Sterling B2B Integrator

Sécurité (version 5.2.3 ou ultérieure)

Version 5.2.3

Sterling B2B Integrator

Sécurité (version 5.2.3 ou ultérieure)

Version 5.2.3

Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 145.

Copyright

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

© Copyright IBM France 2016. Tous droits réservés.

La présente édition s'applique à la version 5.2.3 de Sterling B2B Integrator et à toutes les éditions et modifications ultérieures, sauf mention contraire dans les nouvelles éditions.

© Copyright IBM Corporation 2000, 2015.

Table des matières

© Copyright IBM Corp. 2000, 2015

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	**IBM Canada**
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

© Copyright IBM Corp. 2000, 2015

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Sécurité (version 5.2.3 ou ultérieure)

Sterling B2B Integrator utilise une variété de mécanismes de sécurité, notamment des mots de passe système pour des fonctions d'administration, des stratégies de mot de passe déterminées en fonction des politiques de sécurité de l'entreprise, ainsi que la sécurité basée sur les rôles qui fournissent plusieurs niveaux d'accès à différents utilisateurs au sein de l'organisation.

Les fonctions de sécurité suivantes sont fournies avec Sterling B2B Integrator :

- La sécurité basée sur les rôles permet aux utilisateurs d'accéder à des fichiers, processus techniques, modèles Web, services et fonctions du produit d'après les droits associés au compte utilisateur.
- Les stratégies de mot de passe sont des ensembles de décisions de sécurité que vous prenez et qui s'appliquent à divers comptes utilisateur selon les règles de sécurité en vigueur dans votre entreprise. Ces choix définissent notamment le nombre de jours durant lesquels un mot de passe est valide, ou bien la longueur maximale et minimale d'un mot de passe.
- LDAP permet de déléguer l'authentification d'un compte utilisateur externe à un annuaire LDAP et de fournir l'authentification en utilisant les mêmes informations de sécurité que pour les autres applications de l'entreprise. Si votre entreprise a déjà adopté LDAP, vous pouvez utiliser vos annuaires LDAP existants avec l'application.
- Phrase passe de système à l'installation : lors de l'installation de Sterling B2B Integrator, vous devez créer une phrase passe de système. Cette phrase passe est une chaîne hautement complexe de plus de 16 caractères. La phrase passe de système est requise pour démarrer le système et accéder aux informations protégées du système.
- Prise en charge des certificats x.509 pour la sécurité au niveau du chiffrement, de la signature et de la couche transport.
- Module logiciel certifié FIPS (Federal Information Processing Standards) 140-2 et prise en charge du matériel certifié FIPS 140-2 à partir de nCipher et Safenet.
- Couches SSL (Secure Socket Layer) et TLS (Transport Layer Security).

Les fonctions de sécurité suivantes peuvent également être configurées :

- La fonction de temporisation de la sécurité vous permet de configurer les délais d'attente des sessions utilisateur.
- La fonction Stratégie de mot de passe personnalisé vous permet d'ajouter des règles de stratégie de mot de passe supplémentaires. Ces règles supplémentaires peuvent vous aider à empêcher l'utilisation de mots de passe faibles faciles à pirater et à rejeter les mots de passe non conformes.
- La fonction Connexion unique est un processus d'authentification qui permet aux utilisateurs d'accéder à plusieurs applications en entrant un seul nom d'utilisateur et mot de passe.
- La fonction Chiffrement de documents permet la configuration d'une couche de sécurité supplémentaire qui étend les droits d'accès aux bases de données et aux fichiers traditionnels.

© Copyright IBM Corp. 2000, 2015

Sécurité basée sur les rôles

Présentation de la sécurité basée sur les rôles

La sécurité basée sur les rôles permet aux utilisateurs d'accéder à certains fichiers, processus techniques, modèles Web, services et fonctions du produit, d'après les droits associés au compte utilisateur.

Pour bien maîtriser la gestion de la sécurité basée sur les rôles, vous devez comprendre comment les groupes, droits et comptes utilisateur fonctionnent ensemble.

- Les droits permettent d'accéder aux pages de l'interface utilisateur et aux fonctionnalités proposées sur les pages.
- Les groupes sont des collections de droits d'accès.
- Les comptes utilisateur sont affectés à des droits et des stratégies de mot de passe.

La gestion de la sécurité basée sur les rôles implique les tâches suivantes :

- Créer des droits
- Créer des groupes
- Créer des stratégies de mot de passe
- Créer des comptes utilisateur

Groupes

Les groupes sont des collections de droits d'accès. Ils permettent de centraliser la gestion des droits d'accès de plusieurs utilisateurs à partir d'un seul endroit. Ces groupes contribuent à réduire la charge de travail liée à la gestion des comptes, en particulier lorsque plusieurs utilisateurs occupent la même fonction.

Vous pouvez affecter plusieurs droits à des utilisateurs différents en créant des groupes pour chaque fonction plutôt que pour chaque utilisateur. Vous pouvez également affecter un groupe en tant que sous-groupe d'un autre groupe.

Prenons l'exemple d'un service Achats constitué de cinq employés effectuant des tâches identiques. Au lieu d'affecter des droits à chaque compte employé, vous pouvez créer un groupe Achats et gérer les droits d'accès de tous les employés dans un groupe unique. Dans le groupe Achats, vous avez la possibilité d'affecter des sous-groupes afin d'affiner les droits d'accès en fonction du type d'achats effectué par l'employé. Vous pouvez également affecter des sous-groupes appelés Fournitures de bureau, Machines, Équipement général ou Véhicules au groupe Achats afin d'affiner les droits d'accès.

Pour éviter l'écrasement lors de l'application des mises à niveau ou des correctifs, ne modifiez pas les groupes préconfigurés fournis avec le système.

Les tâches du groupe sont notamment les suivantes :

- Création d'un groupe
- Recherche d'un groupe
- Modification d'un groupe
- Suppression d'un groupe

Groupes préconfigurés

Pour affecter des droits aux utilisateurs, vous pouvez affecter les groupes préconfigurés. Les utilisateurs héritent de tous les droits associés aux groupes. Il est possible qu'un groupe prédéfini soit affecté à un utilisateur si l'accessibilité et le thème sont définis pour le compte utilisateur.

Vous devez disposer des droits requis sur le module Comptes pour créer des groupes.

Conventions de dénomination des groupes

La dénomination des groupes possède une série de conventions.

Utilisez les conventions de dénomination suivantes pour les groupes :

- Les ID de groupe doivent être distincts.
- Les noms sont sensibles à la casse.
- Deux noms de groupe avec une capitalisation différente sont considérés comme des noms distincts.
- Si un nom de groupe a été utilisé, il ne peut pas être utilisé comme nom d'un nouveau groupe. Un message d'erreur s'affiche.

Recherche des groupes

Vous pouvez rechercher un groupe à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour rechercher un groupe :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Groupes**.
2. Effectuez l'une des opérations suivantes :
   - Sous Rechercher, entrez une partie du **Nom du groupe** ou le **Nom du groupe** complet que vous recherchez, puis cliquez sur **OK**. La page Groupes répertorie tous les groupes correspondant à vos critères de recherche.
   - Sous Liste, dans la zone **Par ordre alphabétique**, sélectionnez TOUT ou la lettre qui commence par le nom du groupe que vous recherchez et cliquez sur **OK**. La page Groupes répertorie tous les groupes correspondant à vos critères de recherche.

Création de groupes

Vous pouvez créer un groupe à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Avant de commencer, vous devez connaître :

- L'ID groupe du groupe que vous créez.
- Le nom du groupe que vous créez.
- Le nom du propriétaire du groupe.
- L'identité du partenaire commercial à associer au groupe. Un seul partenaire commercial peut être associé à un groupe mais un compte utilisateur peut être associé à plusieurs groupes. Cela permet à un compte utilisateur d'être associé à plusieurs partenaires commerciaux. La zone Identité est utilisée pour le routage des messages dans la boîte aux lettres.

Pour créer un groupe :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Groupes**.
2. En regard de **Créer un groupe**, cliquez sur **OK**.
3. Dans la page Nouveau groupe, entrez l'**ID groupe**.
4. Entrez le **Nom du groupe**.
5. Entrez le **Propriétaire**.
6. Sélectionnez l'**Identité**.
7. Cliquez sur **Suivant**.
8. Si vous voulez filtrer les groupes par nom, dans la page Affecter les sous-groupes, sous Données de filtre dans la zone **Par nom**, entrez tout ou partie du nom du groupe sur lequel doit porter le filtrage et cliquez sur le bouton de filtre.
9. Sélectionnez les groupes que vous souhaitez affecter à ce groupe. Déplacez les groupes du panneau Disponible vers le panneau Affecté(s).
10. Cliquez sur **Suivant**.
11. Dans la page Affecter des droits, souhaitez-vous filtrer les droits ?
    - Si vous voulez filtrer par nom, sous Filtrer les données dans la zone **Par nom**, entrez tout ou partie du nom du droit d'accès sur lequel doit porter le filtrage, puis cliquez sur le bouton de filtre situé à droite de la zone **Par Type**.
    - Pour filtrer par type, sous Filtrer les données, sélectionnez le type de droit d'accès sur lequel doit porter le filtrage dans la liste Par type, puis cliquez sur le bouton de filtre situé à droite de la zone **Par type**.
12. Sélectionnez les droits d'accès que vous souhaitez affecter à ce groupe. Déplacez les droits d'accès du panneau Disponible vers le panneau Affecté(s). Par défaut, les droits d'accès associés au sous-groupes affectés à ce groupe sont déjà sélectionnés. Les droits d'accès associés ne sont pas affichés dans la colonne Disponible mais ils apparaissent dans la page de confirmation.
13. Cliquez sur **Suivant**.
14. Passez en revue les informations des groupes.
15. Cliquez sur **Terminer**.

Modification des groupes

Vous pouvez modifier un groupe pour mettre à jour des paramètres, des sous-groupes et des droits.

Pourquoi et quand exécuter cette tâche

Lorsque vous modifiez un groupe, vous pouvez mettre à jour les éléments suivants :

- Paramètres
- Sous-groupes
- Droits

Vous ne pouvez pas modifier l'ID groupe. Si vous êtes amené à le modifier, vous devez créer un groupe.

Pour modifier un groupe :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Groupes**.
2. Recherchez le groupe que vous voulez éditer à l'aide de la commande Rechercher par nom de groupe ou Liste par ordre alphabétique, puis cliquez sur **OK**.
3. Sélectionnez **Modifier** pour le groupe que vous souhaitez mettre à jour.
4. Mettez à jour les paramètres du groupe, puis cliquez sur **Suivant**.
5. Mettez à jour les sous-groupes, puis cliquez sur **Suivant**.
6. Mettez à jour les droits affectés, puis cliquez sur **Suivant**.
7. Cliquez sur **Suivant**.
8. Passez en revue les informations du groupe.
9. Cliquez sur **Terminer**.

Suppression des groupes

Vous pouvez supprimer des groupes à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Vous ne pouvez pas retirer le groupe Admin Sterling B2B Integrator ou le droit Comptes de l'interface utilisateur d'un utilisateur administrateur car ces droits permettent à l'administrateur système de gérer le système.

Pour supprimer un groupe :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Groupes**.
2. Dans la page Groupes, recherchez le groupe que vous souhaitez supprimer en utilisant l'option de recherche ou de liste.
3. Dans la page Groupes, en regard du groupe que vous souhaitez supprimer, cliquez sur **Supprimer**.

   Le système supprime le groupe et affiche le message :

   ```
   Mise à jour du système terminée.
   ```

Vérification du nom et de l'ID d'un groupe

Vous pouvez passer en revue le nom et l'ID d'un groupe à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour vérifier le nom et l'ID d'un groupe :

Procédure

1. Dans le menu **Administration**, sélectionnez **Compte** > **Groupe**.
2. Dans la page Groupe, recherchez le groupe que vous souhaitez vérifier en utilisant les options de recherche ou de liste.
3. Sélectionnez le groupe. Le nom et l'ID du groupe sont affichés.

Droits

Les droits permettent d'accéder aux différents modules de Sterling B2B Integrator et représentent le fondement de la sécurité basée sur les rôles. Les droits d'un utilisateur sont constitués des droits issus des groupes ainsi que de tous les droits affectés individuellement.

Les droits permettent notamment de :

- Gérer l'accès de plusieurs utilisateurs à partir d'un seul endroit.
- Gérer les comptes utilisateur avec un minimum d'effort, surtout lorsque plusieurs utilisateurs effectuent les mêmes tâches.

Les tâches relatives aux droits sont notamment :

- Créer un droit
- Rechercher un droit
- Modifier le nom d'un droit
- Supprimer un droit

Avant de créer, modifier ou supprimer un droit, déterminez les modules auxquels les utilisateurs de ce groupe doivent ou non accéder pour remplir leurs tâches. Vous devez disposer des droits nécessaires sur le module Comptes pour créer des droits.

Pour éviter l'écrasement lors de l'application des mises à niveau ou des correctifs, ne modifiez pas les droits préconfigurés fournis avec le système. Lorsque des groupes de droits personnalisés sont nécessaires, créez un nouveau groupe.

Conventions de dénomination des droits

Les noms de droits sont sensibles à la casse et ne peuvent pas être dupliqués.

Les conventions de dénomination des droits d'accès sont notamment celles-ci :

- Les noms sont sensibles à la casse et deux noms avec une capitalisation différente sont considérés comme des noms uniques. Par exemple, "Tout document" et "Tout Document" sont deux noms de droit différents.
- Un nom de droit d'accès existant ne peut pas être utilisé comme nom d'un nouveau droit d'accès. Dans ce cas, un message d'erreur s'affiche.

Deux droits peuvent avoir le même nom avec une capitalisation différente, mais cette méthode est déconseillée.

Droits hérités des groupes

Ces groupes sont préinstallés et les droits sont hérités lorsqu'un groupe de droits est affecté à un compte utilisateur. Les mêmes droits sont hérités lorsqu'un groupe est affecté en tant que sous-groupe.

Chaque groupe contient des droits pour les éléments de menu, ainsi que le droit de l'interface utilisateur correspondant qui est utilisé pour accorder l'accès à la page. Par exemple, EBXML contient le droit de l'interface utilisateur EBXML.

Nom du groupe	ID du groupe	Droits hérités du groupe
ACCOUNTS	ACCOUNTS	PasswordPolicy, Permissions, UI Comptes, UserNews
ADAPTER_UTILITIES	ADAPTER_UTILITIES	BEATuxedo, CDNetmaps, CDNetmapXref, CDNodes, SAPRoutes, SAPRouteXREF, SAPSuiteBuilder, UI Utilitaires d'adaptateur

Nom du groupe	ID du groupe	Droits hérités du groupe
ADVANCED_SETUP	ADVANCED_SETUP	DeliveryChannels, DocumentExchange, Identities, Packaging, Profiles, Transports, UI Configuration du profil commercial avancée
AS2 Edition	as2admin	Tous les droits du sous-groupe BPMONITOR, plus AS2 UI, TestNow, UI Configuration des profils commerciaux AS2, UI Gestionnaire de processus techniques, UI Certificats de l'autorité de certification, UI Supprimer des données de partenaire commercial, UI Journaux, UI Planificateur, UI Certificats de système, UI Partenaires commerciaux
Notification d'événements anormaux	eventAbnormal	Aucun
Comptes	acctadmin	Tous les droits du sous-groupe ACCOUNTS, plus UI Groupes, UI Comptes utilisateur.
Notifications d'alerte	notifications	Aucun
BPMONITOR	BPMONITOR	BPSSCorrelation, BusinessProcesses, CentralSearch, CommunicationSessions, Correlation, CurrentActivities, CurrentDocuments, CurrentProcesses, DataFlows, Documents, EBXMLCorrelation, EDICorrelation, EDIINT, GentranServerforUnix, Message Entry Workstation Home, SWIFTNETCorrelation, UI Moniteur de processus techniques, RosettaNet
Processus technique	bpadmin	Tous les droits des sous-groupes BPMONITOR et SERVICES, plus UI Gestionnaire de processus techniques, UI Processus technique, UI Supprimer un processus technique.
Administrateur proxy de serveur CD	cdsp_admin	Tous les droits des sous-groupes ACCOUNTS, BPMONITOR, Utilisateur proxy de serveur CD, OPERATIONS et SERVICES, plus UI Groupes, UI Licences, UI Stratégie de mot de passe, UI Outil SQL, UI Comptes utilisateur.
Utilisateur proxy de serveur CD	cdsp_user	Ce groupe est affecté par défaut lorsqu'un compte utilisateur est créé avec l'accessibilité CDSP. Tous les droits des sous-groupes ACCOUNTS, BPMONITOR, OPERATIONS et SERVICES, plus Services CDSP, UI Certificats d'autorité de certification, UI Importer/Exporter, UI Gestionnaire de verrouillage, UI Journaux, UI Serveurs de périphérie, UI Rapports, UI Outil Dossier d'assistance, UI Certificats de système, UI Certificats accrédités.
Utilisateur de ligne de commande	commandlineuser	eInvoicing, eInvoicing ALL BUYERS, eInvoicing ALL SUPPLIERS, eInvoicing Archive, eInvoicing Configuration, eInvoicing CREATE/EDIT AGREEMENT, eInvoicing DELETE AGREEMENT, VIEW AGREEMENT
DEPLOYMENT	DEPLOYMENT	UI Déploiement, ResourceTags

Nom du groupe	ID du groupe	Droits hérités du groupe
Utilisateurs du tableau de bord	dashboardUsers	Ce groupe est affecté par défaut lorsqu'un compte utilisateur est créé avec la fonction Accessibilité du Tableau de bord et l'un des thèmes de Tableau de bord suivants : • AFT • Par défaut • Community Management Operator, Participant, Participant Sponsor ou Sponsor Administration Management Console, Business Process Search Portlet, Cache Statistics Portlet, Cache Usage Portlet, Community Management Portlet, Community Statistics Portlet, Database Pool Usage Portlet, Database Status Portlet, Database Usage Portlet, Document Search Portlet, Document Tracking Portlet, Documents Processed Bar Chart Portlet, Documents Processed Time Series Portlet, Event Viewer Portlet, IFrame Portlet, Log File Viewer Portlet, Log File Viewer Portlet 2, ParticipatingCommunities Portlet, Peers Portlet, Queue Priority Statistics Portlet, Quick Links Portlet, RSS Feed Portlet, Sponsored Communities Portlet, System Alerts Portlet, Web Search Portlet, Web View Plus Portlet
Déploiement	deploymentadmin	Tous les droits des sous-groupes ADAPTER_UTILITIES, DEPLOYMENT, EBXML, MAILBOX, MAPS, SERVICES, WEB_EXTENSIONS et WEB_SERVICES, plus UI Connexion : Direct, UI Supprimer un schéma/une extension CPA et CPSS, UI Supprimer une mappe, UI Supprimer un profil PGP, UI Supprimer des routes SAP, UI Supprimer un schéma, UI Supprimer une instance de service, UI Supprimer une règle de routage SWIFTNet, UI Supprimer une ressource Web, UI Supprimer des modèles Web, UI Supprimer WSDL, UI Supprimer un modèle XSLT, UI Générer/Télécharger des fichiers WAR, UI Importer/Exporter, UI Planificateur, UI Schémas, UI Clé d'identité locale SSH, UI Règle de routage SWIFTNet, UI XSLT
Administrateurs EBICS	EBICS_ADM	UI EBICS Bank Profile Configuration, UI EBICS Contract Configuration, UI EBICS File Format Configuration, UI EBICS Offer Configuration,UI EBICS Order Type Configuration, UI EBICS Partner Profile Configuration, UI EBICS User Permission Configuration, UI EBICS User Profile Configuration, UI EBICS Bank Profile Configuration, UI EBICS Contract Configuration, UI EBICS Subscriber Key Validation
Opérateurs EBICS	EBICS_OPERATOR	UI EBICS Bank Profile Configuration, UI EBICS Contract Configuration, UI EBICS File Format Configuration, UI EBICS Offer Configuration, UI EBICS Order Type Configuration, UI EBICS Partner Profile Configuration, UI EBICS Subscriber Key Validation, UI EBICS User Permission Configuration, UI EBICS User Profile Configuration
EBXML	EBXML	BPSS, BPSSExtension, CPA, UI EBXML
ENVELOPES	ENVELOPES	ControlNumberHistory, ControlNumbers, EDISequenceCheckQueue, Envelopes, TransactionRegister, UI Enveloppes
Notifications d'événements exceptionnels	eventExceptional	Aucun
BOÎTE AUX LETTRES	BOÎTE AUX LETTRES	Configuration, Messages, RoutingRules, UI Boîte aux lettres, VirtualRoots

Nom du groupe	ID du groupe	Droits hérités du groupe
MAPPES	MAPS	ExtendedRuleLibraries, Mappes, Normes, UI Mappes
Administrateurs de boîtes aux lettres	mboxadmins	Tous les droits des groupes MAILBOX et Utilisateurs de l'interface de navigation des boîtes aux lettres, plus DeadLetter Mailbox, Mailbox Global Delete, Mailbox Global Query, EBICS_DEADLETTER Mailbox
Utilisateurs de l'interface de navigation des boîtes aux lettres	mbiusers	Mailbox Add Business Process, Mailbox Extract Business Process, Mailbox Path List Process, Mailbox Query Business Process, Mailbox Search Business Process, Mailbox Self Registration Business Process, Mailbox View Business Process, MBISearch JSP
OPERATIONS	OPERATIONS	JDBCMonitor, MessageMonitor, Perfdumps, SequenceManager, Statistics, ThreadMonitor, Troubleshooter, Tuning, UI Systèmes fédérés, UI Opérations
Partenaires commerciaux provisoires	provisionalpartners	Aucun
SERVICES	SERVICES	Configuration, Installation/Configuration, UI Services
SSH	SSH	AuthorizedUserKey, KnownHostKey, RemoteProfiles, Interface utilisateur SSH, UserIdentityKey
Session Demo Web Suite Buyer	sd_buyer	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Invoice Template, WebSuite Invoice View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite PO Ack Template, WebSuite PO Ack View Template, WebSuite Query Business Process, WebSuite RA Send Business Process, WebSuite Self Registration Business Process, WebSuite Session Demo Confirm Send Template, WebSuite Session Demo PO Send Business Process, WebSuite Session Demo PO Template, WebSuite Session Demo PO View Template, WebSuite Session Demo Query List Template
Session Demo Web Suite Suppliers	sd_supplier	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Invoice Template, WebSuite Invoice View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite PO Ack Template, WebSuite PO Ack View Template, WebSuite PO to Advance Ship Notice Template, WebSuite PO to Invoice Template, WebSuite PO Turn Business Process, WebSuite Query Business Process, WebSuite RA Send Business Process, WebSuite Self Registration Business Process, WebSuite Session Demo Confirm Send Template, WebSuite Session Demo PO Send Business Process, WebSuite Session Demo PO View Template, WebSuite Session Demo Query List Template

Nom du groupe	ID du groupe	Droits hérités du groupe
Sterling B2B Integrator Admin	super	Tous les droits des sous-groupes ACCOUNTS, ADAPTER_UTILITIES, ADVANCED_SETUP, BPMONITOR, DEPLOYMENT, EBXML, ENVELOPES, MAILBOX, MAPS, Administrateurs de boîtes aux lettres, OPERATIONS, SERVICES, SSH, WEB_EXTENSIONS et WEB_SERVICES, plus UI Archive, UI Configuration de profils commerciaux AS2, UI Configuration du profil commercial de base, UI Gestionnaire de processus techniques, UI Processus technique, UI Certificats d'autorité de certification, UI CodeLists, UI Connexion : Direct, UI Supprimer un schéma/une extension CPA et CPSS, UI Supprimer une mappe, UI Supprimer un profil PGP, UI Supprimer des routes SAP, UI Supprimer un schéma, UI Supprimer une instance de service, UI Supprimer une règle de routage SWIFTNet, UI Supprimer une ressource Web, UI Supprimer des modèles Web, UI Supprimer WSDL, UI Supprimer un modèle XSLT, UI Générer/Télécharger des fichiers WAR, UI Importer/Exporter, UI Planificateur, UI Schémas, UI Clé d'identité locale SSH, UI Règle de routage SWIFTNet, UI XSLT
Opérations système	operator	Tous les droits du sous-groupe OPERATIONS, plus UI Archive, UI Licences, UI Gestionnaire de verrouillages, UI Journaux, UI Notification, UI Serveurs de périmètres, UI Rapports, UI Planificateur, UI Outil SQL, UI Outil Dossier d'assistance
Profils commerciaux	tpadmin	Tous les droits des sous-groupes ADVANCED_SETUP, ENVELOPES et SSH, plus UI Configuration des profils commerciaux AS2, UI Configuration des profils commerciaux de base, UI Certificats d'autorité de certification, UI CodeLists, UI Contrats, UI Supprimer des données de partenaires commerciaux, UI Certificats de système, UI Partenaires commerciaux, UI Certificats accrédités
WEB_EXTENSIONS	WEB_EXTENSIONS	Utilities, WebResources, WebTemplates
WEB_SERVICES	WEB_SERVICES	SchemaMappings, SecurityToken, UI Web Services, WebServicesManager, WSDLCheckin
Web Suite Buyers	wsbuyers	WebSuite ASN View Template, WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Invoice View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite PO Ack View Template, WebSuite PO Send Business Process, WebSuite PO Template, WebSuite PO View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite RA Send Business Process, WebSuite Remittance Advice Template, WebSuite Remittance Advice View Template, WebSuite Self Registration Business Process

Nom du groupe	ID du groupe	Droits hérités du groupe
Web Suite Employees	wsemployees	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite ER Send Business Process, WebSuite Expense Report Template, WebSuite Expense Report View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Purchase Req Send Business Process, WebSuite Purchase Req Template, Websuite Purchase Req View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process, WebSuite TimeSheet Template, WebSuite TimeSheet View Template, WebSuite TS Send Business Process
Web Suite Finance	wsfinance	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Expense Report View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process
Web Suite Human Resources	wshr	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process, WebSuite TimeSheet View Template
Web Suite Managers	wsmanagers	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite ER Send Business Process, WebSuite Expense Report View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Purchase Req Send Business Process, WebSuite Purchase Req View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process, WebSuite TimeSheet View Template, WebSuite TS Send Business Process
Web Suite Purchasers	wspurchaser	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Purchase Req View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process

Nom du groupe	ID du groupe	Droits hérités du groupe
Web Suite Suppliers	wssupplier	WebSuite ASN Send Business Process, WebSuite ASN Template, WebSuite ASN View Template, WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Invoice Send Business Process, WebSuite Invoice Template, WebSuite Invoice View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite PO Ack Send Business Process, WebSuite PO Ack Template, WebSuite PO Ack View Template, WebSuite PO to Advance Ship Notice Template, WebSuite PO to Invoice Template, WebSuite PO to PO Ack Template, WebSuite PO Turn Business Process, WebSuite PO View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Remittance Advice View Template, WebSuite Self Registration Business Process

Droits nécessaires pour accéder aux ressources de l'interface utilisateur

Il s'agit de l'ensemble des droits minimaux requis pour accéder à une option de menu et à sa page et ses fonctionnalités associées. L'affectation de l'ensemble des droits minimaux peut également rendre certaines fonctionnalités supplémentaires disponibles pour l'utilisateur. Si vous ne disposez pas du droit d'accès à une option de menu et à ses fonctionnalités associées, rien ne s'affichera.

Dans le menu Administration > Processus technique, Ressource de l'interface utilisateur	Nom du droit / ID du droit
Processus technique > Gestionnaire	UI Gestionnaire de processus techniques (BPMANAGE), plus UI Processus technique (BUSINESS_PROCESS)
Processus technique > Moniteur > Recherche avancée > Processus technique	BusinessProcesses (PLTADM2), plus UI Moniteur des processus techniques (BPMONITOR)
Processus technique > Moniteur > Recherche avancée > Corrélation SWIFTNET	SWIFTNETCorrelation (GISADM9), plus UI Moniteur des processus techniques (BPMONITOR) et Règle de routage SWIFTNet (SWIFTNET_ROUTING_RULE)
Processus technique > Moniteur > Recherche avancée > Flux de données	DataFlows (GISADM1), plus UI Moniteur des processus techniques (BPMONITOR)
Processus technique > Moniteur > Recherche avancée > Documents	Documents (GISADM2), plus UI Moniteur des processus techniques (BPMONITOR)
Processus technique > Moniteur > Recherche avancée > Sessions de communication	Sessions de communication (GISADM3), plus UI Moniteur des processus techniques (BPMONITOR)
Processus technique > Moniteur > Recherche avancée > Corrélation	Correlation (GISADM4), plus UI Moniteur des processus techniques (BPMONITOR)
Processus technique > Moniteur > Recherche avancée > Corrélation BPSS	BPSSCorrelations (GISADM5) plus UI Moniteur des processus techniques (BPMONITOR)

Dans le menu Administration > Processus technique, Ressource de l'interface utilisateur	**Nom du droit / ID du droit**
Processus technique > Moniteur > Recherche avancée > Corrélation EBXML	EBXMLCorrelation (GISADM6) plus UI Moniteur des processus techniques (BPMONITOR)
Processus technique > Moniteur > Recherche avancée > Corrélation EDI	EDICorrelation (GISADM7) plus UI Moniteur des processus techniques (BPMONITOR)
Processus technique > Moniteur > Recherche avancée > EDIINT	EDIINT (STDSADM6) plus UI Moniteur des processus techniques (BPMONITOR)
Processus technique > Moniteur > Recherche centrale	CentralSearch (GISADM10) plus UI Moniteur des processus techniques (BPMONITOR)
Processus technique > Moniteur > Processus en cours	CurrentProcesses (PLTADM3) plus UI Moniteur des processus techniques (BPMONITOR)
Processus technique > Moniteur > Documents en cours	CurrentDocuments (GISADM11) plus UI Moniteur des processus techniques (BPMONITOR)
Processus technique > Moniteur > Activités en cours	CurrentActivities (PLTADM4) plus UI Moniteur des processus techniques (BPMONITOR)
Processus technique > Poste de travail d'entrée de message	Message Entry Workstation Home (MESSAGE_ENTRY_HOME)

Dans le menu Administration > Partenaire commercial, Ressource de l'interface utilisateur	**Nom du droit / ID du droit**
Partenaire commercial > Configuration > De base	UI Configuration du profil commercial de base (BASIC_SETUP)
Partenaire commercial > Configuration > Avancée > Identités	Identities (GISADM12) plus UI Configuration des profils commerciaux avancée (ADVANCED_SETUP) La suppression nécessite également le droit UI Supprimer un partenaire commercial (TP_DELETE)
Partenaire commercial > Configuration > Avancée > Transports	Transports (GISADM13) plus UI Configuration des profils commerciaux avancée (ADVANCED_SETUP) La suppression nécessite également le droit UI Supprimer un partenaire commercial (TP_DELETE)
Partenaire commercial > Configuration > Avancée > Echange de documents	DocumentExchange (GISADM14) plus UI Configuration des profils commerciaux avancée (ADVANCED_SETUP) La suppression nécessite également le droit UI Supprimer un partenaire commercial (TP_DELETE)

Dans le menu Administration > Partenaire commercial, Ressource de l'interface utilisateur	Nom du droit / ID du droit
Partenaire commercial > Configuration > Avancée > Canaux de distribution	DeliveryChannels (GISADM15) plus UI Configuration des profils commerciaux avancée (ADVANCED_SETUP) La suppression nécessite également le droit UI Supprimer un partenaire commercial (TP_DELETE)
Partenaire commercial > Configuration > avancée > Package	Packaging (GISADM16) plus UI Configuration des profils commerciaux avancée (ADVANCED_SETUP) La suppression nécessite également le droit UI Supprimer un partenaire commercial (TP_DELETE)
Partenaire commercial > Configuration > Avancée > Profils	Profiles (GISADM17) plus UI Configuration des profils commerciaux (ADVANCED_SETUP) La suppression nécessite également le droit UI Supprimer un partenaire commercial (TP_DELETE)
Partenaire commercial > Certificats numériques > Autorité de certification	UI Certificats de l'autorité de certification (CA_CERTS) plus UI Certificats de système (SYSTEM_CERTS) L'UI Certificats de système ajoute l'option Système.
Partenaire commercial > Certificats numériques > Accrédités	UI Certificats accrédités (TRUSTED_CERTS)
Partenaire commercial > Certificats numériques > Système	UI Certificats de système (SYSTEM_CERTS)
Partenaire commercial > Enveloppes de documents > Enveloppes	Envelopes (STDSADM1) plus UI Enveloppe (ENVELOPE)
Partenaire commercial > Enveloppes de documents > Numéros de contrôle	ControlNumbers (STDSADM2) plus UI Enveloppe (ENVELOPE)
Partenaire commercial > Enveloppes de documents > Registre des transactions	TransactionRegister (STDSADM3) plus UI Enveloppe (ENVELOPE)
Partenaire commercial > Enveloppes de documents > Historique des numéros de contrôle	ControlNumberHistory (STDSADM4) plus UI Enveloppe (ENVELOPE)
Partenaire commercial > Enveloppes de documents > File d'attente de vérification des séquences EDI	EDISequenceCheckQueue (STDSADM5) plus UI Enveloppe (ENVELOPE)
Partenaire commercial > Contrats	UI Contrats (CONTRACTS) plus UI Configuration des partenaires commerciaux avancée (ADVANCED_SETUP)
Partenaire commercial > Listes de codes	UI CodeLists (CODELISTS)
Partenaire commercial > AS2	UI Configuration des profils commerciaux AS2 (AS2_SETUP)

Dans le menu Administration > Partenaire commercial, Ressource de l'interface utilisateur	**Nom du droit / ID du droit**
Partenaire commercial > SSH > Profils distants	RemoteProfiles (ASSETADM1) plus UI SSH
Partenaire commercial > SSH > Clé d'hôte connu	KnownHostKey (ASSETADM2) plus UI SSH
Partenaire commercial > SSH > Clé d'identité utilisateur	UserIdentityKey (ASSETADM3) plus UI SSH
Partenaire commercial > SSH > Clé d'utilisateur autorisé	AuthorizedUserKey (ASSETADM4) plus UI SSH
Partenaire commercial > AS3	UI Configuration des profils commerciaux AS3 (AS3_SETUP)
Partenaire commercial > Profil de partenaire FTP Odette > Partenaire physique	OftpPhysicalPartner (ASSETOFTP1) plus UI Utilitaires d'adaptateur (ADAPTER_UTILITIES)
Partenaire commercial > Profil de partenaire FTP Odette > Contrat de partenaire physique	OftpPhysicalPartnerContract (ASSETOFTP3) plus UI Utilitaires d'adaptateur (ADAPTER_UTILITIES)
Partenaire commercial > Profil de partenaire FTP Odette > Partenaire logique	OftpLogicalPartner (ASSETOFTP2) plus UI Utilitaires d'adaptateur (ADAPTER_UTILITIES)
Partenaire commercial > Profil de partenaire FTP Odette > Contrat de partenaire logique	OftpLogicalPartnerContract (ASSETOFTP4)
Partenaire commercial > PGP > Gestionnaire de serveurs	PGP Server Manager (ASSETADM55) plus UI Gestionnaire de profils PGP (PGP)
Partenaire commercial > PGP > Gestionnaire de commanditaires	PGP Sponsor Manager (ASSETADM56) plus UI Gestionnaire de profils PGP (PGP)
Partenaire commercial > PGP > Gestionnaire de partenaires	PGP Partner Manager (ASSETADM57) plus UI Gestionnaire de profils PGP (PGP)

Dans le menu Administration > Déploiement, Ressource de l'interface utilisateur	**Nom du droit / ID du droit**
Déploiement > Services > Installation/Configuration	Installation/Configuration (PLTADM9) plus UI Services (SERVICES)
Déploiement > Services > Configuration	Configuration (PLTADM10) plus UI Services (SERVICES) et UI Gestionnaire de processus techniques (BPMANAGE). Depuis la version 5.2.4.3 et ultérieure, UI Adapters StartStop est également requis.
Déploiement > Planifications	UI Planificateur (SCHEDULER)
Déploiement > Mappes	Maps (ASSETADM5) plus UI_Maps
Déploiement > Normes	Standards (STDSADM7) plus UI_Maps
Déploiement > Bibliothèques de règles étendues	ExtendedRuleLibraries (ASSETADM6) plus UI_Maps

Dans le menu Administration > Déploiement, Ressource de l'interface utilisateur	**Nom du droit / ID du droit**
Déploiement > XSLT	UI XSLT (XSLT)
Déploiement > Web Extensions > Ressources Web	WebResources (GISADM19) plus UI Web Extensions et UI Web Services (WEB_SERVICES) L'interface utilisateur Web Services permet à l'utilisateur d'archiver un nouveau fichier de ressources Web
Déploiement > Web Extensions > Utilitaires	Utilities (GISADM20) plus UI Web Extensions. Visible uniquement dans le cas d'une mise à niveau à partir d'une version antérieure.
Déploiement > Schémas	UI Schémas (SCHEMAS)
Déploiement > Boîtes aux lettres > Configuration	Configuration (MBXADM1) plus UI Boîtes aux lettres (MAILBOX)
Déploiement > Boîtes aux lettres > Racines virtuelles	VirtualRoots (MBXADM2) plus UI Boîtes aux lettres (MAILBOX)
Déploiement > Boîtes aux lettres > Règles de routage	RoutingRules (MBXADM3) plus UI Boîtes aux lettres (MAILBOX)
Déploiement > Boîtes aux lettres > Messages	Messages (MBXADM4) plus UI Boîtes aux lettres (MAILBOX)
Déploiement > EBXML > BPSS	BPSS (ASSETADM7) plus UI EBXML (EBXML)
Déploiement > EBXML> Extension BPSS	BPSSExtension (ASSETADM8) plus UI EBXML (EBXML)
Déploiement > EBXML > CPA	CPA (ASSETADM9) plus UI EBXM (EBXML)
Déploiement > Gestionnaire de ressources > Indicateurs de ressources	Resource Tags (PLTADM1) plus UI Déploiement (DEPLOYMENT)
Déploiement > Gestionnaire de ressources > Importer/Exporter	UI Importer/Exporter (IMPORT_EXPORT)
Déploiement > Utilitaires d'adaptateur > SAP Suite Builder	SAPSuiteBuilder (ASSETADM10) plus UI Utilitaires d'adaptateur
Déploiement > Utilitaires d'adaptateur > Routes Sap > Routes Sap	SAPRoutes (ASSETADM11) plus UI Utilitaires d'adaptateur
Déploiement > Utilitaires d'adaptateur > Routes Sap > SapRouteXRef	SAPRouteXREF (ASSETADM12) plus UI Utilitaires d'adaptateur
Déploiement > Utilitaires d'adaptateur > BEATuxedo	BEATuxedo (ASSETADM13) plus UI Utilitaires d'adaptateur L'option de menu ne s'affiche pas sauf si le fichier jar BEATuxedo est installé.
Déploiement > Utilitaires d'adaptateur > Règle de routage SWIFTNET	UI Règle de routage SWIFTNET (SWIFTNET_ROUTING_RULE)
Déploiement > Utilitaires d'adaptateur > Profil de service SWIFTNET	UI Profil de service SWIFTNET (SWIFTNET_SVC_PROFILE)
Déploiement > Utilitaires d'adaptateur > Profil de service de copie SWIFTNET	UI Profil de service de copie SWIFTNET (SWIFTNET_COPY_PROFILE)

Dans le menu Administration > Déploiement, Ressource de l'interface utilisateur	**Nom du droit / ID du droit**
Déploiement > Utilitaires d'adaptateur > Gestionnaire de règle de verrouillage	LockoutPolicyManager (ASSETADM50)
Déploiement > Utilitaires d'adaptateur > Netmaps C:D > Noeud C:D	CDNetmaps (ASSETADM51) plus UI Utilitaires d'adaptateur (ADAPTER_UTILITIES)
Déploiement > Utilitaires d'adaptateur > Netmaps C:D > Netmaps C:D	CDNodes (ASSETADM52) plus UI Utilitaires d'adaptateur (ADAPTER_UTILITIES)
Déploiement > Utilitaires d'adaptateur > Netmaps C:D > XREF de netmap C:D	CDNetmapXref (ASSETADM53) plus UI Utilitaires d'adaptateur (ADAPTER_UTILITIES)
Déploiement > Utilitaires d'adaptateur > Configuration de règle	Adapter Policies (ASSETADM54)
Déploiement > Utilitaires d'adaptateur > Chemin d'accès de système de fichiers	Chemin d'accès de système de fichiers (ASSETADM58)
Déploiement > Clé d'identité d'hôte SSH	UI Clé d'identité d'hôte (SSH_LCL_ID_KEY) et UI SSH (SSH)
Déploiement > Web Services > Gestionnaire	WebServicesManager (ASSETADM16) et UI Web Services (WEB_SERVICES)
Déploiement > Web Services > Mappe de schémas	SchemaMappings (ASSETADM17), UI Web Services (WEB_SERVICES) et UI EBXML (EBXML)
Déploiement > Web Services > Restituer le WSDL	WSDLCheckIn (ASSETADM18) plus UI Web Services (WEB_SERVICES)
Déploiement > Web Services > Jeton de sécurité	SecurityToken (ASSETADM18) plus UI Web Services (WEB_SERVICES)

Dans le menu Administration > e-Invoicing, Ressource de l'interface utilisateur	**Nom du droit / ID du droit**
e-Invoicing > Contrats	eInvoicing VIEW AGREEMENT (EINV_VIEW_AGREEMENT) La suppression nécessite également le droit eInvoicing DELETE AGREEMENT (EINV_DELETE_AGREEMENT).
e-Invoicing > Archive intégrée	eInvoicing Archive (EINVOICING_ARCHIVE) plus eInvoicing VIEW INVOICE (EINV_VIEW_INVOICE)
e-Invoicing > Configuration	eInvoicing Configuration (EINVOICING_CONFIGURATION)

Dans le menu Administration > Opérations, Ressource de l'interface utilisateur	**Nom du droit / ID du droit**
Système > Programme d'identification des problèmes	Troubleshooter (PLTADM17) plus UI Opérations (OPERATIONS)
Système > Performance > Optimisation	Tuning (PLTADM18) plus UI Opérations (OPERATIONS)

Dans le menu Administration > Opérations, Ressource de l'interface utilisateur	Nom du droit / ID du droit
Système > Performance > Statistiques	Statistics (PLTADM19) plus UI Opérations (OPERATIONS)
Système > Performance > Moniteur JVM	Perfdumps (GISADMIN27) plus UI Opérations (OPERATIONS)
Système > Outils de support > SQL Manager	UI Outil SQL (SQLMANAGER)
Système > Outils de support > Dossier d'assistance	UI Outil Dossier d'assistance (SUPPORT_CASE)
Système > Journaux	UI Journaux (SYSTEM_LOGS)
Système > Licences	UI Licences (LICENSES)
Rapports	UI Rapports (REPORTS)
Activité du système	ThreadMonitor (PLTADM24) plus UI Opérations (OPERATIONS)
Moniteur JDBC	JDBCMonitor (PLTADM25) plus UI Opérations (OPERATIONS) et UI Outil SQL (SQLMANAGER)
Gestionnaire d'archives	UI Archives (ARCHIVE-UI) plus UI Opérations (OPERATIONS), UI Gestionnaire de processus techniques (BPMANAGE) et UI Processus technique (BUSINESS_PROCESS)
Gestionnaire de verrouillages	UI Gestionnaire de verrouillages (LOCK_MANAGER)
Moniteur de messages	MessageMonitor (GISADM24) plus UI Opérations (OPERATIONS)
Services de périphérie	UI Serveurs de périphérie (PSERVERS)
Serveurs proxy	UI Serveurs proxy (PROXYSERVERS) plus Groupe Sterling B2B Integrator Administrateur

Dans le menu Administration > Comptes, Ressource de l'interface utilisateur	Nom du droit / ID du droit
Groupes	UI Groupes (GROUPS) plus UI Comptes (ACCOUNTS)
Droits	Permissions (PLTADM27) plus UI Comptes (ACCOUNTS)
Comptes utilisateur	UI Comptes utilisateur (USER_ACCOUNTS) plus UI Comptes (ACCOUNTS)
Stratégie de mot de passe	PasswordPolicy (PLTADM29) plus UI Comptes (ACCOUNTS)
Actualités utilisateur	UserNews (GISADM25) plus UI Comptes (ACCOUNTS)
Mon compte	MyAccount (PLTADM30)

Droits d'accès préconfigurés

Des droits d'accès préconfigurés sont fournis avec le système. À l'instar des droits d'accès personnalisés, ils permettent d'accéder aux différents modules du système.

