
sta_admin	STA administrator	Administrator
sta_operator	Operator	Operator

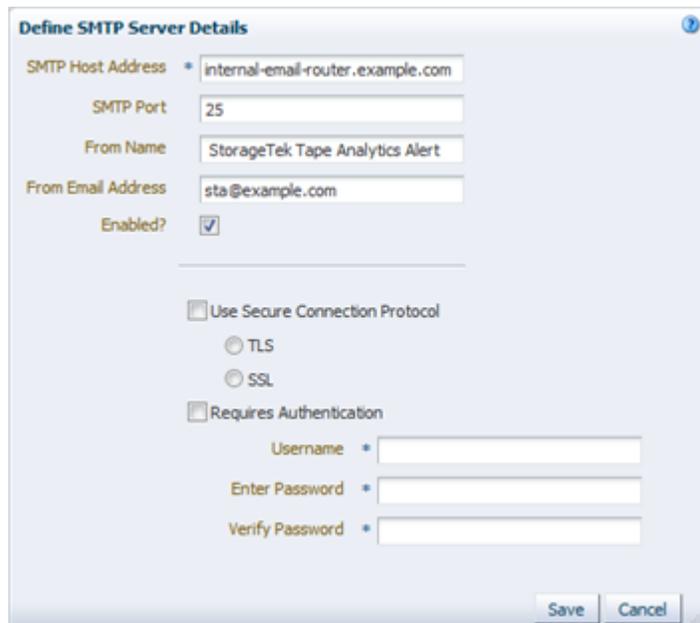
- c. 보존할 사용자 이름 및 역할을 기록합니다.

8.5.3.5. STA 전자 메일 서버 설정 기록

이 절차를 사용하여 STA 전자 메일 프로토콜과, 전자 메일 서버에 인증이 필요한 경우 계정 사용자 이름을 표시 및 기록합니다. 업그레이드 후 이 값을 다시 입력합니다. 암호는 표시할 수 없습니다.

- STA 관리자의 사용자 이름을 사용하여 STA에 로그인합니다.
- Setup & Administration** 탭에서 **Email**을 선택합니다.
- SMTP Server Settings 테이블에서 StorageTek Tape Analytics Alerts 레코드를 선택한 다음 **Edit Selected SMTP Server** 아이콘을 누릅니다.

Define SMTP Server Details 대화 상자가 나타납니다.



- d. 다음 필드의 값을 기록합니다.
- Use Secure Connection Protocol
 - Username

8.5.4. STA- 로 시작하는 사용자 정의 템플릿 이름 바꾸기(선택 사항)

이 절차는 이름이 "STA-"로 시작하는 사용자 정의 템플릿이 있는 경우에만 적용됩니다. STA 2.1.0 설치 중 "STA-"로 시작하는 모든 템플릿은 삭제되고 미리 정의된 새 STA 템플릿으로 교체됩니다.

이 절차를 사용하여 업그레이드 중 템플릿이 보존되도록 템플릿에 새 이름을 지정합니다.

주:

미리 정의된 STA 템플릿은 "STA-"로 시작하므로 Oracle은 사용자 정의 템플릿의 이름을 지정할 때 이 접두어를 사용하지 않도록 권장합니다.

- a. 관리자의 사용자 이름으로 STA에 로그인합니다.
- b. **Setup & Administration** 탭에서 **Templates Management**를 선택합니다.
- c. STA 설치 날짜 이후에 수정된 템플릿에 집중하기 위해 Created/Updated 날짜순으로 테이블을 정렬합니다.
- d. 이름이 "STA-"로 시작하는 사용자 정의 템플릿의 텍스트 링크를 선택합니다.

선택한 템플릿이 적용된 화면으로 이동합니다.

- e. Templates 도구 모음에서 **Save Template**를 누릅니다.

Save Template 대화 상자가 표시됩니다.

- f. **Template Name** 필드에서 "STA - "로 시작하지 않는 새 이름을 지정합니다. 항목은 고유해야 합니다.
- g. **Save**를 누릅니다.

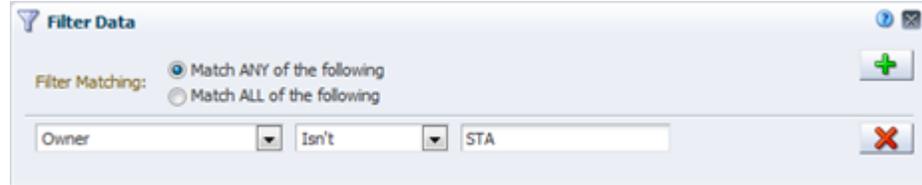
템플릿이 저장됩니다.

8.5.5. 현재 사용자 정의 템플릿 설정 기록(선택 사항)

이 절은 사용자 정의 템플릿이 있는 경우에만 적용됩니다. 업그레이드에서는 사용자 정의 템플릿이 보존되지만, 업그레이드 후 모든 사용자 정의 템플릿은 가시성이 공개로 설정되어 STA 소유가 됩니다.

이 절차를 사용하여 모든 사용자 정의 템플릿의 현재 소유권 및 가시성 설정을 기록하면 업그레이드 후 필요한 경우 해당 설정을 복원할 수 있습니다. 템플릿 소유권 및 가시성이 사용자의 구현에 중요하지 않은 경우 이 절차를 건너뛸 수 있습니다.

- a. 관리자의 사용자 이름으로 STA에 로그인합니다.
- b. **Setup & Administration** 탭에서 **Templates Management**를 선택합니다.
- c. **Filter** 아이콘을 선택하여 STA가 소유하지 않은 템플릿만 표시하도록 화면을 필터링합니다. 이렇게 하면 사용자 정의 템플릿만 표시됩니다.



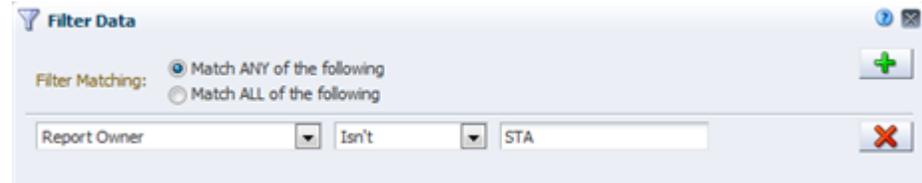
- d. 각 사용자 정의 템플리트의 현재 Owner 및 Public Visibility 설정을 기록합니다. 템플리트가 여러 개인 경우 스크린샷을 만들면 좋습니다.

8.5.6. 실행 보고서 정책 설정 기록(선택 사항)

이 절은 사용자가 실행 보고서 정책을 개인적으로 소유한 경우에만 적용됩니다. 업그레이드 작업은 모든 실행 보고서 정책을 보존하지만 업그레이드 후 모든 개인 정책에는 공용 소유권이 지정됩니다.

이 절차를 사용하여 모든 개인 정책의 현재 소유권 설정을 기록하면 업그레이드 후 필요한 경우 해당 설정을 복원할 수 있습니다. 실행 보고서 정책 소유권이 사용자의 구현에 중요하지 않은 경우 이 절차를 건너뛸 수 있습니다.

- STA 관리자의 사용자 이름을 사용하여 STA에 로그인합니다.
- Setup & Administration** 탭에서 **Executive Reports Policies**를 선택합니다.
- Filter** 아이콘을 선택하여 STA가 소유하지 않은 정책만 표시하도록 화면을 필터링합니다. 이렇게 하면 개인 정책만 표시됩니다.



- d. 각 정책에 대해 현재 Report Owner를 기록합니다. 정책이 여러 개인 경우 스크린샷을 만들면 좋습니다.

8.6. 업그레이드 작업

주의:

Linux 관리자 및 STA 관리자만 업그레이드를 수행해야 합니다. 모든 작업은 필수이며 지정된 순서대로 정확하게 수행되어야 합니다. 그렇지 않으면 데이터가 손실될 수 있습니다.

단일 서버 업그레이드 방식을 사용하는 경우 작업을 순번대로 수행합니다. 자세한 내용은 [그림 8.1. "단일 서버 업그레이드 작업 개요"](#)를 참조하십시오.

두 대의 서버 업그레이드 방식을 사용하는 경우 작업을 순번대로 수행하지 않으며 작업 6은 생략됩니다. 작업 순서는 [그림 8.2. "두 대의 서버 업그레이드 작업 개요"](#)를 참조하십시오.

- [8.6.1절. "작업 1: 이전 STA 데이터베이스 덤프"](#)
- [8.6.2절. "작업 2: 이전 데이터베이스 덤프 전송"](#)

- 8.6.3절. “작업 3a: 새 Linux 버전 설치(STA 1.0.x에서 업그레이드)”
- 8.6.4절. “작업 3b: 이전 STA 버전 제거(STA 2.0.x에서 업그레이드)”
- 8.6.5절. “작업 4: 새 STA 버전 설치”
- 8.6.6절. “작업 5: 새 STA 데이터베이스 덤프(선택 사항)”
- 8.6.7절. “작업 6: 이전 STA 데이터베이스를 STA 서버로 전송”
- 8.6.8절. “작업 7: 이전 STA 데이터베이스 처리 및 로드”
- 8.6.9절. “작업 8: 이전 데이터베이스 업그레이드”
- 8.6.10절. “작업 9: 새 STA 버전 구성”
- 8.6.11절. “실패한 데이터베이스 업그레이드 복구(선택 사항)”

8.6.1. 작업 1: 이전 STA 데이터베이스 덤프

이 절차를 수행하여 이전(현재) STA 데이터베이스의 전체 덤프를 수행합니다.

1. 다음 단계에 따라 현재 STA 데이터베이스의 크기를 표시합니다.
 - a. STA 관리자의 사용자 이름을 사용하여 STA에 로그인합니다.
 - b. 상태 표시줄에서 **About**를 누릅니다.
 - c. About 대화 상자에서 Database Current Size가 표시된 위치까지 아래로 스크롤한 다음 해당 값을 기록합니다.
2. 다음 단계에 따라 데이터베이스를 덤프할 위치에 충분한 공간이 있는지 확인합니다.
 1. STA 서버에서 터미널 세션을 열고 시스템 루트 사용자로 로그인합니다.
 2. 데이터베이스 덤프 대상의 사용 가능한 공간을 표시하고 이 공간이 덤프 파일에 충분한지 확인합니다. 예를 들면 다음과 같습니다.

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

3. 모든 STA 서비스를 중지합니다.

```
# STA stop all
```

4. MySQL 서비스를 시작합니다.

```
# service mysql start
```

5. STA 데이터베이스를 단일 파일로 덤프합니다. 메시지가 표시되면 데이터베이스 루트 사용자 암호를 입력합니다.

```
# 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*

주:

선택 사항인 `-v` 매개변수(상세 정보 출력용)는 권장되지 않습니다. 이 매개변수를 지정하면 많은 수의 메시지가 터미널 창에 표시되어 큰 데이터베이스의 경우 명령 프로세스 속도가 매우 느려질 수 있습니다.

예 8.1. “이전 데이터베이스 덤프”에서 STA 1.0.x 데이터베이스는 `Dec14_dump.sql`이라는 파일 이름으로 STA 서버의 `/dbdumpfiles` 폴더에 덤프됩니다.

예 8.1. 이전 데이터베이스 덤프

```
# 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. 덤프 파일 크기를 약 50%로 줄이기 위해 파일을 gzip으로 압축합니다.

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

8.6.2. 작업 2: 이전 데이터베이스 덤프 전송

이 절차를 사용하여 이전 STA 데이터베이스의 압축된 덤프를 오픈 플랫폼 백업 서버(단일 서버 방식) 또는 새 STA 2.1.0 서버(두 대의 서버 방식)로 전송합니다.

주의:

단일 서버 방식으로 STA 1.0.x에서 업그레이드하는 경우 STA 데이터베이스를 다른 서버에 백업해야 합니다. 8.6.3절. “작업 3a: 새 Linux 버전 설치(STA 1.0.x에서 업그레이드)” [119]에서 Linux 6.x를 설치하면 서버의 모든 데이터가 삭제되므로 데이터베이스를 현재 STA 서버의 파일 시스템에 백업하지 마십시오.

1. 아직 실행 중인 STA 서비스가 있는 경우 모두 중지합니다.

```
# STA stop all
```

2. 파일을 백업 서버로 전송하기 전에 체크섬을 수행합니다.

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

출력에는 체크섬 값과 바이트 수가 포함됩니다. 체크섬 값을 기록하십시오. 이 값은 파일을 백업 서버로 전송한 후 파일 무결성을 확인하는 데 사용됩니다.

3. SCP와 같은 전송 유틸리티를 사용하여 파일을 대상 서버로 전송합니다. `-p` 옵션은 시간 기록 값을 유지합니다.

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

예 8.2. “백업 서버로 이전 데이터베이스 전송(단일 서버 방식)”에서는 SCP를 사용하여 압축된 데이터베이스 덤프 파일 `Dec14_dump.sql.gz`를 백업 호스트 `backup1`의 `/dbdumpfiles` 폴더로 전송합니다. `/dbdumpfiles` 폴더는 백업 호스트에 이미 존재합니다.

예 8.2. 백업 서버로 이전 데이터베이스 전송(단일 서버 방식)

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

예 8.3. “새 STA 서버로 이전 데이터베이스 전송(두 대의 서버 방식)”에서는 SCP를 사용하여 압축된 데이터베이스 덤프 파일 `Dec14_dump.sql.gz`를 STA 2.1.0 호스트 `sta_new`의 `/dbdumpfiles` 폴더로 전송합니다.

예 8.3. 새 STA 서버로 이전 데이터베이스 전송(두 대의 서버 방식)

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

4. 대상 서버에서 전송된 파일의 체크섬을 수행합니다. 체크섬 값이 일치하는지 확인합니다.

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

8.6.3. 작업 3a: 새 Linux 버전 설치(STA 1.0.x에서 업그레이드)

이 절차는 STA 1.0.x에서 업그레이드하는 경우에만 적용됩니다. STA 서버에 Linux 6.3 이상을 설치합니다. 자세한 내용은 [2장. Linux 설치](#)를 참조하십시오.

주의:

이 작업을 수행하면 서버의 모든 데이터가 삭제됩니다. 단일 서버 업그레이드 방식을 사용하는 경우 [8.6.1절. “작업 1: 이전 STA 데이터베이스 덤프”](#) 및 [8.6.2절. “작업 2: 이전 데이터베이스 덤프 전송”](#)을 수행한 후에만 이 절차를 수행하십시오.

8.6.4. 작업 3b: 이전 STA 버전 제거(STA 2.0.x에서 업그레이드)

이 절차는 STA 2.0.x에서 업그레이드하는 경우에만 적용됩니다. 현재 STA 버전을 제거합니다. 자세한 내용은 9.2.1절. "STA 제거" 및 9.2.2절. "성공적인 제거 확인"을 참조하십시오.

주의:

이 작업을 수행하면 서버의 모든 STA 데이터가 삭제됩니다. 단일 서버 업그레이드 방식을 사용하는 경우 8.6.1절. "작업 1: 이전 STA 데이터베이스 덤프" 및 8.6.2절. "작업 2: 이전 데이터베이스 덤프 전송"을 수행한 후에만 이 절차를 수행하십시오.

8.6.5. 작업 4: 새 STA 버전 설치

이 절차를 사용하여 STA 2.1.0을 설치합니다.

1. STA 2.1.0을 설치합니다. 자세한 내용은 3장. STA 설치를 참조하십시오.
2. STA가 제대로 작동하는 지 확인하고 WebLogic에서 STA Administrator 설정을 완료하기 위해 STA 응용 프로그램에 로그인합니다.

Dashboard가 표시됩니다.

주:

업그레이드 프로세스가 아직 완료되지 않았으므로 Dashboard 포틀릿에 "No data to display"라는 메시지가 표시되는데 이것은 정상적인 동작입니다. 데이터베이스를 업그레이드하고 새 STA 버전을 구성하면 라이브러리 데이터가 올바르게 표시됩니다.

3. STA에서 로그아웃합니다.
4. STA 서버에서 터미널 세션을 열고 시스템 루트 사용자로 로그인합니다.
5. 모든 STA 서비스를 중지합니다.

```
# STA stop all
```

6. 이 단계는 STA가 SNMP v2c를 사용하여 라이브러리를 모니터링하는 경우에만 적용됩니다(부록 F. SNMP v2c 모드 구성 참조). STA 2.0.x부터는 SNMP v2c가 기본적으로 사용으로 설정됩니다. 다음 단계를 사용하여 SNMP v2c가 사용으로 설정되었는지 확인합니다.

- a. STA 구성 파일 디렉토리로 변경합니다.

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

- b. SNMP 버전 등록 정보 파일을 표시하고 v2c 매개변수가 true로 설정되었는지 확인합니다.

```
# cat TbiSnmpVersionSupport.properties
V2c=true
Verbal=false
```

- c. 매개변수가 true로 설정되지 않은 경우 해당 매개변수를 변경하는 방법은 [F.1.3절](#). “STA에 대해 SNMP v2c 모드 사용으로 설정”을 참조하십시오.

8.6.6. 작업 5: 새 STA 데이터베이스 덤프(선택 사항)

이 절차는 선택 사항이지만 권장됩니다. 이 절차를 사용하여 만약을 위해 빈 STA 2.1.0 데이터베이스를 덤프합니다. 데이터베이스 업그레이드([작업 8: 이전 데이터베이스 업그레이드](#))를 완료할 수 없는 경우 빈 데이터베이스를 복원하여 STA 2.1.0을 데이터 없이 새로 설치된 것처럼 실행하도록 구성할 수 있는 상태로 복원할 수 있습니다. 복구 프로세스에 대한 자세한 내용은 [실패한 데이터베이스 업그레이드 복구\(선택 사항\)](#)를 참조하십시오.

1. STA 서버에서 터미널 세션을 열고 시스템 루트 사용자로 로그인합니다.
2. 아직 실행 중인 STA 서비스가 있는 경우 모두 중지합니다.

```
# STA stop all
```

3. MySQL 서비스를 시작합니다.

```
# STA start mysql
```

4. 데이터베이스 백업 파일을 만듭니다. 메시지가 표시되면 데이터베이스 루트 사용자 암호를 입력합니다.

```
# 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
```

주:

선택 사항인 `-v` 매개변수(상세 정보 출력용)는 권장되지 않습니다. 이 매개변수를 지정하면 많은 수의 메시지가 터미널 창에 표시되어 큰 데이터베이스의 경우 명령 프로세스 속도가 매우 느려질 수 있습니다.

[예 8.4. “새 데이터베이스 덤프”](#)에서 STA 2.1.0 데이터베이스는 `STA_FRESH_INSTALL_BACKUP.sql`이라는 파일 이름으로 STA 서버의 `/dbdumpfiles` 폴더에 덤프됩니다.

예 8.4. 새 데이터베이스 덤프

```
# 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...
```

주:

"Can't connect to local MySQL server"라는 메시지가 표시되면 MySQL 서버가 실행되지 않는 것입니다. MySQL을 시작했는지 확인하십시오(3단계).

8.6.7. 작업 6: 이전 STA 데이터베이스를 STA 서버로 전송

주:

이 절차는 단일 서버 방식에만 적용됩니다.

이 절차를 사용하여 STA 1.0.x 또는 STA 2.0.x 데이터베이스 백업을 STA 2.1.0 서버로 전송합니다.

1. 아직 실행 중인 STA 서비스가 있는 경우 모두 중지합니다.

```
# STA stop all
```

2. 데이터베이스를 전송합니다. SCP에 대해 `-p` 옵션을 지정하면 시간 기록 값이 유지됩니다.

```
# scp -p backup_host:/path_to_dump_file/dump_file_name.sql.gz /local_path
```

예 8.5. "새 STA 서버로 이전 데이터베이스 전송"에서는 SCP를 사용하여 압축된 데이터베이스 덤프 파일 `Dec14_dump.sql.gz`를 호스트 `backup1`의 `/dbdumpfiles`에서 STA 2.1.0 서버의 `/dbdumpfiles` 폴더로 전송합니다.

예 8.5. 새 STA 서버로 이전 데이터베이스 전송

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

3. 전송된 파일의 체크섬을 수행합니다. 체크섬 값이 8.6.1절. "작업 1: 이전 STA 데이터베이스 덤프" [117]에서 받은 값과 일치하는지 확인합니다.

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

8.6.8. 작업 7: 이전 STA 데이터베이스 처리 및 로드

이 절차를 따라 STA 1.0.x 또는 STA 2.0.x 데이터베이스의 압축을 풀어 STA 2.1.0 서버에 복원합니다. 압축을 푼 데이터베이스는 압축된 데이터베이스보다 10~15배의 공간을 차지할 수 있습니다.

1. 아직 실행 중인 STA 서비스가 있는 경우 모두 중지합니다.

```
# STA stop all
```

2. 백업 파일의 압축을 풉니다.

```
# gunzip dump_file_name.sql.gz
```

3. 다음 단계를 수행하여 더 이상 사용되지 않는 데이터(예: 처리된 SNMP 레코드 및 빈 분석 레코드)가 들어 있는 STA 데이터베이스를 비웁니다.

시간 예상: STA 1.0.x 및 STA 2.0.x의 경우 압축이 풀린 데이터베이스 스냅샷 크기 1GB당 최대 1분입니다.

주:

purgerecs 명령 작업의 영구 레코드는 STA 데이터베이스에 저장됩니다. STA 2.0.x부터는 데이터베이스 비우기도 런타임에 자동으로 발생합니다. 정기적으로 MySQL Event Scheduler는 여러 테이블에서 레코드를 비워 데이터베이스 증가 속도를 줄입니다.

- a. STA 데이터베이스 업데이트 디렉토리로 변경합니다.

```
# cd /Oracle_storage_home/StorageTek_Tape_Analytics/db/updates
```

- b. 비우기를 시작합니다.

```
# ./purgerecs /path_to_dump_file/dump_file_name.sql /path_to_dump_file/dump_file_name_PURGED.sql
```

주:

purgerecs 명령에 대한 도움말을 보려면 다음 명령을 입력하십시오.

```
# ./purgerecs -h
```

예 8.6. “이전 데이터베이스 백업에서 더 이상 사용되지 않는 데이터 비우기”에서 *purgerecs* 유틸리티는 */dbdumpfiles*에 있는 MySQL 덤프 파일 *Dec14_dump.sql*을 처리합니다. 출력은 */dbdumpfiles*에 *Dec14_dump_PURGED.sql*이라는 새 파일로 저장됩니다. 진행 상태 점은 200개의 레코드가 처리될 때마다 나타납니다.

예 8.6. 이전 데이터베이스 백업에서 더 이상 사용되지 않는 데이터 비우기

```
# 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. 이 단계는 선택 사항입니다. 데이터베이스 파일 크기를 파악하고 로드 프로세스 시간을 예상합니다.

시간 예상: STA 1.0.x 및 STA 2.0.x의 경우 압축이 풀린 데이터베이스 스냅샷 크기 1GB당 최대 3~10분입니다.

```
# ls -s -h dump_file_name_PURGED.sql
```

5. MySQL 서버를 시작합니다.

```
# STA start mysql
```

6. STA 1.0.x 또는 STA 2.0.x 데이터베이스를 로드합니다. 메시지가 표시되면 데이터베이스 루트 사용자 암호를 입력합니다. 상세 정보를 표시하는 `-v` 옵션(권장되지 않음)을 지정하지 않을 경우 프로세스가 실행될 때 명령 출력이 없습니다.

주:

선택 사항인 `-v` 매개변수(상세 정보 출력용)는 권장되지 않습니다. 이 매개변수를 지정하면 많은 수의 메시지가 터미널 창에 표시되어 큰 데이터베이스의 경우 명령 프로세스 속도가 매우 느려질 수 있습니다.

```
# mysql -uroot -p -e "SET SESSION SQL_LOG_BIN=0; SOURCE /path_to_dump_file/dump_file_name_PURGED.sql;"
Password: mysql_root_password
```

여기서 각 항목은 다음과 같습니다.

- `-p`—STA 설치 중 설정된 데이터베이스 루트 암호를 물어봅니다.
- `-e`—다음 따옴표로 묶인 명령문을 실행합니다.
 - `SET SESSION SQL_LOG_BIN=0;`—불필요한 바이너리 로깅을 해제하여 로드 속도를 높입니다.
 - `SOURCE /path_to_dump_file/dump_file_name_PURGED.sql`—덤프 파일을 DB로 로드합니다.

명령을 성공할 경우 프로세스가 완료되면 명령 프롬프트로 돌아옵니다.

8.6.9. 작업 8: 이전 데이터베이스 업그레이드

이 절차를 사용하여 STA 1.0.x 또는 STA 2.0.x 데이터베이스를 새 STA 2.1.0 스키마로 업그레이드합니다.

시간 예상: 압축이 풀린 데이터베이스 스냅샷 크기 1GB당 대략적인 시간입니다.

- STA 1.0.x에서 업그레이드하는 경우—1GB당 최대 5분
- STA 2.0.x에서 업그레이드하는 경우—1GB당 최대 30분

1. 아직 실행 중인 STA 서비스가 있는 경우 모두 중지합니다.

```
# STA stop all
```

2. 8.5.1.1절. “업그레이드 필요 조건 확인”에서 */tmp*의 크기가 업그레이드 작업에 충분하지 않다고 파악한 경우 필요에 따라 */tmp*의 크기를 늘립니다.

크기를 늘릴 수 없는 경우 다음 단계를 사용하여 대체 임시 위치를 사용하도록 MySQL에 대한 환경 변수를 설정합니다.

a. 대체 임시 위치를 만들고 열기 권한을 지정합니다. 예를 들면 다음과 같습니다.

```
# mkdir /dbbackup/tmp
# chmod 777 /dbbackup/tmp
```

b. MySQL을 중지합니다.

```
# STA stop mysql
```

c. MySQL 구성 파일을 편집합니다. 예를 들면 다음과 같습니다.

```
# vi /etc/my.cnf
```

d. 파일의 *mysqld* 섹션에 *tmpdir* 변수로 식별되는 대체 임시 위치를 정의하는 라인을 추가합니다. 다음은 이 라인이 추가된 파일의 예입니다.

```
[mysqld]
#----- mysqld MySQL Server Options -----

tmpdir                = /dbbackup/tmp
server-id              = 1
...
```

e. MySQL을 다시 시작합니다.

```
# STA start mysql
```

3. 데이터베이스 업데이트 디렉토리로 변경합니다.

```
# cd /Oracle_storage_home/StorageTek_Tape_Analytics/db/updates
```

4. 업그레이드 스크립트를 시작하고 메시지가 표시되면 데이터베이스 루트 사용자 암호를 입력합니다. 보안상의 이유로, 암호는 화면에 표시되지 않습니다.

```
# ./upgradedb.sh
```

주:

시스템 루트 사용자 또는 Oracle 설치 사용자로 이 단계를 수행할 수 있습니다.

다음은 화면 표시의 예입니다.

```
# ./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...
```

프로세스가 완료되면 다음과 비슷한 배너가 표시됩니다.

주의:

계속하기 전에 배너가 표시될 때까지 기다리십시오.

```
+-----+
| 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. 8.6.9절. “작업 8: 이전 데이터베이스 업그레이드”에서 */tmp*의 크기를 늘렸거나 대체 임시 위치를 만들었다면 정상적인 크기 및 위치로 복원합니다.
6. 모든 STA 서비스를 시작합니다.

```
# STA start all
```

7. 이 단계는 선택 사항입니다. *STA_FRESH_INSTALL_BACKUP.sql* 파일을 삭제하여 STA 데이터베이스 백업 볼륨에 디스크 공간을 확보합니다.

8.6.10. 작업 9: 새 STA 버전 구성

이 절차를 따라 라이브러리 및 STA 2.1.0을 구성하면 STA가 라이브러리 작업 모니터링을 시작할 수 있습니다.

8.6.10.1. 라이브러리에서 STA 트랩 수신자 업데이트

2개의 새 트랩 레벨인 13(테스트 트랩) 및 14(상태 트랩)가 STA 2.0.x에 도입되었습니다. 모니터링되는 각 라이브러리에 대해 다음 단계를 수행하여 이러한 트랩 레벨이 STA 트랩 수신자 정의에 포함되었는지 확인합니다.

1. 업그레이드 경로에 따라 다음과 같이 진행하십시오.
 - 단일 서버 방식을 사용하여 STA 2.0.x에서 업그레이드하는 경우 8.6.10.2절. “STA의 SNMP 설정 구성” [128]으로 진행합니다.
 - 단일 서버 방식을 사용하여 STA 1.0.x에서 업그레이드하는 경우 2단계로 이동하여 모니터링되는 각 라이브러리에서 기존 STA 트랩 수신자에 새 트랩 레벨을 추가합니다.
 - 두 대의 서버 방식을 사용하는 경우 3단계로 이동하여 모니터링되는 각 라이브러리에 새 STA 트랩 수신자를 추가합니다.
2. 단일 서버 방식을 사용하여 STA 1.0.x에서 업그레이드하는 경우 라이브러리 모델에 해당하는 단계를 사용하여 STA 트랩 수신자에 새 트랩 레벨을 추가합니다.

SL150 이외의 모든 라이브러리 모델의 경우 트랩 수신자를 수정하려면 기존 정의를 삭제한 다음 새 정의를 추가해야 합니다.

SL150을 제외한 모든 라이브러리

- a. 라이브러리 CLI에 로그인합니다.
- b. 기존의 모든 트랩 수신자를 표시하고 STA 수신자의 인덱스 번호를 기록해 둡니다.

```
snmp listTrapRecipients
```

- c. STA 트랩 수신자를 삭제합니다.

```
snmp deleteTrapRecipient id index
```

여기서 각 항목은 다음과 같습니다.

- *index*는 STA 트랩 수신자의 인덱스 번호입니다.
- d. STA 트랩 수신자를 다시 추가하고 트랩 레벨 목록에 새 트랩 레벨을 포함합니다. 자세한 내용은 5.2.6절. “STA SNMP v3 트랩 수신자 만들기” 또는 F.1.2절. “라이브러리에서 STA SNMP v2c 트랩 수신자 만들기”를 참조하십시오.
- SL150 라이브러리**
- a. 브라우저 기반 사용자 인터페이스에 로그인합니다.
 - b. **SNMP** 메뉴에서 **SNMP Trap Recipients**를 선택합니다.
 - c. 목록에서 STA 트랩 수신자를 선택합니다.
 - d. **Modify Trap Recipient**를 선택합니다.
 - e. 트랩 레벨 목록에 새 트랩 레벨을 추가한 다음 **Save**를 누릅니다.
3. 두 대의 서버 업그레이드 방식을 사용하는 경우 각 라이브러리에서 새 STA 2.1.0 서버를 트랩 수신자로 추가합니다. 자세한 내용은 5.2.6절. “STA SNMP v3 트랩 수신자 만들기” [79] 또는 F.1.2절. “라이브러리에서 STA SNMP v2c 트랩 수신자 만들기”를 참조하십시오.

8.6.10.2. STA의 SNMP 설정 구성

모든 업그레이드에 대해 이 단계를 수행합니다. 이 단계는 STA에서 수행됩니다.

1. STA 관리자인 사용자로 STA에 로그인합니다.
2. 업그레이드 전에 기록한 값을 사용하여 STA SNMP 클라이언트에 대한 구성 설정을 다시 입력합니다. 8.5.3절. “현재 STA 사용자 및 구성 설정 기록(선택 사항)”을 참조하십시오. 이 값은 모니터링되는 라이브러리에 구성된 값과 일치해야 합니다. 자세한 내용은 6.1.3절. “STA에 대한 SNMP 클라이언트 설정 구성”을 참조하십시오.
3. STA와 라이브러리 사이의 SNMP 통신을 복원하려면 모니터링되는 각 라이브러리에 대한 연결을 테스트합니다. 자세한 내용은 6.1.5절. “라이브러리 SNMP 연결 테스트”를 참조하십시오.

주:

이 단계가 성공적으로 완료되면 STA가 모니터링되는 각 라이브러리에서 데이터를 받아 처리하기 시작합니다.

STA가 중지되었거나 라이브러리 연결이 복원되었을 때 처리 중인 교환으로 인해 Exchanges Overview 화면에 완료되지 않은 교환이 표시될 수 있습니다. 완료되지 않은 교환에 대한 자세한 내용은 STA 사용 설명서를 참조하십시오.

4. 각 라이브러리에서 최신 SNMP 라이브러리 구성 데이터를 가져옵니다. 자세한 내용은 6.1.6절. “수동 데이터 수집 수행”을 참조하십시오.

8.6.10.3. STA 서비스 및 사용자 정보 구성

모든 업그레이드에 대해 이 단계를 수행합니다. 이 단계는 STA 서버에서 수행됩니다.

이전 STA 버전의 설정을 보존하려면 업그레이드 전에 기록한 값을 사용합니다. 8.5.3절. “현재 STA 사용자 및 구성 설정 기록(선택 사항)”을 참조하십시오.

주:

업그레이드가 끝나면 STA가 모든 논리적 그룹을 소유합니다. 논리적 그룹 소유권은 STA 기능에 중요하지 않으며 Operator 또는 Administrator 권한이 있는 모든 STA 사용자는 논리적 그룹을 수정할 수 있습니다.

1. STA 백업 서비스 및 STA 리소스 모니터 서비스 유틸리티를 구성합니다. 자세한 내용은 [7장. STA 서비스 구성](#)을 참조하십시오.
2. STA 사용자 이름 및 암호를 만듭니다. 자세한 내용은 STA 사용 설명서를 참조하십시오. 다음을 수행할 수도 있습니다.
 - 사용자에게 STA 2.1.0의 새 암호 요구 사항을 알립니다.
 - 해당하는 경우 사용자에게 사용자 정의 사용자 환경 설정을 다시 입력하도록 지시합니다.
3. STA 전자 메일 서버에 인증이 필요한 경우 전자 메일 계정 사용자 이름 및 암호를 입력해야 합니다. 자세한 내용 STA 사용 설명서를 참조하십시오.
4. 해당하는 경우 사용자 정의 템플릿에 대한 원래 소유권을 복원합니다. 자세한 내용은 STA 사용 설명서를 참조하십시오.
5. 해당하는 경우 개인 실행 보고서 정책에 대한 원래 소유권을 복원합니다. 자세한 내용은 STA 사용 설명서를 참조하십시오.

8.6.10.4. 이전 STA 서버 구성 해제(선택 사항)

이 절차는 두 대의 서버 업그레이드 방식을 사용한 경우에만 적용됩니다. 새 STA 서버가 예상한 대로 작동 중임을 확인한 후 이 절차를 수행할 수 있습니다.

1. 각 라이브러리의 SNMP 구성의 트랩 수신자에서 이전 STA 1.0.x 또는 STA 2.0.x 서버를 구성 해제합니다. 자세한 내용은 STA 사용 설명서를 참조하십시오.
2. 이전 STA 1.0.x 또는 STA 2.0.x 서버를 구성 해제합니다.

8.6.11. 실패한 데이터베이스 업그레이드 복구(선택 사항)

주의:

이 절차는 반드시 Oracle 지원 담당자의 지시에 따라서 수행하십시오.

이 절차는 [8.6.9절. "작업 8: 이전 데이터베이스 업그레이드" \[125\]](#)의 데이터베이스 업그레이드가 성공적으로 완료되지 않고 업그레이드를 반복하려는 시도도 실패한 경우에만 수행합니다.

1. "[작업 7: 이전 STA 데이터베이스 처리 및 로드](#)" [122], 6단계에서 "[작업 8: 이전 데이터베이스 업그레이드](#)" [125]까지 반복합니다.

업그레이드가 다시 실패할 경우 데이터베이스가 알 수 없는 상태가 되며 손상되었을 가능성이 있으므로 데이터베이스를 새로 설치된 원래 상태로 복원해야 합니다. 다음 단계를 진행합니다.

2. 손상된 업그레이드된 데이터베이스를 삭제합니다.

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

3. STA 데이터베이스 백업 위치로 변경하고 [8.6.6절. “작업 5: 새 STA 데이터베이스 덤프 \(선택 사항\)” \[121\]](#)에서 만든 새 설치 데이터베이스 덤프 파일을 로드합니다.

예를 들면 다음과 같습니다.

```
# cd /dbbackup
```

```
# mysql -uroot -p -e < /home/oracle/STA_FRESH_INSTALL_BACKUP.sql
```

4. [8.6.9절. “작업 8: 이전 데이터베이스 업그레이드” \[125\]](#)를 수행합니다.
5. STA를 새 설치로 구성합니다. 자세한 내용은 다음 절을 참조하십시오.
 - [6장. STA의 라이브러리 연결 구성](#)
 - [7장. STA 서비스 구성](#)

STA 제거 및 복원

이 장은 다음과 같은 절로 구성됩니다.

- [STA 제거 개요](#)
- [STA 제거 작업](#)

주의:

Oracle은 STA를 이전 버전으로 다운그레이드하도록 지원하지 않습니다. 이전 버전의 STA를 설치할 경우 최신 버전의 STA에서 만든 데이터베이스 데이터는 손실됩니다.

9.1. STA 제거 개요

STA 제거 프로그램은 STA 응용 프로그램 및 이와 연관된 모든 데이터와 Oracle 소프트웨어를 제거합니다. 다음과 같은 업데이트가 수행됩니다.

- Oracle 스토리지 홈 위치 내의 *StorageTek_Tape_Analytics* 하위 디렉토리가 완전히 제거됩니다. Oracle 스토리지 홈 위치의 다른 디렉토리는 영향을 받지 않습니다.
- 모든 STA 및 MySQL 로그가 로그 위치에서 제거됩니다. 해당 위치에 대한 자세한 내용은 [2.1.2절. "STA 파일 시스템 레이아웃 검토"](#)을 참조하십시오.
- 모든 STA 서비스 로그가 제거됩니다.
- STA 데이터베이스 및 모든 로컬 백업이 제거됩니다. 데이터베이스 디렉토리 또는 로컬 백업 디렉토리가 마운트 지점이거나 사용자 정의 파일을 포함하고 있는 경우 해당 디렉토리는 보존되고, 그렇지 않으면 해당 디렉토리는 제거됩니다.

