

StorageTek Tape Analytics

Guide d'installation et de configuration

Version 2.1.0

E60938-02

Février 2015

StorageTek Tape Analytics

Guide d'installation et de configuration

E60938-02

Copyright © 2013, 2015, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

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.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer un risque de dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour des applications dangereuses.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Table des matières

Préface	19
Public visé	19
Accessibilité de la documentation	19
Documents connexes	19
Pour les utilisateurs de l'application STA	19
Pour les installateurs et les administrateurs du serveur et de l'application STA	20
Conventions	20
Nouveautés	21
STA 2.1.0 - Janvier 2015	21
1. Planification des tâches de pré-installation	25
1.1. Aperçu du déploiement de STA	25
1.2. Préparez les demande d'assistance pour préparer les bibliothèques	26
2. Installation de Linux	27
2.1. Tâches de préparation	28
2.1.1. Consultation de la documentation connexe	28
2.1.2. Examen de la disposition du système de fichiers STA	28
2.1.3. Téléchargement du pack de supports du programme d'installation de Linux	30
2.2. Tâches d'installation	31
2.2.1. Rassemblement des informations requises	31
2.2.2. Installation de Linux	31
2.2.3. Exécution de l'agent de configuration Linux Setup Agent	33
2.3. Tâches de post-Installation	34
2.3.1. Désactivation de SELinux	34
2.3.2. Désactivation du pare-feu Linux	34
2.3.3. Désactivation du contrôle d'accès	35
2.3.4. Configuration du proxy réseau	36
2.3.5. Vérification de la configuration correcte de Yum (facultatif)	36
2.3.6. Installation des packages Linux requis	38
2.3.7. Vérification de la configuration correcte de SSH	39

2.3.8. Vérification des paramètres DNS appropriés	39
2.3.9. Désactivation des services de noms	39
2.3.10. Vérification du fonctionnement du navigateur local (facultatif)	40
3. Installation de STA	41
3.1. Utilisateurs, groupes et emplacements utilisés par le programme d'installation de STA	41
3.2. Conditions requises de nom d'utilisateur et de mot de passe	43
3.3. Comptes et ports configurés pendant l'installation de STA	44
3.3.1. Comptes utilisateurs pour la gestion de STA	44
3.3.1.1. Comptes WebLogic	44
3.3.1.2. Comptes de base de données STA	44
3.3.2. Ports utilisés par STA	45
3.3.2.1. Ports externes non configurables	45
3.3.2.2. Ports externes configurables	46
3.3.2.3. Ports internes configurables	46
3.4. Journaux d'installation et de désinstallation de STA	46
3.4.1. Emplacements des fichiers journaux	47
3.5. Modes du programme d'installation de STA	48
3.6. Tâches d'installation de STA	48
3.6.1. Identification ou création des informations requises pour l'installation	49
3.6.2. Vérification des prérequis d'installation	51
3.6.3. Téléchargement de STA	53
3.6.4. Installation de STA	54
3.6.5. Vérification de la réussite de l'installation.	56
3.6.6. Déplacement du répertoire des journaux STA (facultatif)	57
3.6.7. Inscrivez l'emplacement de l'inventaire central Oracle	59
4. Configuration des fonctionnalités de bibliothèques pour STA	61
4.1. Fonctionnalités de bibliothèque impactant les données STA	61
4.1.1. Interface ADI pour lecteurs LTO	61
4.1.1.1. Activation de l'interface ADI sur les lecteurs LTO	62
4.1.1.2. Activation de l'interface ADI sur la bibliothèque	62
4.1.2. TCP/IP double et Redundant Electronics (SL3000 et SL8500 uniquement)	62
4.1.2.1. Configuration de la connexion STA pour permettre la prise en charge de ces fonctionnalités	63
4.1.2.2. Éléments supplémentaires à prendre en compte concernant ces fonctionnalités	64

4.1.3. ID de complexe de bibliothèque (SL8500 uniquement)	64
4.1.4. Avertissement de nettoyage de lecteur (SL3000 et SL8500 uniquement)	65
4.1.5. Format de l'étiquette de volume (SL500 et SL150 uniquement)	65
4.1.6. Option SCSI FastLoad (SL500 uniquement)	66
4.1.7. Numéros de série de volumes en double	66
4.2. Interfaces utilisateur de la bibliothèque	66
4.2.1. Conseils d'utilisation de la CLI de la bibliothèque	66
4.2.2. Script de configuration de la bibliothèque (facultatif)	67
4.3. Tâches de configuration de fonctionnalité de bibliothèque	68
4.3.1. Connexion à la bibliothèque	68
4.3.2. Vérification de la version du microprogramme de la bibliothèque	69
4.3.3. Vérification de la version de la carte de contrôleur des lecteurs (bibliothèques SL3000 et SL8500 uniquement)	70
4.3.4. Activation de l'interface ADI sur la bibliothèque (toutes les bibliothèques sauf SL150)	71
4.3.5. Vérification de l'ID de complexe de bibliothèque (SL8500 uniquement)	71
4.3.6. Définition de l'avertissement de nettoyage de lecteur (facultatif, SL3000 et SL8500 uniquement)	72
4.3.7. Définition du format de l'étiquette de volume de la bibliothèque SL500 (SL500 uniquement)	73
4.3.8. Définition du format de l'étiquette de volume de la bibliothèque SL150 et du mode d'adressage de l'élément de lecteur (SL150 uniquement)	74
5. Configuration de SNMP sur les bibliothèques	77
5.1. Comprendre la configuration SNMP de bibliothèque pour STA	77
5.1.1. Configuration du protocole SNMP v3 sur les bibliothèques	78
5.1.1.1. Utilisateur SNMP v3 unique	78
5.1.1.2. SNMP Engine IDs	79
5.2. Tâches de configuration SNMP sur les bibliothèques	79
5.2.1. Récupération de l'adresse IP de la bibliothèque	80
5.2.2. Activation du protocole SNMP sur la bibliothèque	81
5.2.3. Définition d'un utilisateur SNMP v2c	82
5.2.4. Création d'un utilisateur SNMP v3	84
5.2.5. Récupération de l'ID de moteur SNMP de la bibliothèque (toutes les bibliothèques sauf SL150)	86
5.2.6. Créez le destinataire de déROUTement STA SNMP v3.	86
6. Configuration des connexions de bibliothèque dans STA	89

6.1. Tâches de configuration de STA	89
6.1.1. Connexion à STA	89
6.1.2. Vérifiez la communication SNMP avec une bibliothèque	90
6.1.3. Configuration des paramètres client SNMP pour STA	92
6.1.4. Configuration de la connexion SNMP à une bibliothèque.	94
6.1.5. Test d'une connexion SNMP de bibliothèque	96
6.1.6. Exécution d'une collecte de données manuelle	98
7. Configuration des services STA	101
7.1. Présentation des services STA	101
7.2. Tâches de configuration des services STA	101
7.2.1. Mise à jour du chemin de système (facultatif)	102
7.2.2. Redémarrage du démon de services STA (facultatif)	102
7.2.3. Vérification de la connectivité de la bibliothèque	103
7.2.4. Passez en revue les préférences de l'utilitaire de sauvegarde de la base de données STA.	103
7.2.5. Configuration du serveur de sauvegarde de base de données distant	104
7.2.6. Configuration du service de sauvegarde de la base de données STA	105
7.2.7. Examen des préférences de l'utilitaire du contrôleur de ressources STA	107
7.2.8. Configuration du contrôleur de ressources STA	109
8. Mise à niveau vers STA 2.1.0	111
8.1. Présentation du processus de mise à niveau	111
8.2. Chemins de mise à niveau STA 2.1.0 valides	112
8.3. Méthodes de mise à niveau	112
8.3.1. Méthode de mise à niveau à serveur unique	112
8.3.2. Méthode de mise à niveau à deux serveurs	113
8.4. Modifications d'environnement pour STA 2.1.0	114
8.4.1. Version de Linux	114
8.4.2. Numéros de port WebLogic par défaut	115
8.4.3. Ports requis pour STA 2.0.x et ultérieure	115
8.4.4. Conditions requises de nom d'utilisateur et de mot de passe	116
8.5. Tâches de préparation de la mise à niveau	116
8.5.1. Vérifiez que votre site est prêt pour la mise à niveau	116
8.5.1.1. Vérification des prérequis de la mise à niveau	117
8.5.1.2. Vérification de l'activité actuelle de STA	117
8.5.2. Enregistrement des journaux existants (facultatif)	118
8.5.3. Enregistrement de l'utilisateur STA et des paramètres de configuration actuels (facultatif)	119

8.5.3.1. Enregistrement des noms d'utilisateur MySQL	119
8.5.3.2. Enregistrement des paramètres client SNMP STA	119
8.5.3.3. Enregistrement des noms d'utilisateur WebLogic — Mises à niveau de STA 1.0.x uniquement	120
8.5.3.4. Enregistrement des noms d'utilisateur STA — Mises à niveau de STA 2.0.x uniquement	122
8.5.3.5. Enregistrement des paramètres du serveur de messagerie STA	123
8.5.4. Renommage des modèles personnalisés avec préfixe STA– (facultatif)	123
8.5.5. Enregistrement des paramètres actuels de modèle personnalisé (facultatif)	124
8.5.6. Enregistrement des paramètres de stratégie de rapport exécutif (facultatif)	125
8.6. Tâches de mise à niveau	125
8.6.1. Tâche 1: Vidage de l'ancienne base de données STA	126
8.6.2. Tâche 2 : Transfert du vidage de l'ancienne base de données	127
8.6.3. Tâche 3a : Installation de la nouvelle version de Linux (pour les mises à niveau depuis STA 1.0.x)	129
8.6.4. Tâche 3b : Désinstallation de l'ancienne version de STA (pour les mises à niveau depuis STA 2.0.x)	129
8.6.5. Tâche 4: Installation de la nouvelle version de STA	129
8.6.6. Tâche 5 : Vidage de la nouvelle base de données STA (facultatif)	130
8.6.7. Tâche 6 : Transfert de l'ancienne base de données STA sur le serveur STA	131
8.6.8. Tâche 7 : Traitement et chargement de l'ancienne base de données STA	132
8.6.9. Tâche 8 : Mise à niveau de l'ancienne base de données	134
8.6.10. Tâche 9 : Configuration de la nouvelle version de STA	137
8.6.10.1. Mise à jour du destinataire de déROUTement STA sur les bibliothèques	137
8.6.10.2. Configurez les paramètres SNMP dans STA	138
8.6.10.3. Configuration des informations utilisateur et services STA	139
8.6.10.4. Mise hors service de l'ancien serveur STA (facultatif)	139
8.6.11. Récupération d'une mise à niveau de base de données ayant échoué (facultatif)	140
9. Désinstallation et restauration de STA	141
9.1. Présentation de la désinstallation de STA	141
9.2. Tâches de désinstallation de STA	142
9.2.1. Désinstallation de STA	142

9.2.2. Vérification de la réussite de la désinstallation.	143
9.2.3. Restauration de STA	143

A. Référence d'écran Programme d'installation et de désinstallation graphique de STA	145
A.1. Configuration minimale requise pour l'affichage en mode graphique	145
A.1.1. Connexions locales	146
A.1.2. Connexions à distance avec un Secure Shell (SSH)	146
A.1.2.1. Connexion depuis une machine Linux	146
A.1.2.2. Connexion depuis un ordinateur Microsoft Windows	146
A.1.3. Connexions distantes à l'aide du partage de bureau	147
A.1.4. Dépannage des problèmes d'affichage graphique	147
A.2. Ecrans de programme d'installation graphique de STA	148
A.2.1. Configuration d'inventaire et d'installation	149
A.2.1.1. Champs de l'écran	150
A.2.1.2. Boutons spécifiques à l'écran	150
A.2.2. Accueil	151
A.2.2.1. Présentation générale de l'écran du programme d'installation	151
A.2.3. Emplacement de l'installation	153
A.2.3.1. Champs de l'écran	153
A.2.3.2. Boutons spécifiques à l'écran	154
A.2.4. Vérifications des prérequis	156
A.2.4.1. Champs de l'écran	158
A.2.4.2. Boutons spécifiques à l'écran	158
A.2.5. Entrez le mot de passe root	160
A.2.5.1. Champs de l'écran	160
A.2.5.2. Boutons spécifiques à l'écran	160
A.2.6. Configuration des répertoires de base de données	161
A.2.6.1. Champs de l'écran	161
A.2.6.2. Boutons spécifiques à l'écran	162
A.2.7. Configuration des comptes administrateurs	162
A.2.7.1. Champs de l'écran	162
A.2.7.2. Boutons spécifiques à l'écran	163
A.2.8. Administrateur WebLogic	163
A.2.8.1. Champs de l'écran	164
A.2.8.2. Boutons spécifiques à l'écran	164
A.2.9. Administrateur STA	165
A.2.9.1. Champs de l'écran	165
A.2.9.2. Boutons spécifiques à l'écran	166
A.2.10. Configuration des comptes de base de données	167

A.2.10.1. Champs de l'écran	167
A.2.10.2. Boutons spécifiques à l'écran	167
A.2.11. Utilisateur root de base de données	168
A.2.11.1. Champs de l'écran	169
A.2.11.2. Boutons spécifiques à l'écran	169
A.2.12. Utilisateur de l'application de base de données	170
A.2.12.1. Champs de l'écran	170
A.2.12.2. Boutons spécifiques à l'écran	171
A.2.13. Utilisateur des rapports de base de données	172
A.2.13.1. Champs de l'écran	172
A.2.13.2. Boutons spécifiques à l'écran	173
A.2.14. Administrateur de bases de données	174
A.2.14.1. Champs de l'écran	175
A.2.14.2. Boutons spécifiques à l'écran	175
A.2.15. Saisir les ports de communication	176
A.2.15.1. Champs de l'écran	176
A.2.15.2. Boutons spécifiques à l'écran	177
A.2.16. Console d'administration WebLogic	177
A.2.16.1. Champs de l'écran	178
A.2.16.2. Boutons spécifiques à l'écran	178
A.2.17. Moteur STA	178
A.2.17.1. Champs de l'écran	179
A.2.17.2. Boutons spécifiques à l'écran	179
A.2.18. Adaptateur STA	180
A.2.18.1. Champs de l'écran	180
A.2.18.2. Boutons spécifiques à l'écran	181
A.2.19. Interface utilisateur STA	181
A.2.19.1. Champs de l'écran	182
A.2.19.2. Boutons spécifiques à l'écran	182
A.2.20. Agent de diagnostic	182
A.2.20.1. Champs de l'écran	183
A.2.20.2. Boutons spécifiques à l'écran	183
A.2.21. Récapitulatif de l'installation	183
A.2.21.1. Champs de l'écran	184
A.2.21.2. Boutons spécifiques à l'écran	184
A.2.22. Progression de l'installation	185
A.2.22.1. Champs de l'écran	185
A.2.22.2. Boutons spécifiques à l'écran	186
A.2.23. Progression de la configuration	187
A.2.23.1. Champs de l'écran	188

A.2.23.2. Boutons spécifiques à l'écran	188
A.2.24. Installation terminée	189
A.2.24.1. Champs de l'écran	189
A.2.24.2. Boutons spécifiques à l'écran	189
A.3. Ecrans de programme de désinstallation graphique de STA	190
A.3.1. Accueil	190
A.3.1.1. Champs de l'écran	190
A.3.1.2. Boutons spécifiques à l'écran	191
A.3.2. Entrez le mot de passe root	191
A.3.2.1. Champs de l'écran	191
A.3.2.2. Boutons spécifiques à l'écran	191
A.3.3. Récapitulatif de la désinstallation	192
A.3.3.1. Champs de l'écran	192
A.3.3.2. Boutons spécifiques à l'écran	193
A.3.4. Progression de la désinstallation	193
A.3.4.1. Champs de l'écran	194
A.3.4.2. Boutons spécifiques à l'écran	194
A.3.5. Désinstallation terminée	196
A.3.5.1. Champs de l'écran	196
A.3.5.2. Boutons spécifiques à l'écran	196

B. Programme d'installation et de désinstallation de STA en mode silencieux

B.1. Utilisation du programme d'installation et de désinstallation de STA en mode silencieux	197
B.1.1. Configuration requise du mode silencieux	197
B.2. Fichiers et utilitaires utilisés en mode silencieux	198
B.3. Tâches du programme d'installation de STA en mode silencieux	201
B.3.1. Création du fichier de pointeurs d'inventaire central Oracle	201
B.3.2. Création du fichier réponse du programme d'installation en mode silencieux	202
B.3.3. Exécutez le programme d'installation en mode silencieux	204
B.4. Tâches du programme de désinstallation de STA en mode silencieux	206
B.4.1. Création d'un fichier réponse du programme de désinstallation en mode silencieux	206
B.4.2. Exécutez le programme de désinstallation en mode silencieux	208
B.5. Options de commande du programme d'installation de STA	209
B.5.1. Options du mode silencieux	210
B.5.2. Options de journalisation	210
B.5.3. Autre options	211

C. Fiches de travail d'installation et de mise à niveau	213
C.1. Fiche de travail de préparation de mise à niveau	213
C.2. Fiches de travail d'installation et de mise à niveau	214
C.2.1. Fiche de travail des emplacements et utilisateurs de l'installation	214
C.2.2. Fiche de travail des comptes utilisateurs	215
C.2.3. Fiches de travail des numéros de port	216
C.2.4. Fiche de travail du nom de domaine	217
C.3. Fiche de travail de la configuration post-installation	217
D. Configuration des certificats de sécurité	219
D.1. Tâches de configuration du certificat de sécurité	219
D.1.1. Etablissement de la connexion HTTPS/SSL initiale	219
D.1.2. Reconfiguration de WebLogic pour qu'il utilise un certificat de sécurité différent	220
D.1.3. Remplacement du certificat Oracle	227
E. Configuration d'un fournisseur de service de sécurité pour STA	229
E.1. Contrôle d'accès STA via WebLogic OpenLDAP	229
E.1.1. Configuration de WebLogic OpenLDAP	229
E.2. Tâches de contrôle d'accès STA via IBM RACF	233
E.2.1. Tâche 1 : Vérification des conditions minimales requises pour le mainframe IBM RACF	234
E.2.2. Tâche 2 : Activation de la prise en charge du mainframe pour l'autorisation STA RACF	234
E.2.3. Tâche 3 : Configuration AT-TLS	235
E.2.4. Tâche 4 : Création des profils RACF utilisés par la routine CGI	241
E.2.5. Tâche 5 : Importation du fichier de certificat et du fichier de clé privée (facultatif)	241
E.2.6. Tâche 6: Test de la routine CGI	241
E.2.7. Tâche 7 : Configuration de RACF/SSP pour la console WebLogic	242
E.2.8. Tâche 8: Configuration de SSL entre STA et RACF	242
E.2.9. Tâche 9 : Configuration du serveur WebLogic	243
E.2.10. Tâche 10: Installation de RACF/SSP sur la console WebLogic	243
F. Configuration du mode SNMP v2c	249
F.1. Tâches de configuration de SNMP v2c	249
F.1.1. Configuration du mode SNMP v2c	249
F.1.2. Création du destinataire de déROUTement SNMP v2c STA sur la bibliothèque	250

F.1.3. Activation du mode SNMP v2c pour STA 251

Index 253

Liste des illustrations

8.1. Présentation de la tâche de mise à niveau avec serveur unique	113
8.2. Présentation de la tâche de mise à niveau avec deux serveurs	114
A.1. Exemple de liste de Oracle Storage Home	155
A.2. Détail de tâche affiché en sélectionnant la tâche dans la fenêtre principale.	157
A.3. Détail de tâche affiché en sélectionnant l'icône Expand.	158
A.4. Exemple d'affichage de journal de vérification des prérequis	159
A.5. Exemple d'affichage du journal de progression de l'installation	186
A.6. Exemple de détail de progression de la configuration	188
A.7. Exemple d'affichage de journal de progression de la désinstallation	195

Liste des tableaux

2.1. Tâches d'installation de Linux	27
2.2. Disposition du système de fichiers recommandée	29
2.3. Linux Package Selection	32
3.1. Ports externes non configurables	45
3.2. Ports externes configurables	46
3.3. Ports internes configurables	46
4.1. Procédure d'activation de l'interface ADI sur les lecteurs LTO IBM	62
4.2. Adresses IP de bibliothèque recommandées pour la connexion STA	64
4.3. Exemples d'attributions d'ID de complexe	64
4.4. Tâches de configuration des bibliothèques pour STA	68
5.1. Tâches de configuration des bibliothèques pour STA	79
7.1. Attributs de l'utilitaire d'administration du service de sauvegarde STA (staservadm)	103
7.2. Attributs du contrôleur de ressources STA (staresmonadm)	107
8.1. Directives relatives au moment d'exécuter les tâches de préparation de la mise à niveau	116
C.1. Activités de préparation de mise à niveau	213
C.2. Fiche de travail des emplacements et utilisateurs de l'installation	214
C.3. Fiche de travail des comptes utilisateurs	215
C.4. Ports externes non configurables	216
C.5. Ports internes et externes configurables	216
C.6. Nom de domaine de l'entreprise	217
C.7. Informations de configurations de l'utilisateur SNMP v3	217

Liste des exemples

3.1. Statut d'installation de STA réussie	56
4.1. Modification de l'ID de complexe de la bibliothèque SL8500	72
5.1. Création d'un utilisateur SNMP v3 sur la bibliothèque SL3000 ou SL8500	85
5.2. Création d'un utilisateur SNMP v3 sur la bibliothèque SL500	85
5.3. Création du destinataire de détournement SNMP v3 sur les bibliothèques SL3000 ou SL8500	87
5.4. Création du destinataire de détournement SNMP v3 sur la bibliothèque SL500	87
6.1. Commande snmpget réussie	91
6.2. Echec de la commande snmpget — Temporisation réseau	91
6.3. Echec de la commande snmpget — Mot de passe incorrect	91
8.1. Vidage de l'ancienne base de données	127
8.2. Transfert de l'ancienne base de données vers le serveur de sauvegarde (méthode à serveur unique)	128
8.3. Transfert de l'ancienne base de données vers le nouveau serveur STA (méthode à deux serveurs)	128
8.4. Vidage de la nouvelle base de données	131
8.5. Transfert de l'ancienne base de données vers le nouveau serveur STA	132
8.6. Purge des données obsolètes de l'ancienne sauvegarde de base de données	133
A.1. Exemple d'affichage avec X11 correctement configuré	148
A.2. Exemple d'affichages avec X11 mal configuré	148
B.1. Modèle de fichier réponse du programme d'installation de STA en mode silencieux	199
B.2. Modèle de fichier réponse du programme de désinstallation de STA en mode silencieux	200
B.3. Exemple d'exécution d'utilitaire de construction de fichier réponse du programme d'installation	202
B.4. Exemple de fichier d'utilitaire du programme d'installation à l'aide de l'utilitaire de construction	204
B.5. Messages finaux d'installation réussie de STA en mode silencieux	205
B.6. Exemple de messages finaux d'échec d'installation de STA en mode silencieux	206
B.7. Exemple d'exécution d'utilitaire de construction de fichier réponse du programme de désinstallation	207
B.8. Exemple de fichier réponse du programme de désinstallation après avoir utilisé l'utilitaire de construction	207
B.9. Messages finaux de désinstallation réussie de STA en mode silencieux	209
B.10. Exemple de messages finaux d'échec de désinstallation de STA en mode silencieux	209

Préface

Ce document fournit les concepts et les procédures relatifs à l'utilisation et à la configuration de StorageTek Tape Analytics (STA) d'Oracle.

Public visé

Ce document s'adresse aux personnes suivantes :

- Administrateur Linux : installe, configure et gère Linux sur le serveur STA.
- Administrateur STA : installe, configure et gère l'application STA.
- Administrateur de bibliothèque : configure et gère les bibliothèques StorageTek.
- Programmeur du système MVS : Configure et gère l'accès à STA par les utilisateurs du mainframe IBM.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si vous êtes malentendant.

Documents connexes

L'ensemble de la documentation STA comprend les documents suivants.

Pour les utilisateurs de l'application STA

- *Guide de démarrage rapide de STA* : Ce guide permet de vous présenter l'application STA et certaines fonctionnalités de l'interface utilisateur.
- *Guide de l'utilisateur STA* : Ce guide fournit des instructions d'utilisation de toutes les fonctionnalités de l'application STA, comme le tableau de bord, les modèles, les filtres, les alertes, les rapports exécutifs, les groupes logiques et la validation de média STA. Ce guide contient également les instructions relatives à l'administration et la gestion des noms d'utilisateur STA, des adresses électroniques, des journaux de service et des connexions SNMP avec les bibliothèques contrôlées.

- *Guide de présentation des écrans de STA* : Ce guide fournit des informations détaillées sur l'interface utilisateur STA. Il décrit la navigation entre les écrans, la présentation des écrans et l'utilisation des graphiques et des tableaux.
- *Guide de référence sur les données de STA* : Ce guide permet de rechercher des définitions relatives à tous les écrans et attributs de données du système de bibliothèques de bandes STA.

Pour les installateurs et les administrateurs du serveur et de l'application STA

- *Notes de version de STA* : Lisez ce document avant d'installer et d'utiliser STA. Il contient des informations de version importantes, notamment les problèmes connus. Ce document est disponible dans le pack de supports STA à télécharger.
- *Guide des conditions requises pour l'installation de STA* : Ce guide permet de découvrir les conditions requises minimales et recommandées pour l'utilisation de STA. Ce guide aborde les conditions relatives aux éléments suivants : bibliothèque, lecteur, serveur, interface utilisateur, validation de média STA et RACF (programme de contrôle d'accès d'IBM).
- *Guide d'installation et de configuration de STA* : Ce guide permet de planifier l'installation de STA, d'installer le système d'exploitation Linux, d'installer l'application STA, puis de configurer STA pour qu'il commence à contrôler les bibliothèques. Ce guide contient également les instructions relatives à la mise à niveau vers une nouvelle version de STA.
- *Guide d'administration de STA* : Utilisez ce guide pour obtenir des informations relatives aux tâches d'administration du serveur STA, telles que la configuration des services STA, la sauvegarde et la restauration de base de données et l'administration des mots de passes pour les comptes de base de données.
- *Guide de sécurité de STA* : Lisez ce document contenant des informations de sécurité importantes relatives à STA, y compris les conditions requises, les recommandations et les principes de sécurité généraux.
- *Manuel d'utilisateur des informations de licence de STA* : Lisez ce document contenant des informations sur l'utilisation des technologies tierces mises à votre disposition avec le produit STA.

Conventions

Les conventions de texte suivantes sont utilisées dans ce document :

Convention	Explication
gras	Des caractères gras indiquent des éléments d'interface utilisateur graphique associés à une action ou des termes définis dans le texte ou le glossaire.
<i>italique</i>	Les caractères en italique indiquent des titres de livres, la mise en valeur d'un concept ou des variables substituables pour lesquelles vous fournissez des valeurs particulières.
<i>largeur fixe</i>	Le type largeur fixe indique des commandes au sein d'un paragraphe, des adresses URL, des exemples de code, du texte affiché à l'écran ou du texte que vous saisissez.

Nouveautés

Cette section répertorie les nouvelles fonctionnalités et les améliorations présentes dans StorageTek Tape Analytics 2.1.0.

STA 2.1.0 - Janvier 2015

Reportez-vous aux manuels indiqués pour plus de détails sur les nouvelles fonctionnalités et les améliorations.

Le guide *Guide des conditions requises pour l'installation de STA* décrit :

- Les nouveaux niveaux de microprogramme de bibliothèque et de lecteur recommandés pour la prise en charge de STA 2.1.0.
- La prise en charge du protocole TTI 5.50 pour les lecteurs Oracle StorageTek T10000C et T10000D.
- Les nouvelles conditions requises recommandées en matière de bibliothèque et de lecteur pour la prise en charge de STA 2.1.0.
- La mise à jour de la configuration recommandée pour le serveur STA.

Le guide *Guide d'installation et de configuration de STA* décrit :

- Le nouveau programme d'installation et de désinstallation de STA 2.1.0, avec les nouvelles fonctionnalités suivantes :
 - L'utilisateur et groupe du programme d'installation Oracle : utilisateur et groupe Linux utilisé exclusivement pour l'installation et la mise à niveau des produits Oracle sur le serveur STA.
 - La définition par l'utilisateur de l'emplacement de Oracle Storage Home : l'application STA et le logiciel Oracle associé peuvent être installés sur n'importe quel système de fichiers contenant suffisamment d'espace.
 - La définition par l'utilisateur des emplacements de la base de données et de la sauvegarde locale.
 - L'emplacement de l'inventaire central Oracle : répertoire contenant les informations de suivi liées aux produits Oracle installés sur le serveur STA.
 - Le mode silencieux du programme d'installation et de désinstallation de STA : permet de contourner l'interface graphique et de fournir les options d'installation dans un fichier de propriétés XML.
 - Les nouveaux journaux détaillés pour le programme d'installation et de désinstallation de STA.
 - Une aide contextuelle pour tous les écrans du programme d'installation et de désinstallation graphique de STA.

- Une condition requise supplémentaire pour le package Linux RPM : le package *xorg-x11-utils* doit être installé pour pouvoir exécuter le programme d'installation graphique de STA.
- Les ports par défaut de la console d'administration WebLogic ont été remplacés par 7019 (HTTP) et 7020 (HTTPS). Si vous utilisez les assignations par défaut précédentes, vous devrez peut-être les remplacer par les nouvelles.
- Les nouvelles conditions requises pour les mots de passe STA et les noms d'utilisateur MySQL.
- Le nouveau processus pour mettre à niveau des bases de données STA 1.0.x et STA 2.0.x vers STA 2.1.0.

Le guide *Guide de démarrage rapide de STA* décrit :

- Pas de modifications majeures

Le guide *Guide de l'utilisateur STA* décrit :

- Des mises à jour mineures apportées aux modèles suivants pour fournir des informations supplémentaires et améliorer l'ergonomie :
 - STA-Complex-Configuration
 - STA-Complex-Utilization
 - STA-Lib-Configuration
 - STA-Drive-MV
 - STA-Media-All
 - STA-Media-MV-Calibration
 - Ecran Media Validation Overview, modèle STA-Default
- Modification de la documentation : les chapitres suivants ont été retirés du guide *Guide d'administration de STA*. Le guide *Guide de l'utilisateur STA* décrit à présent toutes les fonctionnalités et activités disponibles dans l'interface utilisateur STA.
 - Noms d'utilisateur et adresses e-mail STA
 - Journaux des services STA
 - Gestion des connexions SNMP dans STA

Le guide *Guide de présentation des écrans de STA* décrit :

- Pas de modifications majeures

Le guide *Guide de référence sur les données de STA* décrit que :

- Les attributs figurant dans certains écrans ont été réorganisés pour améliorer l'ergonomie.
- Des attributs "Last messages" sont disponibles dans les écrans respectifs des ports d'accès aux cartouches, des lecteurs, des ascenseurs, des bibliothèques, des ports PTP et des robots.

Le guide *Guide d'administration de STA* décrit que :

- Une modification de la documentation : les chapitres suivants ont été déplacés vers le guide *Guide de l'utilisateur STA* :
 - Noms d'utilisateur et adresses e-mail
 - Journalisation
 - Gestion SNMP

Planification des tâches de pré-installation

Ce chapitre se compose des sections suivantes :

- [Aperçu du déploiement de STA](#)
- [Préparez les demande d'assistance pour préparer les bibliothèques](#)

1.1. Aperçu du déploiement de STA

Pour une première installation et configuration de STA, effectuez les tâches suivantes dans l'ordre indiqué. Vous pouvez effectuer cette opération par vous-même ou acheter les services d'installation Oracle.

Pour une mise à niveau d'une version précédente de STA, reportez-vous au chapitre [Chapitre 8, Mise à niveau vers STA 2.1.0](#).

Ordre	Activité	Détails et instructions
1	Vérifiez et contrôlez les conditions requise de STA sur votre site.	<i>Guide des conditions requises pour l'installation de STA</i>
2	Préparez les demande d'assistance pour les lecteurs et bibliothèques selon vos besoins.	Section 1.2, « Préparez les demande d'assistance pour préparer les bibliothèques »
3	Installez Linux sur le serveur STA.	Chapitre 2, Installation de Linux
4	Installez STA sur le serveur STA.	Chapitre 3, Installation de STA
5	Configurez les bibliothèques pour qu'elles envoient des données vers STA.	Chapitre 5, Configuration de SNMP sur les bibliothèques
6	Configurez STA pour recevoir les données des bibliothèques et commencer le contrôle.	Chapitre 6, Configuration des connexions de bibliothèque dans STA
7	Configurez des adresses e-mail et des noms d'utilisateur STA supplémentaires.	<i>Guide de l'utilisateur STA</i>
8	Configurez le contrôles de STA et les services de sauvegarde de base de données.	Chapitre 7, Configuration des services STA
9	Configurez un certificat de sécurité approuvé (facultatif).	Annexe D, Configuration des certificats de sécurité
10	Configurez un fournisseur externe de contrôle d'accès STA (facultatif).	Annexe E, Configuration d'un fournisseur de service de sécurité pour STA

1.2. Préparez les demande d'assistance pour préparer les bibliothèques

Suivez la procédure et les sections indiquées pour fournir au support Oracle les informations nécessaires à la préparation de vos bibliothèques pour le contrôle par STA.

Remarque:

Si STA doit contrôler un complexe de bibliothèques, préparez une demande d'assistance pour chaque bibliothèque du complexe. Vous pouvez également ouvrir une demande d'assistance pour installer le dernier microprogramme de lecteur pris en charge par STA.

1. Vérifiez la version du microprogramme de la bibliothèque. Voir la section [Section 4.3.2, « Vérification de la version du microprogramme de la bibliothèque »](#)
2. Vérifiez qu'une carte de contrôleur des lecteurs à grande quantité de mémoire (HBT) est installée (sur les modèles SL3000 et SL8500 uniquement). Voir la section [Section 4.3.3, « Vérification de la version de la carte de contrôleur des lecteurs \(bibliothèques SL3000 et SL8500 uniquement\) »](#).
3. Activation de l'interface ADI sur la bibliothèque et les lecteurs LTO : uniquement pour les bibliothèques avec des lecteurs LTO. Voir la section [Section 4.3.4, « Activation de l'interface ADI sur la bibliothèque \(toutes les bibliothèques sauf SL150\) »](#)
4. Définissez l'ID de complexe de bibliothèque (bibliothèque SL8500 uniquement) Voir la section [Section 4.3.5, « Vérification de l'ID de complexe de bibliothèque \(SL8500 uniquement\) »](#).
5. Définissez la date et l'heure de la bibliothèque : pour garantir que l'horodatage des données de la bibliothèque corresponde à l'horodatage du serveur STA, l'horloge de la bibliothèque doit être correctement définie par le support technique Oracle.
6. Soumettez les demandes d'assistance nécessaires.

Installation de Linux

Ce chapitre se compose des sections suivantes :

- [Tâches de préparation](#)
- [Tâches d'installation](#)
- [Tâches de post-Installation](#)

Avant d'installer Linux sur le serveur STA, consultez la configuration système requise dans le guide *Guide des conditions requises pour l'installation de STA*.

Remarque:

Vous ne pouvez pas effectuer une mise à niveau en place de Linux 5.x vers Linux 6.x. Si vous installez Linux 6.x dans le cadre de la mise à niveau vers STA 2.0.x, reportez-vous au chapitre [Chapitre 8, Mise à niveau vers STA 2.1.0](#).

Pour installer et configurer Linux pour STA, exécutez les tâches décrites dans le tableau [Tableau 2.1, « Tâches d'installation de Linux »](#) dans l'ordre indiqué.

Tableau 2.1. Tâches d'installation de Linux

Catégorie	Tâche
Préparation	<ol style="list-style-type: none">1. Section 2.1.1, « Consultation de la documentation connexe » [28]2. Section 2.1.3, « Téléchargement du pack de supports du programme d'installation de Linux » [30]
Installation	<ol style="list-style-type: none">1. Section 2.2.1, « Rassemblement des informations requises » [31]2. Section 2.2.2, « Installation de Linux » [31]3. Section 2.2.3, « Exécution de l'agent de configuration Linux Setup Agent » [33]
Post-installation	<ol style="list-style-type: none">1. Section 2.3.1, « Désactivation de SELinux » [34]2. Section 2.3.2, « Désactivation du pare-feu Linux » [34]3. Section 2.3.3, « Désactivation du contrôle d'accès » [35]4. Section 2.3.4, « Configuration du proxy réseau » [36]5. Section 2.3.5, « Vérification de la configuration correcte de Yum (facultatif) » [36]6. Section 2.3.6, « Installation des packages Linux requis » [38]7. Section 2.3.7, « Vérification de la configuration correcte de SSH » [39]8. Section 2.3.8, « Vérification des paramètres DNS appropriés » [39]9. Section 2.3.9, « Désactivation des services de noms » [39]

Catégorie	Tâche
	10. Section 2.3.10, « Vérification du fonctionnement du navigateur local (facultatif) » [40]

2.1. Tâches de préparation

Suivez ces procédures avant d'installer Linux sur le serveur STA.

- [Section 2.1.1, « Consultation de la documentation connexe »](#)
- [Section 2.1.2, « Examen de la disposition du système de fichiers STA »](#)
- [Section 2.1.3, « Téléchargement du pack de supports du programme d'installation de Linux »](#)

2.1.1. Consultation de la documentation connexe

Les conditions requises et les options de configuration réseau étant très variées, reportez-vous aux documents suivants pour obtenir de l'aide pour l'installation et la configuration du matériel, des logiciels et du réseau. La configuration réseau IPv4 et IPv6 est présentée de façon détaillée dans ces documents.

- Guides d'installation de Oracle Linux :

<http://docs.oracle.com/en/operating-systems/>

- Documentation RedHat Linux :

<https://access.redhat.com/home>

2.1.2. Examen de la disposition du système de fichiers STA

Le chapitre [Tableau 2.2, « Disposition du système de fichiers recommandée »](#) décrit la disposition de système de fichiers recommandée pour le serveur STA. Vous configurez la disposition pendant l'installation de Linux.

Les emplacements suivants sont définis par l'utilisateur, ce qui signifie que vous pouvez configurer la disposition selon les conditions requises par votre site.

- Oracle Storage Home : Le programme d'installation de STA vous invitera à indiquer cet emplacement. Aucune valeur par défaut. Pour plus d'informations, reportez-vous à la section [Emplacement de Oracle Storage Home](#).
- Base de données STA : Le programme d'installation de STA vous invitera à indiquer cet emplacement. La valeur par défaut est `/dbdata`.
- Sauvegarde locale de la base de données STA : Le programme d'installation de STA vous invitera à indiquer cet emplacement. Par défaut, il s'agira de `/dbbackup`.
- Journaux STA et MySQL : Par défaut, il s'agira de `/var/log/tbi`. Si vous souhaitez utiliser un emplacement différent après avoir terminé l'installation de Linux et avant d'installer STA, vous devez créer un lien symbolique de votre emplacement vers `/var/log/tbi` après l'installation de STA. Pour obtenir des instructions, reportez-vous à la section [Section 3.6.6, « Déplacement du répertoire des journaux STA \(facultatif\) »](#).

Oracle recommande de créer ces systèmes de fichiers avant d'installer STA, sans quoi STA sera installé dans les répertoires root "/" et */var*, nécessitant une allocation d'espace supplémentaire à ces répertoires. Même si le programme d'installation STA crée les répertoires nécessaires, vous aurez un plus grand contrôle des propriétés du système de fichiers si vous les créez au préalable.

Tableau 2.2. Disposition du système de fichiers recommandée

Système de fichiers	Point de montage par défaut	Taille	Description et recommandations
root	/	32 Go minimum	Si le répertoire <i>/tmp</i> est inclus dans ce système de fichiers, il sera nécessaire de conserver un minimum de 4 Go d'espace libre, qui sera requis pendant les installations et mises à niveau de STA.
espace de swap	Aucun. Défini comme mémoire.	50 à 100 % de la RAM	Utilisé pour l'espace de swap.
Oracle Storage Home	<i>/Oracle</i>	30 Go minimum 50 Go recommandé	<p>Emplacement des fichiers d'application de STA et Oracle Middleware (WebLogic, MySQL, RDA).</p> <p>Cet emplacement est défini par l'utilisateur. Ce système de fichiers doit être distinct, sur un volume distinct. Conservez un minimum de 4 Go d'espace libre pour les installations et les mises à niveau de STA. Conservez 5 Go supplémentaires d'espace libre pour la rotation des journaux WebLogic.</p> <p>STA crée automatiquement les sous-répertoires Oracle Middleware suivants :</p> <ul style="list-style-type: none"> • Journaux WebLogic permutés : <i>/Oracle_storage_home/Middleware/user_projects/domains/TBI/servers</i> • Instantané de la dernière CLI de RDA : <i>/Oracle_storage_home/Middleware/rda/output</i> • Bundles de journaux d'instantané de l'interface graphique de STA : <i>/Oracle_storage_home/Middleware/rda/snapshots</i>
Emplacement de la base de données STA	<i>/dbdata</i>	250 Go à 2 To	<p>Emplacement de la base de données STA. Cet emplacement est défini par l'utilisateur. Oracle vous recommande fortement de placer ce répertoire sur un volume distinct, isolé de root, de swap, de Oracle Storage Home, et de l'emplacement des journaux STA. Pour assurer performances, sauvegarde et maintenabilité, les meilleures pratiques recommandent d'utiliser un ensemble distinct de lecteurs entrelacés ou en miroir.</p> <p>La taille requise dépend du nombre de bibliothèques, de lecteurs, de médias, d'échanges par jour, et d'années d'historiques de données ; Oracle vous recommande de configurer les services STA pour émettre une alerte si l'utilisation d'espace dépasse un pourcentage défini.</p>
Emplacement de sauvegarde locale de la base de données STA	<i>/dbbackup</i>	70 à 80 % de la taille de <i>/dbdata</i>	Emplacement de la sauvegarde locale de base de données la plus récente. Cet emplacement est défini par l'utilisateur. Oracle recommande de le placer sur un volume différent de celui de la base de données STA, et sur des lecteurs entrelacés ou en miroir, en cas base de données endommagée ou défaillante.
Emplacement des journaux STA	<i>/var/log/tbi</i>	30 Go minimum	Emplacement des journaux STA et MySQL. Il doit s'agir d'un volume distinct sur un point de montage distinct. Les contenus ont tendance à augmenter, et sont gérés par la rotation des journaux. L'emplacement par défaut est <i>/var/log/tbi</i> ,

Système de fichiers	Point de montage par défaut	Taille	Description et recommandations
		50 à 100 Go recommandé	<p>mais vous pouvez le modifier à tout moment après l'installation de STA ; pour obtenir des instructions, reportez-vous à la section Section 3.6.6, « Déplacement du répertoire des journaux STA (facultatif) ».</p> <p>Remarque : A l'exception de la rotation des journaux, STA n'effectue aucune gestion de l'espace.</p> <p>Prudence : Vous devez configurer l'utilitaire de sauvegarde STA de sorte qu'il gère les fichiers journaux dans le répertoire <code>/STA_logs/db/stadb_bin.*</code>. Si ce n'est pas le cas, ces fichiers risquent de nécessiter une gestion manuelle (pour plus d'informations, reportez-vous au guide <i>Guide d'administration de STA</i>).</p>

2.1.3. Téléchargement du pack de supports du programme d'installation de Linux

Utilisez cette procédure pour télécharger le pack de supports du programme d'installation de Linux sur le site Web Oracle Software Delivery Cloud. Le pack de supports est fourni en tant que fichier d'image ISO compressé. Vous pouvez l'extraire et l'écrire sur un média portable de votre choix (lecteur flash, DVD, etc.).

Avant d'effectuer cette tâche, vous avez besoin d'un ID utilisateur et d'un mot de passe Oracle Software Delivery Cloud, que votre représentant du support technique Oracle pourra vous fournir.

- Ouvrez un navigateur Web sur le système et accédez au site Web Oracle Software Delivery Cloud à l'adresse suivante :

<http://edelivery.oracle.com/linux>
- Cliquez sur **Sign In/Register**.
- Saisissez l'ID utilisateur et le mot de passe fournis par le support Oracle.
- A l'écran Terms & Restrictions, sélectionnez les cases à cocher pour indiquer votre accord concernant le contrat de licence et les restrictions d'exportation, puis cliquez sur **Continue**.
- Dans l'écran Media Pack Search :
 - Dans le menu Select a Product Pack, sélectionnez **Oracle Linux**.
 - Dans le menu Platform, sélectionnez **x86 64 bits** (STA nécessite la version 64 bits de Linux).
 - Cliquez sur **Go**.
- Sélectionnez une version de Linux, puis cliquez sur **Continue**.

Pour connaître les conditions minimales de version de Linux, reportez-vous au guide *Guide des conditions requises pour l'installation de STA*.

- Cliquez sur **Download** pour l'option 64 bits.
- Enregistrez le fichier ISO et écrivez-le sur le média.

2.2. Tâches d'installation

Les procédures suivantes impliquent l'installation d'Oracle Enterprise Linux (OEL) 6u4 à l'aide du DVD, du programme d'installation graphique et de l'agent de configuration. Si vous installez une autre version de Linux, utilisez un autre média ou utilisez le mode console ; les étapes et packages peuvent varier.

2.2.1. Rassemblement des informations requises

Pour obtenir les informations suivantes, merci de contacter votre administrateur système :

- Nom d'hôte et l'adresse IP du serveur STA
- Adresse IP de la passerelle et le masque de réseau pour votre réseau
- Adresses IP de serveur DNS et domaines de recherche pour votre réseau
- Adresse IP des serveurs NTP (network time protocol) que vous allez utiliser
- Informations relatives au proxy réseau, le cas échéant

2.2.2. Installation de Linux

Suivez cette procédure pour installer Linux.

1. Connectez le média d'installation au serveur STA.
2. Démarrez le programme d'installation Linux à l'aide des instructions du fichier README se trouvant sur le média.
3. Sélectionnez **Install or upgrade an existing system**.
4. Si vous effectuez l'installation à l'aide d'un DVD, l'écran CD Found s'affiche. Vous pouvez éventuellement effectuer un test du média. Pour ignorer ce test, appuyez sur la touche **Tab** pour sélectionner l'option **Skip**, puis appuyez sur la touche **Spacebar**.
5. A l'écran Welcome, cliquez sur **Next**.
6. Sélectionnez votre langue, puis cliquez sur **Next**.
7. Sélectionnez la configuration du clavier, puis cliquez sur **Next**.
8. Sélectionnez **Basic Storage Devices**, puis cliquez sur **Next**.
9. Saisissez un nom d'hôte pour le serveur STA, puis cliquez sur **Configure Network**.
10. Sélectionnez le nom de l'adaptateur réseau, puis cliquez sur **Edit**.
11. Assurez-vous que les options **Connect automatically** et **Available to all users** sont sélectionnées.
12. Dans les autres onglets, configurez l'adaptateur en fonction des spécifications IPv4 ou IPv6 de votre administrateur réseau. Vous devez indiquer une adresse IP statique pour le serveur STA et au moins un serveur DNS. Une fois fait, cliquez sur **Apply**, **Close**, et **Next**.
13. Sélectionnez le fuseau horaire du serveur STA, sélectionnez la case **System clock uses UTC**, puis cliquez sur **Next**.
14. Saisissez et confirmez un mot de passe root pour le serveur, puis cliquez sur **Next**.

15. Identifiez une mise en page de partitionnement à utiliser sur le serveur :
 - a. STA nécessitant un serveur dédié, Oracle recommande de sélectionner **Use All Space**.
 - b. Sélectionnez la case **Review and modify partitioning layout**, puis cliquez sur **Next**.
16. Servez-vous du tableau [Tableau 2.2, « Disposition du système de fichiers recommandée »](#) pour modifier la disposition du système de fichiers, car celui par défaut ne répond pas aux conditions requises minimales pour STA. Vous pouvez également utiliser l'utilitaire *system-config-lvm* pour modifier le système de fichiers après l'installation de Linux.

Une fois fait, cliquez sur **Next**.
17. Lorsque vous êtes prêt, sélectionnez **Write changes to disk**.
18. A l'écran du programme d'amorçage, conservez toutes les options telles qu'elles sont définies, puis cliquez sur **Next**.
19. A l'écran de sélection de logiciel, sélectionnez **Basic Server** et ne modifiez pas les options du référentiel. Ensuite, sélectionnez **Customize now**, puis cliquez sur **Next**.
20. A l'écran de sélection du package, servez-vous du tableau [Tableau 2.3, « Linux Package Selection »](#) pour configurer les packages pour chaque catégorie de package :
 - a. Sélectionnez une catégorie de package.
 - b. Sélectionnez la case correspondant à chaque package dans la colonne Select.
 - c. Si un package nécessite une option (indiquée par un signe +), sélectionnez le package parent, cliquez sur le bouton **Optional packages**, sélectionnez le package enfant dans la liste, puis cliquez sur **Close**.
 - d. Désactivez la case correspondant à chaque package figurant dans la colonne Deselect.
 - e. Conservez les sélections des autres cases à cocher.

Tableau 2.3. Linux Package Selection

Package Category	Select	Deselect
Base System	<ul style="list-style-type: none"> • Base • Compatibility libraries • Console internet tools • Java Platform • Legacy UNIX compatibility + <i>ksh-xxxxxxx-xx.e16.x86_64</i>	<ul style="list-style-type: none"> • Debugging Tools • Dial-up Networking Support • Directory Client • Hardware monitoring utilities • Large Systems Performance • Network file system client • Performance Tools
Servers (facultative)	<ul style="list-style-type: none"> • System administration tools 	NA
Web Services	NA	All packages
Databases	NA	All packages
System Management	NA	NA
Virtualization	NA	NA
Desktops (recommandée) : Utilisés pour exécuter certaines étapes de post-installation dans un environnement graphique ; pour plus d'informations, reportez-vous à la section	<ul style="list-style-type: none"> • Desktop • Desktop Platform • General Purpose Desktop • Graphical Administration Tools 	NA

Package Category	Select	Deselect
Section 2.3, « Tâches de post-Installation » .	<ul style="list-style-type: none"> + <i>system-config-lvm-x.x.xx-xx.e16</i> <i>.noarch</i>¹ • Legacy X Window System compatibility • X11 (X Window System, version 11) 	
Applications (facultative) — Peut être utilisée pour configurer et gérer le serveur STA en local avec l'interface graphique.	<ul style="list-style-type: none"> • Internet Browser 	NA
Development	<ul style="list-style-type: none"> • Development tools <p>+ <i>expect-x.xx.x.xx-x.e16.x86_64</i></p>	NA
Languages	NA	NA

¹Facultative. Peut être utilisée pour configurer ou reconfigurer le système de fichiers une fois l'installation de Linux terminée.

21. Lorsque vous avez terminé la sélection des packages, cliquez sur **Next**. L'installation va alors démarrer.

Si vous cliquez sur **Next** par inadvertance avant d'avoir configuré tous les packages, cliquez sur **Back** quand le logiciel a terminé un contrôle de dépendance.

22. Lorsque l'écran Congratulations s'affiche, retirez le média d'installation, puis cliquez sur **Reboot**.

Vous trouverez un journal complet de l'installation sous */root/install.log*.

2.2.3. Exécution de l'agent de configuration Linux Setup Agent

L'agent de configuration Linux Setup Agent démarre automatiquement lorsque vous réinitialisez le serveur Linux. Suivez cette procédure pour configurer l'environnement du système.

1. A l'écran Welcome, cliquez sur **Forward**.
2. Lisez le contrat de licence, sélectionnez **Yes, I agree to the License Agreement**, puis cliquez sur **Forward**.
3. A l'écran Software Updates, si vous souhaitez enregistrer votre système pour obtenir des mises à jour, sélectionnez **Yes, I'd like to register now**. Sinon, sélectionnez **No, I prefer to register at a later time**, puis cliquez sur **Forward**.
4. A l'écran Finish Updates Setup, cliquez sur **Forward**.
5. A l'écran Create User, laissez les champs vides, cliquez sur **Forward**, puis sur **Yes** pour continuer. Le serveur STA ne nécessite pas d'utilisateur non administrateur.
6. A l'écran Date and Time :
 - a. Définissez la date et l'heure actuelle.
 - b. Sélectionnez la case à cocher **Synchronize date and time over the network**.
 - c. Ajoutez ou supprimez les serveurs NTP souhaités (selon les instructions de votre administrateur informatique), puis cliquez sur **Forward**.

Remarque:

Pour garantir que les données et les fichiers journaux de STA sont corrects, la date et l'heure du serveur STA doivent être correctes. De plus, toute bibliothèque connectée à STA doit également être définie sur l'heure correcte.

7. A l'écran Kdump, ne sélectionnez *pas* **Enable kdump?**. Cliquez ensuite sur **Finish**.

Le système est réinitialisé.

8. Après la réinitialisation du système, connectez-vous en tant qu'utilisateur root :
 - a. Cliquez sur **Other...**
 - b. Saisissez le nom utilisateur **root**, puis cliquez sur **Log In**.
 - c. Saisissez le mot de passe root, puis cliquez à nouveau sur **Log In**.

Si un message s'affiche pour vous informer que vous êtes connecté en tant que superutilisateur root, vous pouvez ignorer ce message.

9. Confirmez la version de Linux et le niveau de mise à jour. Cette opération est facultative.

```
# 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. Tâches de post-Installation

Exécutez les tâches suivantes pour vous assurer que le serveur STA est correctement configuré pour l'installation de STA.

2.3.1. Désactivation de SELinux

Oracle recommande de désactiver SELinux sur le serveur STA.

1. Ouvrez une session de terminal sur le serveur STA.
2. Ouvrez le fichier de configuration SELinux avec un éditeur de texte.

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

3. Dans le fichier, définissez *SELINUX* sur *disabled* :

```
SELINUX=disabled
```

4. Enregistrez le fichier et fermez-le.

2.3.2. Désactivation du pare-feu Linux

Oracle vous recommande de désactiver le pare-feu sur le serveur STA. Cependant, selon les conditions requises de votre site, vous pouvez choisir d'activer et de configurer le pare-feu.

Suivez cette procédure pour désactiver le pare-feu.

1. Ouvrez une session de terminal sur le serveur STA.
2. Vérifiez les paramètres du pare-feu Linux (pour la prochaine initialisation).

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

Si le pare-feu est désactivé pour la prochaine initialisation, toutes les sorties des IPTables et ip6tables s'afficheront comme *off*. Dans le cas contraire, désactivez le pare-feu.

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

3. Vérifiez le statut actuel du pare-feu Linux.

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

La sortie de la commande indiquera si le pare-feu est en cours d'exécution. Si le pare-feu est en cours d'exécution, arrêtez-le.

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

4. Si l'une des affirmations suivantes s'applique à votre cas, vous devez réinitialiser le serveur.
 - Vous avez désactivé SELinux dans la section [Section 2.3.1, « Désactivation de SELinux » \[34\]](#).
 - Vous avez désactivé le pare-feu Linux (à l'aide de la commande *chkconfig*) dans cette section.

2.3.3. Désactivation du contrôle d'accès

Le contrôle d'accès doit être désactivé pour certains répertoires.

1. Répertoriez les accès à Oracle Storage Home, à la base de données STA, à la sauvegarde locale de la base de données STA, et aux emplacements de journaux STA. Par exemple :

```
# 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. Dans la sortie de chaque commande, recherchez un point à la fin des autorisations indiquées. Dans l'exemple suivant, notez le "." après *drxwr-xr-x*.

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

3. Si aucun répertoire ne contient de point après les déclarations d'autorisation, le contrôle d'accès est déjà désactivé et vous pouvez passer à l'étape suivante.

Si le contrôle d'accès est activé sur un répertoire, connectez-vous en tant qu'utilisateur root du système, et exécutez la commande suivante pour ce répertoire.

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

Par exemple :

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

2.3.4. Configuration du proxy réseau

Vous pouvez configurer le serveur STA pour qu'il se connecte au réseau directement ou via un serveur proxy.

1. Depuis le menu **System** du bureau Linux, sélectionnez **Preferences**, puis **Network Proxy**.
2. Dans la boîte de dialogue Network Proxy Preferences, indiquez la configuration de proxy correspondant aux conditions requises de votre site.
3. Cliquez sur **Close**.

2.3.5. Vérification de la configuration correcte de Yum (facultatif)

Ne suivez cette procédure que si vous utilisez Yum (Yellowdog Updater, Modified) pour installer les packages logiciels Linux RPM (Red Hat Package Manager) requis. (Pour connaître les packages requis, reportez-vous à la section [Section 2.3.6, « Installation des packages Linux requis »](#).)

Il existe plusieurs méthodes d'installation des packages RPM, y compris Yum. L'utilisation de Yum est facultative mais recommandée, car elle simplifie votre installation des packages. Yum recherche automatiquement les référentiels des packages RPM, les dernières versions de packages et leurs dépendances. Suivez cette procédure pour vous assurer que Yum est correctement configuré sur le serveur STA.

Remarque:

Les exemples de commandes suivants utilisent le référentiel Yum pour Oracle Linux. Dans ces commandes, le "l" dans "ol6" est la lettre minuscule "L".

1. Envoyez une requête (ping) au serveur Yum public Oracle pour vous assurer que la connexion réseau fonctionne.

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

2. Passez au répertoire du référentiel Yum et définissez le nom de fichier du référentiel Yum.

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

3. Supprimez le fichier de référentiel Yum existant.

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

4. Téléchargez le dernier fichier de référentiel Yum depuis le site Web Yum.

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

Remarque:

Les exécutions ultérieures de cette commande copieront un nouveau fichier de référentiel dans le dossier *yum.repos.d* avec une nouvelle extension (par exemple, *public-yum-ol6.repo.1*). Cependant, Yum utilise toujours le fichier de référentiel sans extension.

5. Ouvrez le fichier de référentiel avec un éditeur de texte.

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

6. Dans le fichier, recherchez l'entrée correspondant à votre version de Linux et activez-la en indiquant *enabled=1*. Désactivez toutes les autres entrées en indiquant *enabled=0*.

Par exemple :

```
[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. Enregistrez le fichier et fermez-le.

2.3.6. Installation des packages Linux requis

Des packages RPM supplémentaires sont requis pour l'installation et le fonctionnement de STA. Le programme d'installation de STA contrôlera la présence des packages suivants ; s'ils ne sont pas installés, l'installation de STA échouera.

Remarque:

Les noms de package RPM sont sensibles à la casse.

• <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>crontie</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>

Vous pouvez installer les packages RPM requis de différentes façons. Cette procédure décrit l'utilisation de Yum.

La commande Yum d'installation de package vérifie la version la plus récente du package pour votre version de Linux, puis installe le package et ses dépendances. En fonction de votre installation Linux, certains de ces packages peuvent avoir été préalablement installés. Si un package est déjà installé, et à sa version la plus récente, le système vous l'indique.

1. Ouvrez une session de terminal sur le serveur STA.
2. Procédez comme suit :
 - Si vous parvenez à vous connecter au serveur Yum public de Oracle, (voir la section [Section 2.3.5, « Vérification de la configuration correcte de Yum \(facultatif\) »](#)), utilisez l'une des méthodes suivantes pour installer les packages :
 - Installez les packages un par un. Le package indiqué sera téléchargé et vérifié, et vous devrez répondre à toutes les invites.

```
# yum install package_name
```

- Installez tous les packages en une fois sans invite. L'option `-y` répond automatiquement "yes" à toutes les invites de l'installation.

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

- Si le pare-feu de votre réseau bloque les accès extérieurs au réseau, vous pouvez utiliser Yum pour installer des packages disponibles localement à partir du média Linux. Par exemple :

```
# cd /mnt/install_media_mount_location/packages
```

```
# yum install ./package_name
```

2.3.7. Vérification de la configuration correcte de SSH

Suivez cette procédure pour vous assurer que SSH (secure shell) est correctement configuré sur le serveur STA. Cela permettra d'accélérer les transferts de sauvegarde de la base de données STA vers un hôte distant.

1. Ouvrez le fichier de configuration SSH avec un éditeur de texte.

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

2. Recherchez les entrées *AddressFamily* et *UseDNS*. Modifiez-les de façon à ce qu'elles ne soient *pas* précédées d'un caractère de commentaire et à ce qu'elles aient les valeurs suivantes :

```
AddressFamily inet
UseDNS no
```

3. Enregistrez le fichier et fermez-le.
4. Redémarrez le démon sshd.