Recherche des noms de droits

Vous pouvez rechercher un droit à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour rechercher un droit :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Droits**.
2. Dans la page Droits, effectuez l'une des opérations suivantes :
   - Sous Rechercher, dans la zone **Nom du droit**, entrez tout ou partie du nom du droit que vous recherchez et cliquez sur **OK**. La page Droits répertorie tous les droits correspondant à vos critères de recherche.
   - Sous Liste, dans la zone **Par ordre alphabétique**, sélectionnez **TOUT** ou la lettre qui commence par le nom du droit que vous recherchez et cliquez sur **OK**. La page Droits répertorie tous les droits correspondant à vos critères de recherche.

Création des droits

Si vous avez mis à niveau une version précédente du système, les droits existants sont définis sur Autre par défaut. Vous serez peut-être amené à modifier chaque droit afin de leur appliquer un nouveau type.

Pourquoi et quand exécuter cette tâche

Avant de commencer, vous devez connaître les informations suivantes :

Zone	Description
ID de droit	ID du droit que vous créez. L'ID de droit désigne le nom du processus technique, du document XSLT, du modèle Web ou de la ressource pour lesquels vous définissez le droit. Incluez l'extension de la ressource après l'ID. Obligatoire. Les ID de droit : • Doivent être uniques. • Sont sensibles à la casse. • L'ID de droit doit correspondre au nom du processus technique, du document XSLT, du modèle Web ou de la ressource. Si l'ID de droit et le nom de la ressource ne correspondent pas exactement, il ne vous sera pas possible de verrouiller la ressource.
Nom du droit	Nom du droit que vous créez. Obligatoire. Un nom de droit doit être unique. Les noms de droit sont sensibles à la casse. Par exemple, "Tout document" et "Tout Document" sont deux noms de droit différents.

Zone	Description
Type de droit	Type du droit que vous créez. Obligatoire. Les types de droit sont notamment : • Interface utilisateur : permet d'accéder à des éléments de menu spécifiques de l'interface. • Boîte aux lettres : permet d'accéder à des boîtes aux lettres spécifiques du système. • Modèle : permet d'accéder à des modèles Web spécifiques. • Processus technique : permet d'accéder à des processus techniques spécifiques. • Suivi : permet d'accéder à des options de suivi de documents spécifiques. • Communauté : permet d'accéder à des options de gestion des communautés spécifiques. • Service Web • Service • eInvoicing • Autre : permet d'accéder à des ressources qui ne sont pas identifiées par l'un des types précédents.

Pour créer un droit :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Droits**.
2. En regard de **Créer un nouveau droit**, cliquez sur **OK**.
3. Dans la page Droits, entrez l'**ID de droit**.
4. Entrez le **Nom du droit**.
5. Sélectionnez le **Type du droit**.
6. Cliquez sur **Suivant**.
7. Passez en revue les paramètres du droit.
8. Cliquez sur **Terminer**.

Modification des noms de droit

Si vous souhaitez changer le nom d'un droit d'accès pour le rendre plus parlant, vous pouvez l'éditer. Les noms de droit doivent être uniques et sont sensibles à la casse. Vous ne pouvez pas modifier l'ID de droit. Si vous souhaitez malgré tout le faire, vous devez créer un nouveau droit.

Pourquoi et quand exécuter cette tâche

Pour éditer un nom de droit :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Droits**.
2. Recherchez le droit que vous voulez éditer en utilisant la Recherche par nom de droit ou la Liste par ordre alphabétique et cliquez sur **OK**.
3. En regard du droit que vous souhaitez éditer, cliquez sur **Modifier**.
4. Entrez un nouveau nom dans la zone **Nom du droit**.
5. Mettez à jour le type de droit, si nécessaire, et cliquez sur **Suivant**.
6. Passez en revue les informations sur les paramètres des droits.

7. Cliquez sur **Terminer**.

Suppression des droits

Vous pouvez supprimer un droit associé à un compte utilisateur. Lorsque vous supprimez un droit, vous le supprimez de l'utilisation pour tous les comptes utilisateur.

Pourquoi et quand exécuter cette tâche

Si le droit que vous supprimez est le seul droit associé à un compte utilisateur, vous devez modifier le compte utilisateur pour associer un autre droit. Si vous n'associez pas au moins un nouveau droit au compte utilisateur, l'utilisateur peut se connecter mais il ne dispose d'aucun accès aux éléments de menu.

Pour supprimer un droit :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Droits**.
2. Recherchez le droit que vous voulez supprimer en utilisant la Recherche par nom de droit ou la Liste par ordre alphabétique et cliquez sur **OK**.
3. Dans la page Droits, cliquez sur **Supprimer** en regard du droit que vous souhaitez supprimer.
4. Vérifiez que les informations sur le droit correspondent au droit à supprimer, puis cliquez sur **Supprimer**.

   Le système supprime le droit et affiche le message :

   ```
   Mise à jour du système terminée.
   ```

Vérification du nom et de l'ID d'un droit

Vous pouvez passer en revue le nom et l'ID d'un droit à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour vérifier le nom et l'ID d'un droit :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Droits**.
2. Recherchez le droit que vous voulez vérifier en utilisant la Recherche par nom de droit ou la Liste par ordre alphabétique et cliquez sur **OK**.
3. Sélectionnez le droit. Le nom et l'ID du droit sont affichés.

Comptes utilisateur

Les comptes utilisateur sont définis par des groupes, des droits et des stratégies de mot de passe qui contribuent à offrir un environnement sécurisé. Ce type de définition de compte utilisateur est ce que l'on appelle un modèle de sécurité basé sur les rôles.

Avant de créer des comptes utilisateur, vous devez déterminer les groupes, droits et règles de mot de passe nécessaires à votre environnement professionnel. L'affectation de groupes, droits et règles de mot de passe est facultative.

Seul un compte détenant des droits de création peut créer des comptes utilisateur. Les tâches relatives aux comptes utilisateur sont notamment les suivantes :

- Création d'un compte utilisateur
- Recherche d'un compte utilisateur
- Modification d'un compte utilisateur
- Suppression d'un compte utilisateur

Droits des comptes utilisateur par défaut

Les droits MyAccount et Admin Web App sont automatiquement affectés aux comptes utilisateur.

Les droits suivants sont affectés automatiquement aux comptes utilisateur :

- MyAccount (ID de droit PLTADM30) : permet d'accéder à la page Mon compte (Comptes > Mon compte).
- Droits de l'administrateur Web App (ID de droit WebAppAdminPermission) permet d'accéder à d'autres applications Web.

Ne retirez pas ces droits des comptes utilisateur. En cas de suppression involontaire, éditez le Compte utilisateur et enregistrez. Les droits d'accès manquants seront restaurés.

Authentification des comptes utilisateur

L'authentification de comptes utilisateur peut être locale ou externe.

L'authentification de comptes utilisateur peut être au choix :

- Locale – L'authentification est exécutée auprès de la base de données.
- Externe – L'authentification est exécutée auprès d'un serveur LDAP. L'authentification externe ne requiert pas l'adaptateur LDAP, qui est utilisé avec les processus techniques et permet au système de communiquer avec les serveurs LDAP local ou distant à l'aide d'une interface JNDI. Si vous ne disposez pas d'une licence pour la connexion unique ou LDAP, tous les utilisateurs que vous créez sont des utilisateurs locaux et authentifiés par rapport à la base de données de l'application. Pour créer un compte utilisateur externe, vous devez disposer d'une licence d'application pour la connexion unique ou LDAP.

Liste de contrôle de création d'un compte utilisateur

Vous pouvez créer un compte utilisateur.

Utilisez cette liste de contrôle pour créer un compte utilisateur :

Tâche	Liste de contrôle de la sécurité basée sur les rôles	Vos commentaires
1	Créez des droits ou passez en revue les droits préconfigurés qui sont livrés préinstallés.	
2	Créez des groupes ou passez en revue les groupes qui sont livrés préinstallés.	
3	Créez une règle sur les mots de passe personnalisée à affecter à l'utilisateur.	

Tâche	Liste de contrôle de la sécurité basée sur les rôles	Vos commentaires
4	Si vous utilisez l'authentification externe, configurez l'environnement pour l'authentification externe.	
5	Créez le compte utilisateur et affectez les droits, les groupes et les stratégies de mot de passe.	

Configuration de l'environnement d'authentification de compte utilisateur externe

Si vous créez un utilisateur externe, vous pouvez spécifier une autre méthode d'authentification (LDAP en général).

Pourquoi et quand exécuter cette tâche

Pour créer un compte utilisateur externe, vous devez au préalable effectuer les opérations suivantes :

Procédure

1. Arrêtez Sterling B2B Integrator.
2. Indiquez l'autre méthode d'authentification en ajoutant ou en modifiant la configuration de l'authentification dans le fichier authentication_policy.properties.in. Les propriétés doivent suivre ce format : authentication_4.*xxx*=*xxx*_value.
3. Entrez `setupfiles.sh`.
4. Lancez Sterling B2B Integrator.

Recherche des comptes utilisateur

Vous pouvez rechercher un compte utilisateur à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour rechercher un compte utilisateur :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Comptes utilisateur**.
2. Effectuez l'une des opérations suivantes :
   - Sous Rechercher, dans la zone **Nom du compte**, entrez tout ou partie du nom du compte utilisateur que vous recherchez et cliquez sur **OK**. La page Comptes répertorie tous les comptes utilisateur correspondant à vos critères de recherche.
   - Sous Liste, dans la zone **Par ordre alphabétique**, sélectionnez **TOUT** ou la lettre qui commence par le nom du compte utilisateur que vous recherchez et cliquez sur **OK**. La page Comptes répertorie tous les comptes utilisateur correspondant à vos critères de recherche.

Création des comptes utilisateur

Vous créez un nouveau compte utilisateur à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Avant de commencer, vous devez savoir si vous utilisez une authentification locale ou externe :

- Locale – L'authentification est exécutée auprès de la base de données de l'application. Valeur par défaut.
- Externe – L'authentification est exécutée auprès d'un serveur LDAP. L'authentification externe ne requiert pas l'adaptateur LDAP, qui est utilisé avec les processus techniques et permet au système de communiquer avec les serveurs LDAP local ou distant à l'aide d'une interface JNDI.

Si vous affectez une ou plusieurs clés d'utilisateur autorisé à ce compte, les clés doivent être obtenues auprès de votre partenaire commercial et restituées avant de créer le compte utilisateur.

Remarque : Plusieurs langues étrangères étant prises en charge, un compte utilisateur ne doit pas être utilisé avec plusieurs langues spécifiques afin d'éviter tout problème d'affichage dans l'interface utilisateur.

Vous devez également connaître les informations suivantes :

Zone	Description
ID utilisateur	ID utilisateur du compte utilisateur que vous créez. L'ID utilisateur doit contenir au moins cinq caractères alphanumériques. Aucun caractère spécial, ni aucune ponctuation, n'est autorisé(e). Obligatoire. L'identifiant n'est pas sensible à la casse pour la base de données MySQL uniquement. Vous devez toujours utiliser des ID portant un nom unique, de sorte qu'un utilisateur n'utilise pas l'ID d'un autre par inadvertance.
Mot de passe (authentification locale uniquement)	Mot de passe du compte utilisateur que vous créez. Le mot de passe doit contenir au moins six caractères alphanumériques. Les caractères spéciaux sont autorisés. Obligatoire pour les utilisateurs locaux. Cette zone ne s'affiche pas pour les utilisateurs externes.
Confirmer le mot de passe (authentification locale uniquement)	Entrez le mot de passe une deuxième fois. Obligatoire pour les utilisateurs locaux. Cette zone ne s'affiche pas pour les utilisateurs externes.
Règles (authentification locale uniquement)	Règles sur les mots de passe à associer à ce compte utilisateur. Sélectionnez la règle que vous souhaitez associer dans la liste. Facultatif. Cette zone ne s'affiche pas pour les utilisateurs externes. Le système calcule la date d'expiration à partir de la première date à laquelle l'utilisateur se connecte avec ce mot de passe.
Hôte d'authentification (authentification externe uniquement)	Serveur LDAP (Lightweight Directory Access Protocol) sur lequel l'utilisateur est en cours d'authentification. Le ou les serveurs répertoriés dans cette zone sont spécifiés dans le fichier authentication_policy.properties.in.
Délai d'attente de session	Durée en minutes pendant laquelle vous pouvez être inactif avant d'avoir à vous reconnecter. La durée est en minutes. Obligatoire.

Zone	Description
Accessibilité	Portion de l'interface utilisateur du tableau de bord à laquelle le compte utilisateur a accès. Facultatif. Les options suivantes sont des options d'accessibilité : • Interface utilisateur d'administration – Permet d'accéder au panneau Console d'administration dans le tableau de bord uniquement. • UI AS2 – Permet d'accéder à l'interface de l'édition AS2 uniquement. • UI Dashboard – Permet d'accéder à l'interface du tableau de bord. Pour personnaliser le tableau de bord, choisissez un thème.
Thème de tableau de bord	Tableau de bord prédéfini auquel le compte utilisateur a accès. Obligatoire si l'accessibilité est définie sur UI Dashboard. Les options suivantes sont des options de thème de tableau de bord : • Par défaut • Opérateur • Participant • Commanditaire de participant • Commanditaire • AFT
Prénom	Prénom de l'utilisateur. Obligatoire.
Nom	Nom de l'utilisateur. Obligatoire.
E-mail	Adresse électronique de l'utilisateur.
Messageur	Numéro de messager de poche de l'utilisateur.
Langue préférée	Définissez la valeur sur **Utiliser les paramètres de l'application client**. **Remarque :** Cette valeur indique à Sterling B2B Integrator d'utiliser la langue spécifiée dans le navigateur de l'utilisateur et/ou l'environnement local du système d'exploitation du client. **Remarque :** Il s'agit de la valeur par défaut.
ID de gestionnaire	ID utilisateur du gestionnaire de l'utilisateur.
Identité	Identité du partenaire commercial à associer au compte utilisateur. Un seul partenaire commercial peut être associé à un compte utilisateur. Un compte utilisateur peut être associé à plusieurs groupes, chacun avec sa propre association d'identité de partenaire commercial. Cela permet à un compte utilisateur d'être associé à plusieurs partenaires commerciaux. La zone Identité est utilisée pour le routage des messages dans la boîte aux lettres. Sélectionnez une identité de partenaire commercial dans la liste. La valeur par défaut est Hub Organization.

Pour créer un compte utilisateur :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Comptes utilisateur**.
2. En regard de **Créer un nouveau compte**, cliquez sur **OK**
3. Sur la page Nouveau compte, sélectionnez le **Type d'authentification**.
4. Entrez l'**ID utilisateur**.
5. Entrez le **Mot de passe**.
6. Confirmez le mot de passe.
7. Sélectionnez les **Règles**.
8. Entrez le **Délai d'attente de session**.
9. Sélectionnez l'**Accessibilité**.
10. Sélectionnez le **Thème de tableau de bord**.
11. Cliquez sur **Suivant**.
12. Sur la page Clés d'utilisateur autorisé SSH, affectez une ou plusieurs clés publiques. Déplacez les clés du panneau **Disponible** vers le panneau **Affecté(s)**, puis cliquez sur **Suivant**.
13. Sur la page Groupes, affectez des groupes de droits d'accès. Déplacez les noms de groupe du panneau **Disponible** vers le panneau **Affecté(s)**, puis cliquez sur **Suivant**.
14. Sur la page Droits, affectez des droits d'accès individuels. Déplacez les droits d'accès du panneau **Disponible** vers le panneau **Affecté(s)**, puis cliquez sur **Suivant**. Par défaut, les droits associés aux groupes auxquels cet utilisateur est affecté sont déjà sélectionnés. Les droits d'accès requis sont WebAppAdminPermission et MyAccount.
15. Sur la page Informations utilisateur, entrez le **Prénom**.
16. Entrez le **Nom**.
17. Entrez l'**Adresse électronique**.
18. Entrez le numéro de **Messageur**.
19. Sélectionnez la **Langue préférée**. Sélectionnez la valeur **Utiliser les paramètres de l'application client**.

    Remarque : Cette valeur indique à Sterling B2B Integrator d'utiliser la langue spécifiée dans le navigateur de l'utilisateur et/ou l'environnement local du système d'exploitation du client.
20. Entrez l'**ID de gestionnaire**.
21. Sélectionnez l'**Identité**.
22. Cliquez sur **Suivant**
23. Passez en revue les paramètres du compte utilisateur.
24. Cliquez sur **Terminer**. Le compte utilisateur est créé et ce message s'affiche :

    ```
    Mise à jour du système terminée.
    ```

    Si vous avez créé un utilisateur externe, déconnectez-vous du système, puis reconnectez-vous avec l'ID utilisateur ou le compte externe. Le système va authentifier l'ID utilisateur externe sur le serveur LDAP externe.

Édition des comptes utilisateur

Vous pouvez éditer un compte utilisateur à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Remarque : Plusieurs langues étrangères étant prises en charge, un compte utilisateur ne doit pas être utilisé avec plusieurs langues spécifiques afin d'éviter tout problème d'affichage dans l'interface utilisateur.

Pour éditer un compte utilisateur :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Comptes utilisateur**.
2. Recherchez le compte utilisateur que vous souhaitez éditer en utilisant les options de recherche ou de liste.
3. Cliquez sur **Modifier** en regard du compte utilisateur que vous voulez éditer.
4. Apportez les modifications nécessaires au type d'authentification pour cet utilisateur.

   Si vous changez le type d'authentification externe en local, vous devez créer un mot de passe pour l'utilisateur. Si vous changez le type d'authentification local en externe, vous ne pouvez ni modifier le mot de passe de l'utilisateur, ni la règle de mot de passe.
5. Modifiez le **Nouveau mot de passe** et confirmez-le.
6. Modifiez la **Règle**.
7. Modifiez le **Délai d'attente de session** et cliquez sur **Suivant**.
8. Modifiez la **Clé d'utilisateur autorisé SSH** et cliquez sur **Suivant**.
9. Modifiez les groupes et cliquez sur **Suivant**.
10. Modifiez les droits et cliquez sur **Suivant**.

    Le droit Admin Web App ou MyAccount n'est pas modifiable.
11. Modifiez les informations utilisateur et cliquez sur **Suivant**.

    Remarque : Pour les comptes utilisateur affichant l'interface utilisateur dans une langue étrangère prise en charge, vérifiez que la valeur de Langue préférée est définie sur **Utiliser les paramètres de l'application client**. Cette valeur indique à Sterling B2B Integrator d'utiliser la langue spécifiée dans le navigateur de l'utilisateur et/ou l'environnement local du système d'exploitation du client.
12. Passez en revue les paramètres du compte utilisateur.
13. Cliquez sur **Terminer**.

Suppression des comptes utilisateur

Vous pouvez supprimer un compte utilisateur à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour supprimer un compte utilisateur :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Comptes utilisateur**.
2. Localisez le compte utilisateur que vous voulez supprimer à l'aide des options de recherche ou de liste.
3. Cliquez sur **Supprimer** en regard du compte utilisateur que vous voulez supprimer.
4. Cliquez sur **OK**.

5. Passez en revue les paramètres du compte utilisateur.
6. Cliquez sur **Supprimer**. Le compte utilisateur sélectionné est supprimé et ce message s'affiche :

   ```
   Mise à jour du système terminée.
   ```

Mise à jour des informations de Mon compte

Les informations de Mon compte sont associées à votre nom d'utilisateur et votre mot de passe, de sorte que lorsque vous vous connectez, vos informations personnelles s'affichent dans la page Mon compte. Vous pouvez éditer vos propres informations de compte et modifier la page initiale que vous voyez lorsque vous vous connectez au système.

Pourquoi et quand exécuter cette tâche

Il existe de nombreux cas où des changements d'informations de compte personnel nécessitent la modification de vos informations de compte. En outre, vous pouvez avoir besoin de modifier votre mot de passe pour des raisons de sécurité.

Remarque : Plusieurs langues étrangères étant prises en charge, un compte utilisateur ne doit pas être utilisé avec plusieurs langues spécifiques afin d'éviter tout problème d'affichage dans l'interface utilisateur.

Pour mettre à jour vos informations de compte :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Mon compte**.
2. Si vous souhaitez mettre à jour votre mot de passe de compte, entrez votre mot de passe actuel dans la zone **Ancien mot de passe**, puis entrez un nouveau mot de passe dans la zone **Nouveau mot de passe**. Entrez le nouveau mot de passe à nouveau dans la zone **Confirmer le nouveau mot de passe**.
3. Effectuez toutes les modifications nécessaires dans les zones **Prénom**, **Nom**, **E-mail**, ou **Messageur**.
4. Pour modifier les **Clés d'utilisateur autorisé SSH** affectées à ce compte, déplacez les clés du panneau Disponible vers le panneau Affecté(s).
5. Pour changer la **Langue préférée**, sélectionnez une langue.

   Remarque : Dans le cas des comptes utilisateur affichant l'interface utilisateur dans une langue étrangère prise en charge, vérifiez que la valeur est définie sur **Utiliser les paramètres de l'application client**. Cette valeur indique à Sterling B2B Integrator d'utiliser la langue spécifiée dans le navigateur de l'utilisateur et/ou l'environnement local du système d'exploitation du client.
6. Pour modifier la **Page de bienvenue** (Accueil de la console d'administration) qui s'affiche lorsque vous vous connectez, effectuez une sélection dans la liste.
7. Pour modifier le nombre de processus affichés simultanément sur la page Processus en cours, sélectionnez une nouvelle valeur pour **Taille de page pour les processus en cours**.
8. Pour modifier le nombre de documents affichés simultanément sur la page Documents en cours, sélectionnez une nouvelle valeur pour **Taille de page pour les documents en cours**.
9. Si vous souhaitez réutiliser les fenêtres du navigateur pour lancer des raccourcis, sélectionnez **Réutiliser les fenêtres pour lancer des raccourcis**.

10. Si vous souhaitez que le système effectue un remplissage automatique pour les recherches à partir des chaînes que vous avez précédemment saisies, sélectionnez **Remplissage automatique pour les recherches**.
11. Si vous souhaitez que le système mémorise les valeurs de recherche, sélectionnez **Mémoriser les valeurs de recherche**. Cette option enregistre la dernière valeur que vous avez entrée dans chacune des zones de recherche.
12. Cliquez sur **Enregistrer**. Les nouvelles informations de compte sont enregistrées et ce message s'affiche :

    ```
    Votre mise à jour a été effectuée avec succès.
    ```

Exits utilisateur de compte utilisateur pour connexion (version 5.2.5 et ultérieure)

Sterling B2B Integrator offre des exits utilisateur de synchronisation pour Active Directory, que vous pouvez utiliser pour gérer vos comptes utilisateur avec Active Directory au lieu de l'interface utilisateur de Sterling B2B Integrator. Ces exits utilisateur peuvent être configurés par IBM Services lors d'une interaction avec les clients d'IBM Services. Pour plus d'informations, contactez votre ingénieur commercial IBM.

Exit utilisateur	Description
IUserLoginUserExit_preAuthenticate	Utiliser pour insérer du code personnalisé avant l'authentification.
IUserLoginUserExit_postAuthenticateFail	Utiliser pour insérer du code personnalisé après une authentification réussie.
IUserLoginUserExit_postAuthenticateSuccess	Utiliser pour insérer du code personnalisé après un échec d'authentification.

Exits utilisateur de compte utilisateur pour déconnexion (version 5.2.6 et ultérieure)

Sterling B2B Integrator offre des exits utilisateur de synchronisation pour Active Directory, que vous pouvez utiliser pour gérer vos comptes utilisateur avec Active Directory au lieu de l'interface utilisateur de Sterling B2B Integrator. Ces exits utilisateur peuvent être configurés par IBM Services lors d'une interaction avec les clients d'IBM Services. Pour plus d'informations, contactez votre ingénieur commercial IBM.

Exit utilisateur	Description
ILogoutUserExit_OnSessionInvalidate	Utiliser pour insérer du code personnalisé avant l'invalidation de la session.

Connexion unique

Connexion unique

La connexion unique est un processus d'authentification qui permet aux utilisateurs d'accéder à plusieurs applications en entrant un seul nom d'utilisateur et mot de passe. Auparavant, un utilisateur connecté à chaque application devait gérer plusieurs noms d'utilisateur et mots de passe.

L'authentification utilisateur pour la connexion unique ne requiert pas l'adaptateur LDAP, qui est utilisé avec les processus techniques pour communiquer avec les serveurs LDAP local ou distant à l'aide d'une interface JNDI.

Sterling B2B Integrator active la connexion unique via l'intégration avec Netegrity SiteMinder ou via des classes d'implémentation personnalisée de plug-ins de connexion unique pour d'autres applications et serveurs.

La connexion unique est limitée aux composants suivants :

- Interface d'administration
- Interface de boîtes aux lettres
- Interface de tableau de bord
- Interface de la fonction AFT (Advanced File Transfer)
- Interface MyAFT

Classe par défaut du fournisseur de connexion unique

L'URL de connexion unique pour toutes les interfaces, à l'exception du tableau de bord, est similaire à l'interface de connexion normale. L'URL de l'interface du tableau de bord est http:Host:port/dashboard/sso.jsp. L'en-tête de requête pour l'interface du tableau de bord doit avoir la valeur SM_USER= Nom d'utilisateur de connexion unique (ou bien, la valeur peut être configurée dans le fichier security.properties sous SSO_USER_HEADER).

L'interface SSOProviderDefault permet au plug-in Connexion unique de gérer la fonction de connexion unique pour Netegrity SiteMinder.

Vous pouvez configurer la connexion unique de sorte à rediriger l'utilisateur vers une page HTTP externe (au lieu de la page de déconnexion de Sterling B2B Integrator) lorsque celui-ci se déconnecte de la session de connexion unique. La page externe accessible du serveur de connexion unique peut être soit une page de connexion, soit une page de déconnexion.

L'exemple suivant montre la classe SSOProviderDefault.java :

```
package com.sterlingcommerce.server_name.security.authentication;
import javax.servlet.*;
import javax.servlet.http.*;
import com.sterlingcommerce.server_name.security.SecurityManager;
import com.sterlingcommerce.server_name.util.frame.log.Logger;
import java.util.Properties;
import com.sterlingcommerce.server_name.util.frame.Manager;
import java.util.*;
/**
 * Default Single Sign On implementation for ISSOProvider that will use
* Request Header to get SSO_USER
 *
 * @author developer name
 */
public final class SSOProviderDefault implements ISSOProvider {
    private static final String CLASS_NAME = "SSOProviderDefault";
    private static final Logger LOG = SecurityManager.getInstance().getLogger();
    private static final Logger AUTHLOG =
            SecurityManager.getInstance().getAuthenticationLogger();
/**
* Authenticate SSO processing (login)
*
* @param Request : The http request.
*
* @return String : The SSO User ID if the authentication is passed
```

```
* : null if authentication is denied
* << No Exception thrown for the default SSO Provider - Either have value or null >>
*/
public String authenticate(HttpServletRequest request)
                        throws SSOAuthenticationException, SSOException
{
    String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());
    if (AUTHLOG.debug) {
          AUTHLOG.logDebug(CLASS_NAME + " Authenticate user tag : " +
              SecurityManager.getInstance().getSSOAuthenticationHeader() +
              " value : " + sso_user);
    }
    return sso_user;
}
/**
 * AuthenticatePage SSO processing (Page)
 *
 * @param Request : The http request.
*
 * @return boolean : True if the SSO authentication on the Page is passed or no Page
 * authentication is needed because not enable or not SSO User.
 * : False if authentication is denied
 * (Must throw SSOException if return false!!!!)
 */
public boolean authenticatePage(HttpServletRequest request)
                         throws SSOAuthenticationException, SSOException
{
    return true; // Always pass Page Validation for SSOProviderDefault
    /***** Uncomment if want to do SSO_USER_HEADER (SM_USER) check on Page
    String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());
    if (sso_user != null) {
       passed = true;
    } else {
       passed = false;
       throw new
   SSOAuthenticationException(ISSOProvider.REASON_SSO_AUTHENTICATION_FAILURE);
    }
    return passed; ******/
}
/**
 * When user logs out, calling this to do any extra actions
*
 * @param Response : The http response
 * @param Request : The http request.
 * @param int reason : An id to to tell where we called from
* @param String : The String identify the session type: WS, DASHBOARD, MAILBOX,
 * AFT, MYAFT, or null if don't know
*
 * @return boolean : True if executes sucessfully,
 * False if not & should use default logout logic
 *
 */
public boolean invalidate(HttpServletRequest request, HttpServletResponse response,
int reason, String sessionType)
{
    HttpSession session = request.getSession(false);
    String forward = "SSO_FORWARD_URL";
    if (sessionType != null) {
       forward = forward + ".";
       forward = forward + sessionType;
    }
    if (reason == REASON_GIS_SESSION_EXPIRED) {
       forward = forward + ".GIS_TIMEOUT";
    }
    else if (reason == REASON_LOGOUT) {
```

```
       forward = forward + ".LOGOUT";
    }
    else { // Others reason : send all to VALIDATION_FAILED
       forward = forward + ".VALIDATION_FAILED";
    }
    String forwardUrl = getForwardURLParameter(forward);
    if (AUTHLOG.debug) {
       AUTHLOG.logDebug(CLASS_NAME + " Forward properties: " + forward +
" is forwardUrl: " + forwardUrl);
    }
    if (forwardUrl != null) {
       try {
           // Dashboard Timeout - Use JSP to kick outof IFrame
           if ((reason == REASON_GIS_SESSION_EXPIRED)&&
  (sessionType != null) &&
               (sessionType.equalsIgnoreCase(DASHBOARD_SESSION))) {
              if (AUTHLOG.debug) {
                   AUTHLOG.logDebug(CLASS_NAME + " Set ExternalSsoUrl = "
                                                + forwardUrl); }
              request.setAttribute("ExternalSsoUrl", forwardUrl);
              return false; // Set to false, we need to handle redirect in JSP
           } else {
              response.sendRedirect(response.encodeRedirectURL(forwardUrl));
           }
       } catch (Exception e) {
           return false;
       }
       return true;
   }
   return false; // Use default logic (ie: GIS Logout/Login Page)
}
}
```

Composants de plug-in Connexion unique

Sterling B2B Integrator active une classe d'implémentation personnalisée pour les plug-ins ce connexion unique sur d'autres applications et serveurs de connexion unique. Pour implémenter un plug-in de connexion unique, vous devez ajouter une classe d'implémentation SSO_AUTHENTICATION_CLASS.<n>=<Entrée nouvelle classe> dans le fichier security.properties.

Vous pouvez écrire des classes d'implémentation personnalisée pour les plug-ins de connexion unique en fonction de la classe d'interface ISSOProvider.java suivante.

Classe d'interface SSOProvider.java

```
import javax.servlet.*;
import javax.servlet.http.*;
public interface ISSOProvider {
public static final int REASON_UNKNOWN = -1;
public static final int REASON_SSO_SESSION_EXPIRED = 1
public static final int REASON_HTTP_SESSION_EXPIRED = 2;
public static final int REASON_LOGOUT = 3;
public static final int REASON_SSO_AUTHENTICATION_FAILURE = 4;
public static final int REASON_GIS_AUTHENTICATION_FAILURE = 5;
public String authenticate(HttpServletRequest request)
throws SSOAuthenticationException, SSOException;
public boolean invalidate(HttpServletRequest request,
HttpServletResponse response, int reason, String sessionType)
throws SSOAuthenticationException;
public boolean authenticatePage(HttpServletRequest request)
throws SSOAuthenticationException, SSOException;
}
```

SSOException class

```
public class SSOException extends Exception {
private int reason = -1;
public int getReason() { return reason; }
public void setReason(int reason) { this.reason = reason; }
}
```

SSOAuthenticationException class

```
public class SSOAuthenticationException extends SSOException { }
```

Méthode d'authentification des utilisateurs

La méthode authenticate est initialisée lors de la connexion. Elle renvoie l'ID utilisateur en cas de réussite de l'authentification et une exception SSOAuthenticationException en cas d'échec. L'exception doit contenir un code raison pertinent et une page de redirection à traiter, si les en-têtes de connexion unique sont présents. Si ces en-têtes sont absents, le contrôle est renvoyé à l'écran de connexion système.

Méthode d'authentification des pages

La méthode authenticatePage est initialisée sur chaque page. Elle traite les validations supplémentaires à effectuer au cours de la transition de page à partir du serveur de connexion unique. Par exemple, vous pouvez communiquer avec le serveur de connexion unique (à l'aide de la commande PING) pour vérifier si la session de connexion unique a expiré. En cas d'authentification infructueuse, une exception contenant le code raison de l'échec ainsi qu'une page de redirection est émise.

Demandes de connexion unique non valides

La méthode invalidate est initialisée lorsque l'utilisateur se déconnecte, ne parvient pas à authentifier la connexion ou la page, ou lorsque la session expire. La méthode de redirection HTTP doit être exécutée pour invalider les demandes de connexion unique. Les méthodes suivantes sont initialisées en cas d'échec de l'authentification :

- Si l'authentification du serveur de connexion unique réussit et que l'authentification Sterling B2B Integrator échoue, la méthode REASON_GIS_AUTHENTICATION_FAILURE est initialisée avec le code raison.
- Si l'authentification du serveur de connexion unique échoue, la méthode REASON_SSO_AUTHENTICATION_FAILURE est initialisée avec le code raison.
- Si l'utilisateur se déconnecte, la méthode REASON_LOGOUT est initialisée avec le code raison.
- Si la session HTTP expire, la méthode REASON_HTTP_SESSION_EXPIRED est initialisée avec le code raison.
- Si la session de connexion unique de l'utilisateur expire, la méthode REASON_SSO_SESSION_EXPIRED est initialisée avec le code raison.

Configuration de la connexion unique à l'aide de la liste de contrôle de Netegrity SiteMinder

Avant de pouvoir configurer la connexion unique (SSO), vous devez avoir des connaissances sur ce processus et sur Netegrity SiteMinder.

Pour configurer la connexion unique avec Netegrity SiteMinder, utilisez la liste de contrôle suivante :

Tâche	Connexion unique à l'aide de la liste de contrôle de Netegrity SiteMinder	Remarques
1	Installez Netegrity SiteMinder et configurez-le avec un serveur proxy inverse.	
2	Configurez les fichiers de propriétés pour une utilisation avec Netegrity SiteMinder.	
3	Configurez le serveur proxy sécurisé Netegrity.	
4	Créez des domaines sécurisés sur le serveur Netegrity.	

Pour plus d'informations sur l'implémentation personnalisée de plug-ins de connexion unique sur d'autres SSO sur des applications et des serveurs, consultez la section Composants des plug-ins de connexion unique.

Connexion unique à l'aide d'IBM (version 5.2.6 ou ultérieure)

Les utilisateurs Sterling B2B Integrator ayant les droits appropriés peuvent directement accéder à l'outil de gestion d'IBM® par le biais d'une connexion unique depuis Sterling B2B Integrator pour gérer Boîte aux lettres globale .

Avant de commencer

Les utilisateurs de Sterling B2B Integrator doivent appartenir à l'un des groupes suivants pour accéder directement à l'outil de gestion de Boîte aux lettres globale depuis Sterling B2B Integrator :

- *BOÎTE AUX LETTRES*
- *Déploiement*
- *Administrateurs de boîtes aux lettres*
- *Sterling B2B Integrator Admin*

Pourquoi et quand exécuter cette tâche

Lorsque vous choisissez d'accéder à l'outil de gestion de Boîte aux lettres globale par le biais d'une connexion unique, votre nouvelle session Boîte aux lettres globale s'ouvre dans un nouvel onglet de navigateur Web, tandis que votre session Sterling B2B Integrator reste disponible.

Vous pouvez accéder à Boîte aux lettres globale par le biais d'une connexion unique uniquement depuis Sterling B2B Integrator. Si vous vous déconnectez de l'outil de gestion de Boîte aux lettres globale , vous n'êtes pas déconnecté de votre session Sterling B2B Integrator.

Si vous voulez modifier votre mot de passe administrateur de Boîte aux lettres globale , vous devez vous connecter directement dans l'outil de gestion de Boîte aux lettres globale .