STA를 제거해도 Oracle 중앙 인벤토리 위치는 제거되지 않습니다. 모든 STA 설치 및 제거 로그와 Oracle 소프트웨어 인벤토리 정보를 비롯하여 이 디렉토리의 모든 데이터는 보존됩니다. 자세한 내용은 [Oracle 중앙 인벤토리 위치](#)를 참조하십시오.

STA 제거 프로그램은 그래픽 모드와 자동 모드 두 가지로 사용할 수 있습니다. 자세한 내용은 [3.5절. "STA 설치 프로그램 모드"](#)를 참조하십시오.

STA 제거 로그에 대한 자세한 내용은 [3.4절. "STA 설치 및 제거 로그"](#)를 참조하십시오.

9.2. STA 제거 작업

다음 절에서는 STA 제거 프로그램을 사용하는 방법에 대해 설명합니다.

- [9.2.1절. "STA 제거"](#)
- [9.2.2절. "성공적인 제거 확인"](#)
- [9.2.3절. "STA 복원"](#)

9.2.1. STA 제거

이 절차를 사용하여 STA를 제거합니다.

주의:

제거 작업을 수행하면 모든 STA 데이터베이스 데이터가 제거됩니다. 이 절차를 시작하기 전에 전체 데이터베이스 덤프를 수행해야 합니다. 자세한 내용은 [8.6.1절. "작업 1: 이전 STA 데이터베이스 덤프"](#)를 참조하십시오.

주:

STA를 제거하려면 Oracle 설치 그룹의 구성원인 사용자로 로그인해야 합니다. Linux *root* 사용자나 슈퍼유저 권한이 있는 다른 사용자로는 STA를 제거할 수 없습니다. 자세한 내용은 [Oracle 설치 그룹](#)을 참조하십시오.

1. Oracle 설치 사용자로 로그인합니다.
2. Oracle 스토리지 홈 디렉토리로 변경합니다. 예를 들면 다음과 같습니다.

```
$ cd /Oracle
```

3. STA 설치 프로그램 이진 디렉토리로 변경합니다.

```
$ cd StorageTek_Tape_Analytics/oui/bin
```

4. 다음 명령 중 하나를 사용하여 STA 제거 프로그램을 실행합니다.
 - STA 그래픽 제거 프로그램을 사용하는 경우:

```
$ ./deinstall.sh
```

이 모드를 사용하려면 X11 디스플레이가 필요합니다. 자세한 내용은 [부록 A. STA 그래픽 설치 프로그램 및 제거 프로그램 화면 참조](#)를 참조하십시오.

- STA 자동 제거 프로그램을 사용하는 경우:

```
$ ./deinstall.sh -silent -responseFile response_file
```

여기서 *response_file*은 이전에 만든 응답 파일의 절대 경로입니다.

이 모드를 사용하려면 먼저 *silentInstallUtility.jar* 파일을 다운로드하고 설치 옵션을 지정하는 응답 파일을 만들어야 합니다. 자세한 내용은 [부록 B. STA 자동 모드 설치 프로그램 및 제거 프로그램](#)을 참조하십시오.

9.2.2. 성공적인 제거 확인

이 절차를 사용하여 제거 작업을 수행한 후 모든 STA 구성 요소가 STA 서버에서 제거되었는지 확인합니다.

1. Oracle 설치 사용자로 로그인합니다.
2. Oracle 스토리지 홈 디렉토리의 내용을 나열합니다. 이 디렉토리는 비어 있어야 합니다. 예를 들면 다음과 같습니다.

```
$ 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 복원

이 절차를 사용하여 STA를 제거한 후 재설치합니다(예: 현재 설치 복구). STA 설치 프로그램을 사용하여 현재 설치를 재설치하거나 덮어쓸 수 없습니다.

1. 현재 STA 설치에서 서비스 로그 스냅샷을 수행합니다. Oracle 고객지원센터는 생성된 서비스 로그를 사용하여 업그레이드 전에 존재하는 문제를 해결할 수 있습니다. 자세한 내용은 *STA 사용 설명서*를 참조하십시오.
2. 다음과 같이 모든 STA 서비스를 중지합니다.

```
# STA stop all
```

3. 데이터베이스 스냅샷을 수행합니다.
 - a. MySQL 서비스를 시작합니다.

```
# STA start mysql
```

- b. 백업 파일을 만듭니다.

```
# /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
```

출력은 다음과 유사합니다.

```
...
-- Retrieving view structure for table v_mdv_request_states...
-- Retrieving view structure for table version_info...
...
-- Disconnecting from localhost...
```

주:

"Can't connect to local MySQL server"가 표시되는 경우 MySQL 서버가 실행되고 있지 않는 것입니다. a 단계로 돌아가서 MySQL을 시작했는지 확인합니다.

4. 다음 단계에서는 모든 STA 파일이 제거되므로 서비스 로그 스냅샷 및 데이터베이스 스냅샷을 다른 서버로 이동합니다. 스냅샷은 다음 디렉토리에 있습니다.
 - 서비스 로그 스냅샷은 `/Oracle_storage_home/Middleware/rda/snapshots`에 있습니다. 예를 들면 `/Oracle/Middleware/rda/snapshots`일 수 있습니다.
 - 데이터베이스 스냅샷은 STA 설치 중 지정된 데이터베이스 위치에 있습니다. 예를 들면 `/dbbackup`일 수 있습니다.
5. 필요에 따라 기타 파일을 백업합니다.
6. STA를 제거합니다. 자세한 내용은 [9.2.1절. “STA 제거”](#)를 참조하십시오.
7. STA를 재설치합니다. 자세한 내용은 [3장. STA 설치](#)를 참조하십시오.
8. 다음과 같이 모든 STA 서비스를 중지합니다.

```
# STA stop all
```

9. 데이터베이스를 복원합니다. 자세한 내용은 *STA* 관리 설명서를 참조하십시오.
10. 다음과 같이 모든 STA 서비스를 시작합니다.

```
# STA start all
```

11. STA를 구성합니다. 자세한 내용은 [8.6.10.2절. “STA의 SNMP 설정 구성”](#)을 참조하십시오.

STA 그래픽 설치 프로그램 및 제거 프로그램 화면 참조

이 장은 다음과 같은 절로 구성됩니다.

- [그래픽 모드 디스플레이 요구 사항](#)
- [STA 그래픽 설치 프로그램 화면](#)
- [STA 그래픽 제거 프로그램 화면](#)

A.1. 그래픽 모드 디스플레이 요구 사항

STA 그래픽 모드 설치 프로그램 및 제거 프로그램에는 X Window System, 버전 11(X11)이 필요합니다. X11 구성은 이 설명서의 범위를 벗어나지만 다음과 같은 일반적인 지침이 적용됩니다. 자세한 정보는 시스템 관리자에게 문의하십시오.

그래픽 모드 설치 프로그램 및 제거 프로그램을 실행하려면 X11 서비스가 STA 서버에서 실행 중이며 X11 전달을 허용하도록 구성되어 있어야 합니다. Linux가 [2장. Linux 설치](#)에 설명된 대로 설치되었다면 이러한 조건은 이미 충족된 것입니다.

또한 Oracle 설치 사용자에게 대해 X11 권한 및 디스플레이가 올바르게 설정되어 있어야 합니다. 이 설정은 로컬 연결을 통해 로그인했는지 원격 연결을 통해 로그인했는지에 따라 다르게 처리됩니다.

자세한 내용은 다음 절을 참조하십시오.

- [A.1.1절. “로컬 연결”](#)
- [A.1.2절. “SSH\(보안 셸\)를 사용한 원격 연결”](#)
- [A.1.3절. “데스크탑 공유를 사용한 원격 연결”](#)
- [A.1.4절. “그래픽 디스플레이 문제 해결”](#)

주:

원격 연결에 대한 응답 시간은 사용자 네트워크 및 VPN 구성과 성능에 따라 다릅니다.

A.1.1. 로컬 연결

STA 서버에 직접 연결하려면 Oracle 설치 사용자로 로그인한 후 수동으로 `DISPLAY` 변수를 설정해야 합니다. 예를 들면 다음과 같습니다.

```
# export DISPLAY=hostname:0.0
```

Oracle 설치 사용자에게 적절한 X11 권한이 있는지도 확인해야 합니다. 지원이 필요하다면 Linux 관리자에게 문의하십시오.

A.1.2. SSH(보안 셸)를 사용한 원격 연결

X11 전달이 사용으로 설정된 SSH(보안 셸)를 사용하는 경우 로그인 사용자에게 X11 권한 및 디스플레이가 자동으로 처리됩니다. 예를 들어, 이 방법을 사용하고 *oracle* 사용자로 로그인하는 경우 STA 서버의 SSH 서비스가 *oracle* 사용자에게 X11 권한 및 디스플레이를 자동으로 설정합니다. *DISPLAY* 변수를 수동으로 설정해서는 안 됩니다.

하지만 다른 사용자(예: *root*)로 로그인한 후 *oracle*로의 *su*를 실행하는 경우 *oracle* 사용자에게 X11 권한 및 디스플레이가 올바르게 설정되지 않으므로 이 값을 수동으로 설정해야 합니다. 여기에 대한 지침은 이 설명서의 범위를 벗어납니다. 지원이 필요하다면 Linux 관리자에게 문의하십시오.

A.1.2.1. Linux 시스템에서 연결

Linux 시스템에서 X11 전달을 사용으로 설정하려면 *-x* 또는 *-Y* 옵션을 지정하여 *ssh* 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
$ ssh -X oracle@sta_server
```

A.1.2.2. Microsoft Windows PC에서 연결

PC에는 Xming, Cygwin/X 등의 X11 서버와 PuTTY, WinSCP 등의 SSH 클라이언트가 실행되고 있어야 합니다. 다음은 PuTTY를 사용하여 연결하는 절차의 예입니다.

1. PC에서 X11 서버가 실행되고 있는지 확인합니다. 필요한 경우 시스템 관리자에게 문의하십시오.
2. PuTTY를 시작한 후 다음과 같이 진행합니다.
 - a. 기본 세션 창에서 다음과 같이 입력합니다.
 - **Host Name** 필드에 STA 서버의 이름 또는 IP 주소를 입력합니다.
 - **SSH Connection type** 필드에서 **SSH**를 선택합니다.
 - b. Category 메뉴 트리에서 **Connection**, **SSH**를 차례로 확장한 후 **X11**을 선택합니다. 이 창에서 다음과 같이 선택합니다.
 - **X11 forwarding** 필드에서 **Enable X11 forwarding** 확인란을 선택합니다.
 - **Remote X11 authentication protocol** 필드에서 **MIT-Magic-Cookie-1**을 선택합니다.
 - 다른 필드는 비워 둡니다.

A.1.3. 데스크탑 공유를 사용한 원격 연결

데스크탑 공유를 통해 STA 설치 프로그램을 실행하려면 STA 서버와 사용자의 로컬 컴퓨터에 모두 데스크탑 공유 응용 프로그램이 실행되고 있어야 합니다(예: STA 서버의 VNC Server 및 로컬 컴퓨터의 VNC Viewer). 또한 로컬 컴퓨터가 VPN(가상 사설망)과 같은 개인 네트워크를 통해 STA 서버에 연결할 수 있어야 합니다.

다음은 VNC를 사용하여 연결하는 프로세스의 예입니다.

1. STA 서버에 VNC Server를 설치 및 구성합니다.
2. 로컬 컴퓨터에 VNC Viewer를 설치 및 구성합니다.
3. 개인 네트워크를 통해 STA 서버에 연결합니다. 자세한 내용은 IT 관리자에게 문의하십시오.

A.1.4. 그래픽 디스플레이 문제 해결

STA 설치 프로그램 및 제거 프로그램은 Oracle 설치 사용자에게 대해 X11이 적절히 구성되어 있는지 확인합니다. 이 필수 조건 검사가 실패하는 경우 Linux 시스템 관리자에게 지원을 요청하십시오. 다음 단계를 사용하여 문제 해결을 시도할 수 있습니다.

1. Oracle 설치 사용자로 STA 서버에 로그인한 후 현재 설치된 RPM 패키지를 표시합니다.

```
# yum list installed
```

표시된 목록에는 *xorg - x11 - util* 항목이 포함되어 있어야 합니다. 예를 들면 다음과 같습니다.

```
xorg-x11-utils.x86_64          7.5-6.e16
```

2. Oracle 설치 사용자에게 대한 현재 디스플레이 설정을 표시합니다. 예를 들면 다음과 같습니다.

```
$ echo $DISPLAY
:0.0
```

3. 디스플레이의 X11 구성이 올바른지 확인합니다. 예를 들면 다음과 같습니다.

```
$ xdpinfo -display :0.0
```

예 A.1. “올바르게 구성된 X11 디스플레이의 예”은 올바르게 구성된 디스플레이를 보여주는 명령 출력의 첫번째 부분에 대한 예입니다.

예 A.1. 올바르게 구성된 X11 디스플레이의 예

```
$ 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
...
```

예 A.2. “올바르지 구성되지 않은 X11 디스플레이의 예”는 올바르게 구성되지 않은 디스플레이의 명령 출력에 대한 몇 가지 예를 보여 줍니다.