```
# service sshd restart
```

2.3.8. Vérification des paramètres DNS appropriés

Suivez cette procédure pour vous assurer que l'adresse IP du serveur STA est mappée à son nom d'hôte.

1. Ouvrez le fichier des hôtes avec un éditeur de texte.

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

2. A la fin du fichier, ajoutez l'adresse IP du serveur STA, suivie d'une tabulation, puis du nom d'hôte du serveur STA. Par exemple :

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

3. Enregistrez le fichier et fermez-le. Vous n'avez pas besoin de redémarrer le serveur STA pour que les nouveaux paramètres soient appliqués.

2.3.9. Désactivation des services de noms

Les services de noms tels que LDAP peuvent créer des conflits avec l'installation de STA. Suivez cette procédure pour désactiver temporairement ces services.

1. Ouvrez le fichier de configuration du commutateur du service de noms avec un éditeur de texte.

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

2. Désactivez toutes les entrées du service de noms. Par exemple, pour désactiver LDAP, annulez le commentaire "ldap" sur les lignes suivantes :

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

3. Enregistrez le fichier et fermez-le. Vous n'avez pas besoin de redémarrer le serveur STA pour que les nouveaux paramètres soient appliqués. Après avoir installé STA, vous pouvez modifier le fichier nsswitch.conf pour réactiver les services de noms.

2.3.10. Vérification du fonctionnement du navigateur local (facultatif)

Pour configurer et gérer STA localement sur le serveur STA, vérifiez que vous disposez des plug-ins et des versions de navigateur minimales prises en charge (voir le guide *Guide des conditions requises pour l'installation de STA*).

Remarque:

Oracle ne recommande pas l'accès local à l'application STA en raison des répercussions négatives sur les performances du serveur.

Installation de STA

Ce chapitre suppose que vous procédez à une nouvelle installation de STA sur le serveur.

- Si vous effectuez une mise à niveau de STA depuis une version antérieure, reportez-vous au chapitre [Chapitre 8, Mise à niveau vers STA 2.1.0](#). Oracle vous recommande d'installer ou de mettre à niveau vers la dernière version de STA.
- Si vous devez réinstaller STA ou réparer une installation actuelle, reportez-vous au chapitre [Chapitre 9, Désinstallation et restauration de STA](#)

Remarque:

Oracle ne fournira d'assistance que si STA est installé sur un serveur dédié (appelé *serveur STA* tout au long de ce guide).

Ce chapitre se compose des sections suivantes :

- [Utilisateurs, groupes et emplacements utilisés par le programme d'installation de STA](#)
- [Comptes et ports configurés pendant l'installation de STA](#)
- [Journaux d'installation et de désinstallation de STA](#)
- [Modes du programme d'installation de STA](#)
- [Tâches d'installation de STA](#)

L'annexe [Annexe C, Fiches de travail d'installation et de mise à niveau](#) comporte des fiches de travail qui peuvent vous servir à organiser vos activités d'installation et à enregistrer vos paramètres.

3.1. Utilisateurs, groupes et emplacements utilisés par le programme d'installation de STA

Cette section décrit les termes et concepts-clés utilisés pendant le processus d'installation de STA.

Groupe d'installation Oracle

Groupe Linux servant à installer et mettre à jour les produits Oracle sur le serveur STA. Oracle recommande la création d'un groupe distinct dédié à cette tâche.

Pour effectuer une installation de STA, vous devez vous connecter en tant qu'utilisateur faisant partie de ce groupe. Vous ne pouvez pas installer STA en tant qu'utilisateur *root* Linux ni en tant que tout autre utilisateur avec des privilèges superutilisateur.

Les instructions et exemples dans ce guide utilisent *oinstall* comme nom pour ce groupe, remplacez le nom que vous avez choisi s'il est différent.

Utilisateur du programme d'installation Oracle

Utilisateur Linux installant et mettant à niveau les produits Oracle sur le serveur STA. Il peut s'agir de n'importe quel utilisateur du groupe d'installation Oracle.

Les instructions et exemples de ce guide appellent cet utilisateur *oracle*, remplacez le nom que vous avez choisi s'il est différent.

Emplacement de l'inventaire central Oracle

Répertoire contenant les informations de suivi des produits Oracle installés sur le serveur STA. Les journaux du programme d'installation et de désinstallation de STA sont conservés dans le sous-répertoire *logs* de cet emplacement.

L'utilisateur du programme d'installation Oracle doit être propriétaire de ce répertoire et disposer de toutes les autorisations afférentes. Pour garantir que les autres utilisateurs du groupe d'installation Oracle aient accès à ce répertoire et qu'ils puissent installer les produits Oracle, vous ne devez pas utiliser le répertoire personnel de l'utilisateur du programme d'installation Oracle.

Cet emplacement doit être distinct des autres répertoires décrits dans cette section. Les instructions et exemples de ce guide utilisent comme emplacement */opt/oracle/oraInventory*, remplacez le répertoire que vous avez choisi s'il est différent.

Remarque:

Oracle recommande d'inscrire cet emplacement une fois que l'installation de STA est terminée, de sorte que tous les installateurs de Oracle utilisent le même emplacement d'inventaire central sur ce serveur. Pour plus d'informations, reportez-vous à la section [Section 3.6.7, « Inscrivez l'emplacement de l'inventaire central Oracle »](#).

Emplacement de Oracle Storage Home

Répertoire d'installation de STA et du logiciel Oracle associé. STA est automatiquement installé dans le sous-répertoire *StorageTek_Tape_Analytics* de cet emplacement ; voir la section [STA Home](#).

Si ce répertoire existe déjà, l'utilisateur du programme d'installation Oracle doit y avoir tous les droits d'accès. Si ce répertoire n'existe pas, le programme d'installation le créera automatiquement si l'utilisateur du programme d'installation Oracle dispose de tous les droits d'accès au répertoire parent.

Remarque:

Ce répertoire peut exister si une version précédente de STA avait été installée sur ce serveur. Si c'est le cas, vous devez vérifier que le groupe d'installation Oracle en est bien propriétaire, et non l'utilisateur *root*.

Cet emplacement doit être distinct des autres répertoires décrits dans cette section. Les instructions et exemples de ce guide utilisent comme emplacement */Oracle* ; remplacez le répertoire que vous avez choisi s'il est différent.

STA Home

Répertoire d'installation de tout le logiciel STA. Le nom *StorageTek_Tape_Analytics* est affecté à ce répertoire, et le programme d'installation de STA le crée automatiquement au sein de [Emplacement de Oracle Storage Home](#).

Les instructions et exemples de ce guide utilisent comme emplacement */Oracle/StorageTek_Tape_Analytics*.

Emplacement du programme d'installation de STA

Répertoire où télécharger le programme d'installation de STA.

Cet emplacement doit être distinct des autres répertoires décrits dans cette section. Les instructions et exemples de ce guide utilisent comme emplacement */Installers* ; remplacez le répertoire que vous avez choisi s'il est différent.

Répertoire de travail du programme d'installation de STA

Par défaut, la décompression du programme d'installation de STA s'effectue sur le répertoire */tmp*, et prend environ 4 Go d'espace. Vous pouvez indiquer un répertoire de travail différent en exécutant le programme d'installation de STA avec l'option suivante :
-J-Djava.io.tmpdir=working_directory

working_directory doit être un chemin absolu. Par exemple :

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

Pour plus d'informations sur cette option, reportez-vous à la section [Annexe B, Programme d'installation et de désinstallation de STA en mode silencieux](#).

Emplacement des journaux STA

Emplacement des journaux STA et MySQL. Les contenus ont tendance à augmenter, et sont gérés par la rotation des journaux. L'emplacement par défaut est */var/log/tbi*, mais vous pouvez le modifier à tout moment après l'installation de STA ; pour obtenir des instructions, reportez-vous à la section [Section 3.6.6, « Déplacement du répertoire des journaux STA \(facultatif\) »](#).

Pour plus d'informations relatives aux exigences d'espace disque, reportez-vous à la section [Section 2.1.2, « Examen de la disposition du système de fichiers STA »](#).

3.2. Conditions requises de nom d'utilisateur et de mot de passe

Les conditions du nom d'utilisateur requises sont les suivantes :

- Il doit comporter entre 1 et 16 caractères.
- Tous les noms d'utilisateur doivent être uniques.

Les conditions requises en termes de mot de passe sont les suivantes :

- Il doit comporter entre 8 et 31 caractères.
- Il doit comporter au moins un chiffre et une majuscule
- Il ne doit pas comporter d'espace
- Il ne doit pas comporter les caractères spéciaux suivants :

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

3.3. Comptes et ports configurés pendant l'installation de STA

Le programme d'installation de STA configure des comptes utilisateurs et des numéros de port selon les spécifications que vous fournissez.

3.3.1. Comptes utilisateurs pour la gestion de STA

Les comptes requis suivants sont créés pendant l'installation de STA. Ces comptes sont spécifiques à STA, et ne sont *pas* des noms d'utilisateur Linux.

- [Comptes WebLogic](#)
- [Comptes de base de données STA](#)

3.3.1.1. Comptes WebLogic

Les comptes WebLogic suivants servent à se connecter à la console d'administration WebLogic ou à l'application STA.

Administration WebLogic

Sert à se connecter à la console d'administration WebLogic pour apporter des modifications à l'environnement WebLogic (par exemple, pour connecter WebLogic à un serveur LDAP ou RACF).

Prudence:

Il est impossible de récupérer le nom d'utilisateur et mot de passe de ce compte. Si ces informations d'identification sont perdues, STA doit être réinstallé.

Administrateur STA

Sert à se connecter à l'application STA avec tous les droits d'accès.

Une fois l'installation de STA terminée, vous pouvez utiliser l'application STA pour créer des comptes utilisateurs supplémentaires, avec des rôles à leur affecter ; pour plus d'informations, reportez-vous au guide *Guide de l'utilisateur STA*.

3.3.1.2. Comptes de base de données STA

Les comptes de la base de données STA sont des comptes MySQL utilisés par STA pour accéder à et gérer la base de données STA.

Utilisateur root de base de données STA

Possède la base de données MySQL et sert à créer l'installation root de la base de données. Le nom d'utilisateur prédéfini est *root*, il est impossible de le modifier.

Prudence:

Il est impossible de récupérer le mot de passe de ce compte.

Utilisateur de l'application de base de données STA

Nom d'utilisateur MySQL défini par l'utilisateur (par exemple, *stadb*) que STA utilise pour se connecter à la base de données. Il est nécessaire de créer, mettre à jour, supprimer et connaître les privilèges des tables de données.

Utilisateur des rapports de base de données STA

Nom d'utilisateur MySQL défini par l'utilisateur (par exemple, *starpt*) que les applications non-STA et les applications tierces peuvent utiliser pour se connecter à la base de données. Il a un accès lecture seule à certaines tables de la base de données.

Administrateur de la base de données STA

Nom d'utilisateur MySQL défini par l'utilisateur (par exemple, *stadb*) que les utilitaires d'administration et de contrôle STA utilisent pour se connecter à la base de données, principalement pour configurer et exécuter les sauvegardes programmées. Il dispose de tous les privilèges DBA, sauf l'option "grant" sur toutes les tables de base de données.

3.3.2. Ports utilisés par STA

STA utilise les ports suivants pour récupérer et recevoir des données. Ces ports sont dédiés et doivent rester disponibles pour STA. Le programme d'installation de STA vérifiera que les ports ne sont pas déjà en cours d'utilisation sur le réseau.

Prudence:

Une fois ces ports configurés pendant l'installation de STA, ils ne peuvent pas être modifiés sans devoir désinstaller et réinstaller STA.

3.3.2.1. Ports externes non configurables

Les ports décrits dans le tableau [Tableau 3.1, « Ports externes non configurables »](#) sont des ports externes servant à la communication entre le serveur STA et d'autres entités réseau. Les valeurs de port sont fixes et ne peuvent pas être modifiées pendant l'installation de STA.

Configuration de pare-feu/routeur : Elle doit être ouverte entre le serveur STA et le serveur de sauvegarde (pour SSH) et entre le serveur STA et les bibliothèques contrôlées (pour SNMP et SNMPTRAP).

Tableau 3.1. Ports externes non configurables

Port	Protocole	Description/Objet
22	SSH	Secure Shell. Sauvegarde de base de données STA ; connexion à la bibliothèque.

Port	Protocole	Description/Objet
161	SNMP	SNMP (Simple Network Management Protocol, Protocole de gestion de réseau simple) Pour la transmission de demandes SNMP.
162	SNMPTRAP	Pour la réception de notifications SNMP (déroutements).

3.3.2.2. Ports externes configurables

Les ports décrits dans le tableau [Tableau 3.2, « Ports externes configurables »](#) sont des ports externes servant à la communication entre le serveur STA et d'autres entités réseau. Ces ports sont les équivalents configurables des ports 80 et 8080 (HTTP) et 443 (HTTPS) standards. Ils doivent être différents d'autres ports HTTP et HTTPS sur le réseau. Contactez votre administrateur réseau pour obtenir de l'aide dans le choix des valeurs.

Configuration de pare-feu/routeur : Elle doit être ouverte entre le serveur STA et le client exécutant l'interface graphique de STA.

Tableau 3.2. Ports externes configurables

Port par défaut	Protocole	Description/Objet
7019	HTTP	Accès à la console d'administration de WebLogic, non sécurisé
7020	HTTPS	Accès à la console d'administration de WebLogic, sécurisé
7021	HTTP	serveur staUi géré. Accès à l'interface graphique de STA, non sécurisé.
7022	HTTPS	serveur staUi géré. Accès à l'interface graphique de STA, sécurisé.

3.3.2.3. Ports internes configurables

Les ports décrits dans le tableau [Tableau 3.3, « Ports internes configurables »](#) servent à la communication interne de STA. Ces valeurs de port doivent être uniques.

Routeur de pare-feu/routeur : Non applicable

Tableau 3.3. Ports internes configurables

Port par défaut	Protocole	Description/Objet
7023	HTTP	serveur staEngine géré. Eléments internes de base de STA, non sécurisé
7024	HTTPS	serveur staEngine géré. Eléments internes de base de STA, sécurisé
7025	HTTP	serveur staAdapter géré. Communication SNMP, non sécurisé.
7026	HTTPS	serveur staAdapter géré. Communication SNMP, sécurisé.

3.4. Journaux d'installation et de désinstallation de STA

Vous pouvez utiliser les journaux d'installation et de désinstallation de STA pour faciliter le dépannage des problèmes. La plupart des noms de fichiers journaux comporte un horodatage

pour faciliter l'identification de l'instance d'installation ou de désinstallation. L'horodatage représente la date et l'heure de démarrage de l'installation ou de la désinstallation.

Les journaux suivants fournissent notamment des informations précieuses en cas d'échec de l'installation ou de la désinstallation. Pour plus d'informations sur leur emplacement, reportez-vous à la section [/STA_logs/install](#).

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

3.4.1. Emplacements des fichiers journaux

L'emplacement des journaux d'installation et de désinstallation de STA varie en fonction de l'état de l'installation ou de la désinstallation. Les journaux sont situés dans les répertoires suivants. Pour plus d'informations sur ces répertoires, reportez-vous à la section [Section 2.1.2, « Examen de la disposition du système de fichiers STA »](#).

/tmp/OraInstalltimestamp

Ce répertoire comporte les journaux des installations ou désinstallations en cours. Ci-dessous un exemple de différents journaux que vous trouverez dans ce répertoire.

```
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

Où *Oracle_storage_home* est l'emplacement de Oracle Storage Home défini pendant l'installation de STA.

Ce répertoire comporte les journaux des installations et des désinstallations qui ont réussi. Certains journaux, comme les journaux d'erreur ou les journaux de patch y sont inclus, le cas échéant.

Ci-dessous un exemple de différents journaux que vous trouverez dans ce répertoire.

```
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

Par défaut, *STA_logs* est situé sous */var/log/tbi*. Vous pouvez éventuellement déplacer ce répertoire vers l'emplacement de votre choix, à tout moment après l'installation de STA. Pour obtenir des instructions, reportez-vous à la section [Section 3.6.6, « Déplacement du répertoire des journaux STA \(facultatif\) »](#).

Ce répertoire comporte les journaux des installations et des désinstallations qui ont réussi ou échoué. Il comporte des journaux relatifs à l'installation du serveur WebLogic et de la base de données MySQL, ainsi que ceux relatifs à l'installation et à la configuration de l'application STA.

Ci-dessous un exemple de différents journaux que vous trouverez dans ce répertoire.

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

3.5. Modes du programme d'installation de STA

Vous pouvez installer STA à l'aide de l'un de ces modes :

Mode graphique

Il s'agit du mode d'installation recommandé. Ce mode fournit une interface graphique pour l'installation de STA et requiert un affichage X11. Pour plus d'informations, reportez-vous à la section [Annexe A, Référence d'écran Programme d'installation et de désinstallation graphique de STA](#).

Mode silencieux

Ce mode vous permet de contourner l'interface graphique et de fournir les options d'installation dans un fichier de propriétés XML appelé *fichier réponse*. Pour plus d'informations, reportez-vous à la section [Annexe B, Programme d'installation et de désinstallation de STA en mode silencieux](#).

Ce mode est utile pour des installations non surveillées et pour installer STA sur plusieurs machines. Grâce au fichier réponse, vous pouvez fournir un seul ensemble de paramètres et automatiser l'installation. Le mode silencieux du programme d'installation peut s'exécuter soit depuis un script, soit depuis la ligne de commande Linux.

3.6. Tâches d'installation de STA

Pour installer STA, effectuez toutes les tâches suivantes, dans l'ordre indiqué.

- [Section 3.6.1, « Identification ou création des informations requises pour l'installation »](#)
- [Section 3.6.2, « Vérification des prérequis d'installation »](#)
- [Section 3.6.3, « Téléchargement de STA »](#)

- [Section 3.6.4, « Installation de STA »](#)
- [Section 3.6.5, « Vérification de la réussite de l'installation. »](#)
- [Section 3.6.6, « Déplacement du répertoire des journaux STA \(facultatif\) »](#)
- [Section 3.6.7, « Inscrivez l'emplacement de l'inventaire central Oracle »](#)

3.6.1. Identification ou création des informations requises pour l'installation

Suivez cette procédure pour identifier et, si nécessaire, créer des utilisateurs et des emplacements pour exécuter le programme d'installation de STA. Vous pouvez utiliser le tableau [Tableau C.2, « Fiche de travail des emplacements et utilisateurs de l'installation »](#) pour enregistrer ces informations. Pour plus d'informations sur ces éléments, reportez-vous à la section [Section 3.1, « Utilisateurs, groupes et emplacements utilisés par le programme d'installation de STA »](#).

1. Connectez-vous en tant qu'utilisateur root Linux.
2. Déterminez s'il existe un fichier de pointeurs d'inventaire central Oracle, */etc/oraInst.loc*, sur le serveur STA. Le fichier sera présent si l'inventaire central Oracle a été précédemment inscrit ; pour plus d'informations, reportez-vous à la section [Emplacement de l'inventaire central Oracle](#).

- Si le fichier existe, enregistrez son contenu. Par exemple :

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

L'entrée *inventory_loc* identifie l'emplacement de l'inventaire central Oracle, et l'entrée *inst_group* identifie le groupe d'installation Oracle.

- Si le fichier est absent, passez à l'étape 3 pour créer les emplacements et utilisateurs nécessaires. Par exemple :

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

3. S'il n'y avait pas de fichier de pointeurs d'inventaire central Oracle lors de l'étape 2, créez le groupe d'installation Oracle. Pour plus d'informations, reportez-vous à la section [Groupe d'installation Oracle](#). Par exemple :

```
# groupadd oinstall
```

4. Obtenez le nom d'utilisateur et le mot de passe d'un utilisateur du programme d'installation Oracle, ou créez-en un nouveau, si nécessaire. Cet utilisateur doit appartenir au groupe d'installation Oracle. Pour plus d'informations, reportez-vous à la section [Utilisateur du programme d'installation Oracle](#). Par exemple :

```
# 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. S'il n'y avait pas de fichier de pointeurs d'inventaire central Oracle lors de l'étape 2, créez l'emplacement de l'inventaire central Oracle. L'utilisateur du programme d'installation Oracle doit être propriétaire de ce répertoire. Pour plus d'informations, reportez-vous à la section [Emplacement de l'inventaire central Oracle](#). Par exemple :

```
# 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. Déterminez l'emplacement de Oracle Storage Home, ou créez-en un s'il n'existe pas déjà. L'utilisateur du programme d'installation Oracle doit être propriétaire de ce répertoire. Pour plus d'informations, reportez-vous à la section [Emplacement de Oracle Storage Home](#). Par exemple :

```
# 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. Déterminez l'emplacement du programme d'installation de STA, ou créez-en un s'il n'existe pas. Pour plus d'informations, reportez-vous à la section [Emplacement du programme d'installation de STA](#). Par exemple :

```
# mkdir /Installers
```

8. Obtenez le mot de passe de l'utilisateur root Linux. Le programme d'installation de STA requiert l'accès root pour effectuer certaines tâches, et vous invitera à saisir ce mot de passe.
9. Choisissez les noms d'utilisateurs de l'administrateur WebLogic, de l'administrateur STA, et des comptes MySQL qui seront créés pendant l'installation. Pour plus d'informations, reportez-vous à la section [Section 3.3.1, « Comptes utilisateurs pour la gestion de STA »](#).
10. Choisissez les numéros des ports internes et externes configurables requis pour les opérations STA. Assurez-vous que les ports externes sont ouverts sur les réseaux

nécessaires. Pour plus d'informations, reportez-vous à la section [Section 3.3.2, « Ports utilisés par STA »](#).

11. Obtenez le nom de domaine de votre site afin de configurer l'agent de diagnostic distant (RDA) de Oracle. Pour plus d'informations, reportez-vous au guide *Guide de l'utilisateur STA*.

3.6.2. Vérification des prérequis d'installation

Suivez cette procédure pour vérifier les prérequis avant d'exécuter le programme d'installation de STA. Cette procédure est facultative, mais si un seul de ces prérequis n'est pas respecté, l'installation de STA échouera. Pour obtenir une liste complète des prérequis à l'installation, reportez-vous au guide *Guide des conditions requises pour l'installation de STA*.

Toutes ces étapes sont réalisées sur le serveur STA. Contactez votre administrateur Linux si vous avez besoin d'aide.

Remarque:

L'installation de STA suppose que Linux 64 bit a été installé avec les packages RPM Linux indiqués dans le chapitre [Chapitre 2, Installation de Linux](#). Si l'un des packages requis n'est pas installé, l'installation de STA échouera. Pour plus d'informations, reportez-vous aux documents suivants :

- Le guide *Guide des conditions requises pour l'installation de STA* pour les versions Linux prises en charge.
 - La section [Section 2.3.6, « Installation des packages Linux requis » \[38\]](#) pour une liste des package requis.
-

Prudence:

Avant de décider de supprimer ou remplacer un logiciel existant de façon permanente, sauvegardez les fichiers si nécessaire.

1. Vérifiez que STA n'est pas installé sur le serveur. Le programme d'installation de STA ne sert qu'aux nouvelles installations. Pour obtenir d'autres instructions, le cas échéant, reportez-vous aux sections suivantes :
 - Si vous souhaitez mettre à niveau STA depuis une version antérieure, reportez-vous à la section [Chapitre 8, Mise à niveau vers STA 2.1.0](#).
 - Si vous devez réinstaller STA ou réparer une installation actuelle, reportez-vous à la section [Chapitre 9, Désinstallation et restauration de STA](#).

L'exemple suivant montre que STA n'est pas installé.

```
$ 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. Vérifiez que MySQL n'est pas installé sur le serveur STA. Si MySQL est installé, le programme d'installation le supprimera, le réinstallera, et toutes les bases de données MySQL existantes seront supprimées.

- Vérifiez que le répertoire `/tmp` dispose d'au moins 4 Go d'espace libre. Il s'agit du répertoire de travail par défaut du programme d'installation de STA.

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

Remarque:

Vous pouvez éventuellement indiquer un répertoire de travail différent lorsque vous lancez le programme d'installation de STA. Pour plus d'informations, reportez-vous à la section [Répertoire de travail du programme d'installation de STA](#).

- Vérifiez que SELinux est désactivé. Si vous avez suivi les instructions de la section " [Tâches de post-Installation](#) ", SELinux doit déjà être désactivé ; pour plus d'informations, reportez-vous à la section [Section 2.3.1, « Désactivation de SELinux » \[34\]](#).

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

- Vérifiez que le pare-feu Linux (IPTables) est arrêté. Si vous avez suivi les instructions de la section " [Tâches de post-Installation](#) ", IPTables doit déjà être arrêté ; pour plus d'informations, reportez-vous à la section [Section 2.3.2, « Désactivation du pare-feu Linux » \[34\]](#).

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

Remarque:

Si votre site requiert l'exécution de IPTables, vous pouvez démarrer ce service après avoir installé STA, configuré les bibliothèques et confirmé que STA contrôle les bibliothèques. Après avoir démarré IPTables, vous devrez à nouveau confirmer que STA contrôle les bibliothèques.

- Arrêtez et annulez la configuration des services SNMP.

Pour éviter les collisions de port réseau et d'autres problèmes, le serveur STA ne doit pas exécuter d'autres services SNMP. Le programme d'installation de STA s'arrêtera dans l'une des situations suivantes :

- Les services de démon `snmpd` et `snmptrapd` sont en cours d'exécution,
- les ports UDP 161 (SNMP) et 162 (SNMPTRAP) ne sont pas disponibles.

Suivez les étapes requises suivantes :

- Affichez l'état actuel des services SNMP `snmpd` et `snmptrapd`.

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

```
snmptrapd is stopped
```

- b. Arrêtez immédiatement les services SNMP si nécessaire.

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

Remarque:

Si vous recevez une erreur "FAILED" avec l'une de ces commandes, les services peuvent déjà s'être arrêtés.

- c. Saisissez les commandes suivantes pour désactiver les services SNMP dans le fichier de configuration des services Linux, de sorte qu'ils ne se lancent pas automatiquement lors de la réinitialisation de Linux :

```
# 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. Passez en revue et vérifiez les conditions minimales applicables selon le mode, comme suit :
- Pour le programme d'installation graphique de STA reportez-vous à la section [Section A.1, « Configuration minimale requise pour l'affichage en mode graphique »](#).
 - Pour le programme d'installation en mode silencieux de STA reportez-vous à la section [Section B.1.1, « Configuration requise du mode silencieux »](#).

3.6.3. Téléchargement de STA

Le téléchargement du programme d'installation de STA comporte les fichiers suivants. *version* est le numéro de version de l'installation de STA.

- *sta_install_version_linux64.bin* : Requis pour toutes les installations.
- *sta_install_version_linux64-2.zip* : Requis pour toutes les installations.
- *silentInstallUtility_version.jar* : Utilitaire de construction du fichier réponse. Uniquement requis si vous utilisez le programme d'installation ou de désinstallation de STA en mode silencieux. Pour plus d'informations, reportez-vous à l'annexe [Annexe B, Programme d'installation et de désinstallation de STA en mode silencieux](#)

1. Dans une fenêtre de navigateur, accédez au site Oracle Software Delivery Cloud à l'adresse suivante :

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

2. Cliquez sur **Sign In/Register**.
3. Saisissez l'ID utilisateur et le mot de passe fournis par le support Oracle ou créez un nouveau compte.
4. A l'écran Terms & Restrictions, sélectionnez les cases à cocher pour indiquer votre accord concernant le contrat de licence et les restrictions d'exportation, puis cliquez sur **Continue**.
5. Effectuez les tâches suivantes à l'écran Media Pack Search :
 - a. Dans le menu **Select a Product Pack**, sélectionnez Oracle StorageTek Products.
 - b. Dans le menu **Platform**, sélectionnez Linux x86-64.
 - c. Cliquez sur **Go**.
6. Dans le tableau Results, sélectionnez **Oracle StorageTek Tape Analytics 2.1.0** et cliquez sur **Continue**.
7. Cliquez sur **Download** pour chaque fichier ZIP de package de média, puis sauvegardez-les dans un emplacement disposant d'au moins 4 Go d'espace libre.
8. Utilisez un outil de décompression pour extraire le contenu des fichiers zip vers l'emplacement du programme d'installation de STA, que vous avez sélectionné dans la section [Section 3.6.1, « Identification ou création des informations requises pour l'installation »](#) (par exemple */Installers*).
9. Assurez-vous que l'utilisateur du programme d'installation Oracle dispose des autorisations d'exécution du fichier *sta_install_version_linux64.bin* et d'accès en lecture au fichier *sta_install_version_linux64-2.zip*. Par exemple :

```
# 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. Passez en revue les notes *Notes de version de STA*, comprises dans le package de téléchargement du programme d'installation.

3.6.4. Installation de STA

Suivez cette procédure pour exécuter le programme d'installation de STA. Vous pouvez installer STA en mode graphique ou silencieux. Pour plus d'informations, reportez-vous à la section [Section 3.5, « Modes du programme d'installation de STA »](#).

1. Dans une fenêtre de terminal, connectez-vous au serveur STA en tant qu'utilisateur du programme d'installation Oracle. Pour plus d'informations, reportez-vous à la section [Utilisateur du programme d'installation Oracle](#).
2. Passez à l'emplacement du programme d'installation de STA pour plus d'informations, reportez-vous à la section [Emplacement du programme d'installation de STA](#). Par exemple :

```
$ cd /Installers
```

3. Lancez le programme d'installation de STA avec l'une des commandes suivantes :
 - Pour le programme d'installation graphique de STA :

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

Où *version* est la version du programme d'installation de STA que vous avez téléchargé. Par exemple :

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

Ce mode requiert un affichage X11. Pour obtenir des instructions, reportez-vous à l'annexe [Annexe A, Référence d'écran Programme d'installation et de désinstallation graphique de STA](#).

- Pour le programme d'installation en mode silencieux de STA :

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

Où :

- *version* est la version du programme d'installation de STA que vous avez téléchargé.
- *response_file* est le chemin absolu du fichier réponse précédemment créé.

Par exemple :

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

Avant d'utiliser ce mode, vous devrez également avoir téléchargé le fichier *silentInstallUtility.jar* et créé un fichier réponse indiquant les options d'installation. Pour plus d'informations, reportez-vous à l'annexe [Annexe B, Programme d'installation et de désinstallation de STA en mode silencieux](#).

3.6.5. Vérification de la réussite de l'installation.

Suivez la procédure suivante pour vérifier que STA est en cours d'exécution.

1. Suivez les étapes suivantes pour vous assurer que le répertoire bin de STA est compris dans la variable *PATH* de l'utilisateur root du système.
 - a. Ouvrez une session de terminal sur le serveur STA actuel et connectez-vous en tant qu'utilisateur root du système.
 - b. Utilisez un éditeur de texte pour ouvrir le profil utilisateur. Par exemple :

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

- c. Ajoutez le répertoire bin de STA à la définition de *PATH*. Par exemple, ajoutez au fichier la ligne suivante :

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

Où *Oracle_storage_home* est l'emplacement de Oracle Storage Home indiqué pendant l'installation de STA installation.

- d. Enregistrez le fichier et fermez-le.
 - e. Déconnectez-vous puis reconnectez-vous en tant qu'utilisateur root du système.
 - f. Confirmez que la variable *PATH* a correctement été mise à jour.

```
# 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. Utilisez la commande *STA* pour vérifier que tous les services STA sont en cours d'exécution et actifs. [Exemple 3.1, « Statut d'installation de STA réussie »](#) est un exemple de statut. Pour plus d'informations, reportez-vous au guide *Guide d'administration de STA*.

Exemple 3.1. Statut d'installation de STA réussie

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

3. Procédez comme suit :

- Si les services STA sont en cours d'exécution et actifs, vous pouvez commencer à configurer les bibliothèques et STA. Pour obtenir des instructions, reportez-vous aux chapitres [Chapitre 5, Configuration de SNMP sur les bibliothèques](#) et [Chapitre 6, Configuration des connexions de bibliothèque dans STA](#).
- En cas de problèmes avec les services STA, vous pouvez passer en revue les journaux d'installation et les journaux STA pour obtenir plus d'informations. Pour connaître leur emplacement, reportez-vous à la section [Section 3.4, « Journaux d'installation et de désinstallation de STA »](#).

3.6.6. Déplacement du répertoire des journaux STA (facultatif)

Ne suivez cette procédure que si vous souhaitez déplacer les journaux STA et MySQL vers un emplacement différent de celui par défaut (`/var/log/tbi`). Après avoir terminé la procédure, les nouveaux journaux seront créés à l'emplacement que vous aurez désigné. Vous pouvez effectuer cette procédure à tout moment une fois STA installé. Pour connaître les conditions minimales d'emplacement, reportez-vous à la section [Section 2.1.2, « Examen de la disposition du système de fichiers STA »](#).

1. Connectez-vous en tant qu'utilisateur root du système.
2. Arrêtez tous les services STA.

```
# STA stop all
Stopping the stau1 service.....
Successfully stopped the stau1 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. Créez le nouveau répertoire de journaux STA que vous souhaitez utiliser pour les journaux STA et MySQL. Par exemple :

```
# 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. Modifiez les droits d'accès au répertoire pour que STA et MySQL puissent y écrire. Par exemple :

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

5. Déplacer le répertoire `/var/log/tbi` actuel vers le répertoire de journaux STA que vous venez de créer.

```
# 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. Créez un lien symbolique depuis votre nouveau répertoire de journaux STA vers l'emplacement par défaut. Par exemple :

```
# 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. Redémarrez STA.

```
# 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. Inscrivez l'emplacement de l'inventaire central Oracle

Suivez cette procédure après l'installation de STA pour enregistrer l'emplacement de l'inventaire central Oracle sur le serveur STA. Vous ne devez suivre qu'une fois cette procédure sur ce serveur.

Cette procédure crée un fichier de pointeurs d'inventaire central Oracle, */etc/oraInst.loc*, ce qui permet à tous les installateurs de Oracle utilisés sur le serveur de connaître l'emplacement de l'inventaire central Oracle et le groupe d'installation Oracle.

1. Connectez-vous comme utilisateur *root* Linux.
2. Passez au répertoire d'inventaire central Oracle. Par exemple :

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

3. Exécutez le script d'enregistrement situé dans ce répertoire.

```
# ./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
#
```

L'emplacement de l'inventaire central Oracle et le groupe d'installation Oracle sont désormais identifiés dans le fichier de pointeurs de l'inventaire central Oracle, */etc/oraInst.loc*.

Configuration des fonctionnalités de bibliothèques pour STA

Pour que les bibliothèques envoient des données SNMP de haute qualité à STA, les fonctionnalités sélectionnées doivent être configurées de façon adéquate. Ces fonctionnalités sont différentes en fonction du modèle de bibliothèque. Terminez les activités de ce chapitre avant de passer au chapitre [Chapitre 5, Configuration de SNMP sur les bibliothèques](#).

Ce chapitre se compose des sections suivantes :

- [Fonctionnalités de bibliothèque impactant les données STA](#)
- [Interfaces utilisateur de la bibliothèque](#)
- [Tâches de configuration de fonctionnalité de bibliothèque](#)

4.1. Fonctionnalités de bibliothèque impactant les données STA

- [Section 4.1.1, « Interface ADI pour lecteurs LTO »](#)
- [Section 4.1.2, « TCP/IP double et Redundant Electronics \(SL3000 et SL8500 uniquement\) »](#)
- [Section 4.1.3, « ID de complexe de bibliothèque \(SL8500 uniquement\) »](#)
- [Section 4.1.4, « Avertissement de nettoyage de lecteur \(SL3000 et SL8500 uniquement\) »](#)
- [Section 4.1.5, « Format de l'étiquette de volume \(SL500 et SL150 uniquement\) »](#)
- [Section 4.1.6, « Option SCSI FastLoad \(SL500 uniquement\) »](#)
- [Section 4.1.7, « Numéros de série de volumes en double »](#)

4.1.1. Interface ADI pour lecteurs LTO

Les bibliothèques modulaires StorageTek prennent en charge les lecteurs LTO (Linear Tape Open) de HP et IBM. Les lecteurs LTO prenant en charge l'interface Automation/Drive Interface (ADI) permettent à STA de fournir à la bibliothèque des données riches (par exemple, performances et utilisation du lecteur) selon la configuration du lecteur et le niveau du microprogramme.

Pour qu'une bibliothèque envoie des données riches du lecteur LTO à STA, l'interface ADI doit être activée sur la bibliothèque comme sur les lecteurs LTO. Si l'interface ADI n'est pas activée sur les deux, la bibliothèque n'enverra que des données de base sur les lecteurs LTO.

Pour connaître les informations sur les niveaux de microprogramme de lecteur requis, reportez-vous au guide *Guide des conditions requises pour l'installation de STA*.

4.1.1.1. Activation de l'interface ADI sur les lecteurs LTO

La méthode d'activation de l'interface ADI varie selon le fabricant et le modèle du lecteur.

- **HP LTO - 3, LTO - 4, LTO - 5 et LTO-6** : ces lecteurs passent automatiquement au mode ADI lorsque l'interface ADI est activée sur la bibliothèque, que la bibliothèque est réinitialisée et que les lecteurs sont réinitialisés. (Les lecteurs peuvent être réinitialisés avec SL Console.)
- **IBM LTO - 3, LTO - 4, LTO - 5 et LTO-6** : ces lecteurs doivent être configurés de façon explicite pour le mode ADI et ne seront pas reconnus jusqu'à ce que l'interface ADI soit activée sur la bibliothèque et que celle-ci soit réinitialisée. Le tableau [Tableau 4.1, « Procédure d'activation de l'interface ADI sur les lecteurs LTO IBM »](#) fournit des informations complémentaires.

Remarque:

La carte-adaptateur Belisarius fournit l'interface à la solution Oracle de chiffrement de bande Oracle Key Manager (OKM). Le microprogramme du lecteur et celui de la carte Belisarius doivent répondre aux conditions requises minimales pour STA.

Tableau 4.1. Procédure d'activation de l'interface ADI sur les lecteurs LTO IBM

Lecteur LTO IBM	LTO - 3	LTO - 4	LTO - 5, LTO-6
IBM sans carte-adaptateur Belisarius	Le support Oracle configure le matériel du lecteur pour le mode ADI.	Le support Oracle configure le matériel du lecteur pour le mode ADI.	NA
IBM avec la carte-adaptateur Belisarius	NA	Le support Oracle configure le matériel du lecteur pour le mode ADI.	Le microprogramme du lecteur doit être configuré pour le mode ADI avec Virtual Operator Panel (VOP). Contactez le support Oracle pour obtenir de l'aide.

4.1.1.2. Activation de l'interface ADI sur la bibliothèque

Par défaut, le mode interface ADI n'est pas activé sur les bibliothèques SL500, SL3000 et SL8500 et vous ou le support Oracle devez l'activer manuellement. L'activation de l'interface ADI nécessitant une réinitialisation de la bibliothèque, vous devez l'activer à l'avance si vous prévoyez d'installer des lecteurs LTO.

Pour les bibliothèques SL3000 et SL8500, vous pouvez uniquement activer le mode ADI si la bibliothèque dispose d'une carte de contrôleur des lecteurs à grande quantité de mémoire (HBT). Pour plus d'informations sur la carte de contrôleur des lecteurs à grande quantité de mémoire (HBT), reportez-vous au guide *Guide des conditions requises pour l'installation de STA*.

4.1.2. TCP/IP double et Redundant Electronics (SL3000 et SL8500 uniquement)

Redundant Electronics et TCP/IP double sont des fonctionnalités facultatives pour les bibliothèques SL3000 et SL8500.

TCP/IP double protège les opérations de bibliothèque/hôte des défaillances réseau en fournissant deux ports TCP/IP de bibliothèque, généralement configurés sur des sous-réseaux distincts. Dans le cas d'interruptions de réseau ou de défaillance sur un sous-réseau, la connexion de la bibliothèque/hôte basculera automatiquement sur l'autre port.

Redundant Electronics permet une protection contre les défaillances matérielles sur le contrôleur de bibliothèque en fournissant deux cartes de contrôleur de bibliothèque distinctes et pleinement fonctionnelles — une active et une en veille. Si le contrôleur actif présente des erreurs importantes, le contrôle de la bibliothèque peut être basculé sur le contrôleur en veille, avec une interruption minimale des opérations de la bibliothèque et de l'hôte.

Pour plus d'informations sur ces fonctionnalités, reportez-vous au *Guide de l'utilisateur* de la bibliothèque.

4.1.2.1. Configuration de la connexion STA pour permettre la prise en charge de ces fonctionnalités

Selon les fonctionnalités activées — TCP/IP double, Redundant Electronics, ou les deux — une bibliothèque SL3000 ou SL8500 peut disposer d'une, de deux, ou de quatre adresses IP. Cependant, STA ne peut maintenir des connexions ininterrompues qu'avec jusqu'à deux adresses IP de bibliothèque à la fois. Ainsi, sur une bibliothèque donnée, vous pouvez configurer STA pour prendre en charge la fonctionnalité TCP/IP double ou Redundant Electronics, mais pas les deux.

Lorsque vous configurez la connexion STA à la bibliothèque, vous devez toujours indiquer une adresse IP principale pour la bibliothèque. Vous pouvez éventuellement indiquer une adresse IP secondaire, selon la configuration des fonctionnalités de la bibliothèque, et de la fonctionnalité que vous souhaitez que voir prise en charge par STA.

Remarque:

Pour les bibliothèques équipées des deux fonctionnalités, Oracle vous recommande de configurer STA de sorte qu'il prenne en charge Redundant Electronics, car cette fonctionnalité est plus importante pour le maintien de la continuité des opérations de la bibliothèque.

Si STA est configuré pour prendre en charge le TCP/IP double, il maintiendra une connexion avec la bibliothèque en cas de basculement de port.

Si STA est configuré pour prendre en charge Redundant Electronics, et en cas de basculement de carte de contrôleur, il maintiendra une connexion avec la bibliothèque via le port indiqué en tant qu'adresse IP secondaire.

Pour plus d'informations sur ces fonctionnalités, reportez-vous au *Guide de l'utilisateur* de la bibliothèque.

Le tableau [Tableau 4.2, « Adresses IP de bibliothèque recommandées pour la connexion STA »](#) présente les adresses IP de bibliothèque recommandées lors de la configuration de la connexion STA à la bibliothèque.

Tableau 4.2. Adresses IP de bibliothèque recommandées pour la connexion STA

Fonctionnalités activées	Adresse IP principale de bibliothèque	Adresse IP secondaire de bibliothèque
Aucune	Port 2B	NA
TCP/IP double uniquement	Port 2B	Port 2B sur la carte active
Redundant Electronics uniquement	Port 2B sur la carte active	Port 2B sur la carte en veille
Les deux	Port 2B sur la carte active	Port 2B sur la carte en veille

4.1.2.2. Eléments supplémentaires à prendre en compte concernant ces fonctionnalités

- Pour configurer STA afin qu'il prenne en charge la fonctionnalité TCP/IP double sur une bibliothèque SL3000 ou SL8500, vous pouvez devoir utiliser un routage de stratégies. Pour plus d'informations, reportez-vous au *Guide de connectivité d'hôte* des bibliothèques SL3000 ou SL8500 . Si vous avez besoin d'aide pour la configuration de la fonctionnalité TCP/IP double, contactez le support Oracle.
- Si une bibliothèque dispose des fonctions Redundant Electronics et TCP/IP double, le sous-réseau du serveur STA doit être distinct du sous-réseau du port de bibliothèque non configuré pour STA (voir [Section 6.1.4, « Configuration de la connexion SNMP à une bibliothèque. »](#)). Dans le cas contraire, la bibliothèque peut tenter d'envoyer des données via ces ports (inconnus pour STA) et ces données seront rejetées par STA.
- Assurez-vous que votre passerelle par défaut est l'interface 2B.

4.1.3. ID de complexe de bibliothèque (SL8500 uniquement)

Pour que STA puisse consolider correctement les données de complexe de bibliothèques, chaque complexe de bibliothèques de votre site doit disposer d'un ID de complexe unique. Sur les bibliothèques SL8500, les ID de complexe sont définis manuellement. Sur tous les autres modèles de bibliothèques, les ID de complexe sont définis automatiquement, et ne requièrent donc pas de vérification ou d'intervention manuelle.

Chaque bibliothèque SL8500 autonome est considérée comme un complexe distinct et doit donc disposer d'un ID de complexe unique. De plus, chaque complexe multibibliothèques doit disposer d'un ID de complexe unique et toutes les bibliothèques du complexe doivent partager le même ID. Les valeurs d'ID de complexe valides sont comprises entre 1 et 127.

Le tableau [Tableau 4.3, « Exemples d'attributions d'ID de complexe »](#) répertorie certains exemples d'attributions d'ID de complexe SL8500 valides.

Tableau 4.3. Exemples d'attributions d'ID de complexe

Type de complexe	Bibliothèques	ID de complexe attribué
Complexe multibibliothèques	SL8500-1	1
	SL8500-2	1

Type de complexe	Bibliothèques	ID de complexe attribué
	SL8500-3	1
Bibliothèques autonomes	SL8500 - 4	2
	SL8500-5	3

Prudence:

La Service Delivery Platform (SDP) d'Oracle utilise également des ID de complexe uniques pour le suivi des données de bibliothèques. Si votre site utilise SDP, contactez le support Oracle avant de modifier un ID de complexe. La modification de l'ID de complexe peut entraîner une défaillance de SDP. Dans la plupart des cas, les ID de complexe sont définis correctement lorsque la SDP est connectée.

Pour obtenir des instructions à ce sujet, reportez-vous à la section [Section 4.3.5, « Vérification de l'ID de complexe de bibliothèque \(SL8500 uniquement\) »](#).

4.1.4. Avertissement de nettoyage de lecteur (SL3000 et SL8500 uniquement)

La marque d'avertissement du nettoyage des lecteurs indique si un avertissement doit être émis lorsqu'un lecteur requiert un nettoyage. Cette marque est définie au niveau de la bibliothèque, de sorte que le même paramètre s'applique à tous les lecteurs d'une bibliothèque.

- Lorsque cette marque est définie sur "on", chaque lecteur affiche un statut d'avertissement d'intégrité lorsqu'un nettoyage est nécessaire. Le statut d'intégrité de niveau supérieur de la bibliothèque sera également dégradé dans le contrôleur STA.
- Lorsque cette marque est définie sur "off", le statut de chaque lecteur n'est pas impacté par un besoin de nettoyage ; le statut d'intégrité de niveau supérieur de la bibliothèque n'est donc pas dégradé dans STA.

Si la bibliothèque contient un grand nombre de lecteurs, il peut être préférable de définir cette marque sur "off" pour que le statut de niveau supérieur de la bibliothèque ne soit pas dégradé lorsque l'un de ces lecteurs nécessite un nettoyage.

Pour obtenir des instructions à ce sujet, reportez-vous à la section [Section 4.3.6, « Définition de l'avertissement de nettoyage de lecteur \(facultatif, SL3000 et SL8500 uniquement\) »](#).

4.1.5. Format de l'étiquette de volume (SL500 et SL150 uniquement)

Les numéros de série de volume (volers) des données SNMP doivent être formatés de façon adaptée pour que STA puisse correctement traiter les données d'échange de bibliothèque. Le numéro de série de volume comprend un suffixe à deux caractères qui indique le type de média. Par exemple, si un volser de cartouche est ABC123L4, "L4" indique que le type de média est LTO4. Afin de permettre la création correcte de rapports STA, le suffixe de volser doit être exclu.

Pour garantir un formatage adapté, il convient de définir les paramètres suivants :

- Pour toutes les bibliothèques SL500 contrôlées par STA, l'orientation d'étiquette pour l'hôte doit être définie sur *Left6* et le mode STA (contrôlé par la marque *staConfig*) doit être définie sur *on*. Le mode STA n'impacte que le format du volser envoyé au serveur STA via SNMP, et non le format utilisé par la bibliothèque SL500.
- Pour toutes les bibliothèques SL150 contrôlées par STA, "Volume Label Format" doit être défini sur *Trim last two characters*.

Prudence:

Si ces paramètres ne sont pas définis correctement, les volsers ne seront pas formatés correctement, entraînant le blocage du traitement des échanges, des tentatives superflues d'obtenir les dernières données de média et l'affichage d'enregistrements de volser à huit caractères irréversibles sur l'écran "Media – Overview" lorsque la préférence "Show Removed Media" est définie.

Pour obtenir des instructions, reportez-vous aux sections [Section 4.3.7, « Définition du format de l'étiquette de volume de la bibliothèque SL500 \(SL500 uniquement\) »](#) et [Section 4.3.8, « Définition du format de l'étiquette de volume de la bibliothèque SL150 et du mode d'adressage de l'élément de lecteur \(SL150 uniquement\) »](#).

4.1.6. Option SCSI FastLoad (SL500 uniquement)

L'option SCSI FastLoad doit être désactivée pour les bibliothèques SL500, car les déroutements de montage de cartouches ne sont pas correctement envoyés à STA lorsque l'option SCSI FastLoad est activée. La fonction FastLoad est désactivée par défaut. Si vous n'êtes pas sûr du statut de cette option, contactez le support Oracle.

4.1.7. Numéros de série de volumes en double

Dans le magasin de données STA, l'historique de médias est conservé par numéro de série de volume (volser). Tout l'historique d'un média donné étant lié à son volser, Oracle vous recommande donc d'éviter d'utiliser des volsers en double. Les volsers doivent être uniques dans toutes les bibliothèques contrôlées. Les volsers en double entraînent un mélange de données entre différents médias.

Pour des informations supplémentaires sur les volsers en double, reportez-vous au guide *Guide de l'utilisateur STA*.

4.2. Interfaces utilisateur de la bibliothèque

Les bibliothèques SL500, SL3000 et SL8500 disposent d'une interface de ligne de commande (CLI) et d'une interface graphique : il s'agit de la console de la bibliothèque StorageTek (SL Console). La bibliothèque SL150 utilise exclusivement une interface utilisateur basée sur un navigateur. Ces interfaces vous serviront à effectuer les procédures décrites dans ce chapitre.

4.2.1. Conseils d'utilisation de la CLI de la bibliothèque

Pour la plupart des commandes de la CLI, la syntaxe est la même pour les modèles de bibliothèques SL500, SL3000 et SL8500. Pour les quelques commandes pour lesquelles la

syntaxe varie selon le modèle de bibliothèque, des exemples vous sont fournis. La plupart des exemples de la CLI utilisent une bibliothèque SL500. Si vous configurez une bibliothèque SL3000 ou SL8500, les détails renvoyés par chaque commande peuvent légèrement varier par rapport à ce qui est présenté dans les exemples. Voici quelques conseils d'utilisation de la CLI de la bibliothèque.

- Utilisez un émulateur de terminal tel que PuTTY pour établir une connexion SSH (Secure Shell) à la CLI de la bibliothèque.
- Activez la journalisation pour pouvoir passer vos activités en revue au cas où vous devriez résoudre des erreurs.
- Avec certaines versions de microprogramme, la CLI arrive à expiration au bout de six heures.
- Pour afficher de l'aide pour toute commande de la CLI, saisissez *help* suivi du nom de la commande (par exemple : *help snmp*).
- Les commandes de la bibliothèque SL500 sont sensibles à la casse, à l'inverse de celle des bibliothèques SL300 et SL8500.
- Pour éviter les erreurs de saisie dans la CLI, vous pouvez tout d'abord saisir une commande dans un fichier texte, puis la copier et la coller dans la CLI. Pour obtenir de l'aide à propos des commandes de la CLI, saisissez *help snmp*.
- Les fonctions suivantes de la CLI permettent de réduire le nombre de frappes :
 - Appuyez sur la touche **Tabulation** pour un traitement automatique des commandes.
 - Appuyez sur les touches **Up - Arrow** et **Down - Arrow** pour faire défiler l'historique de commandes. Modifiez une commande précédemment saisie puis appuyez sur **Enter** pour l'exécuter.
 - Pour corriger une commande avant d'appuyer sur **Enter** pour l'exécuter, utilisez les touches **Left - Arrow** et **Right - Arrow** pour déplacer le curseur sur l'erreur, puis tapez la correction. Les nouveaux caractères s'inscrivent au niveau du curseur ; pour supprimer des caractères, utilisez la touche **Backspace**.

4.2.2. Script de configuration de la bibliothèque (facultatif)

STA fournit un script de configuration de bibliothèque pour vous faciliter la configuration des bibliothèques. Le script vous invite à saisir les paramètres de configuration de la bibliothèque, et selon les valeurs saisies, affiche les commandes complètes que vous pouvez copier et coller dans la CLI de la bibliothèque.

Remarque:

Il est recommandé d'avoir lu et compris les étapes de la configuration de la bibliothèque de ce chapitre avant d'exécuter ce script.

Pour exécuter le script, ouvrez une session de terminal sur le serveur STA et saisissez la commande suivante :

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

où `Oracle_storage_home` est le répertoire où STA et le logiciel Oracle associé sont installés. Pour plus d'informations, reportez-vous à la section [Section 3.1, « Utilisateurs, groupes et emplacements utilisés par le programme d'installation de STA »](#).

Pour plus d'informations sur le script et pour en voir un exemple d'utilisation, exécutez la commande suivante :

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

4.3. Tâches de configuration de fonctionnalité de bibliothèque

Utilisez le tableau [Tableau 4.4, « Tâches de configuration des bibliothèques pour STA »](#) pour déterminer les tâches qui s'appliqueront aux modèles de bibliothèque de votre site. Vous devez effectuer les tâches adéquates à chaque bibliothèque que vous voulez voir contrôlée par STA.

Tableau 4.4. Tâches de configuration des bibliothèques pour STA

Tâche	SL150	SL500	SL3000	SL8500
Section 4.3.1, « Connexion à la bibliothèque »	Oui	Oui	Oui	Oui
Section 4.3.2, « Vérification de la version du microprogramme de la bibliothèque »	Oui	Oui	Oui	Oui
Section 4.3.3, « Vérification de la version de la carte de contrôleur des lecteurs (bibliothèques SL3000 et SL8500 uniquement) »	–	–	Oui	Oui
Section 4.3.4, « Activation de l'interface ADI sur la bibliothèque (toutes les bibliothèques sauf SL150) »	–	Oui	Oui	Oui
Section 4.3.5, « Vérification de l'ID de complexe de bibliothèque (SL8500 uniquement) »	–	–	–	Oui
Section 4.3.6, « Définition de l'avertissement de nettoyage de lecteur (facultatif, SL3000 et SL8500 uniquement) »	–	–	Oui	Oui
Section 4.3.7, « Définition du format de l'étiquette de volume de la bibliothèque SL500 (SL500 uniquement) »	–	Oui	–	–
Section 4.3.8, « Définition du format de l'étiquette de volume de la bibliothèque SL150 et du mode d'adressage de l'élément de lecteur (SL150 uniquement) »	Oui	–	–	–

Remarque:

Pour les bibliothèques SL500, SL3000 et SL8500, de nombreuses tâches vous permettent de choisir l'interface à utiliser entre la CLI ou la SL Console. Pour les bibliothèques SL150, vous ne pouvez utiliser que l'interface utilisateur basée sur le navigateur.

4.3.1. Connexion à la bibliothèque

A l'aide de la CLI de bibliothèque (toutes les bibliothèques sauf SL150)

1. Établissez une connexion SSH à la bibliothèque à l'aide de l'adresse IP ou de l'alias DNS.
2. Connectez-vous à la CLI à l'aide du nom d'utilisateur et du mot de passe `admin`.

Utilisation de la SL Console (toutes les bibliothèques sauf SL150)

1. Démarrez l'application SL Console.

2. Cliquez sur le bouton **About** pour afficher la version actuelle de SL Console et vérifier qu'elle répond aux conditions minimales requises pour le microprogramme de la bibliothèque.
3. Cliquez sur **Close** pour revenir à l'écran Login.
4. Connectez-vous à l'aide du nom d'utilisateur et du mot de passe *admin* et de l'adresse IP de la bibliothèque ou de l'alias DNS.

Pour les bibliothèques SL3000 et SL8500 avec la fonctionnalité Redundant Electronics, vous pouvez uniquement vous connecter au contrôleur actif.

Utilisation de l'interface utilisateur SL150

1. Accédez au nom d'hôte ou à l'adresse IP de la bibliothèque SL150.
2. Connectez-vous à l'aide de votre ID utilisateur et de votre mot de passe. L'ID utilisateur doit avoir le rôle d'administrateur.

4.3.2. Vérification de la version du microprogramme de la bibliothèque

Suivez cette procédure pour vérifier que le microprogramme de la bibliothèque répond aux conditions minimales requises (ou les dépasse) énoncées dans le guide *Guide des conditions requises pour l'installation de STA*. Si les conditions ne sont pas remplies, soumettez une demande d'assistance au support Oracle pour mettre à niveau le microprogramme.

Pour les bibliothèques SL8500, le support Oracle doit enregistrer les paramètres de connexion réseau avant d'effectuer une mise à niveau du microprogramme, car ces paramètres peuvent devoir être à nouveau saisis ou mis à jour après la mise à niveau.

Utilisation de la CLI de bibliothèque (toutes les bibliothèques sauf SL150, sans objet pour les bibliothèques SL3000 inférieures au modèle FRS 4.x)

1. Exécutez la commande suivante :

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

Remarque:

Si le message *SYNTAX ERROR!!* s'affiche, le microprogramme de la bibliothèque est de niveau inférieur. Contactez le support Oracle pour mettre à niveau le microprogramme.

Utilisation de la SL Console (toutes les bibliothèques sauf SL150)

1. Dans le menu **Tools**, sélectionnez **System Detail**.
2. Sélectionnez **Library** dans l'arborescence de navigation.

3. Sélectionnez l'onglet **Properties**, puis l'onglet **Library Controller**.

La version du microprogramme est affichée sous la section Code Version.

Utilisation de l'interface utilisateur SL150

1. Dans l'arborescence de navigation, sélectionnez **Firmware**.

La version du microprogramme est affichée sous la section Library Firmware. Vous pouvez également cliquer sur le bouton **About** dans la barre d'état pour connaître la version du microprogramme.

4.3.3. Vérification de la version de la carte de contrôleur des lecteurs (bibliothèques SL3000 et SL8500 uniquement)

Pour que les bibliothèques SL3000 et SL8500 envoient des données riches à STA, elles doivent disposer d'une carte de contrôleur des lecteurs à grande quantité de mémoire (HBT). Les anciennes bibliothèques (livrées avant mi-2006) sont principalement concernées, les nouvelles étant livrées avec une carte à grande quantité de mémoire. Pour connaître le détail des conditions requises de niveau de microprogramme, reportez-vous au guide *Guide des conditions requises pour l'installation de STA*.

Suivez cette procédure pour vérifier qu'une carte de contrôleur des lecteurs à grande quantité de mémoire (HBT) est installée dans la bibliothèque. Si la bibliothèque ne dispose pas de carte de contrôleur des lecteurs à grande quantité de mémoire (HBT), soumettez une demande d'assistance au support Oracle pour en installer une.

Cette procédure s'effectue par la SL Console. Pour SL8500 FRS 8.x et SL3000 FRS 4.x, vous pouvez également utiliser la commande *config print* de la CLI pour afficher des informations sur la carte HBT.

Cette procédure s'effectue par la SL Console.

1. Dans le menu **Tools**, sélectionnez **System Detail**.
2. Sélectionnez **Library** dans l'arborescence de navigation.
3. Sélectionnez l'onglet **Properties**, puis l'onglet **Drive Controller**.

L'écran affiche des informations concernant la carte de contrôleur des lecteurs (HBT) active.

4. Vérifiez que la valeur de la section High Memory HBT est définie sur *true*.
5. Si vous avez une bibliothèque SL3000 (FRS 4.x) ou SL8500 (FRS 8.x) avec la fonctionnalité Redundant Electronics, développez le dossier Redundant Electronics, puis sélectionnez chaque carte HBT (hbta, hbtb). La valeur de la section High Memory HBT doit être définie sur *True* pour ces deux bibliothèques.

Remarque:

Les cartes HBT active et de veille doivent être installées et capables de communiquer, et doivent toutes deux disposer d'une grande quantité de mémoire.

4.3.4. Activation de l'interface ADI sur la bibliothèque (toutes les bibliothèques sauf SL150)

Si votre bibliothèque comporte des lecteurs LTO, l'interface ADI doit être activée sur les lecteurs comme sur la bibliothèque pour que STA reçoive des données riches. Suivez cette procédure pour vous assurer que l'interface de lecteur ADI est activée sur la bibliothèque. Pour plus d'informations, reportez-vous à la section [Section 4.1.1, « Interface ADI pour lecteurs LTO »](#).

Cette procédure s'effectue par la SL Console.

Pour les bibliothèques SL3000 ou SL8500

1. Affichez le statut de l'interface ADI.

```
drive adiEnable print
```

2. Si "Attributes Adi Status" est défini sur *true*, vous pouvez quitter cette tâche. Si la valeur est *false*, passez à l'étape suivante.
3. Activez l'interface ADI.

```
drive adiEnable on
```

4. Réinitialisez la bibliothèque pour appliquer la modification.

Pour les bibliothèques SL500

1. Affichez le statut de l'interface ADI.

```
enableADI print
```

2. Si "enableADI set to" est défini sur *on*, vous pouvez quitter cette tâche. Si sa valeur est définie sur *off*, passez à l'étape suivante.
3. Activez l'interface ADI.

```
enableADI on
```

4. Réinitialisez la bibliothèque pour appliquer la modification.

4.3.5. Vérification de l'ID de complexe de bibliothèque (SL8500 uniquement)

Pour que STA puisse consolider correctement les données de complexe de bibliothèques, chaque complexe de bibliothèques de votre site doit disposer d'un ID de complexe unique. Suivez cette procédure pour vérifier que l'ID de complexe de bibliothèques est correct pour chaque bibliothèque SL8500. Pour plus d'informations, reportez-vous à la section [Section 4.1.3, « ID de complexe de bibliothèque \(SL8500 uniquement\) »](#).

Cette procédure s'effectue par la SL Console.

1. Pour chaque bibliothèque SL8500 qui sera contrôlée par STA, affichez l'ID de complexe actuellement attribué :

```
SL8500> config complexId print
...
Complex Id 3
...
```

2. Vérifiez que chaque bibliothèque autonome et chaque complexe de bibliothèques possède un ID de complexe unique et que toutes les bibliothèques de chaque complexe de bibliothèques partagent le même ID de complexe.

Si vous devez modifier l'ID de complexe d'une bibliothèque autonome, poursuivez cette procédure.

Prudence:

Si vous devez modifier l'ID de complexe d'une bibliothèque dans un complexe de bibliothèques, contactez le support Oracle. Ne poursuivez pas cette procédure.

3. Déconnectez la bibliothèque, puis patientez jusqu'à ce que toutes les transactions soient terminées.
4. Modifiez l'ID de complexe d'une bibliothèque autonome. *complex_ID* est un nombre compris entre 1 et 127.