Restriction : Si vous vous connectez dans l'outil de gestion de Boîte aux lettres globale par le biais d'une connexion unique, vous ne pouvez pas modifier votre mot de passe administrateur Boîte aux lettres globale et l'option **Change password**, dans le menu **Administrator**, n'est pas disponible.

Pour accéder à l'outil de gestion d'Boîte aux lettres globale par le biais d'une connexion unique :

Procédure

1. Dans la page Admin Console, développez **Déploiement** dans le menu Administration.
2. Développez **Global Mailbox**.
3. Sélectionnez **Mailbox Administration**.
4. Cliquez sur le lien hypertexte **Launch Global Mailbox Management Tool** pour ouvrir une nouvelle session dans l'outil de gestion de Boîte aux lettres globale .

   A faire : Lorsque vous cliquez sur le lien hypertexte **Launch Global Mailbox Management Tool**, une nouvelle session Boîte aux lettres globale s'ouvre dans un nouvel onglet du navigateur Web.

Configuration des fichiers de propriétés pour la connexion unique avec Netegrity SiteMinder

Vous pouvez configurer des fichiers de propriétés pour la connexion unique avec Netegrity SiteMinder.

Pourquoi et quand exécuter cette tâche

Pour éditer les fichiers neo-ui.properties et security.properties :

Procédure

1. Arrêtez Sterling B2B Integrator.
2. Accédez au répertoire */rép_install*/install/properties.
3. Ouvrez le fichier neo-ui.properties.
4. Ajoutez l'entrée Connexion unique associée pour chaque interface. L'exemple de code suivant montre l'entrée associée à des sites HTTP identiques :

```
url.host=%(host)
url.port=10200
url.cm=http://%(host):10200/communitymanagement/
url.cm.sso=http://%(host):10200/communitymanagement/
url.ob=http://%(host):10233/onboard/
url.ws=http://%(host):10200/ws/
url.ws.sso=http://%(host):10200/ws/
url.dash.sso=http://%(host):10233/dashboard/
url.ds=http://%(host):10200/datastore/
url.help=http://%(host):10200/help/index.htm?context=webhelplocal&single=true&topic=
url.help.ja=http://%(host):10200/help_ja/index.htm?context=webhelplocal&single=true& topic=
url.dash=http://%(host):10233/dashboard/
portlet.refresh.interval.seconds=60
url.aft=http://%(host):10200/aft/
url.aft.sso=http://%(host):10200/aft/
url.dmi=http://%(host):10200/dmi/
url.dmi.sso=http://%(host):10200/dmi/
```

5. Enregistrez et fermez le fichier neo-ui.properties.

6. Ouvrez le fichier */rép_install*/install/properties/security.properties dans un éditeur de texte.
7. Dans le fichier security.properties, recherchez les paramètres de ## Configuration de l'authentification de la connexion unique, comme illustré dans l'exemple de code suivant :

```
## Configuration de l'authentification de la connexion unique
## enable sso authentication (true, false) default=false
SSO_AUTHENTICATION_ENABLED=true
## enable sso authentication on each Page (true, false) default=false
#SSO_PAGE_AUTHENTICATION_ENABLED=false
## http header variable that contains externally authenticated userid
SSO_USER_HEADER=SM_USER
## List of SSOProvider Classes that are supplied to use - If SSO Authentication is
## enable, should have at least one class, the following is the default one that we
## supplied.
## SSO_AUTHENTICATION_CLASS.1= <SSOProvider Class 1> Will try to use this first
## SSO_AUTHENTICATION_CLASS.2= <SSOProvider Class 2> Will try to use this if first
## one failed
## SSO_AUTHENTICATION_CLASS.3= <SSOProvider Class 3> Will try to use this if second ## one failed too
## SSO_AUTHENTICATION_CLASS.<n>= <SSOProvider Class n> Will try to use this if all
## first –1 classes failed
SSO_AUTHENTICATION_CLASS.1=com.sterlingcommerce.woodstock.security.authentication.SS OProviderDefault
## External Page for SSO when Logout (Specify the SSO Server external page for each of
## the cases)
## Example: SSO_FORWARD_URL.MAILBOX.LOGOUT=http://sterlingcommerce.com
## After SSO User logout from Mailbox, instead of display the Mailbox Login Screen
## display IBM Web page.
SSO_FORWARD_URL.AFT.LOGOUT=
SSO_FORWARD_URL.MYAFT.LOGOUT=
SSO_FORWARD_URL.MAILBOX.LOGOUT=
SSO_FORWARD_URL.WS.LOGOUT=
SSO_FORWARD_URL.DASHBOARD.LOGOUT=
## Default handling for LOGOUT if don't know source
SSO_FORWARD_URL.LOGOUT=
## External Page for SSO when Timeout (Specify the SSO Server External page for each ## of the case)
SSO_FORWARD_URL.AFT.GIS_TIMEOUT=
SSO_FORWARD_URL.MYAFT.GIS_TIMEOUT=
SSO_FORWARD_URL.MAILBOX.GIS_TIMEOUT=
SSO_FORWARD_URL.WS.GIS_TIMEOUT=
SSO_FORWARD_URL.DASHBOARD.GIS_TIMEOUT=
## Default handling for TIMEOUT if don't know source
SSO_FORWARD_URL.GIS_TIMEOUT=
## External Page for SSO on Validation/Authentication failure (SSO User Validation
## Failed - At login or Page Validation)
SSO_FORWARD_URL.AFT.VALIDATION_FAILED=
SSO_FORWARD_URL.MYAFT.VALIDATION_FAILED=
SSO_FORWARD_URL.MAILBOX.VALIDATION_FAILED=
SSO_FORWARD_URL.WS.VALIDATION_FAILED=
SSO_FORWARD_URL.DASHBOARD.VALIDATION_FAILED=
##Default handling for VALIDATION FAILED if don't know source
SSO_FORWARD_URL.VALIDATION_FAILED=
```

8. Sous l'entrée ## Configuration de l'authentification de la connexion unique, apportez les modifications suivantes aux paramètres de connexion unique :

Paramètre	Description	Valeur fournie	Nouvelle valeur
SSO_AUTHENTICATION_ ENABLED	Active ou désactive l'utilisation de la connexion unique.	Faux	Vrai

Paramètre	Description	Valeur fournie	Nouvelle valeur
SSO_USER_HEADER	Nom de l'en-tête utilisateur dans Netegrity SiteMinder ou dans la configuration de l'application Connexion unique.	SM_USER Il s'agit de la valeur dans Netegrity SiteMinder.	Doit correspondre à l'entrée dans Netegrity SiteMinder ou votre application Connexion unique.
SSO_PAGE_ AUTHENTICATION_ ENABLED	Active ou désactive l'authentification par connexion unique sur chaque page.	Faux	Vrai : active l'authentification par connexion unique sur chaque page. Ne modifiez cette valeur que si la classe Fournisseur de connexion unique est fournie.
SSO_AUTHENTICATION_ CLASS.n	Classe d'implémentation qui fournit la prise en charge de l'authentification.	com.sterling commerce.woodstock. security.authentication .SSOProviderDefault	Effectuez une sélection dans la liste des classes SSOProvider fournies.
SSO_FORWARD_ URL URL	Affiche la page d'URL fournie lorsque vous vous déconnectez de la boîte aux lettres. Sinon, affiche la valeur par défaut.	Commented Affiche la page par défaut.	Indiquez l'URL.

9. Enregistrez et fermez le fichier security.properties.
10. Lancez Sterling B2B Integrator.

Configuration d'un serveur proxy sécurisé Netegrity

Vous pouvez configurer le serveur proxy sécurisé Netegrity en ajoutant des règles de transfert au fichier proxyrules.xml.

Pourquoi et quand exécuter cette tâche

Avant de configurer le serveur proxy sécurisé Netegrity, vous devez :

- Installer Sterling B2B Integrator sur un serveur tel que acme.si.com.
- Connaître le numéro de port sur lequel l'interface MBI (Mailbox Browser Interface) est installée. Vous devez utiliser ces informations dans les règles de transfert appropriées.
- Connaître le numéro de port sur lequel l'interface utilisateur de tableau de bord Sterling B2B Integrator est installée. Vous devez utiliser ces informations dans les règles de transfert appropriées.

Pour configurer le serveur proxy sécurisé Netegrity :

Procédure

1. Ajoutez les règles de transfert nécessaires pour Sterling B2B Integrator dans le fichier /opt/netegrity/proxy-engine/conf/proxyrules.xml.

   L'exemple suivant montre à quoi le fichier proxyrules.xml terminé doit ressembler une fois que vous avez ajouté les règles de transfert pour accéder aux composants Sterling B2B Integrator :

```
<?xml version="1.0"?>
<?cocoon-process type="xslt"?>
<!DOCTYPE nete:proxyrules SYSTEM "file:////home/netegrity/proxy-engine/conf/dtd/proxyrules.dtd">
<!-- Proxy Rules-->
<nete:proxyrules xmlns:nete="http://acme.com/">
   <nete:cond criteria="beginswith" type="uri">
<nete:case value="/gbm">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/help">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/webxtools">
   <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/mailbox">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/dashboard">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:case value="/portlets">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:case value="/datastore">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:default>
   <nete:forward>http://acme.portalserver.com$0</nete:forward>
</nete:default>
</nete:cond>
</nete:proxyrules>
```

2. Ajoutez ce qui suit aux lignes du fichier proxyrules.xml afin de désactiver la vérification des scripts de serveur intersite sur le serveur proxy sécurisé, car Sterling B2B Integrator ne prend pas en charge l'application des règles de script de serveur intersite Netegrity.

   ```
   # Web Agent.conf
   <WebAgent>
   ...." existing web agent configuration parameters"
   badurlchars=""
   badcsschars=""
   CSSChecking="NO"
   </WebAgent>
   ```

3. Enregistrez et fermez le fichier proxyrules.xml.

Création de domaines sécurisés sur le serveur de stratégies Netegrity

L'administrateur du serveur de stratégies Netegrity doit créer des domaines sécurisés autour de chaque masque d'URL en cours transmis par le serveur proxy sécurisé. Ces domaines de sécurité doivent disposer des droits nécessaires pour l'authentification et l'autorisation.

Pourquoi et quand exécuter cette tâche

En outre, l'agent Web sur le serveur proxy sécurisé doit être configuré pour communiquer avec le serveur de stratégies.

Créez un domaine sécurisé pour chaque masque d'URL répertorié :

Masque d'URL	Permet d'accéder à :
/mbi/*	Interface de boîtes aux lettres de l'application
/dashboard/*	Interface de tableau de bord de l'application, au format http://host:port/dashboard
/datastore/*	Composants de magasin de données
/portlets/*	Composants de portlet d'application dans l'interface de tableau de bord
/help/*	Composants de l'aide contextuelle
/webxtools/*	Utilitaires d'extensions Web
/gbm/*	Composants du modélisateur GPM (Graphical Process Modeler)

Mots de passe

Règles sur les mots de passe

Les stratégies de mot de passe sont des ensembles de décisions de sécurité que vous prenez et qui s'appliquent à divers comptes utilisateur selon les règles de sécurité en vigueur dans votre entreprise. Ces choix définissent notamment le nombre de jours durant lesquels un mot de passe est valide, ou bien la longueur maximale et minimale d'un mot de passe.

Les stratégies de mot de passe permettent de rationaliser vos opérations de sécurité lors de l'ajout de nouveaux utilisateurs. Au lieu d'ajouter des règles individuelles pour chaque utilisateur, il vous suffit de créer une seule règle sur les mots de passe et l'appliquer à tous les utilisateurs qui ont besoin du même accès.

Une fois que vous avez créé une règle sur les mots de passe, appliquez-la uniquement aux comptes utilisateur internes. Vous disposerez ainsi d'une grande souplesse de gestion de vos règles de sécurité. Si vous utilisez LDAP, vous ne pouvez pas appliquer les stratégies de mot de passe à vos comptes externes.

Les valeurs par défaut de la règle sur les mots de passe sont les suivantes :

Paramètre	Valeur par défaut
ID de la règle	utilisateur_défaut
Nom de règle	Règle utilisateur par défaut
Nombre de jours de validité	60
Longueur minimale	6
Longueur maximale	28
Nombre de mots de passe conservés dans l'historique	5
Caractères spéciaux obligatoires dans le mot de passe	Sélectionné
Modification du mot de passe obligatoire à la prochaine tentative de connexion	Sélectionné

Les tâches relatives aux stratégies de mot de passe sont notamment les suivantes :

- Création d'une règle sur les mots de passe

- Recherche d'une règle sur les mots de passe
- Édition d'une règle sur les mots de passe
- Suppression d'une règle sur les mots de passe
- Édition du paramètre de verrouillage
- Édition du message d'expiration de mot de passe

Stratégie de mot de passe personnalisée

La stratégie de mot de passe personnalisée Sterling B2B Integrator est une fonction de sécurité qui ajoute des stratégies de mot de passe. Ces règles supplémentaires peuvent vous aider à empêcher l'utilisation de mots de passe faibles faciles à pirater et à rejeter les mots de passe non conformes.

Pour activer cette fonction, vous devez :

- Implémenter du code Java personnalisé via un plug-point. Une fois activé, le plug-point est utilisé pour tous les utilisateurs du système qui sont associés à une stratégie de mot de passe (il s'agit d'un paramètre global).
- Ajouter la propriété passwordPolicyExtensionImpl au fichier customer_overrides.properties.
- Appliquer la stratégie de mot de passe personnalisée aux Comptes utilisateur.

L'extension de la stratégie de mot de passe personnalisée prévaut sur la stratégie de mot de passe par défaut. Si un mot de passe enfreint plusieurs règles de la stratégie (appliquées par la classe d'extension et par l'implémentation par défaut), seul le message d'erreur renvoyé par la classe d'extension est affiché pour l'utilisateur.

Exemple : Stratégie de mot de passe

Cet exemple affiche un paramètre possible pour une stratégie de mot de passe.

Une stratégie de mot de passe, appelée Test, pourrait avoir les paramètres suivants pour un mot de passe :

- Une validité de 10 jours
- Une longueur minimale de 10 caractères
- Une longueur maximale de 20 caractères
- Doit comporter au moins deux caractères spéciaux
- L'utilisateur doit changer de mot de passe par défaut lors de la connexion initiale
- Le nombre de mots de passe conservés dans l'historique est défini

Si on s'appuie sur l'exemple précédent, l'utilisateur se voit attribuer un nom d'utilisateur et un mot de passe par l'administrateur système. L'utilisateur se connecte à l'aide du nom d'utilisateur et du mot de passe fournis et il est invité à changer le mot de passe. S'il n'entre pas un mot de passe comportant au moins 10 caractères, plus de 20 caractères et au moins deux caractères spéciaux, il est invité à corriger le mot de passe. Une fois que toutes les conditions de changement définies dans la stratégie de mot de passe sont remplies, le système enregistre le nouveau mot de passe et autorise l'accès à l'utilisateur. Chaque compte utilisateur ne peut avoir qu'une seule stratégie de mot de passe associée, mais vous pouvez appliquer une stratégie de mot de passe à plusieurs comptes utilisateur.

Outre les changements de la stratégie de mot de passe dans l'interface, vous pouvez modifier le nombre de connexions infructueuses autorisées avant le verrouillage du compte auquel l'utilisateur tente de se connecter.

Par exemple, si le nombre de tentatives de connexion consécutives avant le verrouillage est de trois et que vous entrez trois fois de suite un mot de passe erroné, vous ne pourrez plus vous connecter à partir de cet ordinateur spécifique. Vous pourrez vous connecter à partir d'un autre ordinateur disposant d'un accès au système.

Mot de passe ou phrase passe d'installation

Lors de l'installation de Sterling B2B Integrator, vous devez créer une phrase passe de système. Cette phrase passe est une chaîne hautement complexe de plus de 16 caractères. La phrase passe de système est requise pour démarrer le système et accéder aux informations protégées du système.

La seule personne habilitée à mettre à jour ou à changer la phrase passe est celle qui a créé ou installé le logiciel. Si vous perdez ou oubliez votre phrase passe, vous ne pourrez pas démarrer le système. Le seul utilisateur habilité à mettre à jour la phrase passe du système est celui qui a effectué l'installation.

La phrase passe de système n'est pas stockée dans le système, sauf sur les installations Windows où elle est stockée dans un format masqué dans le fichier security.properties afin de faciliter l'exécution du système en tant que service non interactif. Cette phrase peut être stockée en clair pour d'autres plateformes dans le fichier security.properties, si bien que vous n'avez pas à les entrer sur la ligne de commande lorsque vous démarrez le système. Cependant, la phrase passe du système est uniquement protégée par le contrôle d'accès au fichiers du système d'exploitation.

Liste de contrôle de la stratégie de mot de passe personnalisée

Vous pouvez implémenter une stratégie de mot de passe personnalisée.

Utilisez la liste de contrôle suivante pour implémenter une stratégie de mot de passe personnalisée :

Tâche	**Liste de contrôle de la stratégie de mot de passe personnalisée**
1	Créez une structure de répertoire dans <rép_install_SI> à des fins de test, de règle et d'extension.
2	Créez la classe java dans le répertoire d'extension.
3	Spécifiez la classe Java implémentant la stratégie de mot de passe (propriété passwordPolicyExtensionImpl) dans le fichier customer_overrides.properties.
4	Ajoutez la classe d'implémentation jar dans le chemin d'accès aux classes.
5	Définissez un message d'erreur.

Exemple : Stratégie de mot de passe personnalisée

Cet exemple illustre une extension de stratégie de mot de passe personnalisée.

Voici un exemple d'extension d'une stratégie de mot de passe personnalisée.

L'interface com.sterlingcommerce.woodstock.security.PasswordPolicyExtension a été ajoutée au système comme suit :

```
public interface IPasswordPolicyExtension {
    /**
     * Implements extended validation on passwords and
returns null if password
     * validation is successful. If validation fails,
an error message key
     * that may be looked up in Login_*.properties* should
be returned.
     * @param password - The password string to validate
     * @param policyId - The PWD_POLICY.POLICY_NAME of
the policy associated with the user in case the extension needs
it.
     * @return String Return null if password validation
was successful, the error message key if password validation fails
     */
    public String validateNewPassword (String password,
String policyName);
}
```

Le renvoi de la valeur NULL de la méthode indique que le mot de passe a été accepté. Le renvoi de toute autre valeur signifie que le mot de passe n'est pas valide.

Exemple d'implémentation

```
package test.policy.extension;
import java.util.regex.Pattern;
public class PwdPolExtnImpl implements com.sterlingcommerce.woodstock.security.IPasswordPolicyExtension
{
   public String validateNewPassword(String
pwd,
                  String policyName) {
           // Additional password validation checks
                  boolean match=Pattern.matches(".*[a-z].*",
pwd) && Pattern.matches(".*[A-Z].*", pwd) && (Pattern.matches(".*[0-9].*",
pwd) || Pattern.matches(".*[^A-Za-z0-9].*",pwd));
                  if (match==true) return null;
                  else return "nogood";
      }

}
```

Recherche de stratégies de mot de passe

Vous pouvez rechercher une stratégie de mot de passe à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour rechercher une stratégie de mot de passe, procédez comme suit :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Règles sur les mots de passe**.
2. Dans la page Règles sur les mots de passe, effectuez l'une des opérations suivantes :
   - Sous Rechercher, dans la zone **Nom de la règle sur les mots de passe**, entrez tout ou partie du nom de la règle sur les mots de passe que vous recherchez et cliquez sur **OK**. La page Règles sur les mots de passe répertorie tous les droits correspondant à vos critères de recherche.
   - Sous Liste, dans la zone **Par ordre alphabétique**, sélectionnez **TOUT** ou la lettre qui commence par le nom de la règle sur les mots de passe que vous recherchez et cliquez sur **OK**. La page Règles sur les mots de passe répertorie tous les droits correspondant à vos critères de recherche.

Création de stratégies de mot de passe

Vous pouvez créer une stratégie de mot de passe pour l'affecter à des comptes utilisateur. Cette démarche n'est pas obligatoire mais elle est très importante pour la gestion de votre sécurité.

Pourquoi et quand exécuter cette tâche

Avant de commencer, vous devez connaître les informations suivantes :

Zone	Description
ID de la règle	Identificateur de la stratégie de mot de passe de la base de données.
Nom de règle	Nom de stratégie de mot de passe qui s'affiche dans l'interface utilisateur lorsque la stratégie de mot de passe est désignée.
Nombre de jours de validité	Nombre de jours de validité d'un mot de passe utilisateur. La valeur par défaut est 0, ce qui signifie que le mot de passe n'expire jamais. Si vous fournissez une valeur comprise entre 1 et 999, l'utilisateur est invité à modifier le mot de passe une fois ce délai arrivé à expiration. Le compteur du délai d'expiration démarre lors de la première connexion de l'utilisateur, après l'attribution d'un mot de passe au compte utilisateur.
Longueur minimale	Longueur minimale du mot de passe. Obligatoire. Les valeurs valides sont des chiffres dont le nombre doit être au moins égal à 6. La valeur par défaut est 6. Si aucune stratégie n'est appliquée, le système impose une longueur minimale de 6 chiffres.
Longueur maximale	Longueur maximale du mot de passe. Obligatoire. Les valeurs valides sont des chiffres dont le nombre doit être au moins égal à celui de la longueur minimale. La valeur par défaut est 28.
Nombre de mots de passe conservés dans l'historique	Nombre de mots de passe à conserver dans la table PWD_HISTORY de la base de données pour un utilisateur. Une fois ce nombre de mots de passe dépassé, le plus ancien mot de passe est supprimé de la table et il peut être réutilisé. La valeur par défaut est 0.

Zone	Description
Caractères spéciaux obligatoires dans le mot de passe	Indique que le mot de passe doit contenir au moins un caractère spécial. Les valeurs valides comprennent des chiffres, des lettres majuscules, !, @, #, $, %, ^, & ou *.
Modification du mot de passe obligatoire à la première tentative de connexion	Indique que l'utilisateur doit modifier le mot de passe par défaut après la première connexion. L'utilisateur est invité à modifier son mot de passe à l'issue de la connexion initiale.

Pour créer une stratégie de mot de passe :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Règles sur les mots de passe**.
2. En regard de **Créer une nouvelle règle sur les mots de passe**, cliquez sur **OK**.
3. Dans la page Règles sur les mots de passe, entrez l'**ID de la règle**.
4. Entrez le **Nom de la règle**.
5. Entrez le **Nombre de jours de validité**.
6. Entrez la **Longueur minimale**.
7. Entrez la **Longueur maximale**.
8. Entrez le **Nombre de mots de passe conservés dans l'historique**.
9. Si le mot de passe doit contenir des caractères spéciaux, cochez la case correspondante.
10. Si l'utilisateur doit changer le mot de passe lors de la première tentative de connexion, cochez la case correspondante.
11. Cliquez sur **Suivant**.
12. Passez en revue les paramètres de la stratégie de mot de passe.
13. Cliquez sur **Terminer**.

Édition des stratégies de mot de passe

Vous pouvez éditer la stratégie de mot de passe à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour éditer les stratégies de mot de passe :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Règles sur les mots de passe**.
2. Recherchez les stratégies de mot de passe que vous souhaitez éditer en utilisant les options de recherche ou de liste.
3. Cliquez sur **Modifier** en regard des stratégies de mot de passe que vous voulez éditer.
4. Dans la page Paramètres de règles sur les mots de passe, apportez les modifications appropriées, puis cliquez sur **Suivant**.
5. Passez en revue les paramètres de la stratégie de mot de passe.
6. Cliquez sur **Terminer**.

   Le message suivant s'affiche :

   ```
   Mise à jour du système terminée.
   ```

Suppression des stratégies de mot de passe

Si vous supprimez une stratégie de mot de passe, les comptes utilisateur qui lui sont associés pourront toujours se connecter, mais l'utilisateur ne sera pas contraint de changer le mot de passe. Si l'utilisateur décide malgré tout de changer le mot de passe, aucune validation ne sera effectuée sur le nouveau mot de passe.

Pourquoi et quand exécuter cette tâche

Pour supprimer une stratégie de mot de passe :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Règles sur les mots de passe**.
2. Recherchez la stratégie de mot de passe que vous souhaitez supprimer en utilisant les options de recherche ou de liste.
3. Cliquez sur **Supprimer** en regard de la stratégie de mot de passe que vous voulez supprimer.
4. Dans la page de confirmation, cliquez sur **Supprimer**.

   Le message suivant s'affiche :

   ```
   Mise à jour du système terminée.
   ```

Modification du nombre de jours d'expiration du mot de passe utilisateur

Le système vous avertit de l'imminence de l'expiration d'un mot de passe en plaçant un message dans la section Alertes système de la page d'accueil de la console d'administration. Les administrateurs système peuvent modifier le nombre de jours précédant l'expiration pour avertir les utilisateurs.

Pourquoi et quand exécuter cette tâche

Le message indique que votre mot de passe expirera dans un nombre spécifique de jours. Chaque jour, le nombre est réduit de un jusqu'à l'expiration du mot de passe, date à laquelle vous êtes invité à modifier le mot de passe.

Les administrateurs système peuvent modifier le nombre de jours précédant l'expiration dans le fichier ui.properties.in. Vous devez apporter toutes les modifications dans le fichier ui.properties.in et non dans le fichier ui.properties. Si vous avez apporté des modifications dans le fichier ui.properties et que vous redémarrez le système, ces modifications seront écrasées par le contenu du fichier ui.properties.in.

Pour modifier le nombre de jours d'expiration d'un mot de passe :

Procédure

1. Arrêtez Sterling B2B Integrator.
2. Accédez au répertoire */rép_install*/install/properties.
3. Ouvrez le fichier ui.properties.in.
4. Recherchez l'entrée MsgPwdExpires= 15.
5. Remplacez la valeur 15 pour le nouveau nombre de jours avant l'expiration du mot de passe de l'utilisateur.
6. Enregistrez le fichier.

7. Accédez au répertoire */rép_install*/install/bin.
8. Entrez **setupfiles.sh**.
9. Redémarrez Sterling B2B Integrator. Les modifications que vous avez effectuées dans le fichier ui.properties.in sont appliquées au fichier ui.properties et sont en vigueur pour tous les comptes utilisateur.

Réinitialisation de votre mot de passe après un verrouillage

Si vous êtes verrouillé, vous pouvez vous connecter à l'aide de n'importe quel autre ordinateur, attendre 30 minutes le temps que le verrouillage arrive à expiration ou contacter l'administrateur système pour qu'il supprime le verrou.

Pourquoi et quand exécuter cette tâche

Si votre compte est verrouillé

- Connectez-vous sur un ordinateur quelconque ayant accès au système.
- Attendez 30 minutes, le temps que le verrouillage arrive à expiration ; vous pourrez ainsi tenter de vous connecter à nouveau sur l'ordinateur verrouillé.
- Contactez l'administrateur système pour qu'il supprime le verrouillage dans la page Gestionnaire de verrouillage. Vous pourrez ainsi tenter de vous connecter à nouveau sur l'ordinateur verrouillé.

Définition des messages d'erreur sur les règles de mot de passe personnalisé

Vous pouvez définir un message d'erreur relatif à une extension de stratégie de mot de passe personnalisée.

Pourquoi et quand exécuter cette tâche

Les messages d'erreur informent l'utilisateur des règles de mot de passe et indiquent les raisons pour lesquelles les changements de mot de passe sont rejetés. Les messages d'erreur sur les mots de passe personnalisés sont définis dans les fichiers Login_*rép_langue*.properties_*IDunique*_ext. Si aucun texte personnalisé n'est fourni, le message d'erreur par défaut est renvoyé à l'utilisateur. Le fichier Login_*rép_langue*.properties_*IDunique*_ext ne fait pas partie du code système par défaut. Il doit être créé après l'installation initiale du système et renseigné afin de correspondre à votre environnement.

Pour définir un message d'erreur relatif à une extension de stratégie de mot de passe personnalisée :

Procédure

1. Accédez au répertoire */rép_install*/install/properties/lang/*rép_langue*. Où *rép_langue* correspond à la langue définie pour l'environnement local du client (par exemple, en, ja, fr).
2. Modifiez le fichier Login_*rép_langue*.properties_*IDunique*_ext. Où rép_langue correspond à la langue définie pour l'environnement local du client et <nom_fichier>, l'identifiant unique de la nouvelle extension de mot de passe personnalisé. Par exemple : Login_en.properties_custompasswd_ext.
3. Ajoutez une entrée au fichier pour la condition d'erreur définie dans le fichier d'extension personnalisé et définissez la chaîne descriptive à renvoyer à l'utilisateur. Par exemple, nogood = Le mot de passe doit contenir au moins une minuscule, une majuscule et un chiffre ou un caractère spécial.

4. Enregistrez et fermez le fichier.

Définition de l'extension de la stratégie de mot de passe personnalisée dans le fichier customer_overrides.property

Vous pouvez spécifier la classe Java qui implémente l'extension de la stratégie de mots de passe.

Pourquoi et quand exécuter cette tâche

Pour connecter l'implémentation personnalisée, le nom de classe Java doit être spécifié dans la propriété passwordPolicyExtensionImpl du fichier customer_overrides.properties.

Pour spécifier la classe Java implémentant l'extension de la stratégie de mot de passe :

Procédure

1. Accédez au répertoire d'installation.
2. Accédez au répertoire de propriétés.
3. Modifiez le fichier customer_overrides.properties.
4. Ajoutez la propriété passwordPolicyExtensionImpl à la fin du fichier et entrez le nom de la classe Java implémentant la validation étendue des mots de passe. Par exemple, security.passwordPolicyExtensionImpl=test.policy.extension.PwdPolExtnImpl.
5. Enregistrez et fermez le fichier.

Ajout du fichier JAR de la classe d'implémentation au chemin d'accès aux classes pour la stratégie de mot de passe personnalisée

Pour une stratégie de mot de passe personnalisée, vous devez ajouter le fichier JAR de la classe d'implémentation au chemin d'accès aux classes.

Pourquoi et quand exécuter cette tâche

La classe d'implémentation de l'extension doit être compilée dans un fichier JAR comme suit :

Procédure

1. Accédez au répertoire *rép_install_SI*.
2. Entrez la commande suivante pour compiler le fichier de classe personnalisé :
   `javac -cp /rép_install_SI/jar/platform_ifcbase/1_3/platform_ifcbase.jar test/policy/extension/*.java`
3. Créez le fichier jar en exécutant la commande suivante depuis *rép_install_SI* :
   `jar cf any_filename.jar chemin_absolu_du_fichier_de_classe_personnalisé.class` où *tout_nom_fichier*`.jar` représente le nom du fichier JAR à créer et *chemin_absolu_du_fichier_de_classe_personnalisé*`.class` représente le nom du fichier de classe Java de l'implémentation personnalisée. Par exemple : `jar cf userExit.jar test/policy/extension/PwdPolExtnImpl.class`
4. Accédez au répertoire *rép_install_SI*/bin.

5. Entrez la commande suivante pour ajouter le fichier jar nouvellement créé au chemin de classes :

   ```
   ./install3rdParty.sh userExit 1_0 -j
   chemin_du_fichier_jar_créé_dans_étape3
   ```

   par exemple, `./install3rdParty.sh userExit 1_0 -j rép_install_SI/userExit.jar`

Authentification LDAP

LDAP comme outil d'authentification pour Sterling B2B Integrator

LDAP (Lightweight Directory Access Protocol) est un ensemble de protocoles utilisé pour accéder aux informations stockées dans un répertoire d'informations appelé annuaire LDAP.

Un annuaire LDAP est une base de données, mais pas une base de données relationnelle, qui permet de gérer des informations réparties entre plusieurs serveurs sur un réseau et qui est optimisé pour les performances de lecture.

LDAP permet de déléguer l'authentification d'un compte utilisateur externe à un annuaire LDAP et de fournir l'authentification en utilisant les mêmes informations de sécurité que pour les autres applications de l'entreprise. Si votre entreprise a déjà adopté LDAP, vous pouvez utiliser vos annuaires LDAP existants.

L'authentification des comptes utilisateur ne requiert pas l'adaptateur LDAP, qui est utilisé avec les processus techniques pour communiquer avec les serveurs LDAP local ou distant à l'aide d'une interface JNDI.

En cas de panne du serveur LDAP, les titulaires de comptes internes conservent l'accès, contrairement aux titulaires de comptes externes qui doivent attendre que le serveur LDAP fonctionne à nouveau.

Avant de pouvoir configurer LDAP avec Sterling B2B Integrator, vous devez :

- Avoir des connaissances sur LDAP
- Disposer d'un accès à un serveur LDAP installé et configuré contenant les informations utilisateur
- Connaître l'emplacement du serveur LDAP
- (Pour SSL) Avoir installé des certificats de sécurité dans le fichier de clés et le fichier de clés certifiées
- Avoir créé des comptes utilisateur externes pour chaque utilisateur qui s'authentifiera via votre serveur LDAP
- (Pour SSL) Connaître l'emplacement du fichier de clés et du fichier de clés certifiées

Exemple : Paramètres de configuration de l'authentification LDAP

Cet exemple illustre les paramètres de configuration de l'authentification LDAP .

L'exemple suivant illustre les paramètres de configuration de l'authentification LDAP :

```
## Configuration de l'authentification GIS/LDAP
## propriétés système java (jsse) ssl facultatives pour la localisation et l'utilisation
## du fichier de clés et du fichier de clés certifiées
## un seul ensemble de propriétés des fichiers de clés et de clés certifiées pour la configuration
# LDAP_SECURITY_TRUSTSTORE=/home/applications/properties/cacerts
# LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit
# LDAP_SECURITY_KEYSTORE=/home/applications/properties/keystore
# LDAP_SECURITY_KEYSTORE_PASSWORD=password
#########################################################################
#
# Configuration de l'authentification GIS
#
#########################################################################
authentication_0.className=com.sterlingcommerce.woodstock.security
.GISAuthentication
authentication_0.display_name=GIS Authentication
#########################################################################
#
# Pour étendre la configuration de l'authentification du serveur LDAP,
# copiez-collez l'ensemble de propriétés suivant et décommentez toutes les propriétés
# commençant par "authentication_<number>". Indiquez dans la balise <number>
# un nombre incrémenté pour la nouvelle méthode d'authentification. Par exemple :
# si la dernière méthode d'authentification est "authentication_0", indiquez dans
# la balise <number> le nombre "1" pour désigner la nouvelle méthode d'authentification LDAP
# suivante.
# Ensuite, modifiez chaque propriété en indiquant les informations de serveur LDAP correctes.
#
# Vous pouvez mettre en commentaire ou ne pas renseigner la propriété
# "authentication_<number>.security_protocol"
# si vous n'avez pas l'intention d'utiliser le protocole de sécurité SSL.
#
# La propriété d'authentification LDAP authentication_1 doit être remplacée si
# le client a déjà utilisé l'authentification LDAP qui a été configurée dans
# le fichier security.properties.
#
#########################################################################
#########################################################################
#
# Configuration de l'authentification du serveur LDAP <number>
#
#########################################################################
# authentication_<number>.className=com.sterlingcommerce.woodstock.security
# .LDAPAuthentication
# authentication_<number>.display_name=LDAP Serveragrona <number>
## enable ldap authentication (true, false) default=false
# authentication_<number>.enabled=true
## jndi parameters for ldap connections
# authentication_<number>.jndi_factory=com.sun.jndi.ldap.LdapCtxFactory
# authentication_<number>.server=acme.inc.com
# authentication_<number>.port=636
# authentication_<number>.security_type=simple
# authentication_<number>.principle=cn=Manager,dc=acme,dc=inc,dc=com
# authentication_<number>.credentials=SecretPassword
## mettez en commentaires ou laissez cette propriété vide si le serveur n'utilise pas
## SSL pour le protocole de sécurité.
# authentication_<number>.security_protocol=ssl
## search parameters for user password
# authentication_<number>.password_attribute=userPassword
# authentication_<number>.search_root=dc=acme,dc=inc,dc=com
# authentication_<number>.search_filter=(uid=<userid>)
# authentication_<number>.with_user_bind=falseBelow the ##LDAP Authentication
```

Liste de contrôle de configuration de l'authentification LDAP

Vous pouvez configurer LDAP avec Sterling B2B Integrator.

Cette liste de contrôle permet de configurer LDAP avec Sterling B2B Integrator :

Tâches	Liste de contrôle de configuration LDAP
1	Configurer LDAP dans l'un des modes suivants : • Mode comparaison de mot de passe • Mode binaire de mot de passe
2	Configurer LDAP avec Sterling B2B Integrator
3	Vérifier la configuration LDAP
4	Facultatif. Chiffrer des mots de passe LDAP.

Configuration LDAP en mode liaisons de mot de passe

Vous pouvez configurer LDAP en mode liaisons de mot de passe en entrant l'**ID utilisateur** et le **mot de passe** de votre compte utilisateur externe.

Pourquoi et quand exécuter cette tâche

Pour configurer LDAP en mode liaisons de mot de passe :

Procédure

Entrez l'**ID utilisateur** et le **mot de passe** de votre compte utilisateur externe. Le système :

- Tente d'effectuer une liaison au référentiel LDAP à l'aide des données d'identification permettant l'exécution des requêtes nécessaires.
- Recherche l'utilisateur dans l'annuaire LDAP à l'aide de l'ID utilisateur approprié.
- Extrait le nom distinctif (DN) de l'utilisateur à partir de l'annuaire LDAP.
- Tente d'effectuer une liaison au référentiel LDAP à l'aide du nom distinctif et du mot de passe de l'utilisateur.
- Succès - Le système se connecte au référentiel LDAP en tant qu'utilisateur.
- Echec - Le système ne parvient pas à se connecter au référentiel LDAP en tant qu'utilisateur.

Configuration LDAP en mode comparaison de mot de passe

Vous pouvez configurer LDAP en mode comparaison de mot de passe.

Pourquoi et quand exécuter cette tâche

Pour configurer LDAP en mode comparaison de mot de passe :

Procédure

1. Entrez l'**ID utilisateur** et le **mot de passe** de votre compte utilisateur externe.
2. Le système tente d'effectuer une liaison au référentiel LDAP à l'aide des données d'identification permettant l'exécution des requêtes nécessaires.
3. Le système recherche l'utilisateur dans l'annuaire LDAP à l'aide de l'ID utilisateur approprié.
4. Le système extrait le mot de passe de l'utilisateur de l'annuaire LDAP.
5. Le système compare le mot de passe fourni par l'utilisateur avec le mot de passe extrait de l'annuaire LDAP. Si les mots de passe correspondent, vous êtes

authentifié et autorisé à accéder au système. Si les mots de passe ne correspondent pas, vous n'êtes pas authentifié et l'accès au système vous est refusé.

Configuration LDAP avec Sterling B2B Integrator

Pour configurer Sterling B2B Integrator afin d'utiliser LDAP, vous devez éditer le fichier authentication_policy.properties.in. Vous pouvez également utiliser le fichier customer_overrides.properties pour définir les valeurs des propriétés qui ne peuvent pas être écrasées par une installation de correctif.

Pourquoi et quand exécuter cette tâche

Pour configurer l'authentification LDAP :

Procédure

1. Arrêtez Sterling B2B Integrator.
2. Accédez au répertoire d'installation.
3. Accédez au répertoire de propriétés.
4. Ouvrez le fichier authentication_policy.properties.in.
5. Dans le fichier authentication_policy.properties.in, recherchez l'entrée de configuration ## Authentification GIS/LDAP.
6. Sous l'entrée de configuration ## Authentification GIS/LDAP, apportez les modifications suivantes aux paramètres LDAP :

Paramètre	Description	Valeur fournie	À remplacer par
#LDAP_SECURITY_ TRUSTSTORE	Chemin d'accès au fichier de clés certifiées local. Ce fichier doit contenir les certificats LDAP requis. Vous ne pouvez pas utiliser les certificats des partenaires commerciaux. Facultatif. Ce paramètre est valide avec SSL seulement.	Chemin d'accès inactif	Chemin d'accès complet au fichier de clés certifiées local.
#LDAP_SECURITY_ TRUSTSTORE_ PASSWORD	Mot de passe permettant l'accès au fichier de clés certifiées. Facultatif. Ce paramètre est valide avec SSL seulement.	changeit	Mot de passe permettant l'accès au fichier de clés certifiées local.
#LDAP_SECURITY_ KEYSTORE	Chemin d'accès au fichier de clés local. Ce fichier doit contenir les certificats LDAP requis. Vous ne pouvez pas utiliser les certificats des partenaires commerciaux. Facultatif. Ce paramètre est valide avec SSL seulement.	Chemin d'accès inactif	Chemin d'accès complet au fichier de clés local.
#LDAP_SECURITY_ KEYSTORE_ PASSWORD	Mot de passe permettant l'accès au fichier de clés. Facultatif. Ce paramètre est valide avec SSL seulement.	password	Mot de passe permettant l'accès au fichier de clés local.