예 A.2. 올바르게 구성되지 않은 X11 디스플레이의 예

```
$ 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 그래픽 설치 프로그램 화면

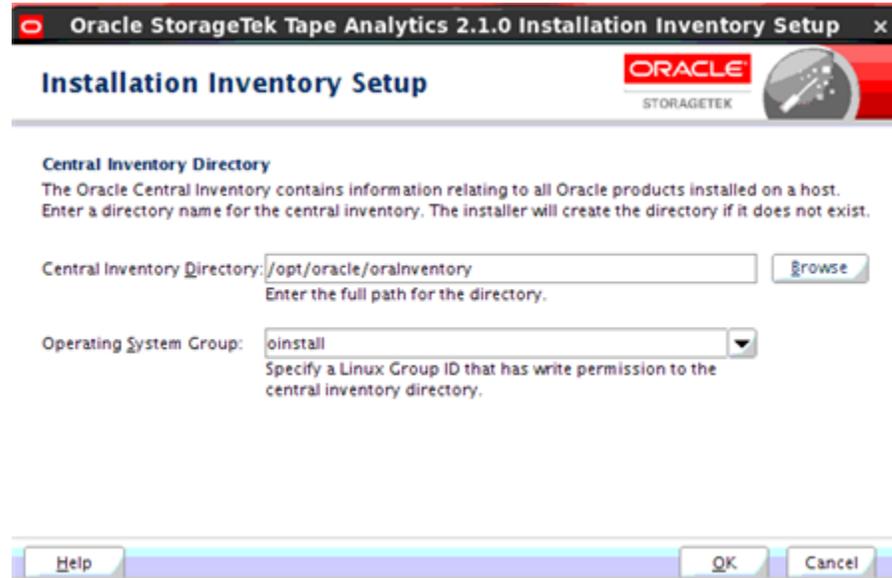
이 절에서는 STA 그래픽 설치 프로그램의 각 화면에 대한 자세한 설명을 제공합니다.

- [A.2.2절. “Welcome”](#)
- [A.2.3절. “Installation Location”](#)
- [A.2.4절. “Prerequisite Checks”](#)
- [A.2.5절. “Enter Root Password”](#)
- [A.2.6절. “Set Up DB Directories”](#)
- [A.2.7절. “Set Up Admin Accounts”](#)
 - [A.2.8절. “WebLogic Administrator”](#)
 - [A.2.9절. “STA Administrator”](#)
- [A.2.10절. “Set Up Database Accounts”](#)
 - [A.2.11절. “Database Root User”](#)
 - [A.2.12절. “Database Application User”](#)
 - [A.2.13절. “Database Reports User”](#)
 - [A.2.14절. “Database Administrator”](#)
- [A.2.15절. “Enter Communication Ports”](#)
 - [A.2.16절. “WebLogic Admin Console”](#)
 - [A.2.17절. “STA Engine”](#)
 - [A.2.18절. “STA Adapter”](#)
 - [A.2.19절. “STA UI”](#)
- [A.2.20절. “Diagnostic Agent”](#)
- [A.2.21절. “Installation Summary”](#)
- [A.2.22절. “Installation Progress”](#)
- [A.2.23절. “Configuration Progress”](#)
- [A.2.24절. “Installation Complete”](#)

주:

STA 그래픽 설치 프로그램을 실행하면 Oracle Universal Installer는 몇 가지 기본 환경 검사를 수행하면서 터미널 창에 메시지를 표시합니다. STA 그래픽 설치 프로그램을 실행하기 위한 요구 사항은 이 최소 검사보다 엄격할 수 있습니다.

A.2.1. Installation and Inventory Setup



Oracle 중앙 인벤토리 디렉토리는 이 서버에 설치된 모든 Oracle 소프트웨어의 이름 및 위치를 추적하는 데 사용됩니다. 모든 STA 설치 및 제거 로그는 자동으로 이 위치에 저장됩니다.

Oracle 설치 그룹의 다른 사용자가 이 디렉토리에 액세스할 수 있도록 이 위치는 Oracle 설치 사용자의 홈 디렉토리와 분리되어야 합니다. 홈 디렉토리에는 Oracle 설치 그룹에 대한 적절한 권한이 없을 수 있습니다.

이 화면은 Oracle Universal Installer의 일부입니다. 권장된 방법을 따라 Oracle 중앙 인벤토리 위치를 등록하는 경우 이 화면은 이 서버에 STA를 처음 설치할 때만 표시됩니다. 차후 설치 시에는 사용자에게 메시지가 표시되지 않고 자동으로 위치가 검색됩니다. 자세한 내용은 [3.6.7절. "Oracle 중앙 인벤토리 위치 등록"](#)을 참조하십시오.

A.2.1.1. 화면 필드

Inventory Directory

Oracle 중앙 인벤토리 디렉토리로 지정할 디렉토리의 이름을 입력합니다.

기본값은 `$USER_HOME/oraInventory`입니다. 절대 경로를 지정하거나 **Browse** 버튼을 눌러 기존 디렉토리를 탐색해야 합니다.

- 기존 디렉토리를 지정하는 경우 Oracle 설치 사용자에게 해당 디렉토리에 대한 전체 권한이 있어야 합니다.

- 존재하지 않는 디렉토리를 지정하는 경우 Oracle 설치 사용자에게 상위 디렉토리에 대한 전체 권한이 있다면 설치 프로그램이 이 디렉토리를 자동으로 생성합니다.

Operating System Group

Oracle 설치 그룹으로 지정할 Linux 그룹을 선택합니다. 이 그룹의 모든 구성원은 이 서버에 Oracle 소프트웨어를 설치할 수 있습니다.

메뉴에는 Oracle 설치 사용자가 속한 모든 그룹이 나열됩니다. 기본값은 Oracle 설치 사용자의 기본 그룹입니다.

A.2.1.2. 화면 관련 버튼

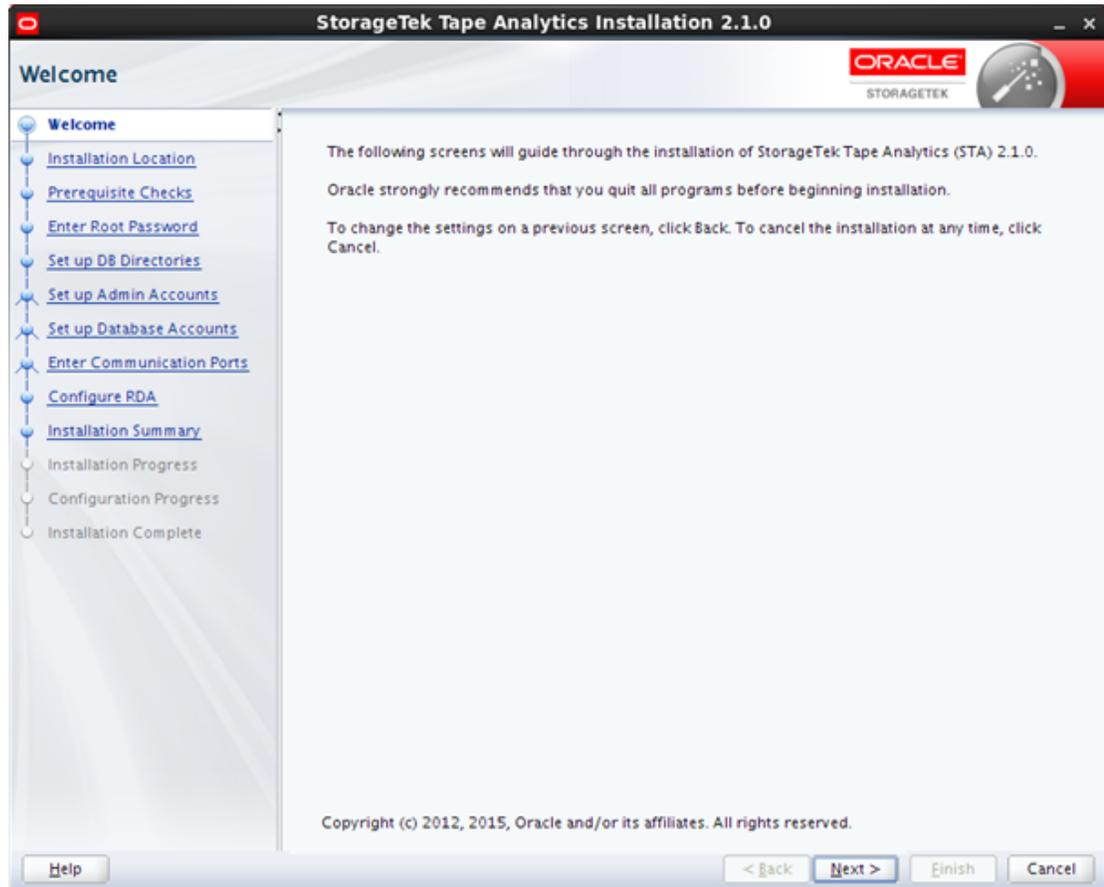
Browse

지정할 디렉토리를 탐색하려면 누릅니다.

OK

STA 설치 프로그램을 시작하려면 누릅니다. Installation Inventory Setup 창이 사라지고 잠시 기다리면 STA 설치 프로그램 시작 화면이 나타납니다.

A.2.2. Welcome



이 화면은 STA 설치 프로그램을 실행하기 위한 몇 가지 일반 정보를 제공합니다. 텍스트를 읽은 후 **Next**를 눌러 설치를 시작합니다.

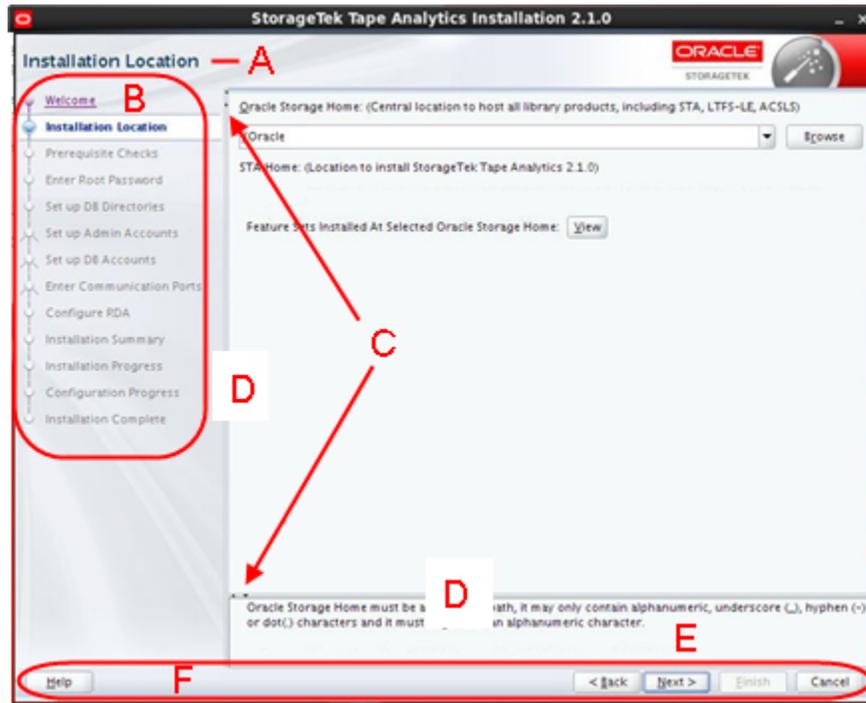
주:

모든 STA 설치 프로그램 입력 화면을 채우고 A.2.21절. "Installation Summary"에서 **Install**을 눌러야 시스템 변경 사항이 구현됩니다. 그 이전에는 언제든지 이전 화면으로 돌아가 입력 사항을 수정할 수 있습니다.

STA 설치 프로그램 화면에 대한 자세한 내용은 A.2.2.1절. "일반 설치 프로그램 화면 레이아웃"을 참조하십시오.

A.2.2.1. 일반 설치 프로그램 화면 레이아웃

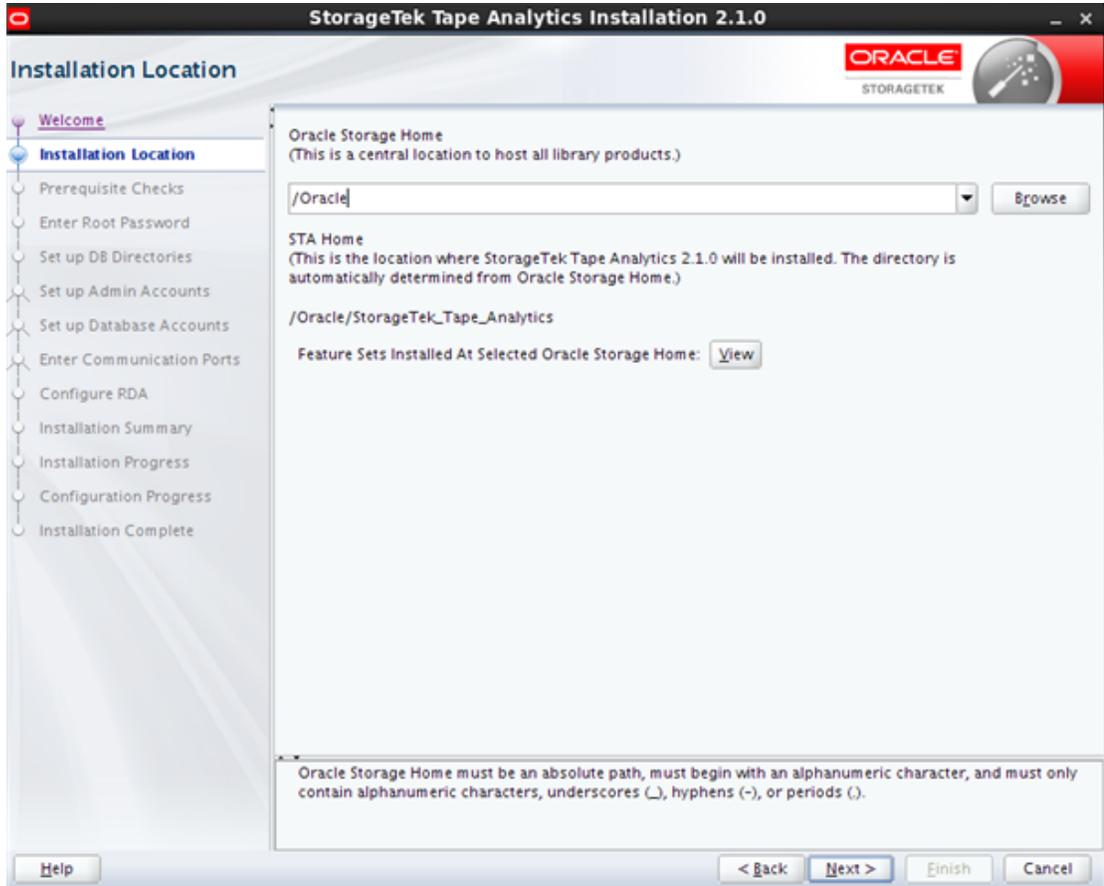
모든 STA 설치 프로그램 화면은 동일한 기본 레이아웃을 사용합니다. 아래에는 기본 부분이 표시 및 설명되어 있습니다.



항목	이름	설명
A	화면 제목	STA 설치 프로그램 화면의 제목입니다.
B	탐색 트리	설치 시퀀스에서 현재 위치를 표시합니다. 각 화면을 완료하면 화면 제목이 활성 링크가 됩니다. 활성 링크를 누르면 해당 화면으로 바로 돌아가 입력한 내용을 검토 또는 변경할 수 있습니다.
C	확장 및 축소 아이콘	탐색 트리 및 메시지 창을 숨기거나 표시하려면 누릅니다.
D	크기 조정 컨트롤 막대	누른 상태로 끌어 탐색 트리 또는 메시지 창의 크기를 조정합니다.
D	메시지 창	선택된 화면에만 포함됩니다. 해당 화면에서 수행되는 프로세스와 관련된 상태 메시지를 표시합니다.
E	공통 버튼	다음은 모든 STA 설치 프로그램 화면에 공통으로 표시되는 버튼입니다. <ul style="list-style-type: none"> • Help—화면에 대한 상황에 맞는 도움말을 표시하려면 누릅니다.

항목	이름	설명
		<ul style="list-style-type: none"> • Back—입력한 내용을 검토 또는 변경하기 위해 이전 화면으로 이동하려면 누릅니다. 한 번에 한 화면씩 설치 시작 화면까지 돌아갈 수 있습니다. • Next—필요한 내용을 입력한 후 다음 화면으로 진행하려면 누릅니다. • Finish—설치를 완료하려면 누릅니다. 이 버튼은 최종 화면에서만 활성화됩니다. • Cancel—언제든지 설치를 취소하려면 누릅니다. 설치가 수행된 부분이 있으면 설치 프로그램은 해당 설치를 롤백하고 서버를 원래 상태로 되돌립니다. 취소를 확인하는 메시지가 표시됩니다.

A.2.3. Installation Location



이 화면에서는 서버에서 STA 및 이와 연관된 Oracle 소프트웨어를 설치할 위치를 지정할 수 있습니다.

이전에 설치된 STA 버전 위에는 설치할 수 없습니다. STA가 특정 위치에 아직 설치되지 않은 것을 확인하려면 **Oracle Storage Home** 필드에 디렉토리를 입력한 후 **View** 버튼을 누릅니다.

- 해당 위치에 설치된 소프트웨어가 없으면 목록은 비어 있습니다.
- 설치된 소프트웨어가 있으면 **그림 A.1. “Oracle 스토리지 홈 목록의 예”**에 표시된 것처럼 나열됩니다.

A.2.3.1. 화면 필드

Oracle Storage Home

STA 및 이와 연관된 Oracle 소프트웨어를 설치할 디렉토리를 입력합니다. 각 소프트웨어 패키지는 이 디렉토리 내의 자체 하위 디렉토리에 설치됩니다. STA가 이미 설치된 디렉토리를 지정할 수 없습니다.

이 디렉토리에 대한 기술적인 권장 사항은 표 2.2. “권장되는 파일 시스템 레이아웃”을 참조하십시오.

이 디렉토리가 이미 존재하는지 여부에 따라 Oracle 설치 사용자 및 그룹에 다음 권한이 있어야 합니다.

- 디렉토리가 존재하는 경우 전체 권한이 있어야 합니다.
- 디렉토리가 존재하지 않는 경우 상위 디렉토리에 대한 전체 권한이 있어야 STA 설치 프로그램이 Oracle 스토리지 홈 디렉토리를 만들 수 있습니다.

절대 경로를 입력하거나 **Browse** 버튼을 눌러 지정할 디렉토리를 탐색해야 합니다.

STA Home

표시 전용입니다. STA를 설치할 Oracle 스토리지 홈 내 하위 디렉토리입니다. 이 하위 디렉토리는 이름이 *StorageTek_Tape_Analytics*로 지정되며 설치 중 자동으로 만들어집니다.

A.2.3.2. 화면 관련 버튼

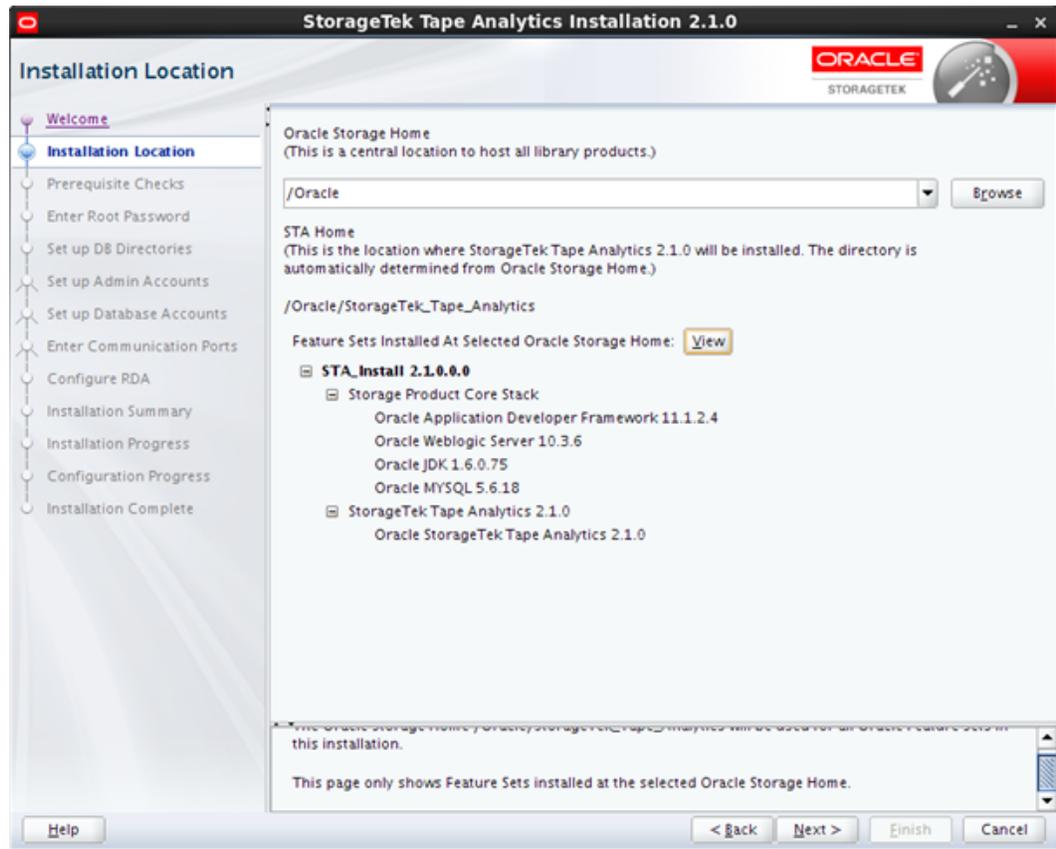
Browse

지정할 디렉토리를 탐색하려면 누릅니다.

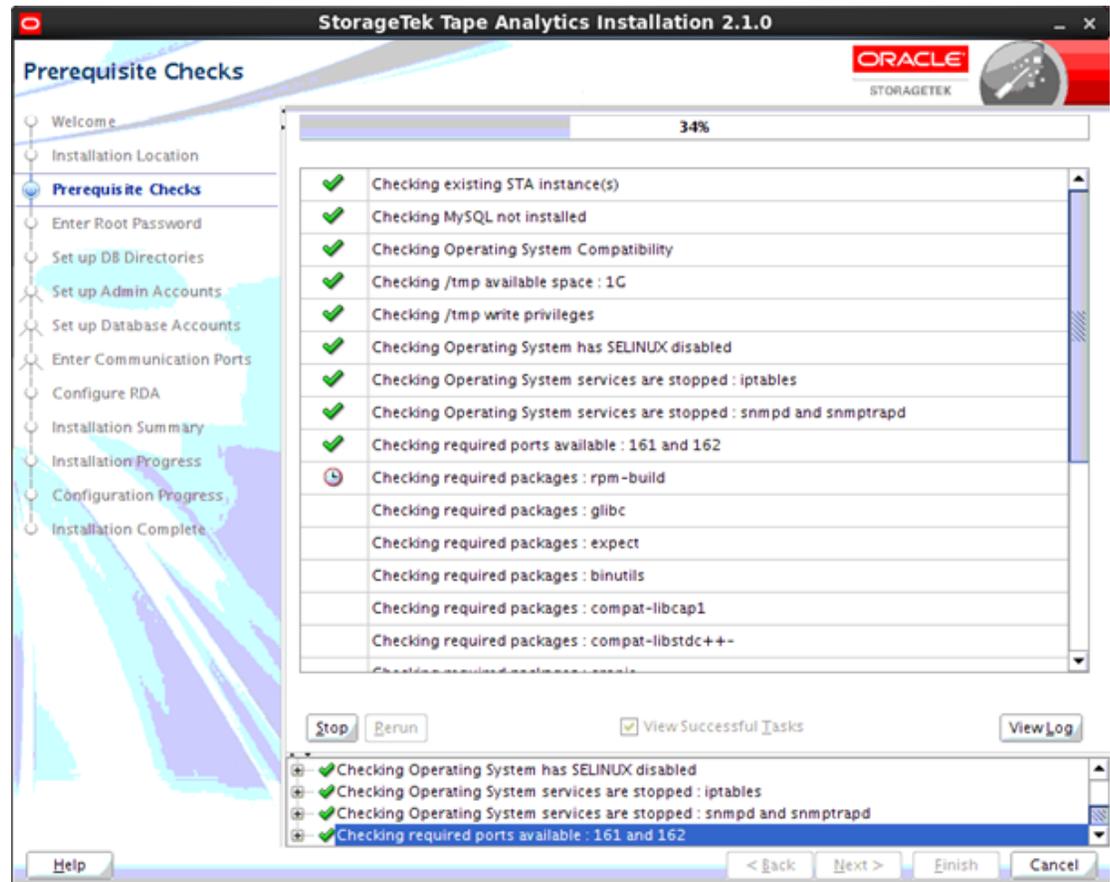
View/

지정한 Oracle 스토리지 홈 디렉토리에 현재 설치되어 있는 모든 소프트웨어 목록을 표시하려면 누릅니다. 새로 설치하는 경우 이 목록은 비어 있습니다. 그림 A.1. “Oracle 스토리지 홈 목록의 예”은 STA가 설치된 후 표시되는 화면의 예입니다.

그림 A.1. Oracle 스토리지 홈 목록의 예



A.2.4. Prerequisite Checks



설치 프로그램은 서버 환경이 필수 사항인 필수 조건 및 권장되는 필수 조건을 모두 충족하는지 확인하는 일련의 작업을 수행합니다. 이 프로세스는 몇 분 정도 걸릴 수 있습니다

각 확인 작업의 결과는 다음과 같이 나타날 수 있습니다.

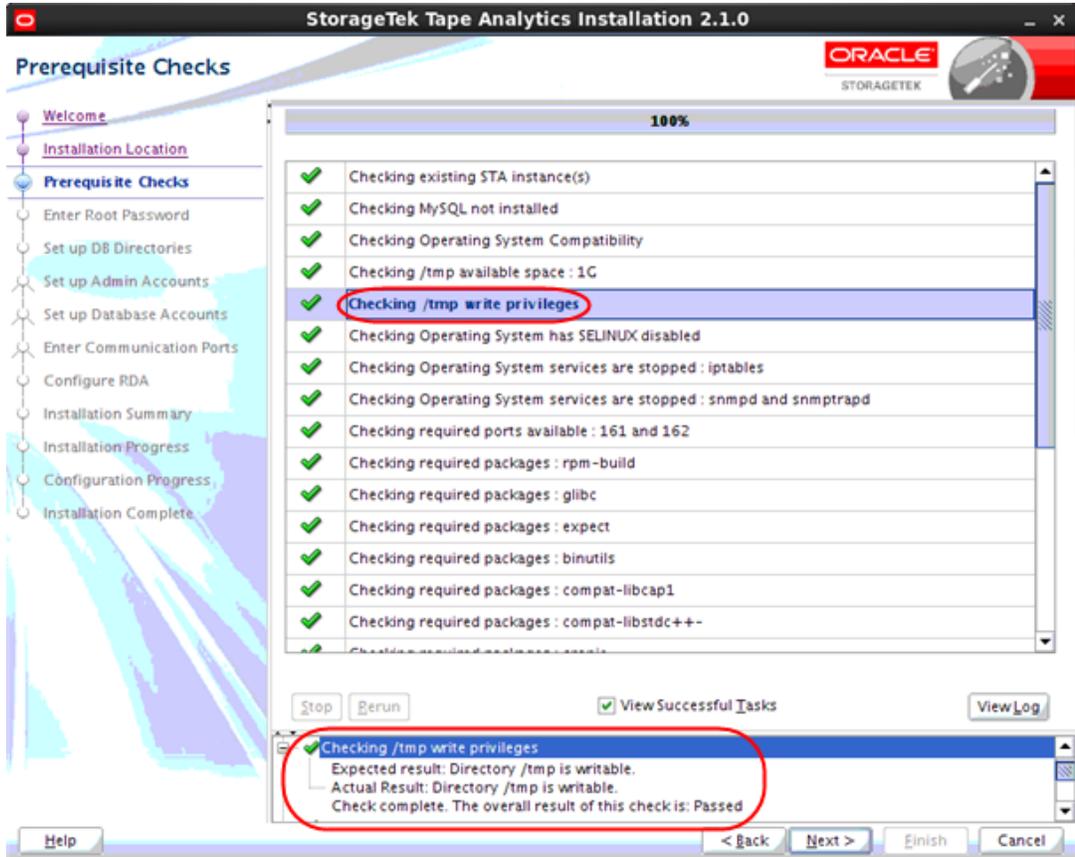
- 성공 —필수 조건 검사를 성공적으로 통과했습니다.
- 경고 —권장되는 필수 조건 검사를 통과하지 못했습니다.
- 실패 —필수 사항인 필수 조건 검사를 통과하지 못했습니다.

실패 출력이 하나라도 있는 경우 설치를 계속할 수 없습니다. 또한 계속하기 전에 모든 경고 결과를 해결할 것을 권장합니다. 설치 프로그램을 이 화면에 남겨두고 문제를 해결한 후 이 화면으로 돌아와 **Rerun**을 눌러 확인 프로세스를 다시 실행할 수 있습니다.

필수 조건의 특성에 따라 문제를 해결하기 위해 서비스를 중지하거나, 사용자 권한을 변경하거나, yum 패키지를 설치해야 할 수 있습니다. 다음 방법 중 하나를 통해 세부 정보를 확장하여 표시하면 문제를 해결하고 취할 조치를 결정하는 데 도움이 될 수 있습니다.

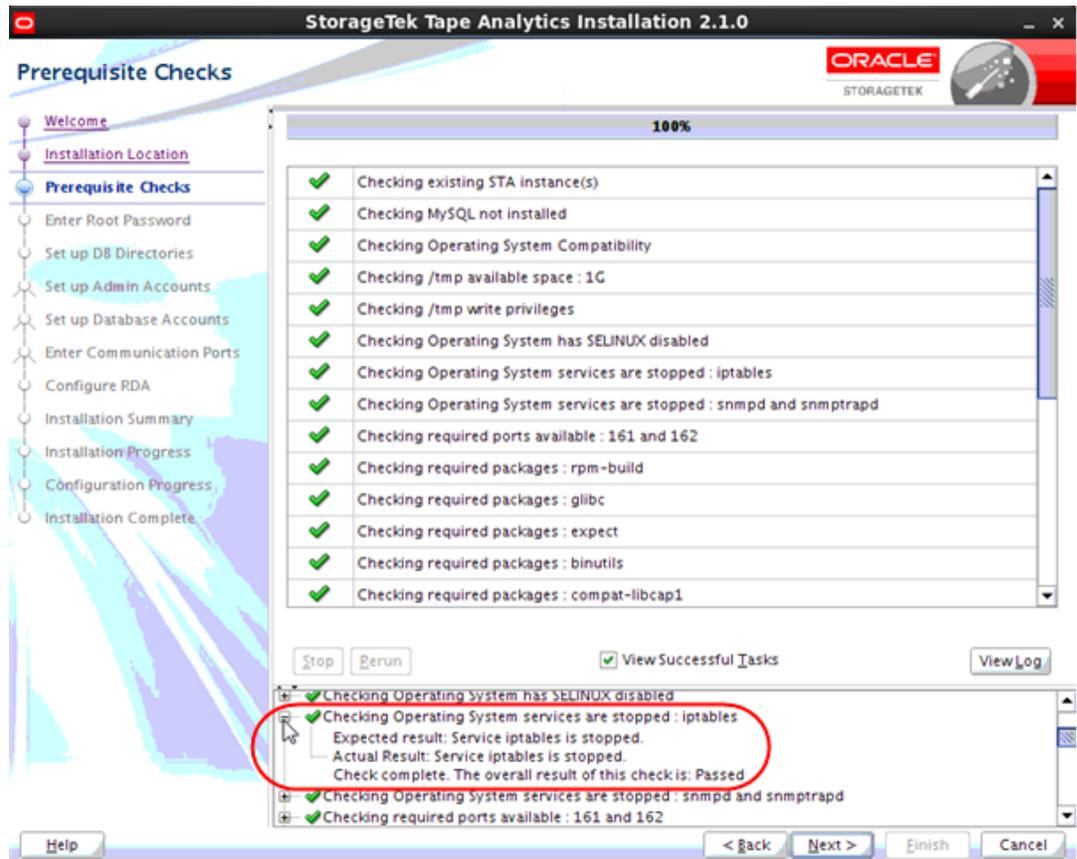
- 기본 창에서 작업을 선택합니다. 작업은 메시지 창에서 확장된 세부 정보와 함께 강조 표시됩니다. 예를 들어 그림 A.2. “기본 창에서 작업을 선택하여 표시된 작업 세부 정보”와 같이 표시됩니다.

그림 A.2. 기본 창에서 작업을 선택하여 표시된 작업 세부 정보



- 메시지 창에서 세부 정보를 표시할 작업 옆의 확장(+) 아이콘을 선택합니다. 예를 들어 그림 A.3. “확장 아이콘을 선택하여 표시된 작업 세부 정보”와 같이 합니다. 세부 정보를 다시 숨기려면 축소(-) 아이콘을 누릅니다.

그림 A.3. 확장 아이콘을 선택하여 표시된 작업 세부 정보



A.2.4.1. 화면 필드

없음

A.2.4.2. 화면 관련 버튼

Stop

현재 작업에서 확인 프로세스를 중지하려면 누릅니다. 이미 완료된 작업을 선택하여 해당 작업에 대한 세부 정보를 표시하기 위해 이 버튼을 누를 수 있습니다.

Rerun

확인 프로세스를 시작부터 다시 실행하려면 누릅니다. 이렇게 하면 STA 설치 프로그램을 종료한 후 다시 시작하지 않고도 실패 또는 경고 출력을 해결할 수 있습니다.

View Successful Tasks

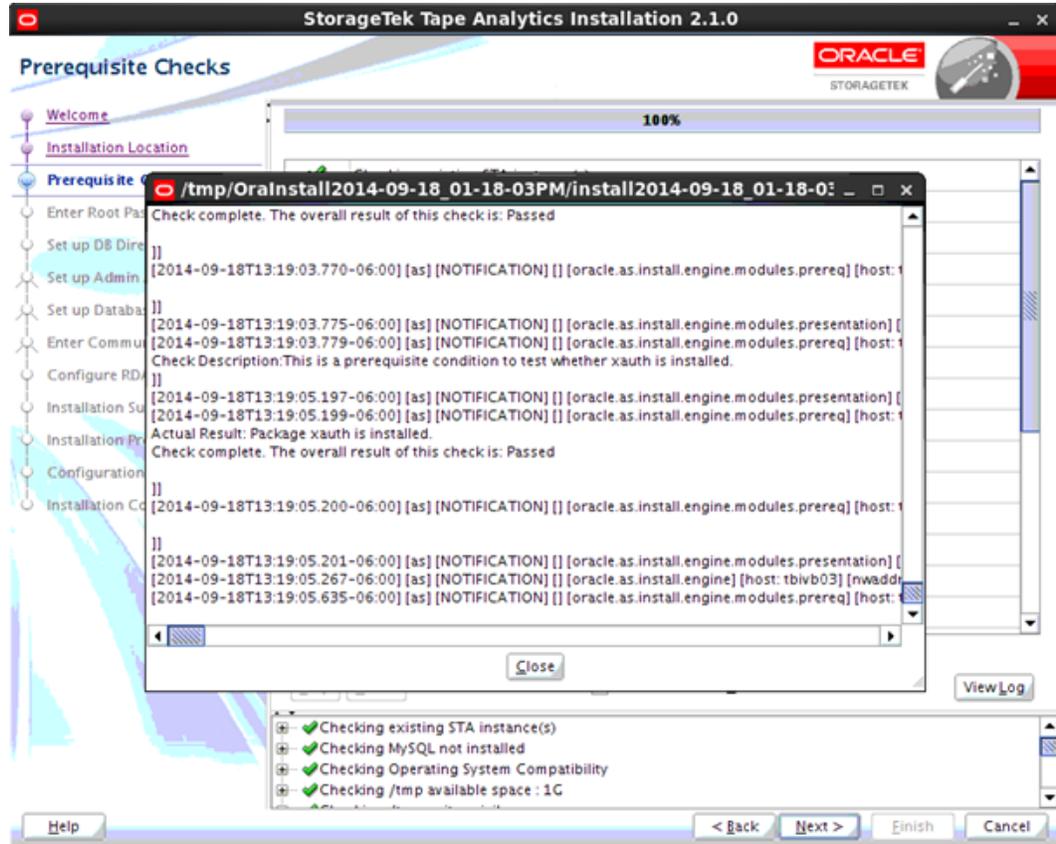
성공 출력도 표시되게 하려면 이 확인란을 선택합니다. 기본적으로 선택됩니다.

실패 또는 경고 출력만 표시하려면 확인란의 선택을 취소합니다. 이렇게 하면 성공적인 작업을 제외하여 주의가 필요한 작업에만 집중할 수 있습니다.

View Log

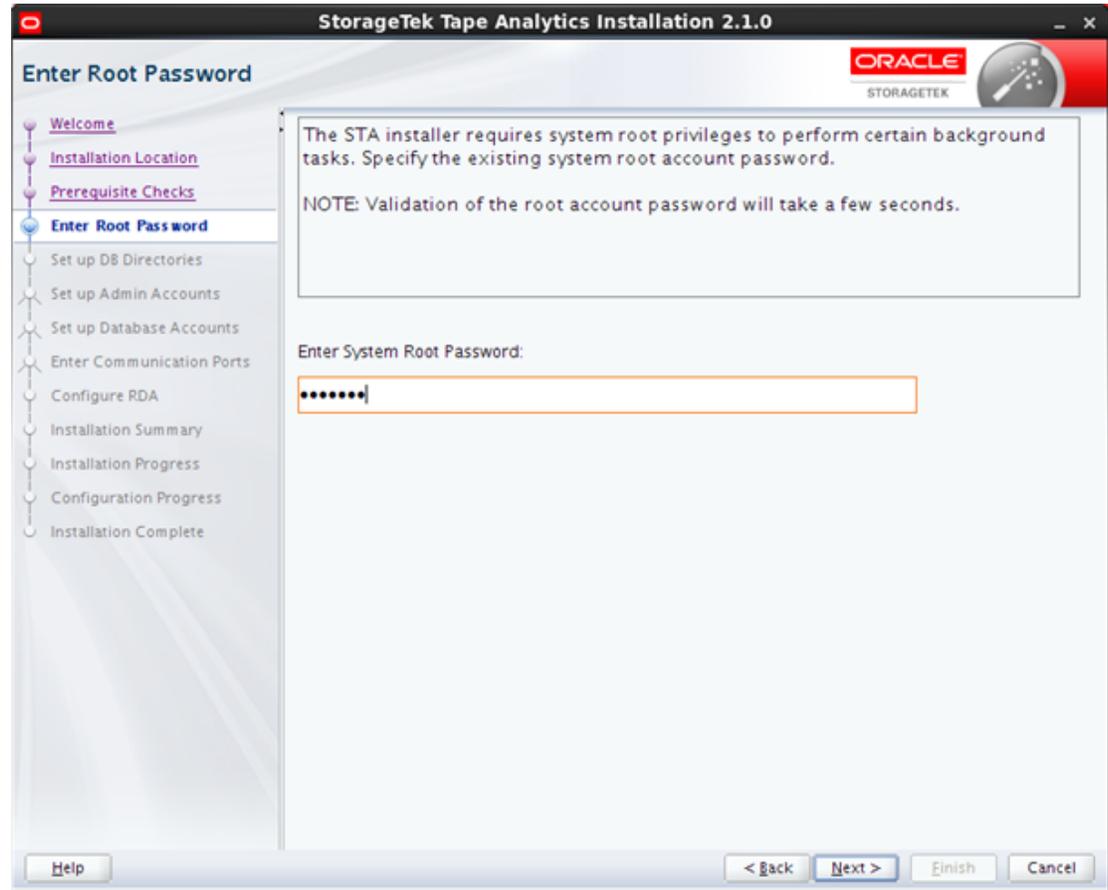
필수 검사 확인 로그를 별도의 창에 표시하려면 누릅니다. 그림 A.4. “필수 조건 확인 로그 표시의 예”는 이러한 예입니다. 로그 창을 닫으려면 **Close**를 누릅니다.

그림 A.4. 필수 조건 확인 로그 표시의 예



Linux 명령줄에서도 로그를 볼 수 있습니다. 설치 프로그램 실행 중에 로그는 */tmp* 내부의 하위 디렉토리에 보관됩니다. 자세한 내용은 3.4절. “STA 설치 및 제거 로그”를 참조하십시오.

A.2.5. Enter Root Password



STA 설치 프로그램이 설치를 수행하려면 Linux 루트로 액세스해야 합니다.

A.2.5.1. 화면 필드

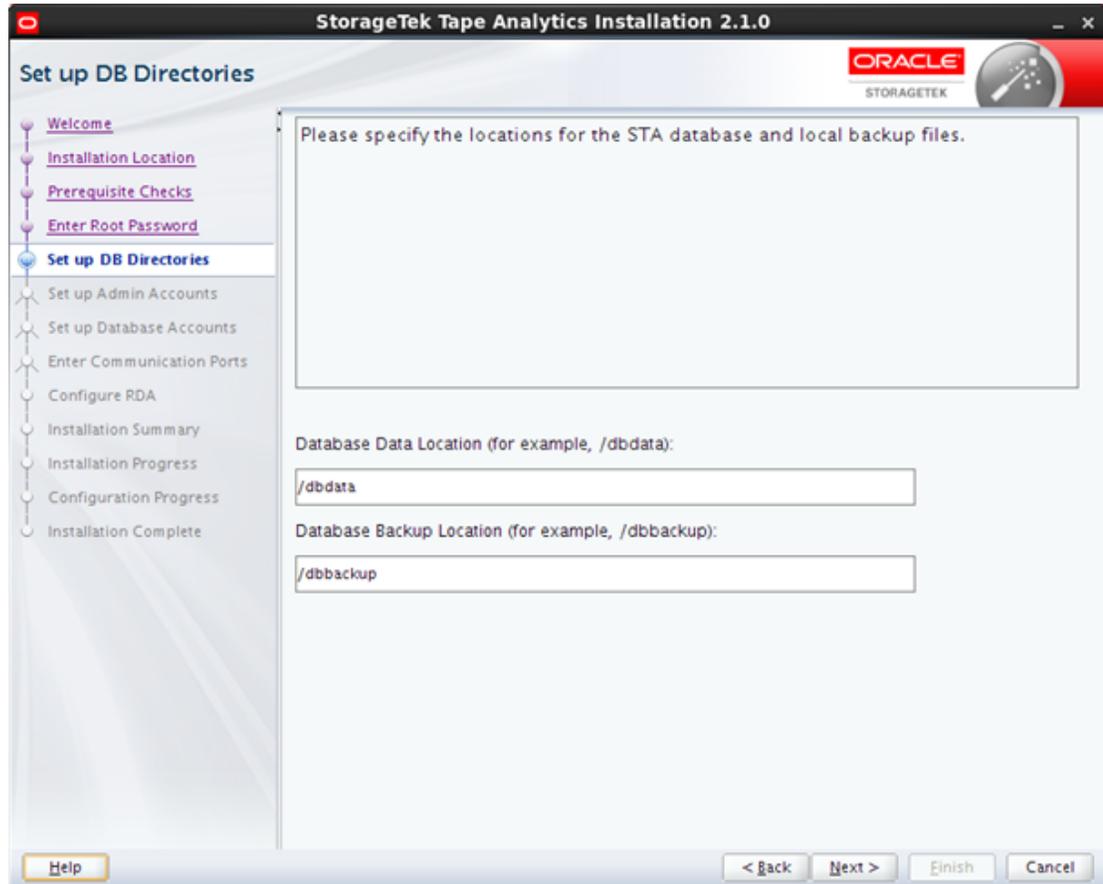
Enter Root Password

Linux 루트 사용자의 암호를 입력합니다. 항목은 입력할 때 마스크되어 표시됩니다. 암호를 검증하는 데 몇 초 정도 걸릴 수 있습니다.

A.2.5.2. 화면 관련 버튼

없음

A.2.6. Set Up DB Directories



이 화면에서는 STA 데이터베이스 및 로컬 STA 데이터베이스 백업의 위치를 지정할 수 있습니다. 디렉토리가 존재하지 않는 경우 STA 설치 프로그램이 이 디렉토리를 만듭니다.

데이터베이스 서비스 및 백업 관리에 대한 자세한 내용은 STA 관리 설명서를 참조하십시오.

A.2.6.1. 화면 필드

Database Data Location

STA 데이터베이스를 배치할 디렉토리를 입력합니다. 이 디렉토리는 **Database Backup Location**과 동일할 수 없습니다. 절대 경로를 지정해야 합니다.

지정한 디렉토리에 이미 데이터베이스 하위 디렉토리(*mysql*)가 포함되어 있으면 경고 메시지가 표시됩니다. 다른 데이터베이스 위치를 지정할 수도 있고 현재 항목을 수락할 수도 있는데, 후자의 경우 STA 설치 중 해당 데이터베이스 하위 디렉토리가 제거됩니다.

Database Backup Location

서버에서 STA 데이터베이스 백업을 배치할 디렉토리를 입력합니다. 이 디렉토리는 **Database Data Location**과 동일할 수 없습니다. 절대 경로를 지정해야 합니다.

지정한 디렉토리에 이미 데이터베이스 백업 하위 디렉토리(*local*)가 포함되어 있으면 경고 메시지가 표시됩니다. 다른 백업 위치를 지정할 수도 있고 현재 항목을 수락할 수도 있는데, 후자의 경우 STA 설치 중 해당 백업 하위 디렉토리가 제거됩니다.

A.2.6.2. 화면 관련 버튼

없음

A.2.7. Set Up Admin Accounts



이 화면에서는 다음 두 화면에서 정의할 정보의 유형을 설명합니다. 텍스트를 읽은 후 **Next**를 눌러 계속 진행합니다.

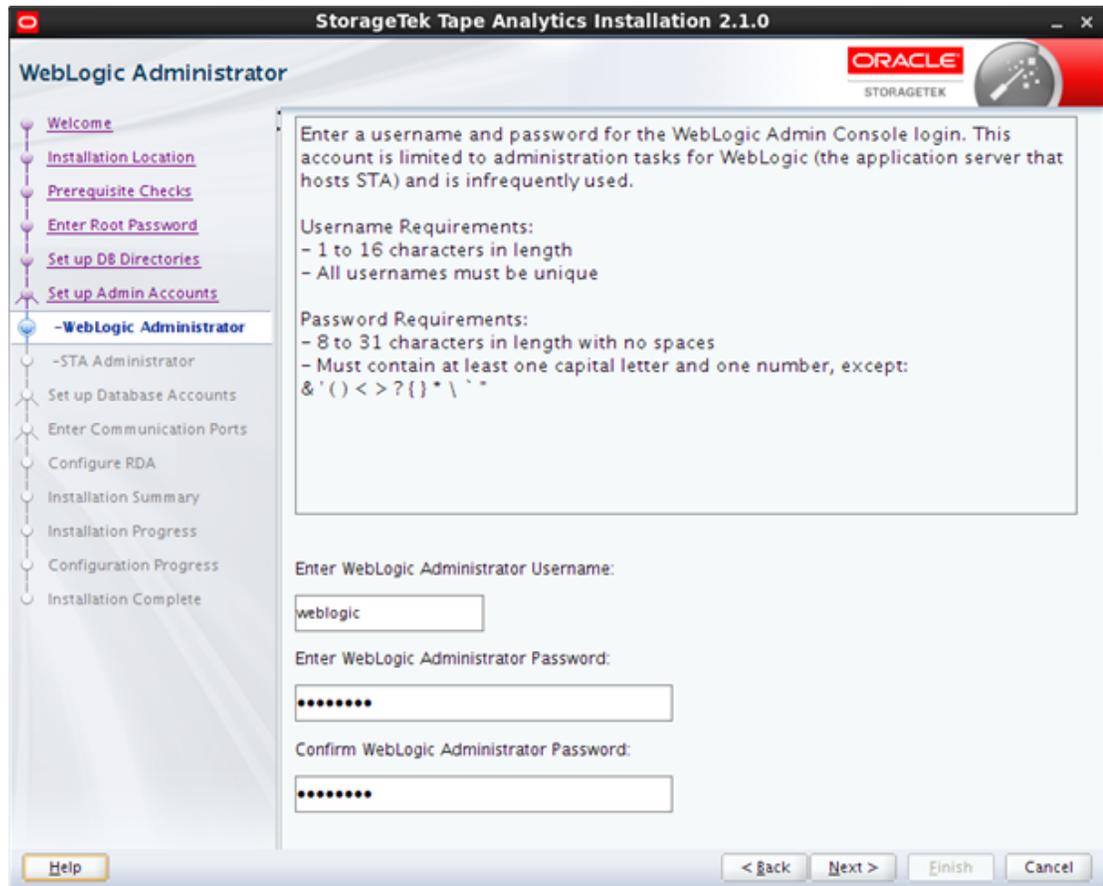
A.2.7.1. 화면 필드

없음

A.2.7.2. 화면 관련 버튼

없음

A.2.8. WebLogic Administrator



WebLogic은 STA를 호스트하는 응용 프로그램 서버입니다. WebLogic 관리자 계정을 통해 WebLogic 관리 콘솔에 로그인하여 WebLogic Server를 구성하고 관리할 수 있습니다. 이 계정은 자주 사용되지 않습니다.

이 계정은 설치 중 사용자가 지정한 자격 증명을 사용하여 만들어집니다.