```
config complexId set complex_ID
```

Exemple 4.1. Modification de l'ID de complexe de la bibliothèque SL8500

```
SL8500> config complexId set 5
...
Complex Id 5
Success true
Done
...
Note: TCP/IP stack reset may take a few seconds after command completion.
```

Remarque:

Toutes les connexions TCP/IP sont arrêtées lorsque vous exécutez cette commande. Vous pouvez devoir vous reconnecter à la bibliothèque.

4.3.6. Définition de l'avertissement de nettoyage de lecteur (facultatif, SL3000 et SL8500 uniquement)

Suivez cette procédure facultative pour vérifier le paramètre actuel de la marque d'avertissement du nettoyage des lecteurs sur la bibliothèque et modifiez-le, si nécessaire.

Pour plus d'informations, reportez-vous à la section [Section 4.1.4, « Avertissement de nettoyage de lecteur \(SL3000 et SL8500 uniquement\) »](#).

Cette procédure s'effectue par la SL Console.

1. Affichez le paramètre actuel de la marque d'avertissement du nettoyage des lecteurs.

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

2. Si vous souhaitez définir cette marque sur *false* (off), exécutez la commande suivante :

```
cleaning driveWarning set off
```

4.3.7. Définition du format de l'étiquette de volume de la bibliothèque SL500 (SL500 uniquement)

Suivez cette procédure pour vous assurer que les numéros de série de volume (volumes) sont correctement formatés dans les données SNMP envoyées à STA. Pour plus d'informations, reportez-vous à la section [Section 4.1.5, « Format de l'étiquette de volume \(SL500 et SL150 uniquement\) »](#).

Cette procédure s'effectue par la CLI de la bibliothèque SL500.

Remarque:

Oracle vous recommande de suspendre toutes les activités de la bibliothèque avant de modifier ces paramètres. Des applications de bande et/ou des hôtes peuvent nécessiter des modifications de leur configuration après la modification de ces paramètres.

1. Affichez le paramètre actuel de l'indicateur *orientlabel*.

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

2. L'indicateur *host* doit être défini sur *left6*. Pour ce faire, exécutez la commande suivante :

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

3. Affichez à nouveau le paramètre pour vérifier qu'il a été correctement mis à jour.

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

```
Op Panel: (left8) Window left-justified with 8 character label
```

4. Affichez le paramètre actuel de l'indicateur *staConfig*.

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

5. L'indicateur *staConfig* doit être défini sur *on*. Pour ce faire, exécutez la commande suivante :

```
SL500> staConfig on
```

6. Affichez à nouveau le paramètre pour vérifier qu'il a été correctement mis à jour.

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

4.3.8. Définition du format de l'étiquette de volume de la bibliothèque SL150 et du mode d'adressage de l'élément de lecteur (SL150 uniquement)

Suivez cette procédure pour vous assurer que les numéros de série de volume (volsers) sont correctement formatés dans les données SNMP envoyées à STA.

De plus, pour le microprogramme 2.xx et supérieur de SL150 , suivez cette procédure pour définir le mode d'adressage de l'élément du lecteur de sorte que les baies de lecteurs vides soient comprises dans les données envoyées à STA.

Pour plus d'informations, reportez-vous à la section [Section 4.1.5, « Format de l'étiquette de volume \(SL500 et SL150 uniquement\) »](#).

Remarque:

Oracle vous recommande de suspendre toutes les activités de la bibliothèque avant de modifier ces paramètres. Des applications de bande et des hôtes peuvent nécessiter des modifications de la configuration après la modification de ces paramètres.

Cette procédure s'effectue par l'interface basée sur un navigateur de la bibliothèque SL150.

1. Dans l'arborescence de navigation, sélectionnez **Configuration**.
2. Sélectionnez le bouton **Configure**.
3. Dans la fenêtre Configuration Wizard, sélectionnez la case à cocher **Configure Library Settings**, puis cliquez sur **Next**.
4. Définissez les paramètres suivants en conséquence :
 - Mode d'adressage de l'élément de lecteur : **Address All Drive Slots (Recommended)**
 - Format d'étiquetage du volume de bibliothèque : **Trim last two characters (Default)**

Remarque:

Après avoir modifié le mode d'adressage de l'élément de lecteur, vous devez patienter au moins 10 minutes avant de configurer le protocole SNMP dans STA.

5. Cliquez sur **Next**.
6. A l'écran Summary of Configuration Changes, sélectionnez la case à cocher **Accept all changes**, puis cliquez sur **Apply**.
7. A l'écran Apply Configuration Changes, sélectionnez la case à cocher **Set the Library back Online after applying the changes**, puis cliquez sur **OK**.
8. Lorsque le message **All configuration changes have been applied successfully** s'affiche, cliquez sur **Close**.

Configuration de SNMP sur les bibliothèques

Pour que STA contrôle les bibliothèques de votre site, vous devrez effectuer certaines activités de configuration sur les bibliothèques, et d'autres sur le serveur STA. Ce chapitre décrit les activités effectuées sur les bibliothèques. Terminez les activités de ce chapitre avant de passer au chapitre [Chapitre 6, Configuration des connexions de bibliothèque dans STA](#).

Ce chapitre se compose des sections suivantes :

- [Comprendre la configuration SNMP de bibliothèque pour STA](#)
- [Tâches de configuration SNMP sur les bibliothèques](#)

Pour des informations générales sur l'implémentation de SNMP sur les bibliothèques StorageTek, reportez-vous au *Guide de référence SNMP des bibliothèques modulaires StorageTek*.

5.1. Comprendre la configuration SNMP de bibliothèque pour STA

La communication entre STA et les bibliothèques qu'il contrôle se fait via SNMP (Simple Network Management Protocol, Protocole de gestion de réseau simple). Les bibliothèques envoient des données à STA via des dérivements SNMP et STA récupère les données de configuration de la bibliothèque via les fonctions SNMP "get". En termes SNMP, STA est un agent *client* et chaque bibliothèque est un agent *serveur*.

SNMP v3 est le protocole recommandé pour la communication SNMP entre STA et les bibliothèques. Les fonctions d'authentification, de chiffrement et d'intégrité des messages dans le protocole SNMP v3 fournissent un mécanisme sécurisé pour l'envoi de données de bibliothèque. SNMP v3 est également requis pour la fonction de validation de média STA. (La validation de média STA n'est disponible que pour les bibliothèques prises en charges ; pour plus d'informations, reportez-vous au guide *Guide des conditions requises pour l'installation de STA*.)

Ce chapitre décrit la configuration SNMP v3 recommandée. Cependant, selon les conditions requises de votre site, vous pouvez choisir d'utiliser SNMP v2c pour une bibliothèque ou plus. Pour obtenir les instructions de configuration de SNMP v2c, reportez-vous à l'annexe [Annexe F, Configuration du mode SNMP v2c](#).

Remarque:

Tandis que le protocole SNMP v3 est utilisé pour les dérouterments SNMP et les fonctions "get", le protocole de transfert initial de communication entre une bibliothèque et STA s'effectue toujours avec le protocole SNMP v2c.

5.1.1. Configuration du protocole SNMP v3 sur les bibliothèques

Sur chaque bibliothèque, vous configurez la communication SNMP v3 entre STA et chaque bibliothèque en définissant la bibliothèque en tant qu'utilisateur SNMP v3 et le serveur STA en tant que destinataire de dérouterment SNMP v3. De plus, vous devez définir des mécanismes et des mots de passe d'autorisation et de confidentialité. Pour STA, la méthode d'autorisation est toujours SHA (Secure Hash Algorithm) et la méthode de confidentialité est toujours DES (Data Encryption Standard).

5.1.1.1. Utilisateur SNMP v3 unique

STA ne prend en charge qu'un seul utilisateur SNMP v3. Le même utilisateur doit être défini sur toutes les bibliothèques contrôlées par une seule instance STA. Pour trouver une fiche de travail où enregistrer les valeurs que vous utiliserez, reportez-vous à l'annexe [Annexe C, Fiches de travail d'installation et de mise à niveau](#).

Remarque:

Vos bibliothèques peuvent déjà avoir au moins un utilisateur SNMP v3, et vous pouvez l'utiliser pour la communication STA ; Oracle recommande néanmoins de configurer un nouvel utilisateur SNMP v3 unique à cette fin.

Ci-après suivent les valeurs à fournir pour définir l'utilisateur SNMP v3.

SNMP v3 username

Le serveur STA écoute les dérouterments envoyés par cet utilisateur. Il s'agit également du nom du destinataire SNMP v3 utilisé lors de la création des destinataires de dérouterments. Il doit être identique sur toutes les bibliothèques.

SNMP v3 authorization password

Mot de passe d'autorisation que vous pouvez attribuer à l'utilisateur SNMP v3.

Il doit contenir au moins huit caractères ; les virgules, points-virgules ou signes "égal" ne sont pas autorisés.

SNMP v3 privacy encryption password

Mot de passe de confidentialité que vous pouvez attribuer à l'utilisateur SNMP v3.

Il doit contenir au moins huit caractères ; les virgules, points-virgules ou signes "égal" ne sont pas autorisés.

SNMP v2c user community

Chaîne de communauté d'utilisateurs SNMP v2c, généralement définie sur *public*. Cette chaîne est requise pour le protocole de transfert initial entre la bibliothèque et le serveur STA, même lorsque vous utilisez le protocole SNMP v3.

Peut uniquement contenir des caractères alphanumériques (a-z, A-Z, 0-9). Les caractères spéciaux ne sont pas autorisés.

SNMP v2c trap community

Nom de la communauté de déroutement SNMP v2c, uniquement utilisée si SNMP v2c est utilisé pour communiquer avec la bibliothèque. Si vous utilisez SNMP v3, gardez la valeur définie par défaut, à savoir *public*.

Peut uniquement contenir des caractères alphanumériques (a-z, A-Z, 0-9). Les caractères spéciaux ne sont pas autorisés.

5.1.1.2. SNMP Engine IDs

Le protocole SNMP v3 requérant que chaque périphérique SNMP ait un ID de moteur unique, le serveur STA et les bibliothèques ont chacun leur propre ID de moteur. Dans le cas des complexes de bibliothèques SL8500, chaque bibliothèque du complexe dispose également de son propre agent SNMP et donc de son propre ID de moteur unique. L'ID de moteur est composé d'un maximum de 31 caractères hexadécimaux.

Les dérouterments utilisent l'ID de moteur de *l'expéditeur* ; ainsi, vous devez indiquer l'ID de moteur de la *bibliothèque* lorsque vous définissez STA comme destinataire de déroutement SNMP v3.

5.2. Tâches de configuration SNMP sur les bibliothèques

Le tableau [Tableau 5.1, « Tâches de configuration des bibliothèques pour STA »](#) récapitule le processus de configuration des bibliothèques afin qu'elles envoient des données SNMP correctes à STA. Vous devez effectuer les tâches dans l'ordre indiqué à chaque bibliothèque que vous voulez voir contrôlée par STA.

Tableau 5.1. Tâches de configuration des bibliothèques pour STA

Tâche	SL150	SL500	SL3000	SL8500
Section 5.2.1, « Récupération de l'adresse IP de la bibliothèque »	Oui	Oui	Oui	Oui
Section 5.2.2, « Activation du protocole SNMP sur la bibliothèque »	Oui	Oui	Oui	Oui
Section 5.2.3, « Définition d'un utilisateur SNMP v2c »	Oui	Oui	Oui	Oui
Section 5.2.4, « Création d'un utilisateur SNMP v3 »	Oui	Oui	Oui	Oui
Section 5.2.5, « Récupération de l'ID de moteur SNMP de la bibliothèque (toutes les bibliothèques sauf SL150) »	–	Oui	Oui	Oui
Section 5.2.6, « Créez le destinataire de déroutement STA SNMP v3. »	Oui	Oui	Oui	Oui

Remarque:

Ces procédures supposent que vous utilisez le protocole SNMP v3 recommandé pour les communications entre STA et les bibliothèques. Pour plus d'informations, reportez-vous à la section [Section 5.1, « Comprendre la configuration SNMP de bibliothèque pour STA »](#).

Remarque:

Pour les bibliothèques SL500, SL3000 et SL8500, certaines tâches vous permettent de choisir quelle interface utiliser entre la CLI et la SL Console. Pour les bibliothèques SL150, vous ne pouvez utiliser que l'interface utilisateur basée sur le navigateur.

5.2.1. Récupération de l'adresse IP de la bibliothèque

Suivez cette procédure pour récupérer et enregistrer l'adresse IP de la bibliothèque, qui vous servira pour configurer la connexion à la bibliothèque.

Pour les bibliothèques SL3000 et SL8500, choisissez la méthode pour prendre en charge Redundant Electronics, TCP/IP double, ou aucun des deux. Pour plus d'informations, reportez-vous à la section [Section 4.1.2, « TCP/IP double et Redundant Electronics \(SL3000 et SL8500 uniquement\) »](#).

Cette procédure s'effectue à partir de SL Console ou de l'interface basée sur un navigateur SL150.

Adresse IP du modèle SL500

1. Dans le menu **Tools**, sélectionnez **System Detail**.
2. Sélectionnez **Library** dans l'arborescence de navigation.
3. Sélectionnez l'onglet **Properties**, puis l'onglet **General**.

L'adresse IP de la bibliothèque est affichée sous la section Library Interface TCP/IP.

4. Enregistrez l'adresse IP de la bibliothèque en tant qu'adresse IP principale de la bibliothèque. (Cette adresse correspond au port 1B.)

Adresses IP des bibliothèques SL3000 ou SL8500 — Prise en charge de la fonctionnalité Redundant Electronics

- a. Dans le menu **Tools**, sélectionnez **System Detail**.
- b. Sélectionnez le dossier **Redundant Electronics** dans l'arborescence de navigation.

Si ce dossier ne figure pas dans la liste, la fonctionnalité Redundant Electronics n'est pas disponible pour la bibliothèque.

- c. Dans le champ Device State, vérifiez qu'un contrôleur de bibliothèque affiche *Duplex: software ready, switch possible* (il s'agit de la carte active) et que l'autre contrôleur affiche *Standby: software ready* (il s'agit de la carte de secours).

Ces statuts indiquent que les cartes de contrôleur fonctionnent normalement. Si vous ne voyez pas ces statuts, contactez le support Oracle.

- d. Développez le dossier **Redundant Electronics**, puis sélectionnez la carte de contrôleur active.
- e. Enregistrez l'adresse IP du port 2B.

- f. Exécutez à nouveau l'étape **d** et l'étape **e** pour la carte de contrôleur alternative (de secours).

Adresses IP des bibliothèques SL3000 ou SL8500 — Prise en charge de la fonctionnalité TCP/IP double

- a. Dans le menu **Tools**, sélectionnez **System Detail**.
- b. Sélectionnez **Library** dans l'arborescence de navigation.
- c. Sélectionnez l'onglet **Properties**, puis l'onglet **General**.

L'adresse IP est affichée dans les sections Host Interface TCP/IP 2B et Host Interface TCP/IP 2A.

Remarque:

Si la bibliothèque comprend également la fonctionnalité Redundant Electronics, les adresses IP affichées sont valables uniquement pour la carte de contrôleur active.

- d. Enregistrez l'adresse IP principale (section 2B) et l'adresse IP secondaire (section 2A).

Adresses IP des bibliothèques SL3000 ou SL8500 — Aucune fonctionnalité TCP/IP double ou Redundant Electronics

- a. Dans le menu **Tools**, sélectionnez **System Detail**.
- b. Sélectionnez **Library** dans l'arborescence de navigation.
- c. Sélectionnez l'onglet **Properties**, puis l'onglet **General**.

L'adresse IP est affichée dans la section Host Interface TCP/IP 2B. Aucune adresse IP ne figure dans la section 2A.

- d. Enregistrez l'adresse IP en tant qu'adresse IP principale de la bibliothèque.

Adresse IP du modèle SL150

1. Dans l'arborescence de navigation, sélectionnez **Configuration**.

Sélectionnez **Settings** puis **Network**. L'adresse IP de la bibliothèque est affichée dans la section **Network Port 1 Settings**. (La section Network Port 2 Settings est réservée au support technique.)

Remarque:

La valeur du champ Configure IPxx doit être définie sur *Static*. Si ce n'est pas le cas, cliquez sur le bouton **Configure**, puis sélectionnez **Configure Network Settings** pour indiquer une adresse IP statique.

5.2.2. Activation du protocole SNMP sur la bibliothèque

Suivez cette procédure pour activer le protocole SNMP sur le port public de la bibliothèque.

A l'aide de la CLI de la bibliothèque.

1. Utilisez l'une des commandes suivantes, en fonction du modèle de bibliothèque :
 - Pour les bibliothèques SL3000 et SL8500, activez le protocole SNMP sur le port 2B. Si la bibliothèque comprend la fonctionnalité TCP/IP double, cette commande active également le protocole SNMP sur le port 2A.

```
snmp enable port2b
```

- Pour les bibliothèques SL500, activez le protocole SNMP sur le port 1B.

```
snmp enable port1B
```

A l'aide de la SL Console (SL500 uniquement)

1. Dans le menu **Tools**, sélectionnez **System Detail**.
2. Sélectionnez **Library** dans l'arborescence de navigation.
3. Sélectionnez l'onglet **SNMP** puis l'onglet **Port Control**.
4. Remplissez la section Port Control comme suit :

Port: Sélectionnez *Public (1B)*.

Command: Sélectionnez *Enable*.

5. Cliquez sur **Apply**.

A l'aide de l'interface utilisateur SL150

1. Sélectionnez **SNMP** dans l'arborescence de navigation.
2. Si SNMP apparaît comme étant désactivé, sélectionnez **Enable SNMP**.
3. Dans la fenêtre de confirmation, cliquez sur **OK**.

5.2.3. Définition d'un utilisateur SNMP v2c

Un utilisateur SNMP v2c est nécessaire pour le protocole de transfert initial entre la bibliothèque et le serveur STA. Cet utilisateur est également nécessaire si vous souhaitez utiliser SNMP v2c pour la communication de STA. Pour plus d'informations, reportez-vous à la section [Section 5.1, « Comprendre la configuration SNMP de bibliothèque pour STA »](#).

Notez les configurations requises suivantes :

- Il doit exister un seul utilisateur SNMP v2c sur la bibliothèque.
- La chaîne de communauté SNMP v2c ne peut comporter que des caractères alphanumériques (a–z, A–Z, 0–9). Les caractères spéciaux ne sont pas autorisés.
- Un utilisateur SNMP v2c existant est généralement défini pour la communauté *public*, mais peut être défini dans un autre nom de communauté.

- Vous ne devez pas supprimer un utilisateur SNMP v2c *public* existant sans consulter Oracle Service. Dans certains cas, un utilisateur SNMP v2c *public* est nécessaire pour la Service Delivery Platform (SDP) d'Oracle.

A l'aide de la CLI de bibliothèque (toutes les bibliothèques sauf SL150)

1. Déterminez si un utilisateur SNMP v2c existe déjà.

```
snmp listUsers
```

2. Si un utilisateur SNMP v2c est déjà défini, comme dans l'exemple suivant, vous pouvez quitter cette tâche. Si ce n'est pas le cas, passez à l'étape suivante.

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

3. Ajout d'un utilisateur SNMP v2c

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

Où *community_name* est *public*, ou autre. Par exemple :

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

4. Dressez à nouveau la liste des utilisateurs SNMP pour vérifier que l'utilisateur SNMP v2c a été correctement ajouté.

```
snmp listUsers
```

A l'aide de la SL Console (SL500 uniquement)

1. Dans le menu **Tools**, sélectionnez **System Detail**.
2. Sélectionnez **Library** dans l'arborescence de navigation.
3. Sélectionnez l'onglet **SNMP**, puis l'onglet **Add Users**.
4. Si un utilisateur SNMP v2c existe déjà dans la section Users, vous pouvez quitter cette tâche. Si ce n'est pas le cas, passez à l'étape suivante.
5. Pour ajouter l'utilisateur SNMP v2c, remplissez les champs de l'onglet **Add Users** comme suit :
 - *Version* : Sélectionnez *v2c*.

- *Community* : indiquez une chaîne de communauté (*public*, par exemple).
6. Cliquez sur **Apply**.

Par défaut, la bibliothèque SL150 est fournie sans utilisateur SNMP v2c défini. Si vous souhaitez utiliser SNMP v2c pour la communication de STA, créez un utilisateur SNMP v2c comme suit :

A l'aide de l'interface utilisateur SL150

1. Sélectionnez **SNMP** dans l'arborescence de navigation.
2. Sous la section (ou l'onglet) SNMP Users, sélectionnez **Add SNMP User**.
3. A l'écran Add SNMP User, renseignez les informations comme suit :

Version : Sélectionnez *v2c*.

Community Name : indiquez une chaîne de communauté (*public*, par exemple).

4. Cliquez sur **OK**.

5.2.4. Création d'un utilisateur SNMP v3

Toutes les données des dérouterments SNMP et de la MIB (base d'informations de gestion) sont envoyées au serveur STA via l'utilisateur SNMP v3. Conservez le nom d'utilisateur et les mots de passe que vous indiquez, car ils vous seront utiles lorsque vous définirez un destinataire de dérouterment SNMP v3.

Notez les configurations requises suivantes :

- La méthode d'autorisation doit être *SHA* (Secure Hash Algorithm) et la méthode de confidentialité doit être *DES* (Data Encryption Standard).
- Toutes les bibliothèques contrôlées par une seule instance STA doivent posséder le même nom d'utilisateur SNMP v3. Nous vous recommandons de créer un nouvel utilisateur unique pour cette procédure.
- Les mots de passe d'autorisation et de confidentialité doivent contenir au moins huit caractères ; les virgules, points-virgules, ou signes "égal" ne sont pas autorisés.

A l'aide de la CLI de bibliothèque (toutes les bibliothèques sauf SL150)

1. Création d'un utilisateur SNMP 3 :

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

Où :

- *name* est le nom de l'utilisateur SNMP v3
- *auth_password* et *priv_password* sont les mots de passe d'autorisation et de confidentialité.

Remarque:

Pour les bibliothèques SL3000 et SL8500, mettez toutes les variables entre guillemets simples (Exemple 5.1, « Création d'un utilisateur SNMP v3 sur la bibliothèque SL3000 ou SL8500 »).

Exemple 5.1. Création d'un utilisateur SNMP v3 sur la bibliothèque SL3000 ou SL8500

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

Exemple 5.2. Création d'un utilisateur SNMP v3 sur la bibliothèque SL500

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

2. Dressez à nouveau la liste des utilisateurs SNMP pour vérifier que l'utilisateur SNMP v3 a été correctement ajouté.

```
snmp listUsers
```

A l'aide de la SL Console (SL500 uniquement)

1. Dans le menu **Tools**, sélectionnez **System Detail**.
2. Sélectionnez **Library** dans l'arborescence de navigation.
3. Sélectionnez l'onglet **SNMP**, puis l'onglet **Add Users**.
4. Remplissez les champs de l'onglet **Add Users** comme suit :
 - *Version* : Sélectionnez *v3*.
 - *UserName* : nom de l'utilisateur SNMP v3.
 - *Auth*: Sélectionnez *SHA*.
 - *AuthPass* : indiquez un mot de passe d'autorisation.
 - *Priv* : Sélectionnez *DES*.
 - *PrivPass* : indiquez un mot de passe de confidentialité.
5. Cliquez sur **Apply**.

A l'aide de l'interface utilisateur SL150

1. Sélectionnez **SNMP** dans l'arborescence de navigation.
2. Dans la section SNMP Users, sélectionnez **Add SNMP User**.
3. Pour le champ Version, sélectionnez *v3*, puis renseignez les informations comme suit :
 - *User Name* : nom de l'utilisateur SNMP v3.
 - *Authentication Protocol* : Sélectionnez *SHA*.
 - *Authentication Passphrase* : indiquez un mot de passe d'autorisation.

- *Privacy Protocol* : Sélectionnez *DES*.
 - *Privacy Passphrase* : indiquez un mot de passe de confidentialité.
4. Cliquez sur **OK**.

5.2.5. Récupération de l'ID de moteur SNMP de la bibliothèque (toutes les bibliothèques sauf SL150)

Suivez cette procédure pour afficher l'ID de moteur SNMP de la bibliothèque (par exemple, 0x81031f88804b7e542f49701753).

Cette procédure s'effectue par la SL Console.

1. Utilisez l'une des commandes suivantes, en fonction du modèle de bibliothèque :
 - Pour les bibliothèques SL3000 et SL8500 :

```
snmp engineId print
```
 - Pour les bibliothèques SL500 :

```
snmp engineId
```
2. Enregistrez l'ID de moteur dans un fichier texte pour pouvoir l'utiliser dans les tâches de configuration SNMP ultérieures.

5.2.6. Créez le destinataire de déROUTement STA SNMP v3.

Suivez cette procédure pour définir le serveur STA en tant que destinataire autorisé des déROUTements SNMP et pour définir les déROUTements que la bibliothèque enverra.

Notez les configurations requises suivantes :

- Pour éviter les enregistrements dupliqués, ne définissez pas le serveur STA comme destinataire de déROUTement pour plusieurs instances. Par exemple, ne créez pas de définition de destinataire de déROUTement SNMP v3 et SNMP v2c pour le serveur STA.
- Les niveaux de déROUTement 13 (déROUTement de test) et 14 (déROUTement d'intégrité) sont des nouveautés de STA 2.0.x. Il est possible que le niveau de déROUTement 4 ne soit pas pris en charge par des versions antérieures du microprogramme de la bibliothèque ; il est cependant possible de le spécifier lors de la création d'un destinataire de déROUTement.

A l'aide de la CLI de bibliothèque (toutes les bibliothèques sauf SL150)

1. Créez un destinataire de déROUTement SNMP v3. Séparez les niveaux de déROUTement par des virgules.

```
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
```

Où :

- *STA_server_IP* est l'adresse IP du serveur STA.
- *recipient_name* est le nom de l'utilisateur SNMP créé dans la section [Section 5.2.4, « Création d'un utilisateur SNMP v3 »](#) [84].
- *auth_password* et *priv_password* sont les mots de passe d'autorisation et de confidentialité créés dans la section [Section 5.2.4, « Création d'un utilisateur SNMP v3 »](#) [84].
- *library_engineID* est l'ID de moteur de bibliothèque visualisé dans la section [Section 5.2.5, « Récupération de l'ID de moteur SNMP de la bibliothèque \(toutes les bibliothèques sauf SL150\) »](#) [86], comprenant le préfixe 0x.

Remarque:

Pour les bibliothèques SL3000 et SL8500, mettez les variables *recipient_name*, *auth_password*, et *priv_password* entre guillemets simples ([Exemple 5.3, « Création du destinataire de détournement SNMP v3 sur les bibliothèques SL3000 ou SL8500 »](#)).

Exemple 5.3. Création du destinataire de détournement SNMP v3 sur les bibliothèques SL3000 ou SL8500

```
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
```

Exemple 5.4. Création du destinataire de détournement SNMP v3 sur la bibliothèque SL500

```
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. Répertoriez les destinataires de détournement et vérifiez que le destinataire a été correctement ajouté.

```
snmp listTrapRecipients
```

A l'aide de la SL Console (SL500 uniquement)

1. Dans le menu **Tools**, sélectionnez **System Detail**.
2. Sélectionnez **Library** dans l'arborescence de navigation.
3. Sélectionnez l'onglet **SNMP**, puis l'onglet **Add Trap Recipients**.
4. Remplissez les champs de l'écran Trap Recipients comme suit :

- *Host* : adresse IP du serveur STA.
 - *TrapLevel* : liste de niveaux de déROUTement séparés par des virgules que la bibliothèque doit envoyer à STA : 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
 - *Version* : Sélectionnez *v3*.
 - *TrapUserName* : Nom de l'utilisateur SNMP créé dans la section [Section 5.2.4, « Création d'un utilisateur SNMP v3 » \[84\]](#).
 - *Auth* : Sélectionnez *SHA*.
 - *AuthPass* : Mot de passe d'autorisation créé dans la section [Section 5.2.4, « Création d'un utilisateur SNMP v3 » \[84\]](#).
 - *Priv* : Sélectionnez *DES*.
 - *PrivPass* : Mot de passe de confidentialité créé dans la section [Section 5.2.4, « Création d'un utilisateur SNMP v3 » \[84\]](#).
 - *EngineID* : ID de moteur de bibliothèque affiché dans la section [Section 5.2.5, « Récupération de l'ID de moteur SNMP de la bibliothèque \(toutes les bibliothèques sauf SL150\) » \[86\]](#). Ne saisissez pas le préfixe 0x.
5. Cliquez sur **Apply**.

A l'aide de l'interface utilisateur SL150

1. Sélectionnez **SNMP** dans l'arborescence de navigation.
2. Dans la section SNMP Trap Recipients, sélectionnez **Add Trap Recipient**.
3. Remplissez les champs comme suit :
 - *Host Address* : Adresse IP du serveur STA.
 - *Trap Level* : Liste de niveaux de déROUTement séparés par des virgules que la bibliothèque doit envoyer à STA : 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
 - *Version* : Sélectionnez *v3*.
 - *Trap User Name* : Nom de l'utilisateur SNMP créé dans la section [Section 5.2.4, « Création d'un utilisateur SNMP v3 » \[84\]](#).
 - *Authentication Protocol* : Sélectionnez *SHA*.
 - *Authentication Passphrase* : Mot de passe d'autorisation créé dans la section [Section 5.2.4, « Création d'un utilisateur SNMP v3 » \[84\]](#).
 - *Privacy Protocol* : Sélectionnez *DES*.
 - *Privacy Passphrase* : Mot de passe de confidentialité créé dans la section [Section 5.2.4, « Création d'un utilisateur SNMP v3 » \[84\]](#).
 - *Engine ID* : Ce champ sera rempli automatiquement. Ne modifiez pas sa valeur.
4. Cliquez sur **OK**.

Configuration des connexions de bibliothèque dans STA

Pour que STA contrôle les bibliothèques de votre site, vous devrez effectuer certaines activités de configuration sur les bibliothèques, et d'autres sur le serveur STA. Ce chapitre décrit les activités effectuées sur le serveur STA.

Ce chapitre se compose de la section suivante :

- [Tâches de configuration de STA](#)

6.1. Tâches de configuration de STA

Effectuez les procédures dans l'ordre indiqué. Une fois ce processus terminé, STA peut commencer la surveillance des bibliothèques et les analyses.

- [Section 6.1.1, « Connexion à STA »](#)
- [Section 6.1.2, « Vérifiez la communication SNMP avec une bibliothèque »](#)
- [Section 6.1.3, « Configuration des paramètres client SNMP pour STA »](#)
- [Section 6.1.4, « Configuration de la connexion SNMP à une bibliothèque. »](#)
- [Section 6.1.5, « Test d'une connexion SNMP de bibliothèque »](#)
- [Section 6.1.6, « Exécution d'une collecte de données manuelle »](#)

6.1.1. Connexion à STA

Suivez cette procédure pour vous connecter à STA afin d'effectuer les autres procédures de cette section. Pour obtenir les instructions complètes, reportez-vous au guide *Guide de l'utilisateur STA*.

1. Lancez un navigateur Web pris en charge sur votre ordinateur et saisissez l'URL de l'application STA.

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

Où :

- *host_name* est le nom d'hôte du serveur STA.
- *port_number* est le numéro de port STA que vous avez indiqué pendant l'installation. Par défaut, le port HTTP est 7021, et le port HTTPS est 7022.

- *STA* doit être saisi en majuscules.

Par exemple :

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

2. A l'écran Login, saisissez le nom et le mot de passe de l'administrateur STA.

6.1.2. Vérifiez la communication SNMP avec une bibliothèque

Suivez cette procédure pour confirmer que la connexion SNMP entre le serveur STA et une bibliothèque est opérationnelle.

Cette procédure vérifie que les ports UDP 161 et 162 sont activés sur tous les noeuds de réseau entre le serveur STA et la bibliothèque. Elle ne permet pas de valider le fait qu'un destinataire de déroulement SNMP v3 a été correctement spécifié.

Effectuez cette procédure pour chaque bibliothèque contrôlée. Pour les bibliothèques SL3000 ou SL8500 prenant en charge Redundant Electronics ou TCP/IP double, effectuez cette procédure deux fois : une fois pour l'adresse IP principale de la bibliothèque, et une fois pour l'adresse IP secondaire.

Remarque:

Cette procédure s'effectue à partir de la ligne de commande système sur le serveur STA.

1. Ouvrez une session de terminal sur le serveur STA et connectez-vous en tant qu'utilisateur root du système.
2. Testez la connexion SNMP v3. Les valeurs que vous indiquez doivent correspondre aux valeurs associées dans la bibliothèque.

```
# 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
```

Où :

- *v3* indique SNMP v3
- *SNMP_user* est le nom d'utilisateur SNMP v3.
- *SHA* indique le protocole d'authentification.
- *auth_pwd* est le mot de passe d'autorisation.
- *DES* indique le protocole de confidentialité.
- *priv_pwd* est le mot de passe de confidentialité.
- *authPriv* indique que la confidentialité est exécutée sur la commande.
- *library_IP_addr* est l'adresse IP du port public sur la bibliothèque.
 - Pour les bibliothèques SL150, il s'agit du port réseau 1.
 - Pour les bibliothèques SL500, il s'agit du port 1B.

- Pour les bibliothèques SL3000 et SL8500, il peut y avoir plusieurs ports à tester, si les fonctionnalités TCP/IP double et/ou Redundant Electronics sont activées sur la bibliothèque. S'il y a plusieurs ports, exécutez cette commande pour chaque adresse IP.
- `1.3.6.1.4.1.1211.1.15.3.1.0` : l'identificateur d'objet (OID) SNMP pour la bibliothèque, identique pour tous les modèles de bibliothèques.

Si la sortie de la commande affiche le modèle de bibliothèque, le test a réussi. Voici quelques exemples de commande :

Exemple 6.1. Commande snmpget réussie

```
# 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"
```

Exemple 6.2. Echec de la commande snmpget — Temporisation réseau

```
# 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.
```

Exemple 6.3. Echec de la commande snmpget — Mot de passe incorrect

```
# 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. Testez la connexion SNMP v2c.

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

Où :

- `v2c` indique SNMP v2c.
 - `public` indique la chaîne de communauté.
 - `authPriv` indique que la confidentialité est exécutée sur la commande.
 - `library_IP_addr` est l'adresse IP du port public sur la bibliothèque.
4. Si les deux tests de connexion SNMP sont couronnés de succès, vous pouvez quitter cette procédure. Si l'un des tests échoue, passez à l'étape suivante pour résoudre les problèmes réseau soupçonnés, le cas échéant.
 5. Confirmez le routage du paquet depuis le serveur STA vers la bibliothèque.

```
# traceroute -I library_IP_addr
```

Où :

- - *I* ("i" majuscule) indique qu'il faut utiliser les paquets de requêtes d'écho Internet Control Message Protocol (ICMP) à la place des datagrammes User Datagram Protocol (UDP).
- *library_IP_addr* est l'adresse IP du port public sur la bibliothèque.

La sortie montre le nombre de sauts et la durée d'un aller-retour pour atteindre chaque saut. La durée d'un aller-retour (la dernière ligne de la sortie de commande) doit être de moins d'une seconde. Si ce n'est pas le cas, vérifiez la performance du réseau auprès de votre administrateur réseau.

6. Surveillez les paquets TCP/IP envoyés entre le serveur STA et la bibliothèque.

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

Où :

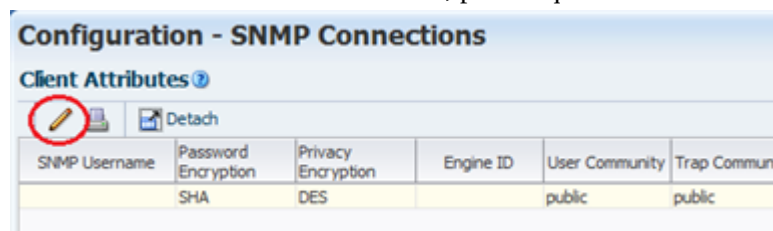
- - *v* indique une sortie détaillée.
- *host* indique qu'il faut collecter les paquets provenant de ou allant vers l'hôte indiqué uniquement (dans le cas présent, la bibliothèque).
- *library_IP_addr* est l'adresse IP du port public sur la bibliothèque.
- *file_name* est le nom du fichier où sauvegarder la sortie.

6.1.3. Configuration des paramètres client SNMP pour STA

Suivez cette procédure pour ajouter ou modifier des paramètres client SNMP pour STA. Ces paramètres configurent STA pour recevoir les données SNMP d'au moins une bibliothèque.

Il n'existe qu'une seule entrée de client SNMP pour chaque instance STA sur votre site.

1. Sous l'onglet **Setup & Administration**, sélectionnez **Configuration**, puis **SNMP Connections**.
2. Procédez comme suit :
 - Pour configurer les paramètres du client pour la première fois, sélectionnez la ligne vide dans le tableau Client Attributes, puis cliquez sur **Edit**.



- Pour modifier les paramètres du client existants, sélectionnez l'entrée dans le tableau Client Attributes, puis cliquez sur **Edit**



La boîte de dialogue Define SNMP Client Settings s'affiche. Dans le cas d'une nouvelle configuration, les champs sont vides.

3. Renseignez la boîte de dialogue comme suit. Les valeurs que vous indiquez doivent correspondre aux valeurs associées dans les bibliothèques.

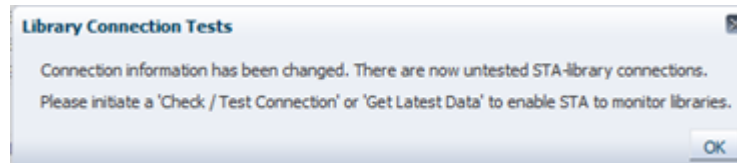
Remarque:

Même si STA contrôle uniquement des bibliothèques configurées pour la communication SNMP v2c, vous devez remplir tous les champs, y compris ceux applicables à SNMP v3. Vous ne pouvez laisser aucun champ vide.

- *STA SNMP Connection Username (Auth)* : Saisissez le nom d'utilisateur SNMP v3.
- *Enter STA SNMP Connection Password (Auth)* : Saisissez le mot de passe d'autorisation de connexion.
- *Enter Privacy Encryption Password (Privacy)* : Saisissez le mot de passe de chiffrement de confidentialité.
- *User Community* : Ce champ est obligatoire pour le protocole de transfert SNMP avec la bibliothèque, ou, si vous utilisez le protocole SNMP v2c, pour la communication de STA avec la bibliothèque. Saisissez le nom de la communauté indiqué sur la bibliothèque. La valeur par défaut est *public*.
- *Trap Community* : Cette option est uniquement utilisée si le protocole SNMP v2c est employé pour la communication avec la bibliothèque. Si vous utilisez SNMP v3, gardez la valeur définie par défaut, à savoir *public*. Si vous utilisez SNMP v2c, saisissez le nom de communauté de déroutement spécifié dans la bibliothèque.

4. Cliquez sur **Save**.

L'enregistrement de configuration est mis à jour et un message s'affiche, indiquant que vous devriez effectuer un test de connexion de bibliothèque pour établir ou rétablir le protocole de communication SNMP avec les bibliothèques.



5. Cliquez sur **OK** pour fermer le message.

6.1.4. Configuration de la connexion SNMP à une bibliothèque.

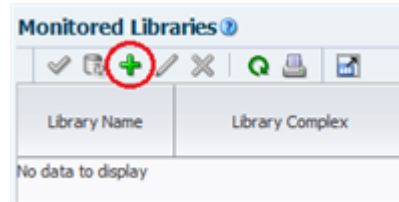
Suivez cette procédure pour configurer une connexion SNMP dans chaque bibliothèque que STA doit contrôler ou pour modifier une connexion existante. Pour les connexions existantes, vous *devez* effectuer cette procédure si des modifications ont été apportées à l'un des paramètres de configuration SNMP sur une bibliothèque contrôlée, par exemple la modification de l'adresse IP de la bibliothèque.

Remarque:

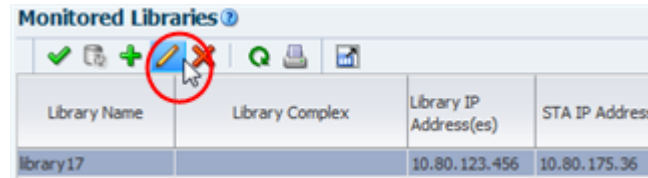
Si vous configurez plusieurs connexions de bibliothèques à la fois, pour réduire les perturbations dans les bibliothèques, effectuez cette procédure pour toutes les bibliothèques avant de tester les connexions SNMP.

1. Sous l'onglet **Setup & Administration**, sélectionnez **Configuration**, puis **SNMP Connections**.
2. Procédez comme suit :

- Pour configurer la connexion à une bibliothèque pour la première fois, cliquez sur **Add** dans la barre d'outils Monitored Libraries.



- Pour modifier une connexion de bibliothèque existante, sélectionnez la bibliothèque dans le tableau Monitored Libraries, puis cliquez sur **Edit**.



La boîte de dialogue Define Library Connection Details s'affiche. Dans le cas d'une nouvelle connexion de bibliothèque, les champs sont vides.

3. Renseignez la boîte de dialogue comme suit. Les valeurs que vous indiquez doivent correspondre aux valeurs associées dans la bibliothèque.
 - *Library Name* : Saisissez un nom pour identifier la bibliothèque dans les écrans de l'interface utilisateur STA (par exemple, le nom d'hôte de la bibliothèque).
 - *Library Primary IP Address* : Saisissez l'adresse IP du port public principal de la bibliothèque. Vous ne pouvez pas indiquer l'adresse IP d'une autre bibliothèque contrôlée.
 - *Library Secondary IP Address* : S'applique uniquement aux bibliothèques SL3000 et SL8500 utilisant TCP/IP double ou Redundant Electronics. Indiquez l'adresse IP du port public secondaire de la bibliothèque. Vous ne pouvez pas indiquer l'adresse IP d'une autre bibliothèque contrôlée. Laissez le champ vide pour toutes les autres bibliothèques, y compris pour les bibliothèques SL500 et SL150.
 - *STA IP Address* : Sélectionnez l'adresse IP du serveur STA.
 - *Library Engine ID* : Ne modifiez pas ce champ. Il s'agit de l'ID de moteur SNMP unique de la bibliothèque, qui est fourni automatiquement lorsque la connexion initiale entre STA et la bibliothèque est établie. Il est vide pour les nouvelles connexions.
 - *Automated Daily Data Refresh* : Indiquez l'heure à laquelle vous souhaitez que STA collecte les dernières données de configuration de la bibliothèque. Les données seront collectées automatiquement toutes les 24 heures à l'heure indiquée. Il est recommandé de choisir une heure où la bibliothèque est généralement moins utilisée. La valeur par défaut est 00:00 (minuit). Utilisez le format de 24 heures.

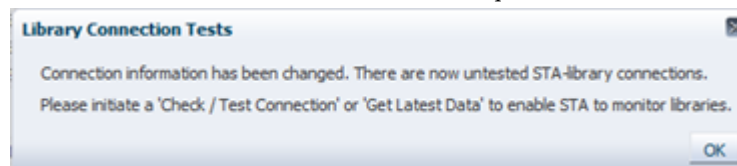
Prudence:

Si vous laissez ce champ vide, les collections automatiques et planifiées des données de bibliothèque seront désactivées. Les données de configuration de la bibliothèque STA ne seront plus synchronisées avec la bibliothèque.

- *Library Time Zone* : Sélectionnez le fuseau horaire local de la bibliothèque.

4. Cliquez sur **Save**.

L'enregistrement de configuration est mis à jour et un message s'affiche, indiquant que vous devriez effectuer un test de connexion de bibliothèque pour établir ou rétablir le protocole de communication SNMP avec les bibliothèques.



5. Cliquez sur **OK** pour fermer le message.

Dans le cas où vous avez modifié une connexion de bibliothèque, le champ Library Engine ID du tableau Monitored Libraries sera vide, indiquant que la connexion SNMP a été perdue.

6.1.5. Test d'une connexion SNMP de bibliothèque

Suivez cette procédure pour tester la connexion SNMP entre STA et une bibliothèque, et pour établir ou rétablir le protocole de communication. Pour éviter la perte de connexion et de dérouterments SNMP, vous devez effectuer cette procédure pour chaque bibliothèque contrôlée, à chaque fois que vous ajoutez ou modifiez des paramètres de configuration SNMP pour la bibliothèque ou le client STA.

Vous ne pouvez tester qu'une connexion de bibliothèque à la fois.

Remarque:

Un test de connexion pouvant entraîner une perte temporaire des paquets SNMP entrants, il est recommandé d'exécuter cette procédure uniquement si nécessaire.

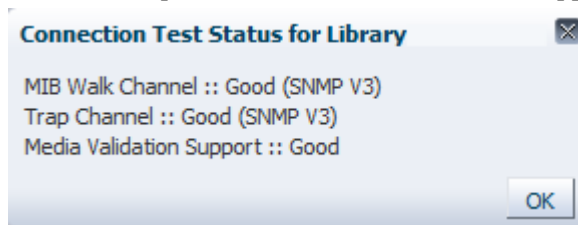
Remarque:

Avant d'effectuer cette procédure, vous pouvez souhaiter vérifier que la bibliothèque est opérationnelle.

1. Sous l'onglet **Setup & Administration**, sélectionnez **Configuration**, puis **SNMP Connections**.
2. Dans le tableau **Monitored Libraries**, sélectionnez une bibliothèque puis cliquez sur **Check / Test Connection**.

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	0x80001f88043537313030303230303030	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

Le message **Connection Test Status** s'affiche, indiquant les résultats des tests MIB Walk Channel, Trap Channel et Media Validation Support.



3. Cliquez sur **OK** pour fermer le message.

Le tableau **Monitored Libraries** est mis à jour avec les résultats du test.

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	0x80001f880431303030303030303031	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

- Si le champ *Library Complex* est vide, il sera renseigné après l'exécution d'une collecte de données manuelle.
- Le champ *Library Engine ID* indique l'ID de moteur SNMP unique pour la bibliothèque.
- Le champ *Last Connection Attempt* indique la date et l'heure de lancement du test de connexion.
- Le champ *Last Successful Connection* indique la date et l'heure de fin du test, si celui-ci a réussi.
- Le champ *Last Connection Status* indique les résultats du test. En cas d'échec du test, STA fournit des informations dans le champ *Last Connection Failure Detail*. (Vous serez peut-être amené à agrandir la colonne pour voir la valeur en entier.)

Remarque:

Si le test échoue à cause d'une temporisation, répétez cette procédure à un moment où l'activité de la bibliothèque est moindre. Une fois que vous avez effectué le test, vous pouvez comparer les horodatages pour vous assurer que la bibliothèque fournit des informations actuelles.

6.1.6. Exécution d'une collecte de données manuelle

Suivez cette procédure pour lancer une collecte de données manuelle pour une bibliothèque et obtenir les données de configuration de bibliothèque les plus récentes. Si cette procédure se termine avec succès, STA commence à contrôler la bibliothèque et à effectuer l'analyse des données.

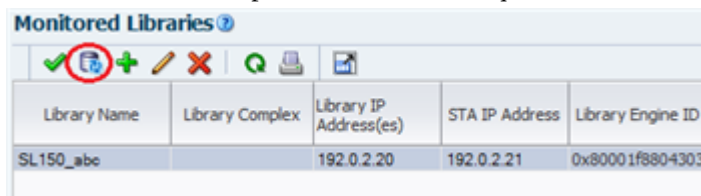
Même si STA effectue automatiquement une collecte de données toutes les 24 heures, à l'heure planifiée, vous devez effectuer une collecte de données manuelle pour chaque bibliothèque contrôlée à chaque fois que vous ajoutez ou modifiez des paramètres de configuration SNMP pour la bibliothèque ou le client STA.

En fonction de la taille de la bibliothèque, la collecte de données peut durer de plusieurs minutes à une heure.

Remarque:

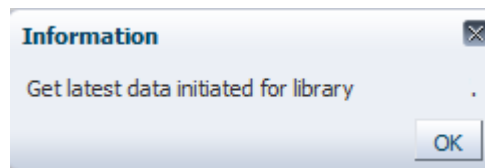
Vous pouvez exécuter plusieurs collectes de données simultanément, mais vous devez les initier une à une. Répétez cette procédure autant de fois que nécessaire, en sélectionnant une bibliothèque différente à chaque fois.

1. Sous l'onglet **Setup & Administration**, sélectionnez **Configuration**, puis **SNMP Connections**.
2. Sélectionnez une bibliothèque dans le tableau **Monitored Libraries** puis cliquez sur **Get latest data**. Vous ne pouvez sélectionner qu'une seule bibliothèque à la fois.



Library Name	Library Complex	Library IP Address(es)	STA IP Address	Library Engine ID
SL150_abc		192.0.2.20	192.0.2.21	0x80001f8804303f

Un message de confirmation s'affiche.



3. Cliquez sur **OK** pour fermer le message.

La collecte des données se poursuit et le tableau **Monitored Libraries** est mis à jour avec les résultats.

- Le champ *Library Complex* indique l'ID du complexe de bibliothèques.
- Le champ *Library Engine ID* indique l'ID de moteur SNMP unique pour la bibliothèque.
- Le champ *Last Connection Attempt* indique la date et l'heure de lancement de la collecte de données.
- Le champ *Last Successful Connection* indique la date et l'heure de fin de la collecte de données, si celle-ci a réussi.
- Le champ *Last Connection Status* est mis à jour comme suit :
 - *IN PROGRESS* : le processus de collection des données est en cours.
 - *SUCCESS* : la collecte de données a réussi. STA commence à recevoir les données d'échange de la bibliothèque.
 - *FAILED* : la collecte de données a échoué. Si possible, STA fournit des informations dans le champ *Last Connection Failure Detail*. (Vous serez peut-être amené à agrandir la colonne pour voir la valeur en entier.)

Remarque:

Le statut est mis à jour toutes les quatre minutes et l'intervalle d'actualisation de l'écran par défaut est de 480 secondes. Vous pouvez cependant cliquer sur le bouton **Refresh Table** pour forcer une actualisation du tableau.



-
- Le champ *Recent SNMP Trap Communication Status* peut parfois indiquer *MISSED HEARTBEAT*. C'est tout à fait normal.

Configuration des services STA

Configurez les utilitaires de service STA Backup et STA Resource Monitor.

Ce chapitre se compose des sections suivantes :

- [Présentation des services STA](#)
- [Tâches de configuration des services STA](#)

7.1. Présentation des services STA

- Service de sauvegarde de base de données STA : Vous pouvez configurer le service de sauvegarde STA avec son utilitaire d'administration, *staservadm*. Pour afficher la liste complète des options de commande de l'utilitaire, saisissez *staservadm -h*. Pour plus d'informations, reportez-vous au guide *Guide d'administration de STA*.
- Service du contrôleur de ressources STA : Vous pouvez configurer le service du contrôleur de ressources STA avec son utilitaire d'administration, *staresmonadm*. Pour afficher la liste complète des options de commande de l'utilitaire, saisissez *staresmonadm -h* dans la ligne de commande. Pour plus d'informations, reportez-vous au guide *Guide d'administration de STA*.

Ces utilitaires de service sont situés dans le répertoire */Oracle_storage_home/StorageTek_Tape_Analytics/common/bin*. Pour plus d'informations sur Oracle Storage Home, reportez-vous à la section [Section 3.1, « Utilisateurs, groupes et emplacements utilisés par le programme d'installation de STA »](#).

7.2. Tâches de configuration des services STA

Tâches générales

- [Section 7.2.1, « Mise à jour du chemin de système \(facultatif\) »](#)
- [Section 7.2.2, « Redémarrage du démon de services STA \(facultatif\) »](#)
- [Section 7.2.3, « Vérification de la connectivité de la bibliothèque »](#)

Tâches de configuration de sauvegarde de la base de données STA

- [Section 7.2.4, « Passez en revue les préférences de l'utilitaire de sauvegarde de la base de données STA. »](#)
- [Section 7.2.5, « Configuration du serveur de sauvegarde de base de données distant »](#)
- [Section 7.2.6, « Configuration du service de sauvegarde de la base de données STA »](#)

Tâches de configuration du contrôleur de ressources STA

- [Section 7.2.7, « Examen des préférences de l'utilitaire du contrôleur de ressources STA »](#)
- [Section 7.2.8, « Configuration du contrôleur de ressources STA »](#)

7.2.1. Mise à jour du chemin de système (facultatif)

Suivez cette procédure pour vous assurer que le répertoire bin de STA est compris dans la variable *PATH* de l'utilisateur root du système. Le répertoire bin comporte les utilitaires de service STA, *staservadm* et *staresmonadm*.

- a. Ouvrez une session de terminal sur le serveur STA actuel et connectez-vous en tant qu'utilisateur root du système.
- b. Utilisez un éditeur de texte pour ouvrir le profil utilisateur. Par exemple :

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

- c. Ajoutez le répertoire bin de STA à la définition de *PATH*. Par exemple, ajoutez au fichier la ligne suivante :

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

Où *Oracle_storage_home* est l'emplacement de Oracle Storage Home indiqué pendant l'installation de STA installation.

- d. Enregistrez le fichier et fermez-le.
- e. Déconnectez-vous puis reconnectez-vous en tant qu'utilisateur root du système.
- f. Confirmez que la variable *PATH* a correctement été mise à jour.

```
# 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. Redémarrage du démon de services STA (facultatif)

Suivez cette procédure pour redémarrer le démon de services STA, *staservd*.

Cette procédure vous sera utile si vous avez modifié les paramètres de configuration des services de sauvegarde STA ou du contrôleur de ressources STA et que vous souhaitez que les nouveaux paramètres soient appliqués immédiatement. Si vous ne suivez pas cette procédure, les nouveaux paramètres seront appliqués dès que le service sortira de l'intervalle de mise en sommeil et qu'il les traitera.

1. Arrêtez le démon des services STA.

```
# STA stop staservd
```

2. Démarrez le démon des services STA.

```
# STA start staservd
```

- Affichez le statut du démon pour confirmer qu'il est en cours d'exécution.

```
# STA status staservd
```

7.2.3. Vérification de la connectivité de la bibliothèque

Lorsque vous avez terminé la configuration des services, confirmez que toutes les bibliothèques configurées ont terminé leurs requêtes de récupération des données les plus récentes (le dernier statut de connexion doit indiquer *SUCCESS*, et STA doit recevoir des données d'échange des bibliothèques). Pour plus d'informations, reportez-vous au guide *Guide de l'utilisateur STA*.

7.2.4. Passez en revue les préférences de l'utilitaire de sauvegarde de la base de données STA.

Consultez le tableau [Tableau 7.1, « Attributs de l'utilitaire d'administration du service de sauvegarde STA \(staservadm\) »](#) pour obtenir les descriptions des paramètres de préférences disponibles et pour définir vos préférences.

Tableau 7.1. Attributs de l'utilitaire d'administration du service de sauvegarde STA (staservadm)

Option	Attribut	Description	Valeur par défaut	Votre valeur
-S, --scp -F, --ftp	Type de transfert de fichiers	Méthode de transfert de fichiers utilisée pour copier les fichiers de sauvegarde STA vers l'hôte de sauvegarde. Les options possibles sont SCP (recommandé) ou FTP.	SCP	
-T, --time	Heure du vidage complet de la sauvegarde	Heure de la journée où STA effectue un vidage complet de la sauvegarde de la base de données. Le vidage est effectué automatiquement toutes les 24 heures aux environs de cette heure. L'heure réelle dépasse parfois cette heure de quelques secondes dans "l'intervalle de mise en sommeil". Le format utilisé est <i>hh:mm</i> , au format 24 heures.	00:00	
-i, --int	Intervalle de mise en sommeil	Nombre de secondes pendant lesquelles le démon de services STA patiente avant de rechercher des nouveaux fichiers de sauvegarde incrémentiels.	300	
-s, --server	Nom d'hôte de sauvegarde	Adresse IPv4 ou IPv6 ou nom d'hôte DNS complet de l'hôte du serveur vers lequel le serveur STA copie ses fichiers de sauvegarde.	NA	
-u, --usr	ID de l'utilisateur de sauvegarde	ID d'utilisateur système autorisé à effectuer des transferts de fichiers SCP vers l'hôte de sauvegarde.	NA	
-p, --pwd	Mot de passe de sauvegarde	Mot de passe attribué à l'utilisateur de sauvegarde.	NA	
-d, --dir	Répertoire de sauvegarde	Répertoire sur l'hôte de sauvegarde dans lequel les fichiers de sauvegarde seront copiés.	NA	

Option	Attribut	Description	Valeur par défaut	Votre valeur
<code>-U, --dbusr</code>	Nom d'utilisateur de la base de données	Nom d'utilisateur de la base de données autorisé à exécuter la commande <code>mysqldump</code> . Vous devez indiquer le nom d'utilisateur du compte DBA de la base de données STA.	NA	
<code>-P, --dbpwd</code>	Mot de passe de la base de données	Mot de passe du nom d'utilisateur de la base de données.	NA	

7.2.5. Configuration du serveur de sauvegarde de base de données distant

Suivez cette procédure pour configurer un serveur de sauvegarde distant (ou équivalent) de façon à ce qu'il reçoive les fichiers de sauvegarde compressés générés par le service de sauvegarde de base de données STA. STA vous recommande de configurer un serveur de sauvegarde distant.

L'espace requis peut varier : la taille doit être un multiple de la taille utilisée pour la sauvegarde locale de la base de données STA, qui dépend du nombre de copies à conserver. L'espace de stockage du serveur de sauvegarde doit être mis en miroir ou entrelacé.

1. Connectez-vous en tant qu'utilisateur root du système au serveur de sauvegarde.
2. Créez un nouveau groupe pour l'utilisateur de sauvegarde STA. Par exemple :

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

Dans cet exemple, l'ID de groupe est "stabckgr" et l'option `-g` est utilisée pour indiquer un GID numérique.

3. Créez l'utilisateur de sauvegarde STA. Par exemple :

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

Dans cet exemple, l'ID utilisateur est "stabck" et les options suivantes sont utilisées :

- `-c` : Commentaire.
- `-m` : Création d'un répertoire de base pour l'utilisateur.
- `-d` : Chemin absolu du répertoire de base.
- `-g` : Attribution de l'utilisateur au groupe indiqué.
- `-s` : Attribution du shell de connexion indiqué à l'utilisateur.
- `-u` : Attribution du numéro d'identification utilisateur (UID) indiqué à l'utilisateur.

4. Attribuez un mot de passe à l'utilisateur de sauvegarde STA. Par exemple :

```
# passwd stabck
Changing password for user stabck.
```



```
New UNIX password: bckpwd1
Retype new UNIX password: bckpwd1
passwd: all authentication tokens updated successfully.
```

5. Créez le répertoire dans lequel les sauvegardes STA seront copiées. Par exemple :

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

Dans cet exemple, le répertoire "STAbackups" est créé dans le répertoire de base de l'utilisateur de sauvegarde STA, et l'option `-p` est utilisée pour créer des répertoires parents, si nécessaire.

6. Affichez les attributs de l'utilisateur pour confirmer que toutes les informations ont été saisies correctement. Par exemple :

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

7. Attribuez la propriété exclusive et des droits d'accès pour le répertoire à l'utilisateur et au groupe de sauvegardes STA. Par exemple :

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

Dans cet exemple, l'option `-R` est utilisée pour attribuer de façon récursive les attributs au répertoire et à ses fichiers.

8. Vérifiez le répertoire pour confirmer que toutes les informations ont été correctement saisies. Par exemple :

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

7.2.6. Configuration du service de sauvegarde de la base de données STA

Suivez cette procédure pour configurer le service de sauvegarde de la base de données STA. Il est possible de désigner un répertoire où les fichiers de sauvegarde seront copiés. Oracle vous recommande de le placer sur un serveur de sauvegarde distant.

Vos paramètres de connexion prennent effet dès que le service sort de l'intervalle de mise en sommeil et traite de nouveaux paramètres ou lorsque vous redémarrez manuellement le démon de services STA (voir la section [Section 7.2.2, « Redémarrage du démon de services STA \(facultatif\) »](#)).

1. Connectez-vous en tant qu'utilisateur root du système au serveur STA.
2. Affichez les paramètres actuels du service de sauvegarde STA à l'aide de la commande `staservadm -Q`.

Cet exemple montre que le service n'est pas encore configuré et n'effectue donc pas de sauvegarde.

```
# ./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. Servez-vous du tableau [Tableau 7.1, « Attributs de l'utilitaire d'administration du service de sauvegarde STA \(staservadm\) »](#) pour définir les valeurs d'attribut à l'aide de la commande `staservadm`.

Vous pouvez définir les attributs avec des commandes distinctes ou les combiner en une seule commande. Par exemple :

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

L'utilitaire définit chaque valeur contenue dans votre commande, puis affiche tous les paramètres actuels. Par exemple :

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

```

4. Consultez la sortie de la commande pour vérifier que les valeurs ont été définies correctement.

7.2.7. Examen des préférences de l'utilitaire du contrôleur de ressources STA

Consultez la description des options dans le tableau [Tableau 7.2, « Attributs du contrôleur de ressources STA \(staresmonadm\) »](#) et définissez vos paramètres. La valeur par défaut "-1" indique que l'attribut n'est pas configuré.

Tableau 7.2. Attributs du contrôleur de ressources STA (staresmonadm)

Option	Attribut	Description	Valeur par défaut	Votre valeur
<code>-T, --time</code>	Heure du rapport quotidien	Heure de la journée où STA envoie un rapport quotidien standard. Le rapport est envoyé automatiquement toutes les 24 heures aux environs de cette heure. L'heure réelle dépasse parfois cette heure de quelques secondes dans "l'intervalle de mise en sommeil". Le format utilisé est <i>hh:mm</i> , au format 24 heures.	00:00	
<code>-i, interval</code>	Intervalle de mise en sommeil	Nombre de secondes pendant lesquelles le contrôleur de ressources STA patiente entre les analyses.	300	
<code>-n, --nag</code>	Mode Répétition	Indique la fréquence des alertes STA si des limites supérieures (HWM) sont atteintes. Si ce mode est défini sur "on", STA envoie des e-mails d'alerte à chaque analyse du système. S'il est défini sur "off", les alertes sont simplement signalées dans le rapport quotidien standard.	Off	
<code>-U, --dbusr</code>	Nom d'utilisateur de la base de données	Nom d'utilisateur de la base de données autorisé à effectuer des requêtes dans les tableaux "information_schema" et dans les variables	NA	

Option	Attribut	Description	Valeur par défaut	Votre valeur
		globales du système interne du serveur MySQL. Vous devez indiquer le nom d'utilisateur du compte DBA de la base de données STA ou le nom d'utilisateur de compte root de la base de données STA (<i>root</i>).		
<i>-P, --dbpwd</i>	Mot de passe de la base de données	Mot de passe attribué au nom d'utilisateur de la base de données.	NA	
<i>-t, --tblsphwm</i>	HWM de tablespace de base de données	Limite supérieure du tablespace de la base de données, saisie sous forme de pourcentage de la valeur maximale disponible.	-1	
<i>-b, --backvolhwm</i>	HWM de sauvegarde locale	Limite supérieure du volume des sauvegardes locales de la base de données STA (<i>/sta_db_backup</i>), saisie sous forme de pourcentage de la valeur maximale disponible.	-1	
<i>-d, --dbvolhwm</i>	HWM du volume de disque de la base de données	Limite supérieure du volume de la base de données STA (<i>/sta_db/mysql</i>), saisie sous forme de pourcentage de la valeur maximale disponible.	-1	
<i>-l, --logvolhwm</i>	HWM du volume de disque de journalisation	Limite supérieure des journaux de la base de données STA (<i>/sta_db/mysql</i>), saisie sous forme de pourcentage de la valeur maximale disponible.	-1	
<i>-z, --rootvolhwm</i>	HWM du volume root	Limite supérieure du volume root (<i>/</i>), saisie sous forme de pourcentage de la valeur maximale disponible.	-1	
<i>-x, --tmpvolhwm</i>	HWM du volume Tmp	Limite supérieure du volume de répertoire temporaire (<i>/tmp</i>), saisie sous forme de pourcentage de la valeur maximale disponible.	-1	
<i>-m, --memhwm</i>	HWM de la mémoire physique (RAM)	Limite supérieure de la mémoire système totale (à l'exception de la mémoire virtuelle), saisie sous forme de pourcentage de la valeur maximale disponible.	-1	
<i>-f, --from</i>	Expéditeur de l'e-mail	Nom ou adresse e-mail qui s'affiche dans le champ "From" de l'e-mail de rapport quotidien standard.	<i>StaResMon@localhost</i>	
<i>-r, --recips</i>	Destinataires d'e-mail	Adresses e-mail des destinataires, saisies sous forme de liste de valeurs séparées par des virgules.	NA	
<i>-s, --subject</i>	Objet de l'e-mail	Saisie qui s'affiche dans le champ "Subject" de l'e-mail de rapport quotidien standard, pouvant contenir jusqu'à 128 caractères. Utilisez des guillemets s'il contient des espaces. Un horodatage au format <i>aaaa-mm-jj hh:mm:ss</i> sera ajouté à votre saisie lors de l'envoi de l'e-mail.	Rapport du contrôleur de ressources STA	
<i>-o, --outfile</i>	Fichiers de données de sortie	Chemin absolu du fichier de données de sortie séparé par des virgules (CSV).	<i>/STA_logs/db/staresmon.csv</i>	Par exemple :

Option	Attribut	Description	Valeur par défaut	Votre valeur
			<code>/var/log/tbi/db/ staresmon.csv</code>	

7.2.8. Configuration du contrôleur de ressources STA

Suivez cette procédure pour configurer le service du contrôleur de ressources STA. Vos paramètres de connexion prennent effet dès que le service sort de l'intervalle de mise en sommeil et traite de nouveaux paramètres ou lorsque vous redémarrez manuellement le démon de services STA (voir la section [Section 7.2.2, « Redémarrage du démon de services STA \(facultatif\) »](#)).

1. Connectez-vous en tant qu'utilisateur root du système au serveur STA.
2. Affichez les paramètres actuels du contrôleur de ressources STA à l'aide de la commande `staresmonadm -Q`.

Cet exemple montre que le service n'est pas configuré et n'effectue donc pas d'analyse.

```
# ./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. Servez-vous du tableau [Tableau 7.2, « Attributs du contrôleur de ressources STA \(staresmonadm\) »](#) pour définir les valeurs d'attribut à l'aide de la commande `staresmonadm`.

Vous pouvez définir les attributs avec des commandes distinctes ou les combiner en une seule commande. Par exemple :

```
# ./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
```

L'utilitaire définit chaque valeur contenue dans votre commande, puis affiche tous les paramètres actuels. Par exemple :

```
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. Consultez la sortie de la commande pour vérifier que les valeurs ont été définies correctement.

Mise à niveau vers STA 2.1.0

Ce chapitre fournit les instructions de mise à niveau de toute version précédente de STA vers STA 2.1.0. Il contient les sections suivantes :

- [Présentation du processus de mise à niveau](#)
- [Chemins de mise à niveau STA 2.1.0 valides](#)
- [Méthodes de mise à niveau](#)
- [Modifications d'environnement pour STA 2.1.0](#)
- [Tâches de préparation de la mise à niveau](#)
- [Tâches de mise à niveau](#)

S'il s'agit d'une première installation de STA, vous devez effectuer une nouvelle installation de base, reportez-vous à au chapitre [Chapitre 3, Installation de STA](#) pour connaître les instructions.

L'annexe [Annexe C, Fiches de travail d'installation et de mise à niveau](#) comporte des fiches à utiliser pour organiser vos activités de mise à niveau et enregistrer vos paramètres.

8.1. Présentation du processus de mise à niveau

Pendant une mise à niveau, vos données STA existantes sont transformées de la version STA actuelle en données de la nouvelle version. Votre base de données STA n'est pas valide avec la nouvelle version de STA jusqu'à ce que ces transformations soient effectuées. Après la mise à niveau, STA traitera de nouvelles données en fonction du nouveau schéma et des nouvelles règles d'analyse ; les données d'historique ne sont pas à nouveau traitées.

Avant de commencer la mise à niveau, lisez toutes les instructions de ce chapitre, et assurez-vous de disposer de suffisamment de temps pour effectuer le processus dans son entier. Certaines tâches de préparation de mise à niveau peuvent demander une coordination avec d'autres groupes de votre site, tel que l'administration réseau. Toutes les tâches de préparation doivent être effectuées à l'avance, afin de terminer la mise à niveau aussi rapidement que possible.

Une fois le processus de mise à niveau commencé, STA ne peut pas être en cours d'exécution, et ne reçoit donc pas les informations d'échange des bibliothèques contrôlées. En outre, la nouvelle version de STA ne commence pas à recevoir d'informations des bibliothèques avant que vous n'ayez terminé toutes les étapes de la mise à niveau et testé la connexion SNMP vers chaque bibliothèque contrôlée.

Remarque:

Certaines étapes de la mise à niveau comportent des estimations de temps, qui ne sont fournies qu'à des fins de planification. Selon les capacités de votre serveur — nombre de CPU, vitesse CPU, vitesse des disques, mémoire et espace de swap disponible — ces durées peuvent varier.

8.2. Chemins de mise à niveau STA 2.1.0 valides

Vous pouvez mettre à niveau vers STA 2.1.0 depuis toutes les versions STA suivantes :

- 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

Remarque:

Si vous effectuez une mise à niveau de STA 1.0.x, vous devez également installer une nouvelle version de Linux avant d'installer STA 2.1.0. Pour plus d'informations, reportez-vous au guide *Guide des conditions requises pour l'installation de STA*.

8.3. Méthodes de mise à niveau

Selon vos buts et vos ressources disponibles, vous pouvez effectuer la mise à niveau de STA avec un ou deux serveurs. Les tâches de mise à niveau sont principalement communes aux deux méthodes, mais leur ordre d'exécution diffère. Ces deux méthodes sont décrites dans les sections suivantes :

- [Section 8.3.1, « Méthode de mise à niveau à serveur unique »](#)
- [Section 8.3.2, « Méthode de mise à niveau à deux serveurs »](#)

8.3.1. Méthode de mise à niveau à serveur unique

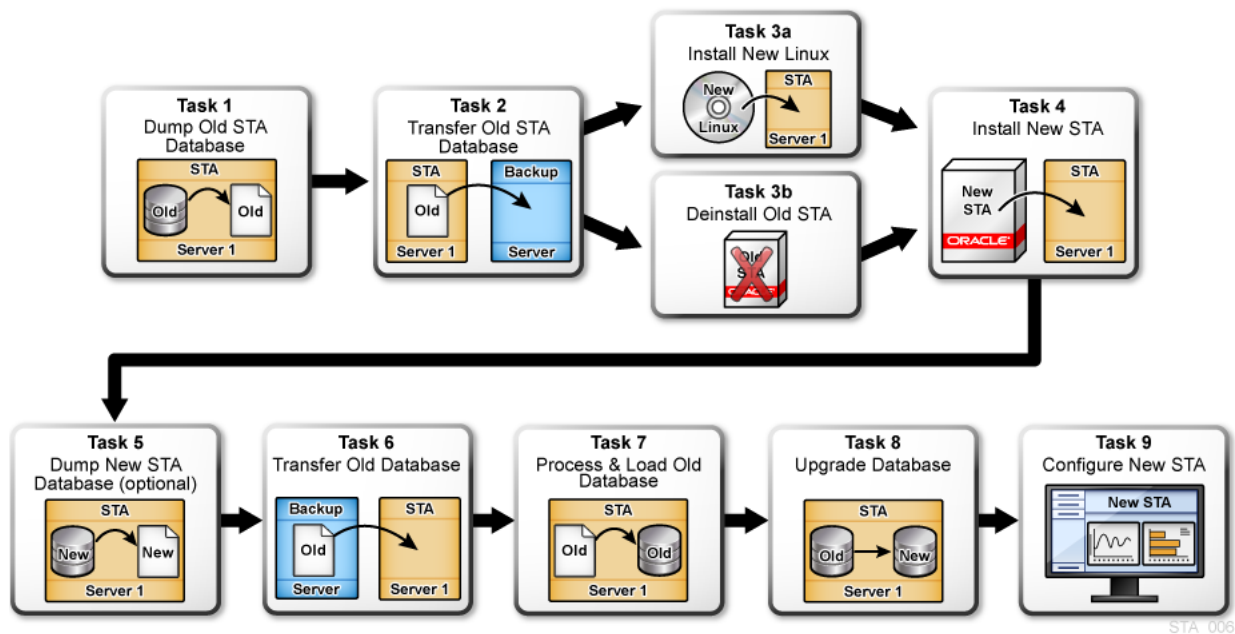
Avec cette méthode, vous devez désinstaller STA avant d'installer la nouvelle version, et mettre à niveau la base de données sur ce serveur. Pendant ce processus, STA ne contrôle pas les bibliothèques.