Paramètre	Description	Valeur fournie	À remplacer par
#authentication_ <number>. enabled	Active ou désactive l'utilisation de LDAP. Faux : tous les utilisateurs créés à partir de cet hôte d'authentification seront désactivés (échec de la connexion). Vrai : chaque utilisateur est accessible soit en interne, soit en externe, mais pas les deux, puisque chaque ID utilisateur est unique. Cette valeur n'est pas vérifiée dans le cas d'une authentification interne.	Faux	Vrai
#authentication_<number> .jndi_factory	Nom de classe de la classe de fabrique qui crée le contexte initial pour le fournisseur de services LDAP. Il s'agit de la fabrique de contexte standard fournie avec le kit JDK.	com.sun. jndi.ldap. LdapCtx Factory	Aucune modification
#authentication_ <number>.server	URL spécifiant le nom d'hôte du serveur LDAP.	Chemin d'accès inactif	URL de l'hôte LDAP local.
#authentication_ <number>.port	Numéro de port du serveur LDAP.		
#authentication_ <number>. security_type	Méthode d'authentification que le fournisseur doit utiliser. Le système ne prend en charge que l'authentification unique.	simple	Aucune modification
#authentication_ <number>. principle	Identité du composant principal à authentifier, qui permet au système d'exécuter les demandes. Ce paramètre désigne le nom du composant dans une demande de liaison LDAP ASN.1.	cn=Manager, dc=amr, dc=stercomm, dc=com	Informations de nommage locales.
#authentication_ <number>. credentials	Configuration de mot de passe dans le référentiel LDAP pour le composant LDAP principal, qui permet au système d'exécuter les demandes.	SecretPassword	Mot de passe local associé à votre composant principal local.
#authentication_ <number>. security_protocol	Objet spécifiant le protocole de sécurité que le fournisseur doit utiliser.	SSL	Aucune modification. Ce paramètre ne s'affiche pas si vous avez choisi de ne pas utiliser SSL.

Paramètre	Description	Valeur fournie	À remplacer par
#authentication_ <number>. password_attribute	Nom de l'attribut LDAP qui contient le mot de passe de l'utilisateur. Ce paramètre n'est utilisé que si le paramètre #LDAP_ AUTHENTICATE_ WITH_USER_BIND est défini su faux.	userPassword	Attribut local contenant le mot de passe.
#authentication_ <number>. search_root	Objet spécifiant la racine sur laquelle repose la demande de l'utilisateur.	dc=amr, dc=stercomm, dc=com	Chemin de recherche local.
#authentication_ <number>.search_filter	Objet spécifiant le modèle à utiliser dans la recherche. La valeur <userid> est remplacée de manière dynamique, lors de la demande, par l'ID utilisateur de l'utilisateur demandant l'authentification.	(uid=<userid>)	Un serveur Windows Active Directory peut utiliser une entrée telle que (sAMAccount Name=<userid>)
#authentication_ <number>. with_user_bind	Indique si un utilisateur est authentifié en fonction d'une liaison réussie. Faux : le système extrait la valeur du mot de passe de l'utilisateur du serveur LDAP et effectue une comparaison avec les données d'identification de l'utilisateur fournies. Vrai : le système établit une liaison avec le serveur LDAP à l'aide du nom distinctif de l'utilisateur et des données d'identification fournies. Une liaison réussie signifie également la réussite de l'authentification.	faux	Remplacez cette valeur par Vrai si vous souhaitez que l'authentification soit effectuée en fonction de la liaison de l'utilisateur.

7. Enregistrez le fichier authentication_policy.properties.in.
8. Entrez */rép_install*/install/bin/setupfiles.sh (UNIX) ou *rép_install*\install\bin\ setupfiles.cmd (Windows) pour mettre à jour des entrées LDAP dans le fichier authentication_policy.properties à partir du fichier authentication_policy.properties.in.
9. Lancez Sterling B2B Integrator.

   Les modifications apportées au fichier authentication_policy.properties sont appliquées et vous pouvez maintenant commencer à utiliser votre serveur LDAP pour authentifier les utilisateurs.

Après le démarrage, le système identifiera les serveurs LDAP à partir du fichier authentication_policy.properties. Il authentifiera les utilisateurs externes lorsqu'ils se connecteront.

Vérification de la configuration LDAP

Pour vérifier que vous avez configuré le protocole LDAP correctement avec Sterling B2B Integrator, consultez le fichier Authentication.log, sous Authentification utilisateur, pour vous assurer que le système a accepté la configuration LDAP.

Pourquoi et quand exécuter cette tâche

Si vous rencontrez des problèmes lors de la connexion à l'annuaire LDAP ou que l'authentification LDAP échoue, vérifiez les instructions de consignation DEBUG dans le fichier Authentication.log pour identifier et résoudre l'incident. Le fichier Authentication.log enregistre toutes les tentatives de connexion, réussies ou non.

Chiffrement des mots de passe LDAP

Vous pouvez masquer les mots de passe LDAP liés des fichiers de propriétés en les chiffrant dans le fichier customer_overrides.property.

Pourquoi et quand exécuter cette tâche

Les paramètres (ou les propriétés) ci-après permettent de chiffrer les mots de passe LDAP dans le fichier customer_overrides.properties :

Paramètre/propriété	Description
authentication_policy.authentication _1.credentials	Ce paramètre ou cette propriété régit le mot de passe principal nécessaire pour accéder à une instance LDAP. Ce processus doit être sécurisé car les mots de passe régissant la sécurité et l'accès ne doivent pas être exposés en texte brut.
authentication_policy. LDAP_SECURITY_ TRUSTSTORE_PASSWORD	Ce paramètre ou cette propriété régit le mot de passe du fichier de clés certifiées (au format JKS) utilisé pour la sécurisation des connexions LDAP. La phrase passe utilisée pour ce fichier JKS doit être indiquée pour que le fichier de clés certifiées puisse être accessible (il s'agit d'un fichier chiffré).
authentication_policy. LDAP_SECURITY_KEYSTORE_PASSWORD	Ce paramètre ou cette propriété régit le mot de passe si l'authentification SSL basée sur le client est utilisée pour sécuriser les connexions à une instance LDAP donnée.

Pour chiffrer des mots de passe LDAP :

Procédure

1. Accédez au répertoire bin.
2. Utilisez le paramètre encrypt_string.[sh/cmd] pour déterminer la valeur réelle de la propriété ou des paramètres que vous voulez chiffrer.
3. Mettez à jour les paramètres/propriétés dans le fichier customer_overrides.properties pour obtenir les entrées suivantes. Remplacez

toutes les variables <ENCVAL> par la valeur chiffrée de la chaîne non chiffrée en commentaire pour cette propriété à l'aide de bin/encrypt_string.sh (ou de .cmd). Par exemple :

```
authentication_policy.LDAP_SECURITY_TRUSTSTORE=&INSTALL_DIR;/../
woodstock2/com/sterlingcommerce/woodstock/security/units/cacerts
# non-encrypted
#authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit
# encrypted
authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD=<ENCVAL>
authentication_policy.LDAP_SECURITY_KEYSTORE=&INSTALL_DIR;/../woodstock2/
com/sterlingcommerce/woodstock/security/units/keystore
# non-encrypted
#authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD=password
# encrypted
authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD=<ENCVAL>
authentication_policy.authentication_2.display_name=LDAP Server agrona 2
authentication_policy.authentication_2.enabled=true
authentication_policy.authentication_2.jndi_factory=com.sun.jndi.ldap.LdapCtxFactory
authentication_policy.authentication_2.server=agrona.sci.local
authentication_policy.authentication_2.port=18100
authentication_policy.authentication_2.security_type=simple
authentication_policy.authentication_2.principle=cn=Manager,dc=amr,dc=stercomm,dc=com
# non-encrypted
#authentication_policy.authentication_2.credentials=Sterling
# encrypted
authentication_policy.authentication_2.credentials=<ENCVAL>
authentication_policy.authentication_2.security_protocol=ssl
authentication_policy.authentication_2.password_attribute=userPassword
authentication_policy.authentication_2.search_root=dc=amr,dc=stercomm,dc=com
authentication_policy.authentication_2.search_filter=(uid=<userid>)
authentication_policy.authentication_2.with_user_bind=false
authentication_policy.authentication_2.className=com.sterlingcommerce.woodstock.security
.LDAPAuthentication
```

Actualités utilisateur

Actualités utilisateur

Actualités utilisateur

La fonction Actualités utilisateur vous permet de publier des messages dans les pages d'accueil de la console d'administration. Cette fonction permet d'informer les utilisateurs sur les modifications apportées aux événements et tâches importants ou de les leur rappeler.

Les messages peuvent être postés pour :

- Tous les utilisateurs
- Un utilisateur spécifique
- Plusieurs utilisateurs

La nouvelle information est affichée en fonction d'une date d'effet et d'une date d'expiration. Vous pouvez également configurer le message en tant que :

Type de message	Symbole	Description
Notification		Fournit des informations d'annonce de portée générale et de faible importance.
Alerte		Fournit des informations d'annonce de grande importance.

Vous devez détenir des droits d'accès en écriture sur les comptes pour créer des messages Actualités utilisateur. La suppression des anciens messages réduit les besoins en stockage et la quantité d'efforts requise pour récupérer des messages spécifiques.

Les tâches de la fonction Actualités utilisateur sont notamment les suivantes :

- Création d'un message Actualités utilisateur pour des utilisateurs spécifiques
- Création d'un message Actualités utilisateur pour tous les utilisateurs
- Recherche d'un message Actualités utilisateur
- Modification d'un message Actualités utilisateur
- Suppression d'un message Actualités utilisateur

Création des messages d'informations utilisateur pour tous les utilisateurs

Vous pouvez créer des messages d'informations utilisateur pour tous les utilisateurs du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Avant de commencer, vous devez connaître les informations suivantes :

Zone	Description
Type	Type du message que vous créez. Les valeurs admises sont Notification et Alerte.
Objet	Objet du message que vous créez.
Message	Corps du message que vous créez.

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Informations utilisateur**.
2. En regard de **Nouveau message**, cliquez sur **OK**.
3. Entrez le **Type**.
4. Entrez l'**Objet**.
5. Entrez le **Message**.
6. Cliquez sur **Suivant**.
7. Sélectionnez **TOUS les utilisateurs** et cliquez sur **Suivant**.
8. Entrez la **Date d'effet** du message (aaaa-mm-jj).
9. Entrez la **Date d'expiration** du message (aaaa-mm-jj).
10. Cliquez sur **Suivant**.
11. Vérifiez les Paramètres de message d'informations.
12. Cliquez sur **Terminer**.

Création des messages d'informations utilisateur pour des utilisateurs spécifiques

Vous pouvez créer des messages d'informations utilisateur pour les utilisateurs spécifiques du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Avant de commencer, vous devez connaître les informations suivantes :

Zone	Description
Type	Type du message que vous créez. Les valeurs admises sont Notification et Alerte.
Objet	Objet du message que vous créez.
Message	Corps du message que vous créez.

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Informations utilisateur**.
2. En regard de **Nouveau message**, cliquez sur **OK**.
3. Entrez le **Type**.
4. Entrez l'**Objet**.
5. Entrez le **Message**.
6. Cliquez sur **Suivant**.
7. Sélectionnez **Utilisateurs sélectionnés**.
8. Sélectionnez le nom de chaque utilisateur qui doit recevoir ce message.
9. Cliquez sur **Suivant**.
10. Entrez la **Date d'effet** du message (aaaa-mm-jj).
11. Entrez la **Date d'expiration** du message (aaaa-mm-jj).
12. Cliquez sur **Suivant**.
13. Vérifiez les Paramètres de message d'informations.
14. Cliquez sur **Terminer**.

Recherche des messages Actualités utilisateur

Vous pouvez rechercher un message d'actualités utilisateur à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour rechercher un message Actualités utilisateur, procédez comme suit :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Informations utilisateur**.
2. Utilisez l'une des options de recherche suivantes :

Options de recherche des Actualités utilisateur	Action
par ID utilisateur	Sélectionnez soit la valeur TOUT, soit l'utilisateur spécifique dans la liste.
par objet	Entrez une partie du texte du message.
par plage de dates effective	Entrez la plage de dates (mm/jj/aaaa).

3. Cliquez sur **OK** La page Actualités utilisateur répertorie tous les messages correspondant à vos critères de recherche.

Édition des messages d'informations utilisateur

Vous pouvez éditer un message d'informations utilisateur à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour éditer un message d'informations utilisateur :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Informations utilisateur**.
2. Recherchez le message d'informations utilisateur que vous souhaitez éditer.
3. Cliquez sur Modifier pour éditer le message d'informations utilisateur souhaité.
4. Mettez à jour le type du message, l'objet ou le message, si nécessaire.
5. Cliquez sur **Suivant**.
6. Mettez à jour les utilisateurs qui recevront ce message, si nécessaire, et cliquez sur **Suivant**.
7. Mettez à jour la **Date d'effet** du message (aaaa-mm-jj), si nécessaire.
8. Mettez à jour la **Date d'expiration** du message (aaaa-mm-jj), si nécessaire.
9. Cliquez sur **Suivant**.
10. Vérifiez les Paramètres de message d'informations.
11. Cliquez sur **Terminer**.

Suppression des messages d'informations utilisateur

Vous pouvez supprimer un message d'informations utilisateur à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour supprimer un message d'informations utilisateur :

Procédure

1. Dans le menu **Administration**, sélectionnez **Comptes** > **Informations utilisateur**.
2. Recherchez le message d'informations utilisateur que vous souhaitez supprimer.
3. Cliquez sur **Supprimer** en regard du message d'informations utilisateur que vous voulez supprimer.
4. Vérifiez les Paramètres de message d'informations.
5. Cliquez sur **Supprimer**. Le message suivant s'affiche :

   ```
   Mise à jour du système terminée.
   ```

Chiffrement de document

Présentation de la fonction de chiffrement de documents

Le chiffrement de documents est une fonction fournie avec Sterling B2B Integrator qui configure une couche de sécurité supplémentaire qui étend les droits d'accès aux bases de données et aux fichiers traditionnels. Si intégrez Sterling File Gateway avec Sterling B2B Integrator, la même fonction de chiffrement de documents est utilisée pour protéger les données inactives.

Sterling File Gateway est une application de transfert sécurisé de fichiers entre des partenaires utilisant plusieurs protocoles, conventions d'attribution de nom de fichier et formats de fichier.

La fonction de chiffrement de documents est destinée à protéger les données inactives de la surveillance de trafic. Elle permet de chiffrer les données utiles stockées dans la base de données et/ou le système de fichiers, mais aussi d'empêcher toute personne située à l'extérieur du système de visualiser les données utiles en accédant directement à la base de données ou au système de fichiers.

Voici quelques aspects importants du chiffrement de documents :

- La configuration par défaut ne prévoit aucun chiffrement lors de l'installation. Si vous voulez que vos documents soient chiffrés, vous devrez activer cette fonction.
- Vous pouvez activer cette fonction à tout moment, mais seuls les documents reçus après l'activation du chiffrement sont chiffrés.
- Une fois que cette fonction est activée, le chiffrement s'applique à toutes les charges de l'ensemble du système.
- Seules les données utiles du document sont chiffrées, **pas** les métadonnées.
- La même clé de chiffrement est utilisée pour le chiffrement et le déchiffrement.
- Le système utilise un certificat prédéfini (doccrypto) pour le chiffrement de documents. Vous avez la possibilité de créer un autre certificat de système. Dans ce cas, vous devez mettre à jour la valeur de CERT_NAME dans le fichier customer_overrides.properties.

Si l'impact sur les performances est réel lorsque le chiffrement est activé, celui-ci sera différent sur chaque client selon le matériel utilisé, le nombre et la taille des documents en cours de traitement, et selon le temps de traitement relatif consacré par un serveur donné à l'archivage et à l'extraction de documents par rapport à d'autres activités.

Clé de chiffrement pour le chiffrement de documents

La même clé de chiffrement est utilisée pour chiffrer et déchiffrer des documents du système de fichiers ou de la base de données. Le certificat numérique est utilisé pour générer et chiffrer les clés, alors que la phrase passe du système est utilisée pour chiffrer les certificats numériques.

Le chiffrement de documents crée une clé par document, stockée avec le document comme métadonnées. Les certificats numériques sont stockés comme n'importe quel autre certificat de système.

Le système utilise un certificat prédéfini (doccrypto) pour générer et chiffrer les clés utilisées pour le chiffrement du document. Vous avez la possibilité de créer un autre certificat de système. Dans ce cas, vous devez mettre à jour la valeur de CERT_NAME dans le fichier customer_overrides.properties.

Affectation d'un autre certificat pour le chiffrement de documents

Le système utilise un certificat prédéfini (doccrypto) pour le chiffrement de documents. Vous avez la possibilité de créer un autre certificat de système à utiliser pour chiffrer les documents, par exemple si le certificat précédent a expiré. Dans ce cas, vous devez mettre à jour la valeur de CERT_NAME dans le fichier customer_overrides.properties.

Pourquoi et quand exécuter cette tâche

ATTENTION : Ne supprimez pas et ne renommez pas le certificat de système précédent. Vous avez besoin du certificat précédent pour déchiffer les documents chiffrés par ce certificat. Votre nouveau certificat de système ne peut pas déchiffrer ces documents, car il n'a pas servi à les chiffrer.

Avant d'exécuter cette procédure, vous devez :

- Générer le nouveau certificat.
- Connaître le nom du certificat.

Pour mettre à jour la valeur de CERT_NAME :

Procédure

1. Accédez au répertoire d'installation.
2. Accédez au répertoire de propriétés.
3. Ouvrez le fichier customer_overrides.properties.
4. Ajoutez la ligne suivante au fichier :
   `security.CERT_NAME=nom_du_nouveau_certificat_de_système`
5. Enregistrez et fermez le fichier customer_overrides.properties.
6. Arrêtez et redémarrez Sterling B2B Integrator.

Activation du chiffrement des documents de base de données et de système de fichiers

Vous pouvez chiffrer des documents de base de données et de système de fichiers à partir du répertoire de propriétés.

Pourquoi et quand exécuter cette tâche

Pour chiffrer les documents de base de données et de système de fichiers :

Procédure

1. Accédez au répertoire d'installation.
2. Accédez au répertoire de propriétés.
3. Ouvrez le fichier customer_overrides.properties.
4. Ajoutez la ligne suivante :
   `security.ENC_DECR_DOCS=ENC_ALL`
5. Enregistrez et fermez le fichier customer_overrides.properties.
6. Arrêtez et redémarrez Sterling B2B Integrator.

Activation du chiffrement des documents de base de données

Vous pouvez chiffrer des documents de base de données à partir du répertoire d'installation.

Pourquoi et quand exécuter cette tâche

Pour chiffrer les documents de base de données :

Procédure

1. Accédez au répertoire d'installation.
2. Accédez au répertoire de propriétés.
3. Ouvrez le fichier customer_overrides.properties.
4. Ajoutez la ligne suivante :
   `security.ENC_DECR_DOCS=ENC_DB`
5. Enregistrez et fermez le fichier customer_overrides.properties.
6. Arrêtez et redémarrez Sterling B2B Integrator.

Activation du chiffrement des documents de système de fichiers

Vous pouvez chiffrer des documents de système de fichiers à partir du répertoire d'installation.

Pourquoi et quand exécuter cette tâche

Pour chiffrer les documents de système de fichiers :

Procédure

1. Accédez au répertoire d'installation.
2. Accédez au répertoire de propriétés.
3. Ouvrez le fichier customer_overrides.properties.
4. Ajoutez la ligne suivante :
   `security.ENC_DECR_DOCS=ENC_FS`
5. Enregistrez et fermez le fichier customer_overrides.properties.
6. Arrêtez et redémarrez Sterling B2B Integrator.

Désactivation du chiffrement de document

Vous pouvez désactiver le chiffrement de document à partir du répertoire de propriétés.

Pourquoi et quand exécuter cette tâche

La configuration par défaut ne prévoit aucun chiffrement lors de l'installation.

Pour désactiver le chiffrement de document :

Procédure

1. Accédez au répertoire d'installation.
2. Accédez au répertoire de propriétés.
3. Ouvrez le fichier customer_overrides.properties.
4. Attribuez à la propriété ENC_DECR_DOCS la valeur NONE. Par exemple :
   `security.ENC_DECR_DOCS=NONE`
5. Enregistrez et fermez le fichier customer_overrides.properties.
6. Arrêtez et redémarrez Sterling B2B Integrator.

Certificats

Certificats numériques

Utilisez IBM Key Management Utility (iKeyman) pour vous aider à gérer vos certificats numériques.

Le système utilise les types de certificats numériques suivants :

- Certificats d'autorité de certification et de confiance : certificats numériques pour lesquels le système ne dispose pas de clés privées. Ces certificats sont stockés au format DER standard.
- Certificats de système : certificat numérique pour lequel la clé privée est conservée dans le système. Ces certificats sont stockés avec la clé privée dans un format sécurisé.

Voici quelques informations élémentaires concernant la manière dont les certificats numériques sont utilisés :

- Chaque organisation échangeant des documents sécurisés doit disposer d'un certificat. Générez le certificat à l'aide d'iKeyman ou en externe. Pour plus d'informations sur iKeyman, voir «IBM Key Management Utility (iKeyman)», à la page 65.
- Chaque profil commercial d'un partenaire avec lequel vous échangez des documents signés et chiffrés doit disposer d'un certificat.
- Un profil d'organisation ou commercial ne peut disposer que d'un seul certificat actif à la fois. Dans le cas de certificats doubles, une organisation peut disposer d'une paire de certificats active ; une pour la signature, une pour le chiffrement.
- Un profil d'organisation ou commercial doit disposer d'un certificat actif pour échanger correctement des documents signés et chiffrés.
- Un profil d'organisation ou commercial peut comporter plusieurs certificats valides.
- Les certificats peuvent être utilisés pour signer les documents que vous transmettez par tout mode de transport.
- La longueur de clé d'un certificat n'a pas besoin d'être identique à celle d'un certificat de partenaire commercial.
- Avant de définir la période de validité du certificat, il est recommandé de lire et d'appliquer les meilleures pratiques d'utilisation contenues dans Microsoft PKI Quick Guide. Pour plus d'informations concernant les recommandations de meilleures pratiques d'utilisation de ces certificats, consultez http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part3.html.

Certificats numériques pris en charge

Sterling B2B Integrator prend en charge la version 3 X.509 des certificats numériques. Ces certificats peuvent être autosignés ou signés par une autorité de certification.

- Un certificat autosigné est un certificat numérique qui est signé avec la clé privée correspondant à la clé publique du certificat, prouvant ainsi que l'émetteur possède la clé privée correspondant à la clé publique du certificat.
- Un certificat signé par une autorité de certification est un certificat numérique qui est signé avec des clés gérées par les autorités de certification. Avant d'émettre un certificat, l'autorité de certification renvoie généralement un demandeur pour déterminer si le demandeur est bien le titulaire du certificat référencé dans le certificat.

Certificats d'autorité de certification

Un certificat d'autorité de certification est un certificat numérique émis par une autorité de certification. L'autorité de certification vérifie les certificats racines de confiance, lesquels constituent le socle sur lequel sont créées les chaînes dignes de confiance dans les certificats.

L'accréditation d'une autorité de certification racine signifie que vous faites confiance à tous les certificats émis par cette autorité. Si vous choisissez de ne pas approuver une autorité de certification racine, Sterling B2B Integrator ne fera confiance à aucun certificat émis par cette autorité.

Les certificats d'autorité de certification doivent contenir une clé publique correspondant à une clé privée. L'autorité de certification détient la clé privée et l'utilise pour signer les certificats qu'elle émet. Pour valider un certificat accrédité, vous devez d'abord restituer un certificat de l'autorité de certification.

Les certificats racine émis par les autorités de certification courantes sont contenus dans un fichier de clés Java (JKS) qui se trouve dans la machine JVM fournie avec Sterling B2B Integrator. Les utilisateurs peuvent ainsi établir des relations de confiance basées sur des droits plus facilement que s'ils avaient dû rechercher et obtenir les certificats à partir du site Web de l'autorité de certification.

Les certificats de l'autorité de certification sont stockés séparément des certificats accrédités dans le produit.

Dans l'interface utilisateur, vous pouvez archiver les certificats racines d'autorité de certification qui proviennent de l'une des sources suivantes :

- Les certificats racines d'autorité de certification courants fournis avec Sterling B2B Integrator dans le fichier de clés JKS.
- Seuls les certificats et les certificats accrédités sont reconnus. Les certificats et les clés privées ne sont pas visibles dans l'interface utilisateur.
- Les certificats SSL importés des partenaires commerciaux.
- D'autres certificats obtenus en externe.

En fonction des règles de sécurité en vigueur sur votre site, des certificats d'autorité de certification du fichier de clés Java (JKS) peuvent également être restitués par le biais de la console. Les certificats d'autorité de certification sont des documents publics mais vous devez choisir avec soin les personnes habilitées à les ajouter. Une personne malveillante pourrait ajouter un faux certificat d'autorité de certification afin de vérifier des faux certificats d'utilisateur final.

Noms des certificats d'autorité de certification

Le nom du certificat d'autorité de certification ne fait pas partie du contenu du certificat. Il est généré à partir du nom distinctif relatif de l'émetteur et du numéro de série du certificat. Toutefois, les certificats provenant du fichier de clés JKS sont nommés avec une chaîne arbitraire.

Etant donné que le nom du certificat est stocké dans la base de données du système et qu'il est utilisé comme alias pour désigner le certificat dans l'interface graphique, vous souhaiterez peut-être renommer des certificats d'autorité de certification en leur attribuant des noms plus courts ou plus évocateurs basés sur les conventions de dénomination de votre fichier. Les certificats peuvent être renommés lorsqu'ils sont archivés ou édités.

Avantages des certificats numériques autosignés et signés par des autorités de certification

Selon vos besoins, les certificats numériques autosignés et signés par des autorités de certification présentent des avantages et des inconvénients.

Lorsque vous et vos partenaires commerciaux devez choisir si vous allez générer un certificat autosigné ou acquérir un certificat signé auprès d'une autorité de certification, tenez compte des éléments suivants :

- Vous pouvez facilement créer des certificats autosignés à l'aide de Sterling B2B Integrator. Toutefois, ces certificats ne seront pas vérifiés par un tiers digne de confiance.
- Le principal avantage de l'utilisation des certificats émis par une autorité de certification est que l'identité du détenteur du certificat est vérifiée par un tiers digne de confiance. Ses inconvénients sont, en revanche, un surcoût et des tâches administratives supplémentaires. Si vous décidez d'utiliser un certificat tiers, obtenez-le auprès d'une autorité de certification.
- Une autorité de certification propose une source centralisée concernant la publication et l'obtention d'informations sur les certificats, notamment des informations relatives aux certificats révoqués.

Par défaut, le système accepte tous les certificats des autorités de certification et les certificats autosignés générés par l'application. Vous pouvez toutefois préciser si tous les certificats émis par une autorité de certification spécifique, ou certains d'entre eux seulement, sont dignes de confiance. En outre, vous ne pouvez pas faire confiance à un certificat autosigné d'un partenaire commercial de manière explicite.

Dates d'expiration des certificats

Si un adaptateur et un servlet sont utilisés pour les communications entrantes, vous devez surveiller les dates d'expiration des certificats de système afin de vous assurer que les certificats sont valides. Les certificats doivent être remplacés par des certificats valides avant d'arriver à expiration.

Définition des paramètres des certificats de système

Si un adaptateur et un servlet sont utilisés pour les communications entrantes, vous devez surveiller les dates d'expiration des certificats de système afin de vous assurer que les certificats sont valides. Les certificats doivent être remplacés par des certificats valides avant d'arriver à expiration.

Paramètre	Description
alias	Nom de clé stocké dans le module HSM. Seuls les noms d'alias comprenant les caractères a-z, A-Z, 0-9 ou le tiret (-) et dont la longueur totale ne dépasse la longueur du GUID du système sont autorisés.
certname	Nom à affecter au certificat de système dans la base de données.
Certtype	Type du certificat à importer. Quatre types de fichiers certificat sont pris en charge : pkcs12, pkcs8, pem et keystore. Sterling B2B Integrator prend uniquement en charge les clés pem chiffrés avec DES ou 3DES. Utilisez keystore pour répertorier ou importer le fichier de clés.
file	Nom du fichier à importer.

Paramètre	Description
keypass	Code confidentiel de l'emplacement sur le périphérique Eracom.
keystoretype	Type du fichier de clés à importer. La valeur valide est CRYPTOKI.
keystoreprovider	Type du fournisseur. Eracom est le seul type de fournisseur pris en charge par HSM. Les valeurs valides sont les suivantes : • ERACOM • ERACOM.n (si vous importez des certificats vers un emplacement autre que la première position)
password	Phrase passe du magasin pour le fichier certificat.
pkcs12file	Nom du fichier PKCS12 à importer.
pkcs12storepass	Phrase passe du magasin utilisé pour la génération du fichier PKCS12.
pkcs12keypass	Phrase passe valide pour le fichier PKCS12.
storepass	Code confidentiel de l'emplacement sur le périphérique Eracom où réside le fichier de clés.
systempass	Phrase passe du système.

IBM Key Management Utility (iKeyman)

IBM Key Management Utility (iKeyman) est un composant d'IBM SDK qui génère des clés, des demandes de certification et des certificats auto-signés.

Vous pouvez utiliser iKeyman pour créer des certificats pour sécuriser les communications et chiffrer et déchiffrer des données. Lors d'un transfert sécurisé à l'aide de SSL, les certificats offrent un niveau de sécurité supplémentaire.

Dans Sterling B2B Integrator, vous pouvez utiliser iKeyman pour créer :

- Des demandes de signature de certificat : un fichier à envoyer par courrier électronique à une autorité de certification pour demander un certificat X.509.
- Des certificats de clés : une combinaison d'un certificat codé en ASCII et d'une clé privée chiffrée PKCS12 codée en ASCII. Si vous générez des certificats de clés en utilisant le format standard (par défaut) avec certains chiffres, le certificat de sortie contiendra des erreurs lors de son importation dans Sterling B2B Integrator. PKCS12 est le format recommandé pour les certificats de clé.

Pour plus d'informations sur la configuration et l'utilisation d'iKeyman, voir iKeyman Overview for IBM SDK, Java Technology Edition 7.0.0

Tâches de certificat

Création d'un certificat autosigné

Vous pouvez créer un certificat autosigné à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour créer un certificat autosigné :

Procédure

1. Choisissez l'une des options suivantes :

- Si vous utilisez Sterling B2B Integrator, sélectionnez **Partenaire commercial>Certificats numériques>Système** à partir du menu **Administration**.
- Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats.**

2. En regard de **Créer certificat autosigné**, cliquez sur **OK**
3. Entrez le **Nom** du certificat autosigné.
4. Entrez le nom de l'**Organisation** d'origine.
5. Sélectionnez le **Pays** ou l'origine du certificat autosigné.
6. Entrez une **Adresse électronique** de contact pour la personne responsable des certificats dans l'organisation, puis cliquez sur **Suivant**.
7. Entrez le **Numéro de série** du certificat. Le numéro de série est le numéro que vous souhaitez affecter au certificat autosigné.
8. Entrez le nombre de jours (**Durée**) pendant lesquels le certificat autosigné est valide.

   Remarque : Dans la version 5.2.6.2 ou ultérieure, la date d'expiration maximum est le *1er janvier 2080*. Toutes les durées entrées qui entraîneraient une date d'expiration ultérieure au 1er janvier 2080 sont redéfinies au *1er janvier 2080* par défaut. Dans les éditions précédentes, aucune limite supérieure n'existe.
9. Entrez les **Adresses IP** des interfaces réseau que vous souhaitez associer au certificat dans la zone SubjectAltName.
10. Entrez les **Noms DNS** des interfaces réseau que vous souhaitez associer au certificat dans la zone SubjectAltName.
11. Sélectionnez la **Longueur de clé** parmi les valeurs suivantes :
    - 512
    - 1024
    - 2048

    Remarque : La longueur de clé 1024 constitue un bon équilibre entre la sécurité, l'interopérabilité et l'efficacité. La longueur de clé 2048 est la plus sécurisée, mais aussi la plus lente ; elle risque de ne pas fonctionner avec certaines applications.

    Remarque : Si vous sélectionnez la longueur de clé 512, vous devez également utiliser JDK 7 SR5. JDK 7 SR7 FP1 ne prend pas en charge les longueurs de clé inférieures à 1024.
12. Sélectionnez l'**Algorithme de signature**.
13. Sélectionnez l'option **Valider lors de l'utilisation**. Les options de validation sont les suivantes :
    - Validité – Vérifie si les dates comprises dans la période de validité du certificat sont toujours en cours. Si les dates ne sont pas en cours, le certificat ne pourra pas être utilisé.
    - Chaîne d'authentification – Construit une chaîne de confiance pour les certificats qui ne sont pas autosignés. Si une chaîne de confiance ne peut pas être construite en utilisant des certificats valides, le certificat n'est pas utilisé. Si le certificat est autosigné, cette option vérifie uniquement la signature du certificat.
14. Cochez la case **Définir le bit de signature du certificat**.
15. Cliquez sur **Suivant**.

16. Consultez les informations sur le certificat autosigné.
17. Cliquez sur **Terminer**.

Obtention automatique d'un certificat accrédité auprès des partenaires commerciaux

L'utilitaire de capture de certificat automatise le processus d'obtention d'un certificat SSL auprès d'un partenaire commercial. Cette méthode d'obtention des informations de certificat permet à un partenaire de se connecter et d'enregistrer aisément un certificat.

Pourquoi et quand exécuter cette tâche

Si vous le souhaitez, un contrôle des droits d'accès hors bande peut ensuite être effectué avant que le certificat ne soit archivé dans le système en tant que certificat accrédité ou émis par une autorité de certification.

Étapes à exécuter préalablement à l'installation :

- Vérifiez que le système hôte de votre partenaire est activé pour SSL.
- Obtenez les informations d'hôte et de port pour le serveur auprès de votre partenaire commercial.
- Si le mode FTPS est utilisé, déterminez s'il sera explicite ou implicite.
- Configurez l'instance du service SSLCertGrabberAdapter par défaut de sorte à utiliser le serveur de périphérie et le serveur de proxy (HTTPS uniquement) appropriés. Pour plus de détails, consultez la documentation de l'adaptateur.

Pour obtenir le certificat SSL automatiquement auprès d'un partenaire commercial :

Procédure

1. Dans le menu **Administration**, sélectionnez **Partenaire commercial > Certificats numériques > Utilitaire de capture de certificat**.
2. En regard de **Capturer le certificat d'un partenaire**, cliquez sur **OK**.
3. Sélectionnez le type de connexion du serveur et cliquez sur **Suivant**.
   - FTPS
   - HTTPS
4. Entrez le **Nom d'hôte** ou l'**Adresse IP**.
5. Entrez le numéro de **Port**.
6. Sélectionnez le mode de connexion FTPS (si vous utilisez HTTPS, ignorez cette étape) :
   - Explicite - La négociation SSL se produit après que la connexion FTP est établie. Valeur par défaut.
   - Implicite - La négociation SSL se produit avant que la connexion FTP ne soit établie.
7. Cliquez sur **Suivant**. Le système tente de se connecter et d'extraire les certificats.
8. Une fois la capture terminée, passez en revue les informations récapitulatives et déterminez les certificats que vous souhaitez enregistrer.
9. Sélectionnez une méthode de codage pour chaque certificat et cliquez sur **Enregistrer**. Les formats de codage sont les suivants :
   - BASE64 - Cette option utilise le codage BASE64 sur le certificat DER standard. Valeur par défaut.

- DER – Format standard des certificats numériques, accepté par la plupart des applications.

10. Cliquez sur **Enregistrer** et accédez à l'emplacement où vous souhaitez enregistrer le fichier.
11. Acceptez le nom de fichier par défaut ou modifiez-le en fonction des conventions de dénomination de votre fichier et cliquez sur **Enregistrer**.
12. Après l'enregistrement, les certificats peuvent être archivés dans le système. Si vous décidez d'archiver un certificat dans le système :
    a. Vérifiez que chaque certificat est valide et accrédité.
    b. Archivez le certificat en tant que certificat de l'autorité de certification ou en tant que certificat accrédité, selon sa fonction. Pour l'accréditation basée sur une autorité de certification, vous devrez peut-être archiver la chaîne de certificats, à l'exception du certificat d'utilisateur final. Pour l'accréditation directe, archivez le certificat d'utilisateur final.

Configuration des informations d'état sur les récapitulatifs des certificats

Par défaut, les informations d'état de certificat sont fournies à la fin de la fenêtre en incrustation récapitulative lorsqu'un nom de certificat lié par hyperlien est sélectionné. Vous pouvez inclure ou exclure les informations d'état. Etant donné que ces informations sont compilées en temps réel, vous ne souhaiterez peut-être pas les inclure.

Pourquoi et quand exécuter cette tâche

La propriété VerificationOnPopupInfo contrôle si les informations d'état sont affichées dans le récapitulatif de certificat. Elle se trouve dans le fichier ui.properties. Les valeurs de la propriété VerificationOnPopupInfo sont les suivantes :

- true - inclure les informations de validation (valeur par défaut)
- false - ne pas compiler ni afficher les informations de validation dans la fenêtre en incrustation
- (toute autre valeur) - inclure les informations de validation

Pour empêcher la compilation et l'affichage des informations d'état :

Procédure

1. Ouvrez le fichier ui.properties.
2. Attribuez à la propriété VerificationOnPopupInfo la valeur false. Par exemple :
   ```
   VerificationOnPopupInfo=false
   ```
3. Enregistrez et fermez le fichier.
4. Redémarrez Sterling B2B Integrator.

Configuration de l'affichage des empreintes

Outre le hachage SHA1 précalculé, des empreintes du certificat supplémentaires peuvent être incluses dans les écrans de résumé, de confirmation et d'affichage des certificats. Les calculs du hachage sont effectués sur demande lors de la génération d'un affichage.

Pourquoi et quand exécuter cette tâche

Les empreintes supplémentaires s'affichent sur les écrans de l'interface graphique, mais n'ont aucune incidence sur le traitement des messages ou sur les communications du système.

Pour configurer le système afin de calculer et d'afficher des empreintes de certificat supplémentaires :

Procédure

1. Dans le fichier ui.properties, modifiez la ligne suivante :

   ```
   AddtlCertThumbprintAlgs=hash_algorithm
   ```

   Pour afficher plusieurs hachages supplémentaires, séparez les valeurs par des virgules. Par exemple :

   ```
   AddtlCertThumbprintAlgs=SHA384,SHA512
   ```

Paramètre	Description
hash_algorithm	Nom d'un algorithme de hachage à appliquer à l'empreinte du certificat. Les valeurs valides sont les suivantes : • SHA-256 • SHA-384 • SHA-512

2. Enregistrez et fermez le fichier ui.properties.
3. Redémarrez Sterling B2B Integrator.

Recherche des certificats d'autorité de certification

Vous pouvez rechercher un certificat d'autorité de certification à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour rechercher un certificat d'autorité de certification :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, dans le **Menu Administration**, sélectionnez **Partenaire commercial>Certificats numériques>Autorité de certification**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats.**
2. Effectuez l'une des opérations suivantes, puis cliquez sur **OK**.
   - Sous Rechercher, dans la zone **par nom de certificat**, entrez tout ou partie du nom du certificat de l'autorité de certification que vous recherchez. La page Certificats numériques de l'autorité de certification répertorie tous les certificats de l'autorité de certification qui correspondent à vos critères de recherche.
   - Sous Liste, dans la zone **Par ordre alphabétique**, sélectionnez **TOUT** ou la lettre qui commence par le nom du certificat de l'autorité de certification que vous recherchez. La sélection de l'option TOUT répertorie tous les certificats de l'autorité de certification. La page Certificats numériques de l'autorité de

certification répertorie tous les certificats de l'autorité de certification qui correspondent à vos critères de recherche.