주의:

이 계정 자격 증명을 잘 기록해 두십시오. 잃어버리면 WebLogic 관리 콘솔에 로그인할 수 없으며 STA를 재설치해야 합니다.

사이트 보안을 유지하기 위해 사용자 이름 및 암호는 사전 구성되거나 하드 코딩되지 않습니다.

A.2.8.1. 화면 필드

Enter Username

WebLogic 관리자 계정에 지정할 이름을 입력합니다.

사용자 이름 요구 사항은 다음과 같습니다.

- 길이가 1~16자여야 합니다.

- 모든 사용자 이름은 고유해야 합니다.

Enter Password

이 계정에 지정할 암호를 입력합니다. 항목은 입력할 때 마스크되어 표시됩니다.

암호 요구 사항은 다음과 같습니다.

- 길이가 8~31자여야 합니다.
- 최소한 숫자 1개와 대문자 1개를 포함해야 합니다.
- 공백을 포함할 수 없습니다.
- 다음 특수 문자를 포함할 수 없습니다.

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

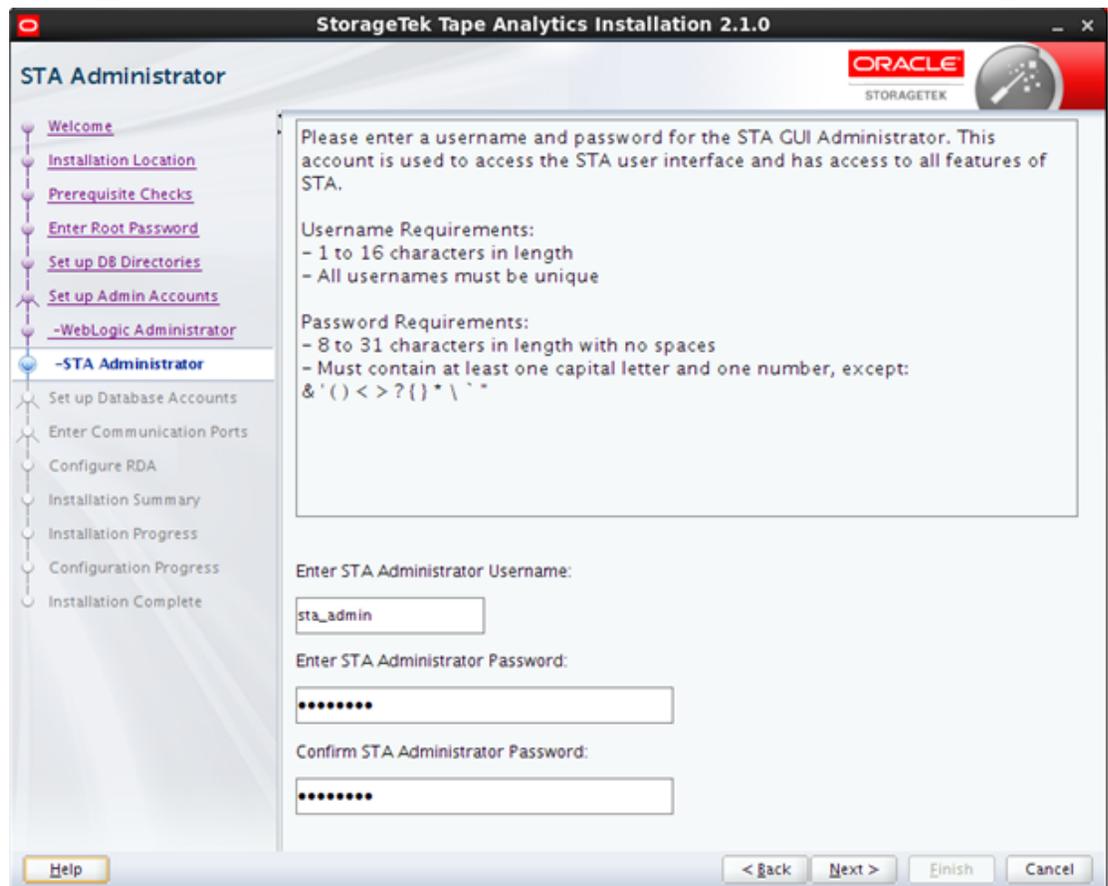
Confirm Password

올바르게 입력했는지 확인하기 위해 암호를 다시 입력합니다.

A.2.8.2. 화면 관련 버튼

없음

A.2.9. STA Administrator



STA Administrator 계정을 사용하여 STA 사용자 인터페이스에 로그인합니다. 이 사용자는 STA 응용 프로그램에 대한 관리자 권한을 가지고 있으므로 모든 STA 화면에 액세스할 수 있습니다.

이 계정은 설치 중 사용자가 지정한 자격 증명을 사용하여 만들어집니다.

주의:

이 계정 자격 증명을 잘 기록해 두십시오. 잃어버리면 STA 사용자 인터페이스에 로그인할 수 없습니다.

사이트 보안을 유지하기 위해 사용자 이름 및 암호는 사전 구성되거나 하드 코딩되지 않습니다.

A.2.9.1. 화면 필드

Enter Username

STA Administrator에 지정할 사용자 이름을 입력합니다.

사용자 이름 요구 사항은 다음과 같습니다.

- 길이가 1~16자여야 합니다.
- 모든 사용자 이름은 고유해야 합니다.

Enter Password

이 계정에 지정할 암호를 입력합니다. 항목은 입력할 때 마스크되어 표시됩니다.

암호 요구 사항은 다음과 같습니다.

- 길이가 8~31자여야 합니다.
- 최소한 숫자 1개와 대문자 1개를 포함해야 합니다.
- 공백을 포함할 수 없습니다.
- 다음 특수 문자를 포함할 수 없습니다.

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

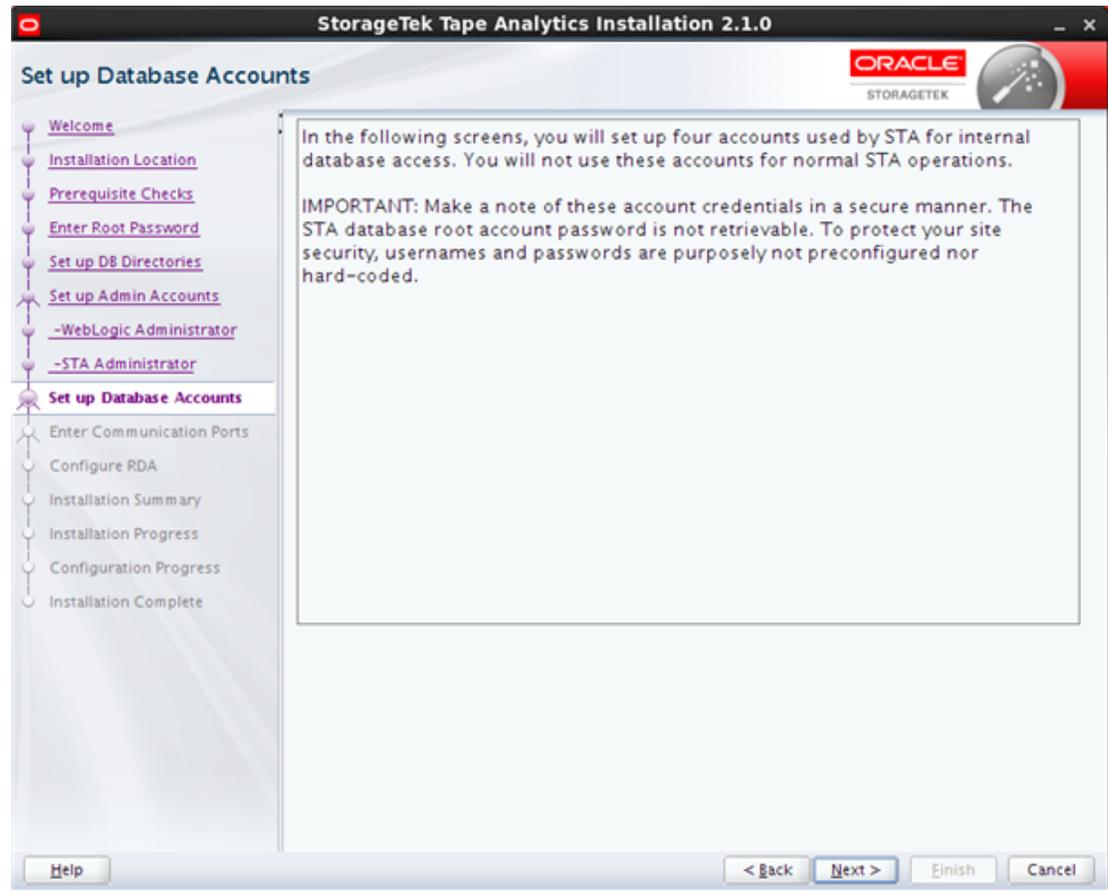
Confirm Password

올바르게 입력했는지 확인하기 위해 암호를 다시 입력합니다.

A.2.9.2. 화면 관련 버튼

없음

A.2.10. Set Up Database Accounts



이 화면에서는 다음 4개 화면에서 정의할 정보의 유형을 설명합니다. 텍스트를 읽은 후 **Next**를 눌러 계속 진행합니다.

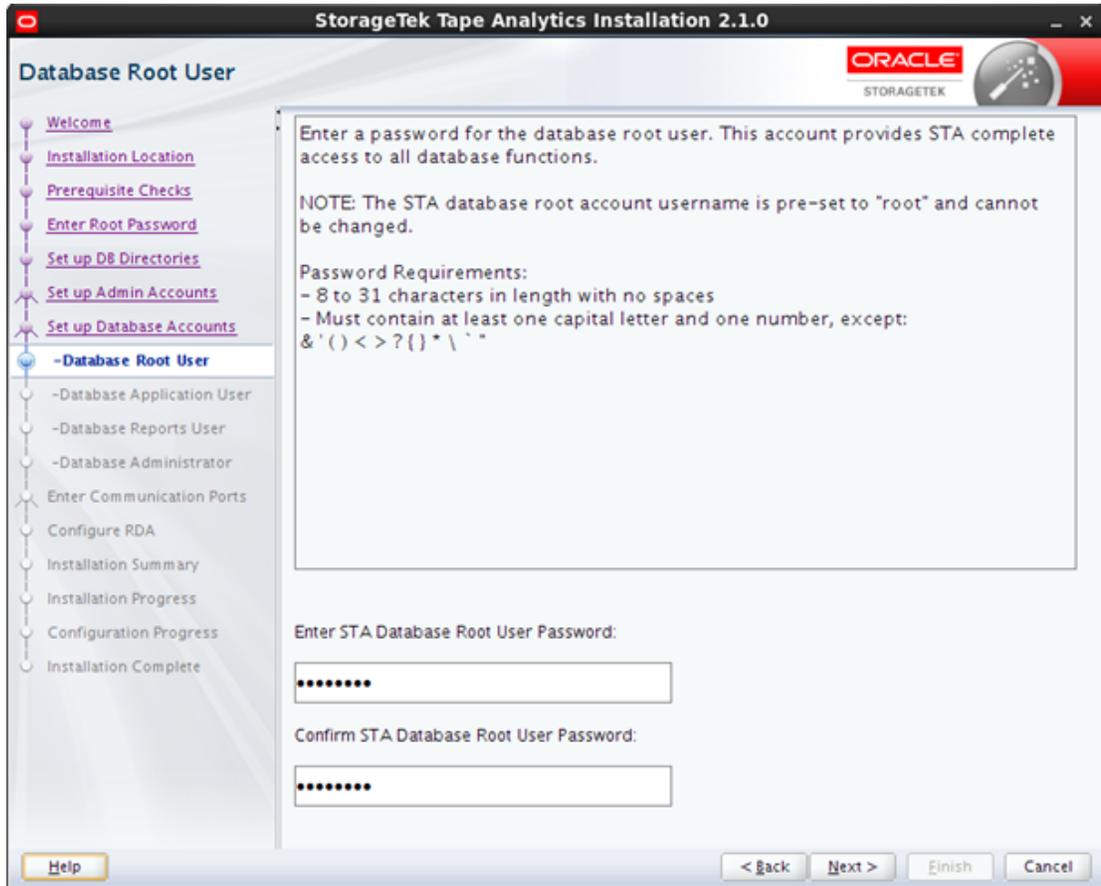
A.2.10.1. 화면 필드

없음

A.2.10.2. 화면 관련 버튼

없음

A.2.11. Database Root User



STA 데이터베이스 루트 사용자는 STA 데이터베이스를 소유합니다. 이 계정은 STA 응용 프로그램이 데이터베이스를 만들 때 내부적으로 사용하며 모든 데이터베이스 테이블에 대한 전체 액세스 권한을 제공합니다. 일반적인 STA 작업에는 이 계정을 사용하지 않습니다.

이 계정에 대한 사용자 이름은 자동으로 *root*로 설정되며 변경할 수 없습니다. 이 계정은 MySQL 계정으로 Linux 루트 사용자와 별개의 계정입니다. 이 계정은 설치 중 사용자가 지정하는 자격 증명을 사용하여 만들어집니다.

주:

이 계정 자격 증명을 잘 기록해 두십시오.

사이트 보안을 유지하기 위해 사용자 이름 및 암호는 사전 구성되거나 하드 코딩되지 않습니다.

A.2.11.1. 화면 필드

Enter Password

STA 데이터베이스 루트 사용자에게 지정할 암호를 입력합니다. 항목은 입력할 때 마스크되어 표시됩니다.

암호 요구 사항은 다음과 같습니다.

- 길이가 8~31자여야 합니다.
- 최소한 숫자 1개와 대문자 1개를 포함해야 합니다.
- 공백을 포함할 수 없습니다.
- 다음 특수 문자를 포함할 수 없습니다.

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

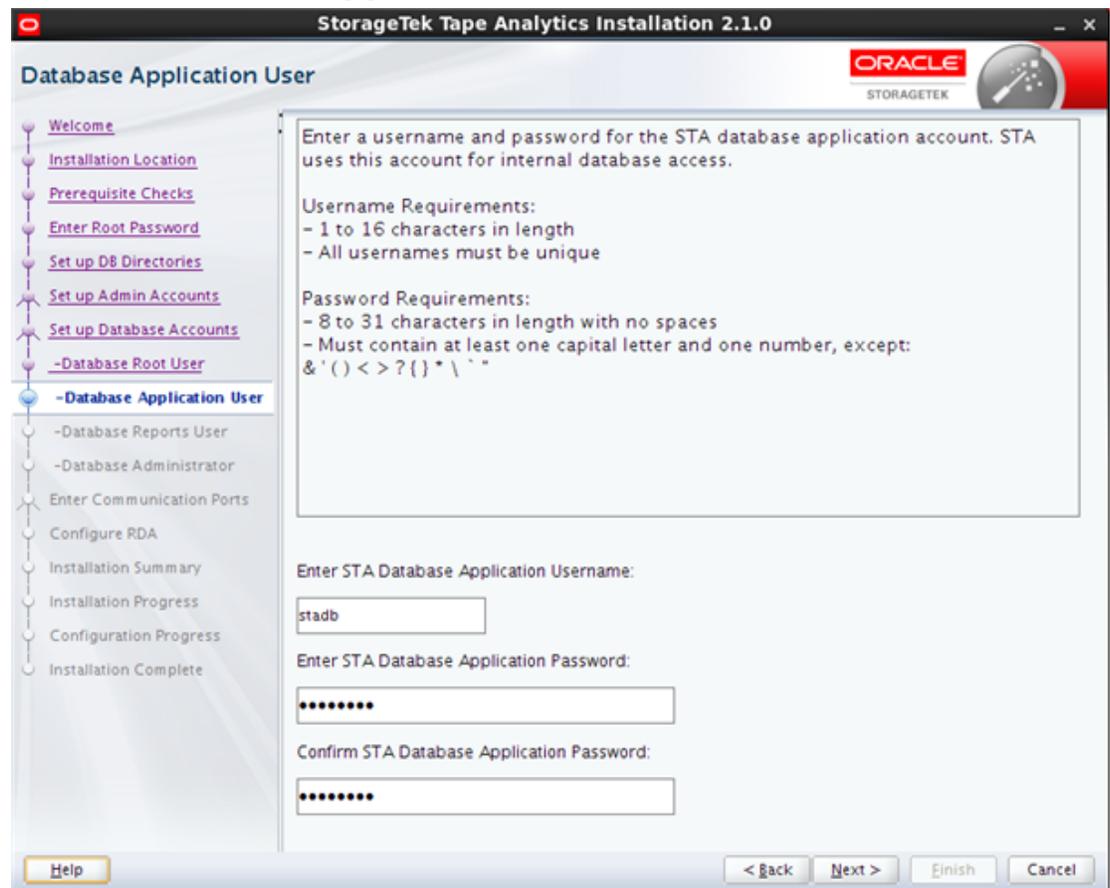
Confirm Password

올바르게 입력했는지 확인하기 위해 암호를 다시 입력합니다.

A.2.11.2. 화면 관련 버튼

없음

A.2.12. Database Application User



데이터베이스 응용 프로그램 계정은 STA 응용 프로그램이 STA 데이터베이스에 연결하여 업데이트할 때 내부적으로 사용하는 MySQL 계정입니다. 이 계정은 모든 데이터베이스 테이블에 대한 만들기, 업데이트, 삭제 및 읽기 액세스 권한을 제공합니다. 일반적인 STA 작업에는 이 계정을 사용하지 않습니다.

이 계정은 설치 중 사용자가 지정하는 자격 증명을 사용하여 만들어집니다.

주:

이 계정 자격 증명을 잘 기록해 두십시오.

사이트 보안을 유지하기 위해 사용자 이름 및 암호는 사전 구성되거나 하드 코딩되지 않습니다.

A.2.12.1. 화면 필드

Enter Username

STA 데이터베이스 응용 프로그램 계정에 지정할 이름을 입력합니다(예: *stadb*).

사용자 이름 요구 사항은 다음과 같습니다.

- 길이가 1~16자여야 합니다.
- 모든 사용자 이름은 고유해야 합니다.

Enter Password

STA 데이터베이스 응용 프로그램 계정에 지정할 암호를 입력합니다. 항목은 입력할 때 마스크되어 표시됩니다.

암호 요구 사항은 다음과 같습니다.

- 길이가 8~31자여야 합니다.
- 최소한 숫자 1개와 대문자 1개를 포함해야 합니다.
- 공백을 포함할 수 없습니다.
- 다음 특수 문자를 포함할 수 없습니다.

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

Confirm Password

올바르게 입력했는지 확인하기 위해 암호를 다시 입력합니다.

A.2.12.2. 화면 관련 버튼

없음

A.2.13. Database Reports User

StorageTek Tape Analytics Installation 2.1.0

Database Reports User

Enter a username and password for the STA database reports account. STA uses this account for internal database access.

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 STA Database Reports Username:

Enter STA Database Reports Password:

Confirm STA Database Reports Password:

Buttons: < Back, Next >, Finish, Cancel

STA 데이터베이스 보고 계정은 STA 이외의 응용 프로그램 및 타사 응용 프로그램이 STA 데이터베이스에 연결할 때 사용하는 MySQL 계정입니다. 이 계정은 선택한 데이터베이스 테이블에 대한 읽기 전용 액세스 권한을 제공합니다. 일반적인 STA 작업에는 이 계정을 사용하지 않습니다.

이 계정은 설치 중 사용자가 지정하는 자격 증명을 사용하여 만들어집니다.

주:

이 계정 자격 증명을 잘 기록해 두십시오.

사이트 보안을 유지하기 위해 사용자 이름 및 암호는 사전 구성되거나 하드 코딩되지 않습니다.

A.2.13.1. 화면 필드

Enter Username

STA 데이터베이스 보고 계정에 지정할 이름을 입력합니다(예: *starpt*).

사용자 이름 요구 사항은 다음과 같습니다.

- 길이가 1~16자여야 합니다.

- 모든 사용자 이름은 고유해야 합니다.

Enter Password

이 계정에 지정할 암호를 입력합니다. 항목은 입력할 때 마스크되어 표시됩니다.

암호 요구 사항은 다음과 같습니다.

- 길이가 8~31자여야 합니다.
- 최소한 숫자 1개와 대문자 1개를 포함해야 합니다.
- 공백을 포함할 수 없습니다.
- 다음 특수 문자를 포함할 수 없습니다.

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

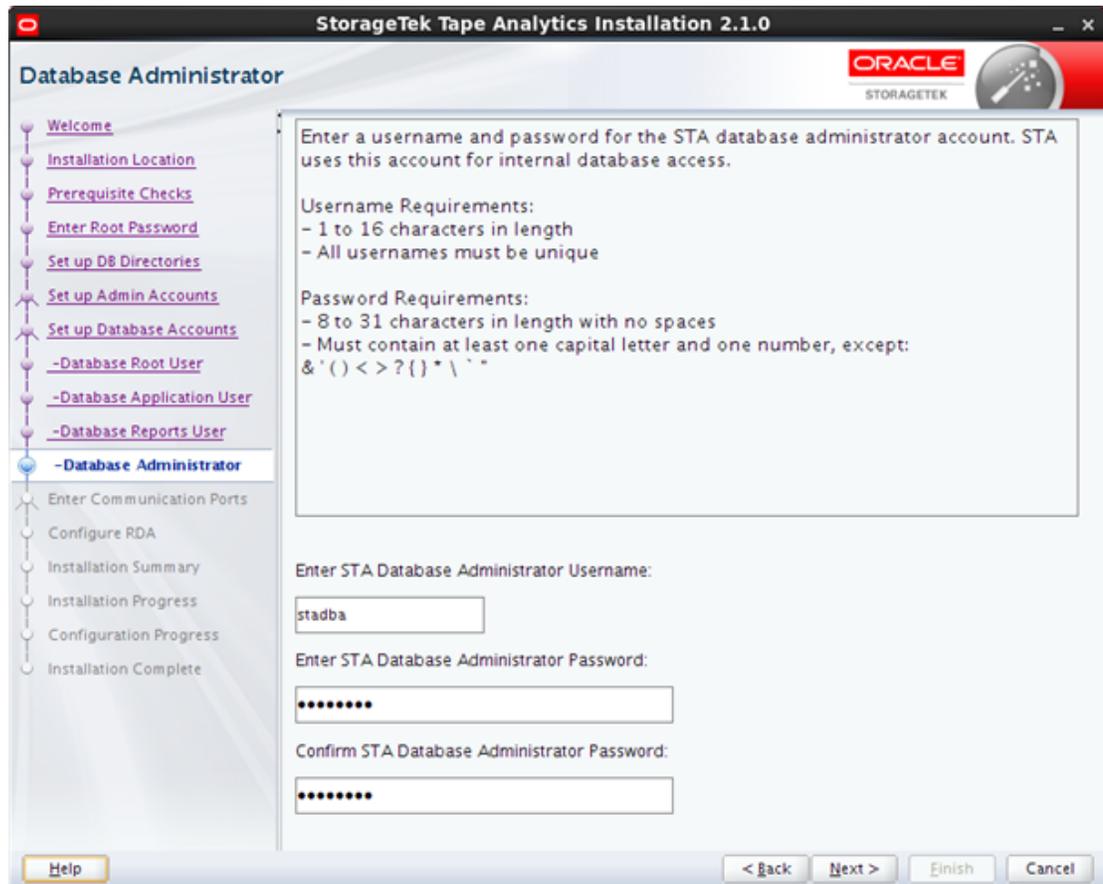
Confirm Password

올바르게 입력했는지 확인하기 위해 암호를 다시 입력합니다.

A.2.13.2. 화면 관련 버튼

없음

A.2.14. Database Administrator



STA 데이터베이스 관리자 계정은 STA 관리 및 모니터링 유틸리티가 STA 데이터베이스에 연결하여 일정이 잡힌 백업을 구성 및 실행하기 위해 내부적으로 사용하는 MySQL 계정입니다. 이 계정은 모든 데이터베이스 테이블에 대해 "grant" 옵션 이외의 전체 액세스 권한을 제공합니다. 일반적인 STA 작업에는 이 계정을 사용하지 않습니다.

이 계정은 설치 중 사용자가 지정하는 자격 증명을 사용하여 만들어집니다.

주:

이 계정 자격 증명을 잘 기록해 두십시오.

사이트 보안을 유지하기 위해 사용자 이름 및 암호는 사전 구성되거나 하드 코딩되지 않습니다.

A.2.14.1. 화면 필드

Enter Username

STA 데이터베이스 관리자 계정에 지정할 이름을 입력합니다(예: *stadba*).

사용자 이름 요구 사항은 다음과 같습니다.

- 길이가 1~16자여야 합니다.
- 모든 사용자 이름은 고유해야 합니다.

Enter Password

이 계정에 지정할 암호를 입력합니다. 항목은 입력할 때 마스크되어 표시됩니다.

암호 요구 사항은 다음과 같습니다.

- 길이가 8~31자여야 합니다.
- 최소한 숫자 1개와 대문자 1개를 포함해야 합니다.
- 공백을 포함할 수 없습니다.
- 다음 특수 문자를 포함할 수 없습니다.

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

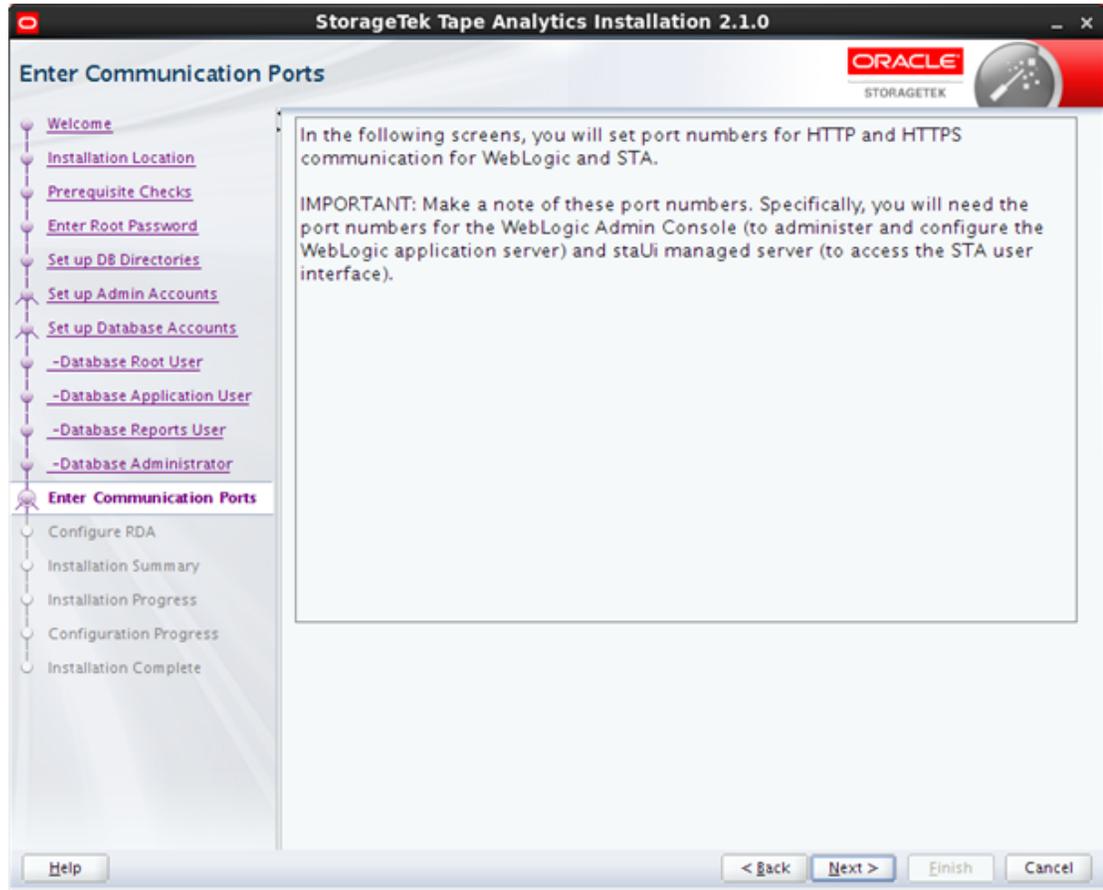
Confirm Password

올바르게 입력했는지 확인하기 위해 암호를 다시 입력합니다.

A.2.14.2. 화면 관련 버튼

없음

A.2.15. Enter Communication Ports



이 화면에서는 다음 4개 화면에서 정의할 정보의 유형을 설명합니다. 텍스트를 읽은 후 **Next**를 눌러 계속 진행합니다.

구성 가능한 내부와 외부 WebLogic 및 STA 포트에 값을 제공합니다. 해당 포트는 설치 중 사용자가 지정하는 값으로 구성되고 사용으로 설정됩니다. 지정하는 포트 번호는 고유해야 하며 포트는 사용 가능하고 STA에서 전용으로 사용하도록 유지되어야 합니다.

주:

이 화면을 완료하기 전에 네트워크 관리자에게 올바른 포트 번호 값을 확인하십시오. STA가 일단 설치되면 STA를 제거하고 재설치하지 않고는 이 포트 번호를 변경할 수 없습니다.

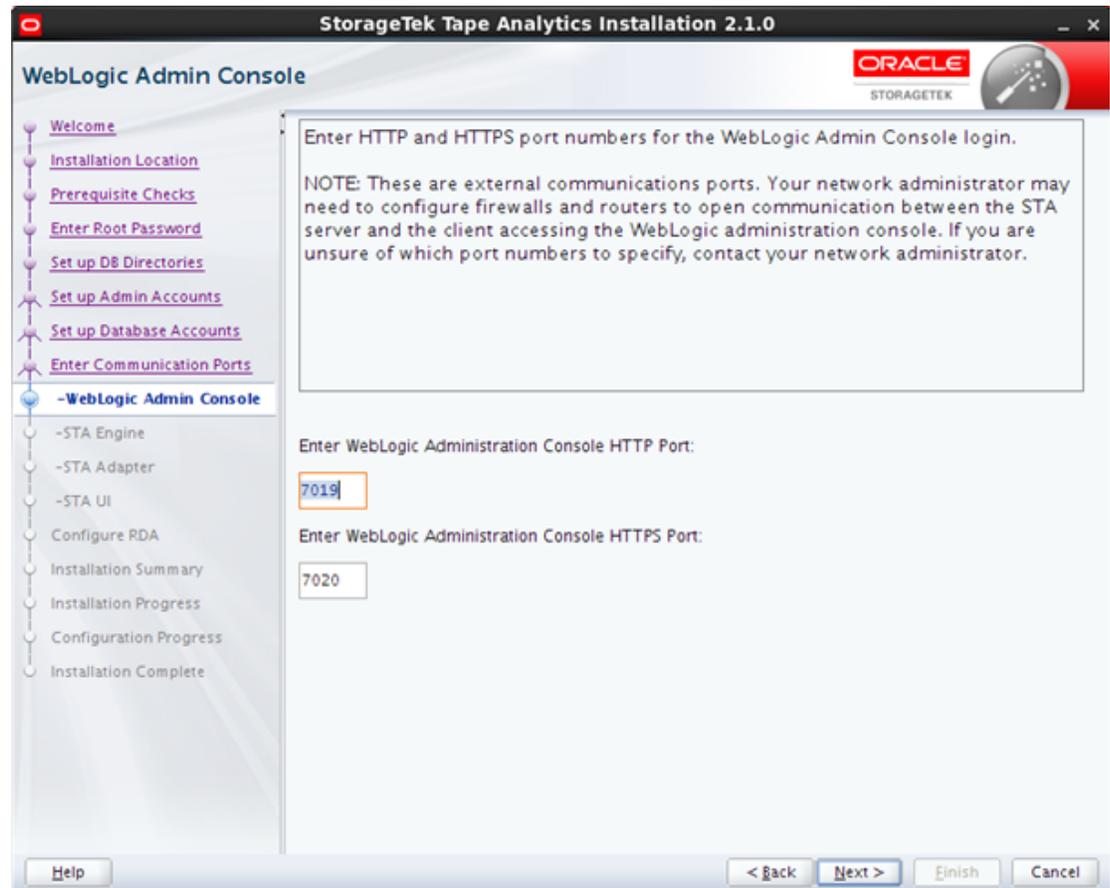
A.2.15.1. 화면 필드

없음

A.2.15.2. 화면 관련 버튼

없음

A.2.16. WebLogic Admin Console



WebLogic 응용 프로그램 서버를 관리하고 구성하는 데 사용되는 WebLogic 관리자 콘솔에 로그인하여 WebLogic 관리자 콘솔 포트 번호를 지정합니다.

주:

이 포트는 외부 통신 포트입니다. 네트워크 관리자는 STA 서버와 WebLogic 관리 콘솔에 액세스하는 클라이언트 사이에 통신을 열기 위해 방화벽 및 라우터를 구성해야 할 수 있습니다.

주:

이 포트 번호를 잘 기록해 두십시오. STA가 일단 설치되면 이 포트 번호를 변경할 수 없습니다.

사이트 보안을 유지하기 위해 이 번호는 사전 구성되거나 하드 코딩되지 않습니다.

A.2.16.1. 화면 필드

Enter HTTP Port

WebLogic 관리자 콘솔 로그인에 대한 비보안 액세스에 사용할 HTTP 포트 번호를 입력합니다. 대개 이 포트 번호는 7019입니다.

포트 번호는 사용 가능하며 고유해야 합니다.

Enter HTTPS Port

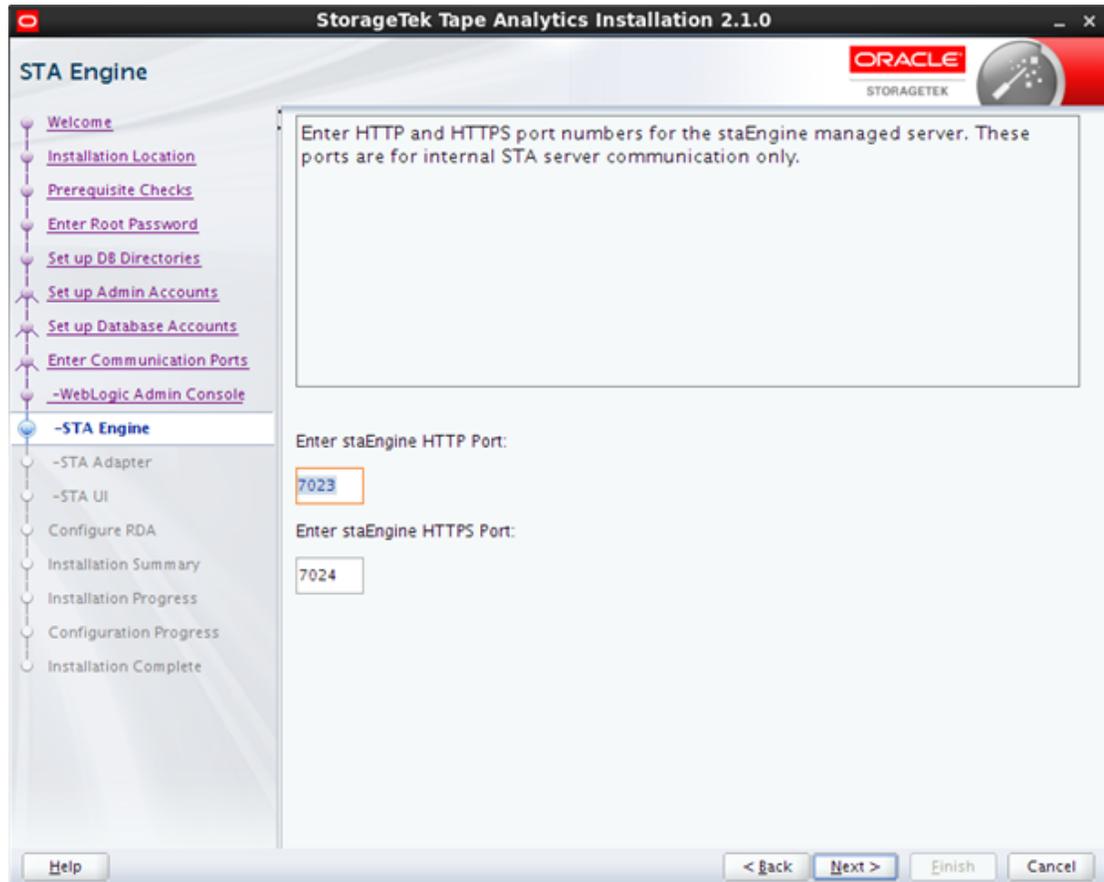
WebLogic 관리자 콘솔 로그인에 대한 보안 액세스에 사용할 HTTPS 포트 번호를 입력합니다. 대개 이 포트 번호는 7020입니다.

포트 번호는 사용 가능하며 고유해야 합니다.

A.2.16.2. 화면 관련 버튼

없음

A.2.17. STA Engine



staEngine 관리 서버 포트는 내부 STA 서버 통신용으로만 사용됩니다.

주:

이 포트 번호를 잘 기록해 두십시오. STA가 일단 설치되면 이 포트 번호를 변경할 수 없습니다.

사이트 보안을 유지하기 위해 이 번호는 사전 구성되거나 하드 코딩되지 않습니다.

A.2.17.1. 화면 필드

Enter HTTP Port

staEngine 관리 서버에 대한 비보안 액세스에 사용할 HTTP 포트 번호를 입력합니다. 대개 이 포트 번호는 7023입니다.

포트 번호는 사용 가능하며 고유해야 합니다.

Enter HTTPS Port

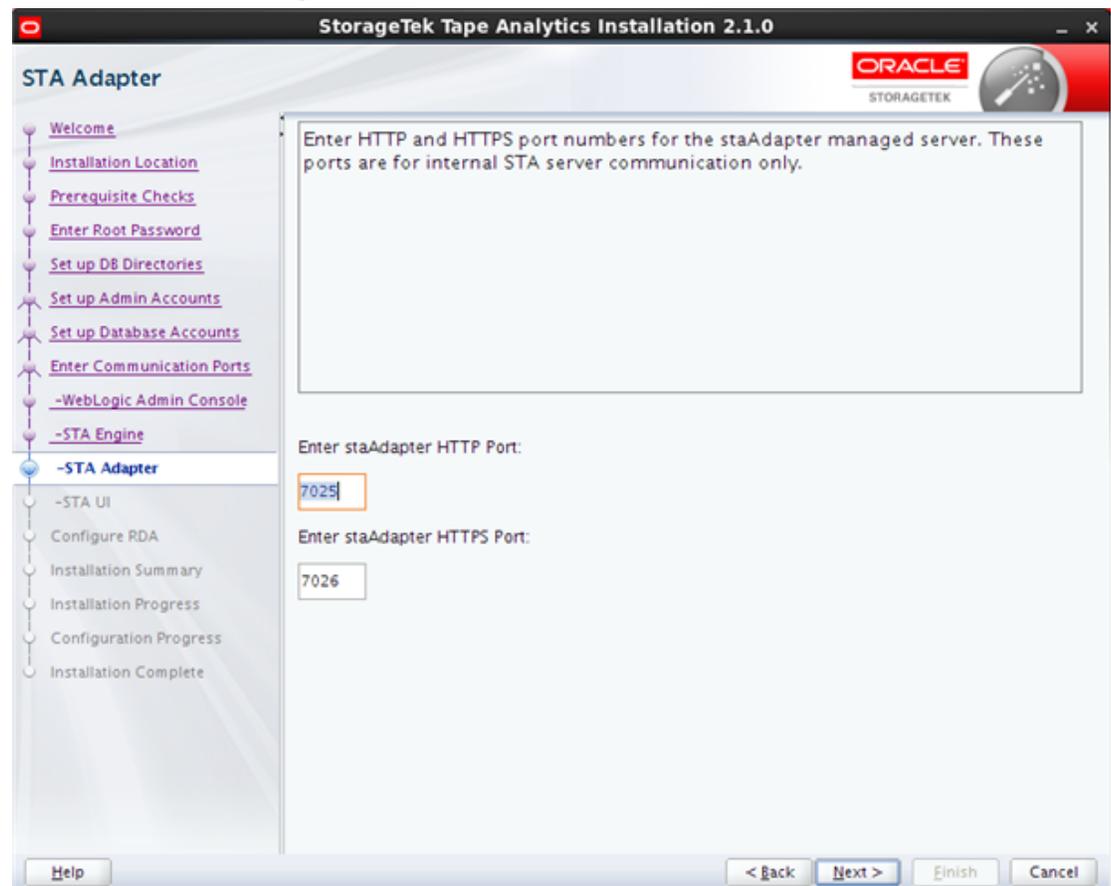
staEngine 관리 서버에 대한 보안 액세스에 사용할 HTTPS 포트 번호를 입력합니다. 대개 이 포트 번호는 7024입니다.

포트 번호는 사용 가능하며 고유해야 합니다.

A.2.17.2. 화면 관련 버튼

없음

A.2.18. STA Adapter



staAdapter 관리 서버 포트는 내부 SNMP 서버 통신용으로만 사용됩니다.

주:

이 포트 번호를 잘 기록해 두십시오. STA가 일단 설치되면 이 포트 번호를 변경할 수 없습니다.

사이트 보안을 유지하기 위해 이 번호는 사전 구성되거나 하드 코딩되지 않습니다.

A.2.18.1. 화면 필드

Enter HTTP Port

staEngine 관리 서버에 대한 비보안 액세스에 사용할 HTTP 포트 번호를 입력합니다. 대개 이 포트 번호는 7025입니다.

포트 번호는 사용 가능하며 고유해야 합니다.

Enter HTTPS Port

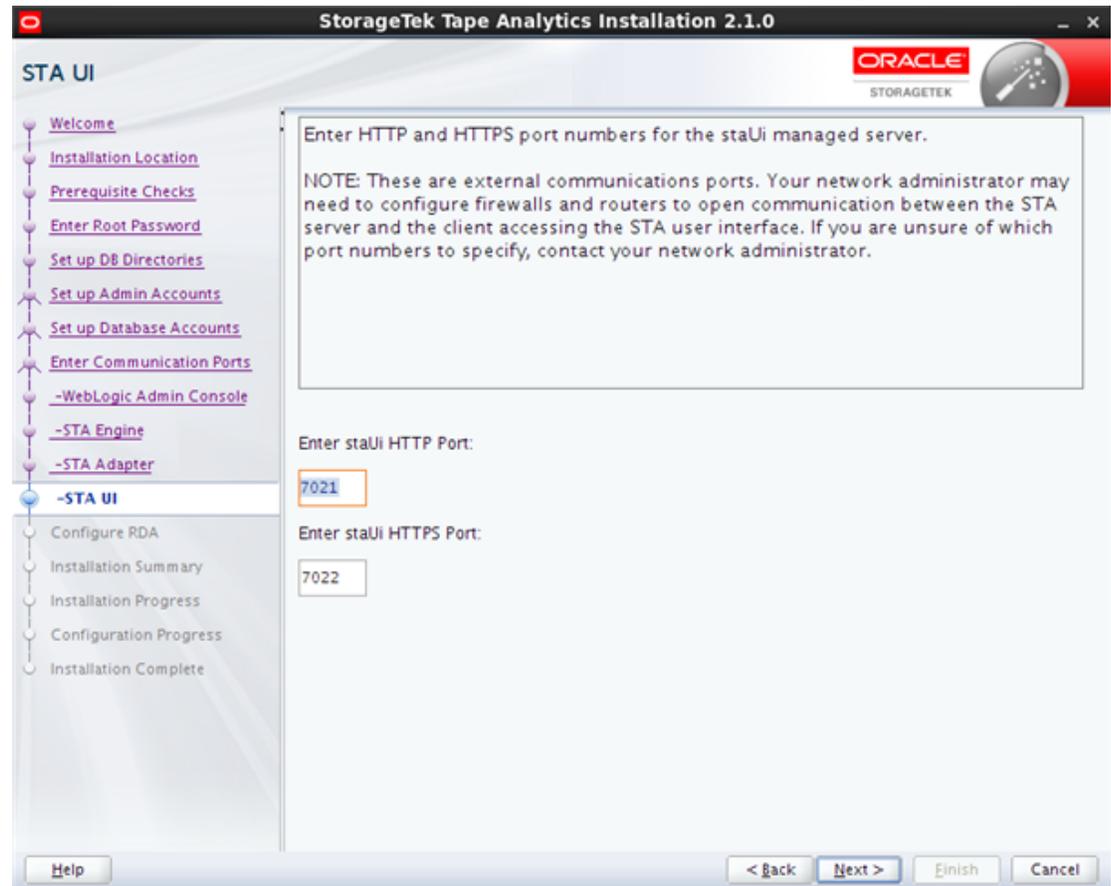
staEngine 관리 서버에 대한 보안 액세스에 사용할 HTTPS 포트 번호를 입력합니다. 대개 이 포트 번호는 7026입니다.

포트 번호는 사용 가능하며 고유해야 합니다.

A.2.18.2. 화면 관련 버튼

없음

A.2.19. STA UI



STA 응용 프로그램 사용자 인터페이스에 로그인할 때 staUi 관리 서버 포트 번호를 지정합니다.

주:

이 포트는 외부 통신 포트입니다. 네트워크 관리자는 STA 서버와 WebLogic 관리 콘솔에 액세스하는 클라이언트 사이에 통신을 열기 위해 방화벽 및 라우터를 구성해야 할 수 있습니다.

주:

이 포트 번호를 잘 기록해 두십시오. STA가 일단 설치되면 이 포트 번호를 변경할 수 없습니다.

사이트 보안을 유지하기 위해 이 번호는 사전 구성되거나 하드 코딩되지 않습니다.

A.2.19.1. 화면 필드

Enter HTTP Port

staUi 관리 서버에 대한 비보안 액세스에 사용할 HTTP 포트 번호를 입력합니다. 대개 이 포트 번호는 7021입니다.

포트 번호는 사용 가능하며 고유해야 합니다.

Enter HTTPS Port

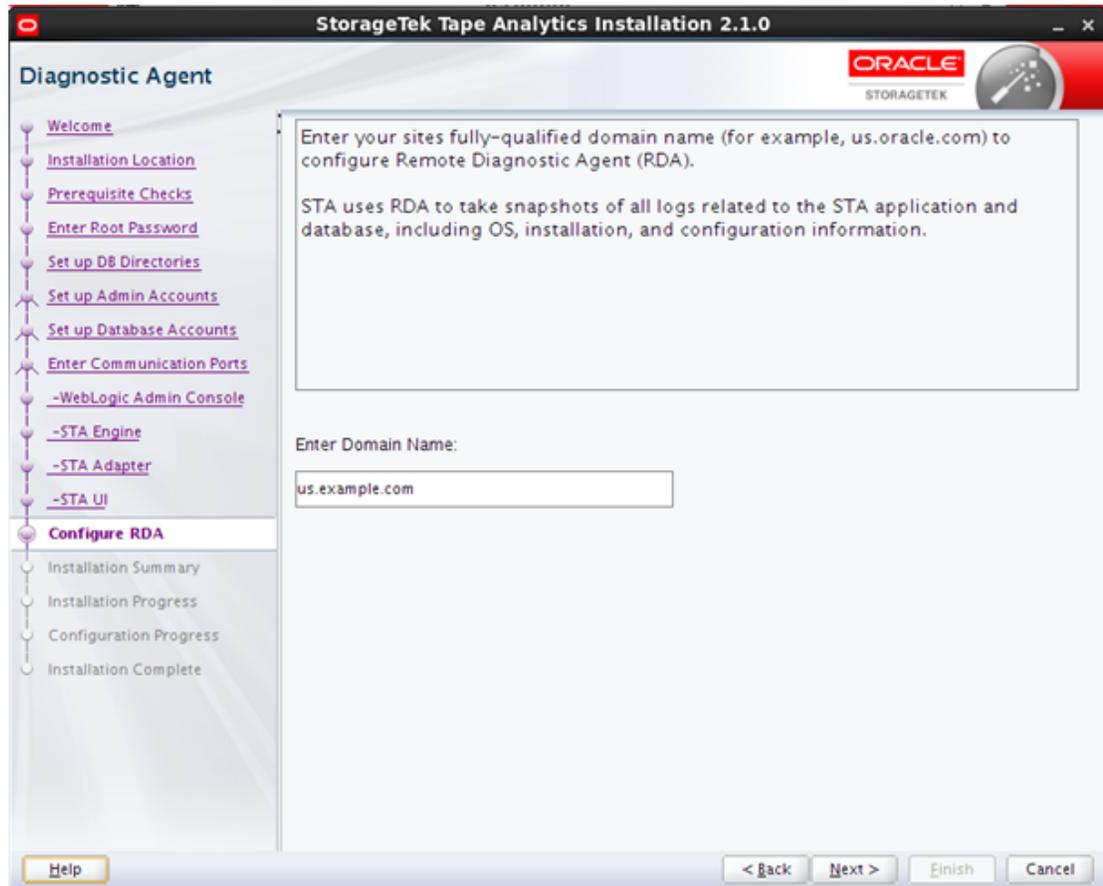
staUi 관리 서버에 대한 보안 액세스에 사용할 HTTP 포트 번호를 입력합니다. 대개 이 포트 번호는 7022입니다.

포트 번호는 사용 가능하며 고유해야 합니다.

A.2.19.2. 화면 관련 버튼

없음