Cette méthode présente l'avantage de ne pas nécessiter de serveur supplémentaire dédié à la mise à niveau. Si vous effectuez une mise à niveau depuis STA 2.0.x, vous n'avez pas besoin d'installer une nouvelle version de Linux, cette méthode peut donc suffire à vos besoins.

La copie d'écran [Figure 8.1, « Présentation de la tâche de mise à niveau avec serveur unique »](#) illustre la méthode à serveur unique. Vous exécuterez les tâches de 1 à 9 dans l'ordre indiqué. En résumé :

- Effectuez le vidage de la base de données actuelle, et transférez-le vers un serveur de sauvegarde à des fins de conservation (Tâche 1 et Tâche 2).
- Selon votre version actuelle de STA, installez Linux 6.x (Tâche 3a) ou désinstallez STA 2.0.x (Tâche 3b).
- Installez STA 2.1.0, et par mesure de précaution, effectuez le vidage de la nouvelle base de données (Tâche 4 et Tâche 5).
- Transférez le vidage de l'ancienne base de données depuis le serveur de sauvegarde, puis chargez-le et mettez-le à niveau vers la nouvelle version de STA (Tâche 6 à Tâche 8).
- Rétablissez les connexions vers les bibliothèques contrôlées et effectuez les tâches de configuration manuelle nécessaires (Tâche 9). L'ancienne version de STA devant être désinstallée avant d'installer STA 2.1.0, vous devez ressaisir manuellement certaines données utilisateur de configuration.

Figure 8.1. Présentation de la tâche de mise à niveau avec serveur unique



8.3.2. Méthode de mise à niveau à deux serveurs

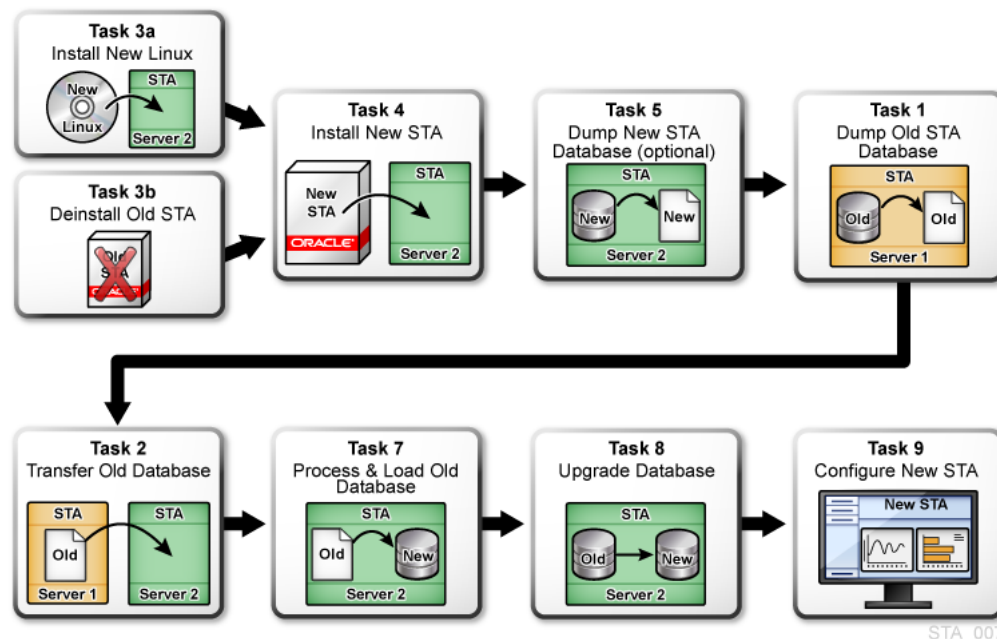
La méthode de mise à niveau à deux serveurs requiert un second serveur STA dédié, mais elle présente l'avantage de réduire le temps d'arrêt de l'application STA. Cette méthode est particulièrement utile pour la mise à niveau de STA 1.0.x, car l'ancienne version de STA peut continuer à contrôler les bibliothèques sur l'ancien serveur tandis que Linux comme la nouvelle version de STA sont installés sur le nouveau serveur.

Cependant, même avec cette méthode, STA ne contrôle pas les bibliothèques pendant la mise à niveau de la base de données actuelle vers la nouvelle version de STA. La durée de temps d'arrêt dépend de la taille de votre base de données actuelle.

La copie d'écran [Figure 8.2, « Présentation de la tâche de mise à niveau avec deux serveurs »](#) présente la méthode de mise à niveau à deux serveurs. Vous devez effectuer les tâches dans l'ordre indiqué — elles ne sont pas effectuées par ordre séquentiel, et la tâche 6 est omise. Notez que vous n'effectuez pas de vidage de la base de données STA actuelle avant d'avoir installé la nouvelle version de STA sur le nouveau serveur. En résumé :

- Selon que le second serveur exécute actuellement une version de STA, installez Linux 6.x (Tâche 3a) ou désinstallez STA 2.0.x (Tâche 3b).
- Installez STA 2.1.0 sur le nouveau serveur, et par mesure de précaution, effectuez le vidage de la nouvelle base de données (Tâche 4 et Tâche 5).
- Effectuez le vidage de la base de données actuelle sur l'ancien serveur, et transférez-la vers le nouveau serveur (Tâche 1 et Tâche 2).
- Chargez et mettez à niveau la base de données actuelle vers la nouvelle version de STA (Tâche 7 et Tâche 8).
- Rétablissez les connexions vers les bibliothèques contrôlées et effectuez les tâches de configuration manuelle nécessaires (Tâche 9).

Figure 8.2. Présentation de la tâche de mise à niveau avec deux serveurs



8.4. Modifications d'environnement pour STA 2.1.0

Un résumé des modifications d'environnement à prendre en compte lorsque vous envisagez la mise à niveau vers STA 2.1.0 est présenté ci-dessous.

8.4.1. Version de Linux

STA 2.1.0 requiert Linux 6.3 ou ultérieure (Pour plus d'informations, reportez-vous au guide *Guide des conditions requises pour l'installation de STA*). Selon votre version actuelle de

STA, pour pourrez devoir installer une nouvelle version de Linux dans le cadre du processus de mise à niveau de STA.

- Si vous effectuez la mise à niveau depuis STA 1.0.x, vous devez installer Linux 6.3 ou supérieure avant d'installer STA 2.1.0. Linux ne prend pas en charge une mise à niveau en place de Linux 5.x vers Linux 6.x ; vous devrez à la place effectuer une nouvelle installation de Linux 6.x sur le serveur STA.
- Si vous effectuez la mise à niveau de STA 2.0.x, vous exécutez déjà Linux 6.3 ou supérieure ; vous devez cependant désinstaller la version actuelle de STA avant d'installer STA 2.1.0. Il est également possible que vous deviez installer ou mettre à niveau les packages Linux RPM requis—dans le cadre de la préparation à la mise à niveau, vous vous assurez que tous les niveaux requis de package RPM sont installés, et, en vérification finale, le programme d'installation de STA vous préviendra en cas de packages manquants.

8.4.2. Numéros de port WebLogic par défaut

Les numéros de port de la console d'administration WebLogic par défaut ont été modifiés pour STA 2.1.0. Si vous utilisez actuellement les anciens numéros de port par défaut, vous pourrez souhaiter les remplacer par les nouveaux. Les nouveaux et anciens numéros de port par défaut sont les suivants :

- Nouveaux numéros par défaut pour STA 2.1.0—7019 (HTTP) et 7020 (HTTPS)
- Anciens numéros par défaut pour (STA 1.0.x et STA 2.x)—7001 (HTTP) et 7002 (HTTPS)

Remarque:

Les ports de la console d'administration WebLogic sont externes. Votre administrateur réseau peut devoir configurer des pare-feu et des routeurs pour ouvrir la communication entre le serveur STA et les clients accédant à l'interface d'administration WebLogic.

8.4.3. Ports requis pour STA 2.0.x et ultérieure

Remarque:

Cette modification a été introduite dans STA 2.0.x, cette opération n'est donc pertinente que si vous effectuez une mise à niveau de STA 1.0.x.

Dans STA 2.0.x, des ports STA ont été ajoutés pour les serveurs gérés StaUi et StaEngine. Les numéros de port des serveurs gérés STA par défaut pour STA2.0.x et STA 2.1.0 sont les suivants :

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

Remarque:

Les ports StaUi sont externes. Votre administrateur réseau peut devoir configurer des pare-feu et des routeurs pour ouvrir la communication entre le serveur STA et les clients accédant à l'interface utilisateur STA.

8.4.4. Conditions requises de nom d'utilisateur et de mot de passe

Les conditions requises de nom d'utilisateur et de mot de passe pour STA et MySQL ont été modifiées pour STA 2.1.0. Vous pourrez devoir coordonner ces conditions avec les conditions internes de votre site.

Les conditions du nom d'utilisateur requises sont les suivantes :

- Il doit comporter entre 1 et 16 caractères.
- Tous les noms d'utilisateur doivent être uniques.

Les conditions requises en termes de mot de passe sont les suivantes :

- Il doit comporter entre 8 et 31 caractères.
- Il doit comporter au moins un chiffre et une majuscule
- Il ne doit pas comporter d'espace
- Il ne doit pas comporter les caractères spéciaux suivants :

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

8.5. Tâches de préparation de la mise à niveau

Les tâches suivantes doivent être exécutées avant de commencer la mise à niveau de STA. La plupart de ces tâches sont facultatives, et le tableau [Tableau 8.1, « Directives relatives au moment d'exécuter les tâches de préparation de la mise à niveau »](#) indique quand utiliser chacune d'entre elles.

Tableau 8.1. Directives relatives au moment d'exécuter les tâches de préparation de la mise à niveau

Tâche	Quand l'exécuter
Section 8.5.1, « Vérifiez que votre site est prêt pour la mise à niveau »	Toutes les mises à niveau
Section 8.5.2, « Enregistrement des journaux existants (facultatif) »	Vous souhaitez conserver les journaux de service de la version actuelle de STA.
Section 8.5.3, « Enregistrement de l'utilisateur STA et des paramètres de configuration actuels (facultatif) »	Vous souhaitez conserver les noms d'utilisateur et les paramètres de configuration actuels de STA.
Section 8.5.4, « Renommage des modèles personnalisés avec préfixe STA- (facultatif) »	Vous disposez de modèles personnalisés avec des noms ayant comme préfixe "STA-".
Section 8.5.5, « Enregistrement des paramètres actuels de modèle personnalisé (facultatif) »	Vous souhaitez conserver les paramètres de propriété et de visibilité des modèles personnalisés existants.
Section 8.5.6, « Enregistrement des paramètres de stratégie de rapport exécutif (facultatif) »	Vous souhaitez conserver les paramètres de propriété pour les stratégies de rapports exécutifs existantes.

8.5.1. Vérifiez que votre site est prêt pour la mise à niveau

Suivez cette procédure pour vérifier les prérequis de la mise à jour et que votre site est prêt.

8.5.1.1. Vérification des prérequis de la mise à niveau

Suivez cette procédure pour vous assurer que votre environnement répond aux prérequis de STA 2.1.0.

1. Affichez votre version actuelle de STA. Certaines tâches de mise à niveau varient selon que vous effectuez la mise à niveau de STA 1.0.x ou STA 2.0.x.
 - a. Connectez-vous à STA avec un nom d'administrateur STA.
 - b. Cliquez sur **About** dans la barre d'état.
 - c. Vérifiez que la version de STA est actuelle. Pour plus d'informations, reportez-vous à la section [Section 8.2, « Chemins de mise à niveau STA 2.1.0 valides »](#).
2. Déterminez la méthode à utiliser pour effectuer la mise à niveau, à serveur unique ou à deux serveurs. Pour plus d'informations, reportez-vous à la section [Section 8.1, « Présentation du processus de mise à niveau »](#).
3. Vérifiez que votre site et le serveur cible répondent aux conditions requises de STA 2.1.0. Pour plus d'informations, reportez-vous au guide *Guide des conditions requises pour l'installation de STA*.
4. Déterminez si le système de fichiers `/tmp` sur le serveur cible STA dispose d'assez d'espace pour la mise à niveau. La taille de `/tmp` doit être au moins équivalente à celle de votre base de données STA non compressée ; un minimum de 4 Go est requis, et, pour les grandes bases de données, Oracle recommande d'augmenter la taille de `/tmp` à 32 Go, au minimum.

Si vous estimez que vous devez augmenter la taille de `/tmp`, vous pouvez le faire juste avant d'exécuter le script de mise à niveau ; reportez-vous aux instructions de la section [Section 8.6.9, « Tâche 8 : Mise à niveau de l'ancienne base de données »](#).

5. Passez en revue les modifications d'environnement concernant votre chemin de mise à niveau, effectuez les ajustements nécessaires à votre plan ou à votre environnement. Pour plus d'informations, reportez-vous à la section [Section 8.4, « Modifications d'environnement pour STA 2.1.0 »](#).
6. Si vous effectuez une mise à niveau de STA 2.0.x, assurez-vous que tous les packages RPM requis sont installés sur le serveur STA. Pour plus d'informations, reportez-vous à la section [Section 2.3.6, « Installation des packages Linux requis »](#). En vérification finale, le programme d'installation de STA vous préviendra également en cas de packages manquants.

8.5.1.2. Vérification de l'activité actuelle de STA

Suivez cette procédure pour vérifier que votre environnement STA actuel fonctionne normalement.

1. Les étapes suivantes servent à vérifier que la version actuelle de STA a récemment eu une communication avec chaque bibliothèque contrôlée.
 - a. Connectez-vous à STA en tant qu'administrateur STA.

- b. Sous l'onglet **Setup & Administration**, sélectionnez **SNMP Connections**.
- c. Vérifiez les valeurs suivantes dans le tableau des bibliothèques surveillées :
 - État de la communication de déROUTement SNMP récent — GOOD
 - Statut de la dernière connexion — SUCCESS
2. Les étapes suivantes servent à vérifier que STA traite les échanges entre toutes les bibliothèques.
 - a. Sous l'onglet **Tape System Activity**, sélectionnez **Exchanges – Overview**.
 - b. Sélectionnez l'icône **Filter** et appliquez le filtre Exchange End (No. Days) Less Than 1.
 - c. Dans la barre d'outils du tableau, sélectionnez **View**, puis **Sort**, et **Advanced**. Triez par nom de bibliothèque de lecteurs ou par numéro de série de lecteur.
 - d. Vérifiez que toutes les bibliothèques ont une activité d'échange.

8.5.2. Enregistrement des journaux existants (facultatif)

Les journaux de service et d'application existants ne sont pas conservés après la mise à niveau, car vous devez désinstaller la version actuelle de STA ou installer une nouvelle version de Linux avant d'installer STA 2.1.0. Suivez cette procédure pour enregistrer tous les journaux que vous souhaitez conserver.

1. Déterminez l'emplacement des journaux de base de données et d'installation que vous souhaitez conserver et déplacez-les vers un emplacement sûr. Les journaux pouvant vous intéresser sont situés à l'emplacement des journaux STA que vous avez défini pour votre installation. Pour plus d'informations, reportez-vous à la section [Section 2.1.2, « Examen de la disposition du système de fichiers STA »](#).
2. Les étapes suivantes servent à effectuer un instantané de journal de service sur l'installation de STA actuelle. Cet étape est facultative, mais recommandée, car l'assistance Oracle peut utiliser ces journaux pour résoudre des problèmes ayant pu survenir avant la mise à niveau.
 - a. Connectez-vous à STA en tant qu'administrateur STA.
 - b. Sous l'onglet **Setup & Administration**, sélectionnez **Logs**.
 - c. A l'écran Service – Logs, cliquez sur l'icône **Create New Log Bundle**.
 - d. Dans la boîte de dialogue Create New Log Bundle, affectez un nom de bundle et cliquez sur **Save**. Ce processus peut durer plusieurs minutes.
3. Suivez les étapes suivantes pour télécharger le bundle de journaux de service que vous venez de créer, ainsi que tout autre bundle que vous souhaitez conserver. Vous devez télécharger les journaux un par un.
 - a. Sur l'écran Service – Logs, sélectionnez le bundle que vous souhaitez télécharger.
 - b. Cliquez sur l'icône **Download Selected Log Bundle**.
 - c. Dans la boîte de dialogue, indiquez l'emplacement cible et enregistrez le bundle de journaux.

8.5.3. Enregistrement de l'utilisateur STA et des paramètres de configuration actuels (facultatif)

Cette section ne s'applique que si vous souhaitez conserver les noms d'utilisateur STA et les paramètres de configuration actuels dans STA 2.1.0. Suivez ces procédures pour afficher et enregistrer les valeurs actuelles afin de les ressaisir pour STA 2.1.0. Vous ressaisirez la plupart de ces valeurs après la mise à niveau ; pour plus d'informations, reportez-vous à la section [Section 8.6.10, « Tâche 9 : Configuration de la nouvelle version de STA »](#).

8.5.3.1. Enregistrement des noms d'utilisateur MySQL

Suivez cette procédure pour afficher et enregistrer des noms d'utilisateur MySQL existants utilisés pour accéder à la base de données STA. Le programme d'installation de STA vous invitera à saisir ces valeurs. Il est impossible de récupérer les mots de passe.

- a. Ouvrez une session de terminal sur le serveur STA actuel et connectez-vous en tant qu'utilisateur root du système.
- b. Affichez tous les noms d'utilisateur de la base de données STA avec la requête suivante. A l'invite, saisissez le mot de passe de l'utilisateur root de base de données. Par exemple :

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

- c. Enregistrez les noms d'utilisateur.

8.5.3.2. Enregistrement des paramètres client SNMP STA

Suivez cette procédure pour afficher et enregistrer les paramètres client SNMP de STA. Vous ressaisirez la plupart de ces valeurs après la mise à niveau.

Remarque:

Dans la nouvelle version de STA, les valeurs SNMP doivent correspondre à l'indication sur les bibliothèques contrôlées.

- a. Connectez-vous à STA avec un nom d'administrateur STA.
- b. Sous l'onglet **Setup & Administration**, sélectionnez **SNMP Connections**.

Le tableau Attributs client affiche les paramètres de configuration du client SNMP STA.

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. Enregistrez les valeurs depuis les colonnes suivantes :
- SNMP Username
 - User Community
 - Trap Community

8.5.3.3. Enregistrement des noms d'utilisateur WebLogic — Mises à niveau de STA 1.0.x uniquement

Pour les mises à jour de STA 1.0.x, suivez cette procédure pour afficher et enregistrer les noms d'utilisateur WebLogic utilisés pour vous connecter à STA. Vous ressaisirez la plupart de ces valeurs après la mise à niveau. Il est impossible de récupérer les mots de passe.

Remarque:

Depuis STA 2.0.x, les noms d'utilisateur sont créés et conservés via l'interface utilisateur de STA ; pour obtenir des instructions, reportez-vous à la section [Section 8.5.3.4, « Enregistrement des noms d'utilisateur STA — Mises à niveau de STA 2.0.x uniquement »](#).

- a. Lancez un navigateur Web pris en charge sur votre ordinateur et saisissez l'URL de la console d'administration WebLogic.

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

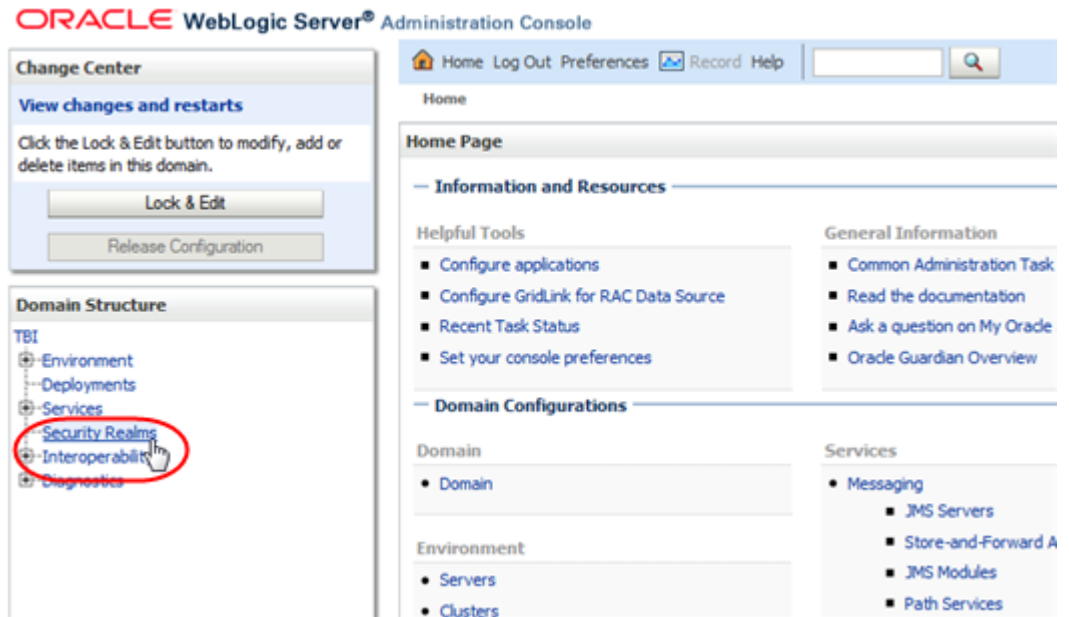
Où :

- *host_name* est le nom d'hôte du serveur STA.
- *port_number* est le numéro de port STA de la console d'administration WebLogic dans la version STA actuelle.
- STA doit être saisi en majuscules.

Par exemple :

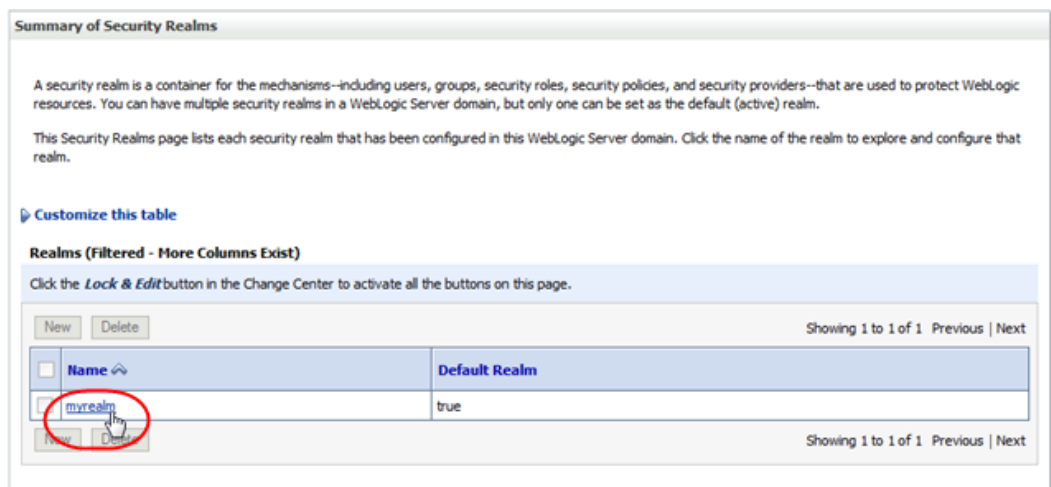
`https://staserver.example.com:7002/console/`

- b. Connectez-vous à l'aide du nom d'utilisateur et du mot de passe de la console d'administration WebLogic.
- c. Dans l'arborescence de navigation de la structure du domaine, cliquez sur **Security Realms**.



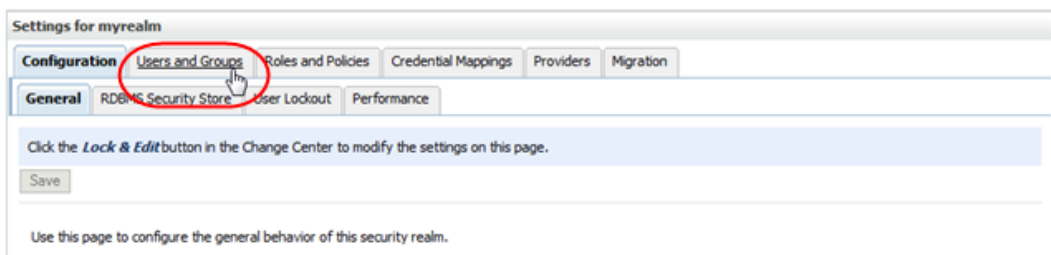
L'écran récapitulatif des Security Realms apparaît.

- d. Dans la colonne Name, sélectionnez le lien actif **myrealm** (ne sélectionnez pas la case).

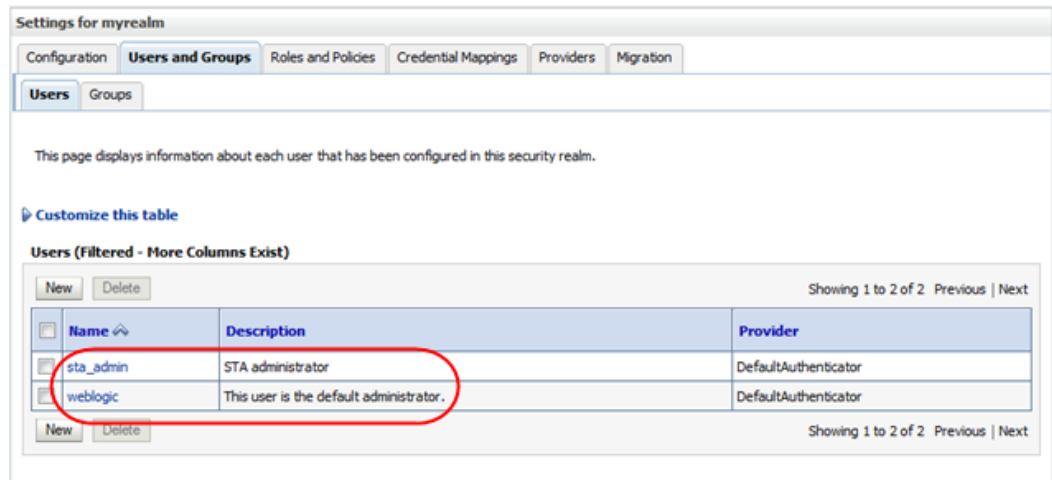


L'écran Settings for myrealm apparaît.

- e. Sélectionnez l'onglet **Users and Groups**.



Le tableau Users répertorie les noms d'utilisateur disponibles.



- f. Enregistrez les noms d'utilisateur à conserver.

8.5.3.4. Enregistrement des noms d'utilisateur STA — Mises à niveau de STA 2.0.x uniquement

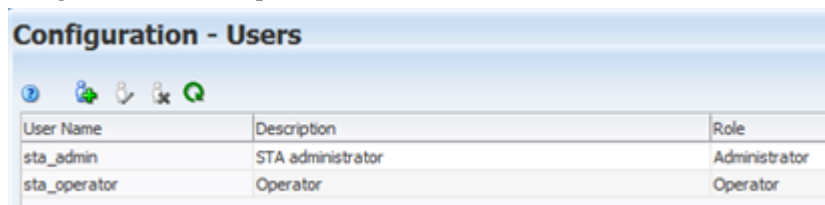
Pour les mises à jour de STA 2.0.x, suivez cette procédure pour afficher et enregistrer les noms d'utilisateur utilisés pour vous connecter à STA. Vous ressaisirez ces informations après la mise à niveau. Il est impossible de récupérer les mots de passe.

Remarque:

Les noms d'utilisateur de STA 1.0.x sont créés et conservés via la console d'administration WebLogic ; pour connaître les instructions, reportez-vous à la section [Section 8.5.3.3, « Enregistrement des noms d'utilisateur WebLogic — Mises à niveau de STA 1.0.x uniquement »](#).

- a. Connectez-vous à STA avec un nom d'administrateur STA.
- b. Sous l'onglet **Setup & Administration**, sélectionnez **Users**.

L'écran Configuration – Users présente tous les noms d'utilisateur STA et leur rôles.



- c. Enregistrez les noms d'utilisateur et les rôles à conserver.

8.5.3.5. Enregistrement des paramètres du serveur de messagerie STA

Suivez cette procédure pour afficher et enregistrer le protocole de messagerie STA et le nom d'utilisateur du compte, dans le cas où le serveur de messagerie requiert une authentification. Vous ressaisirez la plupart de ces valeurs après la mise à niveau. Le mot de passe ne s'affiche pas.

- Connectez-vous à STA avec un nom d'administrateur STA.
- Sous l'onglet **Setup & Administration**, sélectionnez **Email**.
- Dans le tableau des paramètres serveur SMTP, sélectionnez l'enregistrement Alertes StorageTek Tape Analytics, puis cliquez sur l'icône **Edit Selected SMTP Server**.

La boîte de dialogue Define SMTP Server apparaît.

- Enregistrez les valeurs des champs suivants :
 - Use Secure Connection Protocol
 - Username

8.5.4. Renommage des modèles personnalisés avec préfixe STA– (facultatif)

Cette procédure ne s'applique que si vous disposez de modèles personnalisés avec le préfixe "STA–". Pendant l'installation de STA 2.1.0, tous les modèles au préfixe "STA–" sont supprimés et remplacés par de nouveaux modèles STA prédéfinis.

Suivez cette procédure pour affecter de nouveaux noms aux modèles afin de les conserver pendant la mise à niveau.

Remarque:

Les modèles prédéfinis STA portent le préfixe "STA-"; Oracle recommande donc de ne *pas* utiliser ce préfixe pour nommer des modèles personnalisés.

- a. Connectez-vous à STA avec un nom d'administrateur.
- b. Sous l'onglet **Setup & Administration**, sélectionnez **Templates Management**.
- c. Triez le tableau par la date de création/mise à jour, pour cibler les modèles modifiés depuis la date d'installation de STA.
- d. Sélectionnez le lien de texte d'un modèle personnalisé portant le préfixe "STA-".

Vous êtes renvoyé vers l'écran où le modèle sélectionné est appliqué.

- e. Cliquez sur **Save Template** dans la barre d'outils Templates.

La boîte de dialogue Save Template s'affiche.

- f. Dans le champ **Template Name**, affectez un nouveau nom sans le préfixe "STA-". Votre saisie doit être unique.
- g. Cliquez sur **Save**.

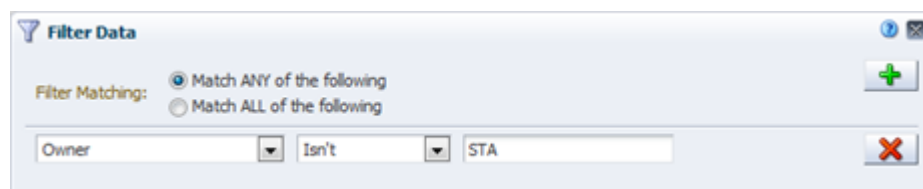
Le modèle est enregistré.

8.5.5. Enregistrement des paramètres actuels de modèle personnalisé (facultatif)

Cette procédure ne s'applique que si vous disposez de modèles personnalisés. La mise à niveau conserve les modèles personnalisés, mais après la mise à niveau, STA est propriétaire de tous les modèles personnalisés, et leur visibilité est publique.

Suivez cette procédure pour enregistrer les paramètres actuels de propriété et de visibilité de tous les modèles personnalisés afin de les restaurer après la mise à niveau, si nécessaire. Vous pouvez ignorer cette procédure si la propriété et la visibilité des modèles ne sont pas critiques pour votre mise en oeuvre.

- a. Connectez-vous à STA avec un nom d'administrateur.
- b. Sous l'onglet **Setup & Administration**, sélectionnez **Templates Management**.
- c. Sélectionnez l'icône **Filter** et appliquez un filtre pour que l'écran n'affiche que les modèles dont STA n'est pas propriétaire — seuls les modèles personnalisés seront présentés.



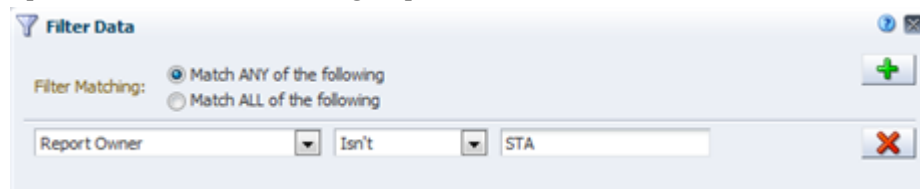
- d. Enregistrez les paramètres Owner et Public Visibility actuels de chaque modèle personnalisé. Si vous disposez de nombreux modèles, vous pourrez souhaiter effectuer une copie d'écran.

8.5.6. Enregistrement des paramètres de stratégie de rapport exécutif (facultatif)

Cette procédure ne s'applique que si vous disposez de stratégies de rapports exécutifs détenues de manière privée. La mise à niveau préserve les stratégies de rapports exécutifs, mais après la mise à jour, la propriété publique est affectée à toutes les stratégies privées.

Suivez cette procédure pour enregistrer les paramètres actuels de propriété de toutes les stratégies privées afin de les restaurer après la mise à niveau, si nécessaire. Vous pouvez ignorer cette procédure si la propriété de stratégie de rapport exécutif n'est pas critique pour votre mise en oeuvre.

- Connectez-vous à STA avec un nom d'administrateur STA.
- Sous l'onglet **Setup & Administration**, sélectionnez **Executive Reports Policies**.
- Sélectionnez l'icône **Filter** pour que l'écran ne présente que les stratégies dont STA n'est pas propriétaire — seules les stratégies privées s'afficheront.



- Enregistrez le propriétaire actuel du rapport pour chaque stratégie. Si vous disposez de nombreuses stratégies, vous pourrez souhaiter effectuer une copie d'écran.

8.6. Tâches de mise à niveau

Prudence:

Seul un administrateur Linux ou STA devra effectuer la mise à niveau. Toutes les tâches sont obligatoires et doivent être effectuées aussi précisément que décrit, dans l'ordre indiqué, sans quoi des pertes de données pourront survenir.

Si vous utilisez la méthode à serveur unique, vous effectuerez ces tâches en ordre séquentiel ; pour plus d'informations, reportez-vous à la copie d'écran [Figure 8.1, « Présentation de la tâche de mise à niveau avec serveur unique »](#).

Si vous utilisez la méthode de mise à niveau à deux serveurs, vous n'effectuerez *pas* les tâches en ordre séquentiel, et la tâche 6 sera omise, reportez-vous à la copie d'écran [Figure 8.2, « Présentation de la tâche de mise à niveau avec deux serveurs »](#) pour connaître l'ordre des tâches à effectuer.

- [Section 8.6.1, « Tâche 1: Vidage de l'ancienne base de données STA »](#)
- [Section 8.6.2, « Tâche 2 : Transfert du vidage de l'ancienne base de données »](#)
- [Section 8.6.3, « Tâche 3a : Installation de la nouvelle version de Linux \(pour les mises à niveau depuis STA 1.0.x\) »](#)
- [Section 8.6.4, « Tâche 3b : Désinstallation de l'ancienne version de STA \(pour les mises à niveau depuis STA 2.0.x\) »](#)

- [Section 8.6.5, « Tâche 4: Installation de la nouvelle version de STA »](#)
- [Section 8.6.6, « Tâche 5 : Vidage de la nouvelle base de données STA \(facultatif\) »](#)
- [Section 8.6.7, « Tâche 6 : Transfert de l'ancienne base de données STA sur le serveur STA »](#)
- [Section 8.6.8, « Tâche 7 : Traitement et chargement de l'ancienne base de données STA »](#)
- [Section 8.6.9, « Tâche 8 : Mise à niveau de l'ancienne base de données »](#)
- [Section 8.6.10, « Tâche 9 : Configuration de la nouvelle version de STA »](#)
- [Section 8.6.11, « Récupération d'une mise à niveau de base de données ayant échoué \(facultatif\) »](#)

8.6.1. Tâche 1: Vidage de l'ancienne base de données STA

Suivez cette procédure pour effectuer un vidage complet de l'ancienne (actuelle) base de données STA.

1. Suivez les étapes suivantes pour afficher la taille de la base de données STA actuelle.
 - a. Connectez-vous à STA avec un nom d'administrateur STA.
 - b. Cliquez sur **About** dans la barre d'état.
 - c. Dans la boîte de dialogue About, faites défiler le menu pour afficher la Database Current Size, et enregistrez cette valeur.
2. Suivez les étapes suivantes pour vérifier que l'emplacement où effectuer le vidage de la base de données dispose de suffisamment d'espace disque.
 1. Ouvrez une session de terminal sur le serveur STA et connectez-vous en tant qu'utilisateur root du système.
 2. Affichez l'espace disponible de la cible du vidage de la base de données, et vérifiez s'il est suffisant pour contenir le fichier de vidage. Par exemple :

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

3. Arrêtez tous les services STA.

```
# STA stop all
```

4. Démarrez le service MySQL.

```
# service mysql start
```

5. Effectuez le vidage de la base de données STA vers un fichier unique. A l'invite, saisissez le mot de passe de l'utilisateur root de base de données.

```
# 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
```

Remarque:

Le paramètre facultatif `-v` (pour la sortie détaillée), n'est pas recommandé, car un grand nombre de messages est affiché sur la fenêtre de terminal, et le traitement de commande des grandes bases de données peut se retrouver ralenti de façon significative.

Dans l'exemple [Exemple 8.1, « Vidage de l'ancienne base de données »](#), le vidage de la base de données STA 1.0.x s'effectue vers le dossier `/dbdumpfiles` du serveur STA, et porte le nom de fichier `Dec14_dump.sql`.

Exemple 8.1. Vidage de l'ancienne base de données

```
# 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. Pour réduire la taille du fichier de vidage d'environ 50 %, compressez le fichier en gzip.

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

8.6.2. Tâche 2 : Transfert du vidage de l'ancienne base de données

Suivez cette procédure pour transférer le vidage compressé de l'ancienne base de données STA vers un serveur de sauvegarde hors de la plateforme, (méthode à serveur unique), ou vers le nouveau serveur STA 2.1.0 (méthode à deux serveurs).

Prudence:

Si vous effectuez une mise à niveau de STA 1.0.x avec la méthode à serveur unique, vous devez sauvegarder la base de données STA sur un autre serveur. Ne sauvegardez pas la base de données sur un système de fichiers sur le serveur STA actuel, car l'installation de Linux 6.x lors de la [Section 8.6.3, « Tâche 3a : Installation de la nouvelle version de Linux \(pour les mises à niveau depuis STA 1.0.x\) » \[129\]](#) détruira toutes les données du serveur.

1. Si ce n'est déjà fait, arrêtez tous les services STA.

```
# STA stop all
```

2. Effectuez une somme de contrôle avant de transférer le fichier sur le serveur de sauvegarde.

```
# cksun dump_file_name.sql.gz
```

Le résultat inclut une valeur de somme de contrôle et un calcul d'octets. Enregistrez la valeur de somme de contrôle ; vous l'utiliserez pour vérifier l'intégrité du fichier après le transfert du fichier vers le serveur de sauvegarde.

3. Transférez le fichier vers le serveur cible à l'aide d'un utilitaire de transfert comme SCP. L'option `-p` conserve les valeurs d'horodatage.

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

Dans l'exemple [Exemple 8.2, « Transfert de l'ancienne base de données vers le serveur de sauvegarde \(méthode à serveur unique\) »](#), SCP sert à transférer le fichier de vidage compressé de la base de données `Dec14_dump.sql.gz` vers le dossier `/dbdumpfiles` de l'hôte de sauvegarde `backup1`. Le dossier `/dbdumpfiles` existe déjà sur l'hôte de sauvegarde.

Exemple 8.2. Transfert de l'ancienne base de données vers le serveur de sauvegarde (méthode à serveur unique)

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

Dans l'exemple [Exemple 8.3, « Transfert de l'ancienne base de données vers le nouveau serveur STA \(méthode à deux serveurs\) »](#), SCP sert à transférer le fichier de vidage compressé de la base de données `Dec14_dump.sql.gz` vers le dossier `/dbdumpfiles` sur l'hôte STA 2.1.0 `sta_new`.

Exemple 8.3. Transfert de l'ancienne base de données vers le nouveau serveur STA (méthode à deux serveurs)

```
# cd /dbdumpfiles
```



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

4. Sur le serveur cible, effectuez une somme de contrôle du fichier transféré. Vérifiez que les valeurs de somme de contrôle correspondent.

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

8.6.3. Tâche 3a : Installation de la nouvelle version de Linux (pour les mises à niveau depuis STA 1.0.x)

Cette procédure ne s'applique qu'aux mises à niveau de STA 1.0.x. Installez Linux 6.3 ou ultérieure sur le serveur STA ; pour obtenir des instructions, reportez-vous au chapitre [Chapitre 2, *Installation de Linux*](#).

Prudence:

Cette activité détruit toutes les données du serveur. Si vous utilisez la méthode à serveur unique, ne suivez cette procédure qu'après avoir effectué les tâches [Section 8.6.1, « Tâche 1: Vidage de l'ancienne base de données STA »](#) et [Section 8.6.2, « Tâche 2 : Transfert du vidage de l'ancienne base de données »](#).

8.6.4. Tâche 3b : Désinstallation de l'ancienne version de STA (pour les mises à niveau depuis STA 2.0.x)

Cette procédure ne s'applique qu'aux mises à niveau de STA 2.0.x. Désinstaller la version actuelle de STA ; pour obtenir des instructions, reportez-vous aux sections [Section 9.2.1, « Désinstallation de STA »](#) et [Section 9.2.2, « Vérification de la réussite de la désinstallation. »](#).

Prudence:

Cette activité détruit toutes les données STA du serveur. Si vous utilisez la méthode à serveur unique, ne suivez cette procédure qu'après avoir effectué les tâches [Section 8.6.1, « Tâche 1: Vidage de l'ancienne base de données STA »](#) et [Section 8.6.2, « Tâche 2 : Transfert du vidage de l'ancienne base de données »](#).

8.6.5. Tâche 4: Installation de la nouvelle version de STA

Suivez cette procédure pour installer STA 2.1.0.

1. Installez STA 2.1.0 ; pour obtenir des instructions, reportez-vous à la section [Chapitre 3, *Installation de STA*](#).
2. Pour vérifier que STA fonctionne correctement et pour terminer la configuration de l'administrateur STA sous WebLogic, connectez-vous à l'application STA.

L'écran Dashboard est affiché.

Remarque:

Le processus de mise à niveau n'étant pas encore terminé, les portlets de tableau de bord affichent le message "No data to display", ce qui est normal. Les données des bibliothèques seront correctement affichées après la mise à niveau de la base de données et la configuration de la nouvelle version de STA.

3. Déconnectez-vous de STA.
4. Ouvrez une session de terminal sur le serveur STA et connectez-vous en tant qu'utilisateur root du système.
5. Arrêtez tous les services STA.

```
# STA stop all
```

6. Cette étape s'applique uniquement si vous souhaitez que STA contrôle les bibliothèques à l'aide de SNMP v2c (pour plus de détails, reportez-vous à la section [Annexe F, Configuration du mode SNMP v2c](#)). Depuis STA 2.0.x, SNMP v2c est activé par défaut. Suivez les étapes suivantes pour confirmer que SNMP V2c est activé.
 - a. Passez au répertoire de fichiers de configuration de STA.

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

- b. Affichez le fichier de propriétés de version de SNMP, et vérifiez que le paramètre `V2c` est défini sur `true`.

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

- c. Si ce n'est pas le cas, reportez-vous à la section [Section F.1.3, « Activation du mode SNMP v2c pour STA »](#) pour obtenir des instructions pour le modifier.

8.6.6. Tâche 5 : Vidage de la nouvelle base de données STA (facultatif)

Cette procédure est facultative, mais elle est recommandée. Suivez cette procédure pour procéder au vidage de la base de données STA 2.1.0 par sûreté. Si la mise à niveau ([Tâche 8 : Mise à niveau de l'ancienne base de données](#)) ne peut pas se terminer, il est possible de restaurer la base de données vide pour récupérer STA 2.1.0 dans un état permettant sa configuration pour l'exécuter comme s'il s'agissait d'une nouvelle installation sans données ; pour obtenir des détails sur le processus de récupération, reportez-vous à la section [Récupération d'une mise à niveau de base de données ayant échoué \(facultatif\)](#).

1. Ouvrez une session de terminal sur le serveur STA et connectez-vous en tant qu'utilisateur root du système.
2. Si ce n'est déjà fait, arrêtez tous les services STA.

```
# STA stop all
```

- Démarrez le service MySQL.

```
# STA start mysql
```

- Créez le fichier de sauvegarde de la base de données. A l'invite, saisissez le mot de passe de l'utilisateur root de base de données.

```
# 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
```

Remarque:

Le paramètre facultatif `-v` (pour la sortie détaillée), n'est pas recommandé, car un grand nombre de messages est affiché sur la fenêtre de terminal, et le traitement de commande des grandes bases de données peut se retrouver ralenti de façon significative.

Sous [Exemple 8.4, « Vidage de la nouvelle base de données »](#), le vidage de la base de données STA 2.1.0 s'effectue vers le dossier `/dbdumpfiles` du serveur STA avec comme nom de fichier `STA_FRESH_INSTALL_BACKUP.sql`.

Exemple 8.4. Vidage de la nouvelle base de données

```
# 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...
```

Remarque:

Si vous voyez le message "Can't connect to local MySQL server", alors le serveur MySQL n'est pas en cours d'exécution. Assurez-vous d'avoir lancé MySQL (Étape 3).

8.6.7. Tâche 6 : Transfert de l'ancienne base de données STA sur le serveur STA

Remarque:

Cette procédure ne s'applique que pour la méthode à serveur unique.

Suivez cette procédure pour transférer la sauvegarde de base de données STA 1.0.x ou STA 2.0.x sur le serveur STA 2.1.0.

1. Si ce n'est déjà fait, arrêtez tous les services STA.

```
# STA stop all
```

2. Transfert de la base de données L'option `-p` activée sur SCP conserve les valeurs d'horodatage.

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

Sous [Exemple 8.5, « Transfert de l'ancienne base de données vers le nouveau serveur STA »](#), SCP sert à transférer le fichier compressé de vidage de la base de données `Dec14_dump.sql.gz` depuis `/dbdumpfiles` sur l'hôte `backup1` vers le dossier `/dbdumpfiles` sur le serveur STA 2.1.0.

Exemple 8.5. Transfert de l'ancienne base de données vers le nouveau serveur STA

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

3. Effectuez une somme de contrôle du fichier transféré. Vérifiez que la valeur de somme de contrôle correspond à la valeur que vous avez reçue dans la [Section 8.6.1, « Tâche 1: Vidage de l'ancienne base de données STA » \[126\]](#).

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

8.6.8. Tâche 7 : Traitement et chargement de l'ancienne base de données STA

Suivez cette procédure pour décompresser la base de données STA 1.0.x ou STA 2.0.x, et la rétablir sur le serveur STA 2.1.0. La base de données décompressée peut requérir 10 à 15 fois plus d'espace que la base de données compressée.

1. Si ce n'est déjà fait, arrêtez tous les services STA.

```
# STA stop all
```

2. Décompressez le fichier de sauvegarde.

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

3. Suivez les étapes suivantes pour purger la base de données STA de données obsolètes telles que des enregistrements SNMP qui ont déjà été traités ou des enregistrements d'analyse vides.

Estimation de la durée : Pour STA 1.0.x et STA 2.0.x, jusqu'à une minute par giga-octet de taille d'instantané de base de données décompressée.

Remarque:

Un enregistrement permanent de l'activité de la commande *purgerecs* est enregistré dans la base de données STA. Depuis STA 2.0.x, la purge de la base de données a lieu automatiquement au moment de l'exécution. MySQL Event Scheduler effectue régulièrement des purges d'enregistrements de différentes tables pour modérer l'augmentation de la base de données.

- a. Passez au répertoire des mises à jour de sauvegarde de la base de données STA.

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

- b. Lancez la purge des données.

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

Remarque:

Pour obtenir de l'aide avec la commande *purgerecs*, tapez la commande suivante :

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

Sous [Exemple 8.6, « Purge des données obsolètes de l'ancienne sauvegarde de base de données »](#), l'utilitaire *purgerecs* traite le fichier de vidage MySQL *Dec14_dump.sql* dans */dbdumpfiles*. La sortie est dirigée vers un nouveau fichier appelé *Dec14_dump_PURGED.sql* dans */dbdumpfiles*. Un point de progression apparaîtra pour tous les 200 enregistrements traités.

Exemple 8.6. Purge des données obsolètes de l'ancienne sauvegarde de base de données

```
# 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. Cette opération est facultative. Déterminez la taille du fichier de la base de données et le temps de traitement.

Estimation de la durée : Pour STA 1.0.x et STA 2.0.x, jusqu'à trois à dix minutes par gigaoctet de taille d'instantané de base de données décompressée.

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

5. Démarrez le serveur MySQL.

```
# STA start mysql
```

6. Chargez la base de données STA 1.0.x ou STA 2.0.x. A l'invite, saisissez le mot de passe de l'utilisateur root de base de données. A moins de spécifier l'option `-v` (détaillée) (non recommandé), vous ne verrez aucune sortie de commande lors de l'exécution du processus.

Remarque:

Le paramètre facultatif `-v` (pour la sortie détaillée), n'est pas recommandé, car un grand nombre de messages est affiché sur la fenêtre de terminal, et le traitement de commande des grandes bases de données peut se retrouver ralenti de façon significative.

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

```
Password: mysql_root_password
```

Où :

- `-p` — demande le mot de passe root de la base de données établi pendant l'installation de STA.
- `-e` — exécute les instructions entre guillemets suivantes :
 - `SET SESSION SQL_LOG_BIN=0;` — Coupe les connexions binaires inutiles, permettant d'accélérer le chargement.
 - `SOURCE /path_to_dump_file/dump_file_name_PURGED.sql` — Charge le fichier de vidage dans la base de données.

Si la commande aboutit, vous revenez à l'invite de commande une fois que le processus se termine.

8.6.9. Tâche 8 : Mise à niveau de l'ancienne base de données

Suivez cette procédure pour mettre à niveau la base de données STA 1.0.x ou STA 2.0.x sur le schéma STA 2.1.0.

Estimation de la durée : Durée approximative, par giga-octet de taille d'instantané de base de données décompressée.

- STA 1.0.x — Jusqu'à cinq minutes par giga-octet
- STA 2.0.x — Jusqu'à 30 minutes par giga-octet

1. Si ce n'est déjà fait, arrêtez tous les services STA.

```
# STA stop all
```

2. Si, lors de l'étape [Section 8.5.1.1, « Vérification des prérequis de la mise à niveau »](#), vous avez déterminé que la taille de */tmp* n'est pas suffisante pour la mise à niveau, augmentez la taille de */tmp* autant que nécessaire.

Si cette opération n'est pas possible, suivez les étapes suivantes pour définir une variable d'environnement que MySQL utilisera comme emplacement temporaire alternatif :

a. Créez un emplacement temporaire alternatif et affectez-lui les autorisations d'ouverture. Par exemple :

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

b. Arrêtez MySQL.

```
# STA stop mysql
```

c. Modifiez le fichier de configuration MySQL. Par exemple :

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

d. Dans la section *mysqld* du fichier, ajoutez une ligne définissant l'emplacement temporaire alternatif, identifié par la variable *tmpdir*. Ci-dessous, un exemple du fichier une fois cette ligne ajoutée.

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

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

e. Redémarrez MySQL.

```
# STA start mysql
```

3. Passez au répertoire des mises à jour de la base de données.

```
# cd /oracle_storage_home/StorageTek_Tape_Analytics/db/updates
```

- Commencez le script de mise à niveau, et, à l'invite, saisissez le mot de passe de l'utilisateur root de la base de données. Pour des raisons de sécurité, le mot de passe ne s'affiche pas à l'écran.

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

Remarque:

Vous pouvez effectuer cette étape en tant qu'utilisateur root du système, ou en tant qu'utilisateur du programme d'installation Oracle.

Ci-dessous, un exemple d'affichage d'écran.

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

Lorsque le traitement est terminé, une bannière similaire à celle-ci s'affiche :

Prudence:

Attendez de voir cette bannière avant de poursuivre.

```
+-----+
| 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. Si pendant la tâche [Section 8.6.9, « Tâche 8 : Mise à niveau de l'ancienne base de données »](#), vous avez augmenté la taille de */tmp* ou créé un emplacement temporaire alternatif, restaurez-le à sa taille normale et dans son emplacement prévu.
6. Démarrez tous les services STA.

```
# STA start all
```

7. Cette opération est facultative. Supprimez le fichier *STA_FRESH_INSTALL_BACKUP.sql* pour libérer de l'espace disque sur le volume de sauvegarde de la base de données STA.

8.6.10. Tâche 9 : Configuration de la nouvelle version de STA

Suivez ces procédures pour configurer les bibliothèques et STA 2.1.0 pour que STA puisse commencer à contrôler l'activité des bibliothèques.

8.6.10.1. Mise à jour du destinataire de déroulement STA sur les bibliothèques

Deux nouveaux niveaux de déroulement, 13 (déroulement de test) et 14 (déroulement d'intégrité) ont été introduits avec STA 2.0.x. Suivez les étapes suivantes sur chaque bibliothèque contrôlée pour vous assurer que ces niveaux de déroulement sont inclus dans la définition du destinataire de déroulement STA.

1. Selon votre chemin de mise à niveau, procédez comme suit :
 - Si vous utilisez la méthode à serveur unique pour mettre à niveau depuis STA 2.0.x, passez à la section [Section 8.6.10.2, « Configurez les paramètres SNMP dans STA » \[138\]](#).
 - Si vous utilisez la méthode à serveur unique pour mettre à niveau de STA 1.0.x, passez à l'étape 2 pour ajouter les nouveaux niveaux de déroulement au destinataire de déroulement STA existant sur chaque bibliothèque contrôlée.
 - Si vous utilisez la méthode de mise à niveau à deux serveurs, passez à l'étape 3 pour ajouter un nouveau destinataire de déroulement STA à chaque bibliothèque contrôlée.
2. Si vous utilisez la méthode à serveur unique pour mettre à niveau depuis STA 1.0.x, suivez les étapes appropriées au modèle de bibliothèque pour ajouter les nouveaux niveaux de déroulement au destinataire de déroulement STA.

Sur tous les modèles de bibliothèque, hormis sur le modèle SL150, vous devez supprimer la définition existante et ajouter une nouvelle.

Toutes les bibliothèques sauf SL150

- a. Connectez-vous à la CLI de la bibliothèque.
- b. Affichez tous les destinataires de déroulement, et notez le numéro d'indice du destinataire STA.

```
snmp listTrapRecipients
```

- c. Supprimez le destinataire de déroutement STA.

```
snmp deleteTrapRecipient id index
```

Où :

- *index* est le numéro d'indice du destinataire de déroutement STA.
- d. Rajoutez le destinataire de déroutement STA et incluez les nouveaux niveaux de déroutement dans la liste des niveaux de déroutement. Pour obtenir des instructions, reportez-vous à la section [Section 5.2.6, « Créez le destinataire de déroutement STA SNMP v3. »](#) ou [Section F.1.2, « Création du destinataire de déroutement SNMP v2c STA sur la bibliothèque »](#).

Bibliothèques SL150

- a. Connectez-vous à l'interface utilisateur basée sur un navigateur.
 - b. Sous le menu **SNMP**, sélectionnez **SNMP Trap Recipients**.
 - c. Dans la liste, sélectionnez le destinataire de déroutement STA.
 - d. Sélectionnez **Modify Trap Recipient**.
 - e. Ajoutez les nouveaux niveaux de déroutement à la liste des niveaux de déroutement, puis cliquez sur **Save**.
3. Si vous utilisez la méthode de mise à niveau à deux serveurs, ajoutez le nouveau serveur STA 2.1.0 comme destinataire de déroutement sur chaque bibliothèque. Voir la section [Section 5.2.6, « Créez le destinataire de déroutement STA SNMP v3. »](#) [86] ou [Section F.1.2, « Création du destinataire de déroutement SNMP v2c STA sur la bibliothèque »](#)

8.6.10.2. Configurez les paramètres SNMP dans STA

Suivez ces étapes pour toutes les mises à niveau. Ces étapes sont effectuées dans STA.

1. Connectez-vous à STA en tant qu'administrateur STA.
2. Ressaisissez les paramètres de configuration du client SNMP STA à l'aide des valeurs enregistrées avant la mise à niveau ; voir la section [Section 8.5.3, « Enregistrement de l'utilisateur STA et des paramètres de configuration actuels \(facultatif\) »](#). Ces valeurs doivent correspondre à la configuration des bibliothèques surveillées. Pour obtenir des instructions à ce sujet, reportez-vous à la section [Section 6.1.3, « Configuration des paramètres client SNMP pour STA »](#).
3. Pour restaurer la communication SNMP entre STA et les bibliothèques, testez la connexion de chaque bibliothèque surveillée. Pour obtenir des instructions, reportez-vous à la section [Section 6.1.5, « Test d'une connexion SNMP de bibliothèque »](#).

Remarque:

Une fois cette étape réussie, STA commence à recevoir et à traiter les données de chaque bibliothèque contrôlée.

Vous pourrez remarquer des échanges incomplets sur l'écran Exchanges Overview, qui sont les échanges en cours soit lorsque STA a été arrêté, soit lorsque les connexions aux bibliothèques ont été restaurées. Reportez-vous au guide *Guide de l'utilisateur STA* pour plus de détails sur les échanges incomplets.

4. Obtenez les dernières données de configuration SNMP de chaque bibliothèque. Pour obtenir des instructions à ce sujet, reportez-vous à la section [Section 6.1.6, « Exécution d'une collecte de données manuelle »](#).

8.6.10.3. Configuration des informations utilisateur et services STA

Suivez ces étapes pour toutes les mises à niveau. Ces étapes s'effectuent sur le serveur STA.

Si vous souhaitez conserver des paramètres de la version STA précédente, utilisez les valeurs enregistrées avant la mise à niveau ; voir l'étape [Section 8.5.3, « Enregistrement de l'utilisateur STA et des paramètres de configuration actuels \(facultatif\) »](#).

Remarque:

Après la mise à niveau, STA est propriétaire de tous les groupes logiques. La propriété de groupes logiques n'est pas critique pour le fonctionnement de STA, et tout utilisateur STA avec des privilèges d'opérateur ou d'administrateur peut modifier les groupes logiques.

1. Configurez les utilitaires de service STA Backup et STA Resource Monitor. Pour plus d'informations, reportez-vous à la section [Chapitre 7, Configuration des services STA](#).
2. Créez des noms d'utilisateur STA et mots de passe ; pour obtenir des instructions, reportez-vous au guide *Guide de l'utilisateur STA*. Vous pourrez également souhaiter :
 - Prévenir les utilisateurs des nouvelles exigences relatives au mot de passe pour STA 2.1.0.
 - Inviter les utilisateurs à ressaisir leurs préférences personnalisables, le cas échéant.
3. Si le serveur de messagerie STA requiert une authentification, vous devez saisir le nom d'utilisateur du compte de messagerie et son mot de passe ; pour obtenir des instructions, reportez-vous au guide *Guide de l'utilisateur STA*.
4. Restaurez la propriété originale des modèles personnalisés, le cas échéant ; pour obtenir des informations, reportez-vous au guide *Guide de l'utilisateur STA*.
5. Restaurez la propriété originale des stratégies de rapports exécutifs, le cas échéant ; pour obtenir des instructions, reportez-vous au guide *Guide de l'utilisateur STA*.

8.6.10.4. Mise hors service de l'ancien serveur STA (facultatif)

Cette méthode s'applique uniquement si vous avez utilisé la méthode de mise à niveau à deux serveurs. Vous pouvez utiliser cette procédure après avoir vérifié que le nouveau serveur STA fonctionne comme prévu.

1. Supprimez l'ancien serveur STA 1.0.x ou STA 2.0.x comme destinataire de déroutement de la configuration SNMP de chaque bibliothèque. Pour obtenir des instructions, reportez-vous au guide *Guide de l'utilisateur STA*.
2. Mettez hors service l'ancien serveur STA 1.0.x ou STA 2.0.x.

8.6.11. Récupération d'une mise à niveau de base de données ayant échoué (facultatif)

Prudence:

Suivez cette procédure uniquement sous la direction de votre représentant du support technique Oracle.

Suivez cette procédure uniquement si la mise à niveau de la base de données pendant la tâche [Section 8.6.9, « Tâche 8 : Mise à niveau de l'ancienne base de données » \[134\]](#) a échoué, et que les essais de répétition de la mise à niveau ont également échoué.

1. Répétez la tâche "[Tâche 7 : Traitement et chargement de l'ancienne base de données STA](#)" [132], de l'étape 6, jusqu'à la tâche "[Tâche 8 : Mise à niveau de l'ancienne base de données](#)" [134].

Si la mise à niveau échoue à nouveau, il est possible que la base de données se trouve dans un état inconnu ou endommagé, et vous devez restaurer la base de données dans son état d'origine juste après installation. Passez à l'étape suivante.

2. Supprimez la base de données mise à niveau et endommagée.

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

3. Passez à l'emplacement de la sauvegarde de la base de données STA et chargez le fichier de vidage de la base de données de la nouvelle installation que vous aviez créé pendant la tâche [Section 8.6.6, « Tâche 5 : Vidage de la nouvelle base de données STA \(facultatif\) » \[130\]](#).

Par exemple :

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

4. Effectuez la tâche [Section 8.6.9, « Tâche 8 : Mise à niveau de l'ancienne base de données » \[134\]](#).
5. Configurez STA en tant que nouvelle installation. Pour plus d'informations, reportez-vous aux sections suivantes :
 - [Chapitre 6, Configuration des connexions de bibliothèque dans STA](#)
 - [Chapitre 7, Configuration des services STA](#)

Désinstallation et restauration de STA

Ce chapitre se compose des sections suivantes :

- [Présentation de la désinstallation de STA](#)
- [Tâches de désinstallation de STA](#)

Prudence:

Oracle ne prend pas en charge une réduction de version de STA. Les données de base de données créées sous une version plus récente de STA seront perdues lors de l'installation d'une version antérieure de STA.

9.1. Présentation de la désinstallation de STA

Le programme de désinstallation de STA supprime l'application STA et toutes les données associées, ainsi que le logiciel Oracle. Les mises à jour suivantes sont apportées :

- Le sous-répertoire *StorageTek_Tape_Analytics* au sein de l'emplacement de Oracle Storage Home est entièrement supprimé. Les autres répertoires du l'emplacement de Oracle Storage Home ne sont pas affectés.
- Tous les journaux STA et MySQL sont supprimés de l'emplacement des journaux. Pour plus d'informations sur cet emplacement, reportez-vous à la section [Section 2.1.2, « Examen de la disposition du système de fichiers STA »](#).
- Tous les journaux de service STA sont supprimés.
- La base de données STA ainsi que toutes les sauvegardes locales sont supprimées. Si le répertoire de la base de données ou le répertoire des sauvegardes locales sont des points de montage ou comportent des fichiers définis par l'utilisateur, ces répertoires sont conservés ; sinon, ils sont supprimés.

L'emplacement de l'inventaire central Oracle n'est *pas* supprimé par la désinstallation de STA. Toutes les données de ce répertoire sont conservées, y compris les journaux d'installation et de désinstallation de STA et les informations d'inventaire du logiciel Oracle. Pour plus d'informations, reportez-vous à la section [Emplacement de l'inventaire central Oracle](#).

Le programme de désinstallation de STA est disponible en mode graphique et en mode silencieux. Pour plus d'informations, reportez-vous à la section [Section 3.5, « Modes du programme d'installation de STA »](#).

Pour plus d'informations sur les journaux de désinstallation de STA, reportez-vous à la section [Section 3.4, « Journaux d'installation et de désinstallation de STA »](#).

9.2. Tâches de désinstallation de STA

Les sections suivantes décrivent l'utilisation du programme de désinstallation de STA.

- [Section 9.2.1, « Désinstallation de STA »](#)
- [Section 9.2.2, « Vérification de la réussite de la désinstallation. »](#)
- [Section 9.2.3, « Restauration de STA »](#)

9.2.1. Désinstallation de STA

Suivez cette procédure pour désinstaller STA.

Prudence:

La désinstallation supprime toutes les données de la base de données STA. Effectuez un vidage complet de la base de données avant de commencer cette procédure. Pour obtenir des instructions à ce sujet, reportez-vous à la section [Section 8.6.1, « Tâche 1: Vidage de l'ancienne base de données STA »](#).

Remarque:

Pour désinstaller STA, vous devez vous connecter en tant que membre du groupe du programme d'installation Oracle. Vous ne pouvez pas désinstaller STA en tant qu'utilisateur *root* ni en tant qu'un autre utilisateur avec des privilèges de superutilisateur. Pour plus d'informations, reportez-vous à la section [Groupe d'installation Oracle](#).

1. Connectez-vous en tant qu'utilisateur du programme d'installation Oracle.
 2. Passez au répertoire de Oracle Storage Home. Par exemple :
- Pour le programme de désinstallation graphique de STA :

```
$ cd /Oracle
```

3. Passez au répertoire binaire du programme d'installation de STA.

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

4. Lancez le programme de désinstallation de STA avec l'une des commandes suivantes :
- Pour le programme de désinstallation graphique de STA :

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

Ce mode requiert un affichage X11. Pour obtenir des instructions à ce sujet, reportez-vous à la section [Annexe A, Référence d'écran Programme d'installation et de désinstallation graphique de STA](#).

- Pour le programme de désinstallation silencieux de STA :

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

Où *response_file* est le chemin absolu du fichier réponse précédemment créé.

Avant d'utiliser ce mode, vous devrez également avoir téléchargé le fichier *silentInstallUtility.jar* et créé un fichier réponse indiquant les options d'installation. Pour plus d'informations, reportez-vous à l'annexe [Annexe B, Programme d'installation et de désinstallation de STA en mode silencieux](#).

9.2.2. Vérification de la réussite de la désinstallation.

Suivez cette procédure pour vérifier que tous les composants STA ont été supprimés du serveur STA après désinstallation.

1. Connectez-vous en tant qu'utilisateur du programme d'installation Oracle.
2. Répertoriez le contenu du répertoire de Oracle Storage Home. Il doit être vide. Par exemple :

```
$ 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. Restauration de STA

Cette procédure permet de désinstaller puis de réinstaller STA (par exemple pour réparer une installation actuelle). Vous ne pouvez pas utiliser le programme d'installation de STA pour réinstaller ou écraser une installation actuelle.