Affichage des informations récapitulatives sur les certificats d'autorité de certification

Lorsqu'une liste de certificats s'affiche, vous pouvez cliquer sur le nom d'un certificat pour consulter les informations récapitulatives le concernant. Vous pouvez configurer le nom de système, l'empreinte numérique et le statut.

Pourquoi et quand exécuter cette tâche

Les zones suivantes sont configurables dans le système.

Zone récapitulative du certificat	Description
Nom de système	Le nom du certificat correspond à l'étiquette de la base de données. Il fait référence à ce certificat dans l'interface graphique et stocke ce nom dans sa base de données. Le nom par défaut d'un certificat provenant du fichier de clés JKS est une chaîne arbitraire. Les noms des autres certificats sont créés à partir du nom distinctif relatif de l'émetteur (RDN) et du numéro de série du certificat. Vous pouvez changer un nom de certificat en un nom plus court ou plus éloquent lors de l'archivage ou de l'édition du certificat.
Empreinte numérique	Les informations sur le hachage SHA1 sont incluses par défaut. Pour configurer le calcul et l'affichage des informations d'empreinte numérique des autres hachages, éditez le fichier ui.properties.
État	Vérification en temps réel de l'état en cours, indiquant si les dates de certificat sont valides et si le certificat a été vérifié. Pour définir si ces informations seront calculées au moment de l'affichage ou non, éditez le fichier ui.properties.

Bien que ces informations s'appliquent aux informations récapitulatives d'un certificat d'autorité de certification, des zones similaires apparaissent dans les écrans de récapitulatif et de confirmation pour d'autres types de certificats.

Restitution des certificats d'autorité de certification à partir de l'interface utilisateur

Vous pouvez restituer un certificat d'autorité de certification à partir de l'interface utilisateur dans le menu **Administration**.

Pourquoi et quand exécuter cette tâche

En fonction des règles de sécurité en vigueur sur votre site, des certificats d'autorité de certification du fichier de clés Java (JKS) peuvent également être restitués par le biais de la console.

Avant de commencer, sauvegardez tout certificat d'autorité de certification obtenu en externe dans un fichier local.

Pour restituer un certificat d'autorité de certification :

Procédure

1. Choisissez l'une des options suivantes :

- Si vous utilisez Sterling B2B Integrator, dans le **Menu Administration**, sélectionnez **Partenaire commercial>Certificats numériques>Autorité de certification**.
- Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats**.

2. En regard de **Restituer le nouveau certificat**, cliquez sur **OK**.
3. Sélectionnez une méthode d'importation des certificats :

Méthode d'importation	Procédure à suivre
Importer à partir de la machine virtuelle Java – Importe à partir du fichier de clés JKS	1. Cliquez sur **Importer** depuis la **Machine virtuelle Java**. 2. Acceptez le mot de passe par défaut qui s'affiche dans la zone de mot de passe, puis cliquez sur **Suivant**. Le mot de passe du fichier de clés par défaut est fourni par Sun Microsystems. Si la zone du mot de passe est vide, le système utilise le mot de passe par défaut.
Importer à partir d'un fichier - Importe les certificats sauvegardés dans un fichier sur une unité locale	1. Cliquez sur **Fichier** > **Importer**. 2. Entrez le nom du fichier ou cliquez sur **Parcourir** pour sélectionner un fichier de certificat d'autorité de certification. Cliquez sur Suivant. Vous pouvez ignorer le mot de passe qui s'affiche dans la zone de mot de passe. Vous n'avez pas besoin d'effacer l'entrée.

   Les certificats disponibles sont répertoriés avec un récapitulatif des informations d'identification. Tous les certificats sont sélectionnés par défaut.
4. Cochez les cases situées à gauche de chaque entrée pour sélectionner ou désélectionner les certificats à importer.
5. Pour chaque certificat sélectionné, acceptez le nom du certificat proposé ou le modifier en fonction des conventions de dénomination de votre fichier.
6. Sélectionnez l'option **Valider lors de l'utilisation**, puis cliquez sur **Suivant**. Les options de validation sont les suivantes :
   - Validité – Vérifie si les dates comprises dans la période de validité du certificat sont toujours en cours. Si les dates ne sont pas en cours, le certificat ne pourra pas être utilisé.
   - Chaîne d'authentification – Tente de construire une chaîne de confiance jusqu'à la racine pour les certificats qui ne sont pas autosignés. Si une chaîne de confiance ne peut pas être construite en utilisant des certificats valides, le certificat n'est pas utilisé. Si le certificat est autosigné, cette option vérifie uniquement la signature du certificat.
7. Si vous recevez un message indiquant que le certificat duplique un certificat déjà dans la base de données, entrez O ou N pour indiquer si vous souhaitez importer le doublon ou non.

   Cette vérification n'est effectuée que sur les certificats uniques. Elle n'a pas lieu lors de la restitution d'un ou de plusieurs certificats à partir d'un fichier.

   Les certificats sont identifiés par le hachage SHA1 afin de déterminer les doublons. Plusieurs copies d'un certificat peuvent être présentes dans la base de données, car chaque certificat renseigne une ligne différente et possède un ID objet distinct. Le certificat existant n'est pas remplacé.

8. Passez en revue les informations du certificat d'autorité de certification.
9. Cliquez sur **Terminer**.

Archivage des certificats d'autorité de certification à partir de la console

Après avoir sauvegardé tous les certificats de l'autorité de certification dans un fichier local, vous pouvez archiver le certificat d'autorité de certification sur la console à partir du répertoire d'installation.

Pourquoi et quand exécuter cette tâche

Les certificats d'autorité de certification courants sont stockés dans un fichier de clés JKS qui fait partie de la JVM livrée avec Sterling B2B Integrator. Le fichier de clés JKS se trouve à l'emplacement /install_dir/jdk/jre/lib/security/cacerts. Vous pouvez également obtenir des certificats en externe.

Pour importer des certificats dans le référentiel de confiance de Sterling B2B Integrator, modifiez la commande à l'emplacement /rép_install/install/bin/ImportCACerts.sh (UNIX) ou \rép_install\install\bin\ImportCACerts.cmd (Windows).

Avant de commencer, enregistrez tout certificat d'autorité de certification obtenu en externe dans un fichier local.

Pour archiver un certificat d'autorité de certification sur la console :

Procédure

1. Accédez au répertoire d'installation.
2. Accédez au répertoire bin.
3. Entrez la commande suivante :

   (UNIX) `./ImportCACerts.sh`

   (Windows) `ImportCACerts.cmd`

   Tous les certificats contenus dans le fichier sont répertoriés, avec les exceptions suivantes :
   - Les entrées contenant des clés symétriques ou privées ne sont ni traitées, ni répertoriées.
   - Seul le premier certificat d'un fichier au format DER est traité et répertorié.
4. À l'invite, entrez Y (non sensible à la casse) en regard des certificats que vous souhaitez importer.
5. Pour chaque certificat accepté, acceptez le nom du certificat proposé ou modifiez-le en respectant vos conventions de dénomination de fichier.
6. Si l'étiquette du certificat est un double d'une étiquette déjà enregistrée dans la base de données, entrez `Y` ou `N` (non sensible à la casse) pour indiquer si vous souhaitez le modifier ou non. Bien que les certificats ne soient généralement pas identifiés par leur étiquette et que la base de données autorise les étiquettes en double, certains services recherchent les certificats d'après leur étiquette. N'utilisez pas les étiquettes en double afin d'éviter tout comportement inattendu.
7. Si le certificat duplique un certificat déjà enregistré dans la base de données (comme indiqué par le hachage SHA1 du certificat), indiquez avec Y ou N si vous souhaitez importer le doublon.

   Les certificats sont identifiés par le hachage SHA1 afin de déterminer les doublons. Plusieurs copies d'un certificat peuvent être présentes dans la base

de données, car chaque certificat renseigne une ligne différente et possède un ID objet distinct. Le certificat existant n'est pas remplacé.

Édition des certificats d'autorité de certification

Vous pouvez éditer un certificat d'autorité de certification à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour éditer un certificat d'autorité de certification :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, dans le **Menu Administration**, sélectionnez **Partenaire commercial>Certificats numériques>Autorité de certification**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats.**
2. En utilisant Rechercher ou Liste, localisez le certificat d'autorité de certification que vous souhaitez Modifier, puis cliquez sur **OK**.
3. En regard du **Certificat d'autorité de certification** que vous souhaitez éditer, cliquez sur **Modifier**.
4. Entrez le nom du certificat.
5. Sélectionnez l'option **Valider lors de l'utilisation**, puis cliquez sur **Suivant**. Les options de validation sont les suivantes :
   - Validité – Vérifie si les dates comprises dans la période de validité du certificat sont toujours en cours. Si les dates ne sont pas en cours, le certificat ne pourra pas être utilisé.
   - Chaîne d'authentification – Construit une chaîne de confiance pour les certificats qui ne sont pas autosignés. Si une chaîne de confiance ne peut pas être construite en utilisant des certificats valides, le certificat n'est pas utilisé. Si le certificat est autosigné, cette option vérifie uniquement la signature du certificat.
6. Passez en revue les informations du certificat d'autorité de certification.
7. Cliquez sur **Terminer**.

Suppression des certificats de l'autorité de certification

Vous pouvez supprimer un certificat d'autorité de certification à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour supprimer un certificat de l'autorité de certification :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, dans le **Menu Administration**, sélectionnez **Partenaire commercial>Certificats numériques>Autorité de certification**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats.**
2. En regard de **Par ordre alphabétique**, cliquez sur **OK**.

3. En regard du certificat de l'autorité de certification que vous souhaitez supprimer, cliquez sur **Supprimer**.

Recherche des certificats de système

Vous pouvez rechercher un certificat de système à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour rechercher un certificat de système :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, sélectionnez **Partenaire commercial>Certificats numériques>Système** à partir du menu **Administration**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats.**
2. Dans la page Certificats de système, effectuez l'une des opérations suivantes, puis cliquez sur **OK** :
   - Sous Rechercher, dans la zone **par nom de certificat**, entrez tout ou partie du nom du certificat de système que vous recherchez. La page Certificats de système répertorie tous les certificats de système contenant le nom complet ou partiel que vous avez entré.
   - Sous **Liste**, dans la zone **Par ordre alphabétique**, sélectionnez **TOUT** ou la lettre qui commence par le nom du certificat de l'autorité de certification que vous recherchez. La sélection de TOUT répertorie tous les certificats de système. La page Certificats système répertorie tous les certificats de système correspondant à vos critères de recherche.

Édition des certificats de système

Vous pouvez éditer un certificat de système à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour éditer un certificat de système :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, sélectionnez **Partenaire commercial>Certificats numériques>Système** à partir du menu **Administration**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats.**
2. En utilisant Rechercher ou Liste, localisez le **certificat de système** que vous souhaitez éditer, puis cliquez sur **OK**.
3. En regard du certificat de système que vous souhaitez éditer, cliquez sur **Modifier**.
4. Entrez le **Nom du certificat**.
5. Sélectionnez l'option **Valider lors de l'utilisation**, puis cliquez sur **Suivant**. Les options de validation sont les suivantes :
   - Validité – Vérifie si les dates comprises dans la période de validité du certificat sont toujours en cours. Si les dates ne sont pas en cours, le certificat ne pourra pas être utilisé.

- Chaîne d'authentification – Construit une chaîne de confiance pour les certificats qui ne sont pas autosignés. Si une chaîne de confiance ne peut pas être construite en utilisant des certificats valides, le certificat n'est pas utilisé. Si le certificat est autosigné, cette option vérifie uniquement la signature du certificat.

6. Passez en revue les informations du certificat de système.
7. Cliquez sur **Terminer**.

Identification des certificats de système dans Sterling B2B Integrator

Vous pouvez identifier un certificat de système à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour identifier un certificat de système :

Procédure

1. Dans le menu **Administration**, sélectionnez **Déploiement > Services > Configuration**.
2. Dans la section Liste, sélectionnez le type d'adaptateur ou de service applicable dans la liste **par type de service**, puis cliquez sur **OK**.
3. Dans la liste des configurations, choisissez celle qui vous convient.
4. Cliquez sur le **nom du service** pour afficher les informations de configuration.
5. Passez en revue les informations récapitulatives de certificat.

Vérification de la date d'expiration d'un certificat de système

Si un adaptateur et un servlet sont utilisés pour les communications entrantes, vous devez surveiller les dates d'expiration des certificats de système afin de vous assurer que les certificats sont valides.

Pourquoi et quand exécuter cette tâche

Pour vérifier la date d'expiration d'un certificat de système :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, sélectionnez **Partenaire commercial>Certificats numériques>Système** à partir du menu **Administration**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats.**
2. Pour afficher tous les certificats de système, sélectionnez **Tout** dans la liste déroulante Alphabétique et cliquez sur **OK**.
3. Sélectionnez le nom du certificat de système que vous souhaitez afficher. Le Récapitulatif de certificat s'affiche.
4. Dans la section **Description** du Récapitulatif de certificat, passez en revue les informations fournies dans la zone **Dates valides**.
5. Passez en revue les informations fournies dans la section **Statut** pour voir si les dates sont valides et si le certificat a été vérifié.

Exportation des certificats de système dans Sterling B2B Integrator

Cette commande d'exportation n'est applicable qu'aux certificats de système Sterling B2B Integrator. Vous ne pouvez pas vous en servir pour exporter des certificats système sur HSM.

Pourquoi et quand exécuter cette tâche

Pour exporter un certificat de système, entrez la commande suivante avec les paramètres appropriés :

```
./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass
```

Paramètre	Description
keyname	Nom de la clé système à exporter.
pkcs12filename	Nom du fichier contenant les informations exportées.
pkcs12storepass	Mot de passe du magasin protégeant le magasin.
pkcs12keypass	Mot de passe de la clé protégeant la clé.

Suppression des certificats de système dans Sterling B2B Integrator

Vous pouvez exporter une copie du certificat de système sur votre disque local avant de le supprimer. Les certificats OpsDrv, OpsKey et UIKeys sont des certificats de système qui ne peuvent pas être supprimés.

Pourquoi et quand exécuter cette tâche

Pour supprimer un certificat de système :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, sélectionnez **Partenaire commercial>Certificats numériques>Système** à partir du menu **Administration**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats.**
2. En regard de **Par ordre alphabétique**, cliquez sur **OK**.
3. En regard du certificat de système que vous souhaitez supprimer, cliquez sur **Supprimer**.
4. Cliquez sur **Supprimer** dans la page de confirmation.

Extraction des certificats de système

Pour exporter un certificat de système, vous devez d'abord l'extraire. Cette procédure ne permet d'exporter que le certificat public, pas la clé privée, et vous fournit un certificat public à envoyer à un partenaire commercial.

Pourquoi et quand exécuter cette tâche

Pour extraire un certificat de système :

Procédure

1. Choisissez l'une des options suivantes :

- Si vous utilisez Sterling B2B Integrator, sélectionnez **Partenaire commercial>Certificats numériques>Système** à partir du menu **Administration**.
- Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats**.

2. En utilisant Rechercher ou Liste, localisez le certificat de système que vous souhaitez extraire.
3. En regard du certificat de système que vous souhaitez extraire, cliquez sur **Extraire**.
4. Dans la boîte de dialogue **Extraction de certificat de système**, sélectionnez le format du certificat et cliquez sur **OK** :
   - PKCS12 - Cette option formate le certificat numérique sous la forme d'un fichier PKCS12. Vous avez également la possibilité de saisir un Mot de passe de la clé privée et un Mot de passe du fichier de clés.
   - BASE64 - Cette option utilise le codage BASE64 sur le certificat DER standard.
   - DER - Ce format standard pour les certificats numériques est accepté par la plupart des applications.
5. Dans la boîte de dialogue **Téléchargement de fichier**, cliquez sur **Enregistrer**.
6. Dans la boîte de dialogue **Enregistrer sous**, sélectionnez l'emplacement dans lequel enregistrer le certificat, puis cliquez sur **Enregistrer**. L'option d'ouverture du certificat n'est pas prise en charge. Vous devez ouvrir le certificat dans le système d'exploitation. Si vous recevez le message d'erreur "il s'agit d'un fichier de certificat de sécurité non valide, ouvrez le fichier dans un éditeur de texte et supprimez toutes les lignes vides avant -----BEGIN CERTIFICATE-----", enregistrez le fichier modifié puis essayez de l'ouvrir.
7. Cliquez sur **Fermer** dans la boîte de dialogue Extraction de certificat de système. La page Certificat de système est affichée.

Recherche des certificats de confiance

Vous pouvez rechercher un certificat de confiance à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour rechercher un certificat de confiance :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, dans le **Menu Administration**, sélectionnez **Partenaire commercial>Certificats numériques>Trusted**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats**.
2. Dans la page Certificats numériques de confiance, effectuez l'une des opérations suivantes, puis cliquez sur **OK** :
   - Sous Rechercher dans la zone **par nom de certificat**, entrez tout ou partie du nom du certificat de confiance que vous recherchez. La page Certificats numériques de confiance répertorie tous les certificats de confiance qui correspondent à vos critères de recherche.
   - Dans la liste déroulante **Par ordre alphabétique** sous Liste, sélectionnez **TOUT** ou la lettre qui commence par le nom du certificat de confiance que

vous recherchez. La page Certificats numériques de confiance répertorie tous les certificats de confiance qui correspondent à vos critères de recherche.

Restitution d'un certificat de système de confiance

Vous pouvez restituer les certificats de confiance tels que des certificats SSL importés à partir de partenaires commerciaux ou d'autres certificats externes.

Pourquoi et quand exécuter cette tâche

Les certificats sécurisés peuvent provenir des sources suivantes :

- Certificats SSL importés des partenaires commerciaux
- Autres certificats obtenus à l'extérieur

Avant de commencer, sauvegardez le certificat de système de confiance dans un fichier sur votre ordinateur local.

Pour restituer un certificat de système de confiance :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, dans le **Menu Administration**, sélectionnez **Partenaire commercial>Certificats numériques>Trusted**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats**.
2. En regard de **Restituer le nouveau certificat**, cliquez sur **OK**.
3. Entrez le **Nom de fichier** ou cliquez sur **Parcourir** pour sélectionner le nom de fichier du certificat de confiance, puis cliquez sur **Suivant**.
4. Entrez le **Nom du certificat**.
5. Vérifiez le nom du certificat de confiance que vous restituez. Pour chaque certificat sélectionné, la zone Nom du certificat indique un nom proposé, suivi d'un récapitulatif des informations d'identification dans le certificat. Vous pouvez modifier le nom en fonction des conventions de dénomination de votre fichier.
6. Si vous possédez plusieurs certificats de confiance figurant dans le fichier sélectionné, cochez la case à gauche de chaque certificat pour restituer chaque certificat.
7. Sélectionnez l'option **Valider lors de l'utilisation**, puis cliquez sur **Suivant**. Les options de validation sont les suivantes :
   - Validité – Vérifie si les dates comprises dans la période de validité du certificat sont toujours en cours. Si les dates ne sont pas en cours, le certificat ne pourra pas être utilisé.
   - Chaîne d'authentification – Tente de construire une chaîne de confiance jusqu'à la racine pour les certificats qui ne sont pas autosignés. Si une chaîne de confiance ne peut pas être construite en utilisant des certificats valides, le certificat n'est pas utilisé. Si le certificat est autosigné, cette option vérifie uniquement la signature du certificat.
   - Cache CRL - Vérifie si le cache CRL (liste de révocation de certificat) est consulté chaque fois que le certificat de système est utilisé.
8. Passez en revue les informations du certificat de confiance.
9. Cliquez sur **Terminer**.

Édition des certificats de confiance

Vous pouvez éditer un certificat de confiance à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour éditer un certificat de confiance :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, dans le **Menu Administration**, sélectionnez **Partenaire commercial>Certificats numériques>Trusted**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats**.
2. En utilisant Rechercher ou Liste, localisez le certificat de confiance que vous souhaitez éditer, puis cliquez sur **OK**.
3. Cliquez sur **Modifier** en regard du certificat de confiance que vous voulez modifier.
4. Entrez le **Nom du certificat**.
5. Sélectionnez l'option **Valider lors de l'utilisation**, puis cliquez sur **Suivant**. Les options de validation sont les suivantes :
   - Validité – Vérifie si les dates comprises dans la période de validité du certificat sont toujours en cours. Si les dates ne sont pas en cours, le certificat ne pourra pas être utilisé.
   - Chaîne d'authentification – Tente de construire une chaîne de confiance jusqu'à la racine pour les certificats qui ne sont pas autosignés. Si une chaîne de confiance ne peut pas être construite en utilisant des certificats valides, le certificat n'est pas utilisé. Si le certificat est autosigné, cette option vérifie uniquement la signature du certificat.
   - Cache CRL - Vérifie si le cache CRL (liste de révocation de certificat) est consulté chaque fois que le certificat de système est utilisé.
6. Passez en revue les informations du certificat.
7. Cliquez sur **Terminer**.

Suppression des certificats de système de confiance

Vous pouvez supprimer un certificat de système de confiance à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour supprimer un certificat de système de confiance :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, dans le **Menu Administration**, sélectionnez **Partenaire commercial>Certificats numériques>Trusted**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats**.
2. En regard de **Par ordre alphabétique**, cliquez sur **OK**.
3. En regard du certificat de confiance que vous souhaitez supprimer, cliquez sur **Supprimer**.

Importation des certificats de système PKCS12

Vous pouvez importer un certificat de système PKCS12.

Pourquoi et quand exécuter cette tâche

Pour importer un certificat de système PKCS12 :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez :

```
./ImportSystemCert.sh -pkcs12 systempass certname pkcs12file
pkcs12storepass pkcs12keypass keystoretype keystoreprovider storepass
keypass
```

Restitution des certificats de système PKCS12

Après avoir sauvegardé le certificat de système PKCS12 dans un fichier sur votre ordinateur local, vous pouvez restituer le certificat de système PKCS12 à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Avant de commencer, sauvegardez le certificat de système PKCS12 dans un fichier sur votre ordinateur local.

Pour restituer un certificat de système PKCS12 :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, sélectionnez **Partenaire commercial>Certificats numériques>Système** à partir du menu **Administration**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats**.
2. Dans la page Certificats de système, sous Restituer, en regard de **Certificat PKCS12**, cliquez sur **OK**.
3. Entrez le **Nom du certificat** PKCS12.
4. Entrez le **Mot de passe de la clé privée**. Ce mot de passe est utilisé pour chiffrer le certificat PKCS12.
5. Entrez le **Mot de passe du fichier de clés**. Ce mot de passe est utilisé pour l'objet PKCS12. Il peut être identique au mot de passe de la clé privée.
6. Entrez le **Nom de fichier** ou cliquez sur **Parcourir** pour sélectionner le nom de fichier du certificat PKCS12, puis cliquez sur **Suivant**.
7. Sélectionnez l'option **Valider lors de l'utilisation**, puis cliquez sur **Suivant**. Les options de validation sont les suivantes :
   - Validité – Vérifie si les dates comprises dans la période de validité du certificat sont toujours en cours. Si les dates ne sont pas en cours, le certificat ne pourra pas être utilisé.
   - Chaîne d'authentification – Construit une chaîne de confiance pour les certificats qui ne sont pas autosignés. Si une chaîne de confiance ne peut pas être construite en utilisant des certificats valides, le certificat n'est pas utilisé. Si le certificat est autosigné, cette option vérifie uniquement la signature du certificat.
8. Passez en revue les informations du certificat de système PKCS12.

9. Cliquez sur **Terminer**.

Importation des certificats de système PEM

Vous pouvez importer un certificat de système PEM chiffré avec DES ou 3DES.

Pourquoi et quand exécuter cette tâche

Seules les clés PEM chiffrées à l'aide de DES ou de 3DES sont prises en charge.

Pour importer un certificat de système PEM :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez :

```
./ImportSystemCert.sh -pem systempass certname file password
keystoretype keystoreprovider storepass keypass
```

Importation des certificats de système de clé

Vous pouvez importer un certificat de système de clé.

Pourquoi et quand exécuter cette tâche

Pour importer un certificat de système de clé :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez :

```
./ImportSystemCert.sh -keycert systempass certname file
password keystoretype keystoreprovider storepass keypass
```

Importation des certificats de système de fichiers de clés

Vous pouvez générer un certificat de système de fichier de clés sur un outil HSM.

Pourquoi et quand exécuter cette tâche

Pour générer un certificat de système de fichiers de clés sur un outil HSM :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez :

```
./ImportSystemCert.sh -keystore systempass certname
alias keystoretype keystoreprovider storepass keypass
```

Restitution des certificats de système de clé

Après avoir sauvegardé le certificat de système de clé dans un fichier sur votre ordinateur local, vous pouvez restituer le certificat de système de clé à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Avant de commencer, sauvegardez le certificat de système de clé dans un fichier sur votre ordinateur local.

Pour restituer un certificat de système de clé :

Procédure

1. Choisissez l'une des options suivantes :
   - Si vous utilisez Sterling B2B Integrator, sélectionnez **Partenaire commercial>Certificats numériques>Système** à partir du menu **Administration**.
   - Si vous utilisez l'édition AS2, à partir du menu **Administration AS2**, sélectionnez **Certificats**.
2. En regard de **Certificat de clé**, cliquez sur **OK**
3. Entrez le **Nom du certificat**.
4. Entrez le **Mot de passe de la clé privée.** Ce mot de passe est utilisé pour chiffrer la clé privée.
5. Entrez le **Nom de fichier** ou cliquez sur **Parcourir** pour sélectionner le nom de fichier du certificat de clé, puis cliquez sur **Suivant**.
6. Sélectionnez l'option **Valider lors de l'utilisation**, puis cliquez sur **Suivant**. Les options de validation sont les suivantes :
   - Validité – Vérifie si les dates comprises dans la période de validité du certificat sont toujours en cours. Si les dates ne sont pas en cours, le certificat ne pourra pas être utilisé.
   - Chaîne d'authentification – Construit une chaîne de confiance pour les certificats qui ne sont pas autosignés. Si une chaîne de confiance ne peut pas être construite en utilisant des certificats valides, le certificat n'est pas utilisé. Si le certificat est autosigné, cette option vérifie uniquement la signature du certificat.
7. Passez en revue les informations du certificat de clé.
8. Cliquez sur **Terminer**.

Protocole OCSP (Online Certificate Status Protocol)

Prise en charge du protocole OCSP (Online Certificate Status Protocol) dans Sterling B2B Integrator

Le protocole OCSP (Online Certificate Status Protocol) est un ensemble de structures de données définies par ASN.1 qui permet de demander et de recevoir des informations sur l'état de révocation des certificats. En principe, ces structures de données peuvent être envoyées et reçues par de nombreux protocoles de transport. Dans la pratique, le protocole HTTP est utilisé.

Un client OCSP envoie des questions et traite les réponses. Un canal répondeur OCSP répond aux questions et génère des réponses.

Fonctionnalités du client OCSP

Une implémentation de client OCSP se compose des structures de données pour la gestion des informations sur les canaux répondeurs OCSP, de la fonctionnalité de génération des demandes OCSP, de la fonctionnalité de traitement des réponses OCSP et de la fonctionnalité de transmission des demandes OCSP et de réception des réponses OCSP.

Une implémentation de client OCSP comprend :

- Des structures de données pour la gestion des informations sur les canaux répondeurs OCSP
- Des fonctionnalités de génération des demandes OCSP
- Des fonctionnalités de traitement des réponses OCSP

- Des fonctionnalités de transmission des demandes OCSP et de réception des réponses OCSP

Comment Sterling B2B Integrator effectue une vérification OCSP

Une vérification OCSP d'un certificat dans Sterling B2B Integrator est déterminée lorsque la vérification OCSP dans Sterling B2B Integrator est implémentée dans le cadre des API système internes utilisées par des services pour récupérer des certificats et des clés dans la base de données.

Pourquoi et quand exécuter cette tâche

Les vérifications OCSP sont exécutées par Sterling B2B Integrator lorsque des méthodes sont appelées pour obtenir des certificats et des clés à partir des objets qui les encapsulent dans la base de données.

Les étapes suivantes décrivent la façon dont la vérification OSCSP est implémentée dans Sterling B2B Integrator :

Procédure

1. Le système examine l'objet qui encapsule le certificat afin de déterminer si la vérification OCSP est activée. Cela lui permet de décider, sans appeler aucune autre base de données, si une vérification OCSP doit être tentée ou non.
2. Si la vérification OCSP est activée, le système récupère le nom de l'émetteur codé à partir d'un certificat.
3. Le système effectue un hachage du nom de l'émetteur codé à l'aide de SHA1.
4. Le système tente de trouver une autorité configurée dans le système ayant un nom dont le hachage correspond à celui du certificat.
5. Si le système ne trouve aucune autorité, aucune vérification n'est effectuée.
6. Si le système trouve une autorité, le système vérifie la stratégie OCSP de l'autorité. Si la stratégie l'autorise ou requiert des vérifications OCSP, reportez-vous au tableau CERT_AUTHORITY pour plus d'informations. Le système tente de trouver un canal répondeur OCSP pour l'autorité.
7. Si aucun canal répondeur OCSP n'est trouvé pour l'autorité, l'une des situations suivantes se produit :
   - Si la stratégie de l'autorité est définie sur Toujours vérifier, une exception est générée et la vérification échoue.
   - Si la stratégie de l'autorité est définie sur Vérifier uniquement lorsqu'un canal répondeur est configuré, aucune vérification n'est effectuée.
   - Si un canal répondeur OCSP est trouvé pour l'autorité, une vérification OCSP est tentée.

Tables de base de données

CERT_AUTHORITY et OCSP_RESPONDER ont été ajoutés pour assurer la gestion les informations liées à OCSP.

Deux nouvelles tables de base de données ont été ajoutées pour assurer la gestion des informations liées à OCSP :

- CERT_AUTHORITY
- OCSP_RESPONDER

CERT_AUTHORITY

La table CERT_AUTHORITY stocke les informations concernant les autorités de certification.

Colonne	Type	Description
OBJECT_ID	VARCHAR (255)	GUID qui constitue l'ID unique d'un enregistrement. Il s'agit de la clé primaire. Cette valeur ne peut pas être NULL.
NAME	VARCHAR (255)	Nom d'un enregistrement. La valeur NULL est autorisée.
CREATE_DATE	DATETIME	Date de création d'un enregistrement.
MODIFIED_DATE	DATETIME	Date de la dernière modification d'un enregistrement.
MODIFIED_BY	VARCHAR(255)	Informations sur l'utilisateur qui a modifié un enregistrement.
ISSUER_NAME	BLOB	Nom distinctif relatif de l'autorité de certification extrait de son certificat.
HASH_ALG	VARCHAR(128)	Algorithme de hachage utilisé pour calculer le nom et la clé de hachage. Seul SHA1 est pris en charge.
RDN_HASH	VARCHAR(255)	Hachage SHA1 (codé en BASE64) du nom distinctif réel de l'émetteur codé en DER extrait du certificat de l'autorité de certification. Cette colonne est indexée.
KEY_HASH	VARCHAR(255)	Hachage SHA1 (codé en BASE64) de la clé publique codée du certificat de l'émetteur.
CERT_OID	VARCHAR(255)	OBJECT_ID du certificat de l'autorité de la table CA_CERT_INFO. Chaque autorité doit disposer d'un certificat d'autorité de certification dans la base de données. Les valeurs NULL ne sont pas autorisées.

Colonne	Type	Description
OCSP_POLICY	VARCHAR(128)	Stratégie OCSP de l'autorité. Ce type est composé de deux valeurs au format CSV. Les valeurs indiquent le moment auquel utiliser OCSP et les éléments à vérifier. Les valeurs valides sont : **OCSP_When** • never : ne jamais utiliser OCSP. • resp : utiliser OCSP uniquement si un répondeur est configuré lorsqu'une demande est effectuée. • always : toujours utiliser OCSP lorsqu'une demande est effectuée. Ce paramètre nécessite la configuration d'un répondeur ; dans l e cas contraire, la vérification du certificat échoue. **OCSP_What** • none : ne jamais vérifier les certificats • end-user : vérifier uniquement les certificats de l'utilisateur final • both : vérifier les certificats intermédiaires et les certificats de l'utilisateur final. Cette fonction n'est actuellement pas prise en charge. • La valeur Null n'est pas admise dans cette colonne
CRL_POLICY	VARCHAR(128)	Non utilisé à l'heure actuelle.

OCSP_RESPONDER

La table OCSP_RESPONDER conserve les informations concernant les répondeurs OCSP.

Colonne	Type	Description
OBJECT_ID	VARCHAR (255)	GUID qui constitue l'ID unique d'un enregistrement. Il s'agit de la clé primaire. Cette valeur ne peut pas être NULL.
NAME	VARCHAR (255)	Nom d'un enregistrement. La valeur NULL est autorisée.
CREATE_DATE	DATETIME	Date de création d'un enregistrement.
MODIFIED_DATE	DATETIME	Date de la dernière modification d'un enregistrement.
MODIFIED_BY	VARCHAR(255)	Informations sur l'utilisateur qui a modifié un enregistrement.
ISSUER_NAME	BLOB	Nom distinctif relatif de l'autorité de certification extrait de son certificat.
HASH_ALG	VARCHAR(128)	Algorithme de hachage utilisé pour calculer le nom et la clé de hachage. Seul SHA1 est pris en charge.

Colonne	Type	Description
RDN_HASH	VARCHAR(255)	Hachage SHA1 (codé en BASE64) du nom distinctif réel de l'émetteur codé en DER extrait du certificat de l'autorité de certification. Cette colonne est indexée.
KEY_HASH	VARCHAR(255)	Hachage SHA1 (codé en BASE64) de la clé publique codée du certificat de l'émetteur.
CERT_OID	VARCHAR(255)	OBJECT_ID du certificat de l'autorité de la table CA_CERT_INFO. Chaque autorité doit disposer d'un certificat d'autorité de certification dans la base de données. Les valeurs NULL ne sont pas autorisées.
CACHE_TTL	VARCHAR(64)	Durée, en secondes, de la durée de vie des réponses OCSP dans la mémoire cache de réponse interne. Si la colonne est NULL, les réponses OCSP sont mises en cache pendant 1 seconde, autant dire rien du tout.
TRANS_PROF_OID	VARCHAR(255)	OBJECT_ID d'un profil dans la base de données GIS. Vous devez créer un profil pour le répondeur OCSP, qui inclut l'URL correcte du répondeur.
COMM_BP	VARCHAR(255)	Nom d'un processus technique utilisé pour communiquer avec le répondeur OCSP. Ce processus technique doit être capable d'assurer les communications HTTP. Les services qu'il propose doivent être configurés pour ne pas exiger ou présenter des en-têtes HTTP lors de l'envoi et de la réception, respectivement. Le processus HTTPClientSend fourni avec le système peut être utilisé et il est recommandé.
COMM_WAIT	VARCHAR(24)	Nombre de secondes d'attente pour établir la communication avec le répondeur OCSP avant le signalement d'une erreur.

Configuration d'OCSP

Vous pouvez créer des droits et des programmes de réponse illimités au moment où vous configurez le système pour qu'il utilise OCSP.

Pourquoi et quand exécuter cette tâche

Lorsque vous configurez le système, vous pouvez créer autant de certificats d'autorité et de répondeurs que vous le souhaitez.

Pour configurer le système afin d'utiliser OCSP :

Procédure

1. Vérifiez que le certificat d'autorité de certification que vous souhaitez archiver avec OCSP dans Sterling B2B Integrator a bien été émis par une autorité de certification.
2. Répertoriez les certificats d'autorité de certification dans le système et récupérez l'ID objet du certificat que vous venez d'installer.

3. Si le certificat de signature de réponse OCSP de l'autorité est différent du certificat émis par l'autorité, archivez le certificat de signature de réponse OCSP de l'autorité dans Sterling B2B Integrator comme un certificat de confiance.

   Remarque : Avec la version 5.2.4.2 ou supérieure, vous pouvez restituer le certificat racine qui a émis le certificat de réponse comme l'autorité de certification, plutôt que le certificat de réponse comme un certificat de confiance. Puisque le certificat de réponse change fréquemment, selon l'autorité de certification, il peut causer l'échec d'OCSP jusqu'à ce que le certificat soit remplacé par un autre valide. La bonne pratique recommandée est désormais de toujours restituer un certificat racine, puisqu'ils sont rarement modifiés. Toutefois, les deux types seront toujours autorisés.
4. Si vous avez archivé un certificat de signature OCSP supplémentaire, répertoriez les certificats de l'autorité de certification dans le système et obtenez l'ID objet du certificat que vous venez d'installer.
5. Accédez au répertoire bin de l'installation de Sterling B2B Integrator.
6. Démarrez la base de données si nécessaire.
7. Démarrez interpréteur de commandes bash ou sh.
8. Entrez la commande suivante : source tmp.sh.
9. Créez une autorité à l'aide de l'utilitaire contenu dans la classe com.sterlingcommerce.security.ocsp.SCICertAuthority.
10. Créez un répondeur OCSP à l'aide de l'utilitaire contenu dans la classe com.sterlingcommerce.security.ocsp.SCIOCSPResponder.
11. Mettez à jour les certificats de l'autorité ou les certificats individuels afin d'activer OCSP. L'utilitaire com.sterlingcommerce.security.ocsp.SetAuthorityCertificatesOCSPInfo configure tous les certificats de confiance et de système d'une autorité. L'utilitaire com.sterlingcommerce.security.ocsp.SetSystemCertificateOCSPInfo configure 1 certificat de système. L'utilitaire com.sterlingcommerce.security.ocsp.SetTrustedCertificateOCSPInfo configure 1 certificat de confiance.

Scripts de configuration OCSP

Les scripts suivants ont été inclus avec le correctif OCSP pour exécuter les utilitaires de configuration OCSP. Il existe une version UNIX/Linux et Windows de chaque script. Les scripts prennent les mêmes arguments de ligne de commande que les programmes utilitaires qu'ils invoquent. Ils sont stockés dans le répertoire bin de l'installation du produit. Les informations sur les arguments de ligne de commande sont, dans les grandes lignes, simplement répétées dans cette section qui décrit les scripts.

ManageCertAuthority.sh et ManageCertAuthority.cmd

Argument	Description

-a, -r, -d	Opération à effectuer : -a add -l list -d delete L'option –l ne prend aucun argument supplémentaire. L'option -d prend un seul argument : l'ID objet de l'enregistrement à supprimer
Name	Nom de l'autorité. Obligatoire avec l'argument -a.
Modified_by	Utilisateur ayant modifié ou créé l'identité. Obligatoire avec l'argument -a.
Hash_alg	Algorithme de hachage de l'autorité. Seule la valeur "SHA1" est prise en charge. Obligatoire avec l'argument -a.
Certificate_id	ID objet du certificat d'autorité de certification associé à l'autorité. Obligatoire avec l'argument -a.
OCSP_policy	Chaîne de la stratégie OCSP de l'autorité. Il s'agit d'une chaîne délimitée par des virgules, comme indiqué dans la section sur la table CERT_AUTHORITY. Obligatoire avec l'argument -a. Pour le premier élément de la chaîne, les paramètres suivants sont autorisés : • never : ne jamais utiliser OCSP. • resp : utiliser OCSP uniquement si un répondeur est configuré lorsqu'une demande est effectuée. • always : toujours utiliser OCSP lorsqu'une demande est effectuée. Ce paramètre nécessite la configuration d'un répondeur ; dans l e cas contraire, la vérification du certificat échoue. Pour le second élément de la chaîne, les paramètres suivants sont autorisés : **OCSP_What** • none : ne jamais vérifier les certificats • end-user : vérifier uniquement les certificats de l'utilisateur final • both : vérifier les certificats intermédiaires et les certificats de l'utilisateur final. Cet argument n'est pas pris en charge actuellement. Exemples : • never,none • always,end-user

Crl_policy	Chaîne de la stratégie de liste de révocation de certificat pour l'autorité. Obligatoire avec l'argument -a. Une valeur est requise pour cet argument, mais elle n'est pas actuellement utilisée. La valeur "None" est acceptable.
Object_ID	ID objet à utiliser lors de la création de cet enregistrement. Facultatif avec l'argument -a.