A.2.20. Diagnostic Agent



STA 설치 프로그램은 사이트의 정규화된 도메인 이름을 사용하여 Oracle의 RDA(원격 진단 에이전트)를 구성합니다.

STA는 RDA를 사용하여 운영 체제, 설치 및 구성 정보를 포함하여 STA 응용 프로그램 및 데이터베이스와 관련된 모든 로그의 스냅샷을 만듭니다. 자세한 내용은 STA 사용 설명서를 참조하십시오.

A.2.20.1. 화면 필드

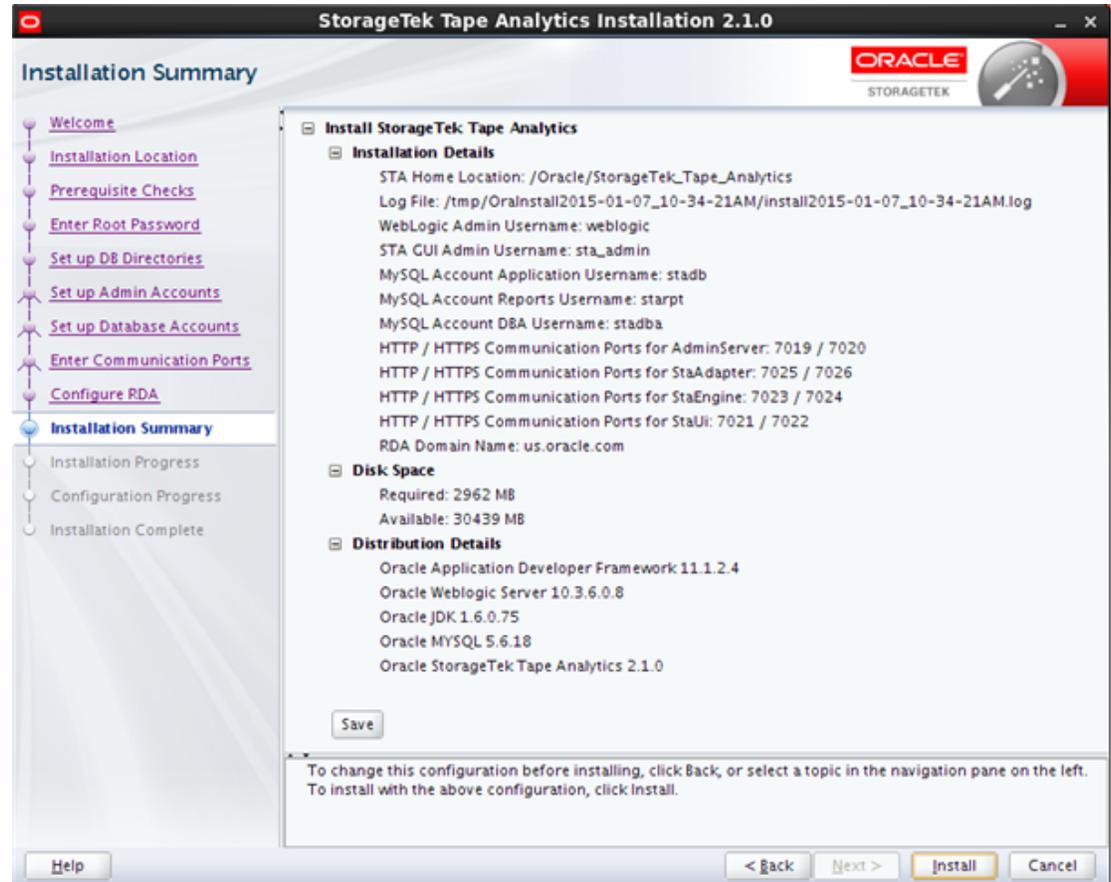
Enter Domain Name

사이트의 정규화된 도메인 이름(예: *us.example.com*)을 입력합니다.

A.2.20.2. 화면 관련 버튼

없음

A.2.21. Installation Summary



이 화면에는 다음과 같은 설치 세부 정보가 표시됩니다. 기록을 위해 이 정보를 텍스트 파일에 저장할 수 있습니다.

- Installation Details—설치 프로그램 화면에 입력한 정보입니다.
- Disk Space—필수 및 사용 가능한 디스크 공간(MB)입니다.
- Distribution Details—설치될 소프트웨어 패키지의 이름 및 버전 번호입니다.

다음과 같이 계속합니다.

- 설치 세부 정보를 변경하려면 **Back**을 눌러 해당 화면으로 돌아가거나 탐색 창의 화면 링크를 선택하여 해당 화면으로 바로 이동합니다.

- 표시된 정보를 텍스트 파일로 저장하려면 **Save**를 누릅니다.
- 표시된 값을 사용하여 설치하려면 **Install**을 누릅니다.
- 설치를 취소하려면 **Cancel**을 누릅니다.

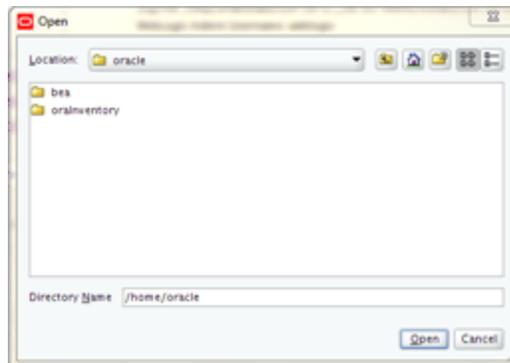
A.2.21.1. 화면 필드

없음

A.2.21.2. 화면 관련 버튼

Save

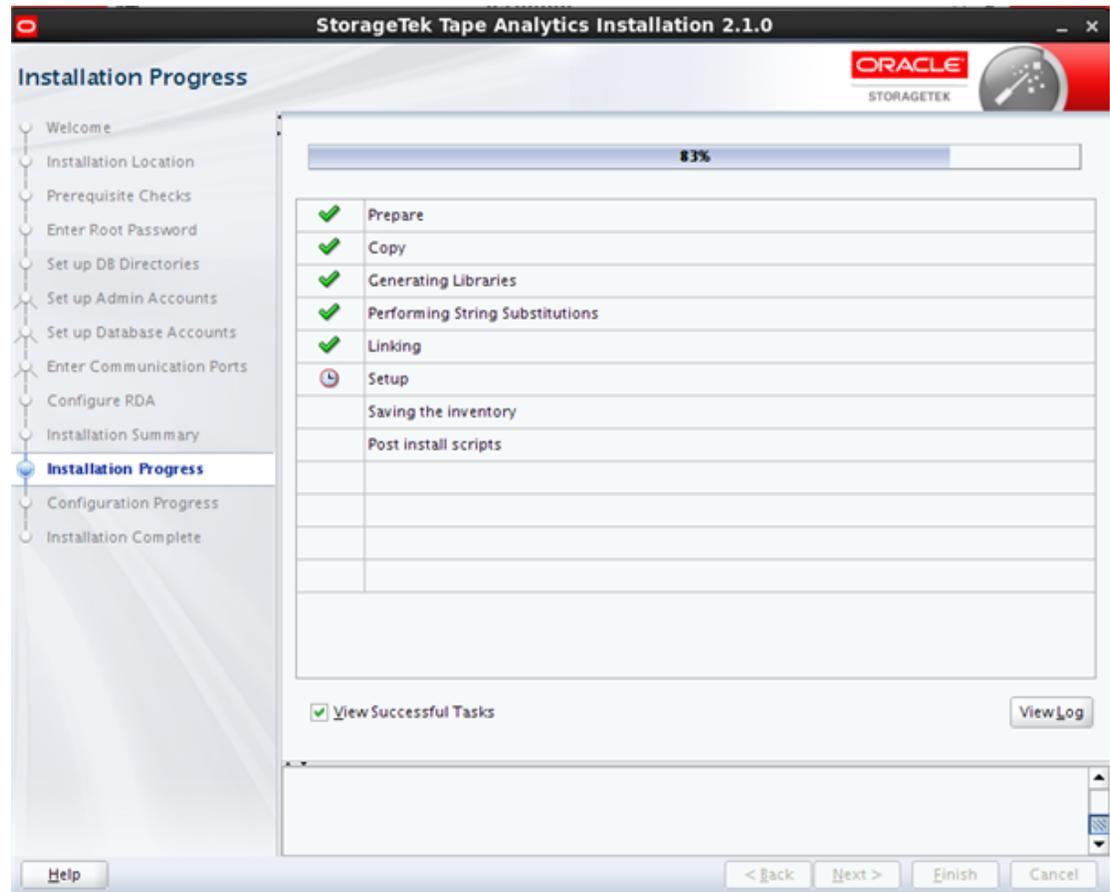
표시된 정보를 *STA_Installation_Profile_timestamp.txt*라는 이름의 텍스트 파일로 저장하려면 누릅니다. Open 대화 상자에서 파일을 저장할 디렉토리를 지정합니다.



Install

설치를 시작하려면 누릅니다. 이 버튼을 누른 후에는 설치를 일시 중지하거나 취소할 수 없습니다.

A.2.22. Installation Progress



STA 설치가 시작되고 화면에는 각 작업의 상태가 표시됩니다.

주의:

이 창을 닫거나 어떤 방식으로든 진행 중인 설치를 중단하지 마십시오. 그렇게 되면 완료되지 않은 설치 구성 요소가 서버에 남을 수 있습니다.

작업이 실패하면 설치는 중단되며, 사용자는 **Cancel**을 눌러 설치 프로그램을 종료해야 합니다. 설치 프로그램은 설치를 롤백하고 서버를 원래 상태로 되돌립니다.

종료하기 전에 메시지 창에서 문제를 해결하고 취할 조치를 결정하는 데 도움이 되는 추가 세부 정보를 확인할 수 있습니다. 설치 로그에서 추가 정보를 확인할 수도 있습니다.

A.2.22.1. 화면 필드

없음

A.2.22.2. 화면 관련 버튼

View Successful Tasks

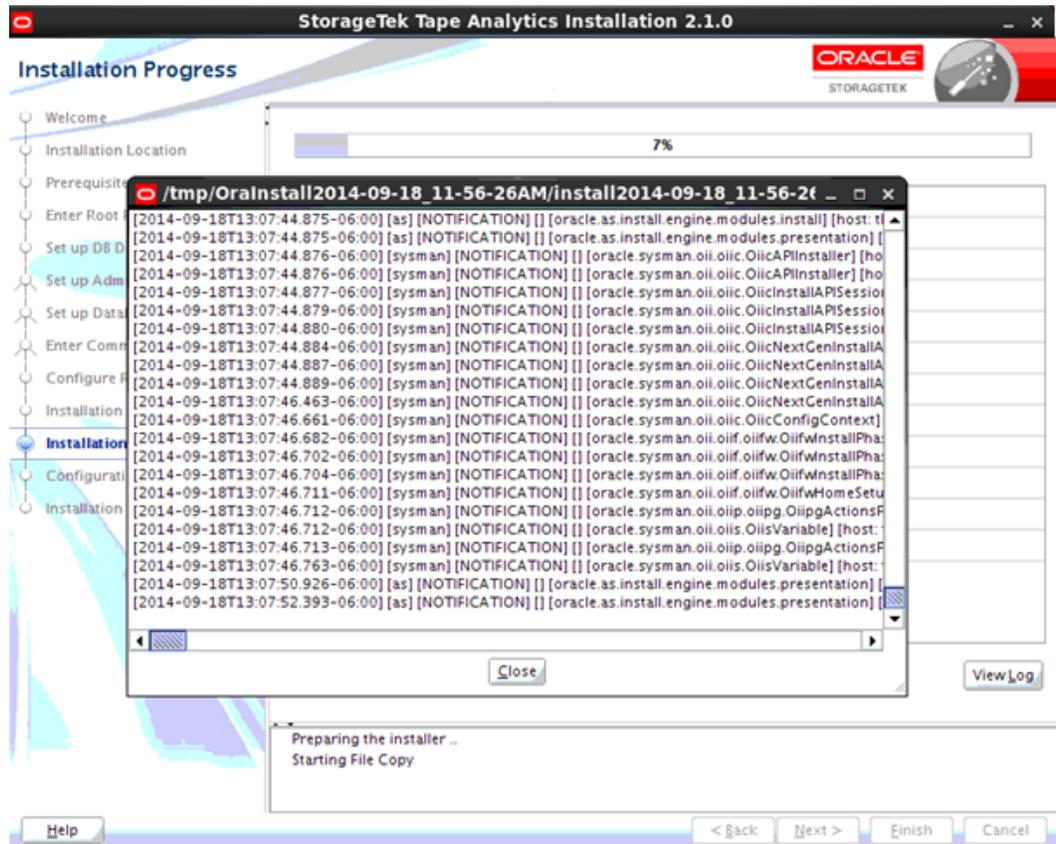
성공 출력도 표시되게 하려면 이 확인란을 선택합니다. 기본적으로 선택됩니다.

실패 출력만 표시하려면 확인란의 선택을 취소합니다. 이렇게 하면 성공적인 작업을 제외하여 주의가 필요한 작업에만 집중할 수 있습니다.

View Log

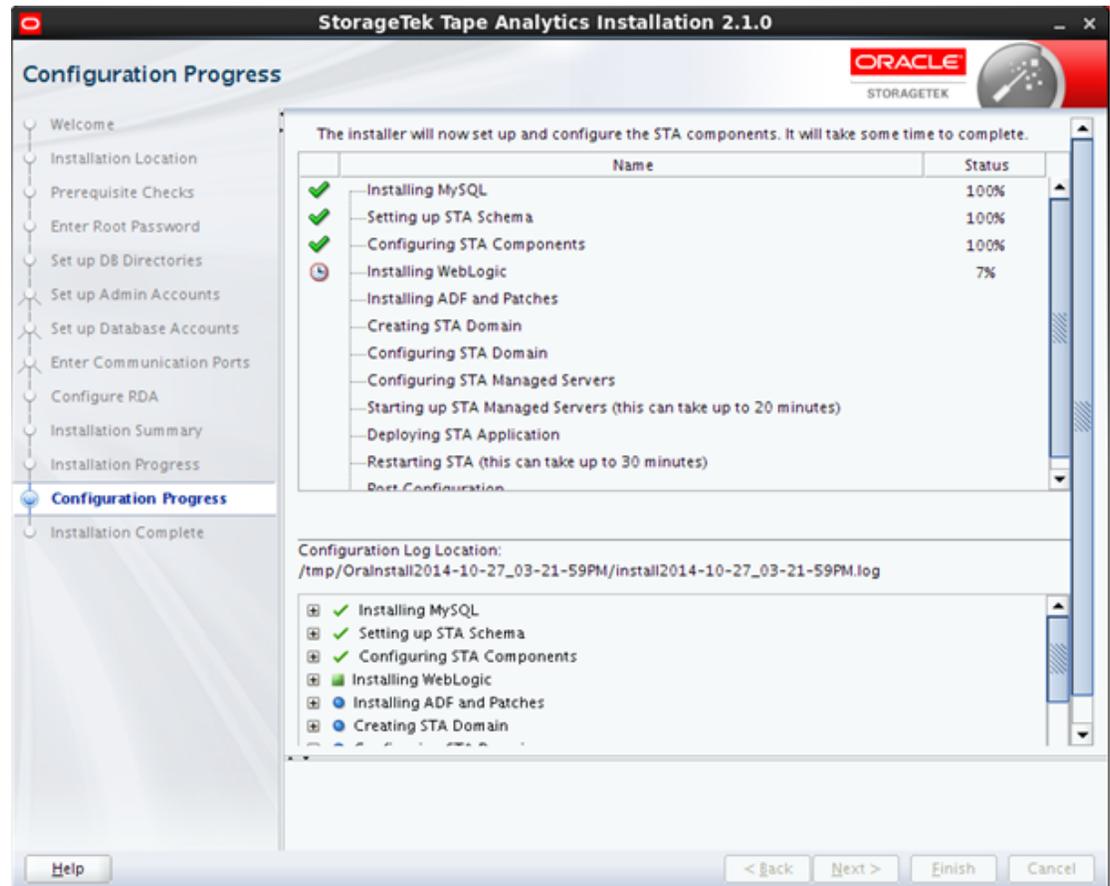
설치 로그를 별도의 창에 표시하려면 누릅니다. [그림 A.5. "Installation Progress 로그 표시의 예"](#)는 이러한 예입니다. 로그 창을 닫으려면 **Close**를 누릅니다.

그림 A.5. Installation Progress 로그 표시의 예



Linux 명령줄에서도 로그를 볼 수 있습니다. 설치 프로그램 실행 중에 로그는 `/tmp` 내부의 하위 디렉토리에 보관됩니다. 자세한 내용은 [3.4절. "STA 설치 및 제거 로그"](#)를 참조하십시오.

A.2.23. Configuration Progress



STA 구성 및 배치가 시작되고 화면에는 각 작업의 상태가 표시됩니다.

주의:

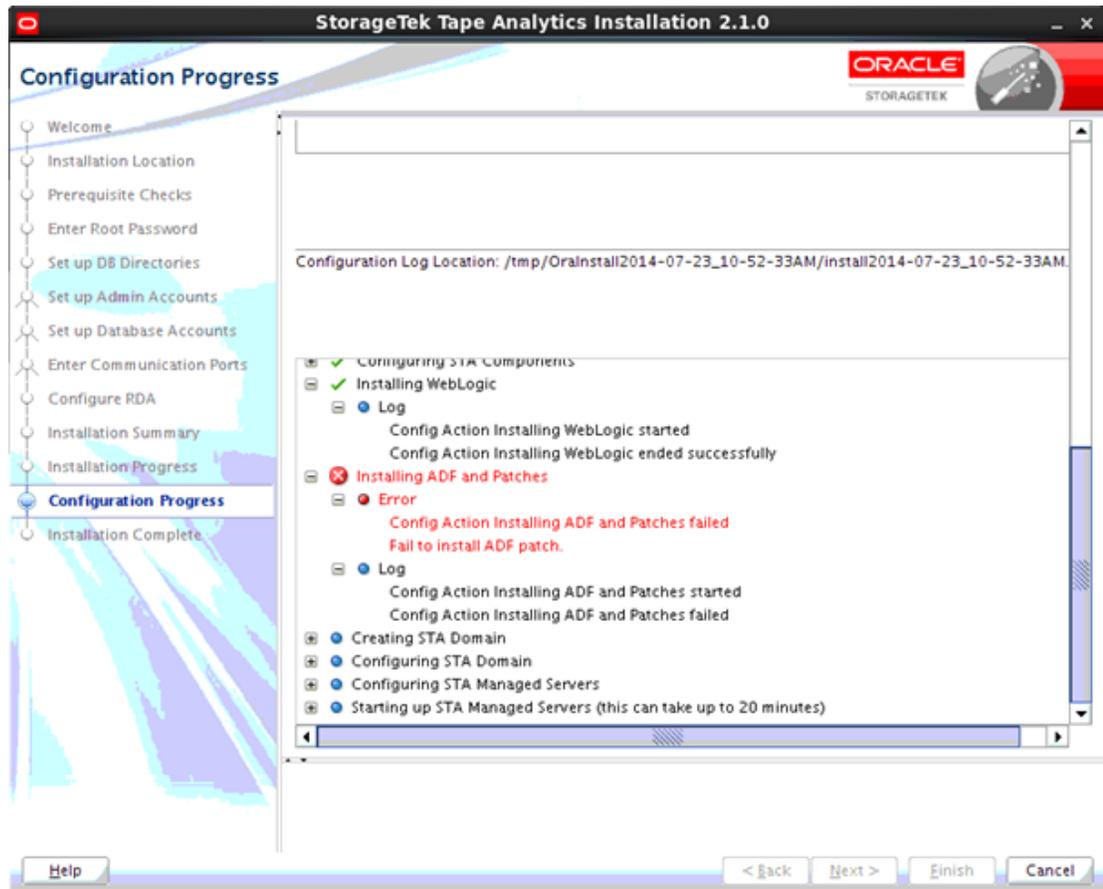
이 창을 닫거나 어떤 방식으로든 진행 중인 구성을 중단하지 마십시오. 그렇게 되면 완료되지 않은 설치 구성 요소가 서버에 남을 수 있습니다.

이 프로세스 중 WebLogic Server, STA 관리 서버 및 STA 응용 프로그램이 구성되고 시작됩니다. 완료하는 데 30~60분 정도 걸릴 수 있습니다.

완료되거나 진행 중인 작업에 대해 확장된 세부 정보를 표시할 수 있습니다. 메시지 창에서 세부 정보를 표시할 작업 옆의 확장(+) 아이콘을 누릅니다. 세부 정보를 다시 숨기려면 축소(-) 아이콘을 누릅니다. [그림 A.6. "Configuration Progress 세부 정보의 예"](#)은 성공한 작업과 실패한 작업에 대해 확장된 세부 정보를 보여 주는 예입니다.

작업이 실패하면 STA 설치 프로그램은 종료되고, 설치는 롤백되고, 서버는 원래 상태로 돌아갑니다. 문제를 해결하기 위해 설치 로그를 확인할 수 있습니다. 자세한 내용은 [3.4절. "STA 설치 및 제거 로그"](#)를 참조하십시오.

그림 A.6. Configuration Progress 세부 정보의 예



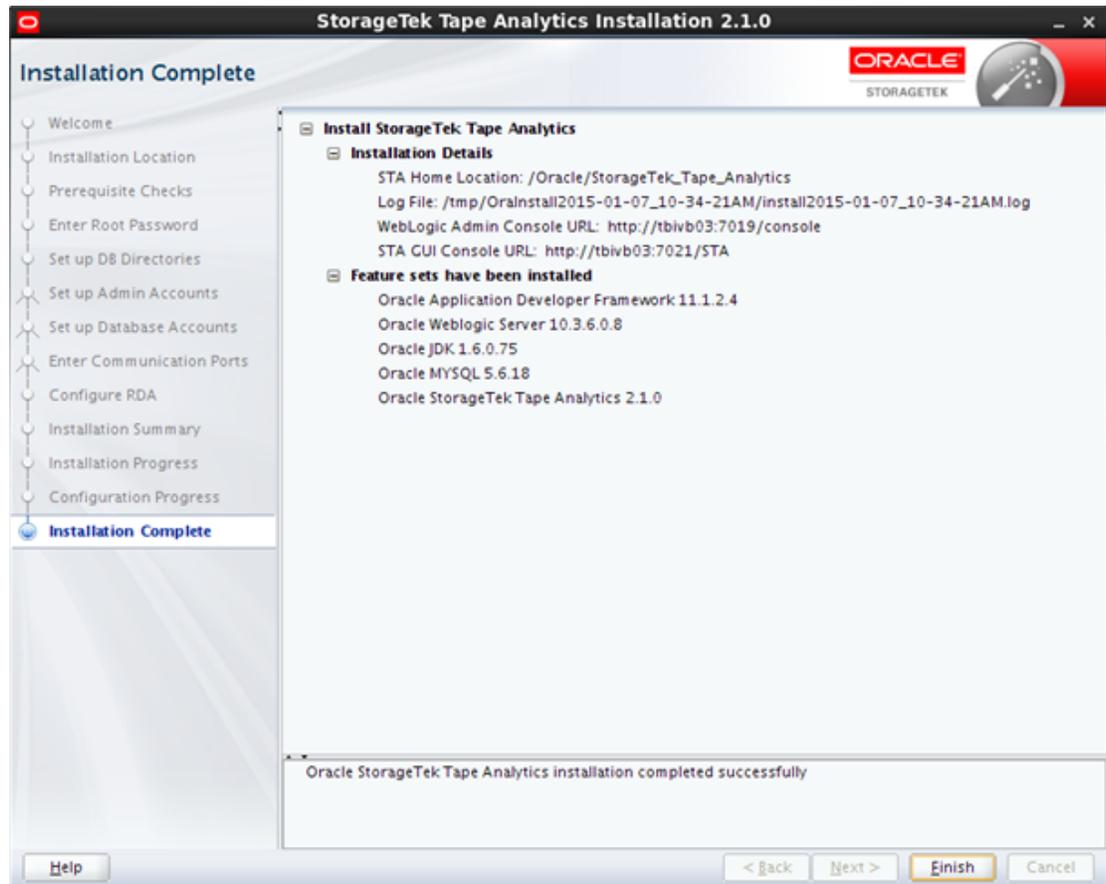
A.2.23.1. 화면 필드

없음

A.2.23.2. 화면 관련 버튼

없음

A.2.24. Installation Complete



이 화면은 완료된 설치에 대한 다음 세부 정보를 표시합니다.

- Installation Details—설치된 STA 응용 프로그램 및 설치 프로그램 로그 파일의 위치, 그리고 WebLogic 및 STA 응용 프로그램 사용자 인터페이스의 연결 세부 정보입니다.
- Feature sets have been installed—설치된 소프트웨어 패키지의 이름 및 버전 번호입니다.

기록을 위해 이 정보의 스크린샷을 저장할 수 있습니다. **Finish**를 눌러 설치 프로그램을 종료합니다.

A.2.24.1. 화면 필드

없음

A.2.24.2. 화면 관련 버튼

Finish

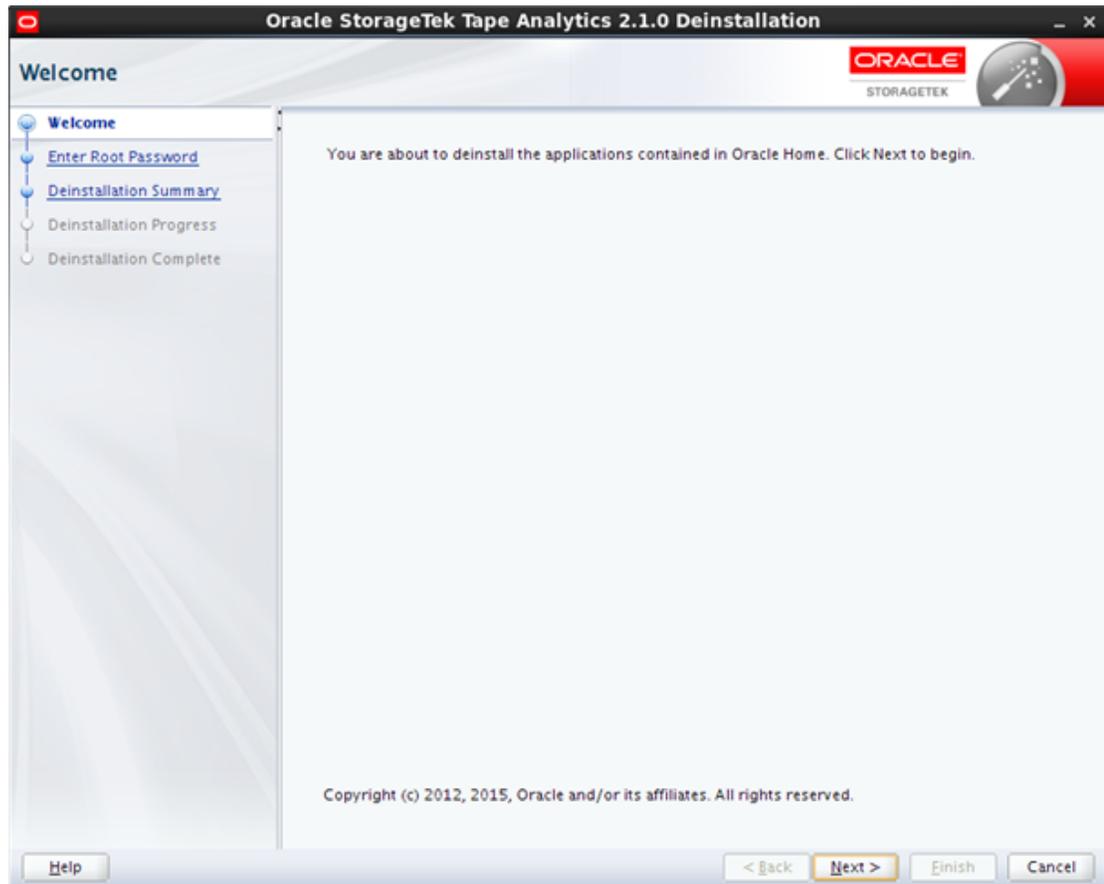
STA 설치 프로그램을 종료하려면 누릅니다.

A.3. STA 그래픽 제거 프로그램 화면

이 절에서는 STA 그래픽 제거 프로그램의 각 화면에 대한 자세한 설명을 제공합니다.

- A.3.1절. “Welcome”
- A.3.2절. “Enter Root Password”
- A.3.3절. “Deinstallation Summary”
- A.3.4절. “Deinstallation Progress”
- A.3.5절. “Deinstallation Complete”

A.3.1. Welcome



이 화면은 사용자가 수행할 동작에 대해 설명합니다. 텍스트를 읽은 후 **Next**를 눌러 진행합니다.

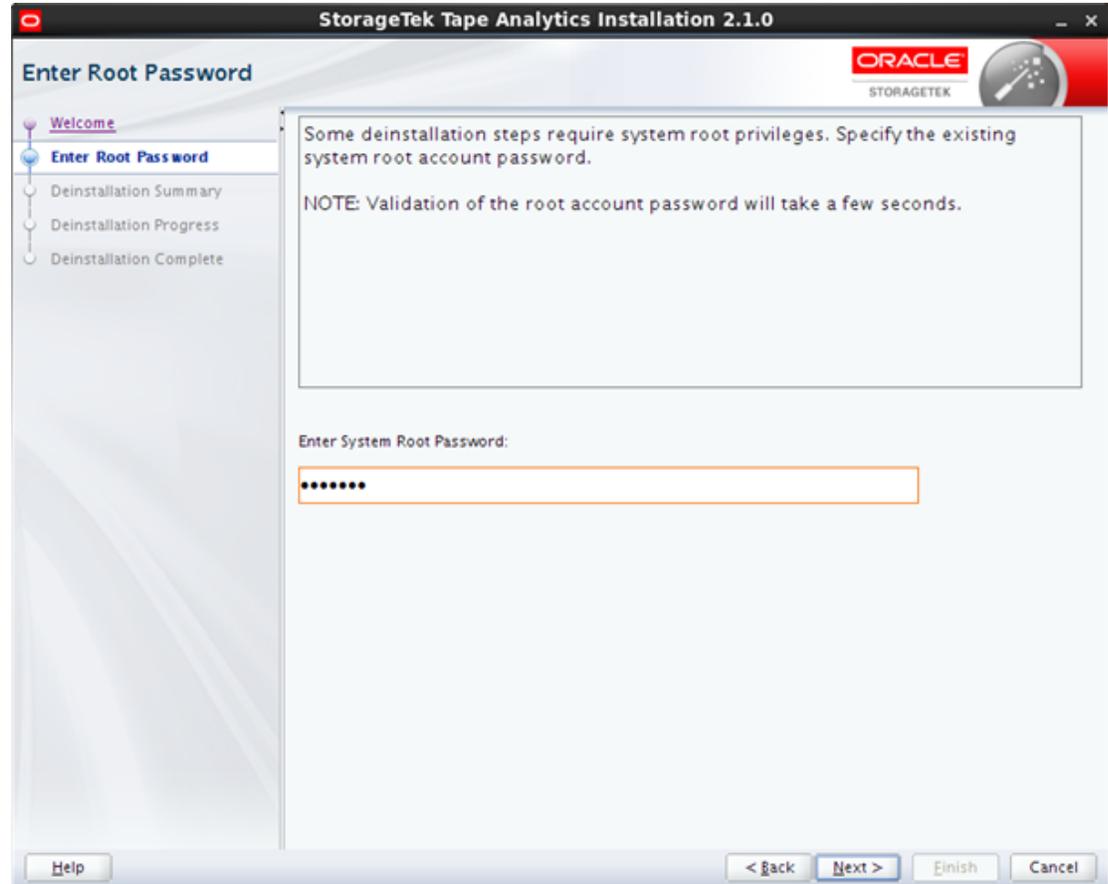
A.3.1.1. 화면 필드

없음

A.3.1.2. 화면 관련 버튼

없음

A.3.2. Enter Root Password



STA 제거 프로그램이 제거 작업을 수행하려면 Linux 루트로 액세스해야 합니다.

A.3.2.1. 화면 필드

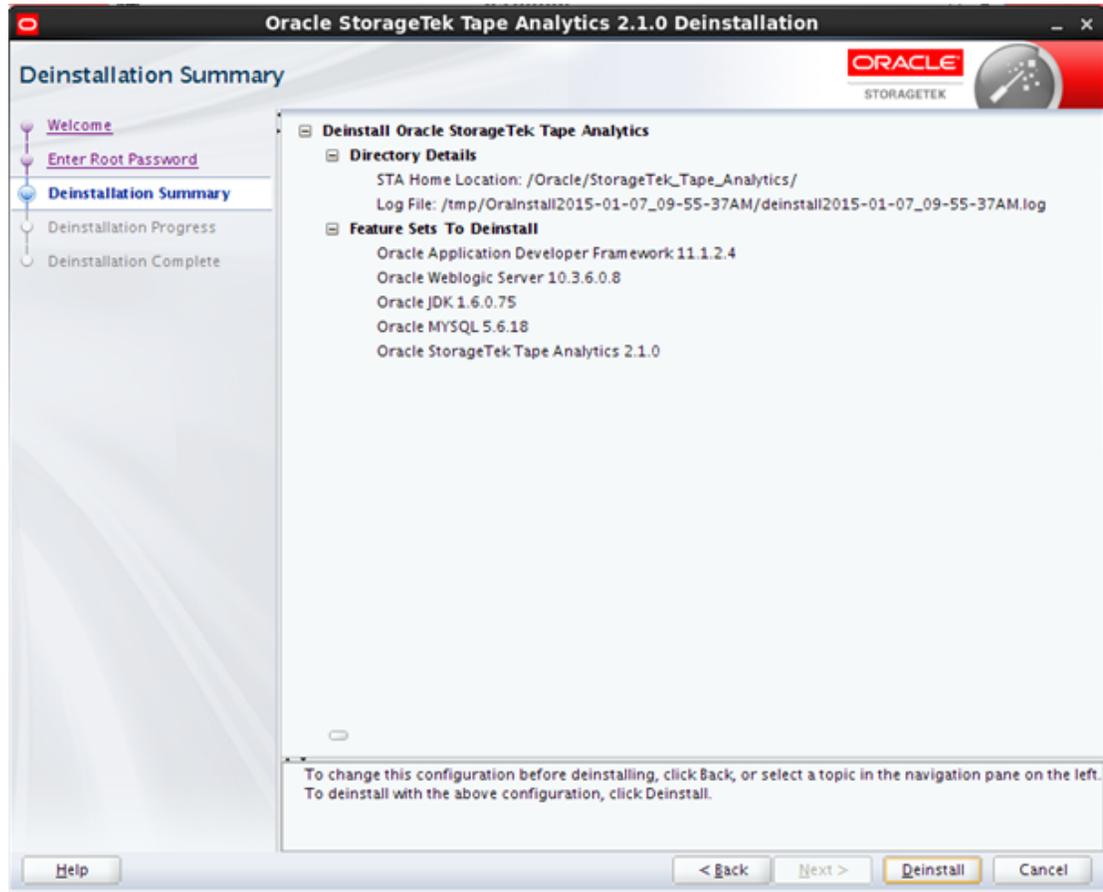
Enter Root Password

Linux 루트 사용자의 암호를 입력합니다. 항목은 입력할 때 마스크되어 표시됩니다. 암호를 검증하는 데 몇 초 정도 걸릴 수 있습니다.

A.3.2.2. 화면 관련 버튼

없음

A.3.3. Deinstallation Summary



이 화면에는 제거될 소프트웨어에 대한 다음 세부 정보가 표시됩니다.

- Directory Details—STA 응용 프로그램 소프트웨어 및 제거 로그의 위치입니다.
- Feature Sets to Deinstall—제거될 소프트웨어 패키지의 이름 및 버전 번호입니다.

이 정보를 확인한 후 다음과 같이 계속합니다.

- 제거 프로그램을 취소하고 종료하려면 **Cancel**을 누릅니다.
- 계속 진행하려면 **Deinstall**을 누릅니다.

A.3.3.1. 화면 필드

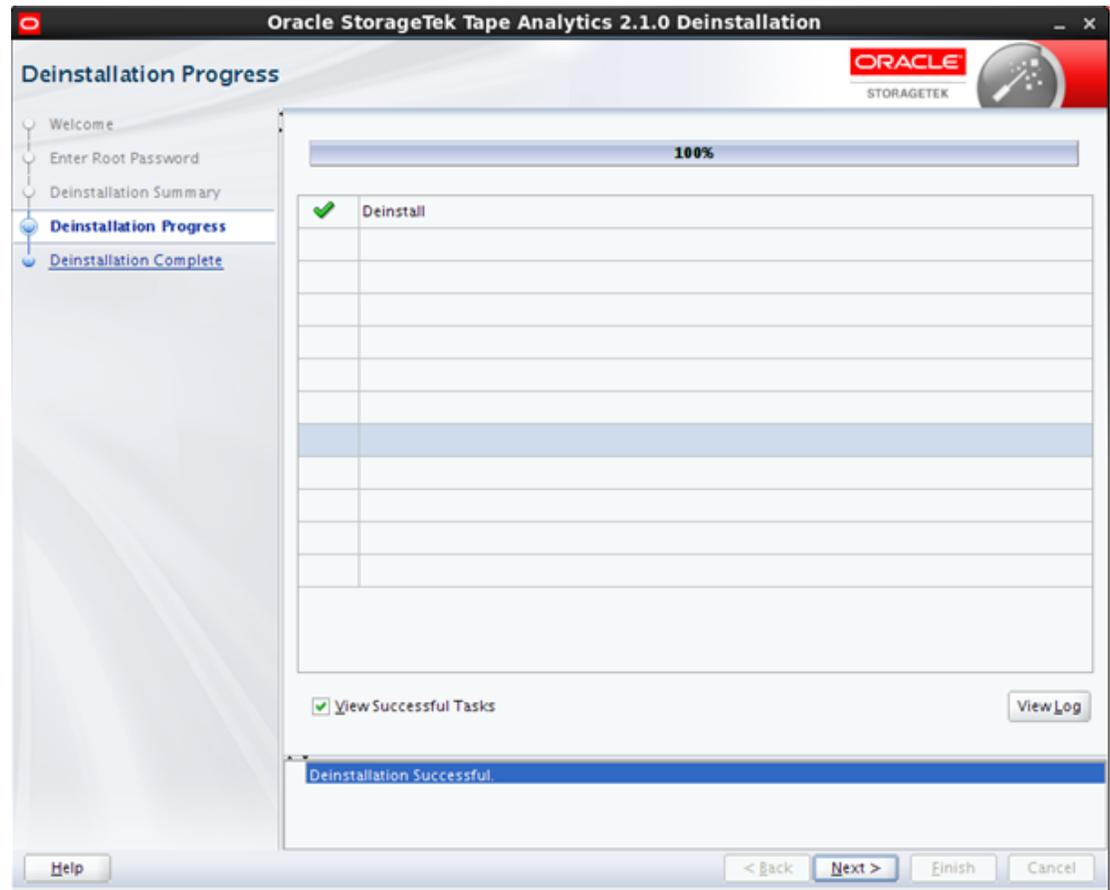
없음

A.3.3.2. 화면 관련 버튼

Deinstall

STA 제거를 시작하려면 누릅니다. 이 버튼을 누른 후에는 제거를 일시 중지하거나 취소할 수 없습니다.

A.3.4. Deinstallation Progress



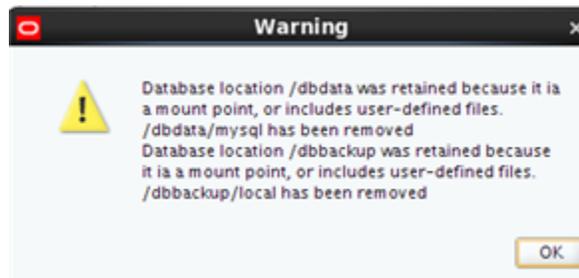
STA 제거가 시작되고 화면에는 각 작업의 상태가 표시됩니다.

주의:

이 창을 닫거나 어떤 방식으로든 진행 중인 제거를 중단하지 마십시오. 그렇게 되면 완료되지 않은 STA 구성 요소가 서버에 남을 수 있습니다.

주:

데이터베이스 위치 중 하나가 STA 서버의 마운트 지점인 경우 마운트 지점이 보존되었음을 알리는 다음 메시지가 표시됩니다. **OK**를 눌러 메시지를 없앱니다.



제거가 완료되면 메시지 창에 "Deinstallation Successful"이라는 메시지가 나타납니다. **Next** 또는 **Finish**를 눌러 최종 화면으로 진행합니다.

작업이 실패하면 STA 제거 프로그램은 종료되고, 제거는 롤백되고, 서버는 원래 상태로 돌아갑니다. 문제를 해결하기 위해 제거 로그를 확인할 수 있습니다. 자세한 내용은 [3.4절. "STA 설치 및 제거 로그"](#)를 참조하십시오.

A.3.4.1. 화면 필드

없음

A.3.4.2. 화면 관련 버튼

View Successful Tasks

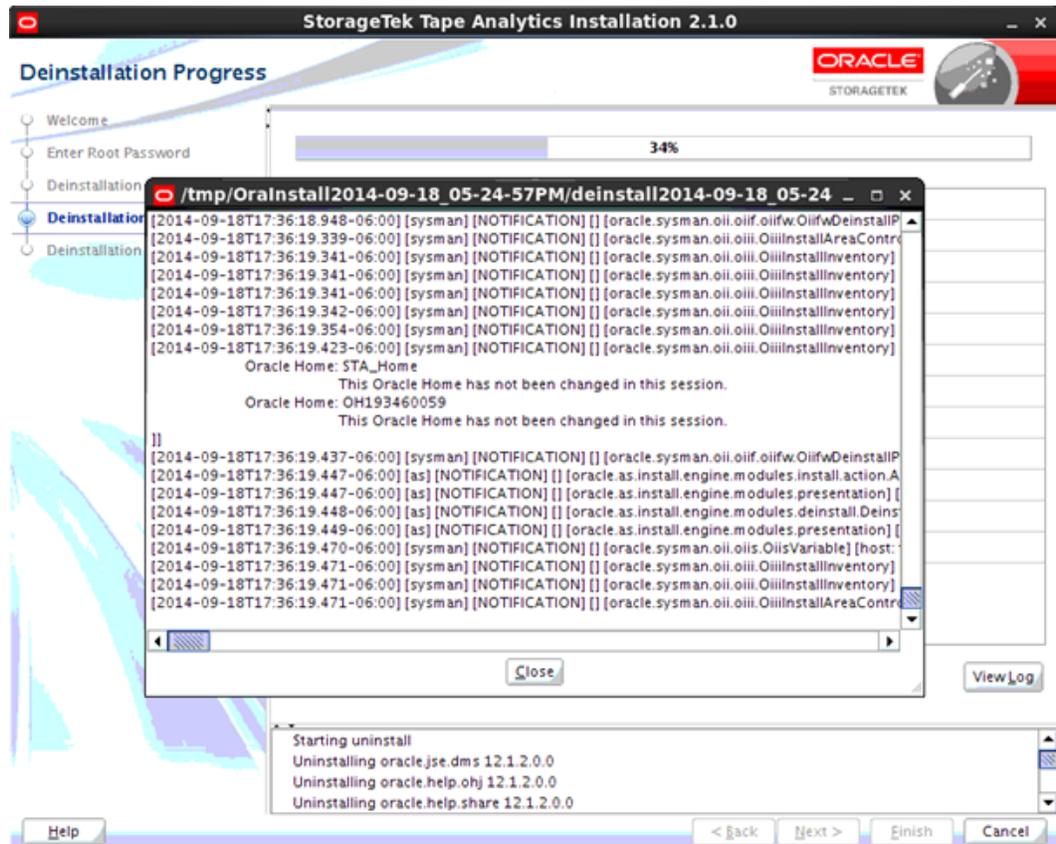
성공 출력도 표시되게 하려면 이 확인란을 선택합니다. 기본적으로 선택됩니다.

실패 출력만 표시하려면 확인란의 선택을 취소합니다. 이렇게 하면 성공적인 작업을 제외하여 주의가 필요한 작업에만 집중할 수 있습니다.

View Log

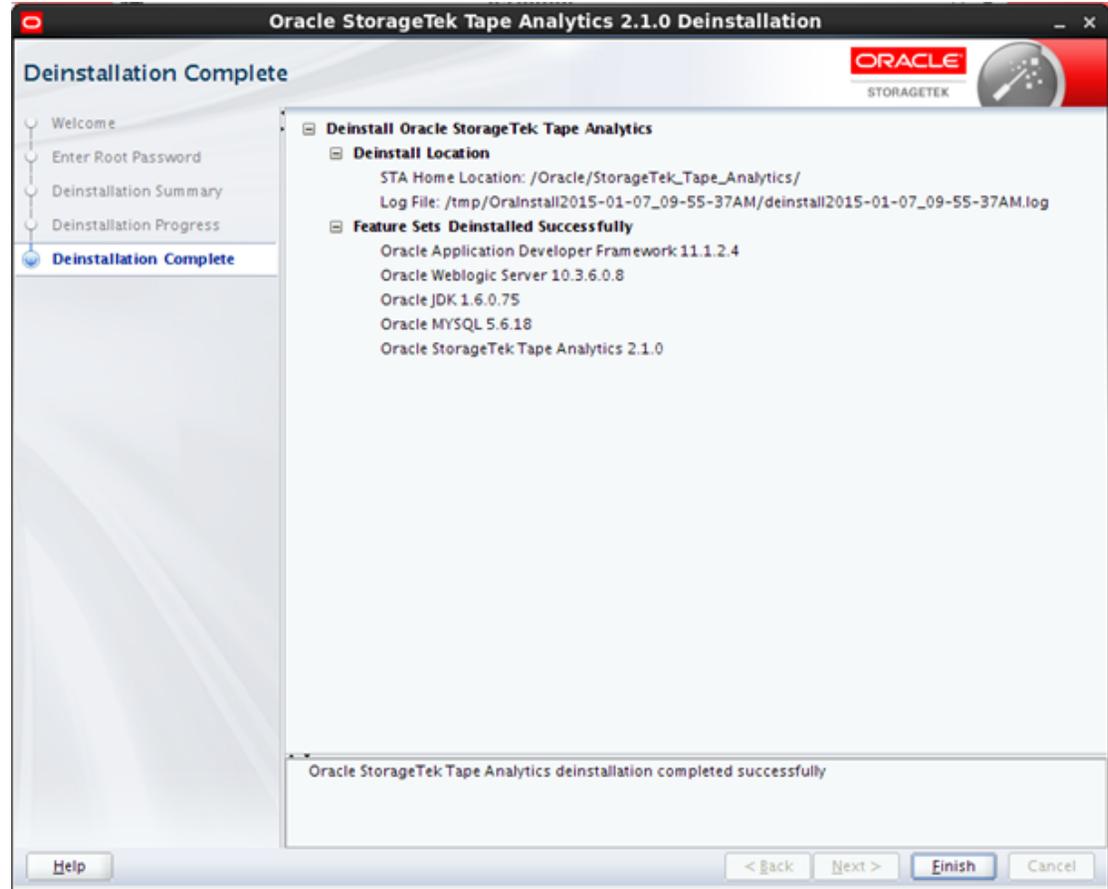
제거 로그를 별도의 창에 표시하려면 누릅니다. [그림 A.5. "Installation Progress 로그 표시의 예"](#)는 이러한 예입니다. 로그 창을 닫으려면 **Close**를 누릅니다.

그림 A.7. Deinstallation Progress 로그 표시의 예



Linux 명령줄에서도 로그를 볼 수 있습니다. 제거 프로그램 실행 중에 로그는 `/tmp` 내부의 하위 디렉토리에 보관됩니다. 자세한 내용은 3.4절. “STA 설치 및 제거 로그”를 참조하십시오.

A.3.5. Deinstallation Complete



이 화면에는 제거된 소프트웨어 패키지에 대한 세부 정보가 표시됩니다.

A.3.5.1. 화면 필드

없음

A.3.5.2. 화면 관련 버튼

Finish

STA 제거 프로그램을 종료하려면 누릅니다.

STA 자동 모드 설치 프로그램 및 제거 프로그램

이 부록에는 다음 절이 포함되어 있습니다.

- [STA 자동 모드 설치 프로그램 및 제거 프로그램 사용](#)
- [자동 모드에서 사용되는 파일 및 유틸리티](#)
- [STA 자동 모드 설치 프로그램 작업](#)
- [STA 자동 모드 제거 프로그램 작업](#)
- [STA 설치 프로그램 명령 옵션](#)

B.1. STA 자동 모드 설치 프로그램 및 제거 프로그램 사용

자동 모드를 사용하면 그래픽 사용자 인터페이스를 건너뛰고 응답 파일이라는 XML 등록 정보 파일에 STA 설치 또는 제거 옵션을 제공할 수 있습니다. 응답 파일 작성 유틸리티인 *silentInstallUtility_version.jar*를 사용하여 응답 파일을 만듭니다. 여기서 *version*은 다운로드한 유틸리티의 버전입니다.

이 모드는 무인 설치 및 여러 시스템에 STA를 설치하는 경우에 유용합니다. 응답 파일을 사용하면 단일 매개변수 세트를 제공하여 설치를 자동화할 수 있습니다. 자동 모드 설치 프로그램은 스크립트 또는 Linux 명령줄에서 실행할 수 있습니다.

B.1.1. 자동 모드 요구 사항

일반적인 STA 설치 요구 사항은 [3.6.2절. “설치 필요 조건 확인”](#)을 참조하십시오. 또한 STA 자동 모드 설치 프로그램 및 제거 프로그램에는 다음과 같은 모드 관련 요구 사항이 있습니다.

- X11 프로토콜을 사용하지 않는 PuTTY와 같은 telnet 클라이언트에서 자동 모드를 사용할 수 있습니다. 하지만 이 경우 *xorg-x11-utils* RPM 패키지가 STA 서버에 설치되어 있어야 합니다.
- 자동 모드를 사용하려면 먼저 *silentInstallUtility_version.jar* 파일을 Oracle Software Delivery Cloud 웹사이트에서 다운로드한 다음 이를 사용하여 암호화된 암호 응답 파일을 만들어야 합니다. 자세한 내용은 [B.3.2절. “자동 모드 설치 프로그램 응답 파일 만들기”](#)를 참조하십시오.
- 자동 모드에는 Oracle 중앙 인벤토리 디렉토리 및 Oracle 설치 그룹의 위치를 지정하는 중앙 인벤토리 포인터 파일도 필요합니다. 이 파일이 존재하지 않으면 수동으로 만들어야 합니다. 자세한 내용은 [Oracle 중앙 인벤토리 포인터 파일](#)을 참조하십시오.

B.2. 자동 모드에서 사용되는 파일 및 유틸리티

이 절에서는 자동 모드 설치 및 제거에 대한 핵심 개념 및 용어에 대해 설명합니다.

Oracle 중앙 인벤토리 포인터 파일

STA 자동 모드 설치 프로그램 및 제거 프로그램은 중앙 인벤토리 포인터 파일에 지정된 Oracle 중앙 인벤토리 위치 및 Oracle 설치 그룹을 사용합니다. 자세한 내용은 3.1절. “STA 설치 프로그램에서 사용하는 사용자, 그룹 및 위치”를 참조하십시오.

기본적으로 자동 모드 설치 프로그램 및 제거 프로그램은 포인터 파일 `/etc/oraInst.loc`를 사용합니다. Oracle 중앙 인벤토리를 등록하면 이 이름과 위치로 파일이 자동으로 만들어집니다. 자세한 내용은 3.6.7절. “Oracle 중앙 인벤토리 위치 등록”을 참조하십시오.

Oracle 중앙 인벤토리 위치가 등록되지 않은 경우 포인터 파일을 수동으로 만들고 파일 이름을 `oraInst.loc`로 지정해야 합니다. 자세한 내용은 B.3.1절. “Oracle 중앙 인벤토리 포인터 파일 만들기”를 참조하십시오. 포인터 파일은 어느 디렉토리에든 배치할 수 있지만 이 파일이 `/etc`에 있지 않으면 자동 모드 설치 프로그램 및 제거 프로그램을 실행할 때 `-invPtrLoc` 매개변수를 사용하여 이 파일의 위치를 지정해야 합니다. 이 매개변수에 대한 자세한 내용은 `-invPtrLoc pointer_file`을 참조하십시오.

자동 모드 설치 프로그램 및 제거 프로그램 응답 파일

무인으로 실행하기 위해 STA 자동 모드 설치 프로그램 및 제거 프로그램은 사용자가 만든 응답 파일에 포함된 구성 설정을 사용합니다. `-responseFile` 매개변수를 사용하여 이 파일의 이름 및 위치를 지정해야 합니다.

설치 프로그램 및 제거 프로그램은 각각 자체 응답 파일을 가지고 있습니다. 예 B.1. “STA 자동 모드 설치 프로그램 응답 파일 템플릿” 및 예 B.2. “STA 자동 모드 제거 프로그램 응답 파일 템플릿”는 각 파일의 내용 및 필요한 항목을 보여 줍니다. 자체 응답 파일을 만들려면 각 템플릿을 텍스트 파일로 복사해서 붙여 넣은 다음 사용자의 사이트에 맞게 변경하면 됩니다.

암호 보안을 위해 응답 파일에 일반 텍스트 암호를 입력하지 마십시오. 다른 모든 구성 설정을 입력하고 파일을 저장한 후 응답 파일 작성 유틸리티를 사용하여 암호화된 암호를 파일에 삽입해야 합니다. 자세한 내용은 STA 설치 프로그램 응답 파일 작성 유틸리티를 참조하십시오.

예 B.1. STA 자동 모드 설치 프로그램 응답 파일 템플릿