1. Prenez un instantané du journal de service de l'installation actuelle de STA. Le support Oracle peut utiliser les journaux de service générés pour dépanner des problèmes éventuels existant avant la mise à niveau. Pour plus d'informations, reportez-vous au guide *Guide de l'utilisateur STA*.
2. Arrêtez tous les services STA :

```
# STA stop all
```

3. Effectuez un instantané de la base de données.
 - a. Démarrez le service MySQL.

```
# STA start mysql
```

- b. Créez un fichier de sauvegarde.

```
# /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
```

Le résultat obtenu est semblable au résultat suivant :

```
...
-- Retrieving view structure for table v_mdv_request_states...
-- Retrieving view structure for table version_info...
...
-- Disconnecting from localhost...
```

Remarque:

Si vous voyez le message "Can't connect to local MySQL server", alors le serveur MySQL n'est pas en cours d'exécution. Retournez à l'étape [a](#) pour vérifier que vous avez bien lancé MySQL.

4. Déplacez l'instantané de journal de service et l'instantané de base de données sur un serveur différent, car tous les fichiers STA seront supprimés à l'étape suivante. Les instantanés se trouvent dans les répertoires suivants :
 - L'instantané de journal de service est sous */Oracle_storage_home/Middleware/rda/snapshots*. Par exemple, */Oracle/Middleware/rda/snapshots*
 - L'instantané de base de données est à l'emplacement de la base de données indiqué pendant l'installation de STA. Par exemple, */dbbackup*
5. Sauvegardez d'autres fichiers si besoin.
6. Désinstallez STA Pour obtenir des instructions, reportez-vous à la section [Section 9.2.1, « Désinstallation de STA »](#).
7. Réinstallez STA Pour obtenir des instructions, reportez -vous au chapitre [Chapitre 3, Installation de STA](#).
8. Arrêtez tous les services STA :

```
# STA stop all
```

9. Restaurez la base de données. Pour obtenir des instructions, reportez-vous au guide *Guide d'administration de STA*.
10. Démarrez tous les services STA :

```
# STA start all
```

11. Configurez STA. Pour obtenir des instructions, reportez-vous à la section [Section 8.6.10.2, « Configurez les paramètres SNMP dans STA »](#).

Référence d'écran Programme d'installation et de désinstallation graphique de STA

Ce chapitre se compose des sections suivantes :

- [Configuration minimale requise pour l'affichage en mode graphique](#)
- [Ecrans de programme d'installation graphique de STA](#)
- [Ecrans de programme de désinstallation graphique de STA](#)

A.1. Configuration minimale requise pour l'affichage en mode graphique

Le programme d'installation et de désinstallation en mode graphique de STA requiert un système X Window, version 11 (X11). La configuration de X11 ne fait pas partie de ce guide, mais les consignes générales suivantes s'appliquent néanmoins. Pour plus d'informations, merci de contacter votre administrateur système.

Pour exécuter le programme d'installation et de désinstallation en mode graphique, le service X11 doit être en cours d'exécution sur le serveur STA, et configuré pour autoriser le transfert X11. Si Linux a été installé comme indiqué dans le chapitre [Chapitre 2, Installation de Linux](#), ces conditions doivent déjà être satisfaites.

En outre, l'affichage et les autorisations X11 doivent être correctement configurés pour l'utilisateur du programme d'installation Oracle. Ces paramètres sont différents selon que vous êtes connecté via une connexion locale ou distante.

Pour plus d'informations, reportez-vous aux sections suivantes :

- [Section A.1.1, « Connexions locales »](#)
- [Section A.1.2, « Connexions à distance avec un Secure Shell \(SSH\) »](#)
- [Section A.1.3, « Connexions distantes à l'aide du partage de bureau »](#)
- [Section A.1.4, « Dépannage des problèmes d'affichage graphique »](#)

Remarque:

Le temps de réponse des connexions distantes dépend de vos configurations et des performances réseau et VPN.

A.1.1. Connexions locales

Pour les connexions directes au serveur STA, vous devez vous connecter comme utilisateur du programme d'installation Oracle, puis définir manuellement la variable *DISPLAY*. Par exemple :

```
# export DISPLAY=hostname:0.0
```

Il est aussi possible que vous deviez vérifier que l'utilisateur du programme d'installation Oracle dispose de la bonne autorisation X11. Contactez votre administrateur Linux pour obtenir de l'aide.

A.1.2. Connexions à distance avec un Secure Shell (SSH)

Si vous utilisez un Secure Shell (SSH) avec transfert X11 activé, l'autorisation et l'affichage seront automatiquement gérés pour l'utilisateur connecté. Par exemple, si vous utilisez cette méthode et que vous vous connectez en tant que l'utilisateur *oracle*, le service SSH du serveur STA configure automatiquement la bonne autorisation X11 et s'affiche pour l'utilisateur *oracle*. Vous ne devez pas définir la variable *DISPLAY* manuellement.

Cependant, si vous vous connectez comme utilisateur différent (*root*, par exemple), puis comme *su* et utilisateur *oracle*, l'affichage et les autorisations X11 ne seront pas correctement configurés pour l'utilisateur *oracle*, vous devez alors les définir manuellement. Les instructions pour effectuer ces opérations se font pas l'objet de ce guide, contactez votre administrateur Linux pour obtenir de l'aide.

A.1.2.1. Connexion depuis une machine Linux

Pour permettre le transfert X11 sur une machine Linux, utilisez la commande *ssh* avec l'option *-X* ou *-Y*. Par exemple :

```
$ ssh -X oracle@sta_server
```

A.1.2.2. Connexion depuis un ordinateur Microsoft Windows

Votre ordinateur doit exécuter un serveur X11, tel que Xming ou Cygwin/X, et un client SSH, tel que PuTTY ou WinSCP. Ci-après une procédure-type de connexion avec PuTTY :

1. Vérifiez que le serveur X11 est en cours d'exécution sur votre PC. Contactez votre administrateur système pour obtenir de l'aide, si nécessaire.
2. Lancez PuTTY et procédez comme suit :
 - a. Dans la fenêtre de session principale, saisissez les entrées suivantes :
 - Dans le champ **Host Name**, saisissez le nom ou l'adresse IP du serveur STA.
 - Dans le champ **SSH Connection type**, sélectionnez **SSH**.
 - b. Dans l'arborescence du menu Category, développez **Connection**, puis **SSH**, et sélectionnez **X11**. Dans cette fenêtre, effectuez les sélections suivantes :

- Dans le champ **X11 forwarding**, sélectionnez la case **Enable X11 forwarding**.
- Dans le champ **Remote X11 authentication protocol**, sélectionnez **MIT-Magic-Cookie-1**.
- Laisser les autres champs vides.

A.1.3. Connexions distantes à l'aide du partage de bureau

Pour exécuter le programme d'installation de STA à l'aide du partage de bureau, le serveur STA comme l'ordinateur local doivent exécuter une application de partage de bureau, telle que VNC Server sur le serveur STA et VNC Viewer sur l'ordinateur local. En outre, votre ordinateur local doit pouvoir se connecter au serveur STA via un réseau privé, tel qu'un réseau privé virtuel (VPN).

Ci-après une procédure-type de connexion avec VNC :

1. Installez et configurez le serveur VNC sur le serveur STA.
2. Installez et configurez VNC Viewer sur votre ordinateur local.
3. Connectez-vous au serveur STA via le réseau privé. Contactez votre administrateur pour plus d'instructions.

A.1.4. Dépannage des problèmes d'affichage graphique

Le programme d'installation et de désinstallation de STA vérifiera que X11 est correctement configuré pour l'utilisateur du programme d'installation Oracle. Si la vérification des conditions requises échoue, contactez votre administrateur système Linux pour obtenir de l'aide. Procédez comme suit pour faciliter le dépannage des problèmes.

1. Connectez-vous au serveur STA en tant qu'utilisateur du programme d'installation Oracle, et affichez les packages RPM alors installés.

```
# yum list installed
```

L'entrée *xorg - x11 - util* doit faire partie de la liste affichée. Par exemple :

```
xorg-x11-utils.x86_64          7.5-6.e16
```

2. Affichez les paramètres d'affichage actuels pour l'utilisateur du programme d'installation Oracle. Par exemple :

```
$ echo $DISPLAY
:0.0
```

3. Vérifiez que l'affichage dispose de la bonne configuration X11. Par exemple :

```
$ xdpinfo -display :0.0
```

L'exemple [Exemple A.1, « Exemple d'affichage avec X11 correctement configuré »](#) est un exemple de la première partie de la sortie de commande, montrant un affichage correctement configuré.

Exemple A.1. Exemple d'affichage avec X11 correctement configuré

```
$ 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
...
```

L'exemple [Exemple A.2, « Exemple d'affichages avec X11 mal configuré »](#) présente certaines sorties de commande d'affichages qui ne sont pas correctement configurés.