ManageOCSPResponder.sh et ManageOCSPResponder.cmd

Argument	Description
-l	Extrait une liste des répondeurs OCSP actuellement configurés. Cette option ne prend aucun argument supplémentaire.
-d	Supprime la configuration du répondeur OCSP avec l'ID objet fourni pour les données de configuration des répondeurs. Cette option prend object_id comme argument supplémentaire.
-u2	Met à jour les enregistrements existants dans la base de données avec les informations correctes sur la clé publique du certificat d'autorité et le nom distinctif de l'objet de l'autorité de certification. Cette option doit être exécutée sur tous les enregistrements existants des répondeurs OCSP et de l'autorité de certification ; sinon vous devez supprimer et recréer les enregistrements pour obtenir les informations correctes dans la base de données. Cette option prend object_id comme argument supplémentaire.
-a	Ajoute les données de configuration d'un nouveau répondeur OCSP qui sera utilisé pour vérifier l'état des certificats émis par l'autorité indiquée. Les arguments supplémentaires sont name, modified_by, hash_alg, authority_cert_oid, response_signing_cert_oid, resp_signing_cert_in_ca_store, cache_ttl, trans_prof_oid, comm_bp, comm_wait, send_nonce, require_nonce et object_id.
name	(Obligatoire avec l'argument -a) Nom de l'autorité.
modified_by	(Obligatoire avec l'argument -a) Utilisateur ayant modifié ou créé l'identité.

hash_alg	(Obligatoire avec l'argument -a) Algorithme de hachage pour l'autorité. Seule la valeur "SHA1" est prise en charge.
authority_cert_oid	(Obligatoire avec l'argument -a) ID objet du certificat d'autorité de certification associé à l'autorité.
response_signing_cert_oid	(Obligatoire avec l'argument -a) ID objet du certificat que le fournisseur de services OCSP a utilisé pour signer la réponse en indiquant l'état des certificats. Ce certificat doit être ajouté au magasin de certificats numériques de l'autorité de certification ou au magasin de certificats numériques accrédités. Il s'agit de l'ID certificat de système du certificat tel qu'il apparaît dans le magasin.
resp_signing_cert_in_ca_store	(Obligatoire avec l'argument -a) Indicateur précisant si la valeur précédente de l'argument response_signing_cert_oid est introuvable dans le magasin de certificats numériques d'autorité de certification dans Sterling B2B Integrator.
cache_ttl	(Obligatoire avec l'argument -a) Durée de vie, en secondes, des réponses OCSP dans le cache interne.
trans_prof_oid	(Obligatoire avec l'argument -a) ID objet d'un transport configuré pour communiquer avec le répondeur OCSP.
comm_bp	(Obligatoire avec l'argument -a) Nom d'un processus technique utilisé pour communiquer avec le répondeur OCSP. Ce processus technique doit être capable d'assurer les communications HTTP. Les services qu'il propose doivent être configurés pour ne pas exiger ou présenter des en-têtes HTTP lors de l'envoi et de la réception, respectivement. Le processus HTTPClientSend fourni avec le système peut être utilisé et il est recommandé.
comm_wait	(Obligatoire avec l'argument -a) Nombre de secondes d'attente pour établir la communication avec le répondeur OCSP avant le signalement d'une erreur.
send_nonce	(Obligatoire avec l'argument -a) Indique si une valeur NONCE sera envoyée au service OCSP. La valeur NONCE est utilisée pour empêcher les attaques de réexécution par certains fournisseurs OCSP.
require_nonce	(Obligatoire avec l'argument -a) Indique si le serveur doit exiger que le service OCSP fournisse une valeur NONCE dans la réponse.
object_id	(Obligatoire avec l'argument -a) ID objet à utiliser lors de la création de cet enregistrement.

SetSystemCertOCSPInfo.sh et SetSystemCerOCSPInfo.cmd

Cet utilitaire définit les informations OCSP dans la base de données pour un certificat de système unique.

Argument	Description
-o, -n	Indique comment interpréter le second argument : -o object_ID -n name
Object_ID/Name	ID objet ou nom de l'autorité, comme indiqué par l'argument 1.

SetSystemCertOCSPInfo.sh et SetTrustedCertOCSPInfo.cmd

Cet utilitaire définit les informations OCSP dans la base de données pour un certificat de système unique.

Argument	Description
-o, -n	Indique comment interpréter le second argument : -o object_ID -n name
Object_ID/Name	ID objet ou nom de l'autorité, comme indiqué par l'argument 1.

Exécution d'un script OCSP

L'exemple suivant montre comment exécuter les scripts de configuration OCSP. Les scripts partent du principe que vous avez déjà archivé les certificats des autorités de certification pour l'autorité, démarré la base de données, et que vous vous trouvez dans le répertoire bin d'installation de Sterling B2B Integrator et avez sourcé le fichier tmp.sh dans le répertoire bin.

Pourquoi et quand exécuter cette tâche

Après avoir obtenu l'ID d'objet du certificat de l'autorité de certification, dans Sterling B2B Integrator, dans le menu **Administration**, sélectionnez **Partenaires commerciaux > Certificats numériques - Autorité de certification**. Sélectionnez un certificat. La boîte de dialogue Récapitulatif de certificat s'affiche avec les informations du certificat, y compris son ID objet.

Pour exécuter un script OCSP, procédez comme suit. Pour la liste complète des commandes de script OCSP, voir «Scripts de configuration OCSP», à la page 87.

Procédure

1. Exécutez une commande similaire à la suivante pour créer une autorité dans le système :

   ```
   ./ManageCertAuthority.sh -a VPCA admin SHA1 "sedna:a1807c:11dc6d53ba4:-7b4b"
    "always,end-user" "none"
   ```

2. Après avoir créé une autorité et un profil pour communiquer avec un canal répondeur OCSP, exécutez une commande similaire à la suivante pour créer un canal répondeur OCSP dans le système :

```
./ManageOCSPResponder.sh -a CertAuth_TestOCSP admin SHA1
"kenny:node1:13727b3f8e4:29762" "kenny:node1:13727275fd9:40698" false (utilisez
true si le certificat signataire enregistré
est identique au certificat de réponse, c'est à dire restitué à
l'autorité de certification dans l'étape 3) "2400" "14ffd4a0:1371823040d:-77c8"
HTTPClientSend 3600 false false
```

3. Exécutez une commande similaire à la suivante pour répertorier toutes les autorités dans le système :

   ```
   ./ManageCertAuthority.sh -l
   ```

   Le retour de sortie pour chaque autorité s'affiche :

   ```
   CERT_AUTHORITY:
   OBJECT_ID: sedna:1ded0fd:11dc9d22929:-7fbd
   NAME: VPCA
   CREATE_DATE: 2008-11-23
   MODIFIED_DATE: 2008-11-23
   MODIFIED_BY: null
   ISSUER_NAME: Country=US, StateOrProvince=Dublin, OrganizationUnit=GIS
    Development, Organization=Sterling,
   CommonName=Test CA
   HASH_ALG: SHA1
   RDN_HASH: 24E63F8AE9F51497529EA0CC34467A4680737A9F
   ENCODED_RDN_HASH: JOY/iun1FJdSnqDMNEZ6RoBzep8=
   KEY_HASH: C96F2FF442EBFA07672DCEC49B729D4D24898313
   ENCODED_KEY_HASH: yW8v9ELr+gdnLc7Em3KdTSSJgxM=
   CERT_OID: sedna:a1807c:11dc6d53ba4:-7b4b
   OCSP_WHEN_POLICY: always
   OCSP_WHAT_POLICY: end-user
   CRL_POLICY: null
   ```

4. Exécutez une commande similaire à la suivante afin d'activer OCSP pour tous les certificats de confiance et de système émis par l'autorité :

   ```
   ./SetAuthorityCertsOCSPInfo.sh -o sedna:1ded0fd:11dc9d22929:-7fbd yes
   ```

Logique de vérification OCSP

Les étapes suivantes décrivent la logique de vérification OCSP dans Sterling B2B Integrator. Si le statut du certificat est OK, la vérification OCSP aboutit. Dans le cas contraire, elle échoue.

Procédure

1. Si une réponse existante dont le délai d'expiration n'a pas été atteint est détectée, elle est utilisée en tant que réponse OCSP.
2. Si aucune réponse existante n'a été trouvée dans la mémoire cache ou si le délai d'expiration pour la réponse dans la mémoire cache a été atteint, une demande OCSP est créée.
3. Si le système crée une demande OCSP, il lance le processus technique configuré pour le répondeur OCSP, qui consiste à envoyer la demande et à obtenir la réponse. Les demandes incluront une valeur nonce si le répondeur a été configuré pour envoyer une demande.
4. Si le processus technique est exécuté correctement, le système tente d'analyser son document principal en tant que réponse OCSP. Le processus technique utilisé pour envoyer des demandes OCSP et recevoir des réponses OCSP supprime les en-têtes HTTP de la réponse.
5. Si le document principal peut être analysé comme étant une réponse OCSP, le système vérifie l'état de la réponse.
6. Si l'état de la réponse indique que la demande a généré une réponse valide, le système vérifie la signature sur la réponse OCSP à l'aide du certificat configuré pour le répondeur OCSP.

7. Si la signature est vérifiée et que le répondeur a été configuré pour exiger la valeur nonce, le système tente de trouver et d'extraire cette valeur de la réponse.
8. Si toutes les autres vérifications ont abouti, le système recherche les informations d'état du certificat pour lequel la demande a été créée et envoyée.
9. S'il trouve les informations d'état, le système met à jour la mémoire cache interne concernant une réponse OCSP existante pour le certificat.

Norme FIPS (Federal Information Processing Standards)

Norme FIPS (Federal Information Processing Standards) 140-2

Pour se conformer aux exigences de sécurité FIPS 200, les applications doivent utiliser des modules cryptographiques certifiés par le programme CMVP (Cryptographic Module Validation Program) et compatibles avec FIPS 140-1 ou 140-2.

La configuration minimale requise pour l'utilisation de la cryptographie validée par les applications est la suivante :

- Toutes les opérations cryptographiques, y compris la génération de clés, doivent être effectuées par des modules cryptographiques validés.
- Seules les fonctions de sécurité accréditées sont autorisées.
- Seules les techniques d'établissement de clés accréditées sont autorisées.

FIPS 140-2 avec Sterling B2B Integrator

GSE (Government Service Edition) Certicom est un module de chiffrement certifié FIPS 140-2 de niveau 1 distribué avec Sterling B2B Integrator. GSE est un kit d'outils de chiffrement de bas niveau en langage Java qui implémente diverses fonctions de sécurité, notamment des fonctions de sécurité accréditées.

En mode FIPS, ce kit effectue les tâches suivantes :

- Activation de la machine d'état FIPS GSE et appel des auto-tests de mise sous tension.
- Copie les appels de la fonction de chiffrement du système principal dans GSE.

Activation du mode FIPS au cours de l'installation

Lorsque, au cours d'une nouvelle installation, vous êtes invité à activer l'exécution en mode FIPS, sélectionnez TRUE.

Activation manuelle du mode FIPS

Vous pouvez activer le mode FIPS manuellement après l'installation de Sterling B2B Integrator. Avant de commencer, vérifiez que vous disposez d'une licence pour travailler en mode FIPS. Votre licence est vérifiée au démarrage et ne démarre pas si le mode FIPS est activé mais n'est pas sous licence.

Pourquoi et quand exécuter cette tâche

Pour activer manuellement le mode FIPS :

Procédure

1. Accédez au répertoire */rép_install*/properties/.
2. Localisez le fichier security.properties.

3. Ouvrez le fichier security.properties dans un éditeur de texte. Si vous apportez des modifications au fichier security.properties, veillez à apporter les mêmes modifications au fichier security.properties.in. Ceci empêchera vos paramètres personnalisés d'être écrasés. Vous devez utiliser le fichier de propriétés de sécurité afin de personnaliser FIPS au lieu d'éditer directement les fichiers de propriétés.
4. Spécifiez les configurations suivantes : FIPSMode=true
5. Enregistrez et fermez le fichier security.properties.
6. Redémarrez Sterling B2B Integrator. Le redémarrage est indispensable pour que les modifications soient prises en compte dans le système.

Désactivation du mode FIPS

Vous pouvez désactiver manuellement le mode FIPS.

Pourquoi et quand exécuter cette tâche

Pour désactiver manuellement le mode FIPS :

Procédure

1. Accédez au répertoire */rép_install*/properties/.
2. Localisez le fichier security.properties.
3. Ouvrez le fichier security.properties dans un éditeur de texte.
4. Spécifiez les configurations suivantes : FIPSMode=false
5. Enregistrez et fermez le fichier security.properties.
6. Redémarrez Sterling B2B Integrator. Le redémarrage est indispensable pour que les modifications soient prises en compte dans le système.

Serveurs proxy

Serveurs proxy

Les serveurs proxy améliorent la sécurité de votre système.

Configuration d'un serveur proxy HTTP

Vous pouvez configurer un serveur proxy HTTP à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour configurer un serveur proxy HTTP :

Procédure

1. Dans le menu **Administration**, sélectionnez **Opérations** > **Serveurs proxy**.
2. Cliquez sur **Ajouter**.
3. Entrez le **Nom** du serveur proxy.
4. Sélectionnez **HTTP** comme **Type**.
5. Entrez le nom de l'**Hôte**. Les adresses IPv6 doivent être placées entre crochets.
6. Entrez le numéro de **Port**.
7. Entrez le **Nombre de nouveaux essais**.
8. Cliquez sur **Suivant**.
9. Si vous souhaitez requérir l'authentification de base pour l'utilisateur :

- Sélectionnez **Oui** et cliquez sur **Suivant**.
- Si l'option sélectionnée est Non (par défaut), cliquez sur **Suivant** et passez à l'étape 13.

10. Entrez l'**ID utilisateur auth**.
11. Entrez le **Mot de passe auth**.
12. Cliquez sur **Suivant**.
13. Passez en revue les paramètres de serveur proxy.
14. Cliquez sur **Terminer**.

Configuration d'un serveur proxy SSP

Vous pouvez configurer un serveur proxy SSP à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour configurer un serveur proxy SSP :

Procédure

1. Dans le menu **Administration**, sélectionnez **Opérations** > **Serveurs proxy**.
2. Cliquez sur **Ajouter**.
3. Entrez le **Nom** du serveur proxy.
4. Sélectionnez **SSP** comme **Type**.
5. Entrez le nom de l'**Hôte**. Les adresses IPv6 doivent être placées entre crochets.
6. Entrez le numéro de **Port**.
7. Entrez le **Nombre de nouveaux essais**.
8. Cliquez sur **Suivant**.
9. L'authentification de base est-elle requise pour l'utilisateur ?, sélectionnez Oui ou Non.
10. La couche SSL est-elle requise ?, sélectionnez Oui ou Non.
11. Cliquez sur **Suivant**.
12. Si vous avez sélectionné l'autorisation de base pour cet utilisateur, vous devez entrer l'**ID utilisateur d'autorisation** et le **Mot de passe d'autorisation**, puis cliquez sur **Suivant**. Si vous n'avez pas besoin de cette autorisation, cette page n'est pas affichée.
13. Si vous sélectionnez Oui pour l'option SSL obligatoire, vous devez sélectionner les options **Puissance de chiffrement**, **Certificats de l'autorité de certification** et **Certificats de clé**, puis cliquez sur **Suivant**. Si vous n'avez pas besoin de SSL, cette page n'est pas affichée.
14. Cliquez sur **Suivant**.
15. Passez en revue les paramètres de serveur proxy.
16. Cliquez sur **Terminer**.

Configuration un serveur proxy pour SSL

Vous pouvez utiliser le protocole SSL avec votre configuration de serveur proxy SSP en créant ou en important un certificat SSL et en définissant la zone **Utiliser SSL** dans la configuration d'adaptateur appropriée sur **Obligatoire**.

Pourquoi et quand exécuter cette tâche

Si vous décidez d'utiliser SSL avec votre configuration de serveur proxy SSP, vous devez :

Procédure

1. Créer un certificat SSL ou importer le certificat de votre autorité de certification dans Sterling B2B Integrator.
2. Attribuer à la zone **Utiliser SSL** dans la configuration d'adaptateur appropriée la valeur **Doit**.

Édition des serveurs proxy

Vous pouvez éditer une configuration de serveur proxy à partir du menu **Administration**.

Pourquoi et quand exécuter cette tâche

Pour éditer une configuration de serveurs proxy :

Procédure

1. Dans le menu **Administration**, sélectionnez **Opérations** > **Serveurs proxy**.
2. Cliquez sur **Modifier** en regard du serveur proxy que vous voulez éditer.
3. Mettez à jour les zones, le cas échéant.
4. Cliquez sur **Suivant**.
5. Passez en revue les paramètres de serveur proxy.
6. Cliquez sur **Terminer**.

Suppression des serveurs proxy

Pourquoi et quand exécuter cette tâche

La suppression d'une configuration de serveur proxy peut provoquer des erreurs dans certaines fonctions de Sterling B2B Integrator. Vous devrez peut-être reconfigurer des adaptateurs et services spécifiques pour qu'ils fonctionnent correctement sans configuration de serveur proxy spécifique.

Pour éditer une configuration de serveurs proxy :

Procédure

1. Dans le menu **Administration**, sélectionnez **Opérations** > **Serveurs proxy**.
2. Cliquez sur **Supprimer** en regard du serveur proxy que vous voulez modifier.
3. Passez en revue les paramètres de serveur proxy.
4. Cliquez sur **Supprimer**.

SSL

À propos de l'implémentation de SSL dans Sterling B2B Integrator

Secure Sockets Layer (SSL) offre une communication sécurisée via Internet. Il utilise à la fois une cryptographie symétrique et asymétrique.

Le protocole de sécurité SSL fournit l'authentification du serveur et du client dans Sterling B2B Integrator :

- L'authentification du serveur est effectuée lorsqu'un client se connecte au serveur. Une fois l'établissement de la liaison initiale terminée, le serveur envoie son certificat numérique au client. Le client valide le certificat serveur ou la chaîne de certificats.
- L'authentification du client est effectuée lorsqu'un serveur envoie une demande de certificat à un client au cours de l'établissement de la liaison. Si le certificat client ou la chaîne de certificats est vérifié et que le message de vérification du certificat est à son tour approuvé, l'établissement de la liaison se poursuit.
- Une authentification supplémentaire facultative est effectuée : le nom commun dans le certificat est comparé au nom de domaine complet du serveur, par le biais d'une recherche inversée dans le DNS où le nom de domaine complet du serveur peut être obtenu.

Types d'accréditation

Deux types d'accréditation des certificats SSL sont pris en charge par Sterling B2B Integrator :

- Accréditation de l'autorité de certification : accréditation hiérarchique basée sur un certificat racine utilisé pour émettre d'autres certificats. IL s'agit du modèle d'accréditation des certificats SSL standard.
- Accréditation directe : accréditation directe des certificats autosignés supposés être distribués via des mécanismes externes sécurisés. Les certificats autosignés et d'accréditation directe ne font pas partie des normes SSL mais sont souvent utilisés dans certaines communautés commerciales.

Certificats SSL

Pour communiquer via le protocole SSL, configurez les systèmes concernés pour prendre en charge l'authentification serveur ou l'authentification client-serveur. Pour effectuer l'authentification sur un serveur, vous devez disposer d'un certificat d'autorité de certification racine et de l'ensemble des certificats intermédiaires de la chaîne ou bien, si le serveur utilise un certificat autosigné, d'une copie du certificat autosigné.

Pour que l'authentification client-serveur soit prise en charge, vous devez disposer d'un certificat autosigné ou émis par une autorité de certification, et d'un certificat de système.

Vous pouvez obtenir un certificat SSL auprès d'une autorité de certification digne de confiance en fournissant une demande de signature de certificat (CSR) à l'autorité de certification. Le certificat SSL lie la clé publique et le serveur ou le client SSL.

Si vous prévoyez d'utiliser l'authentification client-serveur, configurez un certificat de système. Vous pouvez créer des certificats de système de l'une des manières suivantes :

- Archiver un fichier de certificat de clé existant ou un fichier PKCS12.
- Générer un certificat de système autosigné.
- Utiliser Key Management Utility (iKeyman) pour générer une demande de signature de certificat auprès d'une autorité de certification. Pour plus d'informations sur iKeyman, voir «IBM Key Management Utility (iKeyman)», à la page 65.

Algorithmes de cryptographie

Avant d'utiliser Sterling B2B Integrator, vous devez vérifier les listes d'algorithmes de cryptographie prédéfinis et les personnaliser selon les exigences de sécurité de votre entreprise.

Les algorithmes de cryptographie IBM SDK, Java Technology Edition version 7 sont disponibles à l'adresse suivante : http://www-01.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/ciphersuites.html. Pour les autres kits Java Development Kit pris en charge dans Sterling B2B Integrator, voir la documentation du fournisseur JDK pour connaître la liste des algorithmes de chiffrement pris en charge.

Les puissances de chiffrement sont configurées dans `security.properties` ou dans `customer_overrides.properties`. Voici les niveaux des algorithmes de cryptographie disponibles :

- AllCipherSuite (la sélection de l'interface utilisateur est **ALL**) - inclut tous les éléments répertoriés dans WEAK et STRONG.
- WeakCipherSuite (la sélection de l'interface utilisateur est **WEAK**) - ajouter les algorithmes de cryptographie faible pris en charge à utiliser avec Sterling B2B Integrator
- StrongCipherSuite (la sélection de l'interface utilisateur est **STRONG**) - ajouter les algorithmes de cryptographie forte pris en charge à utiliser avec Sterling B2B Integrator
- CipherSuiteDefault (disponible dans la version 5.2.6 et ultérieure) - par défaut, inclut un sous-ensemble de chiffrement pris en charge pour IBM JDK7. Utilisé si WeakCipherSuite et StrongCipherSuite sont vides.

Adaptateurs de client pour la couche SSL

L'adaptateur de client FTP, l'adaptateur de client HTTP et l'adaptateur de demandeur Sterling Connect:Direct FTP+ (avec l'option Secure+) prennent en charge la couche SSL.

Les adaptateurs de client suivants prennent en charge la couche SSL :

- Adaptateur de client FTP
- Adaptateur de client HTTP
- Adaptateur de demandeur Sterling Connect:Direct FTP+ (avec l'option Secure+)

Les paramètres de la couche SSL peuvent être définis dans le profil de partenaire commercial ou pour l'adaptateur. Dans le cas de l'adaptateur de client FTP, ces paramètres sont définis dans le service Début de session du client FTP. Dans le cas de l'adaptateur de client HTTP, ces paramètres sont définis dans le service Début de session du client HTTP. Les paramètres définis dans le service Début de session se substituent aux paramètres définis dans un profil de partenaire commercial.

Les paramètres indiqués dans le tableau suivant contrôlent la couche SSL d'une perspective client. Reportez-vous à la documentation de l'adaptateur ou du service spécifique que vous configurez.

Paramètre	Description
SSL	Détermine une négociation de socket SSL.

Paramètre	Description
IDCertificatCA (trusted_root)	Liste des certificats publics de confiance d'autorités de certification. Dans les données de processus, ce paramètre est affiché sous la forme d'un ID objet.
CipherStrength	Niveau de chiffrement à appliquer aux données qui transitent par la connexion socket.
SystemCertificateId	Effectuez une sélection dans la liste des certificats de système disponibles. Ce certificat confirme l'identité du client pour le serveur.

Adaptateurs de serveur pour la couche SSL

L'adaptateur de serveur FTP, l'adaptateur de serveur HTTP et l'adaptateur de serveur Sterling Connect:Direct (avec Secure+ Option) et l'adaptateur d'envoi SMTP prennent en charge la couche SSL.

Les adaptateurs de serveur suivants prennent en charge la couche SSL :

- Adaptateur de serveur FTP
- Adaptateur de serveur HTTP
- Adaptateur de serveur Sterling Connect:Direct (avec l'option Secure+)
- Adaptateur d'envoi SMTP

Les paramètres figurant dans le tableau suivant contrôlent la couche SSL d'une perspective serveur. Reportez-vous à la documentation de l'adaptateur ou du service spécifique que vous configurez.

Paramètre	Description
SSL	Indique si la couche SSL (Secure Sockets Layer) est active.
Phrase passe du certificat de clé	Mot de passe qui protège le certificat de clé de licence serveur. Cette phrase passe est utilisée en interne par le système afin d'initialiser les bibliothèques SSL.
CipherStrength	Puissance des algorithmes utilisés pour chiffrer les données.
Certificat de clé (magasin système)	Clé privée et certificat pour authentification de serveur.
Certificat de l'autorité de certification	Certificat utilisé, le cas échéant, pour valider le certificat d'un client.

Restitution d'un certificat

Pour que l'authentification client-serveur soit prise en charge, vous devez disposer d'un certificat autosigné, ou émis par une autorité de certification, et d'un certificat système.

Pourquoi et quand exécuter cette tâche

Vous pouvez enregistrer un certificat d'autorité de certification ou autosigné dans un magasin de certificats d'autorité de certification en sélectionnant **Partenaire commercial** > **Certificats numériques** > **Autorité de certification** > **Restituer le nouveau certificat** dans le menu **Administration**.

Création de certificats autosignés à des fins de test

Vous pouvez utiliser des certificats autosignés à des fins de test. Ces certificats peuvent être générés et gérés dans Sterling B2B Integrator.

Pourquoi et quand exécuter cette tâche

Pour créer un certificat autosigné :

Procédure

1. Sélectionnez **Partenaires commerciaux** > **Certificats numériques** > **Certificats de système** > **Créer certificat autosigné**.
2. Une fois le certificat créé, localisez-le et archivez-le dans un fichier.
3. Archivez à nouveau le certificat dans Sterling B2B Integrator en tant que certificat d'autorité de certification en sélectionnant **Partenaires commerciaux** > **Certificats numériques** > **Autorité de certification** > **Restituer le nouveau certificat**.

Renégociation SSL/TLS (version 5.2.6 ou ultérieure)

Sterling B2B Integrator utilise les paramètres IBM JSSE pour contrôler les restrictions de renégociation SSL/TLS. Les paramètres suivants sont disponibles pour être mis à jour dans le fichier `security.properties`.

Nom du paramètre	Définition	Valeurs valides
com.ibm.jsse2. extended. renegotiation.indicator	Utilisez cette propriété pour forcer toutes les négociations à exiger RFC 5746, et pas seulement des renégociations. Cette négociation n'est utile que si tous les partenaires de communication requis ont implémenté RFC 5746. La valeur par défaut est OPTIONAL.	Les valeurs valides sont les suivantes : • BOTH - Provoque la connexion du serveur IBM JSSE2 ou du client IBM JSSE2 uniquement si l'homologue indiqué prend en charge la renégociation RFC 5746. Remarque : Si vous définissez la propriété sur BOTH, des problèmes d'interopérabilité peuvent survenir avec les clients ou les serveurs qui n'ont pas été mis à jour pour prendre en charge RFC 5746. • CLIENT - Provoque la connexion du client IBM JSSE2 uniquement si le serveur indiqué prend en charge la renégociation RFC 5746. Remarque : Si vous définissez la propriété sur CLIENT, des problèmes d'interopérabilité peuvent survenir avec les serveurs qui n'ont pas été mis à jour pour prendre en charge RFC 5746. • OPTIONAL - Cette valeur est la valeur par défaut. L'utilisation de cette option signifie que le serveur IBM JSSE2 ou le client IBM JSSE2 ne nécessite pas l'indicateur de renégociation pendant l'établissement de liaison initial. • SERVER - Provoque la connexion du serveur IBM JSSE2 uniquement si le client indiqué prend en charge la renégociation RFC 5746. Remarque : Si vous définissez la propriété sur SERVER, des problèmes d'interopérabilité peuvent survenir avec les clients qui n'ont pas été mis à jour pour prendre en charge RFC 5746.

Nom du paramètre	Définition	Valeurs valides
com.ibm.jsse2.renegotiate	Utilisez cette propriété pour modifier la capacité de renégociation d'IBM JSSE2. La valeur par défaut est NONE.	Les valeurs valides sont les suivantes : • ABBREVIATED - Cette valeur remplace et permet un établissement de liaison abrégé non sécurisé lors de la renégociation lorsque la continuité de la session est éprouvée. Les renégociations RFC 5746 sont autorisées. • ALL - Cette valeur remplace et permet un établissement de liaison complet non sécurisé, et un établissement de liaison abrégé non sécurisé, au cours de la renégociation. Les renégociations RFC 5746 sont autorisées. • DISABLED - Cette valeur remplace et désactive toutes les renégociations non sécurisées et RFC 5746. • NONE - Cette valeur est la valeur par défaut. Aucune renégociation non sécurisée n'est autorisée. Seules les renégociations RFC 5746 sont autorisées.
com.ibm.jsse2. renegotiation .peer.cert.check	Utilisez cette propriété pour modifier la capacité de renégociation d'IBM JSSE2 pour exiger la prise en charge homologue qui est définie dans RFC 5746. Cette négociation n'est utile que si tous les partenaires de communication requis ont implémenté RFC 5746. La valeur par défaut est OFF.	Les valeurs valides sont les suivantes : • OFF - Cette valeur est la valeur par défaut. Elle empêche le client IBM JSSE2 ou le serveur IBM JSSE2 d'effectuer un contrôle d'identité du certificat homologue. Le résultat consiste à permettre au certificat homologue de changer pendant la renégociation. • ON - Cette valeur entraîne le client IBM JSSE2 ou le serveur IBM JSSE2 à effectuer une comparaison avec le certificat homologue. L'objectif est de garantir que le certificat ne change pas pendant la renégociation. La comparaison est applicable aux renégociations tant sécurisées que non sécurisées.

Traitement des incidents liés à la couche SSL

Si vous recevez un message d'erreur, vous pouvez traiter les incidents liés à la couche SSL.

Messages d'erreur signalant des certificats inutilisables ou endommagés

Si le message d'erreur suivant s'affiche :

```
FATAL Alert:BAD_CERTIFICATE - A corrupt or unusable certificate was
received.
```

Les informations extraites du journal de périphérie sont les suivantes :

```
ERROR <HTTPClientAdapter_HTTPClientAdapter_node1-Thread-19>
HTTPClientAdapter_HTTPClientAdapter_node1-Thread-172105824724com.
sterlingcommerce.perimeter.api.conduit.SSLByteDataConduit@4c2b95c6:
Doing reset3 c
om.certicom.net.ssl.SSLKeyException: FATAL Alert:BAD_CERTIFICATE -
A corrupt or unusable certificate was received.
 at com.certicom.tls.d.b.a(Unknown Source)
 at com.certicom.tls.d.b.do(Unknown Source)
```

Lors de l'archivage du certificat, Sterling B2B Integrator affiche une valeur d'état de "signature non valide" sur l'écran de désignation. Si un processus technique exécutant une commande HTTP POST sortante via SSL échoue sur le service Méthode HTTP avec une erreur, le message suivant s'affiche :

```
HTTP Status Code: -1
HTTP Reason Phrase: Internal Error: Connection was closed from the
perimeter side with error: CloseCode.CONNECTION_RESET
```

Obtenez le certificat d'autorité de certification approprié auprès de votre partenaire commercial. Si le partenaire commercial utilise un certificat autosigné, le certificat lui-même peut faire office de certificat d'autorité de certification.

Autorité de certification et accréditation directe

Lorsque Sterling B2B Integrator est le client, si le serveur possède un certificat émis par une autorité de certification et qui comporte le nom DNS du serveur dans le sujet Nom distinctif relatif (RDN), vous pouvez placer le certificat d'autorité de certification racine dans le magasin de certification et d'accréditation. Si SSL ne fonctionne toujours pas, essayez l'accréditation directe. Placez le certificat serveur dans le magasin de certification et d'accréditation.

Si le serveur utilise un certificat autosigné, placez-le dans le magasin de certification et d'accréditation. Dans ce cas également, l'accréditation est directe.

Utilisation de SSL sans certificat

Vous ne pouvez pas utiliser les adaptateurs activés pour SSL sans le certificat ou le certificat de système requis.

SSL ne fonctionne pas avec un algorithmes de cryptographie basé sur CBC

Si vous avez sélectionné l'algorithme de cryptographie en mode CBC et que SSL ne fonctionne pas, vous devez désactiver la protection CBC.

Pour la version 5.2.5 et antérieure, procédez comme suit :

1. Ouvrez le fichier tmp.sh pour l'éditer.
2. Recherchez l'indicateur de serveur correspondant au système d'exploitation que vous configurez et ajoutez la valeur suivante :

   ```
   -DDisableSSLEmptyRecords=true
   ```
3. Enregistrez et fermez le fichier.

Pour la version 5.2.6 et ultérieure, procédez comme suit :

1. Dans le répertoire *<B2Bi Install>*/bin, localisez `InstallNoappsWindowsService.cmd.in` et `InstallContainerWindowsService.cmd.in` pour Windows ; localisez `tmp.sh_platform_ifcresources_ext.in` pour tous les autres systèmes d'exploitation.
2. Editez le fichier pour changer toutes les instances de la propriété suivante sur false :

   ```
   jsse.enableCBCProtection=true
   ```
3. Exécutez le script `setupfiles`.

Configuration HTTPS pour le modélisateur GPM

L'accès HTTP sécurisé via SSL est déjà pris en charge pour la plupart des applications Web de Sterling B2B Integrator sur le port HTTP de base + 1.

Cette amélioration SSL :

- Active HTTPS (le chiffrement HTTP sur SSL) pour le modélisateur GPM (Graphical Process Modeler)
- Désactive et réachemine les applications Web situées sur le port HTTP de base vers un autre port (via HTTPS).
- Prend en charge l'accès sécurisé aux applications Web par le déploiement des applications Web sur une instance d'adaptateur de serveur HTTP sécurisée.
- Réduit les risques de sécurité.

Si vous utilisez cette fonction, vous devrez configurer le modélisateur GPM (Graphical Process Modeler) pour communiquer avec l'application Web de tableau de bord via HTTPS et non via HTTP. L'accès aux applications Web déployées par le biais d'un adaptateur de serveur HTTP sécurisé peut être plus lent qu'un accès sur le port de base.

Remarque : Dans la version 5.2.6 et ultérieure, le protocole de sécurité par défaut est TLS 1.2 (pour le port HTTP de base + 1.). Si nécessaire, vous pouvez modifier ce paramètre en TLS 1.1 ou TLS 1.0 en mettant à jour le paramètre **`jsseProtocol`** dans `properties_platform_ifcresources_ext`. Les valeurs admises sont :

- **`TLS1-TLS1.1`** - pour TLS1.0 et TLS1.1
- **`TLS1.1-TLS1.2`** - pour TLS1.1 et TLS1.2
- **`TLS1`** - pour TLS1.0 uniquement
- **`TLS1.1`** pour TLS1.1 uniquement

- **TLS1.2** - pour TLS1.2 uniquement

Nouveaux paramètres SSL

De nouveaux paramètres ont été ajoutés à la fonction SSL étendue. Vous devez les configurer pour faciliter la communication SSL entre la fonction GPM (Graphical Process Modeler) et le serveur. Ces nouveaux paramètres doivent être définis dans leurs fichiers de propriétés respectifs.

Toutes les propriétés personnalisées pour votre environnement doivent être définies dans le fichier customer_overrides.properties afin de ne pas être écrasées lors de l'installation de mises à niveau ou de correctifs. Les propriétés définies dans le fichier sandbox.cfg ne doivent pas être définies dans le fichier customer_overrides.properties puisqu'elles seront ignorées dans le fichier customer_overrides.properties. Ces propriétés sont les seules qui ne soient pas définies dans le fichier customer_overrides.properties.

Le tableau suivant décrit les nouveaux paramètres SSL et indique le nom du fichier de propriétés dans lequel le paramètre est stocké.

Nom du paramètre	Définition	Fichier de propriétés
WEBAPP_LIST_PORT	Identifie le port que le client GPM doit utiliser pour communiquer avec le serveur. Ce paramètre prend par défaut le port de base au cours de l'installation. Si les applications Web Tableau de bord et GPM ont été déployées sur une instance de l'adaptateur de serveur HTTP sécurisé, ce paramètre doit être modifié pour correspondre au port de cette instance. Si le port SSL de base (port HTTP de base +1) est utilisé pour le déploiement sécurisé des applications GPM et Tableau de bord, ce paramètre doit être modifié pour correspondre au port SSL de base (PORT_SSL dans le fichier sandbox.cfg).	Fichier sandbox.cfg
WEBAPP_PROTOCOL	Identifie le protocole à utiliser pour communiquer avec l'application Web Tableau de bord (http/https).	Fichier sandbox.cfg

Nom du paramètre	Définition	Fichier de propriétés
SKIP_BASEPORT_ DEPLOYMENT_WARS	Indique quelles applications Web doivent être ignorées lors du déploiement de fichiers war sur le port de base. La liste des fichiers war est délimitée par des virgules, est sensible à la casse et ne comporte pas le suffixe .war. Par défaut, les fichiers war ne sont pas ignorés. Une fois les applications Web Tableau de bord et GPM déployées avec succès sur un adaptateur de serveur HTTP sécurisé, ce paramètre peut être défini sur =admin,dashboard,gbm pour retirer l'accès au port de base pour ces applications web. La liste complète des applications Web comprend : • myaft • portlets La valeur ALL peut être utilisée comme caractère générique pour spécifier que tous les fichiers war déployés sur le port HTTP de base doivent être ignorés. Cette opération peut ne pas être nécessaire si le port de base est bloqué pour l'accès externe. La valeur ALL ne doit pas être utilisée avec une autre valeur.	customer_overrides.properties
HTTPS_REDIRECT_WARS	Indique que les fichiers war seront automatiquement réacheminés du port HTTP de base vers l'adaptateur de serveur HTTP sécurisé ou vers le port SSL de base. La valeur ALL peut être utilisée pour réacheminer tous les fichiers war ignorés sur le port HTTP de base vers HTTPS_LIST_PORT (le port SSL de base ou de l'adaptateur de serveur HTTP sécurisé). La valeur ALL ne doit pas être utilisée avec une autre valeur.	customer_overrides.properties
HTTPS_LIST_PORT	Indique le port de destination de réacheminement pour les demandes effectuées sur le port HTTP de base. Ce paramètre doit être défini sur la valeur de l'adaptateur de serveur HTTP sécurisé ou sur le port SSL de base.	customer_overrides.properties

Nom du paramètre	Définition	Fichier de propriétés
HTTPS_CLIENT_CERTS	Liste séparée par des virgules des certificats de système dont les clés publiques doivent être ajoutées au fichier de clés certifiées par défaut. Ces certificats sont utilisés pour la vérification côté client, au cours de l'établissement de la liaison SSL, lorsque des appels HTTPS sont lancés du serveur ASI vers lui-même. Ce paramètre requiert des clés de certificat serveur possédant un attribut **SubjectAltName**. Si vous utilisez des clés existantes sans ce paramètre, cette fonctionnalité échouera en affichant des messages illisibles. **Remarque :** Le certificat configuré pour HTTPS sur portbase+1 (sslCert) est automatiquement ajouté au fichier de clés certifiées et n'a pas besoin d'être ajouté à cette liste.	customer_overrides.properties

Lorsque vous configurez cette fonction, si vous définissez SKIP_BASEPORT_DEPLOYMENT_WARS, mais pas HTTPS_REDIRECT_WARS ni HTTPS_LIST_PORT, les applications Web sont inaccessibles sur le port de base et l'utilisateur ne sera pas automatiquement réacheminé vers le port HTTPS. Ce scénario est valide si, pour des raisons de sécurité, l'utilisateur préfère ne pas être réacheminé automatiquement. Les applications Web resteront disponibles lors de l'accès à partir de l'adaptateur de serveur HTTP sécurisé ou du port SSL.

Activation de la redirection automatique vers HTTPS

Vous pouvez activer la redirection automatique vers HTTPS.

Pourquoi et quand exécuter cette tâche

Une prise en charge a été ajoutée pour permettre la configuration d'une redirection automatique vers HTTPS des applications Web qui sont déployées sur un port sécurisé (adaptateur de serveur HTTP ou port SSL de base) et ignorées sur le port de base. Cette configuration est facultative, bien que fortement recommandée.

Remarque : Toutes les propriétés personnalisées pour votre environnement doivent être définies dans le fichier customer_overrides.properties afin de ne pas être écrasées lors de l'installation de mises à niveau ou de correctifs.