```
[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 passsword var.
MYSQL ROOT PASSWORD=
#MySQL root confirm passsword 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
STAU HTTP PORT=7021
#staUi HTTPS Port Var
STAU HTTPS PORT=7022
#Domain name var.
DOMAIN NAME=required

```

예 B.2. STA 자동 모드 제거 프로그램 응답 파일 템플릿

```

[ENGINE]
#DO NOT CHANGE THIS. Response File Version=1.0.0.0
[GENERIC]
#This will be blank when there is nothing to be de-installed in distribution level
SELECTED_DISTRIBUTION=STA_Install~2.1.0.0
#Root access passsword var.
DEINSTALL ROOT ACCESS PASSWORD=
RESPONSEFILE_LOC=
KEYFILE_LOC=

```

STA 설치 프로그램 응답 파일 작성 유틸리티

설치 프로그램 응답 파일 작성 유틸리티를 사용하여 자동 모드 설치 프로그램 및 제거 프로그램 응답 파일에 암호화된 암호를 삽입할 수 있습니다. 이 유틸리티는 암호를 묻는 메

시지를 표시하고 해당 암호를 지정된 파일에 암호화된 형태로 추가합니다. 또한 이 유틸리티는 사용자가 선택한 디렉토리에 암호화 키 파일을 저장합니다.

STA 설치 프로그램을 다운로드할 때 응답 파일 작성 유틸리티를 다운로드할 수 있습니다. 유틸리티 이름은 `silentInstallUtility_version.jar`로, 여기서 `version`은 다운로드한 유틸리티의 버전입니다.

STA가 성공적으로 설치 또는 제거된 후 암호화된 암호는 해당 응답 파일에서 제거됩니다. 자동 모드 설치 프로그램 또는 제거 프로그램을 다시 실행하려면 작성 유틸리티를 다시 실행하여 암호화된 암호를 다시 제공합니다.

작성 유틸리티는 응답 파일 위치를 파일 내용에 쓰므로 이 유틸리티로 응답 파일을 업데이트한 후에는 응답 파일의 위치를 바꿀 수 없습니다.

자세한 내용은 [B.3.2절. “자동 모드 설치 프로그램 응답 파일 만들기”](#)를 참조하십시오.

B.3. STA 자동 모드 설치 프로그램 작업

이 작업을 사용하기 전에 필요한 설치 정보를 확보하고, 필수 조건을 확인하고, STA 설치 프로그램을 다운로드해야 합니다. 자세한 내용은 [3.6절. “STA 설치 작업”](#)을 참조하십시오.

그런 다음 자동 모드 설치 프로그램으로 STA를 설치하려면 다음 작업을 나열된 순서로 수행합니다.

- [B.3.1절. “Oracle 중앙 인벤토리 포인터 파일 만들기”](#)
- [B.3.2절. “자동 모드 설치 프로그램 응답 파일 만들기”](#)
- [B.3.3절. “자동 모드 설치 프로그램 실행”](#)

B.3.1. Oracle 중앙 인벤토리 포인터 파일 만들기

이 절차를 사용하여 Oracle 중앙 인벤토리 포인터 파일을 만듭니다(아직 존재하지 않는 경우).

1. Oracle 설치 사용자로 로그인합니다.
2. 다음 명령을 실행하여 Oracle 중앙 인벤토리 포인터 파일 존재하는지 확인합니다.

```
$ cat /etc/oraInst.loc
```

다음은 파일의 존재 여부에 따른 표시의 예입니다.

- 파일이 존재하지 않는 경우:

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

- 파일이 존재하는 경우:

```
inventory_loc=/opt/oracle/oraInventory
```

```
inst_group=oinstall
```

3. 파일이 존재하는 경우 이 절차를 종료할 수 있습니다. 그렇지 않으면 다음 단계로 진행합니다.
4. 텍스트 편집기를 사용하여 인벤토리 포인터 파일을 만듭니다. 이 파일의 이름은 *oraInst.loc*여야 합니다. 파일 내용은 *-invPtrLoc pointer_file*을 참조하십시오.
5. 원하는 디렉토리에 파일을 저장합니다. 파일을 */etc* 디렉토리에 저장하는 경우 STA 자동 모드 설치 프로그램 및 제거 프로그램이 해당 파일을 자동으로 찾습니다. 그렇지 않으면 이 유틸리티를 실행할 때 해당 위치를 지정해야 합니다.

B.3.2. 자동 모드 설치 프로그램 응답 파일 만들기

이 절차를 사용하여 자동 모드 설치 프로그램 응답 파일을 만들고 암호화된 암호를 해당 파일에 추가합니다.

1. Oracle 설치 사용자로 로그인합니다.
2. 텍스트 편집기를 사용하여 원하는 이름으로 프로그램 응답 파일을 만듭니다. 파일 템플리트는 [예 B.1. "STA 자동 모드 설치 프로그램 응답 파일 템플리트"](#)을 참조하십시오.

템플리트를 텍스트 파일로 복사해서 붙여 넣은 다음 사용자의 사이트에 맞게 변경합니다. "required"로 표시된 모든 변수에 값을 제공해야 하며 사이트에 필요한 경우 포트 번호를 변경할 수 있습니다.

- *RESPONSEFILE_LOC*
- *KEYFILE_LOC*
- 모든 *PASSWORD* 변수

3. 원하는 위치에 원하는 이름으로 파일을 저장합니다.
4. 응답 파일 작성 유틸리티가 다운로드된 디렉토리로 이동합니다. 유틸리티의 이름은 *silentInstallUtility_version.jar*입니다. 예를 들면 다음과 같습니다.

```
$ cd /Installers
```

5. 응답 파일 작성 유틸리티를 실행합니다.

```
$ java -jar silentInstallUtility_2.1.0.64.124.jar response_file
```

여기서 *response_file*은 사용자가 만든 응답 파일의 절대 경로입니다.

6. 각 프롬프트에 적절한 정보를 입력합니다. 입력한 암호 값은 화면에 표시되지 않습니다. 암호 요구 사항은 [3.3.1절. "STA 관리용 사용자 계정"](#)을 참조하십시오.

[예 B.3. "설치 프로그램 응답 파일 작성 유틸리티 실행의 예"](#)은 응답 파일 작성 유틸리티의 예입니다.

예 B.3. 설치 프로그램 응답 파일 작성 유틸리티 실행의 예

```
$ 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. 유틸리티가 완료되면 응답 파일이 있는 디렉토리에 암호화 키 파일이 만들어졌는지 확인합니다. 이 파일은 무작위로 생성된 이름("sk"로 시작됨)을 가진 숨겨진 파일입니다. 예를 들면 다음과 같습니다.

```
$ ls -la /Installers/.sk*
-r----- 1 oracle oinstall          17 Sep 22 12:00 .sk1414440339833
```

8. 응답 파일에서 다음 값을 확인합니다.
 - *RESPONSEFILE_LOC*가 올바른 응답 파일 위치로 업데이트되었습니다.
 - *KEYFILE_LOC*가 올바른 암호화 키 파일 위치로 업데이트되었습니다.
 - 모든 암호가 암호화된 값으로 업데이트되었습니다.

예 B.4. “작성 유틸리티를 사용한 후의 설치 프로그램 유틸리티 파일의 예”는 적절한 값을 보여 주는 파일의 첫 부분입니다.

예 B.4. 작성 유틸리티를 사용한 후의 설치 프로그램 유틸리티 파일의 예

```
$ 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. 자동 모드 설치 프로그램 실행

이 절차를 사용하여 자동 모드 설치 프로그램으로 STA를 설치합니다.

1. STA 설치 프로그램 위치로 이동합니다. 예를 들면 다음과 같습니다.

```
$ cd /Installers
```

2. STA 자동 모드 설치 프로그램을 시작합니다. 매개변수의 전체 정의는 [B.5절. "STA 설치 프로그램 명령 옵션"](#)을 참조하십시오.

```
$ ./sta_installer_linux64_version.bin -silent -responseFile response_file -
invPtrLoc pointer_file
```

여기서 각 항목은 다음과 같습니다.

- *version*은 다운로드한 STA 설치 프로그램의 버전입니다.
- *-silent*는 자동 모드를 나타냅니다. 이 매개변수는 필수입니다.
- *-responseFile response_file*은 자동 모드 설치 프로그램 응답 파일의 절대 경로를 지정합니다. 이 매개변수는 필수입니다.
- *-invPtrLoc pointer_file*은 Oracle 중앙 인벤토리 포인터 파일의 절대 경로를 지정합니다. 이 매개변수는 파일이 */etc* 디렉토리에 존재하지 않거나 다른 파일을 사용하려는 경우에 필요합니다.

예를 들면 다음과 같습니다.

```
$ ./sta_install_2.1.0.64.124_linux64.bin -silent -responseFile /Installers/SilentInstall.rsp -invPtrLoc /opt/oracle/oraInst.loc
```

3. 설치 프로그램은 다음 설치 단계를 수행하면서 터미널 창에 상태 메시지를 표시합니다. 이 프로세스를 완료하는 데 30~60분 정도 걸릴 수 있습니다.
 - STA 서버 환경에서 필수 조건 검사를 수행합니다.
 - MySQL, WebLogic 및 STA 응용 프로그램을 비롯하여 포함된 소프트웨어 패키지를 설치합니다.
 - 응답 파일에 제공한 설정을 사용하여 STA 환경을 구성합니다.
 - STA 응용 프로그램을 시작합니다.

예 B.5. “성공적인 STA 자동 모드 설치 최종 메시지”는 성공적으로 설치가 끝나면 표시되는 메시지를 보여 줍니다. 예 B.6. “실패한 STA 자동 모드 설치 최종 메시지”은 실패한 설치 후에 표시될 수 있는 일부 메시지를 보여 줍니다.

예 B.5. 성공적인 STA 자동 모드 설치 최종 메시지

```
...
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.
$
```

예 B.6. 실패한 STA 자동 모드 설치 최종 메시지

```
[ERROR] Rule_CalculateFreeSpace_Error. Aborting Install
Logs are located here: /tmp/OraInstall2014-09-24_09-29-29AM.
** Error during execution, error code = 256.
$
```

4. 설치 프로그램이 성공적으로 완료되면 STA가 실행 중인지 확인합니다. 자세한 내용은 [3.6.5절. “성공적인 설치 확인”](#)을 참조하십시오.

B.4. STA 자동 모드 제거 프로그램 작업

- [B.4.1절. “자동 모드 제거 프로그램 응답 파일 만들기”](#)
- [B.4.2절. “자동 모드 제거 프로그램 실행”](#)

B.4.1. 자동 모드 제거 프로그램 응답 파일 만들기

이 절차를 사용하여 자동 모드 제거 프로그램 응답 파일을 만들고 암호화된 암호를 해당 파일에 추가합니다.

1. Oracle 설치 사용자로 로그인합니다.
2. 텍스트 편집기를 사용하여 원하는 이름으로 제거 프로그램 응답 파일을 만듭니다. 파일 템플리트는 예 B.2. “STA 자동 모드 제거 프로그램 응답 파일 템플리트”를 참조하십시오.

템플리트를 텍스트 파일로 복사해서 붙여 넣습니다. 모든 변수는 비워 둡니다.

3. 원하는 위치에 원하는 이름으로 파일을 저장합니다.
4. 응답 파일 작성 유틸리티가 다운로드된 디렉토리로 이동합니다. 유틸리티의 이름은 *silentInstallUtility_version.jar*입니다. 예를 들면 다음과 같습니다.

```
$ cd /Installers
```

5. 응답 파일 작성 유틸리티를 실행합니다.

```
$ java -jar silentInstallUtility_2.1.0.64.124.jar response_file
```

여기서 *response_file*은 사용자가 만든 응답 파일의 절대 경로입니다.

6. 각 프롬프트에 적절한 정보를 입력합니다. 입력한 암호 값은 화면에 표시되지 않습니다.

예 B.7. “제거 프로그램 응답 파일 작성 유틸리티 실행의 예”은 유틸리티 실행 예입니다.

예 B.7. 제거 프로그램 응답 파일 작성 유틸리티 실행의 예

```
$ 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. 유틸리티가 완료되면 암호화 키 파일이 만들어졌는지 확인합니다. 이 파일은 무작위로 생성된 이름을 가진 숨겨진 파일입니다. 예를 들면 다음과 같습니다.

```
$ ls -la /Installers/.sk*
-r----- 1 oracle oinstall 17 Sep 22 12:00 .sk1414437879829
```

8. 응답 파일에서 다음 값을 확인합니다.
 - 시스템 루트 암호가 암호화된 값으로 업데이트되었습니다.
 - `RESPONSEFILE_LOC`가 올바른 응답 파일 위치로 업데이트되었습니다.
 - `KEYFILE_LOC`가 암호화 키 파일 위치로 업데이트되었습니다.

예 B.8. “작성 유틸리티를 사용한 후의 제거 프로그램 응답 파일의 예”은 적절한 값을 보여 주는 파일의 예입니다.

예 B.8. 작성 유틸리티를 사용한 후의 제거 프로그램 응답 파일의 예

```
$ 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 password var.
DEINSTALL_ROOT_ACCESS_PASSWORD=zMZJYDbrhIRZUQL35r7uEg==
RESPONSEFILE_LOC=/Installers/silentdeinstall.rsp
KEYFILE_LOC=/Installers/.sk1414700056981
```

B.4.2. 자동 모드 제거 프로그램 실행

이 절차를 사용하여 자동 모드 제거 프로그램으로 STA를 제거합니다.

1. Oracle 설치 사용자로 로그인합니다.
2. STA 홈 디렉토리로 이동합니다. 예를 들면 다음과 같습니다.

```
$ cd /Oracle/StorageTek_Tape_Analytics
```

3. STA 유틸리티 디렉토리로 이동합니다.

```
$ cd oui/bin
```

4. STA 자동 모드 제거 프로그램을 시작합니다. 매개변수의 전체 정의는 B.5절. “STA 설치 프로그램 명령 옵션”을 참조하십시오.

```
$ ./deinstall.sh -silent -responseFile response_file -invPtrLoc pointer_file
```

여기서 각 항목은 다음과 같습니다.

- `-silent`는 자동 모드를 나타냅니다. 이 매개변수는 필수입니다.

- `-responseFile response_file`은 STA 제거 프로그램 응답 파일의 절대 경로를 지정합니다. 이 매개변수는 필수입니다.
- `-invPtrLoc pointer_file`은 Oracle 중앙 인벤토리 포인터 파일의 절대 경로를 지정합니다. 이 매개변수는 파일이 `/etc` 디렉토리에 존재하지 않거나 다른 파일을 사용하려는 경우에 필요합니다.

예를 들면 다음과 같습니다.

```
$ ./deinstall.sh -silent -responseFile /Installers/SilentDeinst.rsp -invPtrLoc /opt/oracle/
oraInst.loc
```

5. 제거 프로그램은 다음 제거 단계를 수행하면서 터미널 창에 상태 메시지를 표시합니다. 이 프로세스를 완료하는 데 최대 30분이 걸릴 수 있습니다.

예 B.9. “성공적인 STA 자동 모드 제거 최종 메시지”는 성공적으로 설치가 끝나면 표시되는 메시지를 보여 줍니다. 예 B.10. “실패한 STA 자동 모드 제거 최종 메시지의 예”은 실패한 설치 후에 표시될 수 있는 일부 메시지를 보여 줍니다.

예 B.9. 성공적인 STA 자동 모드 제거 최종 메시지

```
...
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.
```

예 B.10. 실패한 STA 자동 모드 제거 최종 메시지의 예

```
...
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.
```

6. 제거 프로그램이 완료되면 STA 디렉토리가 제거되었는지 확인합니다. 자세한 내용은 9.2.2절. “성공적인 제거 확인”을 참조하십시오.

B.5. STA 설치 프로그램 명령 옵션

이 절에서는 STA 설치 프로그램 옵션에 대한 참조 정보를 제공합니다. 자동 모드 옵션은 자동 모드 설치 프로그램 및 제거 프로그램에서만 사용됩니다. 로깅 및 기타 옵션은 두 가지 설치/제거 모드 모두에서 사용할 수 있습니다.

B.5.1. 자동 모드 옵션

다음 옵션이 자동 모드 설치 프로그램 및 제거 프로그램에서 사용됩니다.

-force

비어 있지 않은 디렉토리로 자동 모드 설치를 수행할 수 있도록 허용합니다.

-invPtrLoc *pointer_file*

*/etc/oraInst.loc*에 있는 파일 대신 지정된 Oracle 중앙 인벤토리 포인터 파일을 사용합니다. *pointer_file*은 절대 경로여야 합니다.

Oracle 중앙 인벤토리 파일의 내용은 다음과 같습니다.

```
inventory_loc=Oracle_central_inventory_location
inst_group=Oracle_install_group
```

여기서 각 항목은 다음과 같습니다.

- *Oracle_central_inventory_location*은 Oracle 중앙 인벤토리의 절대 경로입니다.
- *Oracle_install_group*은 Oracle 설치 그룹의 이름입니다.

-response, -responseFile *response_file*

자동 모드에 필요합니다. STA 자동 모드 설치 프로그램 및 제거 프로그램에 대한 입력을 포함하는 응답 파일의 위치입니다. *response_file*은 절대 경로여야 합니다.

설치 프로그램 및 제거 프로그램 응답 파일의 내용은 예 B.1. “STA 자동 모드 설치 프로그램 응답 파일 템플리트” 및 예 B.2. “STA 자동 모드 제거 프로그램 응답 파일 템플리트”를 참조하십시오.

-silent

자동 모드에 필요합니다. 자동 모드를 사용하도록 지시합니다. 입력은 지정된 응답 파일에서 가져옵니다.

B.5.2. 로깅 옵션

다음 옵션을 통해 설치 프로그램 및 제거 프로그램 로그에서 제공하는 정보의 유형을 제어할 수 있습니다. 이 옵션은 그래픽 모드와 자동 모드 모두에서 사용할 수 있습니다.

-debug

디버그 정보를 기록합니다. 일부 디버그 정보는 콘솔 창에도 표시됩니다.

-logLevel *level*

우선 순위 레벨이 지정된 레벨보다 낮은 로그 메시지를 제외합니다. *level*의 값은 다음과 같습니다.

- severe
- warning
- info
- config
- fine
- finer
- finest

-printdiskusage

디스크 사용량에 대한 디버그 정보를 기록합니다.

-printmemory

메모리 사용량에 대한 디버그 정보를 기록합니다.

-printtime

경과 시간에 대한 디버그 정보를 기록합니다.

B.5.3. 기타 옵션

다음 명령 옵션은 일반적인 용도로 사용됩니다. 이 옵션은 그래픽 모드와 자동 모드 모두에서 사용할 수 있습니다.

-compatibilityFile *compatibility_file*

기능 세트 종속성 변경 사항을 지정하는 파일의 위치입니다.

-executeSysPrereqs

설치 프로그램을 실행하기 위한 시스템 환경 필수 조건 검사를 실행한 후 설치를 수행하지 않고 종료합니다.

-help

도움말을 표시합니다.

-i, -install

그래픽 모드를 사용합니다. 기본값입니다.

-J-Djava.io.tmpdir=*working_directory*

STA 설치 프로그램을 */tmp* 대신 지정된 작업 디렉토리에 풁니다. *working_directory*는 절대 경로여야 합니다.

-paramFile *initialization_file*

*STA_home/oui/oraparam.ini*에 있는 파일 대신 지정된 초기화 파일을 사용합니다. *initialization_file*은 절대 경로여야 합니다.

STA 설치 프로그램은 필수 조건 검사를 비롯한 모든 작업에 사용자가 지정하는 파일을 사용합니다. 기본 위치는 *STA_home/oui* 디렉토리입니다.

설치 및 업그레이드 워크시트

이 부록의 워크시트는 STA 설치 또는 업그레이드를 수행하기 위해 수집해야 하는 작업 및 정보를 구성하는 데 도움을 주는 계획 도구입니다. 이 부록에는 다음 절이 포함되어 있습니다.

- [업그레이드 준비 워크시트](#)
- [설치 및 업그레이드 워크시트](#)
- [사후 설치 구성 워크시트](#)

C.1. 업그레이드 준비 워크시트

표 C.1. “업그레이드 준비 작업”은 이전 STA 버전에서 업그레이드하는 경우에만 사용됩니다. 이 워크시트를 사용하여 업그레이드를 준비하기 위해 수행하는 필수 및 선택 작업을 추적할 수 있습니다. “메모” 열을 사용하여 특별한 계획 정보를 모두 기록합니다. 이러한 작업에 대한 자세한 내용은 [8.5절. “업그레이드 준비 작업”](#)을 참조하십시오.

표 C.1. 업그레이드 준비 작업

작업	메모	완료
현재 STA 버전이 릴리스된 버전인지 확인합니다.		
주: STA 1.0.x에서 업그레이드하는 경우 STA 2.1.0을 설치하기 전에 새 Linux 버전도 설치해야 합니다.		
단일 서버 업그레이드 방식과 두 대의 서버 업그레이드 방식 중에서 선택합니다.		
사이트 및 대상 서버가 STA 2.1.0 요구 사항을 충족하는지 확인합니다.		
업그레이드를 위해 임시로 <code>/tmp</code> 파일 시스템의 크기를 늘려야 할지 여부를 결정합니다.		
STA 2.1.0의 환경 변경 사항이 업그레이드 계획에 영향을 미치는지 검토합니다.		
필요한 모든 RPM 패키지가 설치되어 있는지 확인합니다 (STA 2.0.x에서 업그레이드하는 경우만 해당).		
현재 STA 버전이 모니터되는 각 라이브러리와 최근에 통신을 성공했는지 확인합니다.		
STA가 모니터되는 모든 라이브러리에서 교환을 처리 중인지 확인합니다.		
보존하려는 설치 및 데이터베이스 로그를 안전한 장소로 이동합니다(선택 사항).		
현재 STA 설치에서 서비스 로그 스냅샷을 만듭니다(선택 사항).		

작업	메모	완료
보존하려는 서비스 로그 번들을 다운로드합니다(선택 사항).		
STA- 로 시작하는 사용자 정의 템플릿의 이름을 바꿉니다(선택 사항).		
보존하려는 현재 사용자 정의 템플릿 설정을 기록합니다(선택 사항).		
보존하려는 실행 보고서 정책 설정을 기록합니다(선택 사항).		

C.2. 설치 및 업그레이드 워크시트

이 워크시트에는 STA 설치 프로그램에 필요한 정보가 포함되어 있습니다. 요청되는 정보에 대한 자세한 내용은 3.3절. “STA 설치 중 구성되는 계정 및 포트”를 참조하십시오.

이전 STA 버전에서 업그레이드하는 경우 워크시트의 "현재" 열을 사용하여 현재 설치에 사용된 값을 기록할 수 있습니다. "STA 2.1.0" 열을 사용하여 STA 2.1.0에 사용할 값을 기록합니다.