Exemple A.2. Exemple d'affichages avec X11 mal configuré

```
$ 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. Ecrans de programme d'installation graphique de STA

Cette section fournit une référence détaillée de chaque écran du programme d'installation graphique de STA.

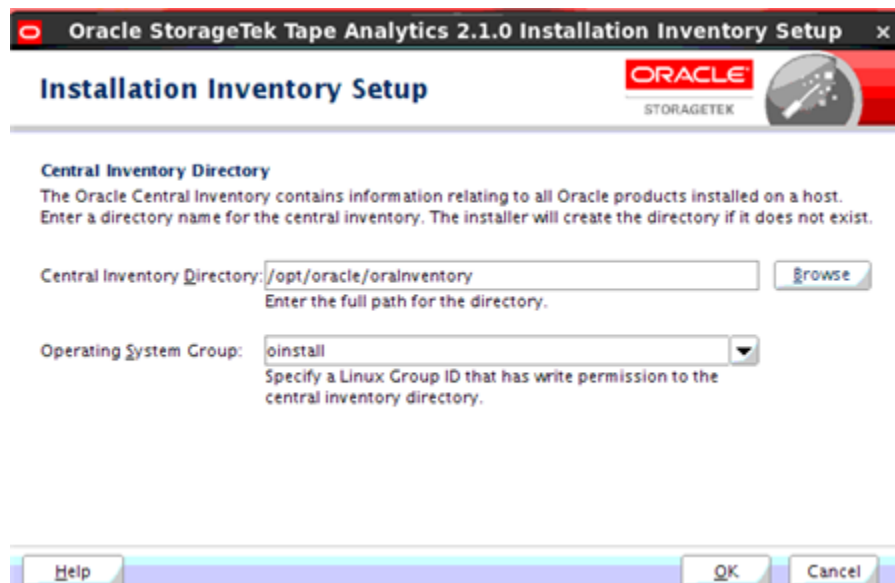
- [Section A.2.2, « Accueil »](#)
- [Section A.2.3, « Emplacement de l'installation »](#)
- [Section A.2.4, « Vérifications des prérequis »](#)
- [Section A.2.5, « Entrez le mot de passe root »](#)
- [Section A.2.6, « Configuration des répertoires de base de données »](#)
- [Section A.2.7, « Configuration des comptes administrateurs »](#)
 - [Section A.2.8, « Administrateur WebLogic »](#)
 - [Section A.2.9, « Administrateur STA »](#)
- [Section A.2.10, « Configuration des comptes de base de données »](#)
 - [Section A.2.11, « Utilisateur root de base de données »](#)
 - [Section A.2.12, « Utilisateur de l'application de base de données »](#)

- Section A.2.13, « Utilisateur des rapports de base de données »
- Section A.2.14, « Administrateur de bases de données »
- Section A.2.15, « Saisir les ports de communication »
 - Section A.2.16, « Console d'administration WebLogic »
 - Section A.2.17, « Moteur STA »
 - Section A.2.18, « Adaptateur STA »
 - Section A.2.19, « Interface utilisateur STA »
- Section A.2.20, « Agent de diagnostic »
- Section A.2.21, « Récapitulatif de l'installation »
- Section A.2.22, « Progression de l'installation »
- Section A.2.23, « Progression de la configuration »
- Section A.2.24, « Installation terminée »

Remarque:

Lorsque vous lancez le programme d'installation graphique de STA, Oracle Universal Installer présente les messages dans la fenêtre de terminal, tandis qu'il effectue certaines vérifications de base de l'environnement. Les conditions requises pour exécuter le programme d'installation graphique de STA peuvent dépasser ces vérifications de base.

A.2.1. Configuration d'inventaire et d'installation



Le répertoire d'inventaire central Oracle sert à suivre les noms et emplacements de tous les logiciels Oracle installés sur ce serveur. Tous les journaux d'installation et de désinstallation de STA y sont automatiquement enregistrés.

Pour garantir que les autres utilisateurs du groupe d'installation Oracle ont accès à ce répertoire, il doit être distinct du répertoire personnel de l'utilisateur du programme

d'installation Oracle. Les répertoires personnels peuvent ne pas avoir les accès corrects pour le groupe d'installation Oracle.

Cet écran fait partie de Oracle Universal Installer. En suivant les pratiques recommandées pour inscrire l'emplacement de l'inventaire central Oracle, cet écran apparaîtra uniquement lors de votre première installation de STA sur ce serveur. Les installations ultérieures trouveront automatiquement le répertoire sans avoir à vous le demander. Pour plus d'informations, reportez-vous à la section [Section 3.6.7, « Inscrivez l'emplacement de l'inventaire central Oracle »](#).

A.2.1.1. Champs de l'écran

Inventory Directory

Saisissez le nom du répertoire que vous souhaitez désigner comme répertoire de l'inventaire central Oracle.

Par défaut, il sera sous `$USER_HOME/oraInventory`. Vous devez indiquer un chemin absolu, ou cliquer sur le bouton **Browse** puis accéder à un répertoire.

- Si vous indiquez un répertoire existant, l'utilisateur du programme d'installation Oracle doit avoir toutes les permissions d'accès.
- Si vous indiquez un emplacement de répertoire qui n'existe pas, le programme d'installation le créera automatiquement si l'utilisateur du programme d'installation Oracle dispose de toutes les permissions d'accès au répertoire parent.

Operating System Group

Sélectionnez le groupe Linux que vous souhaitez désigner comme groupe d'installation Oracle. Tous les membres de ce groupes pourront installer le logiciel Oracle sur ce serveur.

Le menu répertorie tous les groupes auquel l'utilisateur du programme d'installation Oracle appartient. Par défaut, il s'agira du groupe principal de l'utilisateur du programme d'installation Oracle.

A.2.1.2. Boutons spécifiques à l'écran

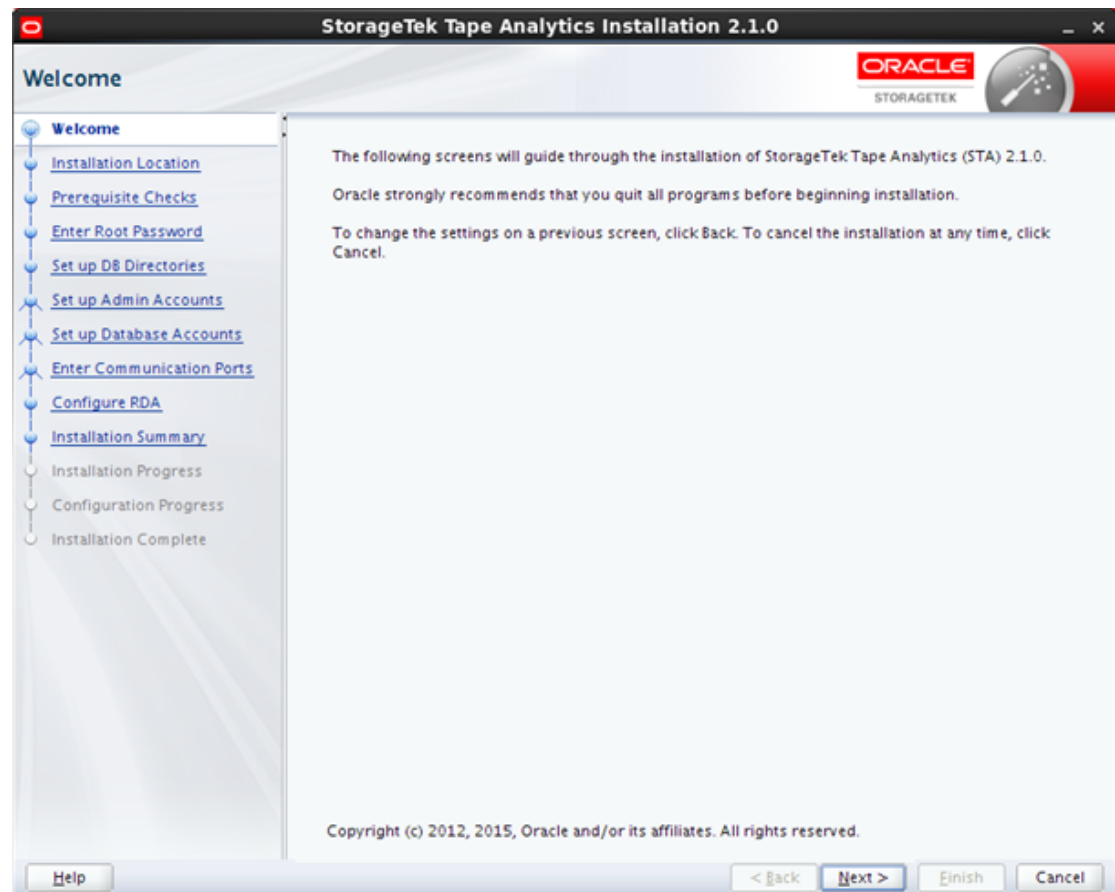
Browse

Cliquez pour vous rendre vers le répertoire que vous souhaitez indiquer.

OK

Cliquez pour lancer le programme d'installation de STA. La fenêtre Installation Inventory Setup disparaît, et un léger décalage peut se produire avant l'affichage de l'écran de démarrage du programme d'installation de STA.

A.2.2. Accueil



Cet écran présente certaines informations générales relatives à l'exécution du programme d'installation de STA. Lisez le texte, puis cliquez sur **Next** pour commencer l'installation.

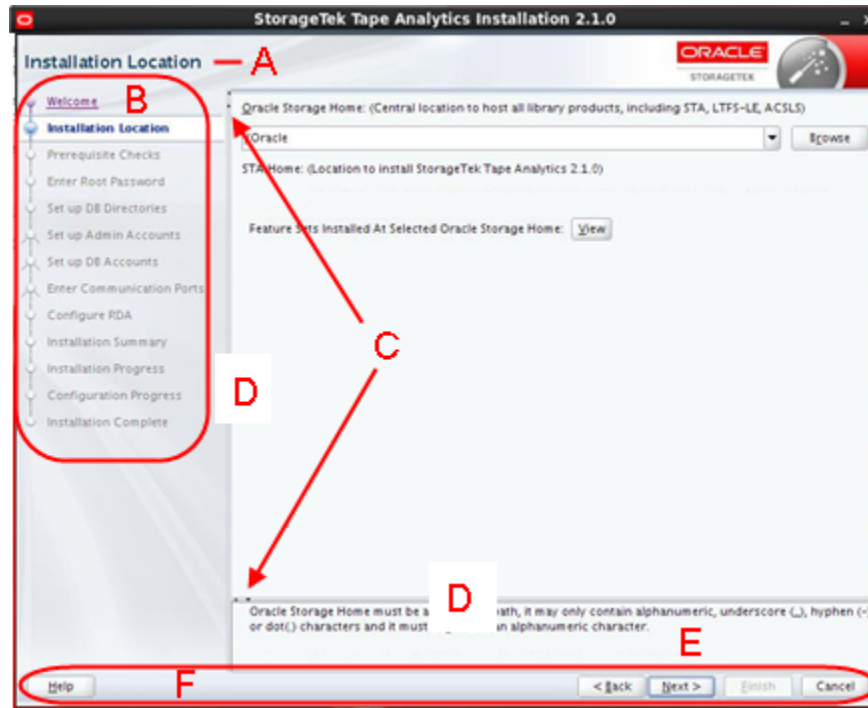
Remarque:

Les modifications apportées au système ne sont pas mises en oeuvre avant d'avoir terminé tous les écrans d'entrée du programme d'installation de STA et cliqué sur **Install** dans le récapitulatif [Section A.2.21, « Récapitulatif de l'installation »](#). A tout moment avant cette étape finale, vous pouvez retourner à un écran précédent et modifier vos saisies.

Pour plus d'informations sur les écrans du programme d'installation de STA, reportez-vous à la section [Section A.2.2.1, « Présentation générale de l'écran du programme d'installation »](#).

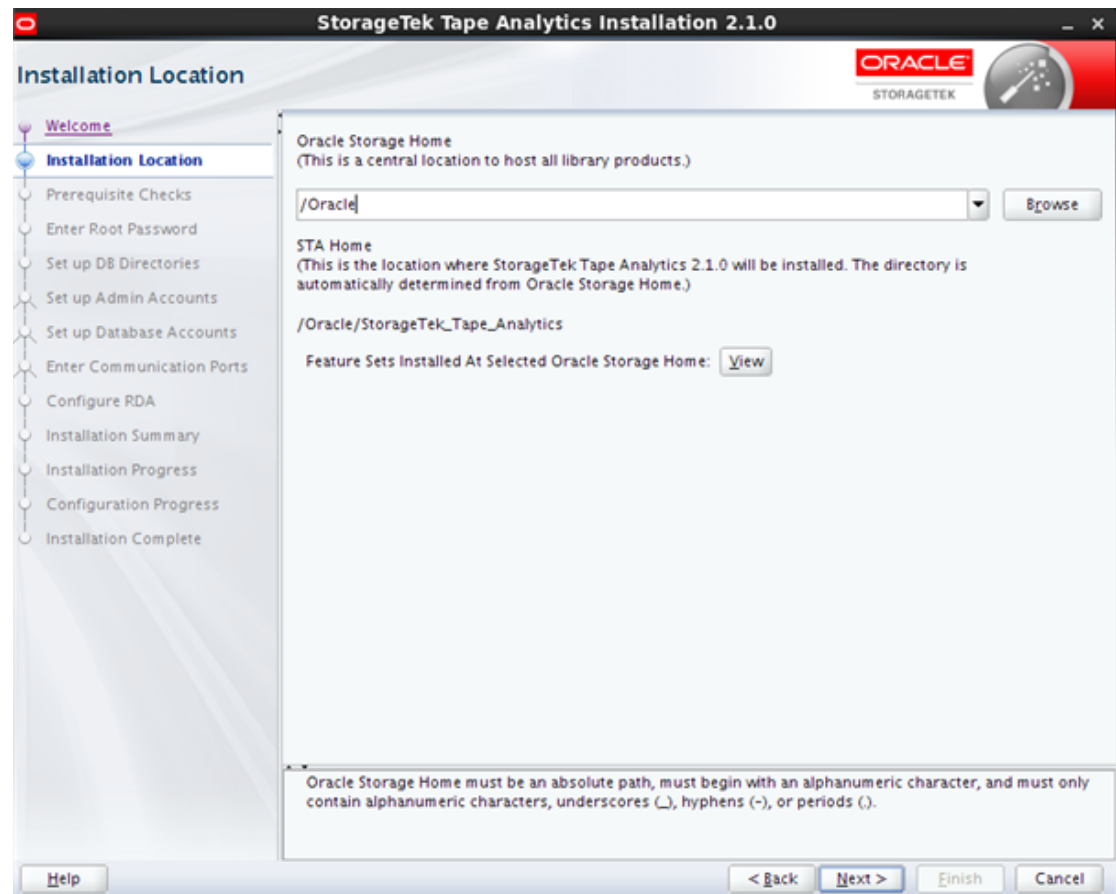
A.2.2.1. Présentation générale de l'écran du programme d'installation

Tous les écrans du programme d'installation de STA suivent la même présentation de base. Leurs parties principales sont illustrées et décrites ci-dessous.



Elément	Nom	Description
A	Titre de l'écran	Titre de l'écran du programme d'installation de STA
B	Arborescence de navigation	Présente votre progression dans la séquence d'installation. Les titres d'écran deviennent des liens actifs lorsque vous terminez chaque écran. Vous pouvez cliquer sur un lien actif pour retourner directement à l'écran souhaité pour vérifier ou modifier vos saisies
C	Icônes Développer et Réduire	Cliquez pour cacher ou afficher l'arborescence de navigation et le volet Message.
D	Barre de contrôle Redimensionner	Cliquez et faites glisser pour redimensionner l'arborescence de navigation ou le volet Message.
D	Volet Message	Uniquement sur les écrans sélectionnés. Affiche les messages d'état concernant les processus effectués sur cet écran.
E	Boutons communs	Les boutons suivants sont communs à tous les écrans du programme d'installation de STA : <ul style="list-style-type: none"> • Help : Cliquer pour afficher l'aide contextuelle de l'écran. • Back : Cliquer pour retourner à l'écran précédent pour vérifier ou modifier vos saisies. Vous pouvez retourner jusqu'au début de l'installation, écran après écran. • Next : Cliquer pour accéder à l'écran suivant après avoir saisi les entrées requises. • Finish : Cliquer pour terminer l'installation. Ce bouton n'est actif que sur l'écran final. • Cancel : Cliquer pour annuler l'installation à tout moment. Si une partie de l'installation a été effectuée, le programme d'installation annulera l'installation et renverra le serveur dans son état d'origine. Vous serez invité à confirmer l'annulation.

A.2.3. Emplacement de l'installation



Cet écran vous permet d'indiquer l'emplacement d'installation sur le serveur de STA et de tous les logiciels Oracle associés.

Il est impossible d'installer STA sur une version précédemment installée. Pour vérifier que STA n'est pas déjà installé dans un emplacement précis, vous pouvez entrer un répertoire dans le champ **Oracle Storage Home** puis cliquer sur le bouton **View**.

- Si aucun logiciel n'est installé à cet emplacement, la liste sera vide.
- Si un logiciel a été installé, il sera répertorié, comme présenté sur la capture d'écran [Figure A.1, « Exemple de liste de Oracle Storage Home »](#).

A.2.3.1. Champs de l'écran

Oracle Storage Home

Entrez le répertoire où installer STA et logiciels Oracle associés. Chaque package logiciel sera installé sur son propre sous-répertoire dans ce répertoire. Vous ne pouvez pas indiquer un répertoire où STA est déjà installé.

Pour obtenir les recommandations techniques relatives à ce répertoire, reportez-vous au tableau [Tableau 2.2, « Disposition du système de fichiers recommandée »](#).

Selon que ce répertoire existe déjà ou non, l'utilisateur et le groupe du programme d'installation Oracle doivent disposer des droits d'accès suivants :

- Si le répertoire n'existe pas, les droits d'accès doivent être complets.
- Si le répertoire n'existe pas, les droits d'accès au répertoire parent doivent être complets, afin que le programme d'installation de STA puisse créer le répertoire Oracle Storage Home.

Vous devez saisir un chemin d'accès absolu ou cliquer sur **Browse** pour accéder au répertoire que vous souhaitez indiquer.

STA Home

Ce champ est en lecture seule. Il s'agit du sous-répertoire sous Oracle Storage Home où STA sera installé. *StorageTek_Tape_Analytics* sera le nom affecté à ce sous-répertoire, et sera créé automatiquement pendant l'installation.

A.2.3.2. Boutons spécifiques à l'écran

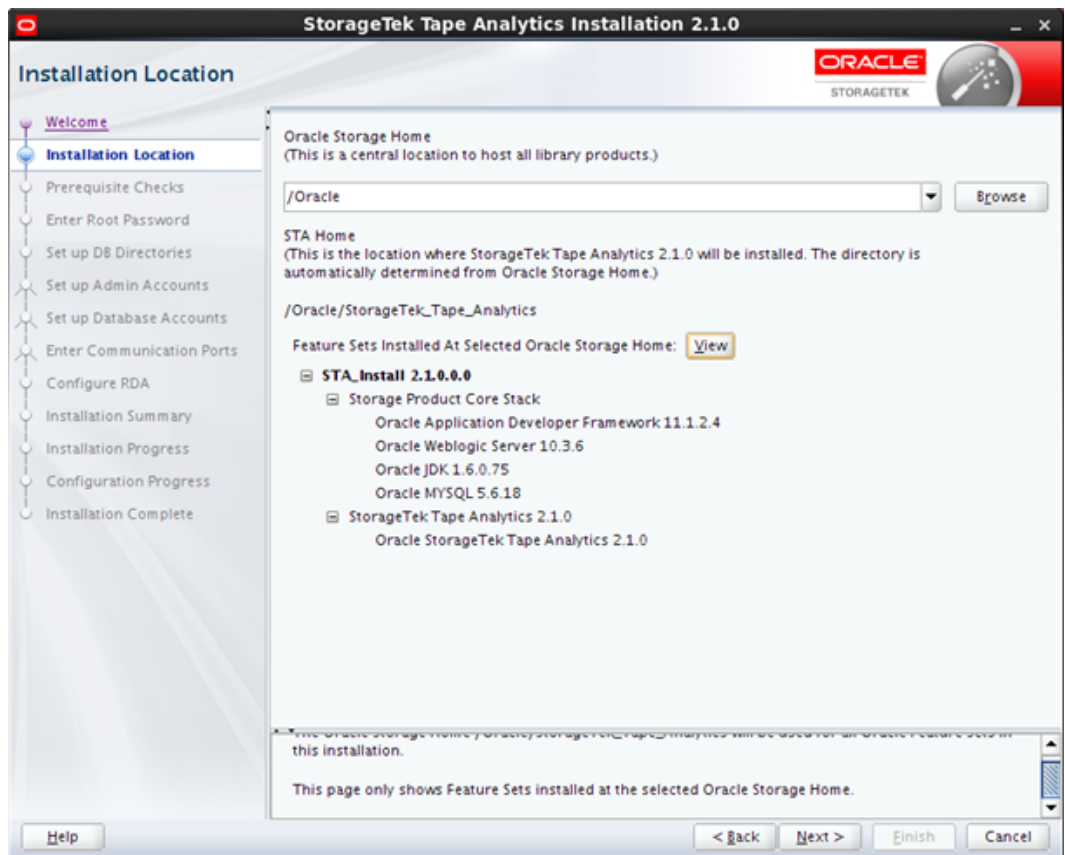
Browse

Cliquez pour vous rendre vers le répertoire que vous souhaitez indiquer.

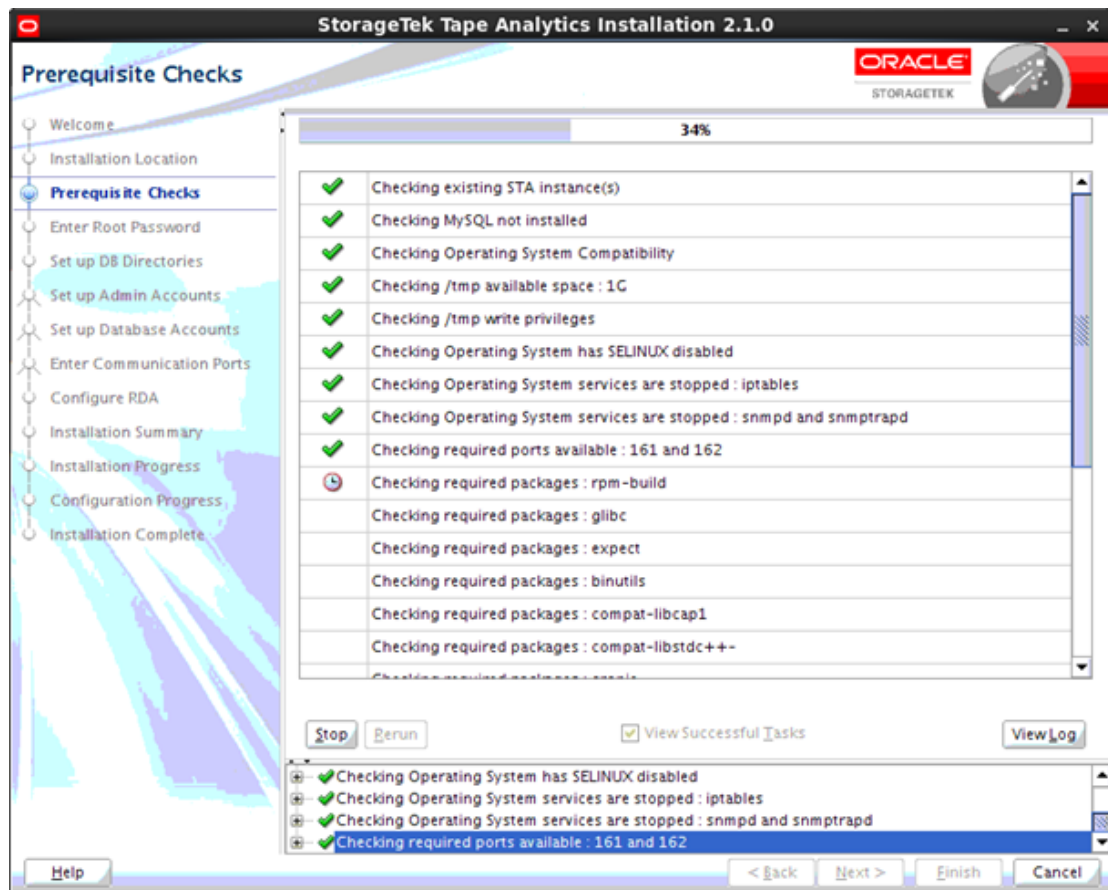
View/

Cliquez pour afficher une liste de tous les logiciels déjà installés sur le répertoire Oracle Storage Home que vous avez indiqué. Pour les nouvelles installations, la liste est vide. La capture d'écran [Figure A.1, « Exemple de liste de Oracle Storage Home »](#) est un exemple d'affichage après l'installation de STA.

Figure A.1. Exemple de liste de Oracle Storage Home






A.2.4. Vérifications des prérequis



Le programme d'installation effectue une série de tâches pour vérifier que l'environnement du serveur répond à tous les prérequis recommandés et requis. Ce processus peut durer plusieurs minutes.

Les résultats possibles de chaque vérifications sont les suivants :

- Succès  — Le prérequis est correct.
- Avertissement  — Le prérequis recommandé est incorrect.
- Echec  — Le prérequis obligatoire est incorrect.

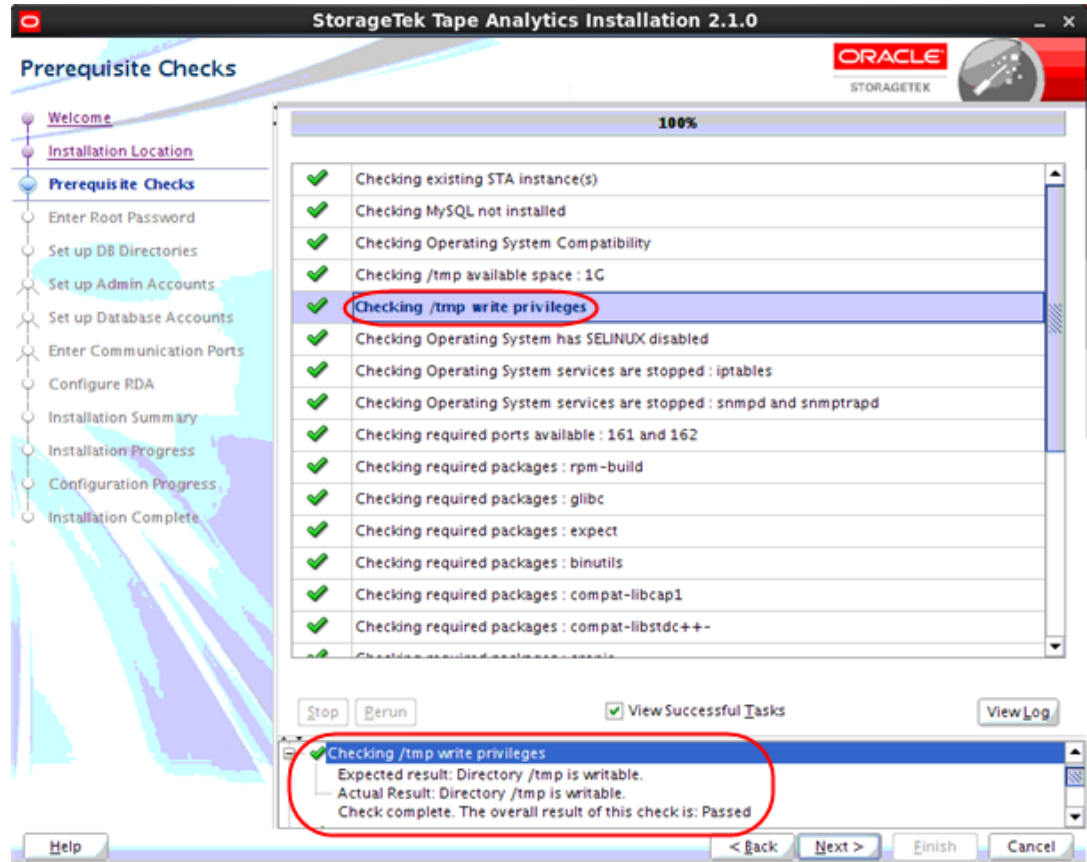
Vous ne pouvez pas poursuivre l'installation en cas d'échec. En outre, il est recommandé de résoudre tous les avertissements avant de poursuivre. Il est possible de conserver le programme d'installation à l'écran pendant la résolution des problèmes, puis de retourner cliquer sur **Rerun** pour exécuter le processus de vérification une nouvelle fois.

Selon la nature du prérequis, il pourra être nécessaire d'arrêter un service, de modifier les privilèges utilisateur, ou d'installer un package Yum pour résoudre les problèmes. Vous

pouvez utiliser l'une des méthodes suivantes pour afficher les détails vous facilitant la résolution des problèmes et la détermination des actions à mener :

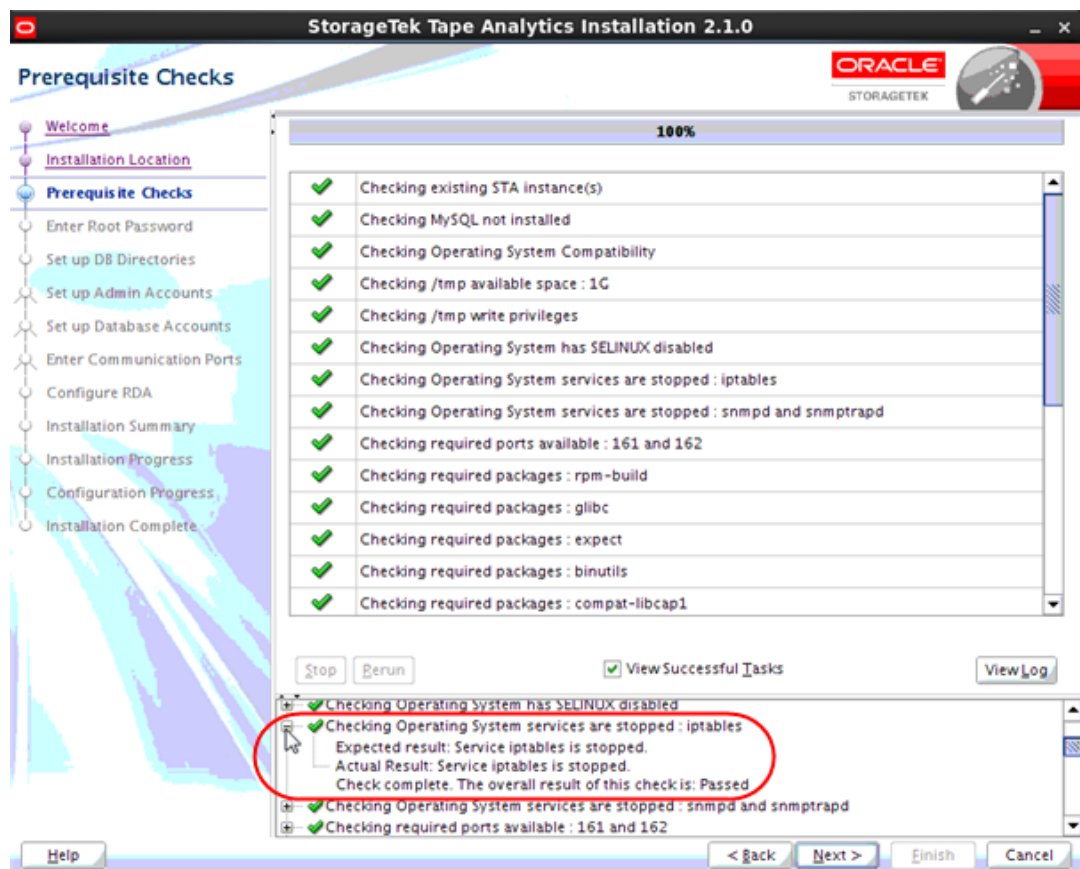
- Sélectionnez la tâche dans la fenêtre principale. La tâche est surlignée dans le volet Message, avec les détails développés. La capture d'écran [Figure A.2, « Détail de tâche affiché en sélectionnant la tâche dans la fenêtre principale. »](#) en est un exemple.

Figure A.2. Détail de tâche affiché en sélectionnant la tâche dans la fenêtre principale.



- Dans le volet Message, cliquez sur l'icône **Expand (+)** à côté de la tâche dont vous souhaitez afficher le détail. La capture d'écran [Figure A.3, « Détail de tâche affiché en sélectionnant l'icône Expand. »](#) en est un exemple. Cliquez sur l'icône **Collapse (-)** pour masquer le détail.

Figure A.3. Détail de tâche affiché en sélectionnant l'icône Expand.



A.2.4.1. Champs de l'écran

Aucun

A.2.4.2. Boutons spécifiques à l'écran

Stop

Cliquez pour arrêter le processus de vérification à la tâche courante. Vous pourrez souhaiter le faire pour afficher les détails d'une tâche sélectionnée qui est déjà terminée.

Rerun

Cliquez pour effectuer un nouveau processus de vérification depuis le départ. Cela vous permet de résoudre toute sortie d'échec ou d'avertissement sans avoir à quitter et à redémarrer le programme d'installation de STA.

View Successful Tasks

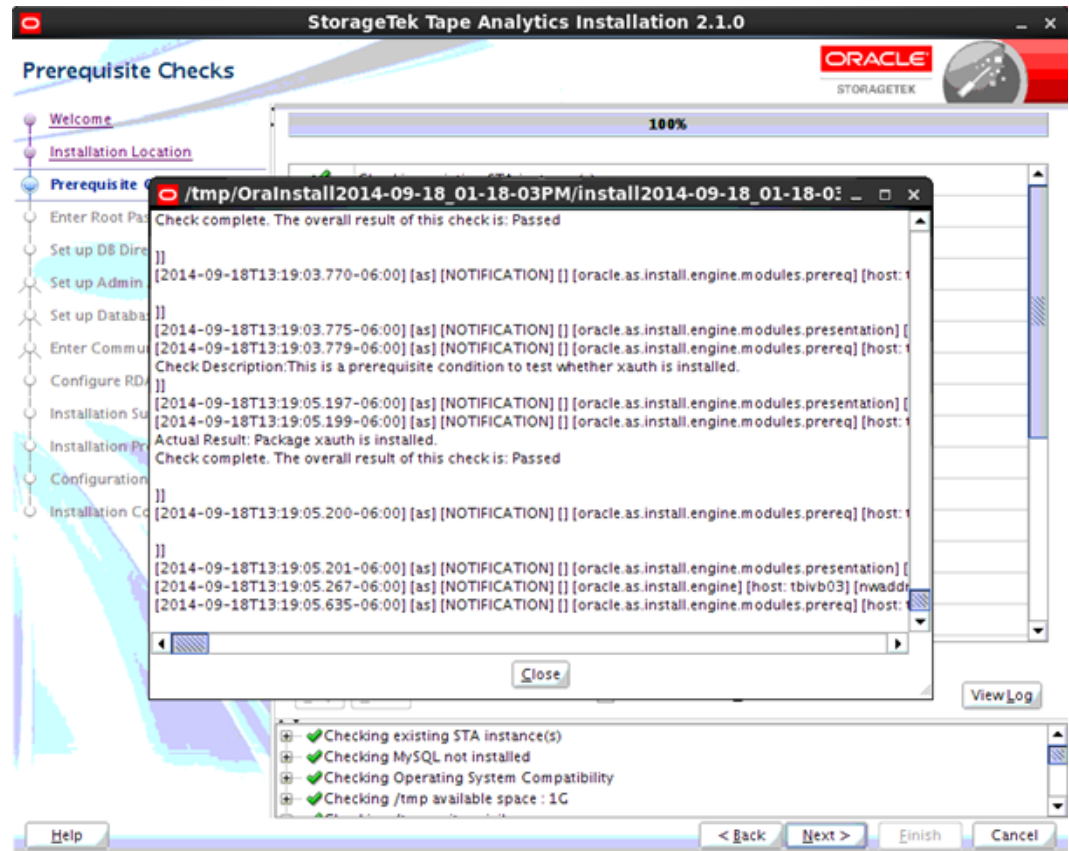
Sélectionnez la case pour inclure les sorties Succès ; cette case est cochée par défaut.

Décochez la case pour n'afficher que les sorties d'échec ou d'avertissement. Cela vous permet d'exclure les tâches réussies pour vous concentrer sur celles requérant votre attention.

View Log

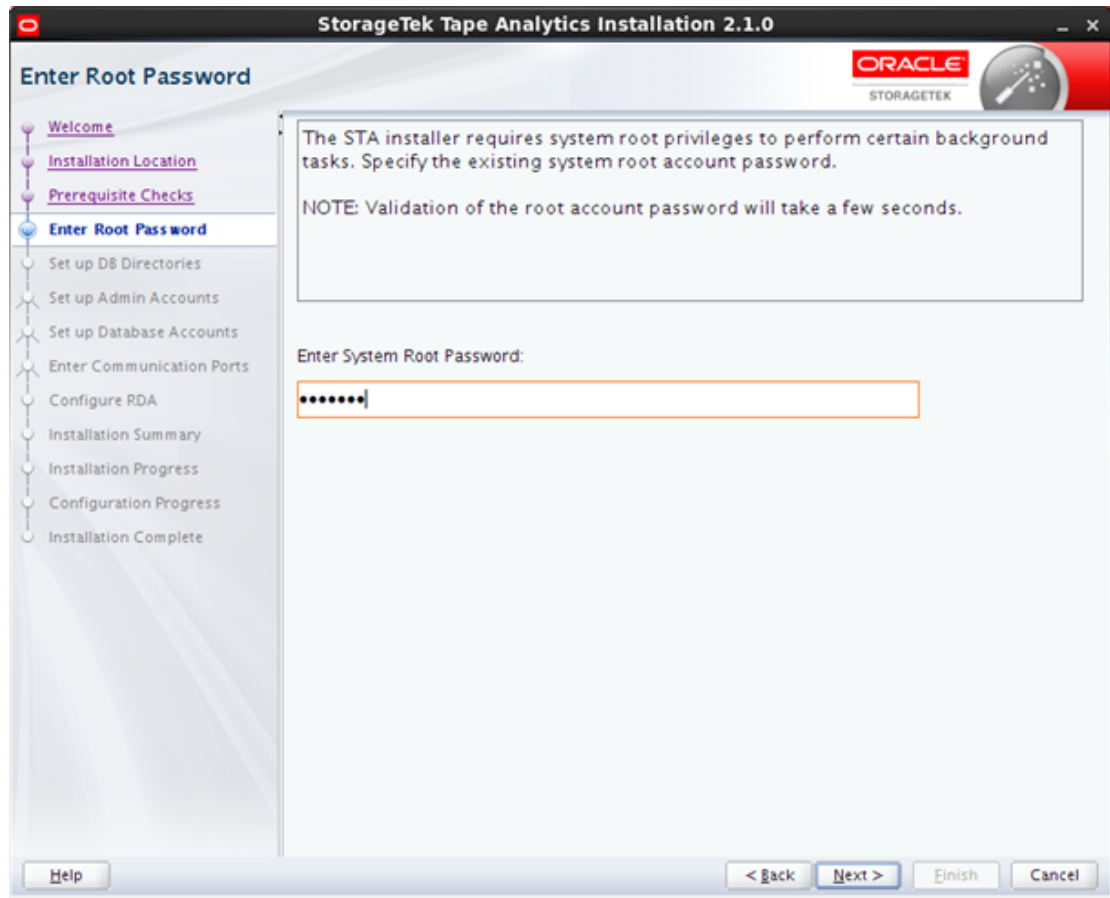
Cliquez pour afficher le journal de vérification des prérequis dans une fenêtre distincte. La capture d'écran [Figure A.4, « Exemple d'affichage de journal de vérification des prérequis »](#) en est un exemple. Cliquez sur **Close** pour fermer la fenêtre du journal.

Figure A.4. Exemple d'affichage de journal de vérification des prérequis



Il est aussi possible de voir le journal depuis la ligne de commande Linux. Pendant que le programme d'installation est en cours d'exécution, les journaux sont conservés dans un sous-répertoire sous */tmp*. Pour plus d'informations, reportez-vous à la section [Section 3.4, « Journaux d'installation et de désinstallation de STA »](#).

A.2.5. Entrez le mot de passe root



Le programme d'installation de STA requiert l'accès root Linux pour effectuer l'installation.

A.2.5.1. Champs de l'écran

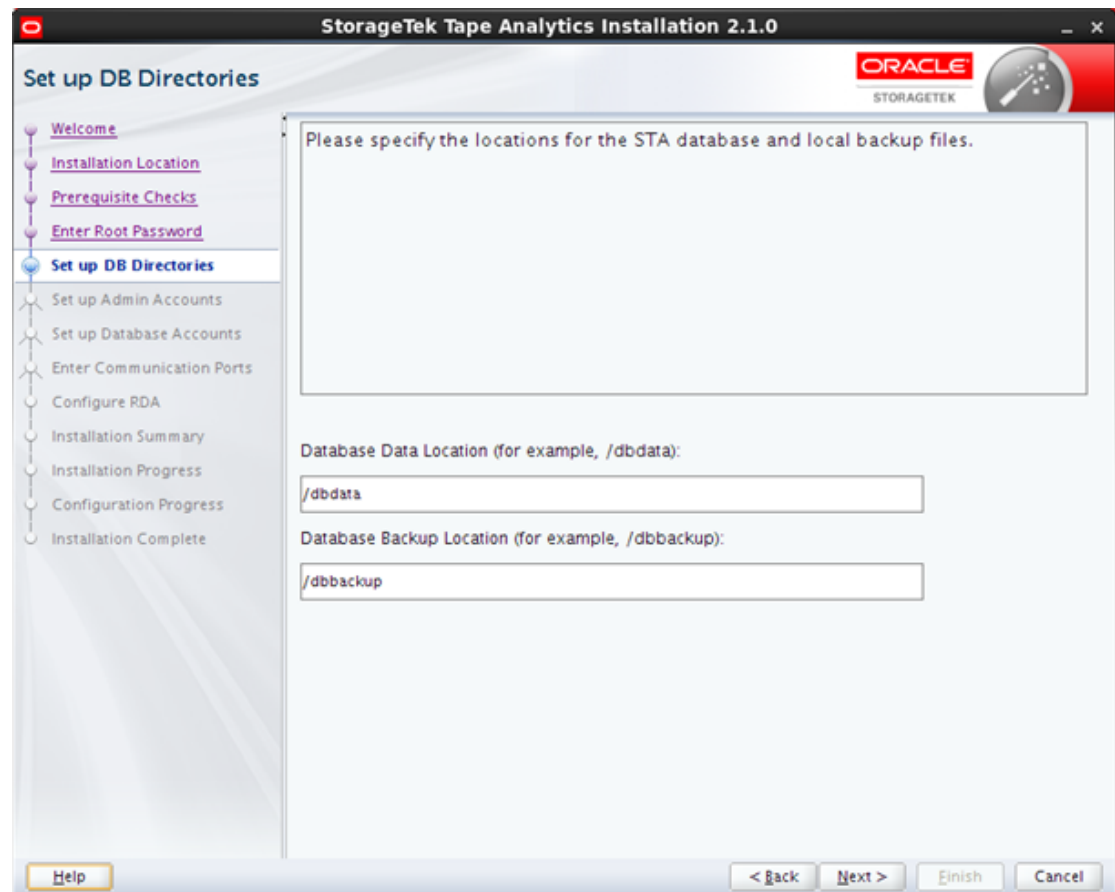
Enter Root Password

Saisir le mot de passe de l'utilisateur root Linux. La valeur saisie est masquée. La validation du mot de passe peut prendre quelques secondes.

A.2.5.2. Boutons spécifiques à l'écran

Aucun

A.2.6. Configuration des répertoires de base de données



Cet écran vous permet d'indiquer des emplacements spécifiques pour la base de données STA et les sauvegardes de la base de données STA. Le programme d'installation de STA créera ces répertoires s'ils n'existent pas déjà.

Pour plus d'informations sur la gestion des services et sauvegardes de bases de données, reportez-vous au guide *Guide d'administration de STA*.

A.2.6.1. Champs de l'écran

Database Data Location

Saisir le répertoire où se trouvera la base de données STA. Ce répertoire ne peut pas être le même que **l'emplacement des sauvegarde de la base de données**. Vous devez indiquer un chemin absolu.

Si le répertoire que vous indiquez comporte déjà un sous-répertoire de base de données (*mysql*), un message d'avertissement s'affichera. Vous pouvez soit indiquer un emplacement de base de données différent, soit accepter l'emplacement actuel, auquel cas le sous-répertoire de la base de données sera supprimé pendant l'installation de STA.

Database Backup Location

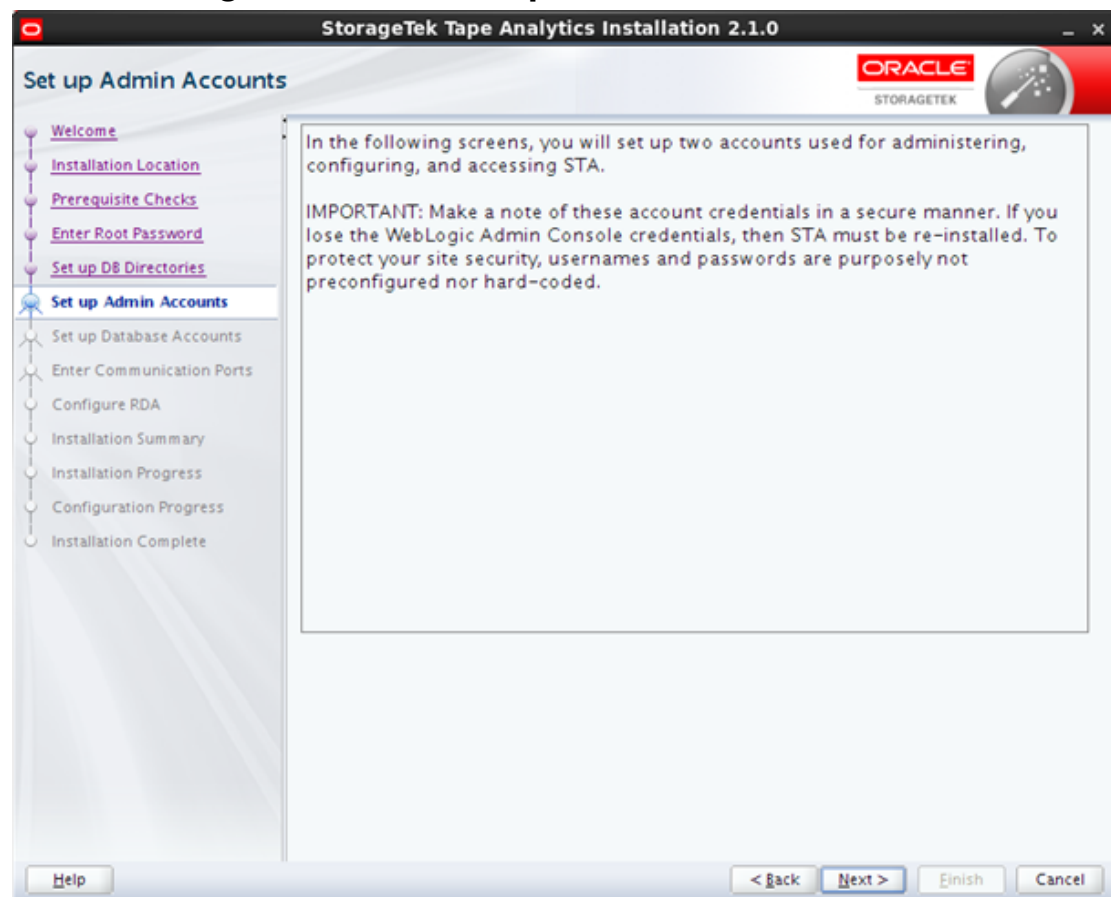
Saisissez le répertoire du serveur sur lesquelles seront situées les sauvegardes de la base de données STA. Le répertoire ne peut pas être le même que **l'emplacement des données de la base de données**. Vous devez indiquer un chemin absolu.

Si le répertoire que vous indiquez contient déjà un sous-répertoire de sauvegarde de base de données (*local*), un message d'avertissement apparaîtra. Vous pouvez soit indiquer un emplacement de sauvegarde différent, soit accepter l'emplacement actuel, auquel cas le sous-répertoire de la sauvegarde sera supprimé pendant l'installation de STA.

A.2.6.2. Boutons spécifiques à l'écran

Aucun

A.2.7. Configuration des comptes administrateurs



Cet écran décrit les types d'informations que vous définirez sur les deux prochains écrans. Lire le texte, puis cliquer sur **Next** pour continuer.

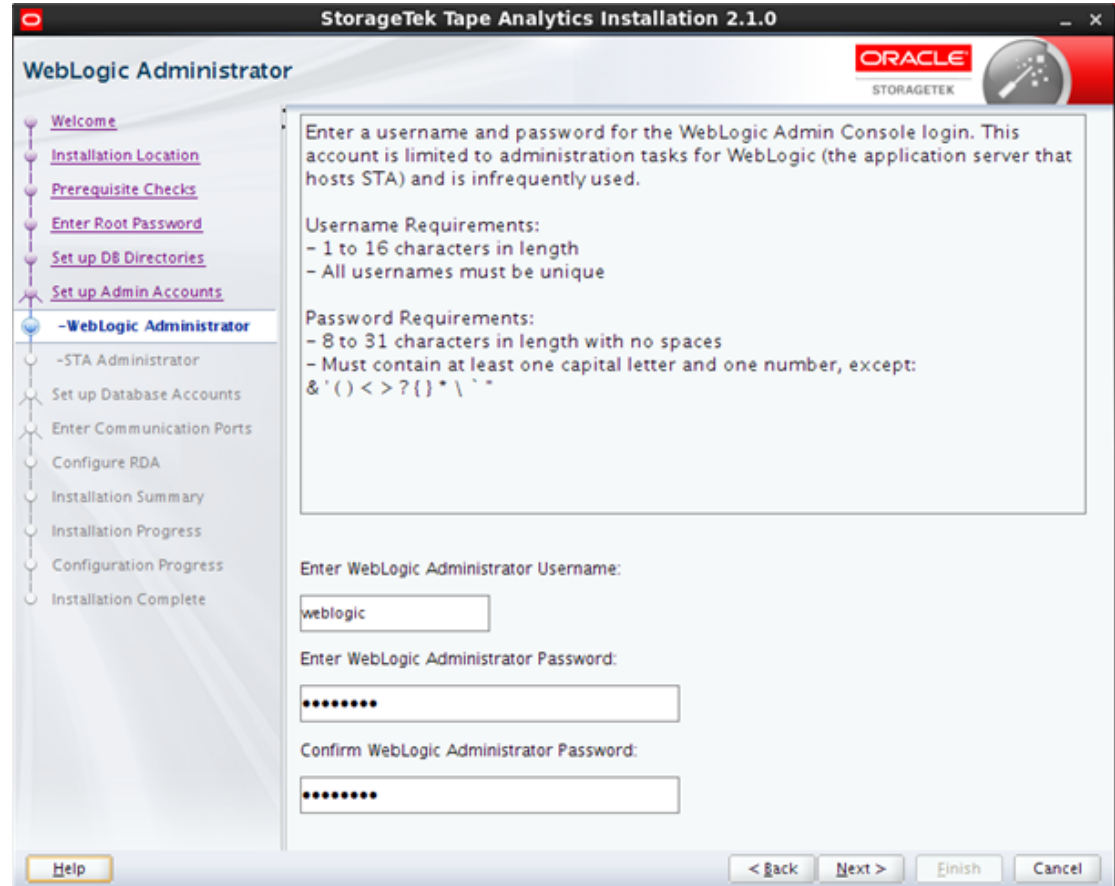
A.2.7.1. Champs de l'écran

Aucun

A.2.7.2. Boutons spécifiques à l'écran

Aucun

A.2.8. Administrateur WebLogic



WebLogic est le serveur d'applications hébergeant STA. Vous utilisez le compte administrateur WebLogic pour vous connecter à la console d'administration WebLogic pour configurer et gérer le serveur WebLogic. Ce compte est rarement utilisé.

Ce compte sera créé pendant l'installation avec les identifiants de connexion que vous indiquerez.

Prudence:

Enregistrez ces identifiants de connexion en toute sécurité ; si vous lez perdez, vous ne pourrez plus vous connecter à la console d'administration WebLogic et STA devra être réinstallé.

Afin de protéger la sécurité de votre site, les noms d'utilisateurs et les mots de passe ne sont, à dessein, ni préconfigurés ni codés.

A.2.8.1. Champs de l'écran

Enter Username

Saisissez le nom que vous souhaitez affecter au compte administrateur WebLogic.

Les conditions du nom d'utilisateur requises sont les suivantes :

- Il doit comporter entre 1 et 16 caractères.
- Tous les noms d'utilisateur doivent être uniques.

Enter Password

Saisissez le mot de passe que vous souhaitez affecter à ce compte. La valeur saisie est masquée.

Les conditions requises en termes de mot de passe sont les suivantes :

- Il doit comporter entre 8 et 31 caractères.
- Il doit comporter au moins un chiffre et une majuscule
- Il ne doit pas comporter d'espace
- Il ne doit pas comporter les caractères spéciaux suivants :

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

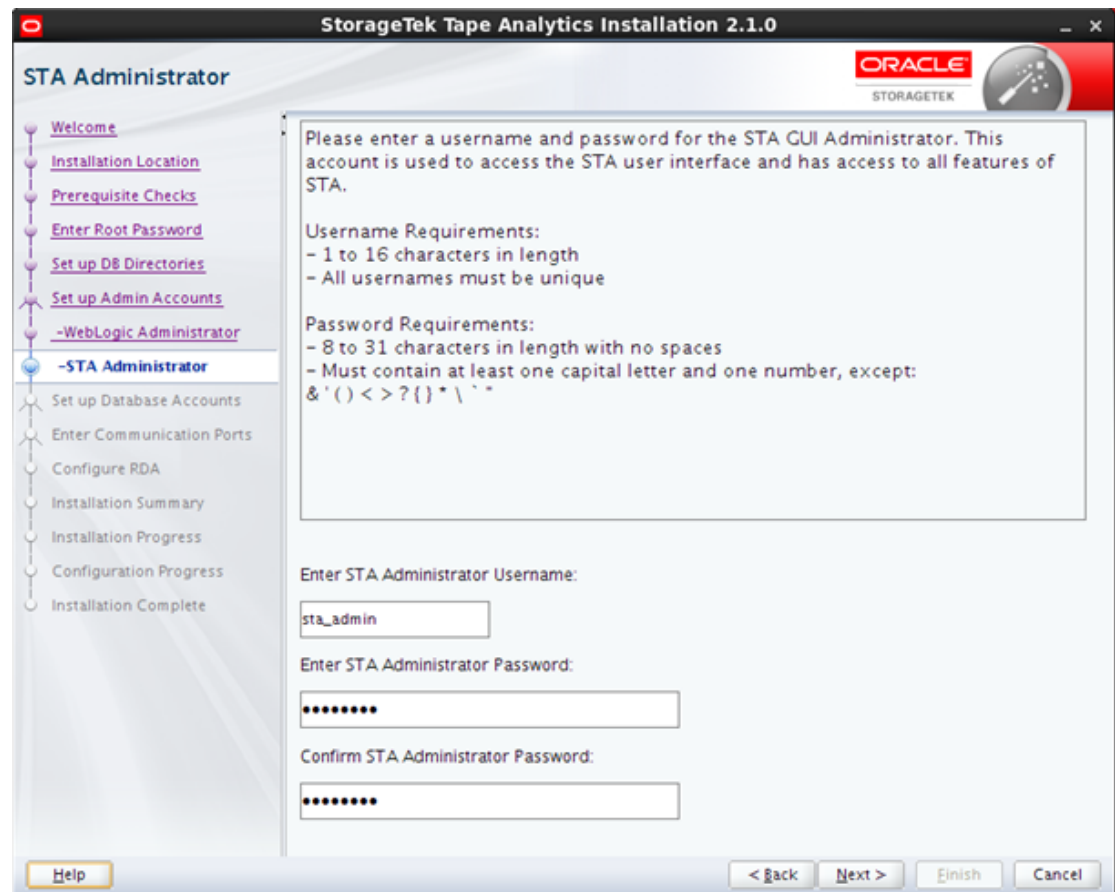
Confirm Password

Saisissez à nouveau le mot de passe pour vérifier que votre saisie est correcte.

A.2.8.2. Boutons spécifiques à l'écran

Aucun

A.2.9. Administrateur STA



Vous utilisez le compte Administrateur STA pour vous connecter à l'interface utilisateur STA. Cet utilisateur dispose des privilèges d'administrateur pour l'application STA et peut donc accéder à tous les écrans STA.

Ce compte sera créé pendant l'installation avec les identifiants de connexion que vous indiquerez.

Prudence:

Enregistrez ces identifiants de connexion en toute sécurité ; si vous lez perdez, vous ne pourrez plus vous connecter à l'interface utilisateur STA.

Afin de protéger la sécurité de votre site, les noms d'utilisateurs et les mots de passe ne sont, à dessein, ni préconfigurés ni codés.

A.2.9.1. Champs de l'écran

Enter Username

Saisissez le nom que vous souhaitez affecter à l'administrateur STA.

Les conditions du nom d'utilisateur requises sont les suivantes :

- Il doit comporter entre 1 et 16 caractères.
- Tous les noms d'utilisateur doivent être uniques.

Enter Password

Saisissez le mot de passe que vous souhaitez affecter à ce compte. La valeur saisie est masquée.

Les conditions requises en termes de mot de passe sont les suivantes :

- Il doit comporter entre 8 et 31 caractères.
- Il doit comporter au moins un chiffre et une majuscule
- Il ne doit pas comporter d'espace
- Il ne doit pas comporter les caractères spéciaux suivants :

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

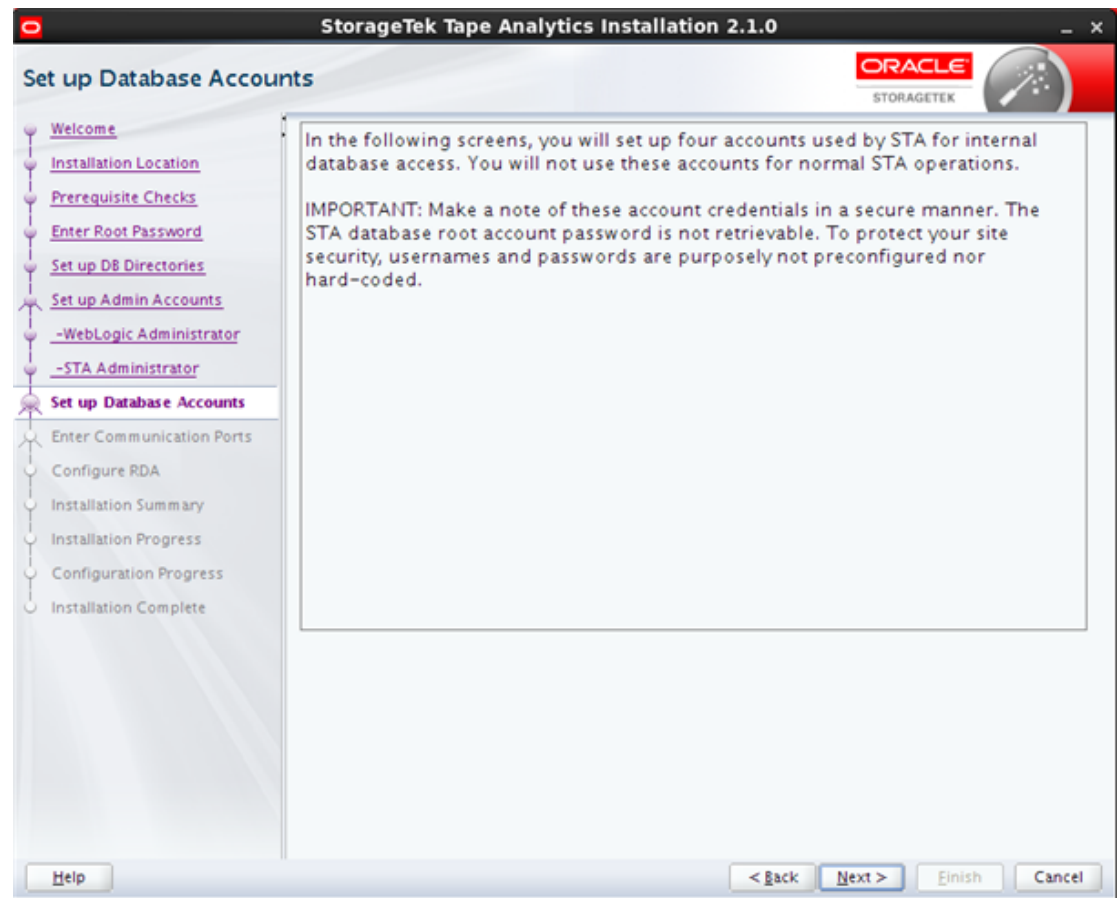
Confirm Password

Saisissez à nouveau le mot de passe pour vérifier que votre saisie est correcte.

A.2.9.2. Boutons spécifiques à l'écran

Aucun

A.2.10. Configuration des comptes de base de données



Cet écran décrit les types d'informations que vous serez amené à définir sur les quatre prochains écrans. Lire le texte, puis cliquer sur **Next** pour continuer.

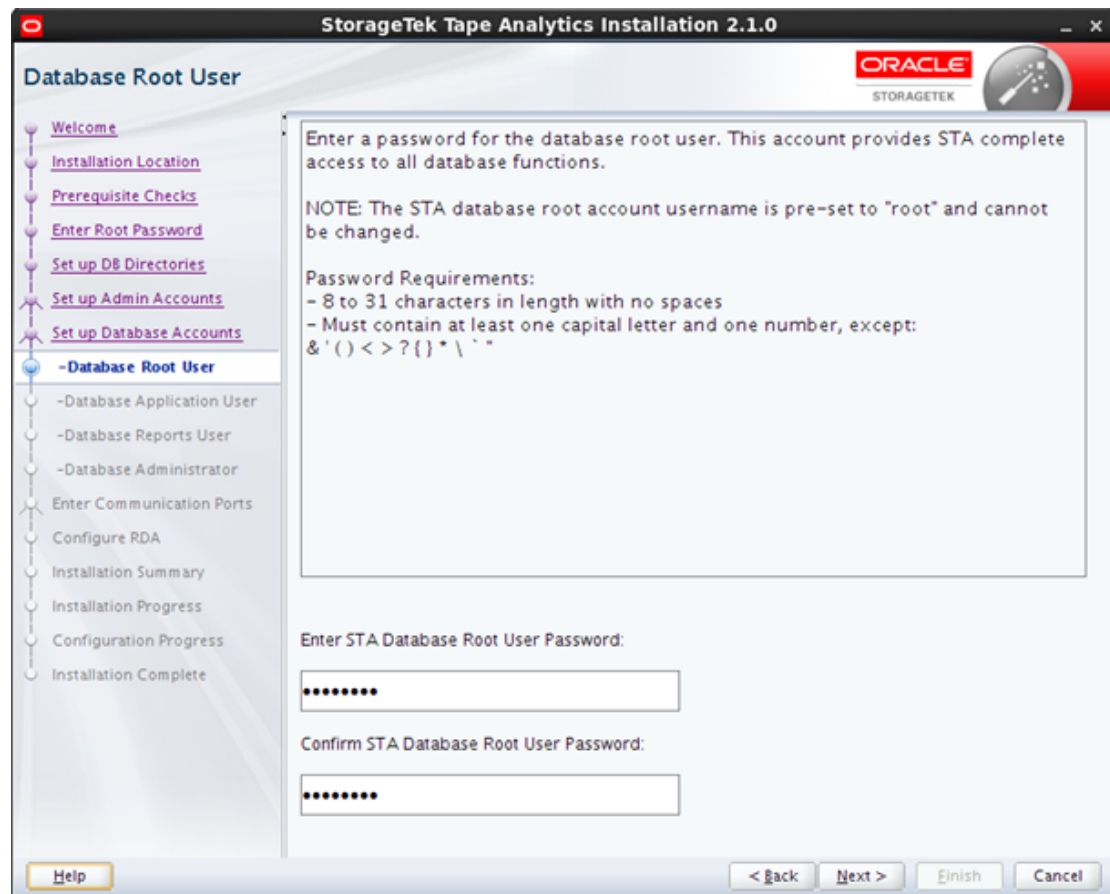
A.2.10.1. Champs de l'écran

Aucun

A.2.10.2. Boutons spécifiques à l'écran

Aucun

A.2.11. Utilisateur root de base de données



L'utilisateur root de base de données STA possède la base de données STA. Ce compte est utilisé en interne par l'application STA pour créer la base de données, et il permet tous les droits d'accès à toutes les tables de la base de données. Vous n'utiliserez pas ce compte pour des opérations STA courantes.

Le nom d'utilisateur de ce compte est automatiquement défini comme *root* et ne peut pas être modifié. Il s'agit d'un compte MySQL, il est distinct de l'utilisateur root Linux. Ce compte sera créé pendant l'installation avec les identifiants de connexion que vous indiquerez.

Remarque:

Enregistrez soigneusement ces identifiants de connexion.

Afin de protéger la sécurité de votre site, les noms d'utilisateurs et les mots de passe ne sont, à dessein, ni préconfigurés ni codés.

A.2.11.1. Champs de l'écran

Enter Password

Saisissez le mot de passe que vous souhaitez affecter à l'utilisateur root de la base de données STA. La valeur saisie est masquée.

Les conditions requises en termes de mot de passe sont les suivantes :

- Il doit comporter entre 8 et 31 caractères.
- Il doit comporter au moins un chiffre et une majuscule
- Il ne doit pas comporter d'espace
- Il ne doit pas comporter les caractères spéciaux suivants :

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

Confirm Password

Saisissez à nouveau le mot de passe pour vérifier que votre saisie est correcte.

A.2.11.2. Boutons spécifiques à l'écran

Aucun

A.2.12. Utilisateur de l'application de base de données

Ce compte d'application de base de données est utilisé en interne par l'application STA pour se connecter à et mettre à jour la base de données STA. Ce compte permet de créer, mettre à jour, supprimer et de lire l'accès à toutes les tables de la base de données. Vous n'utiliserez pas ce compte pour des opérations STA courantes.

Ce compte sera créé pendant l'installation avec les identifiants de connexion que vous indiquerez.

Remarque:

Enregistrez soigneusement ces identifiants de connexion.

Afin de protéger la sécurité de votre site, les noms d'utilisateurs et les mots de passe ne sont, à dessein, ni préconfigurés ni codés.

A.2.12.1. Champs de l'écran

Enter Username

Saisissez le nom que vous souhaitez affecter au compte d'application de base de données STA, *stadb*, par exemple.

Les conditions du nom d'utilisateur requises sont les suivantes :

- Il doit comporter entre 1 et 16 caractères.
- Tous les noms d'utilisateur doivent être uniques.

Enter Password

Saisissez le mot de passe que vous souhaitez affecter au compte d'application de la base de données STA. La valeur saisie est masquée.

Les conditions requises en termes de mot de passe sont les suivantes :

- Il doit comporter entre 8 et 31 caractères.
- Il doit comporter au moins un chiffre et une majuscule
- Il ne doit pas comporter d'espace
- Il ne doit pas comporter les caractères spéciaux suivants :

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

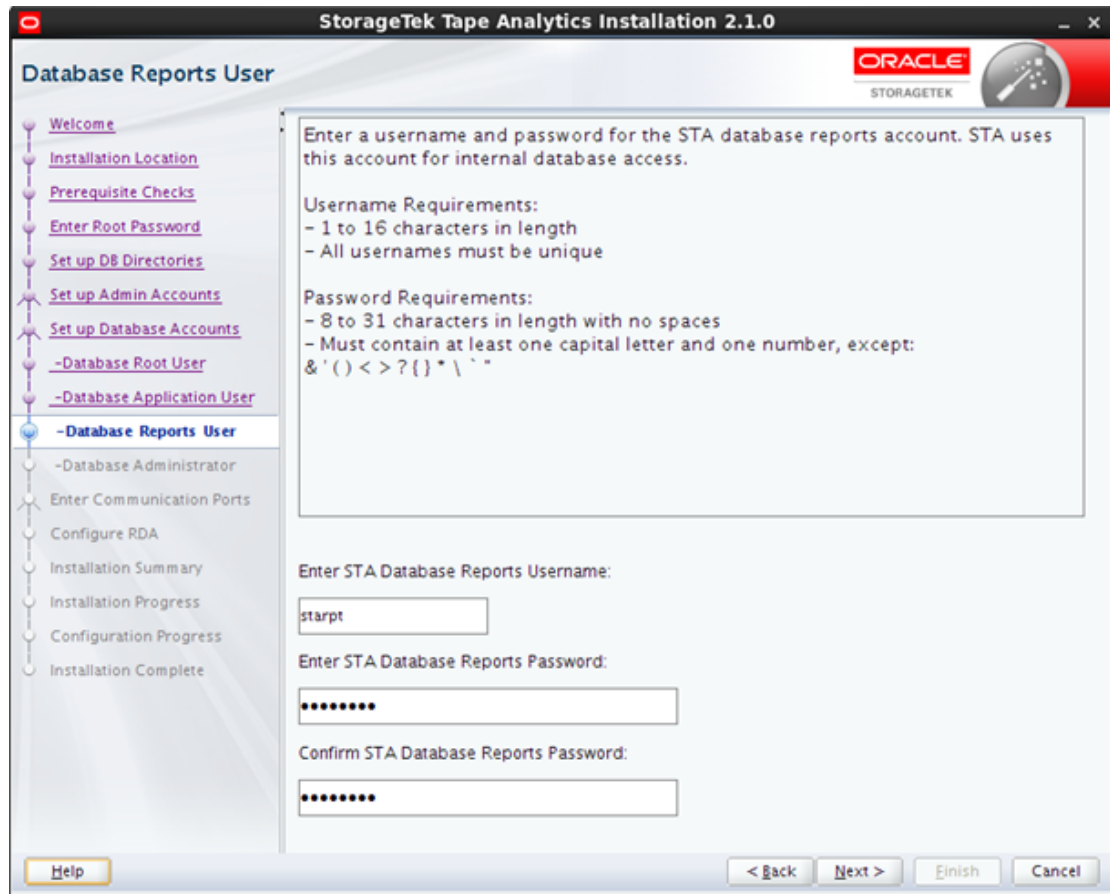
Confirm Password

Saisissez à nouveau le mot de passe pour vérifier que votre saisie est correcte.

A.2.12.2. Boutons spécifiques à l'écran

Aucun

A.2.13. Utilisateur des rapports de base de données



Le compte de rapports de base de données STA est un compte MySQL utilisé par les applications non-STA et les applications tierces pour se connecter à la base de données STA. Ce compte fournit un accès en lecture seule aux tables de base de données sélectionnées. Vous n'utiliserez pas ce compte pour des opérations STA courantes.

Ce compte sera créé pendant l'installation avec les identifiants de connexion que vous indiquerez.

Remarque:

Enregistrez soigneusement ces identifiants de connexion.

Afin de protéger la sécurité de votre site, les noms d'utilisateurs et les mots de passe ne sont, à dessein, ni préconfigurés ni codés.

A.2.13.1. Champs de l'écran

Enter Username

Saisissez le nom que vous souhaitez affecter au compte de rapports de base de données STA, *starpt* par exemple.

Les conditions du nom d'utilisateur requises sont les suivantes :

- Il doit comporter entre 1 et 16 caractères.
- Tous les noms d'utilisateur doivent être uniques.

Enter Password

Saisissez le mot de passe que vous souhaitez affecter à ce compte. La valeur saisie est masquée.

Les conditions requises en termes de mot de passe sont les suivantes :

- Il doit comporter entre 8 et 31 caractères.
- Il doit comporter au moins un chiffre et une majuscule
- Il ne doit pas comporter d'espace
- Il ne doit pas comporter les caractères spéciaux suivants :

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

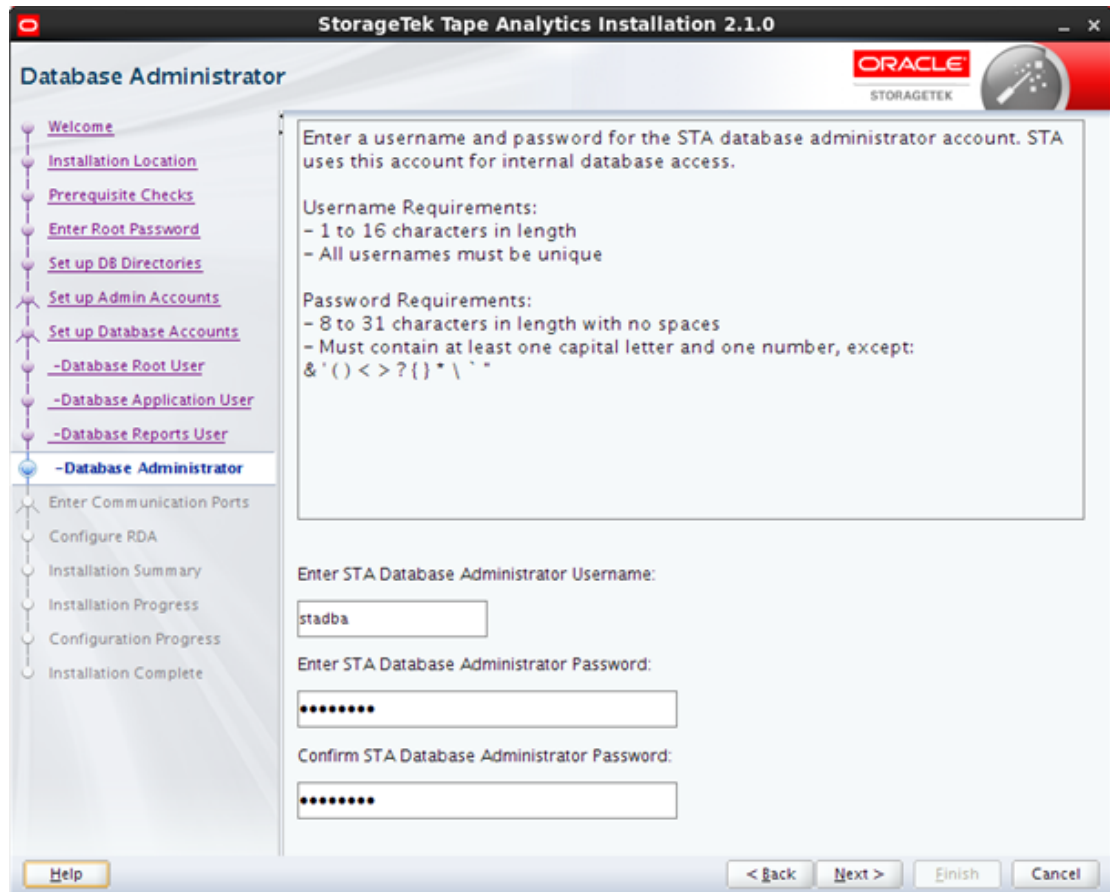
Confirm Password

Saisissez à nouveau le mot de passe pour vérifier que votre saisie est correcte.

A.2.13.2. Boutons spécifiques à l'écran

Aucun

A.2.14. Administrateur de bases de données



Le compte d'administrateur de base de données STA est un compte MySQL utilisé en interne par les utilitaires STA d'administration et de contrôle pour se connecter à la base de données STA et configurer et exécuter des sauvegardes programmées. Ce compte permet l'accès total à toutes les tables de base de données, à l'exception de l'option "grant". Vous n'utiliserez pas ce compte pour des opérations STA courantes.

Ce compte sera créé pendant l'installation avec les identifiants de connexion que vous indiquerez.

Remarque:

Enregistrez soigneusement ces identifiants de connexion.

Afin de protéger la sécurité de votre site, les noms d'utilisateurs et les mots de passe ne sont, à dessein, ni préconfigurés ni codés.

A.2.14.1. Champs de l'écran

Enter Username

Saisissez le nom que vous souhaitez affecter au compte d'administrateur de base de données STA, *stadba*, par exemple.

Les conditions du nom d'utilisateur requises sont les suivantes :

- Il doit comporter entre 1 et 16 caractères.
- Tous les noms d'utilisateur doivent être uniques.

Enter Password

Saisissez le mot de passe que vous souhaitez affecter à ce compte. La valeur saisie est masquée.

Les conditions requises en termes de mot de passe sont les suivantes :

- Il doit comporter entre 8 et 31 caractères.
- Il doit comporter au moins un chiffre et une majuscule
- Il ne doit pas comporter d'espace
- Il ne doit pas comporter les caractères spéciaux suivants :

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

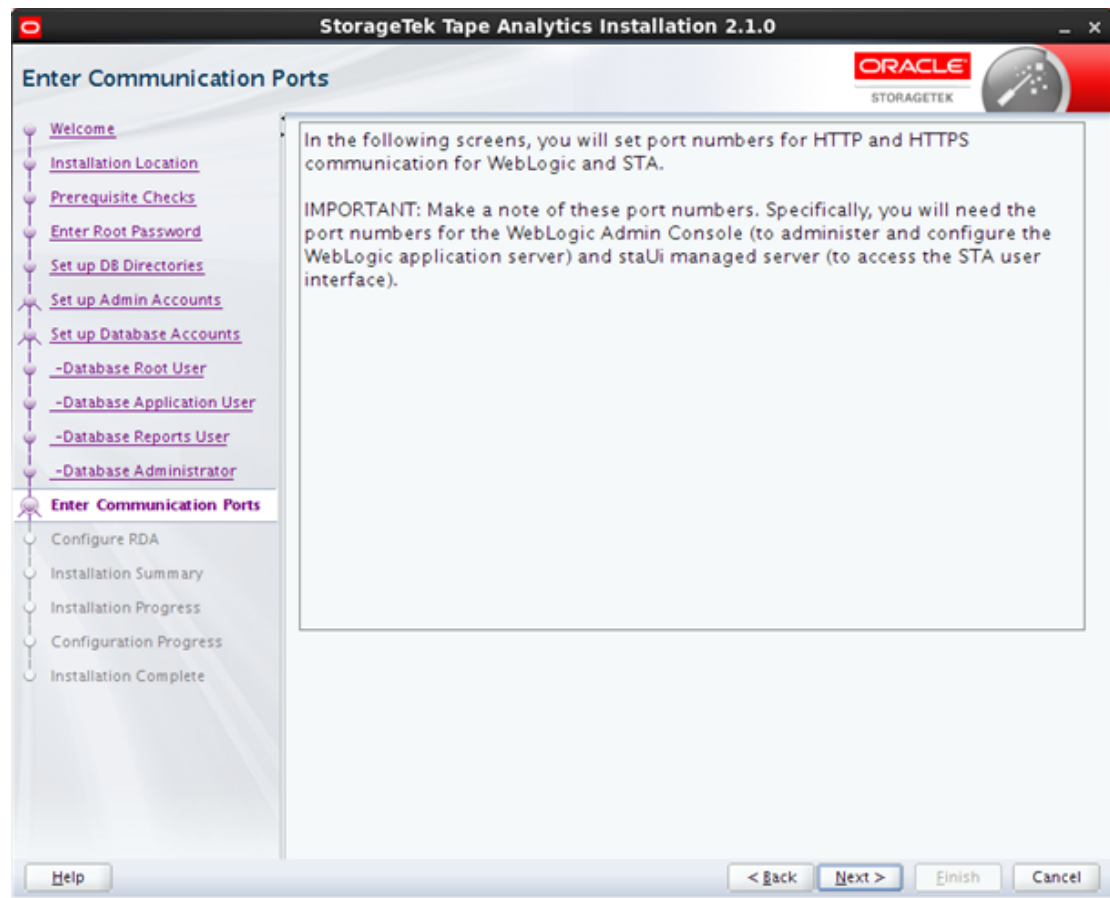
Confirm Password

Saisissez à nouveau le mot de passe pour vérifier que votre saisie est correcte.

A.2.14.2. Boutons spécifiques à l'écran

Aucun

A.2.15. Saisir les ports de communication



Cet écran décrit les types d'informations que vous serez amené à définir sur les quatre prochains écrans. Lire le texte, puis cliquer sur **Next** pour continuer.

Vous fournirez les valeurs des ports configurables WebLogic et STA internes et externes . Ces ports seront configurés et activés pendant l'installation avec les valeurs que vous indiquerez. Les numéros de ports que vous indiquerez doivent être uniques, et les ports doivent rester disponibles et dédiés à STA.

Remarque:

Avant de terminer de remplir ces écrans, vérifiez les bonnes valeurs des numéros de ports avec votre administrateur réseau. Une fois STA installé, les numéros de ports ne peuvent pas être modifiés sans désinstaller et réinstaller STA.

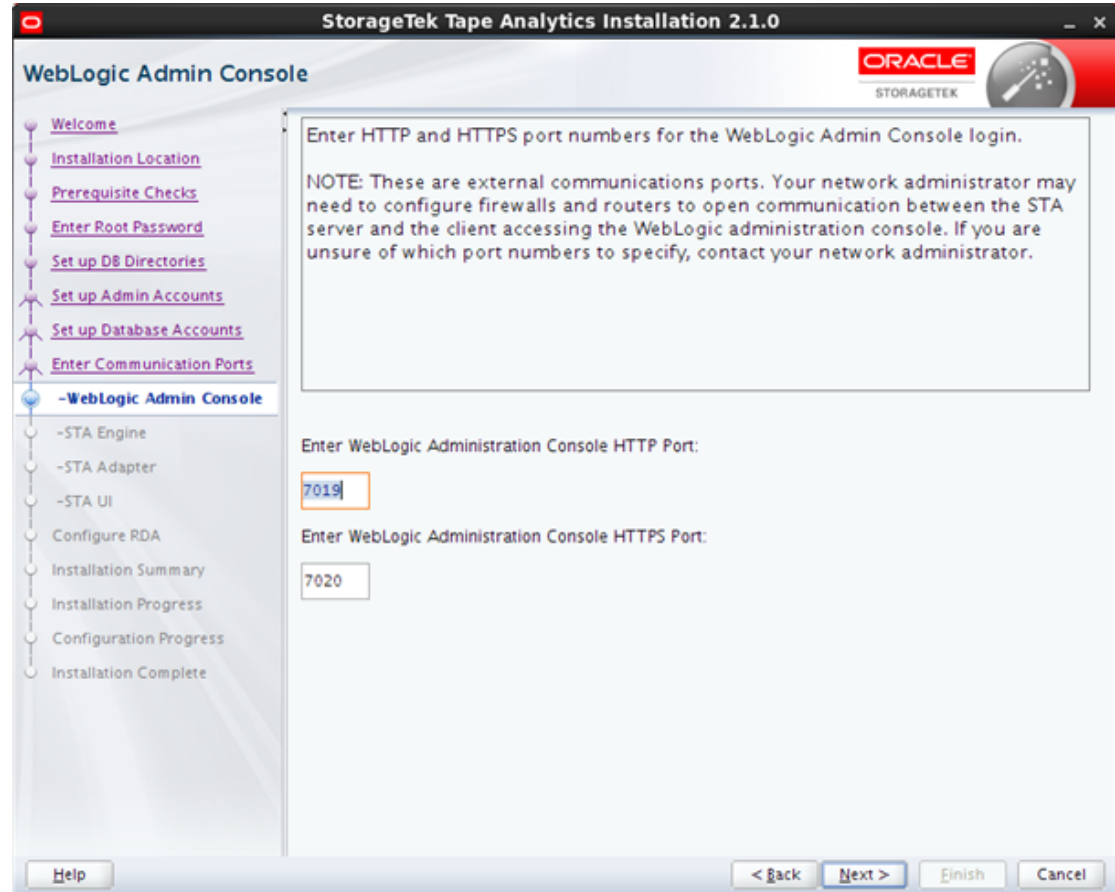
A.2.15.1. Champs de l'écran

Aucun

A.2.15.2. Boutons spécifiques à l'écran

Aucun

A.2.16. Console d'administration WebLogic



Lorsque vous vous connectez à la console d'administrateur WebLogic, vous indiquez le numéro de port de la console d'administrateur WebLogic, qui est utilisé pour administrer et configurer le serveur d'applications WebLogic.

Remarque:

Voici les ports de communication externes. Votre administrateur réseau peut devoir configurer des pare-feu et des routeurs pour ouvrir la communication entre le serveur STA et le client accédant à la console d'administration WebLogic.

Remarque:

Enregistrez soigneusement ces numéros de port, car ils ne peuvent pas être modifiés une fois STA installé.

Afin de protéger la sécurité de votre site, ces numéros de port ne sont, à dessein, ni préconfigurés ni codés.

A.2.16.1. Champs de l'écran

Enter HTTP Port

Saisissez le numéro de port HTTP pour l'accès non sécurisé à la connexion à la console d'administrateur WebLogic. Ce numéro de port est généralement 7019.

Les numéros de port doivent être uniques et disponibles.

Enter HTTPS Port

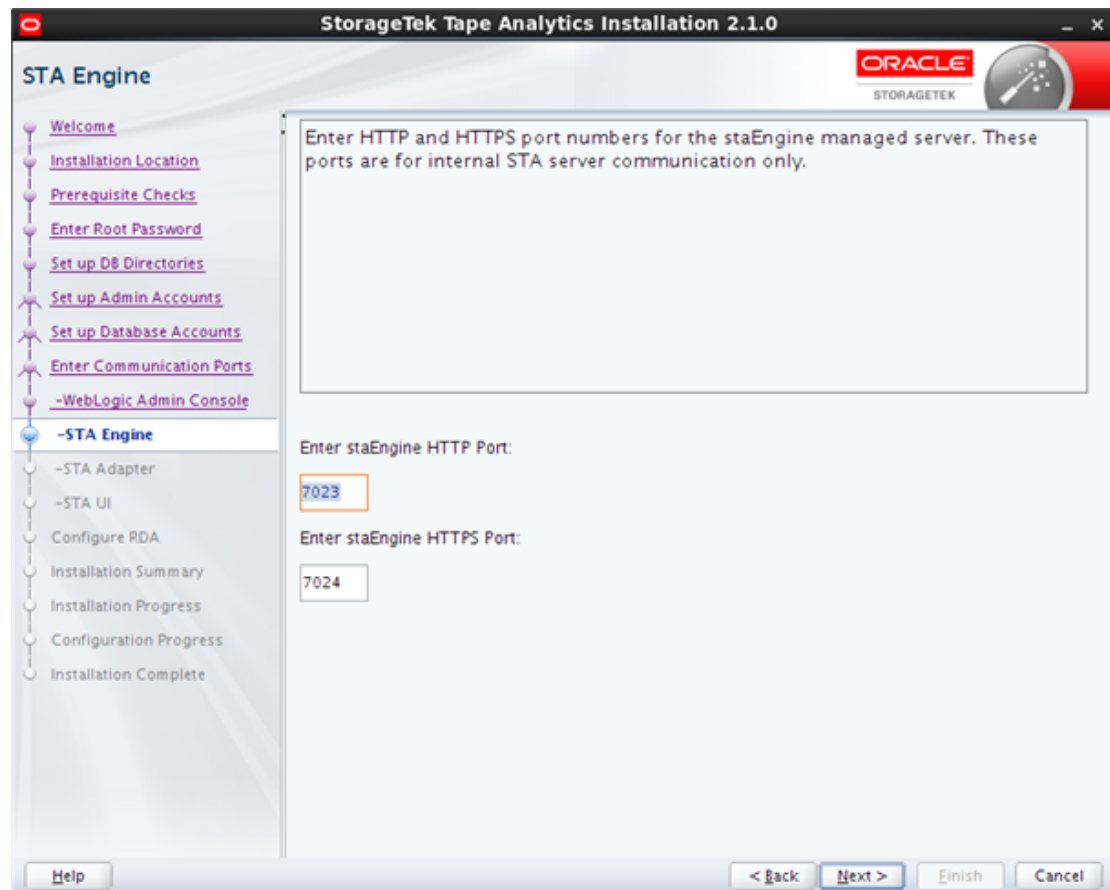
Saisissez le numéro de port HTTPS pour l'accès sécurisé à la connexion à la console d'administrateur WebLogic. Ce numéro de port est généralement 7020.

Les numéros de port doivent être uniques et disponibles.

A.2.16.2. Boutons spécifiques à l'écran

Aucun

A.2.17. Moteur STA



Les ports du serveur staEngine géré ne sont utilisés que pour la communication interne au serveur STA.

Remarque:

Enregistrez soigneusement ces numéros de port, car ils ne peuvent pas être modifiés une fois STA installé.

Afin de protéger la sécurité de votre site, ces numéros de port ne sont, à dessein, ni préconfigurés ni codés.

A.2.17.1. Champs de l'écran

Enter HTTP Port

Saisissez le numéro de port HTTP pour l'accès non sécurisé au serveur staEngine géré. Ce numéro de port est généralement 7023.

Les numéros de port doivent être uniques et disponibles.

Enter HTTPS Port

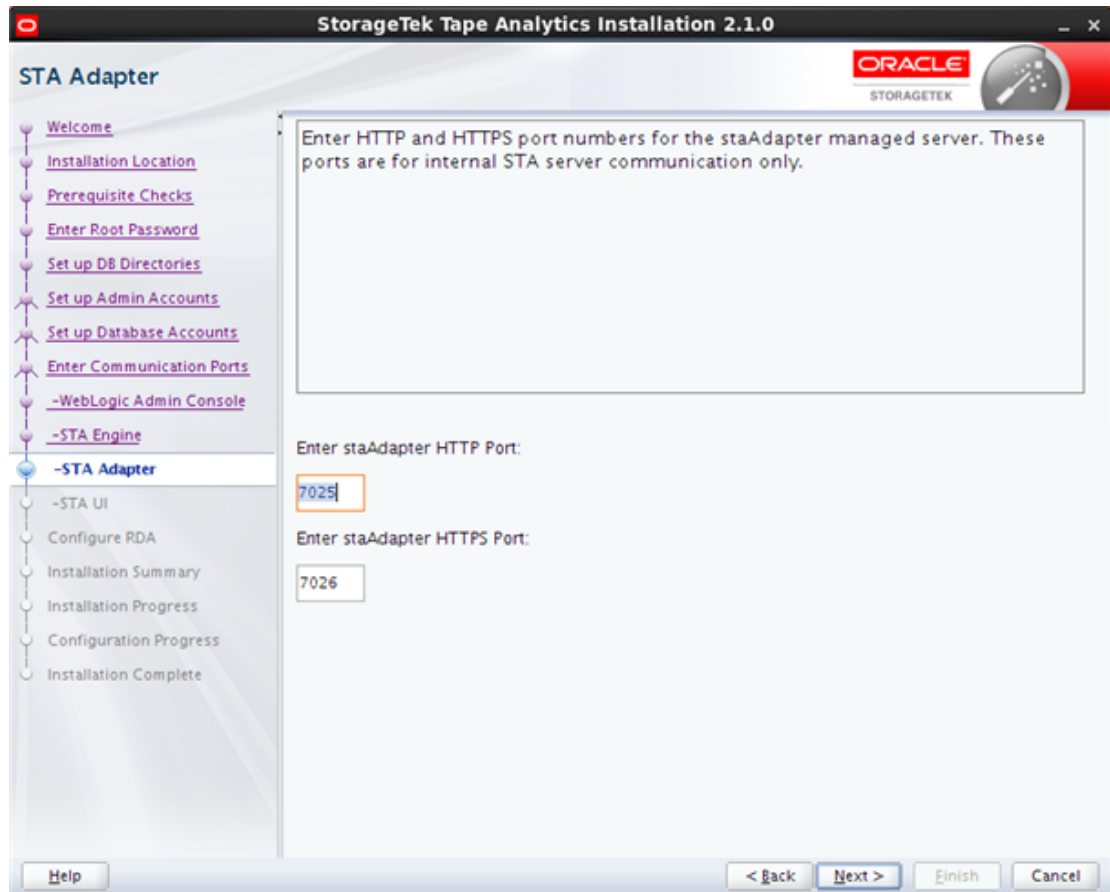
Saisissez le numéro de port HTTPS pour l'accès sécurisé au serveur staEngine géré. Ce numéro de port est généralement 7024.

Les numéros de port doivent être uniques et disponibles.

A.2.17.2. Boutons spécifiques à l'écran

Aucun

A.2.18. Adaptateur STA



Les ports du serveur staAdapter géré ne sont utilisés que pour la communication SNMP interne.

Remarque:

Enregistrez soigneusement ces numéros de port, car ils ne peuvent pas être modifiés une fois STA installé.

Afin de protéger la sécurité de votre site, ces numéros de port ne sont, à dessein, ni préconfigurés ni codés.

A.2.18.1. Champs de l'écran

Enter HTTP Port

Saisissez le numéro de port HTTP pour l'accès non sécurisé au serveur staEngine géré. Ce numéro de port est généralement 7025.

Les numéros de port doivent être uniques et disponibles.

Enter HTTPS Port

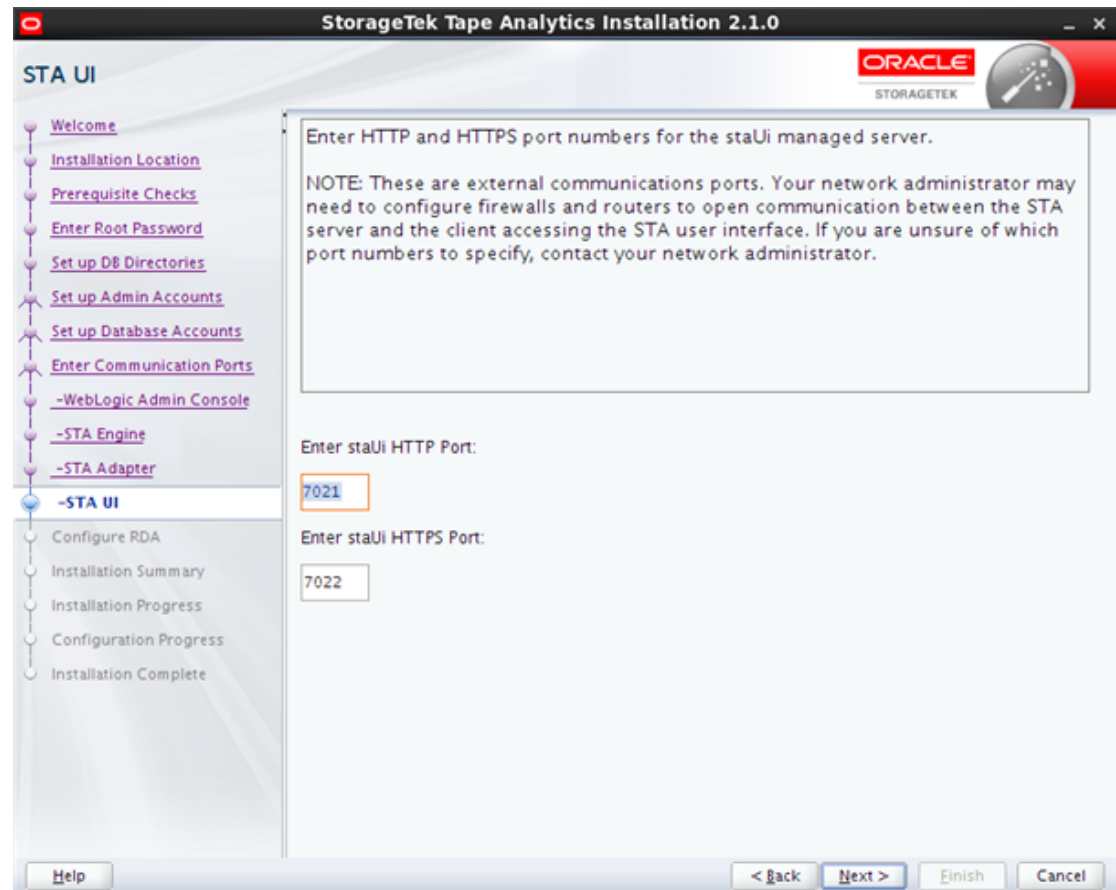
Saisissez le numéro de port HTTPS pour l'accès sécurisé au serveur staEngine géré. Ce numéro de port est généralement 7026.

Les numéros de port doivent être uniques et disponibles.

A.2.18.2. Boutons spécifiques à l'écran

Aucun

A.2.19. Interface utilisateur STA



Vous indiquez le numéro de port du serveur staUi géré lorsque vous vous connectez à l'interface utilisateur de l'application STA.

Remarque:

Voici les ports de communication externes. Votre administrateur réseau peut devoir configurer des pare-feu et des routeurs pour ouvrir la communication entre le serveur STA et le client accédant à la console d'administration WebLogic.

Remarque:

Enregistrez soigneusement ces numéros de port, car ils ne peuvent pas être modifiés une fois STA installé.

Afin de protéger la sécurité de votre site, ces numéros de port ne sont, à dessein, ni préconfigurés ni codés.

A.2.19.1. Champs de l'écran

Enter HTTP Port

Saisissez le numéro de port HTTP pour l'accès non sécurisé au serveur staUi géré. Ce numéro de port est généralement 7021.

Les numéros de port doivent être uniques et disponibles.

Enter HTTPS Port

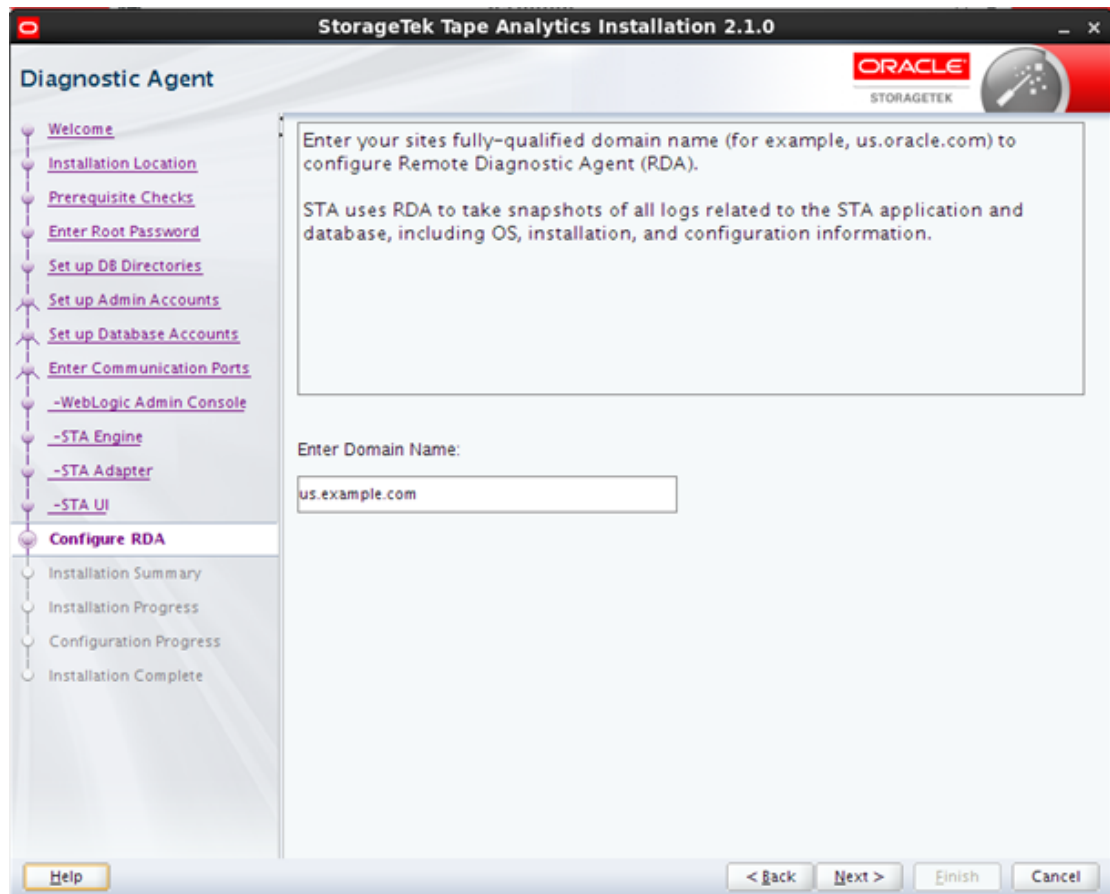
Saisissez le numéro de port HTTP pour permettre l'accès sécurisé au serveur staUi géré. Ce numéro de port est généralement 7022.

Les numéros de port doivent être uniques et disponibles.

A.2.19.2. Boutons spécifiques à l'écran

Aucun

A.2.20. Agent de diagnostic



Le programme d'installation de STA utilise le nom de domaine complet de votre site pour configurer l'agent de diagnostic distant (RDA) de Oracle.

STA utilise RDA pour prendre des instantanés de tous les journaux concernant la base de données et l'application STA, y compris les informations sur le système d'exploitation, l'installation et la configuration. Pour plus d'informations, reportez-vous au guide *Guide de l'utilisateur STA*.

A.2.20.1. Champs de l'écran

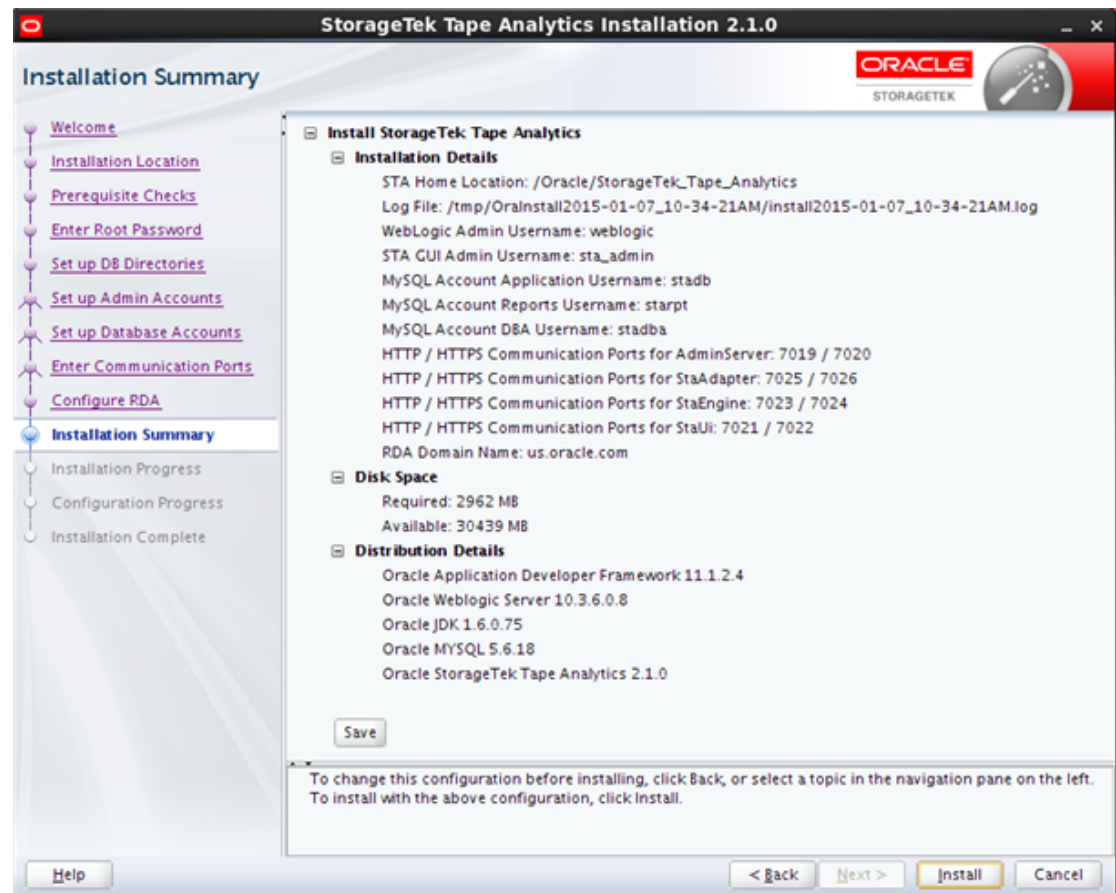
Enter Domain Name

Entrez le nom de domaine complet de votre site, *us.example.com* par exemple.

A.2.20.2. Boutons spécifiques à l'écran

Aucun

A.2.21. Récapitulatif de l'installation



L'écran affiche les détails suivants relatifs à l'installation. Vous pouvez enregistrer ces informations dans un fichier texte pour vos archives.

- Détails de l'installation : Informations que vous avez saisies sur les écrans du programme d'installation.

- Espace disque : Espace disque requis et disponible, en Mo.
- Détails de distribution : Noms et numéros de version des packages logiciels qui seront installés.

Poursuivez comme suit :

- Pour modifier un détail de l'installation, cliquez sur **Back** jusqu'à l'écran concerné, ou sélectionnez le lien de l'écran sur le panneau de navigation pour y accéder directement.
- Pour enregistrer les détails affichés en fichier texte, cliquez sur **Save**.
- Pour procéder à l'installation avec les valeurs affichées, cliquez sur **Install**.
- Pour annuler l'installation, cliquez sur **Cancel**.

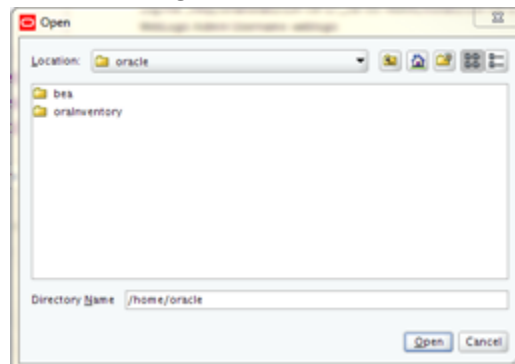
A.2.21.1. Champs de l'écran

Aucun

A.2.21.2. Boutons spécifiques à l'écran

Save

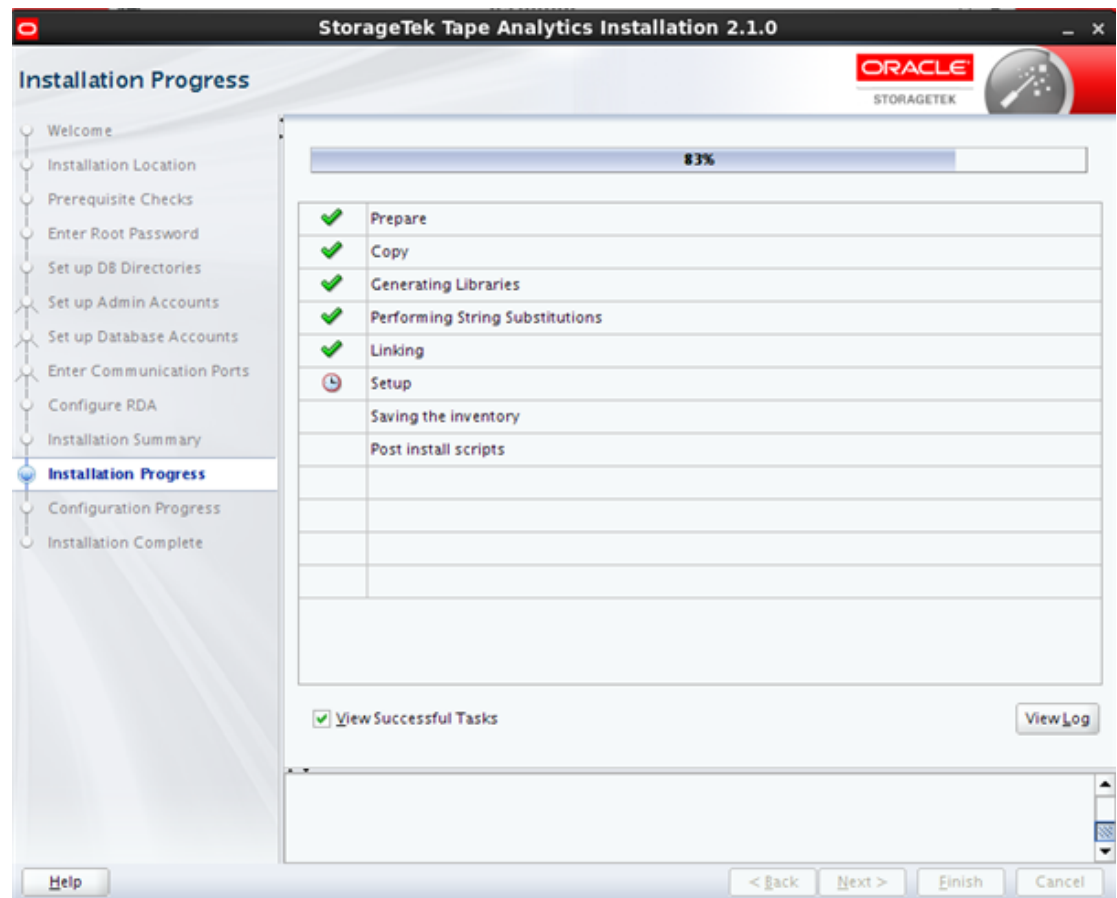
Cliquez pour enregistrer les informations affichées dans un fichier texte avec le nom *STA_Installation_Profile_timestamp.txt*. Dans la boîte de dialogue Open, indiquez le répertoire où vous souhaitez sauvegarder ce fichier.



Install

Cliquez sur Install pour commencer l'installation. Une fois que vous avez cliqué sur ce bouton, il n'est plus possible d'annuler ou de mettre l'installation en pause.

A.2.22. Progression de l'installation



L'installation de STA commence, et l'écran affiche le statut de chaque tâche.

Prudence:

Ne fermez pas cette fenêtre ; sinon, interrompez l'installation en cours, car cela pourrait laisser certains composants dont l'installation n'est pas terminée sur le serveur.

Si une tâche échoue, l'installation s'arrête et vous devez quitter le programme d'installation en cliquant sur **Cancel**. Le programme d'installation annulera l'installation et renverra le serveur dans son état d'origine.

Avant de quitter, vous pouvez visualiser des détails supplémentaires sur le volet Message pour faciliter la résolution des problèmes et la détermination des actions à mener. Vous pouvez également visualiser le journal d'installation pour plus d'informations.

A.2.22.1. Champs de l'écran

Aucun

A.2.22.2. Boutons spécifiques à l'écran

View Successful Tasks

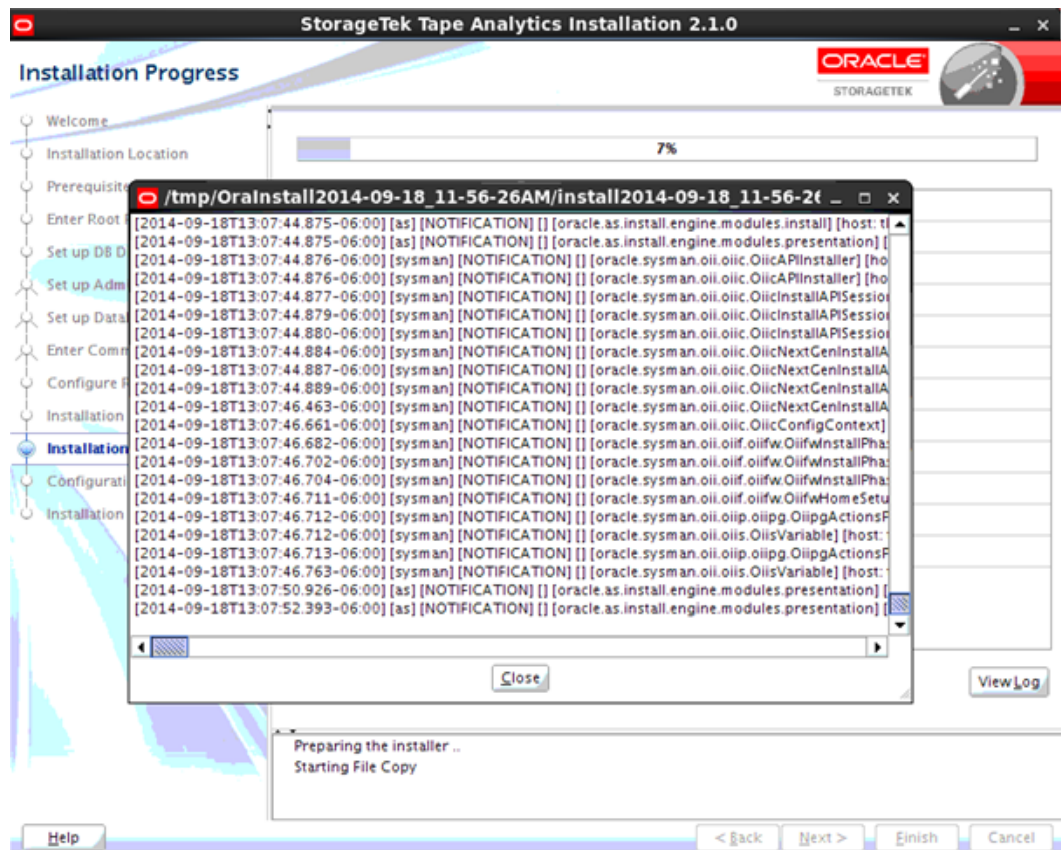
Sélectionnez la case pour inclure les sorties Succès ; cette case est cochée par défaut.

Cochez cette case pour ne faire apparaître que les sorties en Echec. Cela vous permet d'exclure les tâches réussies pour vous concentrer sur celles requérant votre attention.

View Log

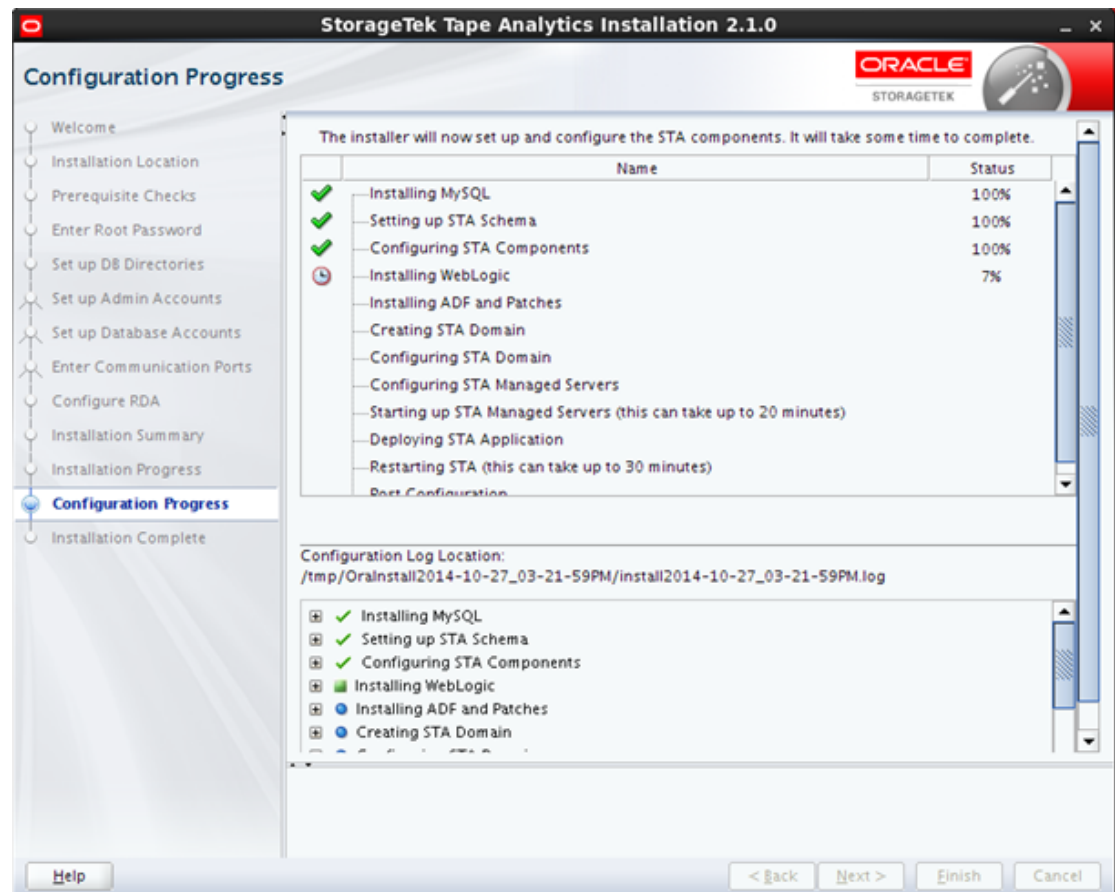
Cliquez pour afficher le journal d'installation dans une fenêtre séparée. La copie d'écran Figure A.5, « Exemple d'affichage du journal de progression de l'installation » en est un exemple. Cliquez sur **Close** pour fermer la fenêtre du journal.

Figure A.5. Exemple d'affichage du journal de progression de l'installation



Il est aussi possible de voir le journal depuis la ligne de commande Linux. Pendant que le programme d'installation est en cours d'exécution, les journaux sont conservés dans un sous-répertoire sous */tmp*. Pour plus d'informations, reportez-vous à la section Section 3.4, « Journaux d'installation et de désinstallation de STA ».

A.2.23. Progression de la configuration



La configuration et le déploiement de STA commence, et l'écran affiche le statut de chaque tâche.

Prudence:

Ne fermez pas cette fenêtre ; sinon, interrompez la configuration en cours, car cela pourrait laisser certains composants dont l'installation n'est pas terminée sur le serveur.

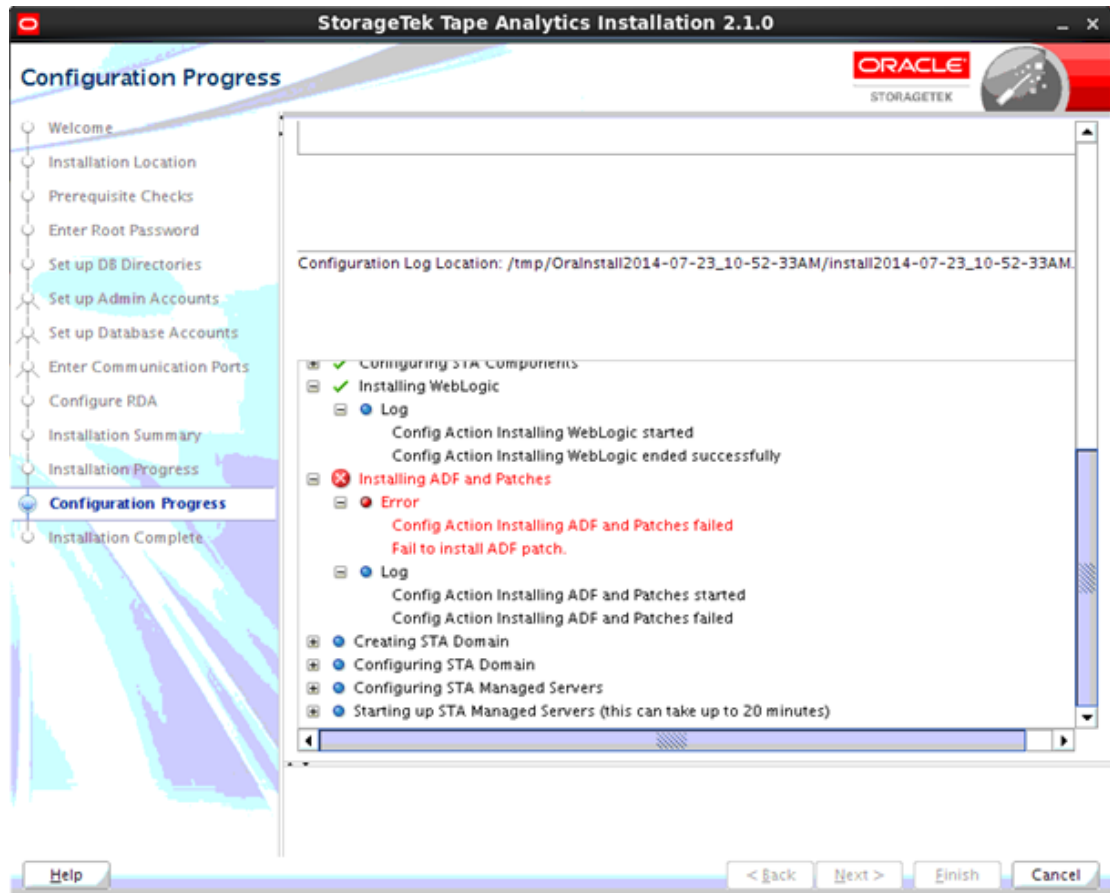
Pendant ce processus, le serveur WebLogic, les serveurs STA gérés, et l'application STA sont configurés et démarrés. Ce processus peut prendre de 30 à 60 minutes.

Vous pouvez développer les détails pour toute tâche terminée ou en cours. Dans le volet Message, cliquez sur l'icône **Expand** (+) à côté de la tâche dont vous souhaitez consulter le détail. Cliquez sur l'icône **Collapse** (–) pour masquer les détails. La copie d'écran [Figure A.6, « Exemple de détail de progression de la configuration »](#) en est un exemple, présentant les détails développés des tâches réussies et en échec.

Si une tâche échoue, le programme d'installation de STA arrête et annule l'installation, et renvoie le serveur dans son état d'origine. Vous pouvez également visualiser le journal

d'installation pour résoudre le problème. Pour plus d'informations, reportez-vous à la section [Section 3.4, « Journaux d'installation et de désinstallation de STA »](#).

Figure A.6. Exemple de détail de progression de la configuration



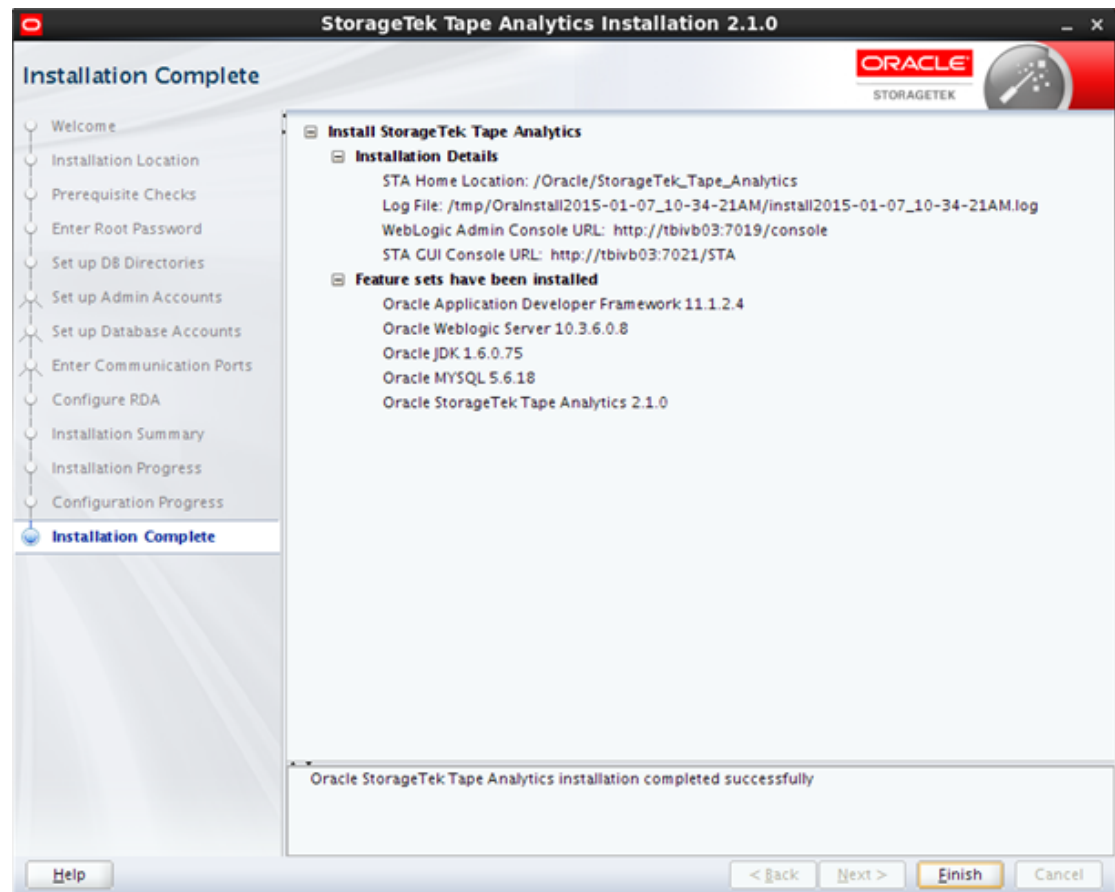
A.2.23.1. Champs de l'écran

Aucun

A.2.23.2. Boutons spécifiques à l'écran

Aucun

A.2.24. Installation terminée



L'écran affiche les détails suivants relatifs à l'installation terminée :

- Détails de l'installation : Emplacements du fichier journal du programme d'installation et de l'application STA, et détails de la connexion des interfaces utilisateur de l'application STA et de WebLogic.
- Les ensembles de fonctionnalités ont été installés—Noms et numéros de version des packages logiciels qui ont été installés.

Vous pourrez souhaiter enregistrer une copie d'écran de ces informations pour les conserver. Cliquez sur **Finish** pour quitter le programme d'installation.

A.2.24.1. Champs de l'écran

Aucun

A.2.24.2. Boutons spécifiques à l'écran

Finish

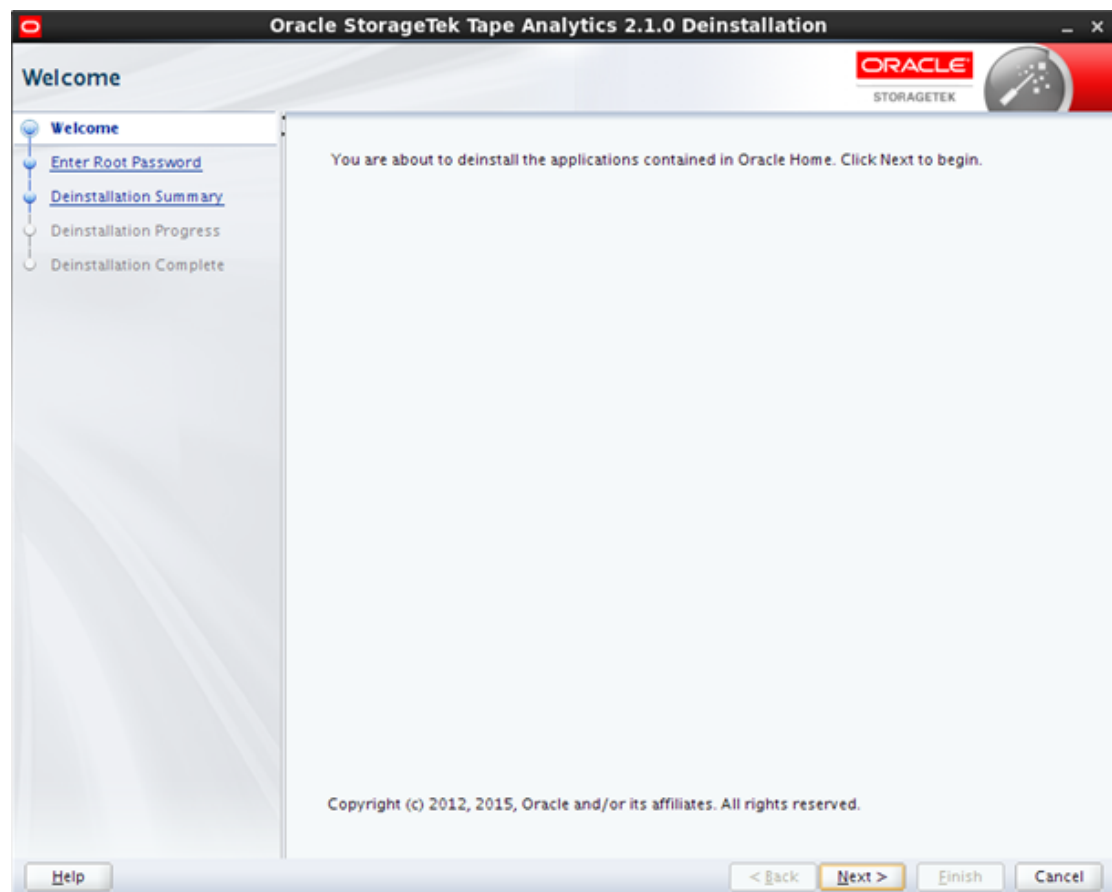
Cliquer pour quitter le programme d'installation de STA.

A.3. Ecrans de programme de désinstallation graphique de STA

Cette section fournit une référence détaillée de chaque écran du programme de désinstallation graphique de STA.

- [Section A.3.1, « Accueil »](#)
- [Section A.3.2, « Entrez le mot de passe root »](#)
- [Section A.3.3, « Récapitulatif de la désinstallation »](#)
- [Section A.3.4, « Progression de la désinstallation »](#)
- [Section A.3.5, « Désinstallation terminée »](#)

A.3.1. Accueil



L'écran décrit les actions que vous êtes sur le point de mener. Lisez le texte, puis cliquez sur **Next** pour continuer.

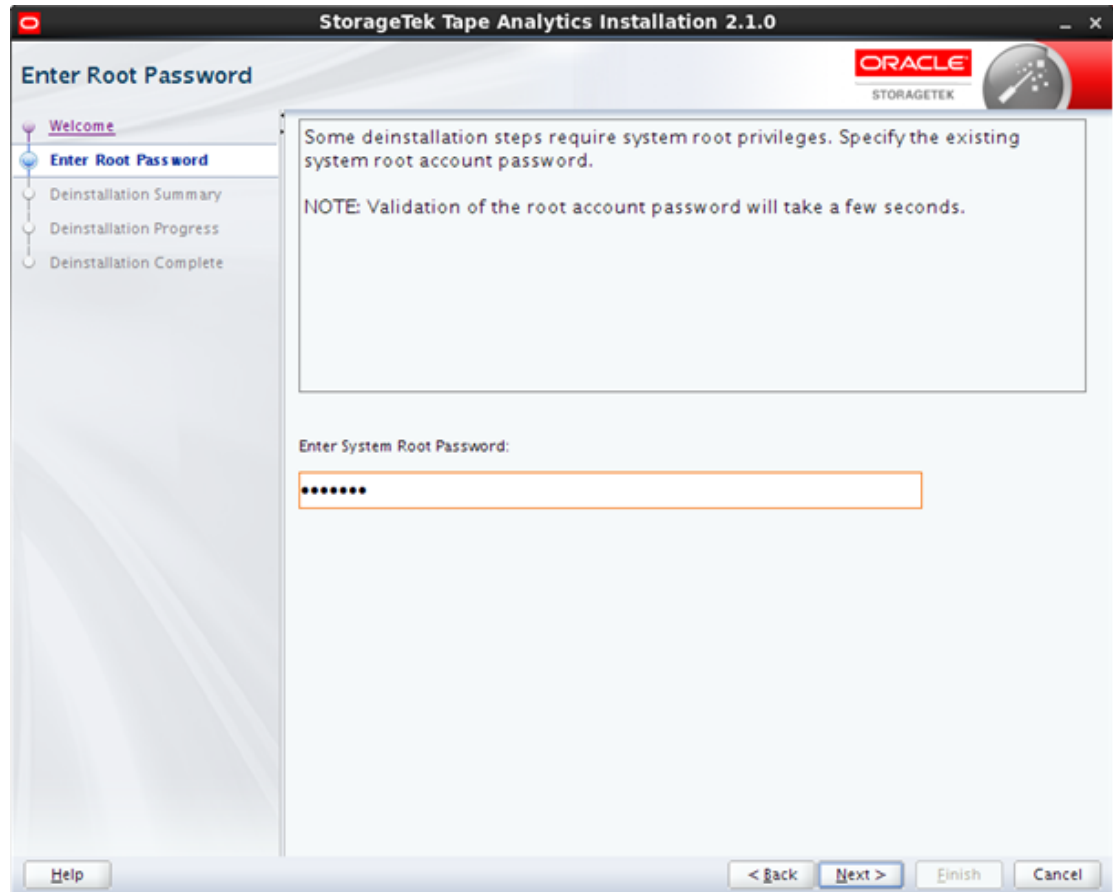
A.3.1.1. Champs de l'écran

Aucun

A.3.1.2. Boutons spécifiques à l'écran

Aucun

A.3.2. Entrez le mot de passe root



Le programme de désinstallation de STA requiert l'accès root Linux pour effectuer les tâches de désinstallation.

A.3.2.1. Champs de l'écran

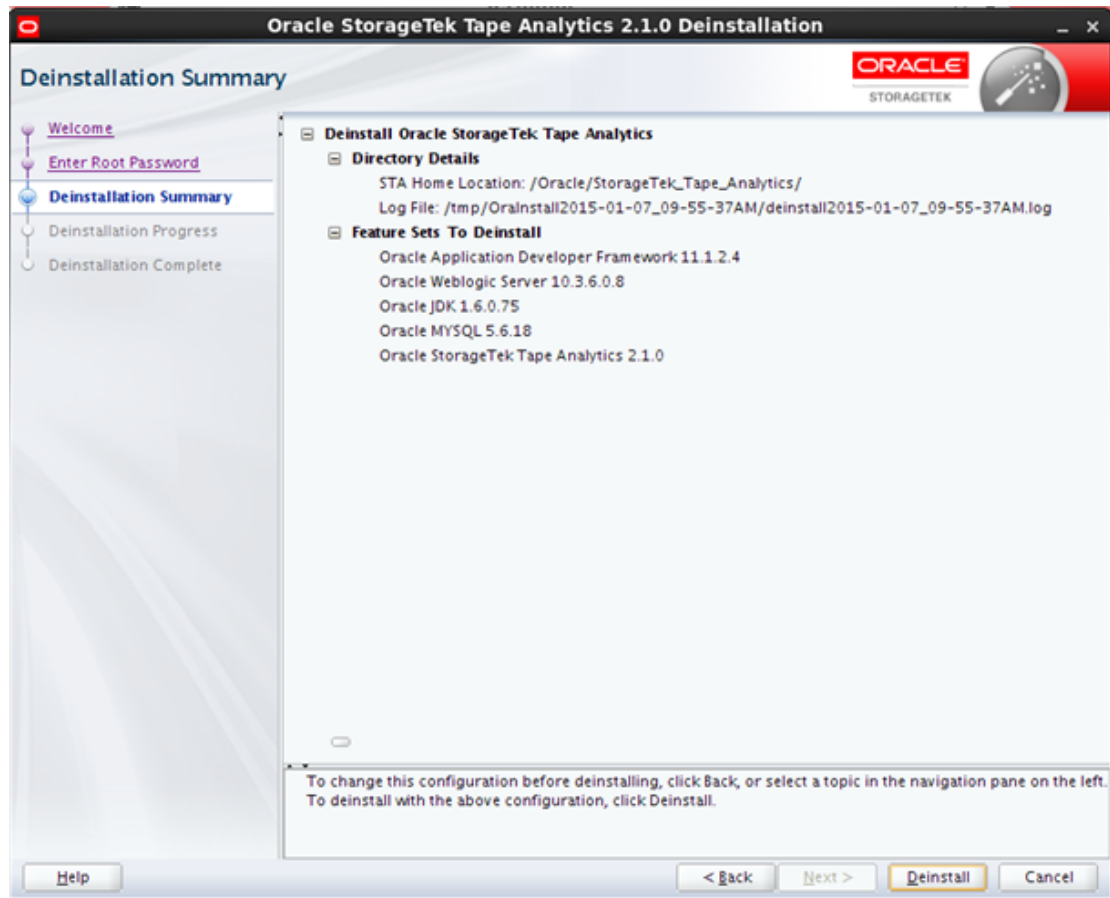
Enter Root Password

Saisir le mot de passe de l'utilisateur root Linux. La valeur saisie est masquée. La validation du mot de passe peut prendre quelques secondes.

A.3.2.2. Boutons spécifiques à l'écran

Aucun

A.3.3. Récapitulatif de la désinstallation



L'écran affiche les détails suivants relatifs au logiciel qui sera désinstallé :

- Directory Details : Emplacements du logiciel applicatif STA et du journal de désinstallation.
- Feature Sets to Deinstall : Noms et numéros de version des packages logiciels qui seront désinstallés.

Vérifiez ces informations avant de poursuivre comme suit :

- Cliquez sur **Cancel** pour annuler et quitter le programme de désinstallation.
- Cliquez sur **Deinstall**.

A.3.3.1. Champs de l'écran

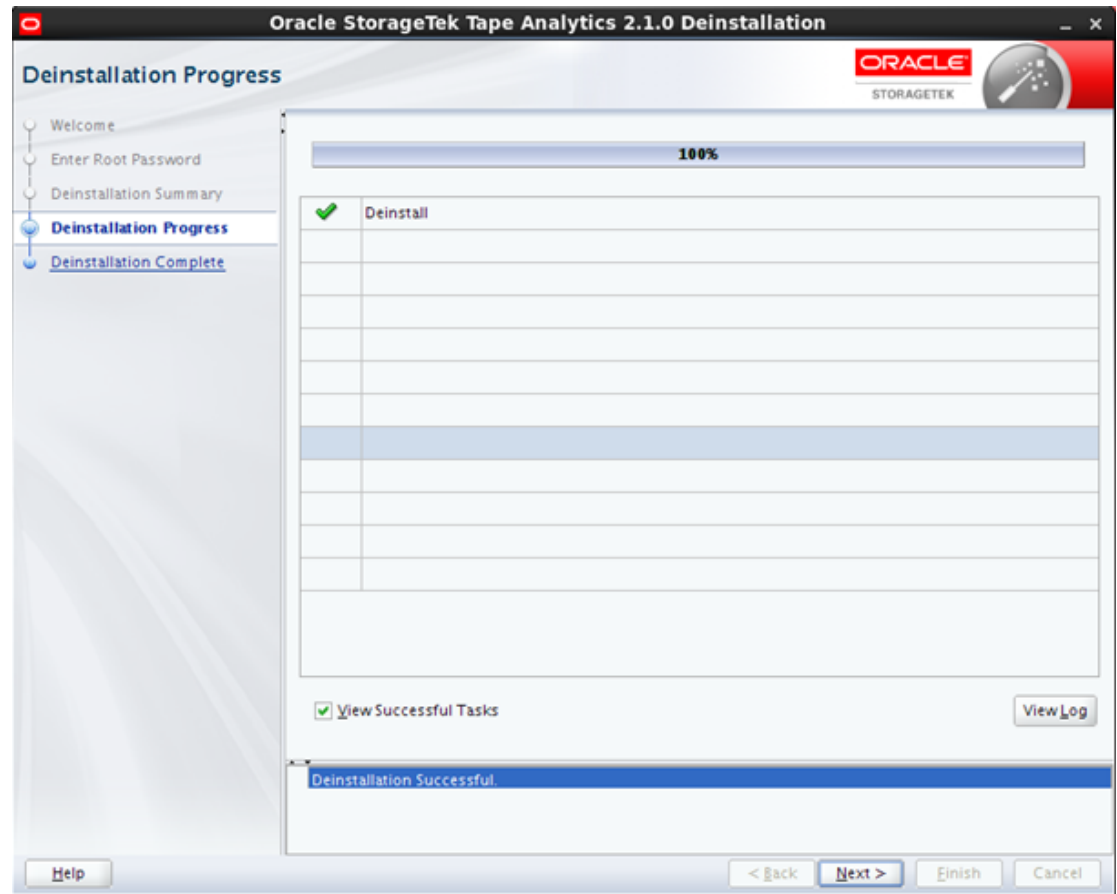
Aucun

A.3.3.2. Boutons spécifiques à l'écran

Deinstall

Cliquez pour commencer à désinstaller STA. Une fois que vous avez cliqué sur ce bouton, il n'est plus possible d'annuler ou de mettre la désinstallation en pause.

A.3.4. Progression de la désinstallation



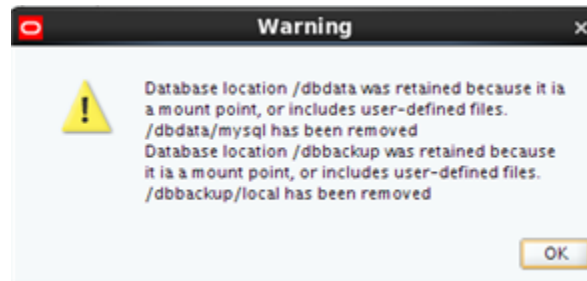
La désinstallation de STA commence, et l'écran affiche le statut de chaque tâche.

Prudence:

Ne fermez pas cette fenêtre, n'interrompez pas la désinstallation en cours, car cela pourrait laisser certains composants STA incomplets sur le serveur.

Remarque:

Si l'un des emplacements de la base de données est un point de montage sur le serveur STA, le message suivant s'affiche, indiquant que le point de montage a été conservé. Cliquez sur **OK** pour fermer le message.



Lorsque la désinstallation se termine, le message "Deinstallation Successful" apparaît dans le volet Message. Cliquez sur **Next** ou **Finish** pour accéder à l'écran final.

Si une tâche échoue, le programme de désinstallation de STA arrête et annule la désinstallation, et renvoie le serveur dans son état d'origine. Vous pouvez également visualiser le journal de désinstallation pour résoudre le problème. Pour plus d'informations, reportez-vous à la section [Section 3.4, « Journaux d'installation et de désinstallation de STA »](#).

A.3.4.1. Champs de l'écran

Aucun

A.3.4.2. Boutons spécifiques à l'écran

View Successful Tasks

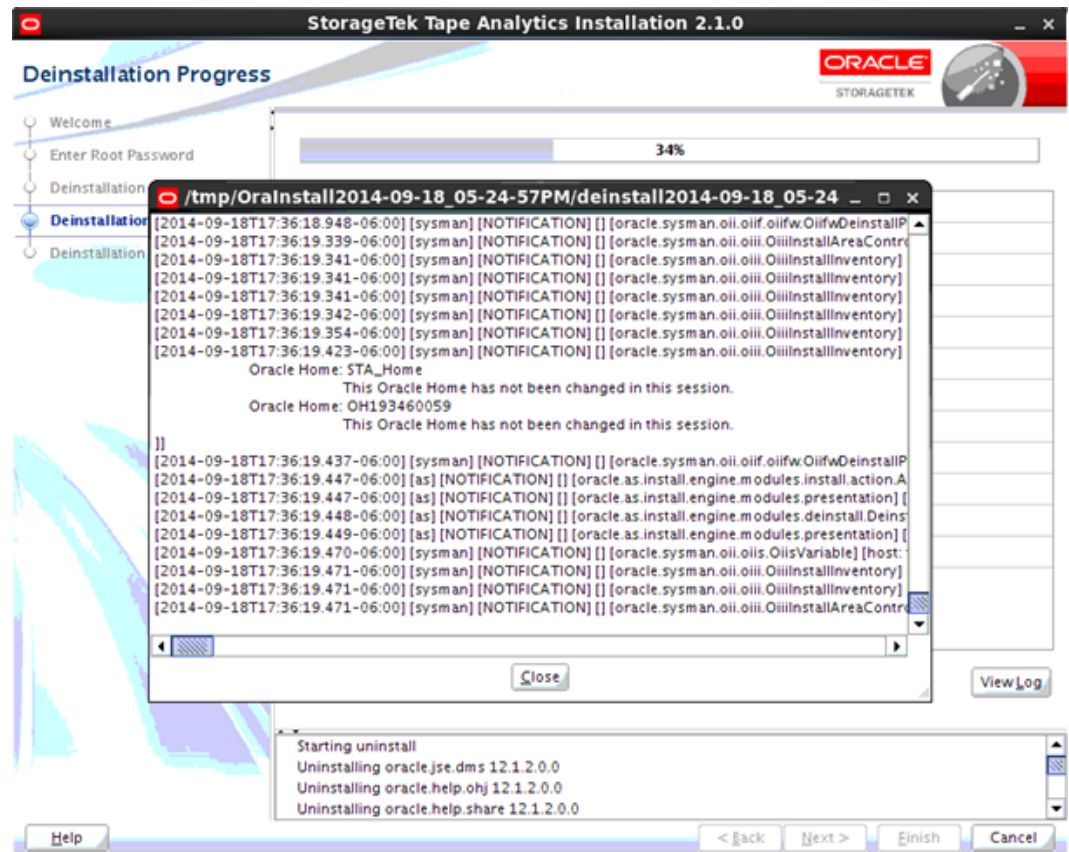
Sélectionnez la case pour inclure les sorties Succès ; cette case est cochée par défaut.

Cochez cette case pour ne faire apparaître que les sorties en Echec. Cela vous permet d'exclure les tâches réussies pour vous concentrer sur celles requérant votre attention.

View Log

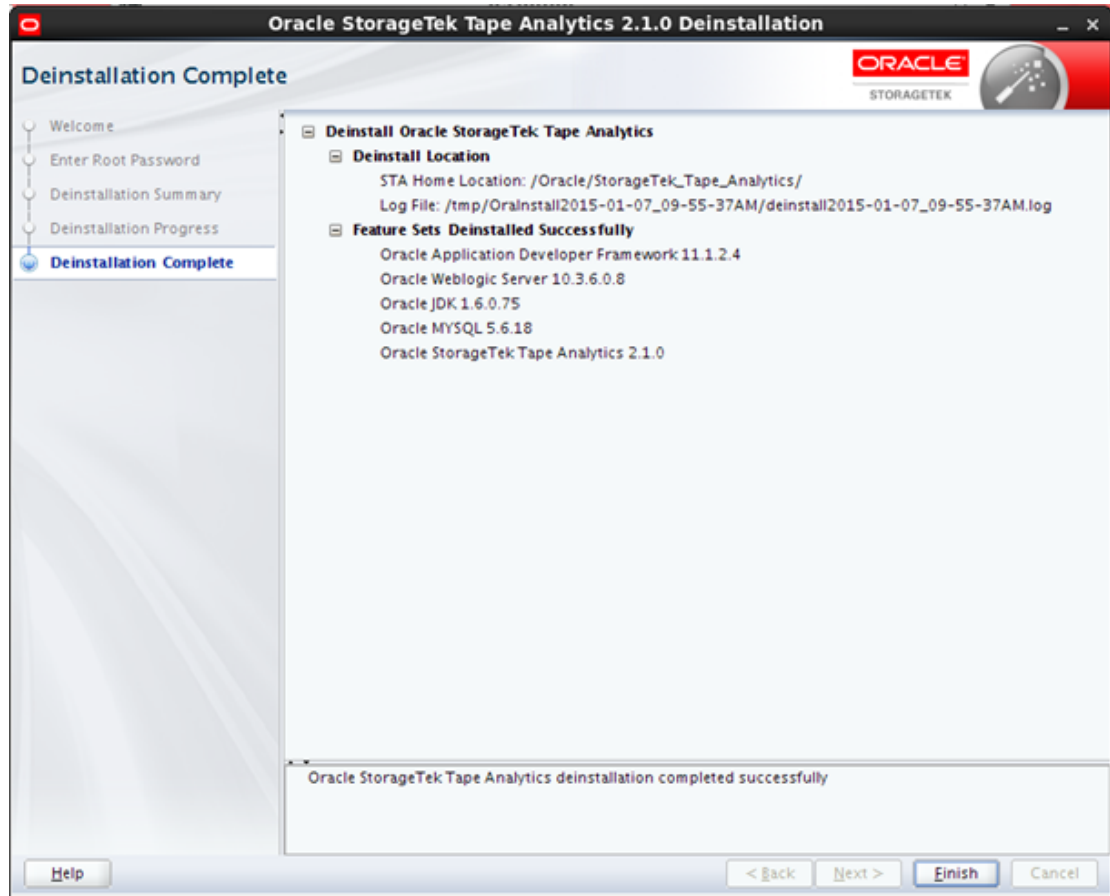
Cliquez pour afficher le journal de désinstallation dans une fenêtre séparée. La copie d'écran [Figure A.5, « Exemple d'affichage du journal de progression de l'installation »](#) en est un exemple. Cliquez sur **Close** pour fermer la fenêtre du journal.

Figure A.7. Exemple d'affichage de journal de progression de la désinstallation



Il est aussi possible de voir le journal depuis la ligne de commande Linux. Pendant que le programme de désinstallation est en cours d'exécution, les journaux sont conservés dans un sous-répertoire sous */tmp*. Pour plus d'informations, reportez-vous à la section [Section 3.4, « Journaux d'installation et de désinstallation de STA »](#).

A.3.5. Désinstallation terminée



L'écran affiche les détails suivants relatifs aux packages logiciels ayant été désinstallés :

A.3.5.1. Champs de l'écran

Aucun

A.3.5.2. Boutons spécifiques à l'écran

Finish

Cliquez pour quitter le programme de désinstallation de STA.

Programme d'installation et de désinstallation de STA en mode silencieux

Cette annexe comprend les sections suivantes :

- [Utilisation du programme d'installation et de désinstallation de STA en mode silencieux](#)
- [Fichiers et utilitaires utilisés en mode silencieux](#)
- [Tâches du programme d'installation de STA en mode silencieux](#)
- [Tâches du programme de désinstallation de STA en mode silencieux](#)
- [Options de commande du programme d'installation de STA](#)

B.1. Utilisation du programme d'installation et de désinstallation de STA en mode silencieux

Le mode silencieux vous permet de contourner l'interface graphique et de fournir les options d'installation dans un fichier de propriétés XML appelé *fichier réponse*. Vous créez le fichier réponse à l'aide de l'utilitaire de construction de fichier réponse *silentInstallUtility_version.jar*, où *version* est la version de l'utilitaire téléchargé.

Ce mode est utile pour des installations non surveillées et pour installer STA sur plusieurs machines. Grâce au fichier réponse, vous pouvez fournir un seul ensemble de paramètres et automatiser l'installation. Le mode silencieux du programme d'installation peut s'exécuter soit depuis un script, soit depuis la ligne de commande Linux.

B.1.1. Configuration requise du mode silencieux

Pour connaître les conditions minimales d'installation de STA, reportez-vous à la section [Section 3.6.2, « Vérification des prérequis d'installation »](#). En outre, le programme d'installation et de désinstallation de STA en mode silencieux présente les conditions minimales spécifiques au mode suivantes :

- Il est possible d'utiliser le mode silencieux depuis des clients Telnet, tels que PuTTY, qui n'utilisent pas le protocole X11. Le package RMP *xorg-x11-utils* doit cependant être installé sur le serveur STA.
- Avant d'utiliser le mode silencieux, vous devez télécharger le fichier *silentInstallUtility_version.jar* du site Oracle Software Delivery Cloud, et l'utiliser pour créer le fichier réponse avec mots de passe chiffrés. Pour obtenir des

instructions, reportez-vous à la section [Section B.3.2, « Création du fichier réponse du programme d'installation en mode silencieux »](#).

- Le mode silencieux nécessite également un fichier de pointeurs d'inventaire central, indiquant l'emplacement du répertoire de l'inventaire central Oracle et le groupe d'installation Oracle. S'il n'existe pas déjà, vous devrez créer le fichier manuellement. Pour plus d'informations, reportez-vous à la section [Fichiers de pointeurs d'inventaire central Oracle](#).

B.2. Fichiers et utilitaires utilisés en mode silencieux

Cette section décrit les termes et les concepts-clés utilisés pendant le processus d'installation et de désinstallation en mode silencieux.

Fichiers de pointeurs d'inventaire central Oracle

Le programme d'installation et de désinstallation de STA en mode silencieux utilise l'emplacement de l'inventaire central Oracle et le groupe d'installation Oracle identifiés dans le fichier de pointeurs d'inventaire central. Pour plus d'informations, reportez-vous à la section [Section 3.1, « Utilisateurs, groupes et emplacements utilisés par le programme d'installation de STA »](#).

Le programme d'installation et de désinstallation en mode silencieux utilise par défaut le fichier de pointeurs `/etc/oraInst.loc`. Lorsque vous inscrivez l'inventaire central Oracle, le fichier est automatiquement créé avec son nom et son emplacement. Pour plus d'informations, reportez-vous à la section [Section 3.6.7, « Inscrivez l'emplacement de l'inventaire central Oracle »](#).

Si l'emplacement de l'inventaire central Oracle n'a *pas* été inscrit, vous devez créer le fichier de pointeurs manuellement et lui donner le nom de fichier `oraInst.loc`. Pour plus d'informations, reportez-vous à la section [Section B.3.1, « Création du fichier de pointeurs d'inventaire central Oracle »](#). Vous pouvez définir l'emplacement du fichier dans n'importe quel répertoire, mais s'il n'est pas situé sous le répertoire `/etc`, vous devez utiliser le paramètre `-invPtrLoc` pour préciser l'emplacement du fichier lorsque vous exécutez le programme d'installation ou de désinstallation en mode silencieux. Pour plus d'informations sur ce paramètre, reportez-vous à la section [-invPtrLoc pointer_file](#).

Fichiers réponses du programme d'installation et de désinstallation en mode silencieux

Pour qu'il s'exécute sans surveillance, le programme d'installation et de désinstallation de STA en mode silencieux utilise les paramètres de configuration inclus dans un fichier réponse que vous créez. Vous devez utiliser le paramètre `-responseFile` pour indiquer le nom et l'emplacement de ce fichier.

Le programme d'installation et de désinstallation disposent de leur propre fichier réponse respectif. Les exemples [Exemple B.1, « Modèle de fichier réponse du programme d'installation de STA en mode silencieux »](#) et [Exemple B.2, « Modèle de fichier réponse du programme de désinstallation de STA en mode silencieux »](#) présentent le contenu et les entrées requises de chacun. Pour créer vos propres fichiers réponses, vous pouvez

copier et coller chaque modèle dans un fichier texte et apporter les modifications adaptées à votre site.

Pour garantir la sécurité du mot de passe, ne saisissez pas les mots de passe en texte clair dans le fichier réponse. Après avoir saisi les paramètres de configuration et enregistré le fichier, vous devez utiliser l'utilitaire de construction de fichier réponse pour insérer des mots de passe chiffrés dans le fichier. Pour plus d'informations, reportez-vous à la section [Utilitaire de construction du fichier réponse du programme d'installation de STA](#).

Exemple B.1. Modèle de fichier réponse du programme d'installation de STA en mode silencieux