Pour activer la redirection automatique vers HTTPS :

Procédure

1. Accédez au répertoire `/<rép_install>/install/properties`.
2. Ouvrez le fichier customer_overrides.properties et définissez les valeurs de paramètre suivantes, comme illustré ci-dessous :

```
HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
HTTPS_LIST_PORT=<port_adaptateur_serveur_http ou port_ssl_base>
```

Ces paramètres sont configurés pour rediriger automatiquement l'utilisateur à l'instance HTTPS de l'application Web.

Remarque : Le fichier customer_overrides.properties ne fait pas partie du code système par défaut. Il doit être créé après l'installation initiale du système et renseigné afin de correspondre à votre environnement.

3. Enregistrez et fermez le fichier.

Exemple d'implémentation

Exemple d'implémentation dans le fichier customer_overrides.properties :

```
 ## Identifies wars for auto-redirect to the https port. Utilisez une liste au format csv
## pour spécifier plusieurs fichiers war
HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifie le port https pour les fichiers war redirigés. S'il est spécifié,
## doit correspondre à WEBAPP_LIST_PORT dans le fichier sandbox.cfg
HTTPS_LIST_PORT=<port_adaptateur_serveur_http ou port_ssl_base>
```

Remarque : Si vous utilisez une instance de l'adaptateur de serveur HTTP sécurisée, la configuration impose que tous les fichiers war spécifiés sous la forme HTTPS_REDIRECT_WARS soient déployés sur la même instance de l'adaptateur de serveur HTTP.

HTTPS_CLIENT_CERTS

Si une instance de l'adaptateur Secure HTTP Server est utilisée, le certificat SSL utilisé pour la configurer doit être ajouté dans la liste des certificats accrédités.

Cette opération est nécessaire car certains des écrans du Tableau de bord renvoient les appels HTTP au serveur ASI. Pour que ces appels puissent établir une liaison SSL correctement, les certificats doivent être configurés dans le fichier de clés certifiées sur le serveur ASI. Cette opération peut être effectuée en spécifiant le nom de certificat dans la liste HTTPS_CLIENT_CERTS.

Ces certificats de système doivent posséder les noms DNS et l'adresse(s) IP qui ont été spécifiés en tant que noms secondaires lors de la création des certificats de système. La vérification du nom d'hôte SSL par défaut fournie par le JDK nécessite que le nom du certificat présenté par le serveur SSL corresponde au nom d'hôte utilisé dans l'URL http ou à l'une des chaînes de l'attribut "SubjectAltName" défini dans le certificat. Certains écrans du Tableau de bord ne fonctionneront pas sans la définition de l'attribut "SubjectAltName".

Les noms secondaires sont configurés dans les zones "Liste des adresses IP séparées par des virgules" et "Liste des noms DNS séparés par une virgule" de l'assistant de création de certificats de système (**Partenaire commercial** > **Certificats numériques** > **Système**).

Prise en charge du protocole HTTPS pour l'application GPM

Java Web Start (JavaWS) est utilisé pour lancer l'application GPM (Graphical Process Modeler) via HTTP. Il prend en charge HTTPS et l'importation dynamique de certificats de manière similaire à celle des navigateurs.

Au cours de l'établissement de liaison SSL, le serveur fournit son certificat et JavaWS gère la vérification de la confiance. Si le certificat n'a pas pu être vérifié par JavaWS, l'utilisateur est invité à l'accepter ou à le refuser. Les certificats SSL ne peuvent pas être vérifiés automatiquement par JavaWS et ce sont les utilisateurs qui doivent s'en charger.

Importation des certificats pour Java Web Start

Si vous souhaitez éviter l'affichage d'une invite de certificat non accrédité au cours de l'opération JavaWS (Java Web Start), vous pouvez importer les certificats dans le magasin de la machine locale avant de lancer l'application GPM (Graphical Process Modeler).

Pourquoi et quand exécuter cette tâche

La confusion sera moindre pour l'utilisateur si jamais le certificat SSL associé à l'adaptateur de serveur HTTP sécurisé ou au port SSL de base n'était pas accrédité par la machine locale de l'utilisateur.

Pour importer des certificats racine accrédités dans JavaWS :

Procédure

1. Enregistrez le certificat racine accrédité dans un fichier sur votre ordinateur local.
2. Ouvrez le **Panneau de configuration Java** sur votre ordinateur local (javaws.exe sous `jre\bin`).
3. Ouvrez l'onglet **Sécurité** et cliquez sur **Certificats**.
4. Cliquez sur **Importer** pour accéder à un certificat racine accrédité et sélectionnez-le.
5. Cliquez sur **Ouvrir** pour importer le certificat racine accrédité. Une fois que le certificat racine accrédité est archivé, JavaWS l'utilise pour vérifier l'accréditation pendant l'établissement de la liaison SSL.

Passage du mode HTTP au mode HTTPS via le port SSL de base

Vous pouvez passer du mode HTTP au mode HTTPS via le port SSL de base.

Pourquoi et quand exécuter cette tâche

Pour passer du mode HTTP au mode HTTPS via le port SSL de base :

Procédure

1. Accédez au répertoire `/rép_install/install/properties`.
2. Ouvrez le fichier sandbox.cfg.
3. Modifiez les paramètres suivants :

   ```
   WEBAPP_PROTOCOL=https
   WEBAPP_LIST_PORT=<port_base + 1>
   ```

   Ces paramètres sont utilisés par le modélisateur GPM (Graphical Process Modeler) pour établir la communication avec le serveur.
4. (Facultatif, recommandé). Si vous souhaitez désactiver l'accès aux applications Web Tableau de bord et GPM sur le port de base et configurer la redirection automatique vers le port HTTPS, spécifiez les paramètres suivants dans un fichier customer_overrides.properties :

```
SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
HTTPS_LIST_PORT=<base_port + 1>
```

Par exemple :

```
## Identifiee les fichiers war à ignorer pendant le déploiement sur le port de base.
## Utilisez une liste séparée par des virgules pour spécifier plusieurs fichiers war
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifie le fichiers war pour une redirection automatique sur le port https. Utilisez une liste séparée par des virgule
## pour spécifier plusieurs fichiers war
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifie le port https pour les fichiers war redirigés. S'il est spécifié,
## doit correspondre à WEBAPP_LIST_PORT dans le fichier sandbox.cfg
noapp.HTTPS_LIST_PORT=<base_port + 1>
```

5. Enregistrez et fermez le fichier.
6. Accédez au répertoire `/rép_install/install/bin`.
7. Arrêtez Sterling B2B Integrator.
8. Appliquez les modifications de configuration. Entrez `./setupfiles.sh`.
9. Déployez la nouvelle configuration. Entrez `./deployer.sh`.
10. Lancez Sterling B2B Integrator.
11. (Facultatif) Si vous avez désactivé l'accès aux applications Web GPM et Tableau de bord sur le port de base (étape 4), vérifiez les modifications effectuées. Par exemple, vous pouvez vérifier que :
    - L'application Web Tableau de bord sur http://host:baseport/dashboard est inaccessible ou est réacheminée automatiquement vers https://host:<base_port > 1 + /dashboard.
    - L'application Web GPM sur http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp est inaccessible ou est réacheminée automatiquement vers https://host:<base_port + 1>/gbm/pmodeler/ProcessModeler.jnlp.

Passage du mode HTTP au mode HTTPS via un adaptateur de serveur HTTP sécurisé

Vous pouvez passer du mode HTTP au mode HTTPS via un adaptateur de serveur HTTP sécurisé

Pourquoi et quand exécuter cette tâche

Pour passer du mode HTTP au mode HTTPS :

Procédure

1. Créez une nouvelle instance de l'adaptateur de serveur HTTP avec SSL activé. Vous devez configurer les paramètres suivants comme indiqué :
   - Le paramètre **Authentification d'utilisateur requise** est défini sur **Non**
   - La paramètre **Utiliser SSL** est défini sur **Obligatoire**
2. Déployez les fichiers WAR requis sur l'instance de l'adaptateur de serveur HTTP avec SSL activé.

   Remarque : Tous les fichiers WAR doivent être sélectionnés dans le répertoire `/rép_install/install/noapp/deploy` lors de la configuration de l'instance de l'adaptateur de serveur HTTP. En outre, le nom de contexte de l'application Web d'administration doit correspondre au paramètre ADMIN_CONTEXT_PATH dans le fichier `/rép_install/install/properties/sandbox.cfg`. Pour toutes les autres applications Web, le nom de contexte doit être le nom du fichier war sans l'extension ".war".

   Cette opération est nécessaire pour que toutes les modifications apportées par le biais d'un correctif ou d'un correctif logiciel soient automatiquement répercutées dans le déploiement de l'adaptateur de serveur HTTP.

Les fichiers WAR requis sont notamment :

- admin.war
- dashboard.war
- gbm.war
- myaft.war
- portlets.war

Des fichiers WAR supplémentaires peuvent s'avérer nécessaires pour prendre en charge les nouvelles fonctionnalités que vous ajoutez à votre Tableau de bord.

3. Ouvrez le fichier sandbox.cfg file et modifiez les paramètres suivants :

   ```
   WEBAPP_PROTOCOL=https
   WEBAPP_LIST_PORT=<port_adaptateur_serveur_http_sécurisé>
   ```

   Ces paramètres sont utilisés par l'application GPM pour établir la communication avec le serveur.

4. (Facultatif, recommandé). Si vous souhaitez désactiver le déploiement des applications Web Tableau de bord et GPM sur le port de base, spécifiez les paramètres suivants dans un fichier customer_overrides.properties :

```
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
noapp.HTTPS_LIST_PORT=<port_adaptateur_serveur_http_sécurisé>
```

Par exemple :

```
## Identifies the war files to be skipped during deployment on the base port.
## Use comma-separated list to specify multiple wars
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies wars for auto-redirect to the https port.
## Use comma-separated list to specify multiple wars
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies the https port for the redirected wars.
## If specified, this should match the WEBAPP_LIST_PORT in sandbox.cfg
noapp.HTTPS_LIST_PORT=<port_adaptateur_serveur_http_sécurisé>
```

5. Si vous souhaitez utiliser un certificat différent pour cette fonction, modifiez `/install_dir/install/properties/customer_overrides.properties` en ajoutant la ligne suivante : *noapp.sslCert={mentionnez_le_nom_de_votre_propre_certificat}*. Si vous n'indiquez pas un certificat différent, la fonction utilise ASISslCert.
6. (Facultatif) Si vous souhaitez envoyer des cookies du navigateur via un protocole sécurisé comme HTTPS, accédez à `/install_dir/install/properties` et indiquez le paramètre suivant dans un fichier customer_overrides.properties :

   ```
   ## sending cookies as secure over https
   http.useSecureCookie=true
   ```

7. Accédez au répertoire `/rép_install/install/bin`.
8. Arrêtez Sterling B2B Integrator.
9. Appliquez les modifications de configuration. Entrez `./setupfiles.sh`.
10. Déployez la nouvelle configuration. Entrez `./deployer.sh`.
11. Lancez Sterling B2B Integrator.
12. 11. Vérifiez que l'application Web Tableau de bord est accessible par le biais de l'adaptateur de serveur HTTP en accédant à https://host:*<port_adaptateur_serveur_http_sécurisé>*/dashboard.

13. Vérifiez que l'application Web GPM est accessible par le biais de l'adaptateur de serveur HTTP en accédant à https://host:<*port_adaptateur_serveur_http_sécurisé*>/gbm/pmodeler/ProcessModeler.jnlp.
14. Enregistrez et fermez le fichier.
15. Si vous avez désactivé le déploiement des applications Web Tableau de bord et GPM sur le port de base (Etape 4), vérifiez les points suivants :
    - L'application Web Tableau de bord sur http://host:baseport/dashboard est réacheminée automatiquement vers https://host:<*port_adaptateur_serveur_http_sécurisé*>/dashboard.
    - L'application Web GPM sur http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp est réacheminée automatiquement vers https://host:<*port_adaptateur_serveur_http_sécurisé*>/gbm/pmodeler/ProcessModeler.jnlp.

Passage du mode HTTPS au mode HTTP

Vous pouvez passer du mode HTTPS au mode HTTP.

Pourquoi et quand exécuter cette tâche

Pour passer du mode HTTPS au mode HTTP :

Procédure

1. Accédez au répertoire `/rép_install/install/properties`.
2. Ouvrez le fichier **sandbox.cfg**.
3. Modifiez les paramètres suivants :
   ```
   WEBAPP_PROTOCOL=http
   WEBAPP_LIST_PORT=<port_base>
   ```
4. Enregistrez et fermez le fichier.
5. (Facultatif) Si le déploiement des applications Web Tableau de bord et GPM sur le port de base a été désactivé lors du passage en mode HTTPS, vous devez ouvrir le fichier customer_overrides.properties et mettre en commentaire les paramètres suivants pour qu'ils ne soient pas appliqués :

```
## SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## HTTPS_LIST_PORT=<http_server_adapter_port>
```

6. (Facultatif) Enregistrez et fermez le fichier.
7. Accédez au répertoire `/rép_install/install/bin`.
8. Arrêtez Sterling B2B Integrator.
9. Appliquez les modifications de configuration. Entrez `./setupfiles.sh`.
10. Déployez la nouvelle configuration. Entrez `./deployer.sh`.
11. Lancez Sterling B2B Integrator.
12. Vérifiez les points suivants :
    - L'application Web Tableau de bord est accessible sur http://host:baseport/dashboard
    - L'application Web GPM est accessible sur http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp
13. (Facultatif) Annulez le déploiement des applications Web à partir de l'instance de l'adaptateur de serveur HTTP activée pour SSL.

Module HSM (Hardware Security Module) version 5.2.3 - 5.2.5

Module HSM (Hardware Security Module)

HSM est un dispositif de sécurité matériel qui génère, stocke et protège les clés de chiffrement. Vous pouvez stocker les certificats de système dans une base de données à l'aide de Sterling B2B Integrator ou sur un HSM.

Sterling B2B Integrator prend en charge les dispositifs HSM suivants :

- SafeNet Eracom ProtectServer Orange externe
- Périphériques PCI ProtectServer Gold

Vous pouvez utiliser HSM pour :

- Créer des certificats de système sur HSM
- Importer des certificats de système de Sterling B2B Integrator
- Exporter des certificats de système de Sterling B2B Integrator
- Supprimer des certificats de système de HSM
- Afficher les détails des certificats de système sur HSM

Fonctions Sterling B2B Integrator de prise en charge du module HSM

Sterling B2B Integrator stocke une entrée dans la table CERTS_AND_PRI_KEY pour chaque paire de clés et chaque certificat.

Cette entrée contient des informations sur :

- Les clés et les certificats, y compris la période de validité, le numéro de série, les restrictions d'utilisation, l'auteur et le sujet utilisés par l'interface utilisateur à afficher à l'attention de l'utilisateur, sans qu'il soit nécessaire d'accéder réellement à la clé ou au certificat.
- Les normalisations du nom distinctif utilisé par le système dans les recherches.
- Les modifications de l'enregistrement.
- Des informations sur l'état de révocation des certificats.
- Le type du fichier de clés.
- Les références à un objet fichier de clés binaires enregistré dans la table DATA_TABLE. Lorsqu'un fichier de clés logicielles est utilisé, l'objet référencé peut contenir des éléments sur les clés. Dans le cas d'un HSM, il contient soit des informations de référence (nCipher), soit une marque de réservation (Eracom).

Paramètres des certificats de système HSM

Le tableau suivant contient les paramètres des commandes CreateSystemCert, ImportSystemCert et ExportSystemCert.

Paramètre	Description
autogen	Indique s'il faut utiliser les informations générées par le système pour contrôler l'accès à la clé et au fichier de clés. Ce paramètre doit être défini sur false pour les clés des modules HSM.

Paramètre	Description
alias	Nom de clé stocké dans le module HSM. Seuls les noms d'alias comprenant les caractères a-z, A-Z, 0-9 ou le tiret (-) et dont la longueur totale ne dépasse la longueur du GUID du système sont autorisés.
Certtype	Type du certificat à importer. Quatre types de fichiers certificat sont pris en charge : pkcs12, pkcs8, pem et keystore. Sterling B2B Integrator prend uniquement en charge les clés pem chiffrées à l'aide de DES ou de 3DES. Utilisez keystore pour répertorier ou importer le fichier de clés.
certname	Nom d'affectation du certificat dans la base de données Sterling B2B Integrator.
file	Fichier Keycert ou PEM à importer.
keyname	Nom de la clé système de Sterling B2B Integrator à créer.
keypass	Code confidentiel du jeton qui protège le module HSM SafeNet Eracom où réside le fichier de clés.
keypassphrase	Phrase passe de la clé privée. Cette valeur est facultative sur la ligne de commande. Si vous ne l'indiquez pas, un message vous invite à le spécifier. Définit le code confidentiel du jeton sur le module SafeNet Eracom où réside le fichier de clés.
keysize	Longueur, en bits, du modulo RSA. Les valeurs valides sont 768, 1024, 2048, 3072 ou 4096.
keystoretype	Type du fichier de clés à importer. La valeur valide est CRYPTOKI.
keystoreprovider	Type du fournisseur. SafeNet Eracom est le seul module HSM pris en charge. ERACOM ou ERACOM.n est pris en charge si vous importez des certificats dans un emplacement autre que l'emplacement par défaut 0.
keytype	Algorithme de la clé publique. RSA est le seul algorithme pris en charge.
ObjectID	ID du certificat de système.
pkcs12file	Fichier pkcs12 à importer.
password	Phrase passe du magasin pour le fichier keycert ou PEM.
pkcs12storepass	Phrase passe du magasin pour le fichier PKCS12.
pkcs12keypass	Phrase passe de la clé utilisée pour chiffrer la clé privée dans le fichier PKCS12.
fournisseur	Fournisseur du type de fichier de clés. ERACOM ou ERACOM.n est pris en charge si vous importez des certificats dans un emplacement autre que l'emplacement par défaut 0.
rfc1779rdnsequence	Zone de la chaîne de nom distinctif contenant les zones identifiées dans la colonne Valeurs valides. Seule la zone Nom commun est requise. Séparez chaque zone par une virgule. Les informations valides sont : • CN = Nom commun • O = Organisation • OU = Unité organisationnelle • L = Emplacement • ST = État • C = Pays (code ISO3166-1 alpha-2 à deux lettres)

Paramètre	Description
storetype	Type du fichier de clés. CRYPTOKI est le seul type de fichier de clés pris en charge.
signingbit	Définit le bit d'utilisation de la clé de signature pour le certificat autosigné. Les valeurs valides sont true et false.
serial	Numéro de série du certificat.
system passphrase	Phrase passe du système Sterling B2B Integrator. Cette valeur est facultative sur la ligne de commande.
store passphrase	Phrase passe permettant d'accéder au fichier de clés. Code confidentiel du jeton sur le module HSM SafeNet Eracom où réside le fichier de clés. Cette valeur est facultative sur la ligne de commande.
systempass	Phrase passe du système Sterling B2B Integrator.
storepass	Code confidentiel du jeton qui protège le module HSM SafeNet Eracom où réside le fichier de clés.
totrusttable	Indique si le certificat est ajouté à la table des certificats de confiance. Les valeurs valides sont true et false.
validityindays	Durée de validité du certificat, en jours.

HSM SafeNet Eracom

Avant de pouvoir utiliser un HSM avec Sterling B2B Integrator, vous devez configurer Sterling B2B Integrator pour qu'il utilise et reconnaisse le HSM SafeNet Eracom.

Pour installer et configurer le HSM SafeNet Eracom, suivez les instructions communiquées par le fournisseur ; assurez-vous également que Java Runtime est installé. Utilisez le fournisseur de l'emplacement où les clés Sterling B2B Integrator seront stockées lorsque vous configurerez et utiliserez des utilitaires. Une fois que vous avez créé un code confidentiel pour l'emplacement SafeNet Eracom, ne le modifiez pas. Sterling B2B Integrator ne pourra pas accéder à une clé sur le HSM si vous modifiez le code confidentiel.

L'architecture SafeNet Eracom divise le HSM en plusieurs emplacements. Installez et configurez les cartes ou les HSM conformément aux instructions du fournisseur. Chaque emplacement est associé à un fournisseur de sécurité et peut être protégé par un code confidentiel distinct. Vous pouvez créer un emplacement spécifique sur le HSM pour Sterling B2B Integrator et le protéger avec un code confidentiel unique. Le fournisseur de l'emplacement par défaut 0 est ERACOM. Les fournisseurs des emplacements supplémentaires s'appellent ERACOM.*n*, où *n* désigne le numéro de l'emplacement. Assurez-vous que les composants Java Runtime sont disponibles pour fonctionner conjointement avec le périphérique.

Configuration de Sterling B2B Integrator pour utiliser l'outil HSM Eracom SafeNet

Vous pouvez configurer Sterling B2B Integrator pour utiliser l'outil HSM Eracom SafeNet.

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Ajoutez les lignes suivantes aux fichiers tmp.sh et tmp.sh.in :

```
LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/Eracom/lib
```

```
export LD_LIBRARY_PATH
```

3. Si vous configurez un serveur réseau, ajoutez les lignes suivantes aux fichiers tmp.sh et tmp.sh.in, où *nomhôte_OU_adresseIP_périphérique_réseau* est l'adresse IP ou le nom de domaine complet du serveur sur le réseau Eracom SafeNet

   ```
   ET_HSM_NETCLIENT_SERVERLIST=nomhôte_OU_adresseIP_périphérique_réseau
   export ET_HSM_NETCLIENT_SERVERLIST
   ```

4. Copiez jprov.jar depuis le répertoire /opt/Eracom/lib vers le répertoire */rép_install*/install/jdk/jre/lib/ext.
5. Ajoutez une définition pour chaque fournisseur de sécurité dans le fichier */rép_install*/install/bin/jdk/jre/lib/security/java.security. Pour ajouter une définition, identifiez le numéro affecté au fournisseur Certicom et attribuez n+1 au fournisseur Eracom SafeNet. Pour tous les autres fournisseurs identifiés après le fournisseur Eracom SafeNet, augmentez le numéro du security.provider de 1.

   ```
   security.provider.n=com.certicom.ecc.jcae.Certicom
   security.provider.n+1=au.com.eracom.crypto.provider.ERACOMProvider
   ```

   Si vous utilisez un emplacement différent de zéro sur le module HSM SafeNet Eracom, indiquez l'emplacement comme suit, où *x* désigne le numéro de l'emplacement :

   ```
   security.provider.n+1=au.com.eracom.crypto.provider.slotx.ERACOMProvider
   ```

6. Définissez le paramètre TLSProviderPolicy dans le fichier */rép_install*/install/properties/security.properties.
   - Si le fournisseur est défini dans l'emplacement 0, vérifiez que la seule ligne en commentaire pour le paramètre TLSProviderPolicy est la suivante :

```
TLSProviderPolicy= TLS:*:ECMQV:P:.CT;TLS:SIG:MD2withRSA:P:ERACOM;TLS:Cipher:RawRSA:P:ERACOM;TLS:*
:RSA:P:ERACOM;TLS:*:*:P:Certicom
```

   - Si le fournisseur est défini dans un emplacement autre que 0, modifiez le paramètre TLSProviderPolicy comme suit, où *x* désigne l'emplacement que vous configurez :

```
TLSProviderPolicy=TLS:*:ECMQV:P:.CT;TLS:SIG:MD2withRSA:P:ERACOM.x;TLS:Cipher:RawRSA:P:ERACOM.
x;TLS:*:RSA:P:ERACOM.x;TLS:*:*:P:Certicom
```

7. Définissez la commande KeyStoreProviderKey dans le fichier */rép_install*/install/properties/security.properties :
   - Si le fournisseur est défini dans l'emplacement 0, vérifiez que le paramètre KeyStoreProviderMap est défini comme suit :

```
KeyStoreProviderMap=SCIKS,SCIKS,false,Certicom,Certicom,false;
nCipher.sworld,nCipherKM,false,nCipherKM,nCipherKM,true;CRYPTOKI,ERACOM, true,ERACOM,ERACOM,true
```

   - Si le fournisseur est défini dans un emplacement autre que 0, modifiez le paramètre KeyStoreProviderMap comme suit, où *x* désigne le numéro de l'emplacement :

```
KeyStoreProviderMap=SCIKS,SCIKS,false,Certicom,Certicom,false;
nCipher.sworld,nCipherKM,false,nCipherKM,nCipherKM,true; CRYPTOKI,ERACOM.x,true,ERACOM.x,ERACOM.x,true
```

Cartes PCI et périphériques réseau nCipher et SafeNet/Eracom pris en charge

Sterling B2B Integrator prend actuellement en charge la carte PCI Safenet/Eracom ProtectServer Orange et le périphérique réseau Orange External, en plus de la prise en charge de nCipher.

Les composants suivants sont pris en charge :

Fabricant	Types de périphérique pris en charge
nCipher	• Séries nShield de cartes PCI • Périphériques réseau NetHSM
Safenet/Eracom	• Carte PCI ProtectServer Gold • Carte PCI ProtectServer Orange PCI • Périphérique réseau ProtectServer Orange External

Utilisation d'un module HSM

Création des certificats de système à stocker dans l'outil HSM

Vous pouvez créer un certificat de système autosigné à stocker dans l'outil HSM.

Avant de commencer

Étapes à exécuter préalablement à l'installation :

- Arrêtez Sterling B2B Integrator.
- Assurez-vous que la base de données Sterling B2B Integrator est en cours d'exécution.

Pourquoi et quand exécuter cette tâche

Pour créer un certificat de système autosigné à stocker dans l'outil HSM :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez : `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase] [store passphrase] [key passphrase]`
3. Si vous n'avez pas entré la phrase passe du système, la phrase passe du magasin et la phrase passe de la clé sur la ligne de commande, vous êtes invité à le faire.

Lister les certificats de système stockés dans l'outil HSM

Vous pouvez lister les informations sur les certificats de système stockés dans l'outil HSM.

Pourquoi et quand exécuter cette tâche

Pour lister les informations sur les certificats de système stockés dans l'outil HSM :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.

2. Entrez : `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

Exemple

Voici un exemple du fichier de résultat de la commande :

```
Key exists with alias rayado-e5305c3-10d8f4bde7f--7fc1
Certificate Subject Info CN=test, OU=test, O=test, L=test, ST=Alabama, C=US
Certificate Issuer Info CN=Pythagoras, OU=System Verification, O=Sterling, L=Dublin,
ST=OH, C=US, EMAILADDRESS=caussuer@company.com
```

Importation d'un certificat de système HSM dans la base de données Sterling B2B Integrator

Utilisez cette procédure si une clé et un certificat ont été ajoutés dans un HSM indépendamment de Sterling B2B Integrator. Vous devez d'abord importer les informations relatives à un certificat de système stocké sur un HSM dans la base de données pour que Sterling B2B Integrator puisse les utiliser.

Pourquoi et quand exécuter cette tâche

Selon la méthode utilisée pour ajouter la clé privée et le certificat dans le HSM, la fonction de liste peut afficher des entrées en double pour une paire de clé/certificat unique.

Vous devez obtenir l'alias du certificat de système avant de pouvoir importer les informations concernant un certificat de système dans la base de données.

Pour importer le certificat de système :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez : `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

Supprimer des certificats de système stockés dans l'outil HSM

Vous pouvez supprimer de manière permanente le certificat de système stocké dans l'outil HSM. Les données de clé privée contenues dans le certificat ne pourront pas être récupérées.

Pourquoi et quand exécuter cette tâche

Pour supprimer un certificat de système stocké dans l'outil HSM :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez : `./RemoveSystemCert.sh -r` *xxxx*
   où *xxxx* désigne l'ID objet du certificat que vous souhaitez supprimer.

Exportation des certificats de système

Vous pouvez exporter des certificats de système à partir de Sterling B2B Integrator afin qu'ils puissent être importés dans l'outil HSM.

Pourquoi et quand exécuter cette tâche

Les certificats de système sur un outil HSM (Hardware Service Manager) ne peuvent pas être exportés à l'aide de ExportSystemCert.sh.

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez : `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. Entrez l'expression de passe.

Exemple : Certificat de système HSM

Vous pouvez importer un certificat de système dans le module HSM au format keycert, pkcs12 ou pem. L'importation d'un certificat de système ajoute la clé et le certificat dans le module HSM et crée une entrée correspondante dans la base de données Sterling B2B Integrator.

Si vous importez un certificat et une clé de type pem, vérifiez que la clé privée est créée dans le format chiffré DES ou 3DES (triple DES).

Ce qui suit est un exemple de clé privée pem créée dans le format 3DES :

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CE0243B4833BD321
RtN+AFGTmx6EROcbo8fMXnMaRM/JcKIc3jbKYB5t6H6H5uvUrAmv+Si62QEtqg9V
x5r+GhiLcA9sdllKpnIXYg63Y+egn8DsxdGUCqnC+HDUlRVHX0NWKJ3FwXukr9iN
WP4MBr+NXMSETaBA0O0B4oSRCWvxelc2U2GItvUqJsOjLSILbahAgZk/j6LUDMy4
2FWoRtWZyGVz/gc+pN+bOwFHpbrZxd1YqZGRNKeZKTpXWslqxp5NDraBl1cmJ3vL
0RTnkwZnnyJ1Brc/WynlVfRK1gEEg8MPa3B9veat70ET/mLERuA4Ke8r0WAy5Y/w
7Yowicmwbo4q7RLVLm1ZmvPF4OXL8xIvaIUMOCW8/MNpanxZ4BB1CfTwQKQ9koJ7
9MT8K8ofu6V9TSK4Rw1cCpTKvattg/H72Ut39Yz185Ec+E8sV0BtilpqVsYSt1g6
lO805MqPym6gPo2NLpvk1iPLUZ1vIfthz+qb5cyXj1ng9aZSeRF/lytPLxSSy3LN
J9SZrnfHwbuhnyuQmco3SsCtYXnZ81cDHX+4O8sGqHA1zMwuqErorUvwxD6ZNnlc
DTmKIt826oows4Gtw48aEwjV4lk8FXQsWQjDWJHjFNNvGiyszPJjvPvM8zL1EwxO
mJFeNxBb0U3zgLs5aK/HHRn1/gzOBHwtr8bdFFBkpLoVGnbW+mRVxmJOvvPe7Zo+
sJXLEWC8Bm4klV8H6ynx6aQJ8a62HqbjPvShq1VH2I+1iwbyE3DzxY5sHrzZA2rb
dHabk3f0nBUvMegKI9Ye4ktLJf8yIQfsSBSJTEYXHqyx5ptoAEIlIQ==
-----END RSA PRIVATE KEY-----
```

Gestion d'utilitaires de certificats de système

Paires de clés HSM et demandes de signature de certificat

L'utilitaire GenCSR génère une paire de clés sur un HSM et crée une demande de signature de certificat PKCS10 avec la clé publique provenant de cette paire de clés. Vous pouvez alors soumettre la demande de signature de certificat à une autorité de certification.

Une fois que vous avez reçu un certificat émis par l'autorité de certification, vous pouvez utiliser l'utilitaire GenCSR pour mettre à jour le certificat. Le certificat de système n'est pas disponible dans Sterling B2B Integrator tant qu'il n'a pas été mis à jour avec un certificat émis par l'autorité de certification.

Vous pouvez également utiliser cet utilitaire pour afficher une liste des demandes de signature de certificat, écrire des informations sur une demande de signature de certificat dans un fichier, supprimer une demande de signature de certificat ou bien écrire des informations sur un certificat émis par cette autorité (et stocké sur HSM(

dans un fichier. Les informations relatives aux demandes de signature de certificat sont stockées dans la base de données Sterling B2B Integrator, alors que les clés réelles sont stockées sur le HSM.

Pour utiliser l'utilitaire, déterminez d'abord quelle action vous souhaitez effectuer. Ensuite, utilisez l'utilitaire GenCSR et identifiez l'action sur la ligne de commande. Pour chaque action, fournissez les arguments requis pour l'action dans le fichier de propriétés. Un exemple de fichier de propriétés, appelé csr.properties.sample, est fourni dans le répertoire */rép_install*/install/properties.

L'utilitaire GenCSR réside dans le répertoire */rép_install*/install/bin.

La syntaxe de la commande est : `GenCSR.sh -a ACTION -p PROPERTIES`

Paramètres GenCSR

Le tableau suivant contient les paramètres utilisés lors de l'exécution du script GenCSR.

Paramètre	Description	Valeurs valides
-a ACTION	Action à effectuer.	Les actions valides sont : • CREATE • UPDATE • LISTE • DELETE • GETPCKS10 • GETCACERT
-p PROPERTIES	Fichier de propriétés qui contient les paramètres supplémentaires nécessaires pour les actions. Vous devez inclure le chemin d'accès au fichier de propriétés.	Nom d'un fichier de propriétés. Par exemple : `csr_create.properties`

Mise à jour du fichier de clés HSM à l'aide de certificats émis par l'autorité de certification

Utilisez l'utilitaire GenCSR avec l'argument de mise à jour pour ajouter des informations sur les certificats émis par l'autorité de certification dans le fichier de clés HSM.

Procédure

1. Assurez-vous que le fichier csr.properties est configuré correctement.

   Le tableau suivant décrit les paramètres requis dans le fichier csr.properties pour l'argument de mise à jour.

Paramètre	Description	Valeurs valides
fournisseur	Nom du fournisseur du fichier de clés.	ERACOM ou ERACOM.n
keystoretype	Nom du fichier de clés utilisé.	CRYPTOKI
certificate.request.Name	Nom de la demande de signature de certificat à mettre à jour.	Nom affecté à une demande de signature de certificat

Paramètre	Description	Valeurs valides
add.trusted	Indique si les informations de certificat sont ajoutées à la table des certificats de confiance.	True | false
ca.cert.file	Nom et chemin du fichier dans lequel écrire des informations sur le certificat émis par une autorité de certification.	Nom et chemin valides d'un fichier de certificat émis par l'autorité de certification.

2. Mettez à niveau le fichier de clés de l'outil HSM.

   La syntaxe de la commande est : `./GenCSR.sh -a update -p ../properties/csr_update.properties`

Liste des demandes de signature de certificat

Utilisez l'utilitaire GenCSR avec l'argument de liste pour afficher les demandes de signature de certificat dans la base de données HSM. Aucune configuration de fichier de propriétés n'est requise pour l'argument de liste.

Pourquoi et quand exécuter cette tâche

La syntaxe de la commande est : `./GenCSR.sh -a list`

Suppression d'une demande de signature de certificat

Utilisez l'utilitaire GenCSR avec l'argument de suppression pour supprimer une demande de signature de certificat. Cet utilitaire ne supprime que la demande de signature de certificat. Il ne supprime pas les certificats de système qui sont mis à jour avec un certificat émis par cette autorité.

Procédure

1. Assurez-vous que le fichier cacert.properties est configuré correctement. Vous devez configurer le fichier de propriétés préalablement à l'utilisation de l'argument de suppression. Le tableau suivant décrit les paramètres requis dans le fichier cacert.properties pour l'argument de suppression.

Paramètre	Description	Valeurs valides
certificate.request.Name	Nom de la demande de signature de certificat à supprimer.	Nom d'une demande de signature de certificat
keystoretype	Nom du fichier de clés utilisé.	CRYPTOKI
fournisseur	Nom du fournisseur du fichier de clés.	ERACOM[.N]

2. Supprime la demande de signature de certificat. La syntaxe de la commande est : `./GenCSR.sh -a delete -p ../properties/cacert.properties`

Écriture des informations de demande de signature de certificat dans un format pkcs10

Utilisez l'utilitaire GenCSR avec l'argument getpkcs10 pour écrire une demande de signature de certificat au format pkcs10 dans le fichier spécifié.

Procédure

1. Assurez-vous que le fichier csr_getpkcs10.properties est configuré correctement.

   Le tableau suivant décrit les paramètres requis dans le fichier csr_getpkcs10.properties pour l'argument getpkcs10. Vous devez configurer le fichier de propriétés préalablement à l'utilisation de l'argument getpkcs10.

Paramètre	Description	Valeurs valides
certificate.request.Name	Nom de la demande de signature de certificat.	Nom affecté à une demande de signature de certificat
keystoretype	Nom du fichier de clés utilisé.	CRYPTOKI
csr.file	Chemin complet du fichier dans lequel écrire des informations sur la demande de signature de certificat.	Chemin et nom de fichier d'un fichier pour l'écriture des informations de demande de signature de certificat

2. Écrivez la demande de signature de certificat dans un fichier.

   La syntaxe de la commande est : `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

Déplacement des certificats de système dans l'outil HSM

Vous pouvez déplacer des certificats d'autosignature ou des certificats émis par l'autorité de certification de la base de données vers l'outil HSM.

Pourquoi et quand exécuter cette tâche

Il est plus sûr de régénérer des clés et des certificats à l'aide de CreateSystemCert.sh ou de GenCSR.sh.

Pour déplacer des certificats d'autosignature ou des certificats émis par l'autorité de certification de la base de données vers l'outil HSM :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Arrêtez Sterling B2B Integrator.
3. Démarrez la base de données.
4. Exportez le certificat de système vers un fichier PKCS12 :

   `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
5. Recherchez l'ID objet du certificat de système à supprimer. Entrez :

   `./RemoveSystemCert.sh -l.`
6. Supprimez le certificat de système de la base de données. Entrez :

   `RemoveSystemCert.sh -r` *xxxx*où *xxxx* désigne l'ID objet du certificat que vous souhaitez supprimer.
7. Pour importer le certificat de système que vous avez exporté vers l'outil HSM et créer une entrée de base de données correspondante :

   `./ImportSystemCert.sh -pkcs12 systempass certname pkcs12file pkcs12storepass pkcs12keypass keystoretype keystoreprovider storepass keypass`

Remarque : Si vous déplacez les certificats OpsDrv, OpsKey et UIKey vers l'outil HSM, utilisez le nom exact. Sinon, Sterling B2B Integrator ne fonctionnera pas correctement. Pour tous les autres certificats de système, le nom n'est pas critique. Lorsque vous déplacez des certificats de système autre que OpsDrv, OpsKey et UIKey, l'ID objet utilisé par les services et les adaptateurs change. Reconfigurez les services qui utilisent les certificats de système déplacés.

Écriture d'un certificat émis par une autorité de certification dans un fichier

Utilisez l'utilitaire GenCSR avec l'argument getcacert pour écrire le certificat émis par l'autorité de certification dans un fichier.

Procédure

1. Assurez-vous que le fichier getcacert.properties est configuré correctement.

   Le tableau suivant décrit les paramètres requis dans le fichier getcacert.properties pour l'action getcacert. Vous devez configurer le fichier getcacert.properties préalablement à l'utilisation de l'argument getcacert.

Paramètre	Description	Valeurs valides
certificate.request.Name	Nom de la demande de signature de certificat.	Nom du certificat
keystoretype	Nom du fichier de clés utilisé.	CRYPTOKI
ca.cert.file	Chemin complet du fichier dans lequel écrire des informations sur le certificat émis par l'autorité de certification.	Nom et chemin d'un fichier de certificat d'autorité de certification

2. Écrivez le certificat dans un fichier.

   La syntaxe de la commande est : `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

Génération des certificats système internes (OpsDrv, OpsKey, UIKey) sur l'outil HSM

Trois certificats de système sont installés avec Sterling B2B Integrator et permettent de sécuriser les opérations internes. Les déplacer dans l'outil HSM présente peu d'intérêt au niveau de la sécurité. Votre règle de sécurité peut exiger que tous les certificats contenant des clés privées soient stockés sur HSM.

Pourquoi et quand exécuter cette tâche

Lorsque vous générez les certificats de système internes de Sterling B2B Integrator (OpsDrv, OpsKey et UIKey) sur HSM, utilisez mes noms exacts. Sinon, Sterling B2B Integrator ne fonctionnera pas correctement.

Pour générer des certificats de système internes :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez `./RemoveSystemCert.sh -l` pour afficher les certificats de la base de données. Notez l'ID objet pour chaque certificat de système.

3. Pour supprimer les certificats de système de la base de données, exécutez la commande suivante pour chaque certificat : `./RemoveSystemCert.sh -r xxxx`, où *xxxx* désigne l'ID objet du certificat que vous souhaitez supprimer.
4. Pour générer le certificat de système sur l'outil HSM pour chaque certificat, entrez :

   ```
   ./CreateSystemCert.sh storetype provider autogen totrusttable signingbit
   keytype keysize keyname rfc1779rdnsequence serial validityindays [system
   passphrase] [store passphrase] [key passphrase]
   ```

Utilisation de nCipher et de SafeNetEracom

Mappage des fournisseurs de fichiers de clés

Sterling B2B Integrator dispose d'un type de fichier de clés unique pour tous les fournisseurs de services cryptographiques ; il est en mesure de définir un mappage entre les types de fichiers de clés et les fournisseurs nécessaires pour l'implémentation du fichier de clés lui-même, les algorithmes de signature et les algorithmes de transport de clé.

La clé et l'objet abstraction des informations de clé contiennent ces données avec une référence à com.sterlingcommerce.security.PrivateKeyInfo.

De cette façon, Sterling B2B Integrator peut utiliser simultanément une combinaison de clés dans les HSM et magasins logiciels de la base de données, sans qu'il soit nécessaire d'effectuer des configurations supplémentaires après le chargement initial de la clé ou des informations de clé dans la base de données. Pour Sterling B2B Integrator, les clés ont toutes la même présentation, quel que soit l'emplacement où elles sont stockées.

Le mappage est implémenté sous la forme d'une propriété, appelée KeyStoreProviderMap, dans le fichier security.properties. Il se compose d'un ensemble d'entrées délimitées par des points-virgules (;). Chaque entrée comporte six éléments qui sont séparés par des virgules et qui suivent ce format :