C.2.1. 설치 사용자 및 위치 워크시트

표 C.2. “설치 사용자 및 위치 워크시트”에는 STA 설치 프로그램을 실행하는 데 필요한 사용자 계정 및 위치가 포함되어 있습니다.

표 C.2. 설치 사용자 및 위치 워크시트

항목	설명	현재 값	STA 2.1.0 값
Oracle 설치 그룹	STA 서버에 Oracle 제품을 설치 및 업그레이드하는 데 사용되는 Linux 그룹입니다. STA 2.1.0에 새로 도입되었습니다.		
Oracle 설치 사용자	STA 서버에 Oracle 제품을 설치 및 업그레이드하는 데 사용되는 Linux 사용자입니다. STA 2.1.0에 새로 도입되었습니다.		
Oracle 중앙 인벤토리 위치	STA 서버에 설치된 Oracle 제품에 대한 정보를 추적하는 데 사용되는 디렉토리입니다. STA 2.1.0에 새로 도입되었습니다.		
Oracle 스토리지 홈 위치	STA 및 이와 연관된 Oracle 소프트웨어가 설치된 디렉토리입니다. STA 2.1.0에 새로 도입되었습니다.		
STA 설치 프로그램 위치	STA 설치 프로그램이 다운로드되는 위치입니다.		
STA 데이터베이스 데이터 위치	STA 데이터베이스의 위치입니다.		
STA 데이터베이스 백업 위치	STA 서버의 STA 데이터베이스 백업 위치입니다.		

C.2.2. 사용자 계정 워크시트

표 C.3. “사용자 계정 워크시트”에는 STA 관리 작업을 수행하는 데 사용할 사용자 계정 및 STA 응용 프로그램이 STA 데이터베이스를 액세스 및 관리하기 위해 내부적으로 사용하는 MySQL 계정이 포함됩니다.

주:

STA 2.1.0에서는 암호 요구 사항이 변경되었습니다. 자세한 내용은 3.2절, “사용자 이름 및 암호 요구 사항”을 참조하십시오.

표 C.3. 사용자 계정 워크시트

계정	설명	현재 사용자 이름 및 암호	STA 2.1.0 사용자 이름 및 암호
WebLogic 관리	WebLogic 관리 콘솔에 로그인하는 데 사용됩니다. 주의: 이 계정의 사용자 이름 및 암호는 검색할 수 없습니다. 이 자격 증명을 분실하면 STA를 재설치해야 합니다.		
STA 관리자	전체 액세스 권한으로 STA 응용 프로그램에 로그인하는 데 사용됩니다.		
STA 데이터베이스 루트 사용자	MySQL 데이터베이스를 소유합니다. 사전 정의된 사용자 이름인 <i>root</i> 는 변경할 수 없습니다. 주의: 이 계정의 암호는 검색할 수 없습니다.	사용자 이름 = <i>root</i>	사용자 이름 = <i>root</i>
STA 데이터베이스 응용 프로그램 사용자	STA는 이 계정을 사용하여 데이터베이스에 연결합니다.		
STA 데이터베이스 보고서 사용자	STA 이외의 프로그램 및 타사 응용 프로그램은 이 계정을 사용하여 데이터베이스에 연결합니다.		
STA 데이터베이스 관리자 사용자	STA 관리 및 모니터링 유틸리티는 이 계정을 사용하여 데이터베이스에 연결하며, 주로 예약된 백업을 수행합니다.		

C.2.3. 포트 번호 워크시트

표 C.4. “구성 불가능한 외부 포트”에는 STA 응용 프로그램에서 사용하는 외부 포트가 포함됩니다. 이러한 포트 번호는 미리 정의되어 있으며 변경할 수 없습니다. “확인” 열을 사용하여 네트워크 관리자에게 이 포트가 열려 있으며 사용 가능한지 확인했음을 기록합니다.

표 C.4. 구성 불가능한 외부 포트

포트 설명	프로토콜	STA 2.1.0 포트	확인
보안 셸입니다. STA 서버에서 STA 데이터베이스 백업 및 모니터링되는 라이브러리로 로그인하는 데 사용됩니다.	SSH	22	
SNMP(Simple Network Management Protocol) 요청을 모니터링되는 라이브러리로 전송하는 데 사용됩니다.	SNMP	161	
모니터되는 라이브러리에서 SNMP 알림(트랩)을 받는 데 사용됩니다.	SNMPTRAP	162	

표 C.5. “구성 가능한 내부 및 외부 포트”에는 STA 응용 프로그램이 사용하는 구성 가능한 외부 및 내부 포트가 포함됩니다. “확인” 열을 사용하여 네트워크 관리자에게 이 포트가 열려 있으며 사용 가능한지 확인했음을 기록합니다.

주:

STA 2.1.0에서는 기본 WebLogic 관리 콘솔 포트가 변경되었습니다.

표 C.5. 구성 가능한 내부 및 외부 포트

포트 설명	유형	프로토콜	STA 2.1.0 기본 포트	현재 포트	STA 2.1.0 확인 포트	확인
WebLogic 관리 콘솔에 대한 비보안 포트(STA 1.0.x 및 2.0.x의 기본값은 7001)	외부	HTTP	7019			
WebLogic 관리 콘솔에 대한 보안 포트(STA 1.0.x 및 2.0.x의 기본값은 7002)	외부	HTTPS	7020			
STA GUI를 관리하는 staUi 관리 서버에 대한 비보안 포트	외부	HTTP	7021			
staUi 관리 서버에 대한 비보안 포트	외부	HTTPS	7022			
기본 STA 내부를 관리하는 staEngine 관리 서버에 대한 비보안 포트	내부	HTTP	7023			
staEngine 관리 서버에 대한 보안 포트	내부	HTTPS	7024			
모니터되는 라이브러리와 SNMP 통신을 관리하는 staAdapter 관리 서버에 대한 비보안 포트	내부	HTTP	7025			
staAdapter 관리 서버에 대한 보안 포트	내부	HTTPS	7026			

C.2.4. 도메인 이름 워크시트

표 C.6. “회사 도메인 이름”에는 STA 서비스 로그를 생성할 때 Oracle의 RDA(Remote Diagnostic Agent)가 사용하는 사이트의 정규화된 도메인 이름이 포함됩니다.

표 C.6. 회사 도메인 이름

필요한 정보	현재 값	STA 2.1.0 값
회사 도메인 이름(예: us.example.com)		

C.3. 사후 설치 구성 워크시트

표 C.7. “SNMP v3 사용자 구성 정보”에는 STA와 모니터되는 라이브러리 사이의 SNMP 연결을 구성하는 데 사용하는 정보가 포함됩니다. 모니터되는 각 라이브러리와 STA 인스턴스에서 동일한 SNMP v3 사용자를 구성해야 합니다. 요청되는 정보에 대한 자세한 내용은 5.1.1.1절. “고유한 SNMP v3 사용자”를 참조하십시오.

표 C.7. SNMP v3 사용자 구성 정보

필요한 정보	이전 값	STA 2.1.0 값
SNMP v3 사용자 이름		
SNMP v3 권한 부여 암호(Auth)		
SNMP v3 프라이버시 암호화 암호(Privacy)		
SNMP v2c 사용자 커뮤니티		
SNMP v2c 트랩 커뮤니티		

보안 자격 증명 구성

Oracle은 HTTPS/SSL 포트에서 사용할 자체 생성된 보안 인증서를 제공합니다. 설치 중 STA는 Java keytool을 통해 STA 서버에 서버 호스트 이름을 사용하여 인증서를 생성합니다. 선택적으로 Oracle 인증서를 선택한 인증 기관(예: VeriSign)에서 승인된 고유의 인증서로 바꿀 수 있습니다.

이 장은 다음과 같은 절로 구성됩니다.

- [보안 인증서 구성 작업](#)

D.1. 보안 인증서 구성 작업

기본값과 다른 보안 인증서를 사용하려는 경우 나열된 순서대로 이 절차를 수행하십시오.

- [D.1.1절. “초기 HTTPS/SSL 연결 설정”](#)
- [D.1.2절. “다른 보안 인증서를 사용하도록 WebLogic 재구성”](#)
- [D.1.3절. “Oracle 인증서 바꾸기”](#)

주:

이 절차에서는 Windows 플랫폼에서 실행되는 Mozilla Firefox를 사용합니다.

D.1.1. 초기 HTTPS/SSL 연결 설정

1. 컴퓨터에서 지원되는 웹 브라우저를 시작하고 STA 응용 프로그램에 대한 URL의 HTTPS/SSL 버전을 입력합니다.

```
https://STA_host_name:port_number/STA/
```

여기서 각 항목은 다음과 같습니다.

- *host_name*은 STA 서버의 호스트 이름입니다.
- *port_number*는 설치 중 지정한 STA 포트 번호입니다. 기본 HTTP 포트는 7021이고, 기본 HTTPS 포트는 7022입니다.
- *STA*는 대문자여야 합니다.

예를 들면 다음과 같습니다.

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

Connection is Untrusted 화면이 표시됩니다.

2. **I Understand the Risks**를 선택한 다음 **Add Exception**을 누릅니다.

Add Security Exception 화면이 표시됩니다.

3. **View**를 누릅니다.

Certificate Viewer 화면이 표시됩니다. 인증서는 인증 기관의 인증서가 아니므로 확인된 것으로 표시되지 않습니다.

4. 인증서를 검토하기 위해 **Details** 탭을 누릅니다.
5. Certificate Fields 패널에서 **issuer**를 선택합니다. 다음은 표시 샘플입니다. CN은 인증서가 생성된 서버 이름을 나타냅니다.

```
CN = staserver.example.com
OU = Tape Systems
O = Oracle America Inc
L = Redwood City
ST = California
C = USA
```

6. **Close**를 눌러 Add Security Certificate 화면으로 돌아갑니다.
7. **Confirm Security Exception**을 선택합니다.

인증서가 STA 서버에 추가되었으므로 이제 이 인증서로 HTTPS를 사용할 수 있습니다.

D.1.2. 다른 보안 인증서를 사용하도록 WebLogic 재구성

1. 브라우저 창을 열고 WebLogic 관리 콘솔의 URL을 입력합니다. 기본 HTTP 포트는 7019이고, 기본 HTTPS 포트는 7020입니다.

https://your_hostname:port number/console/

예를 들면 다음과 같습니다.

https://staserver.company.com:7019/console/

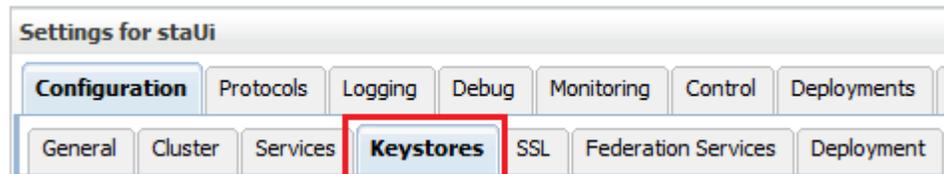
2. STA 설치 중 정의한 WebLogic 관리 콘솔 사용자 이름과 암호를 사용하여 로그인합니다.
3. Domain Structure 섹션에서 **Environment**를 선택한 후 **Servers**를 선택합니다.



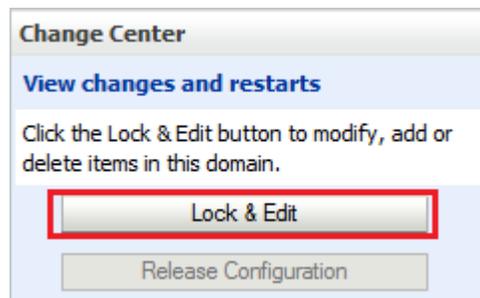
4. Servers 테이블에서 **staUi** 활성 링크를 선택합니다(확인란이 아닌 이름 자체를 선택).

<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	

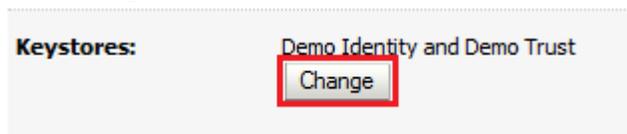
5. **Keystores** 탭을 선택합니다.



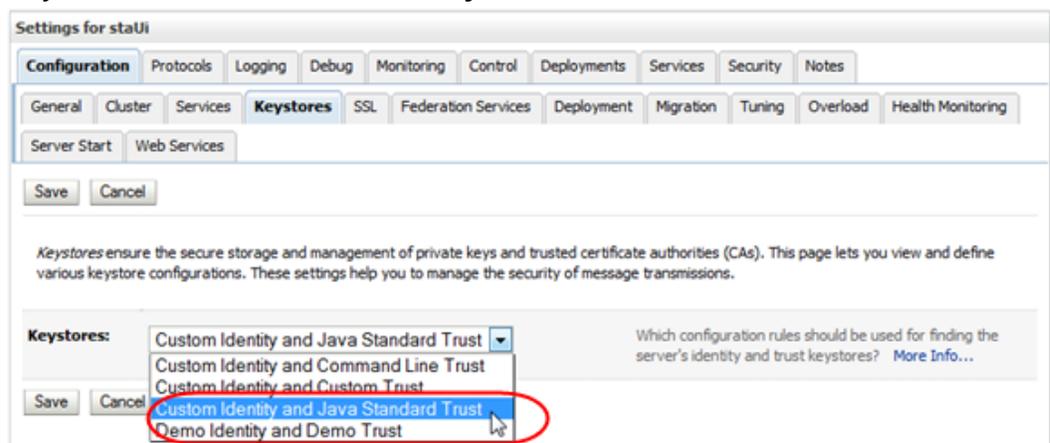
6. Change Center 섹션에서 **Lock & Edit**를 누릅니다.



7. Keystores 섹션에서 **Change**를 누릅니다.



8. Keystores 메뉴에서 **Custom Identity and Java Standard Trust**를 선택합니다.



9. **Save**를 누릅니다.

10. 다음과 같이 Keystores 화면을 채웁니다.

- **Custom Identity Keystore:** 개인 키 파일의 경로와 파일입니다.
- **Custom Identity Keystore Type:** 키 저장소 유형입니다. RACF 인증에 대해 구성하는 경우 PKCS12를 입력합니다.
- **Custom Identity Keystore Passphrase:** MVS 시스템 관리자가 제공한 암호입니다.
- **Java Standard Trust Keystore Passphrase:** Java Standard Trust Keystore 파일에 대한 새 암호입니다.

주의:

이러한 암호를 잊어버린 경우 STA를 재설치해야 합니다.

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

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

Keystores: Custom Identity and Java Standard Trust [Change](#) Which configuration rules should be used for finding the server's identity and trust keystores? [More Info...](#)

— Identity —

Custom Identity Keystore: /Oracle/Middleware/us The path and file name of the identity keystore. [More Info...](#)

Custom Identity Keystore Type: PKCS12 The type of the keystore. Generally, this is JKS. [More Info...](#)

Custom Identity Keystore Passphrase: [Masked] The encrypted custom identity keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. [More Info...](#)

Confirm Custom Identity Keystore Passphrase: [Masked]

— Trust —

Java Standard Trust Keystore: /Orade/StorageTek_Tape_Analytics/jdk1.6.0_75/jre/lib/security/cacerts The path and file name of the trust keystore. [More Info...](#)

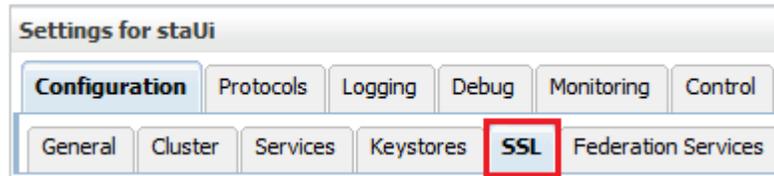
Java Standard Trust Keystore Type: jks The type of the keystore. Generally, this is JKS. [More Info...](#)

Java Standard Trust Keystore Passphrase: [Masked] The password for the Java Standard Trust keystore. This password is defined when the keystore is created. [More Info...](#)

Confirm Java Standard Trust Keystore Passphrase: [Masked]

Save

11. **Save**를 누릅니다.
12. **SSL** 탭을 선택합니다.



13. MVS 시스템 프로그래머가 제공한 Private Key Alias 및 Private Key Passphrase를 입력합니다.

주:

Private Key Alias를 확인하려면 시스템 명령줄에서 `keytool` 명령을 사용하십시오. 예를 들면 다음과 같습니다.

```
# keytool -list -keystore CLTBI.PKCS12DR.D080411 -storetype PKCS12
```

```
Enter keystore password: (password from the MVS sysadmin)
```

```
Keystore type: PKCS12
```

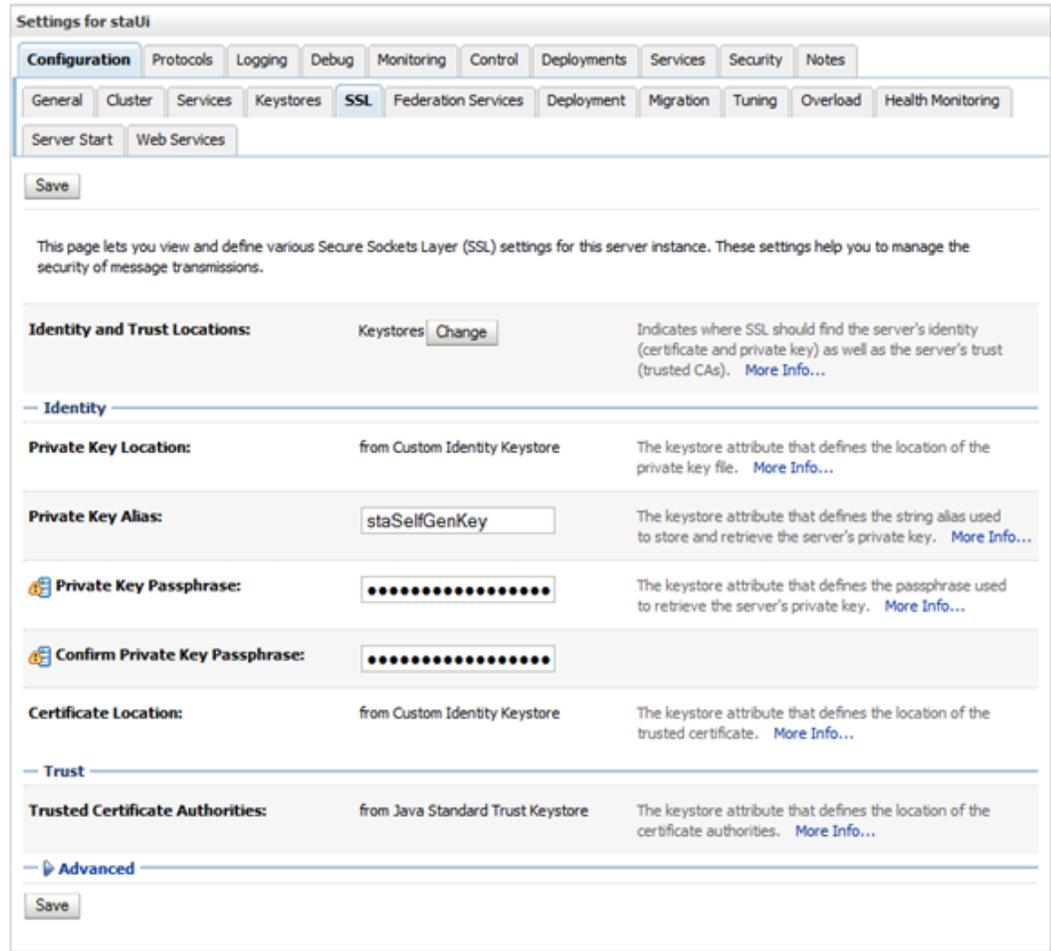
```
Keystore provider: SunJSSE
```

```
Your keystore contains 1 entry
```

```
tbiclient, Aug 17, 2011, PrivateKeyEntry,
```

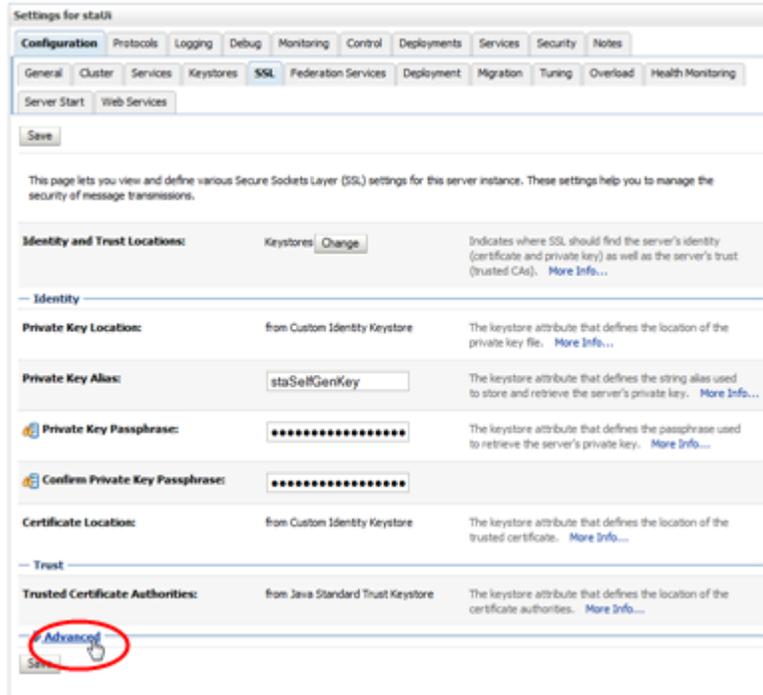
```
Certificate fingerprint (MD5):
```

```
9A:F7:D1:13:AE:9E:9C:47:55:83:75:3F:11:0C:BB:46
```



14. **Save**를 누릅니다.

15. Trusted Certificate Authorities 섹션에서 **Advanced**를 누릅니다.



16. SSL 화면의 Advanced 섹션을 다음과 같이 채웁니다.

- a. **Use Server Certs** 확인란을 선택합니다.
- b. **Two Way Client Cert Behavior** 메뉴에서 Client Certs Requested But Not Enforced를 선택합니다.
- c. **Inbound Certification Validation** 및 **Outbound Certificate Validation** 메뉴에서 Builtin SSL Validation Only를 선택합니다.

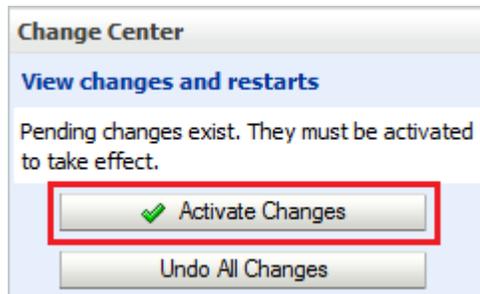
Advanced

Hostname Verification:	BEA Hostname Verifier	Specifies whether to ignore the installed implementation of the <code>weblogic.security.SSL.HostnameVerifier</code> 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 <code>weblogic.security.SSL.HostnameVerifier</code> 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...
<input checked="" type="checkbox"/> 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 <code>weblogic.security.ad.CertAuthenticator</code> 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...
<input checked="" type="checkbox"/> SSLRejection Logging Enabled		Indicates whether warning messages are logged in the server log when SSL connections are rejected. More Info...
<input type="checkbox"/> Allow Unencrypted Null Cipher		Test if the <code>AllowUnEncryptedNullCipher</code> 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...
<input type="checkbox"/> Use JSSE SSL		Select the JSSE SSL implementation to be used in Weblogic. More Info...

Save

17. **Save**를 누릅니다.

18. Change Center 섹션에서 **Activate Changes**를 누릅니다.



19. WebLogic에서 로그아웃합니다.

20. STA 명령을 사용하여 STA를 중지하고 다시 시작합니다. 명령 사용법 세부 정보는 STA 관리 설명서를 참조하십시오.

```
# STA stop all
# STA start all
```

D.1.3. Oracle 인증서 바꾸기

1. 컴퓨터에서 지원되는 웹 브라우저를 시작하고 STA 응용 프로그램에 대한 URL의 HTTPS/SSL 버전을 입력합니다.

```
https://STA_host_name:port_number/STA/
```

여기서 각 항목은 다음과 같습니다.

- *host_name*은 STA 서버의 호스트 이름입니다.
- *port_number*는 설치 중 지정한 STA 포트 번호입니다. 기본 HTTP 포트는 7021이고, 기본 HTTPS 포트는 7022입니다.
- *STA*는 대문자여야 합니다.

예를 들면 다음과 같습니다.

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

2. This Connection is Untrusted 화면에서 **I Understand the Risks**를 선택합니다.
3. **Add Exception**을 누릅니다.
4. 자신의 조직에 대한 인증서를 지정하려면 Add Security Certificate 화면에서 **Get Certificate**를 누르고 알맞은 파일을 선택합니다.
5. **Confirm Security Exception**을 누릅니다.

STA의 보안 서비스 공급자 구성

사용자가 STA에 액세스하려면 먼저 인증을 받아야 합니다. STA 내에서 로컬로 사용자를 만들 수도 있고, 외부 SSP(보안 서비스 공급자)를 사용하여 STA에 대한 액세스 제어를 제공할 수도 있습니다.

이 부록에서는 STA 액세스 제어를 위해 WebLogic OpenLDAP(Lightweight Directory Access Protocol) 및 IBM RACF(Resource Access Control Facility)를 사용하는 방법에 대해 설명합니다 다음과 같은 절로 구성됩니다.

- [WebLogic OpenLDAP를 통한 STA 액세스 제어](#)
- [IBM RACF 작업을 통한 STA 액세스 제어](#)

STA 응용 프로그램을 사용하여 사용자를 만들려면 *STA* 사용 설명서를 참조하십시오.

E.1. WebLogic OpenLDAP를 통한 STA 액세스 제어

이 절차를 사용하여 STA에 대해 OpenLDAP를 구성합니다.

E.1.1. WebLogic OpenLDAP 구성

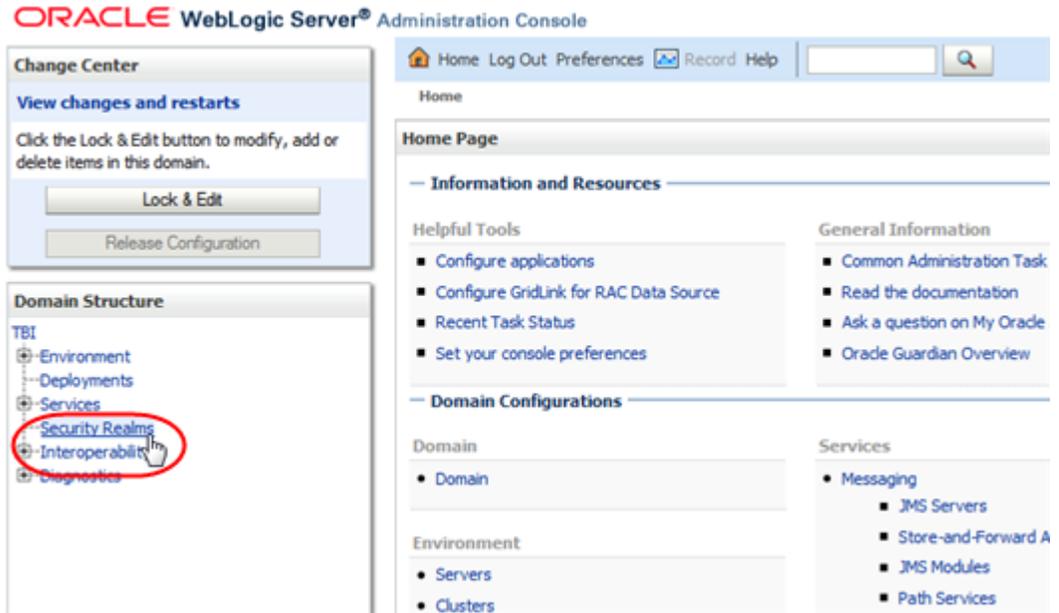
1. STA 설치 중 선택한 HTTP(STA 2.1.0 기본값은 7019) 또는 HTTPS(STA 2.1.0 기본값은 7020) 포트 번호를 사용하여 WebLogic 콘솔 로그인 화면으로 이동합니다.

```
https://yourHostName:PortNumber/console/
```

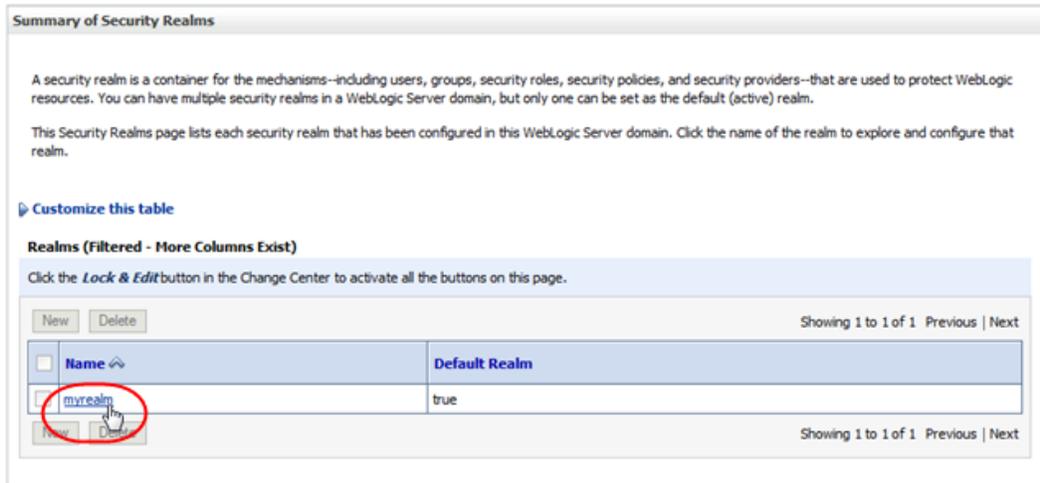
예를 들면 다음과 같습니다.

```
https://sta_server:7020/console
```

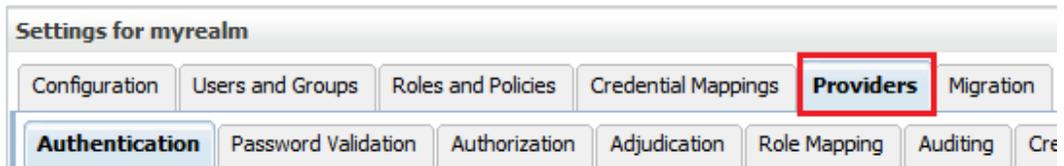
2. STA 설치 중 정의한 WebLogic 관리 콘솔 사용자 이름과 암호를 사용하여 로그인합니다.
3. Domain Structure 섹션에서 **Security Realms**를 누릅니다.



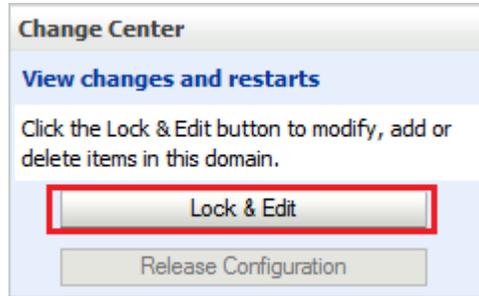
4. Realms 테이블에서 **myrealm** 활성 링크를 선택합니다(확인란이 아닌 링크 자체를 선택).



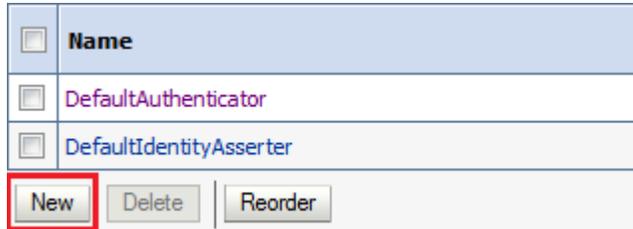
5. **Providers** 탭을 누릅니다.



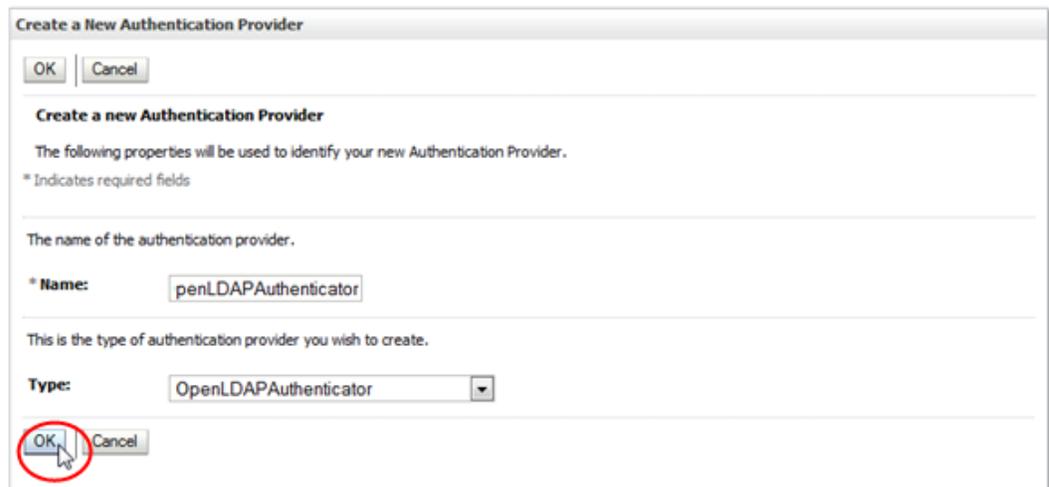
6. Change Center 섹션에서 **Lock & Edit**를 누릅니다.



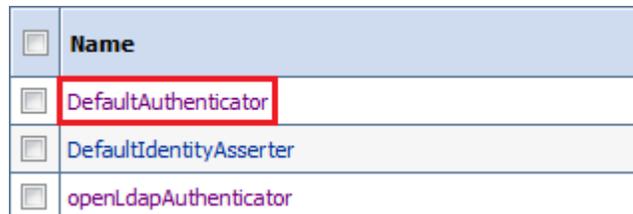
7. Authentication Providers 섹션에서 **New**를 누릅니다.



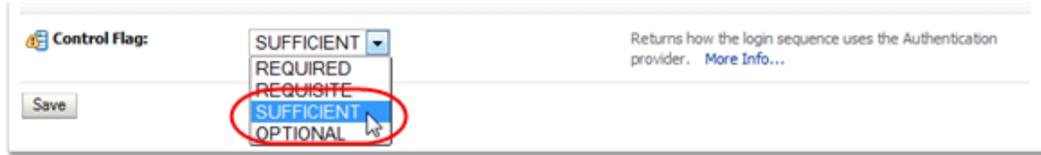
8. 만들려는 인증 공급자의 이름(예: OpenLdapAuthenticator)을 입력하고 **Type** 메뉴에서 OpenLDAPAuthenticator를 선택합니다. **OK**를 누릅니다.



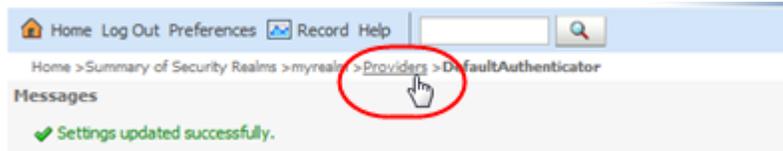
9. **DefaultAuthenticator** 활성 링크를 선택합니다(확인란이 아닌 링크 자체를 선택).



10. **Control Flag** 메뉴에서 Sufficient를 선택한 다음 **Save**를 누릅니다.



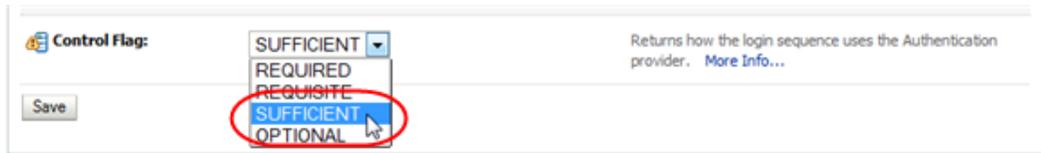
11. **Providers** 로케이터 링크를 선택하여 Authentication Providers 화면으로 돌아갑니다.



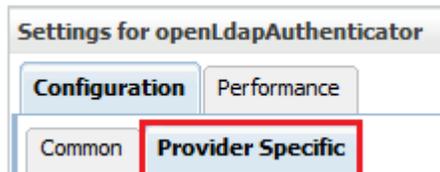
12. Authentication Providers 테이블에서 8 단계에서 만든 OpenLDAP 인증자 이름을 선택합니다(확인란이 아닌 이름 자체를 선택).

<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** 메뉴에서 Sufficient를 선택한 다음 **Save**를 누릅니다.



14. **Provider Specific** 탭을 누릅니다.

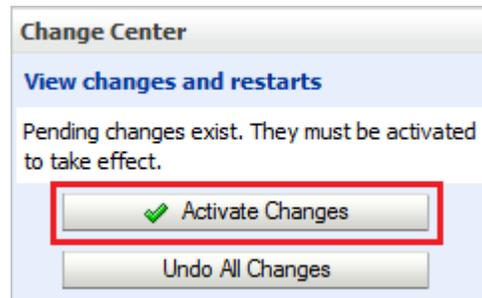


15. 사이트 요구 사항에 따라 화면 필드를 채웁니다. 다음 예는 *Ises-ldap1* 서버에 적용되며 각 고객 환경에 특정된 것입니다.

- Host = *Ises-ldap1*
- Port = 389
- Principal = 비워 둠
- Credential = 비워 둠
- 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. **Save**를 누릅니다.

17. Change Center 섹션에서 **Activate Changes**를 누릅니다.



18. 다음 단계를 수행하여 구성을 테스트합니다.