```
[ENGINE]
#DO NOT CHANGE THIS. Response File Version=1.0.0.0.0
[GENERIC]
#The oracle storage home location. This can be an existing Oracle Storage Home or
#a new Oracle Storage Home
STORAGE_HOME=required
#Root access password var.
ROOT ACCESS PASSWORD=
RESPONSEFILE_LOC=
KEYFILE_LOC=
#DBDATA LOC
DBDATA LOC=required
#DBBACKUP LOC
DBBACKUP LOC=required
#Weblogic Admin Name Var
WEBLOGIC ADMIN NAME=required
#Weblogic Admin Password Var
WEBLOGIC ADMIN PASSWORD=
#Weblogic Admin ConfirmPassword Var
WEBLOGIC ADMIN CONFIRMPASSWORD=
#STAGUI Admin Name Var
STAGUI ADMIN NAME=required
#STAGUI Admin Password Var
STAGUI ADMIN PASSWORD=
#STAGUI Admin ConfirmPassword Var
STAGUI ADMIN CONFIRMPASSWORD=
#MySQL root password var.
MYSQL ROOT PASSWORD=
#MySQL root confirm password var.
MYSQL ROOT CONFIRM PASSWORD=
#MySQL App Name Var
MYSQL APP NAME=required
#MySQL App Password Var
MYSQL APP PASSWORD=
#MySQL App ConfirmPassword Var
MYSQL APP CONFIRMPASSWORD=
#MySQL RPTS Name Var
MYSQL RPTS NAME=required
#MySQL RPTS Password Var
MYSQL RPTS PASSWORD=
#MySQL RPTS ConfirmPassword Var
MYSQL RPTS CONFIRMPASSWORD=
#MySQL DBA Name Var
MYSQL DBA NAME=required
#MySQL DBA Password Var
MYSQL DBA PASSWORD=
#MySQL DBA ConfirmPassword Var
MYSQL DBA CONFIRMPASSWORD=
```

```
#ADMINSERVER HTTP Port Var
ADMINSERVER HTTP PORT=7019
#ADMINSERVER HTTPS Port Var
ADMINSERVER HTTPS PORT=7020
#staEngine HTTP Port Var
STAENGINE HTTP PORT=7023
#staEngine HTTPS Port Var
STAENGINE HTTPS PORT=7024
#staAdapter HTTP Port Var
STAADAPTER HTTP PORT=7025
#staAdapter HTTPS Port Var
STAADAPTER HTTPS PORT=7026
#staUi HTTP Port Var
STAUI HTTP PORT=7021
#staUi HTTPS Port Var
STAUI HTTPS PORT=7022
#Domain name var.
DOMAIN NAME=required
```

Exemple B.2. Modèle de fichier réponse du programme de désinstallation de STA en mode silencieux

```
[ENGINE]
#DO NOT CHANGE THIS. Response File Version=1.0.0.0.0
[GENERIC]
#This will be blank when there is nothing to be de-installed in distribution level
SELECTED_DISTRIBUTION=STA_Install~2.1.0.0.0
#Root access password var.
DEINSTALL_ROOT_ACCESS_PASSWORD=
RESPONSEFILE_LOC=
KEYFILE_LOC=
```

Utilitaire de construction du fichier réponse du programme d'installation de STA

L'utilitaire de construction du fichier réponse du programme d'installation vous permet d'insérer des mots de passe chiffrés dans les fichiers réponses du programme d'installation et de désinstallation en mode silencieux. L'utilitaire vous invite à saisir les mots de passe et les ajoute dans le fichier indiqué, sous forme chiffrée. Il enregistre également un fichier de clé de chiffrement dans le répertoire de votre choix.

Vous pouvez télécharger l'utilitaire de construction de fichier réponse en même temps que le programme d'installation de STA. Le nom de l'utilitaire est *silentInstallUtility_version.jar*, où *version* est la version de l'utilitaire téléchargé.

Après l'installation ou désinstallation réussie de STA, les mots de passe chiffrés sont supprimés des fichiers réponses respectifs. Pour exécuter le programme d'installation ou de désinstallation en mode silencieux une nouvelle fois, vous pouvez exécuter à nouveau l'utilitaire de construction pour fournir à nouveau les mots de passe chiffrés.

L'utilitaire de construction écrit l'emplacement du fichier réponse dans le contenu du fichier, et vous ne pourrez de fait pas déplacer le fichier réponse une fois que vous l'aurez mis à jour avec cet utilitaire.

Pour obtenir des instructions, reportez-vous à la section [Section B.3.2, « Création du fichier réponse du programme d'installation en mode silencieux »](#).

B.3. Tâches du programme d'installation de STA en mode silencieux

Avant d'exécuter ces tâches, vous aurez besoin d'obtenir les informations de configuration nécessaires, de vérifier les prérequis, et de télécharger le programme d'installation de STA. Pour obtenir des instructions, reportez-vous à la section [Section 3.6, « Tâches d'installation de STA »](#).

Pour installer STA avec le programme d'installation en mode silencieux, effectuez alors les tâches suivantes dans l'ordre indiqué.

- [Section B.3.1, « Création du fichier de pointeurs d'inventaire central Oracle »](#)
- [Section B.3.2, « Création du fichier réponse du programme d'installation en mode silencieux »](#)
- [Section B.3.3, « Exécutez le programme d'installation en mode silencieux »](#)

B.3.1. Création du fichier de pointeurs d'inventaire central Oracle

Suivez cette procédure pour créer le fichier de pointeurs d'inventaire central Oracle s'il n'existe pas déjà.

1. Connectez-vous en tant qu'utilisateur du programme d'installation Oracle.
2. Saisissez la commande suivante pour déterminer si le fichier de pointeurs d'inventaire central Oracle existe déjà.

```
$ cat /etc/oraInst.loc
```

Ci-après des exemples de sortie, selon que le fichier existe ou non :

- Le fichier n'existe pas :

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

- Le fichier existe :

```
inventory_loc=/opt/oracle/oraInventory  
inst_group=oinstall
```

3. Si le fichier existe, vous pouvez quitter cette procédure ; sinon, passez à l'étape suivante.
4. Utilisez un éditeur de texte pour créer le fichier de pointeurs d'inventaire. Il doit s'appeler *oraInst.loc*. Pour plus d'informations sur le contenu de ce fichier, reportez-vous à la section [-invPtrLoc pointer_file](#).
5. Enregistrez le fichier dans le répertoire de votre choix. Si vous enregistrez le fichier dans le répertoire */etc*, le programme d'installation et de désinstallation de STA en mode

silencieux le trouvera automatiquement ; sinon, vous devez indiquer son emplacement lorsque vous exécutez ces utilitaires.

B.3.2. Création du fichier réponse du programme d'installation en mode silencieux

Suivez cette procédure pour créer le fichier réponse du programme d'installation en mode silencieux et ajoutez-y les mots de passe chiffrés.

1. Connectez-vous en tant qu'utilisateur du programme d'installation Oracle.
2. Utilisez un éditeur de texte pour créer le fichier réponse, avec le nom de votre choix. Pour voir un modèle de fichier, reportez-vous à l'exemple [Exemple B.1, « Modèle de fichier réponse du programme d'installation de STA en mode silencieux »](#).

Copiez et collez le modèle dans un fichier texte et apportez-y les modifications adaptées à votre site. Vous devez saisir des valeurs pour toutes les valeurs marquées comme "required," et vous pouvez modifier les numéros de port en fonction de votre site.

- *RESPONSEFILE_LOC*
- *KEYFILE_LOC*
- Toutes les variables *PASSWORD*

3. Enregistrez le fichier sous le nom et dans le répertoire de votre choix.
4. Passez au répertoire où l'utilitaire de construction du fichier réponse a été téléchargé. Le nom de l'utilitaire est *silentInstallUtility_version.jar*. Par exemple :

```
$ cd /Installers
```

5. Exécutez l'utilitaire de construction du fichier réponse

```
$ java -jar silentInstallUtility_2.1.0.64.124.jar response_file
```

Où *response_file* est le chemin absolu du fichier réponse que vous avez créé.

6. Fournissez les informations demandées par chaque invite. Pour des raisons de sécurité, le mot de passe ne s'affiche pas à l'écran. Pour connaître les conditions requises de mot de passe, reportez-vous à la section [Section 3.3.1, « Comptes utilisateurs pour la gestion de STA »](#).

L'exemple [Exemple B.3, « Exemple d'exécution d'utilitaire de construction de fichier réponse du programme d'installation »](#) est un exemple d'exécution d'utilitaire de construction de fichier réponse.

Exemple B.3. Exemple d'exécution d'utilitaire de construction de fichier réponse du programme d'installation

```
$ 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. Une fois l'utilitaire terminé, vérifiez que le fichier de la clé de chiffrement a été créé sur le répertoire où se trouve le fichier réponse. Il s'agit d'un fichier caché avec un nom généré aléatoirement et commençant par "sk". Par exemple.

```
$ ls -la /Installers/.sk*
-r-----  1 oracle oinstall      17 Sep 22 12:00 .sk1414440339833
```

8. Affichez le fichier réponse et vérifiez les valeurs suivantes :
- Le *RESPONSEFILE_LOC* a été mis à jour avec l'emplacement correct du fichier réponse.
 - Le *KEYFILE_LOC* a été mis à jour avec l'emplacement correct du fichier de la clé de chiffrement.
 - Tous les mots de passe ont été mis à jour avec une valeur chiffrée.

L'exemple [Exemple B.4, « Exemple de fichier d'utilitaire du programme d'installation à l'aide de l'utilitaire de construction »](#) présente la première partie du fichier, montrant les valeurs correctes.

Exemple B.4. Exemple de fichier d'utilitaire du programme d'installation à l'aide de l'utilitaire de construction

```
$ 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. Exécutez le programme d'installation en mode silencieux

Suivez cette procédure pour installer STA à l'aide du programme d'installation en mode silencieux.

1. Passez à l'emplacement du programme d'installation de STA. Par exemple :

```
$ cd /Installers
```

2. Lancez le programme d'installation de STA en mode silencieux. Pour connaître les définitions complètes de ces paramètres, reportez-vous à la section [Section B.5, « Options de commande du programme d'installation de STA »](#).

```
$ ./sta_installer_linux64_version.bin -silent -responseFile response_file -
invPtrLoc pointer_file
```

Où :

- *version* est la version du programme d'installation de STA que vous avez téléchargé.

- `-Silencieux` indique Mode silencieux ; ce paramètre est requis.
- `-responseFile response_file` indique le chemin absolu du fichier réponse du programme d'installation en mode silencieux ; ce paramètre est requis.
- `-invPtrLoc pointer_file` indique le chemin absolu du fichier de pointeurs d'inventaire central Oracle ; ce paramètre n'est requis que si le fichier n'existe pas dans le répertoire `/etc` ou que vous souhaitez utiliser un fichier différent.

Par exemple :

```
$ ./sta_install_2.1.0.64.124_linux64.bin -silent -responseFile /Installers/SilentInstall.rsp -invPtrLoc /opt/oracle/oraInst.loc
```

3. Le programme d'installation présente les messages d'état dans la fenêtre du terminal pendant qu'il effectue les étapes d'installation suivantes. Ce processus peut prendre 30 à 60 minutes.
 - Il effectue les vérifications des prérequis sur l'environnement du serveur STA.
 - Il installe les packages logiciels inclus, y compris MySQL, WebLogic, et l'application STA.
 - Il configure l'environnement STA à l'aide des paramètres indiqués dans le fichier réponse.
 - Il lance l'application STA.

L'exemple [Exemple B.5, « Messages finaux d'installation réussie de STA en mode silencieux »](#) présente les messages apparaissant à la fin d'une installation réussie. L'exemple [Exemple B.6, « Exemple de messages finaux d'échec d'installation de STA en mode silencieux »](#) présente certains messages affichés à la fin d'une installation qui a échoué.

Exemple B.5. Messages finaux d'installation réussie de STA en mode silencieux

```
...
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.
$
```

Exemple B.6. Exemple de messages finaux d'échec d'installation de STA en mode silencieux

```
[ERROR] Rule_CalculateFreeSpace_Error. Aborting Install
Logs are located here: /tmp/OraInstall2014-09-24_09-29-29AM.
** Error during execution, error code = 256.
$
```

4. Lorsque le programme d'installation termine avec succès, vérifiez que STA est en cours d'exécution. Pour obtenir des instructions, reportez-vous à la section [Section 3.6.5, « Vérification de la réussite de l'installation. »](#).

B.4. Tâches du programme de désinstallation de STA en mode silencieux

- [Section B.4.1, « Création d'un fichier réponse du programme de désinstallation en mode silencieux »](#)
- [Section B.4.2, « Exécutez le programme de désinstallation en mode silencieux »](#)

B.4.1. Création d'un fichier réponse du programme de désinstallation en mode silencieux

Suivez cette procédure pour créer le fichier réponse du programme de désinstallation en mode silencieux et ajoutez-y les mots de passe chiffrés.

1. Connectez-vous en tant qu'utilisateur du programme d'installation Oracle.
2. Utilisez un éditeur de texte pour créer le fichier réponse du programme de désinstallation, avec le nom de votre choix. Pour voir un modèle de fichier, reportez-vous à l'exemple [Exemple B.2, « Modèle de fichier réponse du programme de désinstallation de STA en mode silencieux »](#).

Copiez et collez le modèle dans un fichier texte et laissez toutes les variables vides.

3. Enregistrez le fichier sous le nom et dans le répertoire de votre choix.
4. Passez au répertoire où l'utilitaire de construction du fichier réponse a été téléchargé. Le nom de l'utilitaire est *silentInstallUtility_version.jar*. Par exemple :

```
$ cd /Installers
```

5. Exécutez l'utilitaire de construction du fichier réponse

```
$ java -jar silentInstallUtility_2.1.0.64.124.jar response_file
```

Où *response_file* est le chemin absolu du fichier réponse que vous avez créé.

6. Fournissez les informations demandées par chaque invite. Pour des raisons de sécurité, le mot de passe ne s'affiche pas à l'écran.

[Exemple B.7, « Exemple d'exécution d'utilitaire de construction de fichier réponse du programme de désinstallation »](#) est un exemple d'exécution de l'utilitaire.

Exemple B.7. Exemple d'exécution d'utilitaire de construction de fichier réponse du programme de désinstallation

```
$ 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. Une fois l'utilitaire terminé, vérifiez que le fichier de la clé de chiffrement a été créé. Il s'agit d'un fichier caché avec un nom généré aléatoirement. Par exemple.

```
$ ls -la /Installers/.sk*
-r----- 1 oracle oinstall          17 Sep 22 12:00 .sk1414437879829
```

8. Affichez le fichier réponse et vérifiez les valeurs suivantes :
- Le mot de passe root du système a été mis à jour avec une valeur chiffrée.
 - Le `RESPONSEFILE_LOC` a été mis à jour avec l'emplacement correct du fichier réponse.
 - Le `KEYFILE_LOC` a été mis à jour avec l'emplacement correct du fichier de la clé de chiffrement.

L'exemple [Exemple B.8, « Exemple de fichier réponse du programme de désinstallation après avoir utilisé l'utilitaire de construction »](#) présente un fichier montrant les valeurs correctes.

Exemple B.8. Exemple de fichier réponse du programme de désinstallation après avoir utilisé l'utilitaire de construction

```
$ 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. Exécutez le programme de désinstallation en mode silencieux

Suivez cette procédure pour désinstaller STA à l'aide du programme de désinstallation en mode silencieux.

1. Connectez-vous en tant qu'utilisateur du programme d'installation Oracle.
2. Passez au répertoire d'accueil de STA. Par exemple :

```
$ cd /Oracle/StorageTek_Tape_Analytics
```

3. Passez au répertoire des utilitaires STA.

```
$ cd oui/bin
```

4. Lancez le programme de désinstallation de STA en mode silencieux. Pour connaître les définitions complètes de ces paramètres, reportez-vous à la section [Section B.5, « Options de commande du programme d'installation de STA »](#).

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

Où :

- *-Silencieux* indique Mode silencieux ; ce paramètre est requis.
- *-responseFile response_file* indique le chemin absolu du fichier réponse du programme de désinstallation en mode silencieux ; ce paramètre est requis.
- *-invPtrLoc pointer_file* indique le chemin absolu du fichier de pointeurs d'inventaire central Oracle ; ce paramètre n'est requis que si le fichier n'existe pas dans le répertoire */etc* ou que vous souhaitez utiliser un fichier différent.

Par exemple :

```
$ ./deinstall.sh -silent -responseFile /Installers/SilentDeinst.rsp -invPtrLoc /opt/oracle/oraInst.loc
```


5. Le programme de désinstallation présente les messages d'état dans la fenêtre du terminal pendant qu'il effectue les étapes de désinstallation suivantes. Ce processus peut prendre jusqu'à 30 minutes.

L'exemple [Exemple B.9, « Messages finaux de désinstallation réussie de STA en mode silencieux »](#) présente les messages apparaissant à la fin d'une désinstallation réussie. L'exemple [Exemple B.10, « Exemple de messages finaux d'échec de désinstallation de STA en mode silencieux »](#) présente certains messages affichés à la fin d'une désinstallation qui a échoué.

Exemple B.9. Messages finaux de désinstallation réussie de STA en mode silencieux

```
...
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.
```

Exemple B.10. Exemple de messages finaux d'échec de désinstallation de STA en mode silencieux

```
...
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. Lorsque le programme de désinstallation a terminé, vérifiez que les répertoires de STA ont été supprimés. Pour obtenir des instructions, reportez-vous à la section [Section 9.2.2, « Vérification de la réussite de la désinstallation. »](#).

B.5. Options de commande du programme d'installation de STA

Cette section fournit les informations de référence pour les options du programme d'installation de STA. Les options du mode silencieux sont exclusives au programme

d'installation et de désinstallation en mode silencieux. Les options Logging et Other peuvent être utilisées avec les deux modes du programme d'installation et de désinstallation.

B.5.1. Options du mode silencieux

Les options suivantes sont utilisées avec le programme d'installation et de désinstallation en mode silencieux.

-force

Permet l'installation en mode silencieux dans un répertoire non vide.

-invPtrLoc *pointer_file*

Utilisez le fichier de pointeurs d'inventaire central Oracle indiqué et non celui situé sous */etc/oraInst.loc.pointer_file* doit être un chemin absolu.

Le contenu du fichier d'inventaire central Oracle est le suivant :

```
inventory_loc=Oracle_central_inventory_location
inst_group=Oracle_install_group
```

Où :

- *Oracle_central_inventory_location* est le chemin absolu de l'inventaire central Oracle.
- *Oracle_install_group* est le nom du groupe d'installation Oracle.

-response, -responseFile *response_file*

Requis pour le mode silencieux. Emplacement du fichier réponse comportant les entrées pour le programme d'installation de désinstallation de STA en mode silencieux. *response_file* doit être un chemin absolu.

Pour voir des exemples de contenus de fichiers réponses du programme d'installation ou de désinstallation, reportez-vous aux exemples [Exemple B.1, « Modèle de fichier réponse du programme d'installation de STA en mode silencieux »](#) et [Exemple B.2, « Modèle de fichier réponse du programme de désinstallation de STA en mode silencieux »](#).

-silent

Requis pour le mode silencieux. Indique qu'il faut utiliser le mode silencieux. Les entrées sont prises depuis le fichier réponse indiqué.

B.5.2. Options de journalisation

Les options suivantes vous permettent de contrôler le type d'informations fournies aux journaux d'installation et de désinstallation. Elles peuvent être utilisées avec les modes graphique et silencieux.

-debug

Journalise les informations de débogage. Certaines informations de débogage apparaîtront également dans la fenêtre de console.

–logLevel *level*

Ignore les messages journaux dont les niveaux de priorité sont inférieurs à celui indiqué. Les valeurs de *level* sont les suivantes :

- grave
- avertissement
- informations
- configuration
- précis
- plus précis
- le plus précis

–printdiskusage

Journalise des informations de débogage concernant l'utilisation du disque.

–printmemory

Journalise des informations de débogage concernant l'utilisation de la mémoire.

–printtime

Journalise les informations de débogage concernant le temps écoulé.

B.5.3. Autre options

Les options de commande suivantes sont à usage général. Elles peuvent être utilisées avec les modes graphique et silencieux.

–compatibilityFile *compatibility_file*

Emplacement du fichier indiquant les modifications de dépendances de l'ensemble de fonctionnalités.

–executeSysPrereqs

Exécute les vérifications des prérequis d'environnement système pour l'exécution du programme d'installation, puis quitte sans effectuer l'installation.

–help

Affiche l'aide.

–i, –install

Utilise le mode graphique. Il s'agit de la valeur par défaut.

–J–Djava.io.tmpdir=*working_directory*

Télécharge le programme d'installation de STA dans le répertoire de travail indiqué au lieu du répertoire */tmp.working_directory* doit être un chemin absolu.

–paramFile *initialization_file*

Utilise le fichier d'initialisation indiqué au lieu de celui indiqué dans *STA_home/oui/oraparam.ini.initialization_file* doit être un chemin absolu.

Le programme d'installation de STA utilise le fichier que vous indiquez pour effectuer toutes les opérations, y compris les vérifications de prérequis. L'emplacement par défaut se situe dans le répertoire *STA_home/oui*.

Fiches de travail d'installation et de mise à niveau

Les fiches de travail de cette annexe sont des outils de planification vous facilitant l'organisation des activités et des informations à réunir pour effectuer une installation ou une mise à niveau de STA. Cette annexe comprend les sections suivantes :

- [Fiche de travail de préparation de mise à niveau](#)
- [Fiches de travail d'installation et de mise à niveau](#)
- [Fiche de travail de la configuration post-installation](#)

C.1. Fiche de travail de préparation de mise à niveau

Le tableau [Tableau C.1, « Activités de préparation de mise à niveau »](#) est uniquement utilisé pour des mises à niveau d'une version précédente de STA. Utilisez-le pour suivre les activités obligatoires et facultatives de préparation de la mise à niveau. Utilisez la colonne "Comments" pour enregistrer toute information de planification particulière. Pour plus d'informations sur cette activité, reportez-vous à la section [Section 8.5, « Tâches de préparation de la mise à niveau »](#).

Tableau C.1. Activités de préparation de mise à niveau

Activité	Commentaires	Terminé
Vérifiez que la version actuelle de STA est une version récente.		
Remarque : Si vous effectuez une mise à niveau de STA 1 .0.x, vous devez également installer une nouvelle version de Linux avant d'installer STA 2.1.0.		
Choisissez la méthode de mise à niveau à serveur unique ou à deux serveurs.		
Vérifiez que le site et le serveur cible répondent aux conditions minimales de STA 2.1.0.		
Déterminez si vous aurez besoin d'une augmentation temporaire de la taille de votre système de fichiers <i>/tmp</i> pour la mise à niveau.		
Passez en revue les changements d'environnement de STA 2.1 .0 qui peuvent impacter votre plan de mise à jour.		
Assurez-vous que tous les packages RPM requis sont installés STA (uniquement pour les mises à niveau de STA 2.0.x).		
Vérifiez que la version actuelle de STA a récemment eu une communication avec les bibliothèques contrôlées.		

Activité	Commentaires	Terminé
Vérifiez que STA procède aux échanges entre toutes les bibliothèques contrôlées.		
Déplacez les journaux de base de données et d'installation que vous souhaitez conserver vers un emplacement sûr.		
Effectuez un instantané de journal de service sur l'installation actuelle de STA (facultatif).		
Téléchargez les bundles de journaux de service que vous souhaitez conserver (facultatif).		
Renommez les modèles personnalisés avec préfixe "STA-" (facultatif).		
Enregistrez les paramètres actuels de modèle personnalisé que vous souhaitez conserver (facultatif)		
Enregistrez les paramètres de stratégie de rapport exécutif que vous souhaitez conserver (facultatif)		

C.2. Fiches de travail d'installation et de mise à niveau

Ces fiches de travail comportent les informations requises par le programme d'installation de STA. Pour plus d'informations sur les informations requises, reportez-vous à la section [Section 3.3, « Comptes et ports configurés pendant l'installation de STA »](#).

Si vous effectuez une mise à niveau d'une version précédente de STA, vous pouvez utiliser les colonnes "Current" des fiches de travail pour enregistrer les valeurs utilisées par votre installation actuelle. Utilisez les colonnes "STA 2.1.0" pour enregistrer les valeurs que vous utiliserez avec {STA.} 2.1.0.

C.2.1. Fiche de travail des emplacements et utilisateurs de l'installation

Le tableau [Tableau C.2, « Fiche de travail des emplacements et utilisateurs de l'installation »](#) comporte les comptes utilisateurs et emplacements dont vous avez besoin pour exécuter le programme d'installation de STA.

Tableau C.2. Fiche de travail des emplacements et utilisateurs de l'installation

Élément	Description	Valeur actuelle	Valeur STA 2.1.0
Groupe d'installation Oracle	Groupe Linux servant à installer et à mettre à niveau les produits Oracle sur le serveur STA. Nouveauté de STA 2.1.0	–	
Utilisateur du programme d'installation Oracle	Utilisateur Linux installant et mettant à niveau les produits Oracle sur le serveur STA. Nouveauté de STA 2.1.0	–	
Emplacement de l'inventaire central Oracle	Répertoire contenant les informations de suivi liées aux produits Oracle installés sur le serveur STA. Nouveauté de STA 2.1.0	–	
Emplacement de Oracle Storage Home	Répertoire où STA et le logiciel Oracle associé sont installés. Nouveauté de STA 2.1.0	–	

Élément	Description	Valeur actuelle	Valeur STA 2.1.0
Emplacement du programme d'installation de STA	Emplacement où sera téléchargé le programme d'installation de STA.		
Emplacement des données de la base de données STA	Emplacement de la base de données STA.		
Emplacement de sauvegarde de base de données STA	Emplacement des sauvegardes de base de données STA sur le serveur STA.		

C.2.2. Fiche de travail des comptes utilisateurs

Le tableau [Tableau C.3, « Fiche de travail des comptes utilisateurs »](#) comporte les comptes utilisateurs utilisés pour l'administration de STA, et les comptes MySQL utilisés en interne par l'application STA pour accéder à et gérer la base de données STA.

Remarque:

Les conditions requises de mot de passe ont changé avec STA 2.1.0. Pour plus d'informations, reportez-vous à la section [Section 3.2, « Conditions requises de nom d'utilisateur et de mot de passe »](#).

Tableau C.3. Fiche de travail des comptes utilisateurs

Compte	Description	Nom d'utilisateur et mot de passe actuels	Nom utilisateur et mot de passe STA 2.1.0
Administration WebLogic	Utilisée pour se connecter à la console d'administration WebLogic. Prudence : Il est impossible de récupérer le nom d'utilisateur et mot de passe de ce compte. Si ces informations d'identification sont perdues, STA doit être réinstallé.		
Administrateur STA	Utilisé pour se connecter à l'application STA avec tous les droits d'accès.		
Utilisateur root de la base de données STA	Propriétaire de la base de données MySQL. Le nom d'utilisateur prédéfini est <i>root</i> , il est impossible de le modifier. Prudence : Il est impossible de récupérer le mot de passe de ce compte.	nom d'utilisateur = <i>root</i>	nom d'utilisateur = <i>root</i>
Utilisateur de l'application de la base de données STA	STA utilise ce compte pour se connecter à la base de données.		
Utilisateur des rapports de la base de données STA	Les applications non-STA et tierces utilisent ce compte pour se connecter à la base de données.		
Administrateur de la base de données STA	Les utilitaires d'administration et de contrôle STA utilisent ce compte pour se connecter à la base de données,		

Compte	Description	Nom d'utilisateur et mot de passe actuels	Nom utilisateur et mot de passe STA 2.1.0
	principalement pour configurer et exécuter les sauvegardes programmées.		

C.2.3. Fiches de travail des numéros de port

Le chapitre [Tableau C.4, « Ports externes non configurables »](#) comporte les ports externes utilisés par l'application STA. Ces numéros de port sont prédéfinis et ne peuvent pas être modifiés. Utilisez la colonne "Verified" pour consigner que vous avez vérifié avec votre administrateur réseau que ces ports sont ouverts et disponibles.

Tableau C.4. Ports externes non configurables

Description du port	Protocole	Port STA 2.1.0	Vérfié
Secure Shell. Utilisé pour se connecter depuis le serveur STA à la sauvegarde de la base de données STA et aux bibliothèques contrôlées.	SSH	22	
Utilisé pour transmettre des demandes SNMP (Simple Network Management Protocol, Protocole de gestion de réseau simple) aux bibliothèques contrôlées.	SNMP	161	
Utilisé pour recevoir des notifications SNMP (déroutements) depuis les bibliothèques contrôlées.	SNMPTRAP	162	

Le chapitre [Tableau C.5, « Ports internes et externes configurables »](#) comporte les ports internes et externes configurables utilisés par l'application STA. Utilisez la colonne "Verified" pour consigner que vous avez vérifié avec votre administrateur réseau que ces ports sont ouverts et disponibles.

Remarque:

Les ports par défaut de la console d'administration WebLogic ont été modifiés pour STA 2.1.0.

Tableau C.5. Ports internes et externes configurables

Description du port	Type	Protocole	Port par défaut STA 2.1.0	Port actuel	Port STA 2.1.0	Vérfié
Port non sécurisé de la console d'administration WebLogic (le numéro de port par défaut pour STA 1.0.x et 2.0.x était 7001)	Externe	HTTP	7019			
Port sécurisé de la console d'administration WebLogic (le numéro de port par défaut pour STA 1.0.x et 2.0.x était 7002)	Externe	HTTPS	7020			
Port non sécurisé du serveur staUi géré, qui gère l'interface graphique de STA	Externe	HTTP	7021			
Port sécurisé du serveur staUi géré	Externe	HTTPS	7022			
Port non sécurisé du serveur staEngine géré, qui gère les éléments internes de STA	Interne	HTTP	7023			
Port sécurisé du serveur staEngine géré	Interne	HTTPS	7024			

Description du port	Type	Protocole	Port par défaut STA 2.1.0	Port actuel	Port STA 2.1.0	Vérifié
Port non sécurisé du serveur staAdapter géré, qui gère la communication SNMP avec les bibliothèques contrôlées	Interne	HTTP	7025			
Port sécurisé du serveur staAdapter géré	Interne	HTTPS	7026			

C.2.4. Fiche de travail du nom de domaine

Le tableau [Tableau C.6, « Nom de domaine de l'entreprise »](#) comporte le nom de domaine complet de votre site utilisé par l'agent de diagnostic distant (RDA) de Oracle lors de la génération des journaux de service Oracle.