- a. WebLogic 관리 콘솔에서 로그아웃합니다.
- b. STA 명령을 사용하여 STA를 중지하고 다시 시작합니다. 명령 사용법 세부 정보는 STA 관리 설명서를 참조하십시오.

```
# STA stop all
# STA start all
```

- c. WebLogic 콘솔에 로그인합니다.
- d. Domain Structure 섹션에서 **Security Realms**를 선택합니다.
- e. Realms 테이블에서 **myrealm** 활성 링크를 선택합니다(확인란이 아닌 링크 자체를 선택).
- f. **Users and Groups** 탭을 누릅니다.



- g. **Users** 및 **Groups** 탭에서 OpenLDAP 공급자에 대한 항목이 Provider 열에 존재하는지 확인합니다.

E.2. IBM RACF 작업을 통한 STA 액세스 제어

다음 절차를 사용하여 STA에 대한 IBM RACF(Resource Access Control Facility) 인증을 구성합니다. 나열된 순서대로 절차를 완료해야 합니다.

- E.2.1절. “작업 1: IBM RACF 메인프레임 최소 요구 사항 검토”
- E.2.2절. “작업 2: STA RACF 권한 부여를 위한 메인프레임 지원 사용으로 설정”
- E.2.3절. “작업 3: AT-TLS 구성”
- E.2.4절. “작업 4: CGI 루틴에서 사용되는 RACF 프로파일 만들기”
- E.2.5절. “작업 5: 인증서 파일 및 개인 키 파일 가져오기(선택 사항)”
- E.2.6절. “작업 6: CGI 루틴 테스트”
- E.2.7절. “작업 7: WebLogic 콘솔에 대한 RACF/SSP 설정”
- E.2.8절. “작업 8: STA와 RACF 간 SSL 구성”
- E.2.9절. “작업 9: WebLogic Server 구성”

- E.2.10절. “작업 10: WebLogic 콘솔에 RACF/SSP 설치”

주:

STA는 IBM RACF와 호환되는 타사 제품을 지원합니다(예: CA의 ACF - 2 및 Top Secret). 설치된 보안 제품에 알맞은 명령을 실행하는 것은 STA를 설치하는 사람 또는 보안 관리자의 책임입니다.

E.2.1. 작업 1: IBM RACF 메인프레임 최소 요구 사항 검토

RACF 요구 사항에 대한 자세한 내용은 STA 요구 사항 설명서를 참조하십시오.

E.2.2. 작업 2: STA RACF 권한 부여를 위한 메인프레임 지원 사용으로 설정

STA에 대한 RACF 서비스의 메인프레임 측면은 ELS 7.0 및 7.1에 대한 SMC 구성 요소의 일부인 CGI 루틴으로 제공됩니다. 이 CGI 루틴은 SMC HTTP 서버에 의해 호출되고 FACILITY 클래스에서 정의된 RACF 프로파일을 사용합니다.

STA가 RACF를 액세스 인증 방법으로 사용하려면 메인프레임에서 HTTP 서버를 실행하는 SMC 시작 작업을 설정해야 합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 ELS 문서 *Configuring and Managing SMC*에서 찾을 수 있습니다.

주:

SMC 시작 작업은 정의된 AT-TLS 규칙과 일치해야 합니다. 또는 AT-TLS 정의에서 일반 작업 이름(예: SMCW)을 사용할 수 있도록 허용하십시오.

값이 제공된 STC 식별자(예: JOBNAME.JOB)를 사용할 경우 이로 인해 CGI 루틴 연결을 실패합니다.

HTTP 서버에 사용되는 포트 번호는 WebLogic 콘솔에서 정의된 포트 번호와 일치해야 하고, 호스트는 SMC 작업이 실행되는 호스트에 대한 IP 이름과 일치해야 합니다.

주:

기존 SMC는 RACF 권한 부여가 수행될 호스트에 존재하는 경우 사용할 수 있습니다. 이러한 경우 WebLogic 구성을 수행할 때 기존 HTTP 서버의 포트 번호를 사용하십시오.

E.2.3. 작업 3: AT-TLS 구성

AT-TLS는 응용 프로그램 서버 및 클라이언트에 투명한 TCP/IP 응용 프로그램에 대한 암호화 솔루션입니다. 패킷 암호화 및 해독은 TCP 프로토콜 레벨의 z/OS TCPIP 주소 공간에서 발생합니다. RACF 권한 부여를 위한 AT - TLS 요구 사항은 STA 요구 사항 설명서에 나와 있습니다.

다음 RACF 명령은 구성 프로세스에서 정의할 다양한 RACF 객체의 상태를 나열합니다.

- *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-TLS를 구성하려면 다음 작업을 수행하십시오.

1. TCP/IP 프로파일 데이터 세트에 다음 매개변수를 지정하여 AT - TLS를 활성화합니다.

TCPCONFIG TTLS

이 명령문은 TCP OBEY 파일에 놓일 수 있습니다.

2. 정책 에이전트(PAGENT) 구성

정책 에이전트 주소 공간은 어떤 TCP/IP 트래픽이 암호화되는지 제어합니다.

- a. PAGENT 시작 작업 JCL을 입력합니다.

예를 들면 다음과 같습니다.

```
//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 환경 변수를 입력합니다. *pagentdataset* 데이터 세트에 PAGENT 환경 변수가 포함됩니다.

예를 들면 다음과 같습니다.

```
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
```

이 예에서는 */etc/pagent.conf*에 PAGENT 구성 매개변수가 포함됩니다. TZ 매개 변수에 대해 해당하는 시간대를 사용합니다.

- c. PAGENT를 구성합니다.

예를 들면 다음과 같습니다.

```
TTLRule TBI-T0-ZOS
{
  LocalAddr localtcpipaddress
  RemoteAddr remotetcpipaddress
  LocalPortRange localportrange
  RemotePortRange remoteportrange
  Jobname HTTPserverJobname
  Direction Inbound
  Priority 255
  TTLGroupActionRef gAct1~TBI_ICSF
  TTLEnvironmentActionRef eAct1~TBI_ICSF
  TLSConnectionActionRef cAct1~TBI_ICSF
}
TTLGroupAction gAct1~TBI_ICSF
{
  TTLEnabled On
  Trace 2
}
TTLEnvironmentAction eAct1~TBI_ICSF
{
  HandshakeRole Server
  EnvironmentUserInstance 0
  TLSKeyringParmsRef keyR~ZOS
}
TLSConnectionAction cAct1~TBI_ICSF
{
  HandshakeRole ServerWithClientAuth
  TLSCipherParmsRef cipher1~AT-TLS__Gold
  TLSConnectionAdvancedParmsRef cAdv1~TBI_ICSF
  CtraceClearText Off
  Trace 2
}
TLSConnectionAdvancedParms cAdv1~TBI_ICSF
{
  ApplicationControlled Off
  HandshakeTimeout 10
  ResetCipherTimer 0
  CertificateLabel certificatelabel
  SecondaryMap Off
}
TLSKeyringParms keyR~ZOS
{
  Keyring keyringname
}
TLSCipherParms cipher1~AT-TLS__Gold
```

```
{
  V3CipherSuites TLS_RSA_WITH_3DES_EDE_CBC_SHA
  V3CipherSuites TLS_RSA_WITH_AES_128_CBC_SHA
}
```

여기서 각 항목은 다음과 같습니다.

- *localtcpipaddress*: HTTP 서버의 로컬 TCP/IP 주소
- *remotetcpipaddress*: STA 클라이언트의 원격 TCP/IP 주소. 모든 TCP/IP 주소에 대해 ALL이 될 수 있습니다.
- *localportrange*: HTTP 서버의 로컬 포트(HTTP 또는 SMC 시작 시 지정됨)
- *remoteportrange*: 원격 포트 범위(모든 임시 포트에 대해 1024-65535)
- *HTTPserverJobname*: HTTP 서버의 작업 이름
- *certificateLabel*: 인증서 정의의 레이블
- *keyringname*: RACF Keyring 정의의 이름

3. RACF 클래스를 활성화합니다. RACF 패널 또는 CLI를 사용할 수 있습니다.

RACF 클래스에는 다음이 포함됩니다.

- *DIGTCERT*
- *DIGTNMAP*
- *DIGTRING*

SERVAUTH 클래스는 *PORTMAP* 및 *RXSERV*가 비정상 종료되지 않도록 *RACLIST*되어야 합니다.

```
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 Keyring 및 인증서 정의

- a. 다음 RACF 명령을 입력하여 Keyring 및 인증서를 만듭니다.

```
RACDCERT ID(stcuser) ADDRING(keyringname)
```

여기서 각 항목은 다음과 같습니다.

- *stcuser*: TCPIP 주소 공간과 연관된 RACF 사용자 ID
- *keyringname*: keyring의 이름이며, PAGENT 구성에 지정된 Keyring과 일치해야 함

```
RACDCERT ID(stcuser) GENCERT CERTAUTH SUBJECTSDN(CN('serverdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('calabel') TRUST
SIZE(1024) KEYUSAGE(HANDSHAKE, DATAENCRYPT, CERTSIGN)
```

주:

STA 시스템에 대한 CA 인증서입니다.

여기서 각 항목은 다음과 같습니다.

- *stcuser*: TCPIP 주소 공간과 연관된 RACF 사용자 ID
- *serverdomainname*: z/OS 서버의 도메인 이름(예: *MVSA.COMPANY.COM*)
- *companyname*: 조직 이름
- *unitname*: 조직 단위 이름
- *country*: 국가
- *calabel*: 인증 기관에 대한 레이블(예: *CATBISERVER*)

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('serverdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('serverlabel') TRUST
SIZE(1024) SIGNWITH(CERTAUTH LABEL('calabel'))
```

주:

SERVER 인증서입니다.

여기서 각 항목은 다음과 같습니다.

- *stcuser*: TCPIP 주소 공간과 연관된 RACF 사용자 ID
- *serverdomainname*: z/OS 서버의 도메인 이름(예: *MVSA.COMPANY.COM*)
- *companyname*: 조직 이름
- *unitname*: 조직 단위이름
- *country*: 국가
- *serverlabel*: 서버 인증서에 대한 레이블(예: *TBISERVER*)
- *calabel*: CA 인증서 정의에 지정된 인증 기관에 대한 레이블

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('clientdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('clientlabel') TRUST
SIZE(1024) SIGNWITH(CERTAUTH LABEL('calabel'))
```

주:

CLIENT 인증서입니다.

여기서 각 항목은 다음과 같습니다.

- *stcuser*: TCPIP 주소 공간과 연관된 RACF 사용자 ID
- *clientdomainname*: STA 클라이언트의 도메인 이름(예: *TBIA.COMPANY.COM*)

- *companyname*: 조직 이름
 - *unitname*: 조직 단위 이름
 - *country*: 국가
 - *clientlabel*: 서버 인증서에 대한 레이블 –TBICLIENT
 - *calabel*: CA 인증서 정의에 지정된 인증 기관에 대한 레이블
- b. CA, SERVER 및 CLIENT 인증서를 PAGENT 구성에 지정된 Keyring에 연결합니다.

```
RACDCERT ID(stcuser) CONNECT(CERTAUTH LABEL('calabel') RING('keyringname')
  USAGE(CERTAUTH))
```

여기서 각 항목은 다음과 같습니다.

- *stcuser*: TCPIP 주소 공간과 연관된 RACF 사용자 ID
- *calabel*: CA 인증서 정의에 지정된 인증 기관에 대한 레이블
- *keyringname*: keyring의 이름이며, PAGENT 구성에 지정된 Keyring과 일치해야 함

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('serverlabel')
  RING('keyringname') DEFAULT USEAGE(PERSONAL))
```

여기서 각 항목은 다음과 같습니다.

- *stcuser*: TCPIP 주소 공간과 연관된 RACF 사용자 ID
- *serverlabel*: 서버 인증서에 대한 레이블
- *keyringname*: keyring의 이름이며, PAGENT 구성에 지정된 Keyring과 일치해야 함

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('clientlabel')
  RING('keyringname') USEAGE(PERSONAL))
```

여기서 각 항목은 다음과 같습니다.

- *stcuser*: TCPIP 주소 공간과 연관된 RACF 사용자 ID
 - *clientlabel*: 클라이언트 인증서에 대한 레이블
 - *keyringname*: keyring의 이름이며, PAGENT 구성에 지정된 Keyring과 일치해야 함
- c. STA로 전송할 CA 및 클라이언트 인증서를 내보냅니다.

```
RACDCERT EXPORT (LABEL('calabel')) CERTAUTH DSN('datasetname') FORMAT(CERTB64)
```

여기서 각 항목은 다음과 같습니다.

- *calabel*: CA 인증서 정의에 지정된 인증 기관에 대한 레이블

- *datasetname*:: 내보낸 인증서를 수신할 데이터 세트

```
RACDCERT EXPORT (LABEL('clientlabel')) ID(stcuser) DSN('datasetname')
FORMAT(PKCS12DER) PASSWORD(' password ')
```

여기서 각 항목은 다음과 같습니다.

- *clientlabel*: 클라이언트 인증서에 대한 레이블
- *stcuser*: TCPIP 주소 공간과 연관된 RACF 사용자 ID
- *datasetname*: 내보낸 인증서를 수신할 데이터 세트
- *password*: 데이터 암호화를 위한 암호. 인증서가 STA에서 수신될 때 필요합니다. 암호는 8자 이상이어야 합니다.

내보내기 데이터 세트는 이제 STA로 전송되고, FTP를 사용할 수 있습니다. CA 인증서는 EBCDIC에서 ASCII로 변환되어 전송됩니다. CLIENT 인증서는 BINARY 파일로 전송되며 이 파일에는 클라이언트 인증서 및 해당 개인 키가 모두 포함되어 있습니다.

E.2.4. 작업 4: CGI 루틴에서 사용되는 RACF 프로파일 만들기

프로파일은 FACILITY 클래스에서 정의됩니다. 첫번째 프로파일의 이름은 *SMC.ACCESS.STA*이며 사용자가 STA 응용 프로그램에 대한 액세스 권한을 가지는지 여부를 결정합니다.

STA에 액세스해야 하는 사용자에게는 이 프로파일에 대한 READ 액세스 권한이 있어야 합니다. 기타 프로파일은 모두 *SMC.ROLE.nnn*으로 표시되며 로그인되었을 때 사용자가 가지는 역할을 결정합니다.

주:

STA에 대해 정의된 유일한 역할은 *StorageTapeAnalyticsUser*입니다. 이 역할을 얻으려면 사용자 ID가 READ 액세스 권한과 함께 *SMC.ROLE.STORAGETAPEANALYTICSUSER* 프로파일에 추가되도록 요청해야 합니다.

E.2.5. 작업 5: 인증서 파일 및 개인 키 파일 가져오기(선택 사항)

이 절차는 공개 및 개인 키가 성공적으로 생성되고 적절한 권한을 가진 사용자 ID 및 암호가 올바르게 정의되었는지 테스트하는 데 중요할 수 있습니다.

테스트는 모든 브라우저를 사용하여 수행할 수 있지만, 여기에서는 Firefox가 예로 사용되었습니다.

1. Firefox **Tools** 메뉴에서 **Options**를 선택합니다.
2. **Advanced** 탭을 선택한 다음 **Encryption** 탭을 선택합니다.
3. **View Certificates**를 누릅니다.
4. **Certificate Manager** 대화 상자에서 **Authorities** 탭을 선택한 다음, 가져올 인증서 파일을 선택합니다.
5. **Import**를 누릅니다.

6. **Your Certificates** 탭을 선택한 다음, 가져올 개인 키 파일을 입력합니다.
7. **Import**를 누릅니다.
8. **OK**를 눌러 저장하고 대화 상자를 종료합니다.

E.2.6. 작업 6: CGI 루틴 테스트

브라우저에서 CGI 루틴을 테스트하려면 다음 URL을 입력합니다. 여기서 *host*, *port*, *userid* 및 *password*를 적절한 값으로 설정합니다.

```
https://host:port/smcgsaf?
type=authentication&userid=userid&password=password&roles=StorageTapeAnalyticsUser
```

결과 출력에서는 사용자에게 STA에 대한 액세스 권한이 부여되었는지 여부 및 *StorageTapeAnalyticsUser* 역할을 보여 줍니다.

주:

STA RACF 권한 부여 기능은 메인프레임 사용자 ID의 암호 변경을 지원하지 않습니다. 사용자 ID 암호가 만료될 경우 STA에 이 사실이 표시되며, STA에 다시 로그인을 시도하기 전에 일반 메인프레임 채널을 통해 암호를 재설정해야 합니다.

E.2.7. 작업 7: WebLogic 콘솔에 대한 RACF/SSP 설정

RACF Security Service Provider(또는 RACF SSP)는 WebLogic에 플러그인으로 설치되어 있어야 합니다.

RACF SSP가 설치된 경우 STA 설치 프로그램이 WebLogic 내의 적당한 위치에 RACF SSP를 두어야 합니다. 설치되지 않은 경우 RACF 보안 *jar* 파일을 다음 디렉토리에 두십시오.

```
/Oracle_storage_home/Middleware/wlserver_10.3/server/lib/mbeantypes/staRACF.jar
```

여기서 *Oracle_storage_home*은 STA 설치 중 지정된 Oracle 스토리지 홈 위치입니다.

E.2.8. 작업 8: STA와 RACF 간 SSL 구성

1. MVS 시스템에 필요한 PTF를 설치합니다. 이러한 PTF는 STA에 로그인할 때 RACF 또는 기타 타사 보안 소프트웨어를 사용한 인증을 허용합니다. PTF 요구 사항은 STA 요구 사항 설명서를 참조하십시오.

SMC HTTP Server 및 WebLogic에 대해 정의된 포트 번호가 서버에 대해 암호화되도록 AT-TLS(Application Transparent TLS)가 MVS에서 구성되었습니다.

진행하기 전에 MVS 서버 인증서(ASCII 형식) 및 STA 클라이언트 개인 키(바이너리 PKCS12 형식)의 두 파일을 가지고 있는지 확인하십시오. MVS 시스템 관리자가 PKCS12 파일에 대한 암호를 제공했을 것입니다.

- 인증서를 `/Oracle_storage_home/Middleware/user_projects/domains/tbi/cert`에 저장합니다.

여기서 `Oracle_storage_home`은 STA 설치 중 지정된 Oracle 스토리지 홈 위치입니다.

- 인증서를 DER 형식에서 PEM 형식으로 변환합니다.

```
openssl pkcs12 -clcerts -in PKCS12DR.xxxxxx -out mycert.pem
```

가져오기 암호(인증서와 함께 제공), 새로운 PEM 암호 및 확인용 암호를 입력합니다.

- Java keytool 명령을 사용하여 인증서 파일을 `/Oracle_storage_home/Middleware/jdk1.6.0_xx/jre/lib/security/cacerts` 파일로 가져옵니다.

```
# /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. 작업 9: WebLogic Server 구성

RACF 인증을 위해 WebLogic을 구성하려면 [D.1.2절. “다른 보안 인증서를 사용하도록 WebLogic 재구성”](#)의 절차를 따르십시오.

E.2.10. 작업 10: WebLogic 콘솔에 RACF/SSP 설치

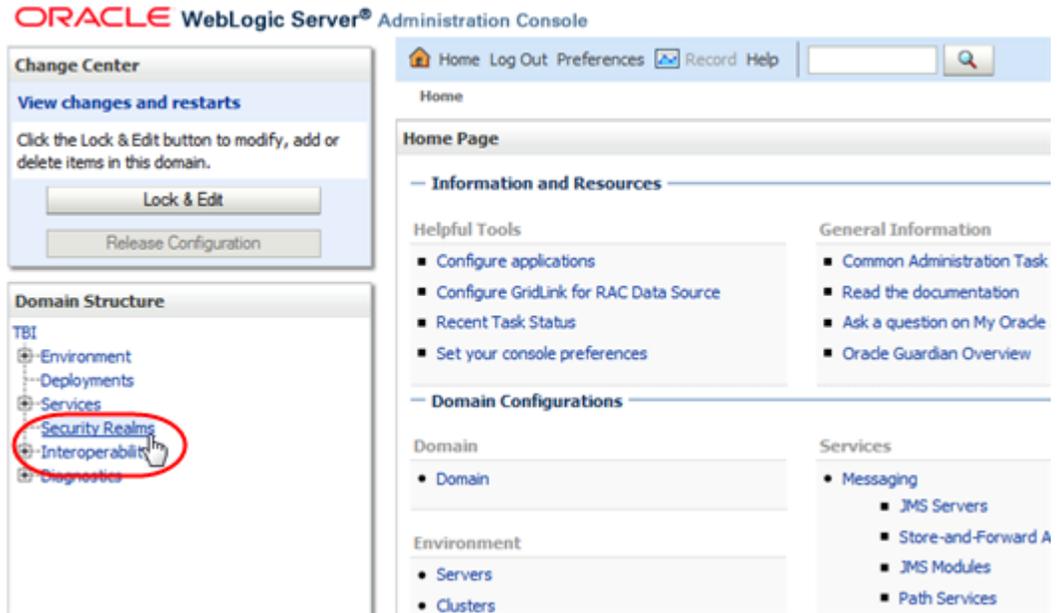
- STA 설치 중 선택한 HTTP(STA 2.1.0 기본값은 7019) 또는 HTTPS(STA 2.1.0 기본값은 7020) 포트 번호를 사용하여 WebLogic 콘솔 로그인 화면으로 이동합니다.

```
https://yourHostName:PortNumber/console/
```

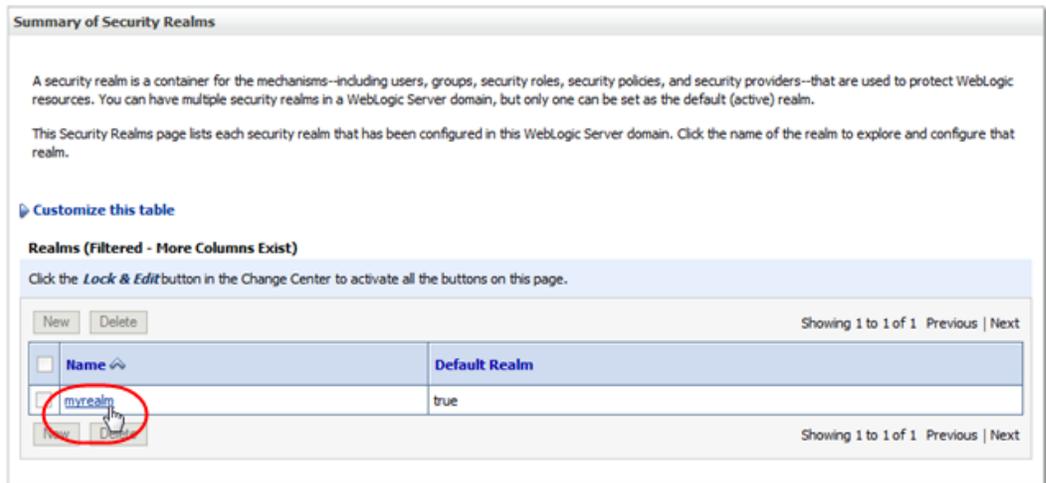
예를 들면 다음과 같습니다.

```
https://sta_server:7020/console/
```

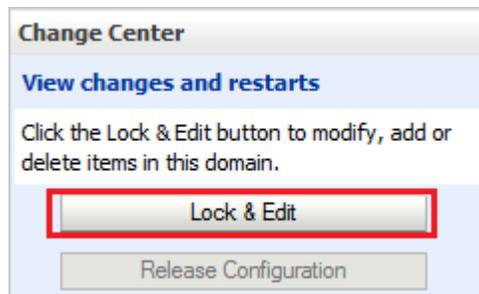
- STA 설치 중 정의한 WebLogic 관리 콘솔 사용자 이름과 암호를 사용하여 로그인합니다.
- Domain Structure 섹션에서 **Security Realms**를 선택합니다.



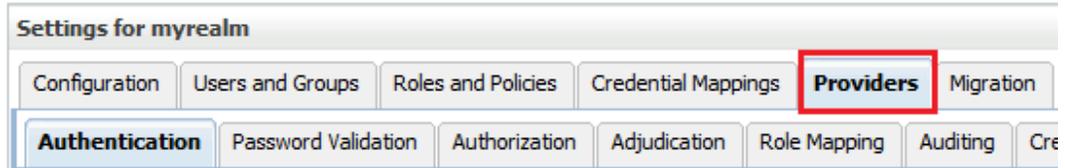
4. Realms 섹션에서 **myrealm** 활성 링크를 선택합니다(확인란이 아닌 이름 자체를 선택).



5. Change Center 섹션에서 **Lock & Edit**를 누릅니다.



6. **Providers** 탭을 선택합니다.



7. Authentication Providers 섹션에서 **New**를 누릅니다.



8. 추가하려는 인증 공급자의 이름(예: *STA RacfAuthenticator*)을 입력한 다음 **Type** 메뉴에서 *RacfAuthenticator*를 선택합니다. **OK**를 누릅니다.

주:

RACF jar 파일이 **Type** 메뉴에 나열되어야 합니다. 그렇지 않은 경우 *STA* 명령을 사용하여 *STA*를 중지하고 다시 시작합니다. 명령 사용법 세부 정보는 *STA* 관리 설명서를 참조하십시오.

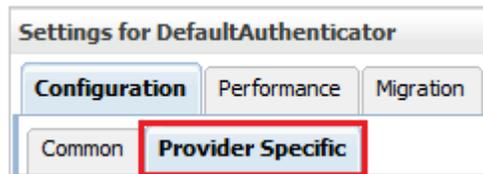
9. RACF 공급자가 Authentication Providers 테이블에 포함되었는지 확인합니다. *DefaultAuthenticator* 및 *DefaultIdentityAsserter*는 이 목록에서 항상 처음 두 항목이어야 합니다.

10. **DefaultAuthenticator** 활성 링크를 선택합니다(확인란이 아닌 이름 자체를 선택).

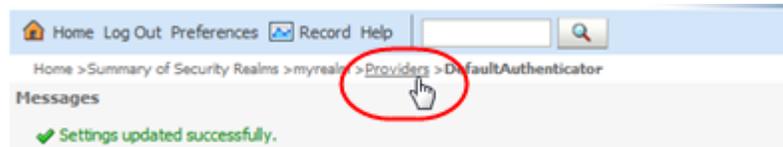


11. **Control Flag** 메뉴에서 Sufficient를 선택한 다음 **Save**를 누릅니다.

12. **Provider Specific** 탭을 누른 다음 **Save**를 누릅니다.



13. **Providers** 로케이터 링크를 눌러 Authentication Providers 화면으로 돌아갑니다.



14. Authentication Providers 테이블에서 8 단계에서 만든 RACF 인증자 이름을 선택합니다(확인란이 아닌 이름 자체를 선택).

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider
<input type="checkbox"/>	RacAuthenticator	WebLogic TBI Racf Authentication Provider

15. Control Flag 메뉴에서 *Sufficient*를 선택한 다음 **Save**를 누릅니다.

Settings for RacAuthenticator

Configuration

Common Provider Specific

Save

This page allows you to define the general configuration of this provider.

Name: RacAuthenticator

Description: WebLogic TBI Racf Authentication Provider

Version: 1.0

Control flag: OPTIONAL

Save

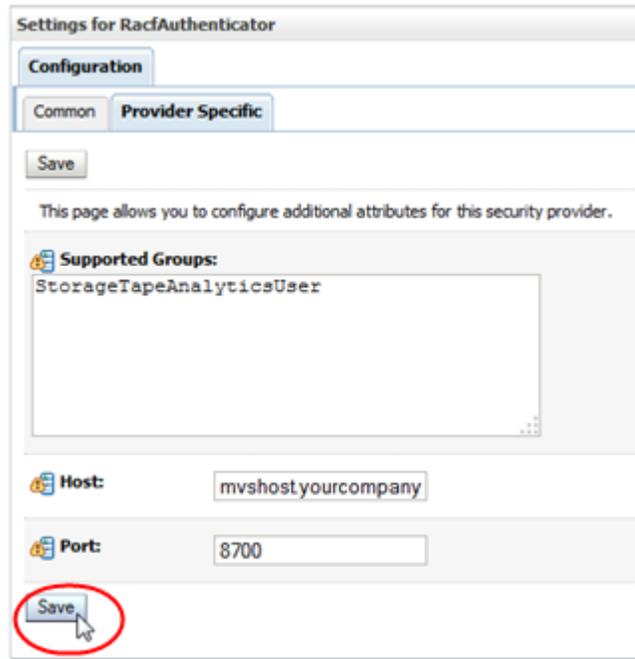
16. Provider Specific 탭을 누릅니다.

Settings for RacAuthenticator

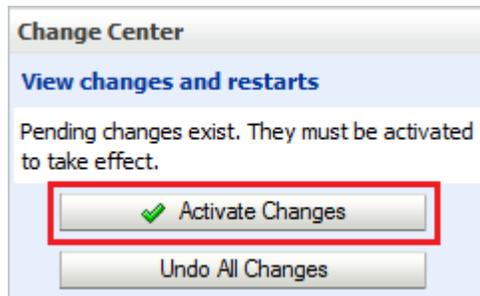
Configuration

Common Provider Specific

17. MVS 시스템이 실행 중인 호스트 이름(예: *mvshost.yourcompany.com*) 및 포트 번호(예: *8700*)를 입력한 다음 **Save**를 누릅니다.



18. Change Center 섹션에서 **Activate Changes**를 누릅니다.



19. WebLogic 관리 콘솔에서 로그아웃합니다.

20. STA 명령을 사용하여 STA를 중지하고 다시 시작합니다. 명령 사용법 세부 정보는 STA 관리 설명서를 참조하십시오.

```
# STA stop all  
# STA start all
```

SNMP v2c 모드 구성

STA가 SNMP v2c 모드로 구성된 라이브러리를 하나라도 모니터링하는 경우 SNMP v2c 모드를 구성해야 합니다.

STA는 항상 권장되는 SNMP v3 프로토콜을 사용하여 라이브러리와 통신을 시도합니다. SNMP v3 통신이 가능하지 않은 경우(예: 라이브러리에 SNMP v3이 구성되지 않음) STA는 SNMP v2c가 이 부록의 지침대로 사용으로 설정되어 있다면 이 프로토콜을 사용합니다.

SNMP v3 구성 프로세스는 [5장. 라이브러리에서 SNMP 구성](#) 및 [6장. STA의 라이브러리 연결 구성](#)에 설명되어 있습니다. 이 부록에서는 SNMP v2c 구성의 경우 달라지는 절차에 대해 설명합니다.

이 부록은 다음 절로 구성됩니다.

- [SNMP v2c 구성 작업](#)

F.1. SNMP v2c 구성 작업

- [F.1.1절. “SNMP v2c 모드 구성”](#)
- [F.1.2절. “라이브러리에서 STA SNMP v2c 트랩 수신자 만들기”](#)
- [F.1.3절. “STA에 대해 SNMP v2c 모드 사용으로 설정”](#)

F.1.1. SNMP v2c 모드 구성

이 절차를 사용하여 SNMP 통신에 SNMP v2c를 사용하도록 STA 및 라이브러리를 구성하십시오.

1. [5장. 라이브러리에서 SNMP 구성](#)에서 다음을 제외하고 [표 5.1. “STA에 대한 라이브러리 구성 작업”](#)에 나온 모든 절차를 따릅니다.
 - “[STA SNMP v3 트랩 수신자 만들기](#)” [79]를 [F.1.2절. “라이브러리에서 STA SNMP v2c 트랩 수신자 만들기”](#)로 바꿉니다.
 - [표 5.1. “STA에 대한 라이브러리 구성 작업”](#)의 프로세스를 완료한 후 [F.1.3절. “STA에 대해 SNMP v2c 모드 사용으로 설정”](#)을 수행합니다.
2. STA에서 SNMP v2c를 구성합니다. 자세한 내용은 [6장. STA의 라이브러리 연결 구성](#) [83]을 참조하십시오.

F.1.2. 라이브러리에서 STA SNMP v2c 트랩 수신자 만들기

이 절차를 사용하여 STA 서버를 SNMP v2c 트랩의 권한이 부여된 수신자로 정의하고 라이브러리에서 보내는 트랩을 정의하십시오. 라이브러리 모델에 따라 라이브러리 CLI, SL

Console 또는 SL150 브라우저 인터페이스를 사용할 수 있습니다. 다음 사항에 유의하십시오.

- 트랩 레벨은 콤마로 구분하십시오.
- 중복 레코드를 피하기 위해 STA 서버를 여러 인스턴스에서 트랩 수신자로 정의하지 마십시오. 예를 들어, STA 서버에 대해 SNMP v3 및 SNMP v2c 트랩 수신자 정의를 둘 다 만들지는 마십시오.
- 트랩 레벨 4는 이전 라이브러리 펌웨어 버전에서 지원되지 않을 수 있지만, 트랩 수신자를 만들 때는 항상 지정할 수 있습니다.
- CLI에서 입력 오류를 피하기 위해 먼저 텍스트 파일에 명령을 입력한 다음 복사하고 CLI에 붙여 넣을 수 있습니다. CLI 명령에 대한 도움말을 보려면 `help snmp`를 입력하십시오.

라이브러리 CLI 사용(SL150을 제외한 모든 라이브러리)

1. SNMP v2c 트랩 수신자를 만듭니다.

```
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
```

여기서 각 항목은 다음과 같습니다.

- `STA_server_IP`: STA 서버의 IP 주소입니다.
- `community_name`: SNMP v2c 트랩 커뮤니티입니다. `public` 또는 다른 이름이 될 수 있습니다.

예를 들면 다음과 같습니다.

```
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. 트랩 수신자를 나열하여 STA 서버가 올바르게 추가되었는지 확인합니다.

```
snmp listTrapRecipients
```

SL Console 사용(SL500 라이브러리만 해당)

1. **Tools** 메뉴에서 **System Detail**을 선택합니다.
2. 탐색 트리에서 **Library**를 선택합니다.
3. **SNMP** 탭을 선택한 다음 **Add Trap Recipients** 탭을 선택합니다.
4. 다음 정보를 입력합니다.
 - `Host`: STA 서버의 IP 주소입니다.
 - `TrapLevel`: 라이브러리에서 STA로 보내야 하는 콤마로 구분된 트랩 레벨 목록입니다(1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100).
 - `Version`: `v2c`를 선택합니다.

- *Community – public* 또는 다른 이름이 될 수 있습니다.
5. **Apply**를 눌러 트랩 수신자를 추가합니다.

SL150 사용자 인터페이스 사용

1. 탐색 트리에서 **SNMP**를 선택합니다.
2. SNMP Trap Recipients 섹션(또는 탭)에서 **Add Trap Recipient**를 선택합니다.
3. Add Trap Recipient 필드를 다음과 같이 입력합니다.
 - *Host Address*: STA 서버의 IP 주소입니다.
 - *Trap Level*: 라이브러리에서 STA로 보내야 하는 콤마로 구분된 트랩 레벨 목록입니다(1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100).
 - *Version*: v2c를 선택합니다.
 - *Community Name*: *public* 또는 다른 이름이 될 수 있습니다.
4. **OK**를 눌러 트랩 수신자를 추가합니다.

F.1.3. STA에 대해 SNMP v2c 모드 사용으로 설정

1. STA 서버와의 터미널 세션을 설정하고 시스템 루트 사용자로 로그인합니다.
2. STA 구성 파일 디렉토리로 변경합니다.

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

3. SNMP 버전 등록 정보 파일을 편집합니다.

```
# vi TbiSnpVersionSupport.properties
```

4. SNMP v2c 매개변수의 값이 *true*로 설정되었는지 확인합니다.

```
V2c=true
```

5. 파일을 저장하고 종료합니다.
6. 4 단계에서 SNMP v2c 매개변수의 값을 변경한 경우 모든 STA 프로세스를 중지하고 다시 시작합니다.

```
# STA stop all
# STA start all
```


색인

기호

LDAP 구성, 211

Linux 설치

개요,

사후 설치 작업, 31

작업, 28

준비 작업, 25

Linux PATH 설정, 94

RACF 구성, 215

SNMP

관리

클라이언트 속성 변경, 86

트랩 수신자 추가, 128

연결 확인, 84

SNMP 클라이언트 속성 변경, 86

SSP

RACF 구성, 215

WebLogic Open LDAP 구성, 211

구성,

STA

다운로드, 50

STA 구성

SNMP,

STA 데이터베이스 백업 서비스, 93

서비스,

Linux PATH 설정 업데이트, 94

라이브러리 연결 확인, 95

리소스 모니터, 93

서비스 데몬 다시 시작, 94

인증서,

Oracle 인증서 바꾸기, 209

WebLogic 재구성, 202

초기 연결 설정, 201

작업, 83

STA 서버

포트 구성, 43

STA 설치

개요,

그래픽 설치 프로그램, 51

설치 단계, 51

일반 필수 조건, 47

콘솔 설치 프로그램, 51

STA 업그레이드,

v2c 모드

개요,

구성 프로세스, 229

사용으로 설정, 231

트랩 수신자 만들기, 229

ㄹ

라이브러리 구성,

SL500 빠른 로드, 61

SNMP 구성, 71

SNMP 워크시트, 200

볼륨 레이블 형식 지정, 61

사용자 인터페이스, 62

선택적 구성 스크립트, 62

이중 TCP/IP, 58

작업, 63

중복 전자 부품, 58

컴플렉스 ID, 60

ㅂ

방화벽 포트 구성, 43

볼륨 레이블 형식 지정, 61

볼륨 일련 번호, 중복, 61

ㅅ

사용자 계정

MySQL 요구 사항, 41

WebLogic 요구 사항, 41

서비스 요청, 23

ㅈ

재설치, , 133

제거, , 131

ㅋ

컴플렉스 ID, 60

클라이언트 속성, 86

ㅌ

트랩 수신자

추가, 128