Tableau C.6. Nom de domaine de l'entreprise

Informations requises	Valeur actuelle	Valeur STA 2.1.0
Nom de domaine d'entreprise (par exemple, us.oracle.com)		

C.3. Fiche de travail de la configuration post-installation

Le chapitre [Tableau C.7, « Informations de configurations de l'utilisateur SNMP v3 »](#) comporte les informations dont vous avez besoin pour configurer la connexion SNMP entre STA et les bibliothèques contrôlées ; le même utilisateur SNMP v3 doit être configuré sur chaque bibliothèque contrôlée et sur chaque instance STA. Pour connaître les détails complets des informations nécessaires, reportez-vous à la section [Section 5.1.1.1, « Utilisateur SNMP v3 unique »](#).

Tableau C.7. Informations de configurations de l'utilisateur SNMP v3

Informations requises	Valeurs précédentes	Valeurs STA 2.1.0
Nom d'utilisateur SNMP v3		
Mot de passe d'autorisation SNMP v3 (Autorisation)		
Mot de passe de chiffrement de confidentialité SNMP v3 (Confidentialité)		
Communauté d'utilisateurs SNMP v2c		
Communauté de dérouterments SNMP v2c		

Configuration des certificats de sécurité

Oracle fournit des certificats de sécurité générés automatiquement à utiliser avec les ports HTTPS/SSL. Lors de l'installation, Oracle utilise la commande Java keytool pour générer un certificat sur le serveur Oracle à l'aide du nom d'hôte du serveur. Vous pouvez éventuellement remplacer le certificat Oracle par votre propre certificat approuvé par une autorité de certification sélectionnée (VeriSign, par exemple).

Ce chapitre se compose de la section suivante :

- [Tâches de configuration du certificat de sécurité](#)

D.1. Tâches de configuration du certificat de sécurité

Si vous souhaitez utiliser un certificat de sécurité différent de celui par défaut, suivez ces procédures dans l'ordre indiqué.

- [Section D.1.1, « Etablissement de la connexion HTTPS/SSL initiale »](#)
- [Section D.1.2, « Reconfiguration de WebLogic pour qu'il utilise un certificat de sécurité différent »](#)
- [Section D.1.3, « Remplacement du certificat Oracle »](#)

Remarque:

Les procédures suivantes utilisent Mozilla Firefox sur une plateforme Windows.

D.1.1. Etablissement de la connexion HTTPS/SSL initiale

1. Lancez un navigateur Web pris en charge sur votre ordinateur et saisissez la version HTTPS/SSL de l'URL de l'application STA.

`https://STA_host_name:port_number/STA/`

Où :

- *host_name* est le nom d'hôte du serveur STA.
- *port_number* est le numéro de port STA que vous avez indiqué pendant l'installation. Par défaut, le port HTTP est 7021, et le port HTTPS est 7022.
- *STA* doit être saisi en majuscules.

Par exemple :

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

L'écran The Connection is Untrusted s'affiche.

2. Sélectionnez **I Understand the Risks**, puis cliquez sur **Add Exception**.

L'écran Add Security Exception s'affiche.

3. Cliquez sur **View**.

L'écran Certificate Viewer s'affiche. Le certificat n'est *pas* indiqué comme étant vérifié car il ne provient pas d'une autorité de certification.

4. Pour examiner le certificat, cliquez sur l'onglet **Details**.
5. Dans le volet Certificate Fields, sélectionnez **issuer**. Voici un exemple d'affichage. CN indique le nom du serveur sur lequel le certificat a été généré.

```
CN = staserver.example.com
OU = Tape Systems
O = Oracle America Inc
L = Redwood City
ST = California
C = USA
```

6. Cliquez sur **Close** pour retourner à l'écran Add Security Certificate.
7. Sélectionnez **Confirm Security Exception**.

Le certificat est ajouté au serveur STA, vous pouvez désormais utiliser HTTPS avec le certificat.

D.1.2. Reconfiguration de WebLogic pour qu'il utilise un certificat de sécurité différent

1. Ouvrez une fenêtre de navigateur et saisissez l'URL de la console d'administration WebLogic. Par défaut, le port HTTP est 7019, le port HTTPS est 7020.

`https://your_hostname:port number/console/`

Par exemple :

`https://staserver.company.com:7019/console/`

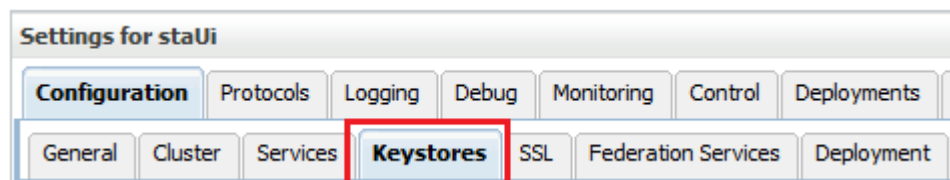
2. Connectez-vous à l'aide du nom d'utilisateur et du mot de passe de la console d'administration WebLogic que vous avez définis lors de l'installation de STA.
3. Dans la section Domain Structure, sélectionnez **Environment**, puis **Servers**.



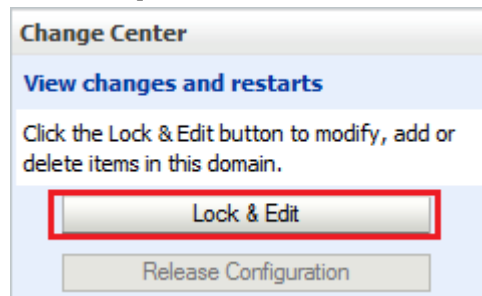
4. Dans le tableau Servers, sélectionnez le lien actif **staUi** (sélectionnez le nom lui-même et non la case).

<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	

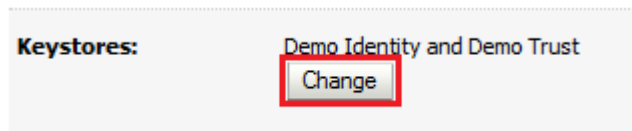
5. Sélectionnez l'onglet **Keystores**.



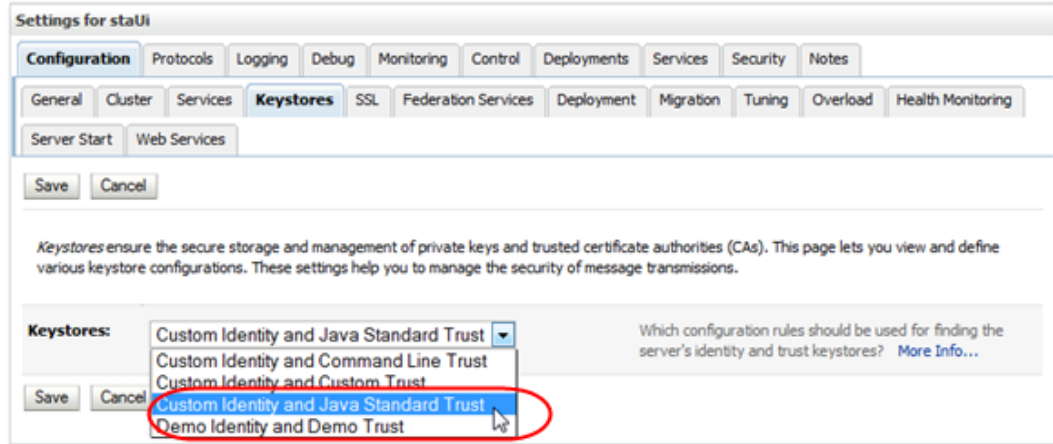
6. Dans la section Change Center, cliquez sur **Lock & Edit**.



7. Dans la section Keystores, cliquez sur **Change**.



8. Dans le menu Keystores, sélectionnez **Custom Identity and Java Standard Trust**.



9. Cliquez sur **Save**.

10. Remplissez l'écran Keystores de la manière suivante :

- **Custom Identity Keystore** : chemin et fichier du fichier de clés privées.
- **Custom Identity Keystore Type** : type de keystore. Si vous effectuez une configuration pour l'authentification RACF, saisissez PKCS12.
- **Custom Identity Keystore Passphrase** : mot de passe fourni par l'administrateur système MVS.
- **Java Standard Trust Keystore Passphrase** : nouveau mot de passe du fichier Java Standard Trust Keystore.

Prudence:

Si vous oubliez ces mots de passe, vous devrez réinstaller STA.

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. Cliquez sur **Save**.
12. Sélectionnez l'onglet **SSL**.

Settings for staUi

Configuration Protocols Logging Debug Monitoring Control

General Cluster Services Keystores **SSL** Federation Services

13. Saisissez l'alias de clé privée et la phrase de passe de clé privée fournis par le programmeur du système MVS.

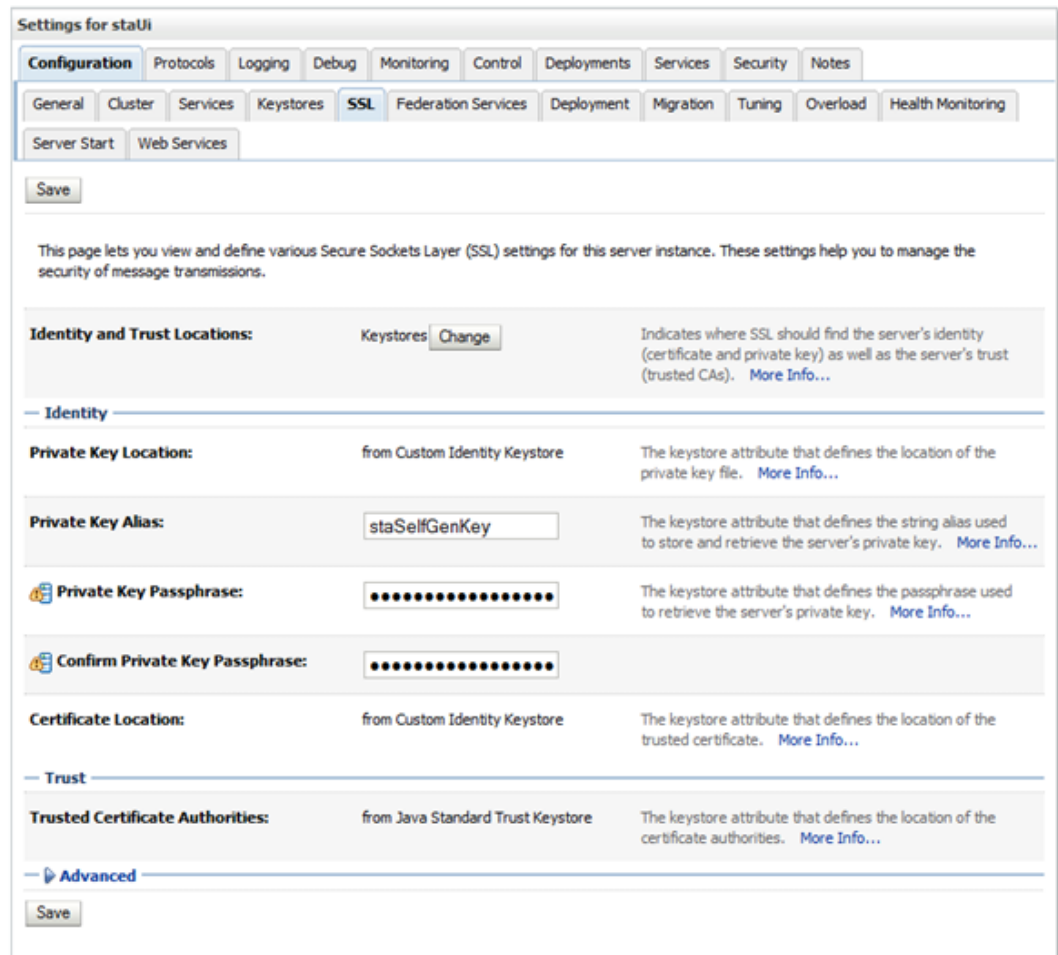
Remarque:

Pour définir l'alias de clé privée, utilisez la commande `keytool` dans la ligne de commande du système. Par exemple :

```
# keytool -list -keystore CLTBI.PKCS12DR.D080411 -storetype PKCS12
Enter keystore password: (password from the MVS sysadmin)
Keystore type: PKCS12
Keystore provider: SunJSSE
```

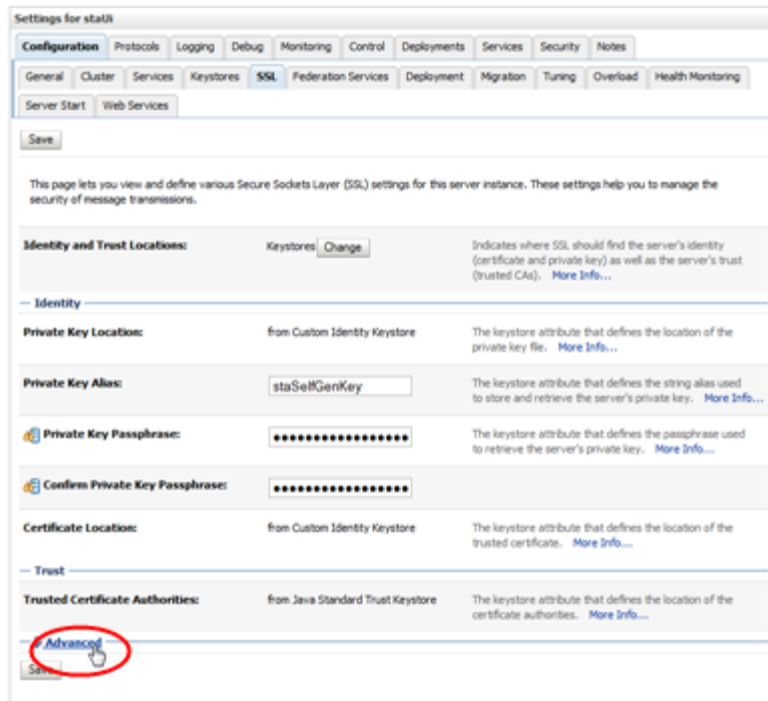
Your keystore contains 1 entry

```
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. Cliquez sur **Save**.

15. Dans la section Trusted Certificate Authorities, cliquez sur **Advanced**.



16. Remplissez la section Advanced de l'écran SSL comme suit :

- a. Sélectionnez la case **Use Server Certs**.
- b. Dans le menu **Two Way Client Cert Behavior**, sélectionnez Client Certs Requested But Not Enforced.
- c. Dans les menus **Inbound Certification Validation** et **Outbound Certificate Validation**, sélectionnez Builtin SSL Validation Only.

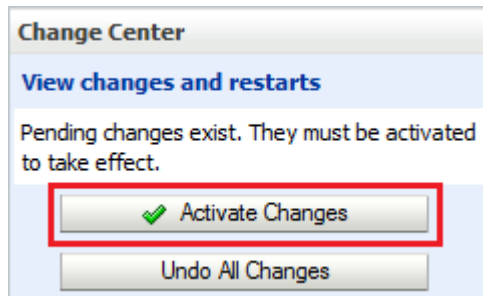
Advanced

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. Cliquez sur **Save**.

18. Dans la section Change Center, cliquez sur **Activate Changes**.



19. Déconnectez-vous de WebLogic.

20. Arrêtez puis relancez STA avec la commande *STA*. Pour plus d'informations sur l'utilisation de la commande, reportez-vous au guide *Guide d'administration de STA*.

```
# STA stop all
# STA start all
```

D.1.3. Remplacement du certificat Oracle

1. Lancez un navigateur Web pris en charge sur votre ordinateur et saisissez la version HTTPS/SSL de l'URL de l'application STA.

```
https://STA_host_name:port_number/STA/
```

Où :

- *host_name* est le nom d'hôte du serveur STA.
- *port_number* est le numéro de port STA que vous avez indiqué pendant l'installation. Par défaut, le port HTTP est 7021, et le port HTTPS est 7022.
- *STA* doit être saisi en majuscules.

Par exemple :

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

2. Sélectionnez **I Understand the Risks** sur l'écran This Connection is Untrusted.
3. Cliquez sur **Add Exception**.
4. Pour définir un certificat pour votre entreprise, cliquez sur **Get Certificate** à l'écran Add Security Certificate, puis sélectionnez le fichier adéquat.
5. Cliquez sur **Confirm Security Exception**.

Configuration d'un fournisseur de service de sécurité pour STA

Les utilisateurs doivent s'identifier avant de voir leur accès accordé à STA. Il est possible de créer des utilisateurs localement, dans STA, ou d'utiliser des fournisseurs de services de sécurité (SSP), pour fournir le contrôle d'accès à STA.

Cette annexe décrit l'utilisation de WebLogic OpenLDAP (Lightweight Directory Access Protocol) et IBM RACF (Resource Access Control Facility) pour le contrôle d'accès à STA. Elle contient les sections suivantes :

- [Contrôle d'accès STA via WebLogic OpenLDAP](#)
- [Tâches de contrôle d'accès STA via IBM RACF](#)

Pour créer des utilisateurs avec l'application STA, reportez-vous au guide *Guide de l'utilisateur STA*.

E.1. Contrôle d'accès STA via WebLogic OpenLDAP

Suivez cette procédure pour configurer OpenLDAP pour STA.

E.1.1. Configuration de WebLogic OpenLDAP

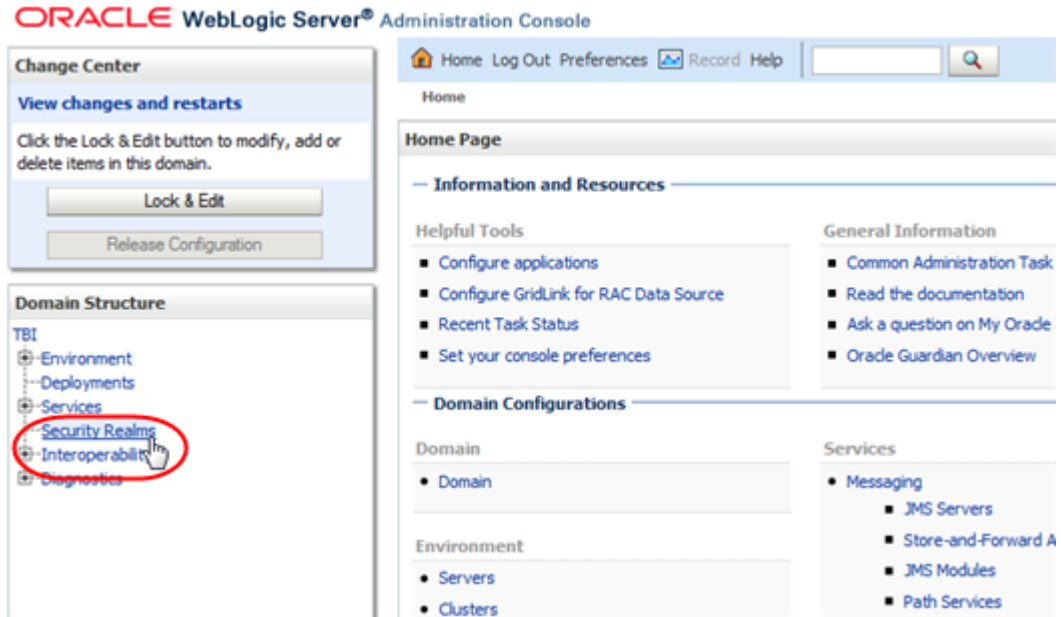
1. Allez à l'écran de connexion de la console WebLogic à l'aide du numéro de port HTTP (7019 par défaut pour STA 2.1.0) ou HTTPS (7020 par défaut pour STA 2.1.0) que vous avez sélectionné pendant l'installation de STA.

```
https://yourHostName:PortNumber/console/
```

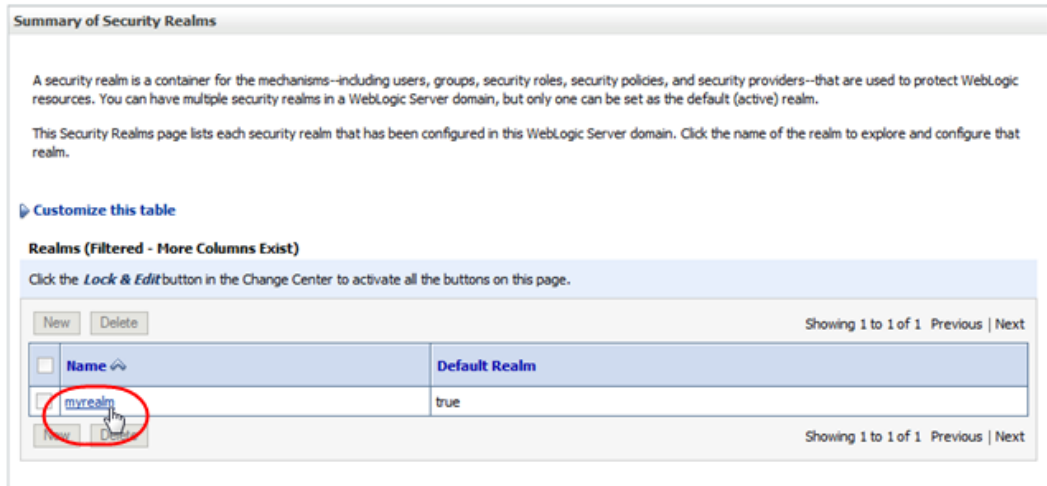
Par exemple :

```
https://sta_server:7020/console
```

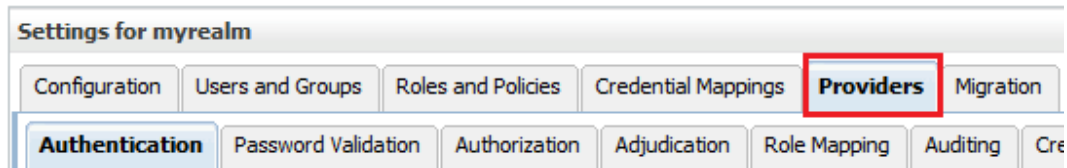
2. Connectez-vous à l'aide du nom d'utilisateur et du mot de passe de la console d'administration WebLogic que vous avez définis lors de l'installation de STA.
3. Dans la section Domain Structure, cliquez sur **Security Realms**.



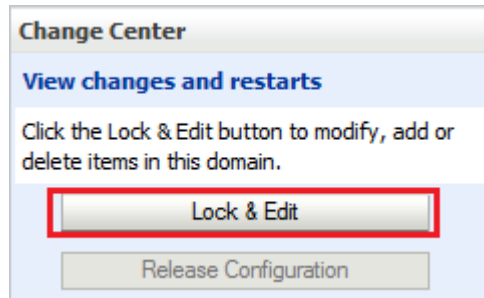
4. Dans le tableau Realms, sélectionnez le lien actif **myrealm** (sélectionnez le lien lui-même, et non sa case).



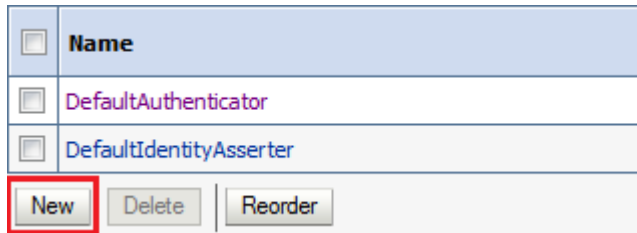
5. Cliquez sur l'onglet **Providers**.



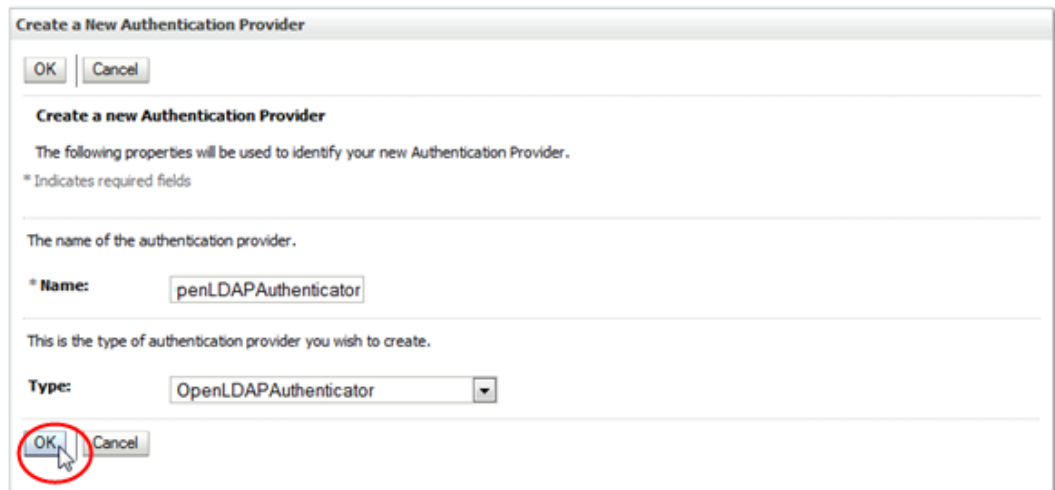
6. Dans la section Change Center, cliquez sur **Lock & Edit**.



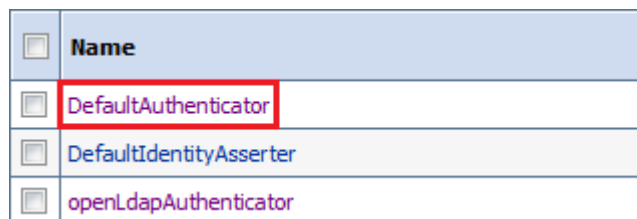
7. Dans la section Authentication Providers, cliquez sur **New**.



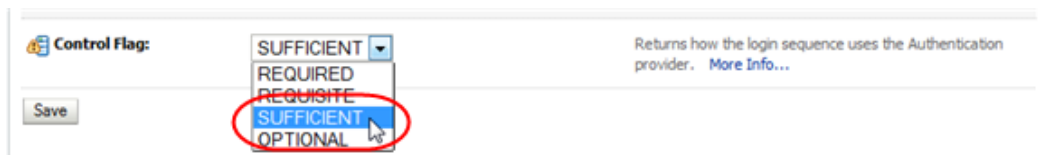
8. Saisissez le nom du fournisseur d'authentification que vous souhaitez créer (OpenLdapAuthenticator, par exemple), et sélectionnez OpenLDAPAuthenticator dans le menu **Type**. Cliquez sur **OK**.



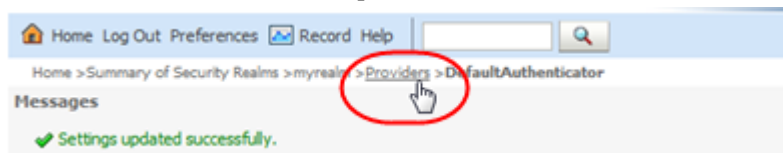
9. Sélectionnez le lien actif **DefaultAuthenticator** (sélectionnez le lien lui-même et non la case).



10. Dans le menu **Control Flag**, sélectionnez Sufficient, puis cliquez sur **Save**.



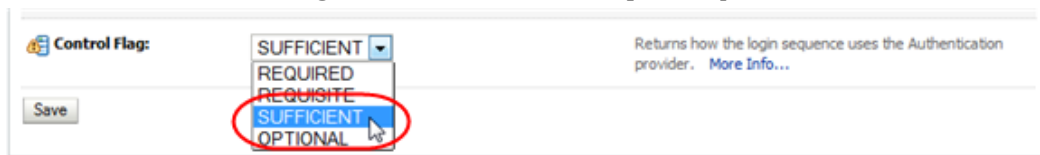
11. Cliquez sur le lien localisateur **Providers** pour revenir à l'écran Authentication Providers.



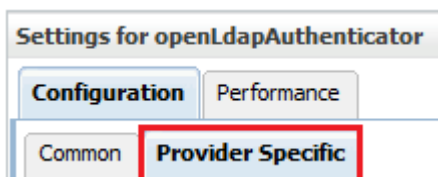
12. Dans le tableau Authentication Providers, sélectionnez le nom d'authentificateur Open LDAP créé à l'étape 8 (sélectionnez le nom lui-même et non la case).

<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. Dans le menu **Control Flag**, sélectionnez Sufficent, puis cliquez sur **Save**.



14. Cliquez sur l'onglet **Provider Specific**.

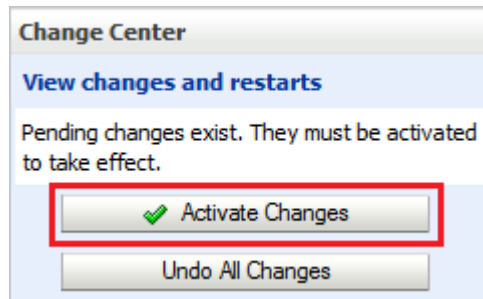


15. Remplissez les champs de l'écran selon les configurations requises de votre site.

L'exemple suivant s'applique au serveur *Ises-ldap1* et chaque environnement client est spécifique.

- Host = *Ises-ldap1*
- Port = *389*
- Principal = laissez vide
- Credential = laissez vide
- 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))*

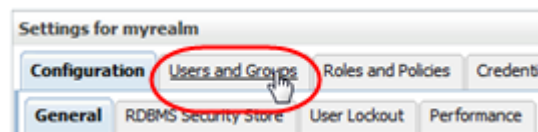
16. Cliquez sur **Save**.
17. Dans la section Change Center, cliquez sur **Activate Changes**.



18. Suivez les étapes suivantes pour tester la configuration.
 - a. Déconnectez-vous de la console d'administration WebLogic.
 - b. Arrêtez et redémarrez STA à l'aide de la commande *STA*. Pour plus d'informations sur l'utilisation de la commande, reportez-vous au guide *Guide d'administration de STA*.

```
# STA stop all
# STA start all
```

- c. Connectez-vous à la console WebLogic.
- d. Dans la section Domain Structure, sélectionnez **Security Realms**.
- e. Dans le tableau Realms, sélectionnez le lien actif **myrealm** (sélectionnez le lien lui-même, et non sa case).
- f. Cliquez sur l'onglet **Users and Groups**.



- g. Dans les onglets **Users** et **Groups**, vérifiez que les entrées existent dans la colonne Provider pour le fournisseur OpenLDAP.

E.2. Tâches de contrôle d'accès STA via IBM RACF

Suivez les procédures suivantes pour configurer l'authentification IBM RACF (Resource Access Control Facility) pour STA. Les procédures doivent être effectuées dans l'ordre indiqué.

- [Section E.2.1, « Tâche 1 : Vérification des conditions minimales requises pour le mainframe IBM RACF »](#)
- [Section E.2.2, « Tâche 2 : Activation de la prise en charge du mainframe pour l'autorisation STA RACF »](#)
- [Section E.2.3, « Tâche 3 : Configuration AT-TLS »](#)
- [Section E.2.4, « Tâche 4 : Création des profils RACF utilisés par la routine CGI »](#)

- [Section E.2.5, « Tâche 5 : Importation du fichier de certificat et du fichier de clé privée \(facultatif\) »](#)
- [Section E.2.6, « Tâche 6: Test de la routine CGI »](#)
- [Section E.2.7, « Tâche 7 : Configuration de RACF/SSP pour la console WebLogic »](#)
- [Section E.2.8, « Tâche 8: Configuration de SSL entre STA et RACF »](#)
- [Section E.2.9, « Tâche 9 : Configuration du serveur WebLogic »](#)
- [Section E.2.10, « Tâche 10: Installation de RACF/SSP sur la console WebLogic »](#)

Remarque:

STA prend en charge les produits tiers compatibles avec IBM RACF — par exemple, l'autorité de certification ACF-2 et Top Secret. Il incombe à la personne responsable de l'installation de STA ou à l'administrateur de sécurité, d'exécuter les commandes correspondant au produit de sécurité installé.

E.2.1. Tâche 1 : Vérification des conditions minimales requises pour le mainframe IBM RACF

Pour connaître toutes les conditions minimales requises de RACF, reportez-vous au guide *Guide des conditions requises pour l'installation de STA*.

E.2.2. Tâche 2 : Activation de la prise en charge du mainframe pour l'autorisation STA RACF

Le mainframe du service RACF pour STA est fourni par une routine CGI qui fait partie du composant SMC pour ELS 7.0 et 7.1. Cette routine CGI est appelée par le serveur SMC HTTP et utilise les profils RACF définis dans la classe FACILITY.

Pour que STA utilise RACF comme moyen d'authentification d'accès sur le mainframe, vous devez définir une tâche SMC qui exécute le serveur HTTP. Vous pouvez trouver des informations concernant cette action dans le document ELS *Configuring and Managing SMC*.

Remarque:

La tâche SMC doit correspondre à la règle AT-TLS définie. Vous pouvez également permettre à la définition AT-TLS d'utiliser un nom de tâche générique (par exemple, SMCW).

L'utilisation d'un identificateur STC à valeur ajoutée (par exemple, NOMDETACHE.TACHE) peut entraîner un échec de la connexion de la routine CGI.

Le numéro de port utilisé pour le serveur HTTP doit correspondre à celui défini dans la console WebLogic et l'hôte doit correspondre au nom IP de l'hôte où la tâche SMC est exécutée.

Remarque:

Un SMC existant peut être utilisé s'il existe sur l'hôte où l'autorisation RACF doit être effectuée. Dans ce cas, utilisez le numéro de port du serveur HTTP existant lorsque vous effectuez la configuration WebLogic.

E.2.3. Tâche 3 : Configuration AT-TLS

AT-TLS est une solution de chiffrement pour les applications TCP/IP, transparente pour le serveur et le client d'applications. Le chiffrement et le déchiffrement de paquets ont lieu dans l'espace d'adressage z/OS TCPIP au niveau du protocole TCP. Les conditions AT-TLS requises pour l'autorisation RACF sont indiquées dans le guide *Guide des conditions requises pour l'installation de STA*.

Les commandes RACF suivantes répertorient le statut des différents objets RACF que vous définirez dans le processus de configuration :

- `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`

Pour configurer AT-TLS, procédez comme suit :

1. Indiquez le paramètre suivant dans le jeu de données de profil TCPIP pour activer la fonction AT-TLS.

```
TCPCONFIG TTLS
```

Cette déclaration peut est placée dans le fichier TCP OBEY.

2. Configuration de l'agent de stratégie (PAGENT)

L'espace d'adressage de l'agent de stratégie indique quel trafic TCP/IP est chiffré.

- a. Saisissez la tâche démarrée JCL de PAGENT.

Par exemple :

```
//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. Saisissez les variables d'environnement de *PAGENT*. Le jeu de données *pagentdataset* comporte les variables d'environnement de *PAGENT*.

Par exemple :

```
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
```

Dans cet exemple, */etc/pagent.conf* comporte les paramètres de configuration de *PAGENT*. Utilisez votre propre fuseau horaire pour le paramètre *TZ*.

- c. Configurez *PAGENT*.

Par exemple :

```
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
  TTLConnectionActionRef cAct1~TBI_ICSF
}
TTLGroupAction gAct1~TBI_ICSF
{
  TTLEnabled On
  Trace 2
}
TTLEnvironmentAction eAct1~TBI_ICSF
{
  HandshakeRole Server
  EnvironmentUserInstance 0
  TLSKeyringParmsRef keyR~ZOS
}
TTLConnectionAction cAct1~TBI_ICSF
{
  HandshakeRole ServerWithClientAuth
```

```

TTLSCipherParmsRef cipher1~AT-TLS__Gold
TTLSConnectionAdvancedParmsRef cAdv1~TBI_ICSF
CtracedClearText Off
Trace 2
}
TTLSConnectionAdvancedParms cAdv1~TBI_ICSF
{
ApplicationControlled Off
HandshakeTimeout 10
ResetCipherTimer 0
CertificateLabel certificatelabel
SecondaryMap Off
}
TTLSSKeyringParms keyR~ZOS
{
Keyring keyringname
}
TTLSCipherParms cipher1~AT-TLS__Gold
{
V3CipherSuites TLS_RSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites TLS_RSA_WITH_AES_128_CBC_SHA
}

```

où :

- *localtcpipaddress* : Adresse TCP/IP locale pour le serveur HTTP
- *remotetcpipaddress* : Adresse TCP/IP distante pour le client STA. Il peut s'agir de ALL pour toutes les adresses TCP/IP
- *localportrange* : Port local du serveur HTTP (indiqué au démarrage de HTTP ou de SMC)
- *remoteportrange* : Plage de ports distants (1024-65535 pour tous les ports éphémères)
- *HTTPserverJobname* : Nom de tâche du serveur HTTP
- *certificateLabel* : Etiquette de la définition du certificat
- *keyringname* : Nom de la définition du trousseau de clés RACF

3. Activez les classes RACF. Vous pouvez utiliser les panneaux RACF ou la CLI.

Les classes RACF incluent :

- *DIGTCERT*
- *DIGTNMAP*
- *DIGTRING*

L'option RACLIST doit être appliquée à la classe *SERVAUTH* pour empêcher la fin anormale de *PORTMAP* et de *RXSERV*.

```
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. Définition des trousseaux de clés et des certificats RACF

- a. Saisissez les commandes RACF suivantes pour créer des trousseaux de clés et des certificats :

```
RACDCERT ID(stcuser) ADDRING(keyringname)
```

où :

- *stcuser* : ID d'utilisateur RACF associé à l'espace d'adressage TCPIP
- *keyringname* : nom du trousseau de clés. Il doit correspondre au trousseau de clés indiqué dans la configuration PAGENT

```
RACDCERT ID(stcuser) GENCERT CERTAUTH SUBJECTSDN(CN('serverdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('calabel') TRUST
SIZE(1024) KEYUSAGE(HANDSHAKE, DATAENCRYPT, CERTSIGN)
```

Remarque:

Il s'agit du certificat CA pour le système STA.

où :

- *stcuser* : ID d'utilisateur RACF associé à l'espace d'adressage TCPIP
- *serverdomainname* : Nom de domaine du serveur z/OS (par exemple, *MVSA.COMPANY.COM*)
- *companyname* : Nom de l'entreprise
- *unitname* : Nom de l'entité de l'entreprise
- *country* : Pays
- *calabel* : Etiquette pour l'autorité de certification (par exemple, *CATBISERVER*)

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('serverdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('serverlabel') TRUST
SIZE(1024) SIGNWITH(CERTAUTH LABEL('calabel'))
```

Remarque:

Il s'agit du certificat SERVER.

où :

- *stcuser* : ID d'utilisateur RACF associé à l'espace d'adressage TCPIP
- *serverdomainname* : Nom de domaine du serveur z/OS (par exemple, MVSA .COMPANY.COM)
- *companyname* : : Nom de l'entreprise
- *unitname* : : Nom de l'entité de l'entreprise
- *country* : Pays
- *serverlabel* : Etiquette pour le certificat de serveur (par exemple, TBISERVER)
- *calabel* : Etiquette pour l'autorité de certification, indiquée dans la définition du certificat CA

```
RACDCERT ID(stcuser) GENCERT SUBJECTSDN(CN('clientdomainname')
O('companyname') OU('unitname') C('country')) WITHLABEL('clientlabel') TRUST
SIZE(1024) SIGNWITH(CERTAUTH LABEL('calabel'))
```

Remarque:

Il s'agit du certificat CLIENT.

où :

- *stcuser* : ID d'utilisateur RACF associé à l'espace d'adressage TCPIP
- *clientdomainname* : Nom de domaine du client STA (par exemple, TBIA .COMPANY.COM)
- *companyname* : Nom de l'entreprise
- *unitname* : Nom de l'entité de l'entreprise
- *country* : Pays
- *clientlabel* : Etiquette du certificat de serveur –TBICLIENT
- *calabel* : Etiquette pour l'autorité de certification, indiquée dans la définition du certificat CA

- b. Les commandes suivantes connectent les certificats CA, SERVER et CLIENT au trousseau de clés indiqué dans la configuration PAGENT :

```
RACDCERT ID(stcuser) CONNECT(CERTAUTH LABEL('calabel') RING('keyringname')
USAGE(CERTAUTH))
```

où :

- *stcuser* : ID d'utilisateur RACF associé à l'espace d'adressage TCPIP
- *calabel* : Etiquette pour l'autorité de certification, indiquée dans la définition du certificat CA
- *keyringname* : Nom du trousseau de clés. Il doit correspondre au trousseau de clés spécifié dans la configuration PAGENT

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('serverlabel')
RING('keyringname') DEFAULT USAGE(PERSONAL))
```

où :

- *stcuser* : ID d'utilisateur RACF associé à l'espace d'adressage TCPIP
- *serverlabel* : Etiquette pour le certificat de serveur
- *keyringname* : Nom du trousseau de clés. Il doit correspondre au trousseau de clés indiqué dans la configuration PAGENT

```
RACDCERT ID(stcuser) CONNECT(ID(stcuser) LABEL('clientlabel'))  
RING('keyringname') USEAGE(PERSONAL)
```

où :

- *stcuser* : ID d'utilisateur RACF associé à l'espace d'adressage TCPIP
- *clientlabel* : Etiquette du certificat de client
- *keyringname* : Nom du trousseau de clés. Il doit correspondre au trousseau de clés indiqué dans la configuration PAGENT

- c. Saisissez les commandes suivantes pour exporter les certificats CA et client vers STA :

```
RACDCERT EXPORT (LABEL('calabel')) CERTAUTH DSN('datasetname') FORMAT(CERTB64)
```

où :

- *calabel* : Etiquette pour l'autorité de certification, indiquée dans la définition du certificat CA
- *datasetname* : Jeu de données pour recevoir le certificat exporté

```
RACDCERT EXPORT (LABEL('clientlabel')) ID(stcuser) DSN('datasetname')  
FORMAT(PKCS12DER) PASSWORD(' password ')
```

où :

- *clientlabel* : Etiquette du certificat de client
- *stcuser* : ID d'utilisateur RACF associé à l'espace d'adressage TCPIP
- *datasetname* : Jeu de données pour recevoir le certificat exporté
- *password* : Mot de passe pour le chiffrement des données. Nécessaire lorsque le certificat est reçu sur STA. Le mot de passe doit comporter au moins huit caractères.

Les jeux de données d'export sont alors transmis à STA et le FTP peut être utilisé. Le certificat CA est transmis avec une conversion d'EBCDIC à ASCII. Le certificat CLIENT est transmis en tant que fichier BINARY et contient le certificat client et sa clé privée.

E.2.4. Tâche 4 : Création des profils RACF utilisés par la routine CGI

Les profils sont définis dans la classe FACILITY. Le premier profil est appelé *SMC.ACCESS.STA* et détermine si un utilisateur a accès à l'application STA.

Un utilisateur nécessitant d'accéder à STA doit avoir un accès lecture pour ce profil. Les autres profils sont tous affichés en tant que *SMC.ROLE.nnn* et sont utilisés pour déterminer quels rôles sont attribués à l'utilisateur une fois connecté.

Remarque:

Le seul rôle défini à STA est *StorageTapeAnalyticsUser*. Pour obtenir ce rôle, vous devez demander à ce que votre ID utilisateur soit ajouté au profil *SMC.ROLE.STORAGETAPEANALYTICSUSER* en accès lecture.

E.2.5. Tâche 5 : Importation du fichier de certificat et du fichier de clé privée (facultatif)

Cette procédure peut être précieuse pour savoir si les clés publiques et privées ont été générées et si les ID et les mots de passe utilisateur, disposant des autorisations appropriées, ont été correctement définis.

Le test peut être effectué sur n'importe quel navigateur, mais pour cet exemple nous utilisons Firefox.

1. Dans le menu **Tools** de Firefox, sélectionnez **Options**.
2. Sélectionnez l'onglet **Advanced**, puis l'onglet **Encryption**.
3. Cliquez sur **View Certificates**.
4. Accédez à l'onglet **Authorities** dans la boîte de dialogue **Certificate Manager** puis sélectionnez le fichier de certificat à importer.
5. Cliquez sur **Import**.
6. Cliquez ensuite sur l'onglet **Your certificates** et saisissez le fichier de clé privée à importer.
7. Cliquez sur **Import**.
8. Cliquez sur **OK** pour fermer la boîte de dialogue.

E.2.6. Tâche 6: Test de la routine CGI

Pour tester la routine CGI dans un navigateur, saisissez l'URL suivante, où *host*, *port*, *userid* et *password* sont définis selon les valeurs appropriées.

```
https://host:port/smcgsaf?  
type=authentication&userid=userid&password=password&roles=StorageTapeAnalyticsUser
```

Le résultat indique si l'utilisateur est autorisé à accéder à STA et au rôle *StorageTapeAnalyticsUser*.

Remarque:

L'utilitaire d'autorisation STA RACF ne prend pas en charge la modification du mot de passe des ID utilisateur du mainframe. Si le mot de passe d'un ID utilisateur expire, STA vous le signale et vous devez le réinitialiser à l'aide de canaux normaux du mainframe avant d'essayer de vous reconnecter à STA.

E.2.7. Tâche 7 : Configuration de RACF/SSP pour la console WebLogic

Le fournisseur de service de sécurité RACF (ou RACF SSP) doit être installé sur WebLogic en tant que plug-in.

Si le RACF SSP a été installé, le programme d'installation de STA doit placer le RACF SSP au bon emplacement dans WebLogic. S'il n'a pas été installé, placez le fichier *jar* de sécurité RACF dans le répertoire, comme suit :

```
/Oracle_storage_home/Middleware/wlserver_10.3/server/lib/mbeantypes/staRACF.jar
```

où *Oracle_storage_home* est l'emplacement de Oracle Storage Home indiqué pendant l'installation de STA.

E.2.8. Tâche 8: Configuration de SSL entre STA et RACF

1. Installez les PTF requis sur le système MVS. Ces PTF permettent l'authentification avec RACF ou un autre logiciel de sécurité tiers, lorsque vous vous connectez à STA. Pour les conditions minimales requises par les PTF, reportez-vous au guide *Guide des conditions requises pour l'installation de STA*.

Le protocole Application Transparent TLS (AT-TLS) a été configuré sur MVS pour que le numéro de port soit défini sur le serveur SMC HTTP et que WebLogic soit chiffré sur le serveur.

Avant de continuer, assurez-vous de posséder deux fichiers : le certificat de serveur MVS (au format ASCII) et la clé privée de client STA (au format PKCS12 binaire). L'administrateur système MVS vous a donné le mot de passe pour accéder au fichier PKCS12.

2. Placez le certificat sous `/Oracle_storage_home/Middleware/user_projects/domains/tbi/cert`.

où *Oracle_storage_home* est l'emplacement de Oracle Storage Home indiqué pendant l'installation de STA.

3. Convertissez le certificat du format DER au format PEM.

```
openssl pkcs12 -clcerts -in PKCS12DR.xxxxxx -out mycert.pem
```

Vous serez invité à saisir le mot de passe d'importation (fourni avec le certificat), un nouveau mot de passe PEM et la vérification du mot de passe.

4. A l'aide de la commande Java keytool, importez le fichier de certificat dans le fichier `/Oracle_storage_home/Middleware/jdk1.6.0_xx/jre/lib/security/cacerts`.

```
# /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. Tâche 9 : Configuration du serveur WebLogic

Pour configurer WebLogic pour l'authentification RACF, suivez la procédure dans la section [Section D.1.2, « Reconfiguration de WebLogic pour qu'il utilise un certificat de sécurité différent »](#)

E.2.10. Tâche 10: Installation de RACF/SSP sur la console WebLogic

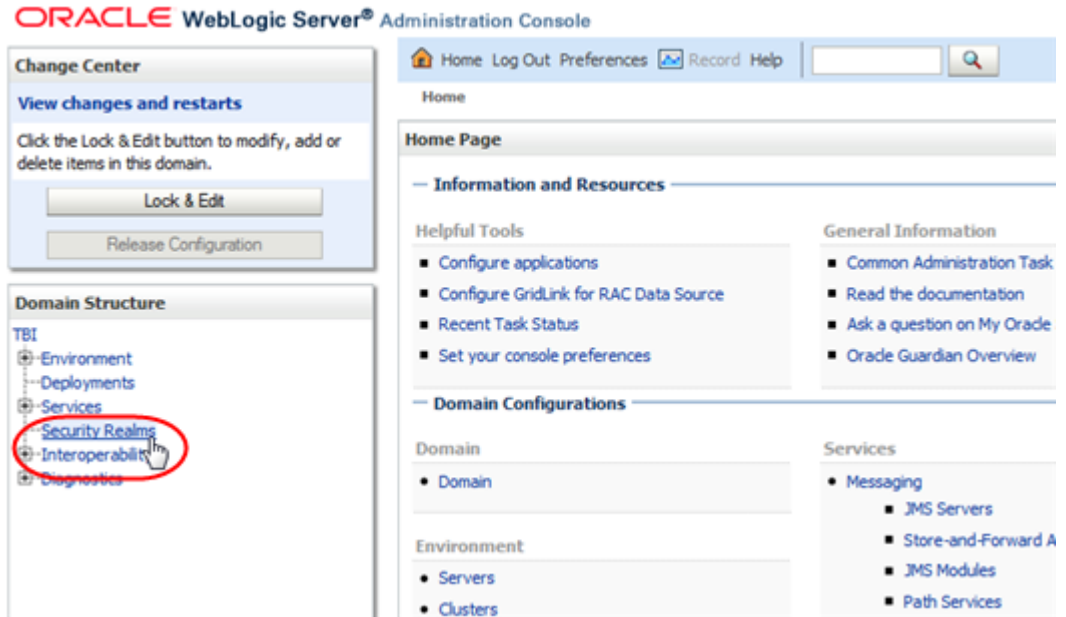
1. Allez à l'écran de connexion de la console WebLogic à l'aide du numéro de port HTTP (7019 par défaut pour STA 2.1.0) ou HTTPS (7020 par défaut pour STA 2.1.0) que vous avez sélectionné pendant l'installation de STA.

```
https://yourHostName:PortNumber/console/
```

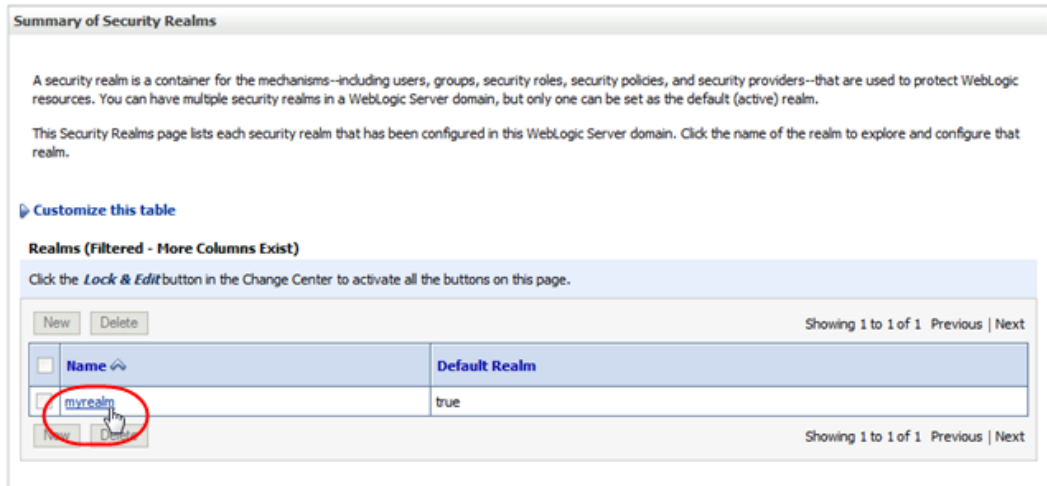
Par exemple :

```
https://sta_server:7020/console/
```

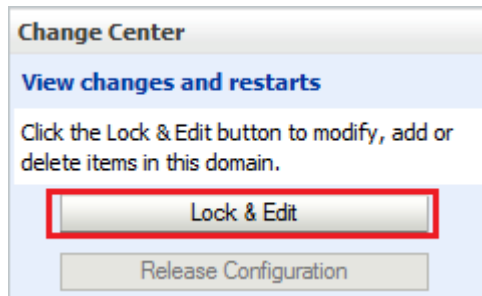
2. Connectez-vous à l'aide du nom d'utilisateur et du mot de passe de la console d'administration WebLogic que vous avez définis lors de l'installation de STA.
3. Dans la section Domain Structure, sélectionnez **Security Realms**.



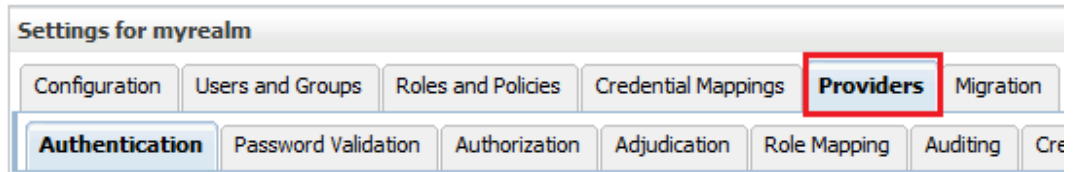
4. Dans la section Realms, sélectionnez le lien actif **myrealm** (sélectionnez le nom lui-même, et non la case).



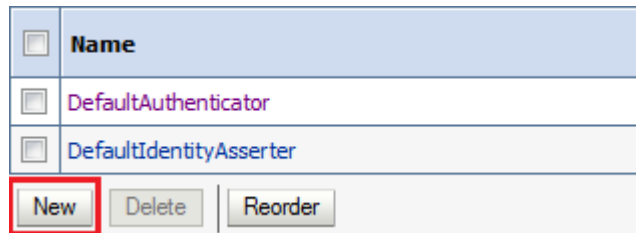
5. Dans la section Change Center, cliquez sur **Lock & Edit**.



6. Sélectionnez l'onglet **Providers**.



7. Dans la section Authentication Providers, cliquez sur **New**.



8. Saisissez le nom du fournisseur d'authentification que vous souhaitez ajouter (par exemple, *STA RacfAuthenticator*), et sélectionnez *RacfAuthenticator* dans le menu **Type**. Cliquez sur **OK**.

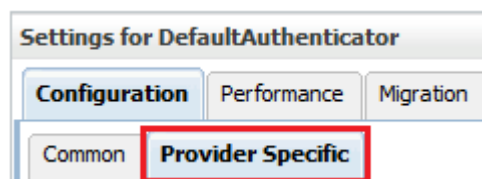
Remarque:

Le fichier RACF jar doit être répertorié dans le menu **Type**. S'il ne l'est pas, arrêtez puis redémarrez STA à l'aide de la commande *STA*. Pour plus d'informations sur l'utilisation de la commande, reportez-vous au guide *Guide d'administration de STA*.

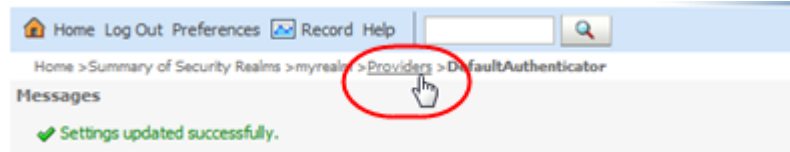
9. Vérifiez que le fournisseur RACF est inclus dans le tableau Authentication Providers. Les fournisseurs *DefaultAuthenticator* et *DefaultIdentityAsserter* doivent figurer en premier sur cette liste.
10. Sélectionnez le lien actif **DefaultAuthenticator** (sélectionnez le nom lui-même et non la case).



11. Dans le menu **Control Flag**, sélectionnez Sufficent, puis cliquez sur **Save**.
12. Cliquez sur l'onglet **Provider Specific** puis sur **Save**.



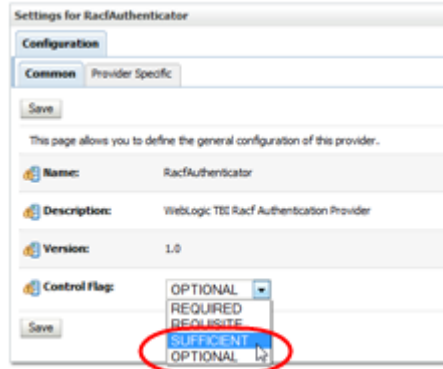
13. Cliquez sur le lien localisateur **Providers** pour revenir à l'écran Authentication Providers.



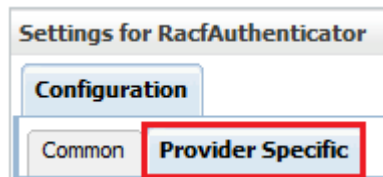
14. Dans le tableau Authentication Providers, sélectionnez le nom d'authentificateur RACF créé à l'étape 8 (sélectionnez le nom lui-même et non la case).

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider
<input type="checkbox"/>	RacfAuthenticator	WebLogic TBI Racf Authentication Provider

15. Dans le menu **Control Flag**, sélectionnez *Sufficient*, puis cliquez sur **Save**.



16. Cliquez sur l'onglet **Provider Specific**.



17. Saisissez le nom d'hôte (par exemple, *mvshost.yourcompany.com*) et le numéro de port (par exemple, *8700*) où le système MVS est exécuté, puis cliquez sur **Save**.

Settings for RacfAuthenticator

Configuration

Common Provider Specific

Save

This page allows you to configure additional attributes for this security provider.

Supported Groups:
StorageTapeAnalyticsUser

Host: mvshostyourcompany

Port: 8700

Save

18. Dans la section Change Center, cliquez sur **Activate Changes**.

Change Center

View changes and restarts

Pending changes exist. They must be activated to take effect.

Activate Changes

Undo All Changes

19. Déconnectez-vous de la console d'administration WebLogic.

20. Arrêtez et redémarrez STA à l'aide de la commande *STA*. Pour plus d'informations sur l'utilisation de la commande, reportez-vous au guide *Guide d'administration de STA*.

```
# STA stop all  
# STA start all
```

Configuration du mode SNMP v2c

Vous devez configurer le mode SNMP v2c si STA est amené à contrôler toute bibliothèque configurée pour SNMP v2c.

STA essaie toujours de communiquer avec les bibliothèques à l'aide du protocole SNMP v3 recommandé. Si la communication SNMP v3 n'est pas possible (par exemple, si SNMP v3 n'est pas configuré sur une bibliothèque), STA utilise SNMP v2c, si ce mode a été activé, selon les instructions de cette annexe.

Le processus de configuration SNMP v3 est décrit dans les chapitres [Chapitre 5, Configuration de SNMP sur les bibliothèques](#) et [Chapitre 6, Configuration des connexions de bibliothèque dans STA](#). Cette annexe décrit les procédures spécifiques de la configuration de SNMP v2c.

Cette annexe comprend la section suivante :

- [Tâches de configuration de SNMP v2c](#)

F.1. Tâches de configuration de SNMP v2c

- [Section F.1.1, « Configuration du mode SNMP v2c »](#)
- [Section F.1.2, « Création du destinataire de déroulement SNMP v2c STA sur la bibliothèque »](#)
- [Section F.1.3, « Activation du mode SNMP v2c pour STA »](#)

F.1.1. Configuration du mode SNMP v2c

Cette procédure permet de configurer STA et permet aux bibliothèques d'utiliser SNMP v2c pour les communications SNMP.

1. Dans le chapitre [Chapitre 5, Configuration de SNMP sur les bibliothèques](#), suivez toutes les procédures affichées dans la section [Tableau 5.1, « Tâches de configuration des bibliothèques pour STA »](#), sauf :
 - Remplacez la section " [Créez le destinataire de déroulement STA SNMP v3.](#) " [86] par la section [Section F.1.2, « Création du destinataire de déroulement SNMP v2c STA sur la bibliothèque »](#)
 - Après avoir terminé le processus du tableau [Tableau 5.1, « Tâches de configuration des bibliothèques pour STA »](#), exécutez la tâche [Section F.1.3, « Activation du mode SNMP v2c pour STA »](#)
2. Configurez SNMP v2c pour STA. Pour obtenir des instructions, reportez-vous au chapitre [Chapitre 6, Configuration des connexions de bibliothèque dans STA](#) [89].

F.1.2. Création du destinataire de déROUTement SNMP v2c STA sur la bibliothèque

Cette procédure permet de définir le serveur STA comme destinataire autorisé des déROUTements SNMP v2c et de définir les déROUTements que la bibliothèque envoie. Vous pouvez utiliser la CLI, la SL Console ou l'interface de navigateur SL150, en fonction du modèle de bibliothèque. Remarques :

- Séparez les niveaux de déROUTement par des virgules.
- Pour éviter les enregistrements dupliqués, ne définissez pas le serveur STA comme destinataire de déROUTement pour plusieurs instances. Par exemple, ne créez pas de définition de destinataire de déROUTement SNMP v3 et SNMP v2c pour le serveur STA.
- Il est possible que le niveau de déROUTement 4 ne soit pas pris en charge par des versions antérieures du microprogramme de la bibliothèque ; il est cependant possible de l'indiquer lors de la création d'un destinataire de déROUTement.
- Pour éviter les erreurs de saisie dans la CLI, vous pouvez tout d'abord saisir la commande dans un fichier texte, puis la copier et la coller dans la CLI. Pour obtenir de l'aide à propos des commandes de la CLI, saisissez *help snmp*.

A l'aide de la CLI de bibliothèque (toutes les bibliothèques sauf SL150)

1. Créez un destinataire de déROUTement SNMP v2c.

```
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
```

Où :

- *STA_server_IP* : est l'adresse IP du serveur STA.
- *community_name* : est la communauté de déROUTement SNMP v2c. Cela peut être *public* ou un autre nom.

Par exemple :

```
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. Répertoirez les destinataires de déROUTement pour vérifier que le serveur STA. a été correctement ajouté.

```
snmp listTrapRecipients
```

A l'aide de la SL Console (SL500 uniquement)

1. Dans le menu **Tools**, sélectionnez **System Detail**.

2. Sélectionnez **Library** dans l'arborescence de navigation.
3. Sélectionnez l'onglet **SNMP**, puis l'onglet **Add Trap Recipients**.
4. Saisissez les informations suivantes :
 - *Host* : adresse IP du serveur STA.
 - *TrapLevel* : la liste de niveaux de déROUTement séparés par des virgules que la bibliothèque doit envoyer à STA : 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
 - *Version* : Sélectionnez *v2c*.
 - *Community* : Cela peut être *public*, ou un autre nom.
5. Cliquez sur **Apply** pour ajouter le destinataire de déROUTement.

A l'aide de l'interface utilisateur SL150

1. Sélectionnez **SNMP** dans l'arborescence de navigation.
2. Dans la section (ou l'onglet) SNMP Trap Recipients, sélectionnez **Add Trap Recipient**.
3. Remplissez les champs Add Trap Recipient comme suit :
 - *Host Address* : Adresse IP du serveur STA.
 - *TrapLevel* : Liste des niveaux de déROUTement séparés par des virgules que la bibliothèque doit envoyer à STA : 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
 - *Version* : Sélectionnez *v2c*.
 - *Community Name* : Cela peut être *public*, ou un autre nom.
4. Cliquez sur **OK** pour ajouter le destinataire de déROUTement.

F.1.3. Activation du mode SNMP v2c pour STA

1. Ouvrez une session de terminal sur le serveur STA et connectez-vous en tant qu'utilisateur root du système.
2. Passez au répertoire de fichiers de configuration de STA.

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

3. Modifiez le fichier de propriétés de version SNMP.

```
# vi TbiSnmPVersionSupport.properties
```

4. Vérifiez que le paramètre SNMP v2c est défini sur *true*.

```
V2c=true
```

5. Enregistrez le fichier et fermez-le.
6. Si vous aviez modifié la valeur du paramètre SNMP v2c à l'étape 4, arrêtez-vous et recommencez tous les processus STA.

```
# STA stop all
```

STA start all

Index

A

attributs client, 92

C

comptes utilisateurs

conditions requises de MySQL, 44

conditions requises de WebLogic, 44

configuration de la bibliothèque,

Configuration SNMP, 78

Fiche de travail SNMP, 217

formatage d'étiquette de volume, 65

ID de complexe, 64

interfaces utilisateur, 66

Redundant Electronics, 62

script de configuration facultatif, 67

SL500 FastLoad, 66

tâches, 68

TCP/IP double, 62

configuration de port de pare-feu, 45

configuration de RACF, 233

Configuration LDAP, 229

Configuration STA

certificats,

établissement de la connexion initiale, 219

reconfiguration de WebLogic, 220

remplacement du certificat Oracle, 227

Service de sauvegarde de base de données STA,
101

services,

contrôleur de ressources, 101

mise à jour du paramètre PATH de Linux, 102

redémarrage du démon de services, 102

vérification de la connectivité de la
bibliothèque, 103

SNMP,

tâches, 89

D

demandes d'assistance, 26

désinstallation, , 141

destinataires de déroutement

ajout, 138

F

formatage d'étiquette de volume, 65

I

ID de complexe, 64

Installation de Linux

présentation,

tâches, 31

tâches de post-installation, 34

tâches de préparation, 28

Installation de STA

étapes de l'installation, 54

prérequis généraux, 51

présentation,

programme d'installation de la console, 54

programme d'installation graphique, 54

M

Mise à niveau de STA,

mode v2c

activation, 251

création d'un destinataire de déroutement, 250

présentation,

processus de configuration, 249

modification des attributs client SNMP, 92

N

numéros de série de volumes, en double, 66

P

paramètre PATH de Linux, 102

R

réinstallation, , 143

S

serveur STA

configuration de port, 45

SNMP

confirmation de la connectivité, 90

gestion

ajout d'un destinataire de déroutement, 138

modification des attributs client, 92

SSP

configuration,

configuration de RACF, 233
configuration de WebLogic Open LDAP, 229
STA
téléchargement, 53