```
KeyStoreType, KeyStoreProvider, DoesAliasMatter, SignatureProvider,
EncryptionProvider, KeyOnHSM
```

Ces éléments sont décrits dans le tableau suivant :

Élément	Description	Informations supplémentaires
KeyStoreType	Type de chaîne du fichier de clés.	
KeyStoreProvider	Nom du fournisseur de services cryptographiques qui implémente le fichier de clés.	
DoesAliasMatter	Indique si l'alias des clés doit être unique pour ce type de fichier de clés.	Les valeurs possibles sont true ou false. Les clés doivent avoir des alias uniques dans le cas où il n'existe qu'un seul fichier de clés par périphérique.

Élément	Description	Informations supplémentaires
SignatureProvider	Nom du fournisseur de services cryptographiques utilisé pour créer des signatures à l'aide des clés provenant du fichier de clés.	
EncryptionProvider	Nom du fournisseur de services cryptographiques utilisé lors du déchiffrement des informations à l'aide des clés provenant du fichier de clés.	Ce paramètre est surtout utilisé pour les opérations de transport de clés RSA.
KeyOnHSM	Indique si le fichier de clés est stocké sur un HSM.	

La chaîne NULL est une valeur acceptable qui sera traitée comme si aucun fournisseur n'avait été spécifié. Une entrée doit comporter au moins deux valeurs. Si une entrée contient moins de six valeurs, celles-ci seront attribuées de gauche à droite au fournisseur de fichiers de clés, si l'alias est significatif lors du stockage de la clé, au fournisseur de signature, au fournisseur de chiffrement, si la clé se trouve sur un HSM pour le type de fichier de clés. Les autres valeurs seront traitées comme des valeurs NULL et aucun fournisseur spécifique ne sera demandé pour les opérations ayant des clés de ce type.

Le paramètre KeyStoreProviderMap par défaut est :

```
KeyStoreProviderMap=SCIKS,SCIKS,false,Certicom,Certicom,false;nCipher.sworld,
nCipherKM,false,nCipherKM,nCipherKM,true;CRYPTOKI,ERACOM,true,ERACOM,ERACOM,true
```

Gestion des clés HSM et des informations de clés

Sterling B2B Integrator contient plusieurs scripts Java de gestion des clés sur des HSM.

Les programmes Java sont répertoriés ci-dessous.

Programme	Objet
com.sterlingcommerce.db.RemoveSystemCert	Permet de répertorier et de supprimer des certificats de système Sterling B2B Integrator. Pendant une suppression, le programme tente d'effacer la clé dans le fichier de clés et d'écraser l'objet fichier de clés dans la base de données.
com.sterlingcommerce.db.CreateCertEx	Permet de générer une paire de clés sur un HSM et un certificat autosigné contenant la clé publique de la paire de clés.
com.sterlingcommerce.security.util. CertificateSigningRequest	Permet de générer une paire de clés sur un HSM, ainsi que de créer et de gérer une demande de signature de certificat PKCS10 associée. La demande PKCS10 peut être envoyée à une autorité en vue d'obtenir un certificat signé de cette autorité. Le programme peut être utilisé pour charger ce certificat dans le fichier de clés et associer celui-ci à la paire de clés appropriée.

Programme	Objet
com.sterlingcommerce.db.ImportSystemCert	Permet d'importer une clé privée et le certificat, dans un format pris en charge (PEM ou PKCS12), dans un fichier de clés sur un HSM. Permet également d'importer des informations concernant une clé privée et un certificat sur un HSM dans la base de données Sterling B2B Integrator.

Modifications du kit JDK pour la prise en charge de HSM nCipher

Afin que Sterling B2B Integrator puisse utiliser HSM nCipher, vous devez installer les fournisseurs de services cryptographiques Java nCipher. Pour effectuer l'installation, copiez les fichiers jar suivants dans le sous-répertoire jre/lib/ext de votre kit JDK. Modifiez le fichier java.security pour charger les fournisseurs nCipher.

Les fichiers suivants sont placés dans /opt/nfast/java/classes par le programme d'installation de nCipher :

- rsaprivenc.jar
- nfjava.jar
- kmjava.jar
- jutils.jar
- kmcsp.jar

Vous devez ajouter les fournisseurs nCipher après le fournisseur IBM JCE (Java Cryptography Extension) et avant le fournisseur Certicom. Par exemple :

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ncipher.fixup.provider.nCipherRSAPrivateEncrypt
security.provider.3=com.ncipher.provider.km.nCipherKM
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.ibm.jsse2.IBMJSSEProvider2
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
```

Sur les systèmes Solaris dotés du kit JDK SUN, vous devez placer les fournisseurs nCipher après les fournisseurs Sun JCA et JCE et avant le fournisseur Certicom. Par exemple :

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.certicom.ecc.jcae.Certicom
security.provider.3=com.ncipher.fixup.provider.nCipherRSAPrivateEncrypt
security.provider.4=com.ncipher.provider.km.nCipherKM
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=com.sun.net.ssl.internal.ssl.Provider
security.provider.7=com.sun.rsajca.Provider
security.provider.8=sun.security.jgss.SunProvider
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
```

Configurez une stratégie TLSProvider à l'aide de l'exemple de fichier security.properties. Par exemple :

```
TLSProviderPolicy=TLS:MD:MD5:P:Certicom;TLS:MD:SHA1:P:Certicom;TLS:MAC:HmacMD5:P:Certicom;
TLS:MAC:HmacSHA1:P:Certicom;TLS:SIG:MD2withRSA:P:Certicom;TLS:Cipher:RawRSA:P:Certicom;
TLS:*:ECDH:P:Certicom;TLS:*:ECDSA:P:Certicom;TLS:*:*:P:nCipherKM
```

Modifications du kit JDK pour la prise en charge de HSM Eracom

Afin que Sterling B2B Integrator puisse utiliser les HSM Eracom, vous devez installer le fournisseur de services cryptographiques Java Eracom. Pour effectuer l'installation, placez les fichiers .jar appropriés dans le sous-répertoire jre/lib/ext de votre kit JDK, puis modifiez le fichier java.security pour charger les fournisseurs nCipher.

Ces fichiers sont placés dans /opt/nfast/java/classes par le programme d'installation de nCipher :

- jcprov.jar
- jprov.jar

Vous devez ajouter le fournisseur Eracom après le fournisseur Certicom. Par exemple :

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.certicom.ecc.jcae.Certicom
security.provider.3=au.com.eracom.crypto.provider.ERACOMProvider
security.provider.4=com.ibm.jsse2.IBMJSSEProvider2
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.8=com.sterlingcommerce.security.provider.SCI
```

Remarque : Eracom a un fournisseur qui peut être spécifié pour chaque emplacement sur la carte. Pour le fournisseur à l'emplacement 8, utilisez :

```
security.provider.3=au.com.eracom.crypto.provider.slot8.ERACOMProvider
```

Modifications de l'environnement Linux pour la prise en charge du HSM nCipher

nCipher vous recommande de créer un compte utilisateur spécial pour l'exécution du hardserver nCipher.

Le compte à partir duquel vous exécutez Sterling B2B Integrator doit avoir des droits équivalents, ou vous devez exécuter Sterling B2B Integrator à partir du compte spécial nCipher ou en tant que root. Si vous effectuez l'une de ces opérations et que vous utilisez MySQL, vous devez modifier les droits d'accès de MySQL, ou démarrer MySQL à partir de votre compte normal avant d'appeler run.sh.

Modifications de l'environnement Linux pour la prise en charge du HSM Eracom

Pour utiliser le dispositif Eracom, vous devez fournir des informations dans des variables d'environnement à la session qui accède dispositif.

Les modifications recommandées pour PATH, LD_LIBRARY_PATH et MANPATH sont les suivantes :

```
PATH=$PATH:/opt/Eracom/bin LD_LIBRARY_PATH=$LD_LIBRARY_PATH:
/opt/Eracom/lib MANPATH=$MANPATH:/opt/Eracom/man
```

En outre, si vous utilisez un périphérique réseau plutôt qu'une carte PCI locale, vous devez indiquer ET_HSM_NETCLIENT_SERVERLIST, comme suit :

```
ET_HSM_NETCLIENT_SERVERLIST=nomhôte_OU_adresseIP_périphérique_réseau
```

Vous devez exporter ces variables dans tmp.sh.

Module HSM (Hardware Security Module) version 5.2.6 ou ultérieure

Module HSM (Hardware Security Module)

HSM est un dispositif de sécurité matériel qui génère, stocke et protège les clés de chiffrement. Vous pouvez stocker les certificats de système dans une base de données à l'aide de Sterling B2B Integrator ou sur un HSM.

Sterling B2B Integrator prend en charge les dispositifs HSM suivants :

- SafeNet Luna SA
- nCipher nShield Connect

Vous pouvez utiliser HSM pour :

- Créer des certificats de système sur HSM
- Importer des certificats de système de Sterling B2B Integrator
- Exporter des certificats de système de Sterling B2B Integrator
- Supprimer des certificats de système de HSM
- Afficher les détails des certificats de système sur HSM

Fonctions Sterling B2B Integrator de prise en charge du module HSM

Sterling B2B Integrator stocke une entrée dans la table CERTS_AND_PRI_KEY pour chaque paire de clés et chaque certificat.

Cette entrée contient des informations sur :

- Les clés et les certificats, y compris la période de validité, le numéro de série, les restrictions d'utilisation, l'auteur et le sujet utilisés par l'interface utilisateur à afficher à l'attention de l'utilisateur, sans qu'il soit nécessaire d'accéder réellement à la clé ou au certificat.
- Les normalisations du nom distinctif utilisé par le système dans les recherches.
- Les modifications de l'enregistrement.
- Des informations sur l'état de révocation des certificats.
- Le type du fichier de clés.
- Les références à un objet fichier de clés binaires enregistré dans la table DATA_TABLE. Lorsqu'un fichier de clés logicielles est utilisé, l'objet référencé peut contenir des éléments sur les clés. Dans le cas d'un HSM, il contient soit des informations de référence (nCipher), soit une marque de réservation (Luna).

Paramètres des certificats de système HSM

Le tableau suivant contient les paramètres des commandes CreateSystemCert, ImportSystemCert et ExportSystemCert.

Paramètre	Description
autogen	Indique s'il faut utiliser les informations générées par le système pour contrôler l'accès à la clé et au fichier de clés. Ce paramètre doit être défini sur false pour les clés des modules HSM.

Paramètre	Description
alias	Nom de clé stocké dans le module HSM. Seuls les noms d'alias comprenant les caractères a-z, A-Z, 0-9 ou le tiret (-) et dont la longueur totale ne dépasse la longueur du GUID du système sont autorisés.
Certtype	Type du certificat à importer. Quatre types de fichiers certificat sont pris en charge : pkcs12, pkcs8, pem et keystore. Sterling B2B Integrator prend uniquement en charge les clés pem chiffrées à l'aide de DES ou de 3DES. Utilisez keystore pour répertorier ou importer le fichier de clés.
certname	Nom d'affectation du certificat dans la base de données Sterling B2B Integrator.
file	Fichier Keycert ou PEM à importer.
keyname	Nom de la clé système de Sterling B2B Integrator à créer.
keypass	Code confidentiel du jeton qui protège le module HSM SafeNet ou nCipher où réside le fichier de clés.
keypassphrase	Phrase passe de la clé privée. Cette valeur est facultative sur la ligne de commande. Si vous ne l'indiquez pas, vous êtes invité à le faire.
keysize	Longueur, en bits, du modulo RSA. Les valeurs valides sont 1024, 2048, 3072 ou 4096.
keystoretype	Type du fichier de clés à importer. Les valeurs valides sont nCipher.sworld, Luna et PKCS11IMPLKS (à partir de 5.2.6.2).
keystoreprovider	Type du fournisseur. Les valeurs valides sont nCipherKM, LunaProvider et IBMPKCS11Impl (à partir de 5.2.6.2).
keytype	Algorithme de la clé publique. RSA est le seul algorithme pris en charge.
ObjectID	ID du certificat de système.
pkcs12file	Fichier pkcs12 à importer.
password	Phrase passe du magasin pour le fichier keycert ou PEM.
pkcs12storepass	Phrase passe du magasin pour le fichier PKCS12.
pkcs12keypass	Phrase passe de la clé utilisée pour chiffrer la clé privée dans le fichier PKCS12.
fournisseur	Fournisseur du type de fichier de clés. Les valeurs valides sont nCipherKM, LunaProvider et IBMPKCS11Impl (à partir de 5.2.6.2).
rfc1779rdnsequence	Zone de la chaîne de nom distinctif contenant les zones identifiées dans la colonne Valeurs valides. Seule la zone Nom commun est requise. Séparez chaque zone par une virgule. Les informations valides sont : • CN = Nom commun • O = Organisation • OU = Unité organisationnelle • L = Emplacement • ST = État • C = Pays (code ISO3166-1 alpha-2 à deux lettres)
storetype	Type du fichier de clés. Les valeurs valides sont nCipher.sworld, Luna et PKCS11IMPLKS (à partir de 5.2.6.2).
signingbit	Définit le bit d'utilisation de la clé de signature pour le certificat autosigné. Les valeurs valides sont true et false.

Paramètre	Description
serial	Numéro de série du certificat.
system passphrase	Phrase passe du système Sterling B2B Integrator. Cette valeur est facultative sur la ligne de commande.
store passphrase	Phrase passe permettant d'accéder au fichier de clés. Cette valeur est facultative sur la ligne de commande. Si vous ne l'indiquez pas, vous êtes invité à le faire.
systempass	Phrase passe du système Sterling B2B Integrator.
storepass	Code confidentiel du jeton qui protège le module HSM SafeNet ou nCipher où réside le fichier de clés.
totrusttable	Indique si le certificat est ajouté à la table des certificats de confiance. Les valeurs valides sont true et false.
validityindays	Durée de validité du certificat, en jours.

Utilisation d'un module HSM

Création des certificats de système à stocker dans l'outil HSM

Vous pouvez créer un certificat de système autosigné à stocker dans l'outil HSM.

Avant de commencer

Étapes à exécuter préalablement à l'installation :

- Arrêtez Sterling B2B Integrator.
- Assurez-vous que la base de données Sterling B2B Integrator est en cours d'exécution.

Pourquoi et quand exécuter cette tâche

Pour créer un certificat de système autosigné à stocker dans l'outil HSM :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez : `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase] [store passphrase] [key passphrase]`
3. Si vous n'avez pas entré la phrase passe du système, la phrase passe du magasin et la phrase passe de la clé sur la ligne de commande, vous êtes invité à le faire.

Liste des certificats de système stockés dans l'outil HSM

Vous pouvez lister les informations sur les certificats de système stockés dans l'outil HSM.

Pourquoi et quand exécuter cette tâche

Pour lister les informations sur les certificats de système stockés dans l'outil HSM :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez : `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

Exemple

Voici un exemple du fichier de résultat de la commande :

```
Key exists with alias rayado-e5305c3-10d8f4bde7f--7fc1
Certificate Subject Info CN=test, OU=test, O=test, L=test, ST=Alabama, C=US
Certificate Issuer Info CN=Pythagoras, OU=System Verification, O=Sterling, L=Dublin,
ST=OH, C=US, EMAILADDRESS=caussuer@company.com
```

Remarque : A partir de la version 5.2.6.2, la valeur valide de Keystoretype est PKCS11IMPLKS.

Importation d'un certificat de système HSM dans la base de données Sterling B2B Integrator

Utilisez cette procédure si une clé et un certificat ont été ajoutés dans un HSM indépendamment de Sterling B2B Integrator. Vous devez d'abord importer les informations relatives à un certificat de système stocké sur un HSM dans la base de données pour que Sterling B2B Integrator puisse les utiliser.

Pourquoi et quand exécuter cette tâche

Selon la méthode utilisée pour ajouter la clé privée et le certificat dans le HSM, la fonction de liste peut afficher des entrées en double pour une paire de clé/certificat unique.

Vous devez obtenir l'alias du certificat de système avant de pouvoir importer les informations concernant un certificat de système dans la base de données.

Pour importer le certificat de système :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez : `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

Suppression des certificats de système stockés dans l'outil HSM

Pourquoi et quand exécuter cette tâche

Cette procédure supprime de façon définitive le certificat de système à partir de l'outil HSM. Les données de clé privée contenues dans le certificat ne pourront pas être récupérées.

Pour supprimer un certificat de système stocké dans l'outil HSM :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez : `./RemoveSystemCert.sh -r` *xxxx*
   où *xxxx* désigne l'ID objet du certificat que vous souhaitez supprimer.

Exportation des certificats de système

Vous pouvez exporter des certificats de système à partir de Sterling B2B Integrator afin qu'ils puissent être importés dans l'outil HSM.

Pourquoi et quand exécuter cette tâche

Les certificats de système sur un outil HSM (Hardware Service Manager) ne peuvent pas être exportés à l'aide de ExportSystemCert.sh.

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez : `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. Entrez l'expression de passe.

Exemple : Certificat de système HSM

Vous pouvez importer un certificat de système dans le module HSM au format keycert, pkcs12 ou pem. L'importation d'un certificat de système ajoute la clé et le certificat dans le module HSM et crée une entrée correspondante dans la base de données Sterling B2B Integrator.

Si vous importez un certificat et une clé de type pem, vérifiez que la clé privée est créée dans le format chiffré DES ou 3DES (triple DES).

Ce qui suit est un exemple de clé privée pem créée dans le format 3DES :

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CE0243B4833BD321
RtN+AFGTmx6EROcbo8fMXnMaRM/JcKIc3jbKYB5t6H6H5uvUrAmv+Si62QEtqg9V
x5r+GhiLcA9sdllKpnIXYg63Y+egn8DsxdGUCqnC+HDUlRVHX0NWKJ3FwXukr9iN
WP4MBr+NXMSETaBA0O0B4oSRCWvxelc2U2GItvUqJsOjLSILbahAgZk/j6LUDMy4
2FWoRtWZyGVz/gc+pN+bOwFHpbrZxd1YqZGRNKeZKTpXWslqxp5NDraBl1cmJ3vL
0RTnkwZnnyJ1Brc/WynlVfRK1gEEg8MPa3B9veat70ET/mLERuA4Ke8r0WAy5Y/w
7Yowicmwbo4q7RLVLm1ZmvPF4OXL8xIvaIUMOCW8/MNpanxZ4BB1CfTwQKQ9koJ7
9MT8K8ofu6V9TSK4Rw1cCpTKvattg/H72Ut39Yz185Ec+E8sV0BtilpqVsYSt1g6
lO805MqPym6gPo2NLpvk1iPLUZ1vIfthz+qb5cyXj1ng9aZSeRF/lytPLxSSy3LN
J9SZrnfHwbuhnyuQmco3SsCtYXnZ81cDHX+4O8sGqHA1zMwuqErorUvwxD6ZNnlc
DTmKIt826oows4Gtw48aEwjV4lk8FXQsWQjDWJHjFNNvGiyszPJjvPvM8zL1EwxO
mJFeNxBb0U3zgLs5aK/HHRn1/gzOBHwtr8bdFFBkpLoVGnbW+mRVxmJOvvPe7Zo+
sJXLEWC8Bm4klV8H6ynx6aQJ8a62HqbjPvShq1VH2I+1iwbyE3DzxY5sHrzZA2rb
dHabk3f0nBUvMegKI9Ye4ktLJf8yIQfsSBSJTEYXHqyx5ptoAEIlIQ==
-----END RSA PRIVATE KEY-----
```

Gestion d'utilitaires de certificats de système

Paires de clés HSM et demandes de signature de certificat

L'utilitaire GenCSR génère une paire de clés sur un HSM et crée une demande de signature de certificat PKCS10 avec la clé publique provenant de cette paire de clés. Vous pouvez alors soumettre la demande de signature de certificat à une autorité de certification.

Une fois que vous avez reçu un certificat émis par l'autorité de certification, vous pouvez utiliser l'utilitaire GenCSR pour mettre à jour le certificat. Le certificat de système n'est pas disponible dans Sterling B2B Integrator tant qu'il n'a pas été mis à jour avec un certificat émis par l'autorité de certification.

Vous pouvez également utiliser cet utilitaire pour afficher une liste des demandes de signature de certificat, écrire des informations sur une demande de signature de certificat dans un fichier, supprimer une demande de signature de certificat ou bien écrire des informations sur un certificat émis par cette autorité (et stocké sur HSM(

dans un fichier. Les informations relatives aux demandes de signature de certificat sont stockées dans la base de données Sterling B2B Integrator, alors que les clés réelles sont stockées sur le HSM.

Pour utiliser l'utilitaire, déterminez d'abord quelle action vous souhaitez effectuer. Ensuite, utilisez l'utilitaire GenCSR et identifiez l'action sur la ligne de commande. Pour chaque action, fournissez les arguments requis pour l'action dans le fichier de propriétés. Un exemple de fichier de propriétés, appelé csr.properties.sample, est fourni dans le répertoire */rép_install*/install/properties.

L'utilitaire GenCSR réside dans le répertoire */rép_install*/install/bin.

La syntaxe de la commande est : `GenCSR.sh -a ACTION -p PROPERTIES`

Paramètres GenCSR

Le tableau suivant contient les paramètres utilisés lors de l'exécution du script GenCSR.

Paramètre	Description	Valeurs valides
-a ACTION	Action à effectuer.	Les actions valides sont : • CREATE • UPDATE • LISTE • DELETE • GETPCKS10 • GETCACERT
-p PROPERTIES	Fichier de propriétés qui contient les paramètres supplémentaires nécessaires pour les actions. Vous devez inclure le chemin d'accès au fichier de propriétés.	Nom d'un fichier de propriétés. Par exemple : `csr_create.properties`

Mise à jour du fichier de clés HSM à l'aide de certificats émis par l'autorité de certification

Pourquoi et quand exécuter cette tâche

Utilisez l'utilitaire GenCSR avec l'argument de mise à jour pour ajouter des informations sur les certificats émis par l'autorité de certification dans le fichier de clés HSM.

Procédure

1. Assurez-vous que le fichier csr.properties est configuré correctement.

   Le tableau suivant décrit les paramètres requis dans le fichier csr.properties pour l'argument de mise à jour.

Paramètre	Description	Valeurs valides
fournisseur	Nom du fournisseur du fichier de clés.	IBMPKCS11IMPL (à partir de la version 5.2.6.2) ou nCipherKM ou LunaProvider

Paramètre	Description	Valeurs valides
keystoretype	Nom du fichier de clés utilisé.	PKCS11IMPLKS (à partir de la version 5.2.6.2) ou nCipher.sworld ou Luna **Remarque :** La valeur 'type_de_magasin_de_clés' doit être synchrone avec la valeur 'fournisseur'.
certificate.request.Name	Nom de la demande de signature de certificat à mettre à jour.	Nom affecté à une demande de signature de certificat
add.trusted	Indique si les informations de certificat sont ajoutées à la table des certificats de confiance.	True | false
ca.cert.file	Nom et chemin du fichier dans lequel écrire des informations sur le certificat émis par une autorité de certification.	Nom et chemin valides d'un fichier de certificat émis par l'autorité de certification.

2. Mettez à niveau le fichier de clés de l'outil HSM.

   La syntaxe de la commande est : `./GenCSR.sh -a update -p ../properties/csr_update.properties`

Liste des demandes de signature de certificat

Utilisez l'utilitaire GenCSR avec l'argument de liste pour afficher les demandes de signature de certificat dans la base de données HSM. Aucune configuration de fichier de propriétés n'est requise pour l'argument de liste.

Pourquoi et quand exécuter cette tâche

La syntaxe de la commande est : `./GenCSR.sh -a list`

Suppression d'une demande de signature de certificat

Utilisez l'utilitaire GenCSR avec l'argument de suppression pour supprimer une demande de signature de certificat. Cet utilitaire ne supprime que la demande de signature de certificat. Il ne supprime pas les certificats de système qui sont mis à jour avec un certificat émis par cette autorité.

Procédure

1. Assurez-vous que le fichier cacert.properties est configuré correctement. Vous devez configurer le fichier de propriétés préalablement à l'utilisation de l'argument de suppression. Le tableau suivant décrit les paramètres requis dans le fichier cacert.properties pour l'argument de suppression.

Paramètre	Description	Valeurs valides
certificate.request.Name	Nom de la demande de signature de certificat à supprimer.	Nom d'une demande de signature de certificat
keystoretype	Nom du fichier de clés utilisé.	PKCS11IMPLKS (à partir de la version 5.2.6.2) ou nCipher.sworld ou Luna

Paramètre	Description	Valeurs valides
fournisseur	Nom du fournisseur du fichier de clés.	IBMPKCS11IMPL (à partir de la version 5.2.6.2) ou nCipherKM ou LunaProvider **Remarque :** La valeur 'type_de_magasin_de_clés' doit être synchrone avec la valeur 'fournisseur'.

2. Supprime la demande de signature de certificat. La syntaxe de la commande est : `./GenCSR.sh -a delete -p ../properties/cacert.properties`

Écriture des informations de demande de signature de certificat dans un format pkcs10

Pourquoi et quand exécuter cette tâche

Utilisez l'utilitaire GenCSR avec l'argument getpkcs10 pour écrire une demande de signature de certificat au format pkcs10 dans le fichier spécifié.

Procédure

1. Assurez-vous que le fichier csr_getpkcs10.properties est configuré correctement.

   Le tableau suivant décrit les paramètres requis dans le fichier csr_getpkcs10.properties pour l'argument getpkcs10. Vous devez configurer le fichier de propriétés préalablement à l'utilisation de l'argument getpkcs10.

Paramètre	Description	Valeurs valides
certificate.request.Name	Nom de la demande de signature de certificat.	Nom affecté à une demande de signature de certificat
keystoretype	Nom du fichier de clés utilisé.	PKCS11IMPLKS (à partir de la version 5.2.6.2) ou nCipher.sworld ou Luna
csr.file	Chemin complet du fichier dans lequel écrire des informations sur la demande de signature de certificat.	Chemin et nom de fichier d'un fichier pour l'écriture des informations de demande de signature de certificat

2. Écrivez la demande de signature de certificat dans un fichier.

   La syntaxe de la commande est : `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

Déplacement des certificats de système dans l'outil HSM

Vous pouvez déplacer des certificats d'autosignature ou des certificats émis par l'autorité de certification de la base de données vers l'outil HSM.

Pourquoi et quand exécuter cette tâche

Il est plus sûr de régénérer des clés et des certificats à l'aide de CreateSystemCert.sh ou de GenCSR.sh.

Pour déplacer des certificats d'autosignature ou des certificats émis par l'autorité de certification de la base de données vers l'outil HSM :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Arrêtez Sterling B2B Integrator.
3. Démarrez la base de données.
4. Exportez le certificat de système vers un fichier PKCS12 :

   ```
   ./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass
   pkcs12keypass
   ```
5. Recherchez l'ID objet du certificat de système à supprimer. Entrez :

   ```
   ./RemoveSystemCert.sh -l.
   ```
6. Supprimez le certificat de système de la base de données. Entrez :

   `RemoveSystemCert.sh -r` *xxxx*où *xxxx* désigne l'ID objet du certificat que vous souhaitez supprimer.
7. Pour importer le certificat de système que vous avez exporté vers l'outil HSM et créer une entrée de base de données correspondante :

   ```
   ./ImportSystemCert.sh -pkcs12 systempass certname pkcs12file
   pkcs12storepass pkcs12keypass keystoretype keystoreprovider storepass
   keypass
   ```

   Remarque : Si vous déplacez les certificats OpsDrv, OpsKey et UIKey vers l'outil HSM, utilisez le nom exact. Sinon, Sterling B2B Integrator ne fonctionnera pas correctement. Pour tous les autres certificats de système, le nom n'est pas critique. Lorsque vous déplacez des certificats de système autre que OpsDrv, OpsKey et UIKey, l'ID objet utilisé par les services et les adaptateurs change. Reconfigurez les services qui utilisent les certificats de système déplacés.

Écriture d'un certificat émis par une autorité de certification dans un fichier

Pourquoi et quand exécuter cette tâche

Utilisez l'utilitaire GenCSR avec l'argument getcacert pour écrire le certificat émis par l'autorité de certification dans un fichier.

Procédure

1. Assurez-vous que le fichier getcacert.properties est configuré correctement.

   Le tableau suivant décrit les paramètres requis dans le fichier getcacert.properties pour l'action getcacert. Vous devez configurer le fichier getcacert.properties préalablement à l'utilisation de l'argument getcacert.

Paramètre	Description	Valeurs valides
certificate.request.Name	Nom de la demande de signature de certificat.	Nom du certificat
keystoretype	Nom du fichier de clés utilisé.	PKCS11IMPLKS (à partir de la version 5.2.6.2) ou nCipher.sworld ou Luna
ca.cert.file	Chemin complet du fichier dans lequel écrire des informations sur le certificat émis par l'autorité de certification.	Nom et chemin d'un fichier de certificat d'autorité de certification

2. Écrivez le certificat dans un fichier.

La syntaxe de la commande est : `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

Génération des certificats système internes (OpsDrv, OpsKey, UIKey) sur l'outil HSM

Trois certificats de système sont installés avec Sterling B2B Integrator et permettent de sécuriser les opérations internes. Les déplacer dans l'outil HSM présente peu d'intérêt au niveau de la sécurité. Votre règle de sécurité peut exiger que tous les certificats contenant des clés privées soient stockés sur HSM.

Pourquoi et quand exécuter cette tâche

Lorsque vous générez les certificats de système internes de Sterling B2B Integrator (OpsDrv, OpsKey et UIKey) sur HSM, utilisez mes noms exacts. Sinon, Sterling B2B Integrator ne fonctionnera pas correctement.

Pour générer des certificats de système internes :

Procédure

1. Accédez au répertoire */rép_install*/install/bin.
2. Entrez `./RemoveSystemCert.sh -l` pour afficher les certificats de la base de données. Notez l'ID objet pour chaque certificat de système.
3. Pour supprimer les certificats de système de la base de données, exécutez la commande suivante pour chaque certificat : `./RemoveSystemCert.sh -r xxxx`, où *xxxx* désigne l'ID objet du certificat que vous souhaitez supprimer.
4. Pour générer le certificat de système sur l'outil HSM pour chaque certificat, entrez :

   ```
   ./CreateSystemCert.sh storetype provider autogen totrusttable signingbit
   keytype keysize keyname rfc1779rdnsequence serial validityindays [system
   passphrase] [store passphrase] [key passphrase]
   ```

Configuration des périphériques nCipher et SafeNet Luna

Mappage des fournisseurs de fichiers de clés

Sterling B2B Integrator dispose d'un type de fichier de clés unique pour tous les fournisseurs de services cryptographiques ; il est en mesure de définir un mappage entre les types de fichiers de clés et les fournisseurs nécessaires pour l'implémentation du fichier de clés lui-même, les algorithmes de signature et les algorithmes de transport de clé.

La clé et l'objet abstraction des informations de clé contiennent ces données avec une référence à com.sterlingcommerce.security.PrivateKeyInfo.

De cette façon, Sterling B2B Integrator peut utiliser simultanément une combinaison de clés dans les HSM et magasins logiciels de la base de données, sans qu'il soit nécessaire d'effectuer des configurations supplémentaires après le chargement initial de la clé ou des informations de clé dans la base de données. Pour Sterling B2B Integrator, les clés ont toutes la même présentation, quel que soit l'emplacement où elles sont stockées.

Le mappage est implémenté sous la forme d'une propriété, appelée KeyStoreProviderMap, dans le fichier security.properties. Il se compose d'un ensemble d'entrées délimitées par des points-virgules (;). Chaque entrée comporte six éléments qui sont séparés par des virgules et qui suivent ce format :

```
KeyStoreType, KeyStoreProvider, DoesAliasMatter, SignatureProvider,
EncryptionProvider, KeyOnHSM
```

Ces éléments sont décrits dans le tableau suivant :

Élément	Description	Informations supplémentaires
KeyStoreType	Type de chaîne du fichier de clés.	
KeyStoreProvider	Nom du fournisseur de services cryptographiques qui implémente le fichier de clés.	
DoesAliasMatter	Indique si l'alias des clés doit être unique pour ce type de fichier de clés.	Les valeurs possibles sont true ou false. Les clés doivent avoir des alias uniques dans le cas où il n'existe qu'un seul fichier de clés par périphérique.
SignatureProvider	Nom du fournisseur de services cryptographiques utilisé pour créer des signatures à l'aide des clés provenant du fichier de clés.	
EncryptionProvider	Nom du fournisseur de services cryptographiques utilisé lors du déchiffrement des informations à l'aide des clés provenant du fichier de clés.	Ce paramètre est surtout utilisé pour les opérations de transport de clés RSA.
KeyOnHSM	Indique si le fichier de clés est stocké sur un HSM.	

La chaîne NULL est une valeur acceptable qui sera traitée comme si aucun fournisseur n'avait été spécifié. Une entrée doit comporter au moins deux valeurs. Si une entrée contient moins de six valeurs, celles-ci seront attribuées de gauche à droite au fournisseur de fichiers de clés, si l'alias est significatif lors du stockage de la clé, au fournisseur de signature, au fournisseur de chiffrement, si la clé se trouve sur un HSM pour le type de fichier de clés. Les autres valeurs seront traitées comme des valeurs NULL et aucun fournisseur spécifique ne sera demandé pour les opérations ayant des clés de ce type.

Le paramètre KeyStoreProviderMap par défaut est :

```
nCipher = nCipher.sworld,nCipherKM,false,nCipherKM,nCipherKM,true
SafeNet Luna = Luna,LunaProvider,true,LunaProvider,LunaProvider,true
Utilisez "PKCS11IMPLKS,IBMPKCS11Impl,true,IBMPKCS11Impl,IBMPKCS11Impl,true" pour nCipher et SafeNet
```

Modifications du kit JDK pour la prise en charge de HSM nCipher

Afin que Sterling B2B Integrator puisse utiliser HSM nCipher, vous devez installer les fournisseurs de services cryptographiques Java nCipher. Pour effectuer l'installation, copiez les fichiers jar suivants dans le sous-répertoire jre/lib/ext de votre kit JDK. Modifiez le fichier java.security pour charger les fournisseurs nCipher.

Remarque :

1. La configuration suivante n'est pas nécessaire si vous créez de nouvelles clés ou de nouveaux certificats en utilisant l'implémentation de "PKCS11IMPLKS" à partir de la version 5.2.6.2.
2. Pour continuer d'utiliser les clés ou certificats existants après la mise à niveau vers la version 5.2.6.2, exécutez les étapes suivantes.

Ces fichiers sont placés dans /opt/nfast/java/classes par le programme d'installation de nCipher :

- jcetools.jar
- jutils.jar
- keysafe.jar
- kmjava.jar
- nCipherKM.jar
- nfjava.jar
- rsaprivenc.jar

Vous devez ajouter les fournisseurs nCipher après le fournisseur IBM JCE (Java Cryptography Extension) et avant le fournisseur Certicom.

Vous devez également supprimer IBMJCEFIPS de la liste.

Par exemple :

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ncipher.provider.km.nCipherKM
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
security.provider.10=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.11=com.certicom.jsse.provider.CerticomJSSE
```

Utilisez l'exemple suivant à partir de la version 5.2.6.2 pour prendre en charge les clés ou certificats existants.

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ncipher.provider.km.nCipherKM
security.provider.3=org.bouncycastle.jce.provider.BouncyCastleProvider
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.jsse2.IBMJSSEProvider2
security.provider.7=com.ibm.security.jgss.IBMJGSSProvider
security.provider.8=com.ibm.security.cert.IBMCertPath
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
security.provider.11=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.12=com.certicom.jsse.provider.CerticomJSSE
```

Modifications du kit JDK pour la prise en charge de HSM SafeNet Luna

Afin que Sterling B2B Integrator puisse utiliser les HSM SafeNet Luna, vous devez installer le fournisseur de services cryptographiques Java SafeNet Luna. Pour effectuer l'installation, placez les fichiers .jar appropriés dans le sous-répertoire jre/lib/ext du kit JDK, puis modifiez le fichier java.security pour charger les fournisseurs Luna.

Remarque :

1. La configuration suivante n'est pas nécessaire si vous créez de nouvelles clés ou de nouveaux certificats en utilisant l'implémentation de "PKCS11IMPLKS" à partir de la version 5.2.6.2.
2. Pour continuer d'utiliser les clés ou certificats existants après la mise à niveau vers la version 5.2.6.2, exécutez les étapes suivantes.

Ces fichiers sont placés dans /opt/nfast/java/classes par le programme d'installation de nCipher :

- libLunaAPI.so
- LunaProvider.jar

Vous devez ajouter le fournisseur LunaProvider après le fournisseur IBM JCE (Java Cryptography Extension) et avant le fournisseur Certicom.

Vous devez également supprimer IBMJCEFIPS de la liste.

Par exemple :

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.safenetinc.luna.provider.LunaProvider
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
security.provider.10=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.11=com.certicom.jsse.provider.CerticomJSSE
```

Utilisez l'exemple suivant à partir de la version 5.2.6.2 pour prendre en charge les clés ou certificats existants.

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.safenetinc.luna.provider.LunaProvider
security.provider.3=org.bouncycastle.jce.provider.BouncyCastleProvider
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.jsse2.IBMJSSEProvider2
security.provider.7=com.ibm.security.jgss.IBMJGSSProvider
security.provider.8=com.ibm.security.cert.IBMCertPath
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
security.provider.11=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.12=com.certicom.jsse.provider.CerticomJSSE
```

Configuration d'HSM à l'aide d'IBM PKCS11IMPLKS (version 5.2.6.2 ou ultérieure)

Configuration d'HSM à l'aide de l'implémentation d'IBM PKCS11 IMPLKS (version 5.2.6.2 ou ultérieure)

Pourquoi et quand exécuter cette tâche

A partir de la version 5.2.6.2, le système prend en charge l'implémentation d'IBM PKCS11 pour les périphériques HSM. Les HSM implémentent l'API Java JCE. Cette interface a accès aux clés du périphérique.

Procédure

1. Un nouveau fichier de propriétés **hsm.properties.in** est ajouté pour la prise en charge de PKCS11IMPLKS/IBMPKCS11Impl.

   La table suivante répertorie les propriétés spécifiques à la configuration d'HSM.

Attribut	Description
HSM_KEYSTORE_TYPE	Si HSM_ENABLED est défini sur *true*, la valeur d'attribut doit être *IBMPKCS11IMPLKS*.
HSM_KEYSTORE_PROVIDER	Si HSM_ENABLED est défini sur *true* la valeur d'attribut doit être *IBMPKCS11Impl*.
HSM_KEYSTORE_FILE	<Doit être laissé vide>
HSM_ADAPTER_TYPE	ncipher ou safeNetFor ncipher, exécutez la commande suivante lors de la création ou de la mise à jour des clés ou des certificats - Sous UNIX : exportez CKNFAST_OVERRIDE_SECURITY_ASSURANCES= "longterm;tokenkeys" Sous Windows : définissez CKNFAST_OVERRIDE_SECURITY_ASSURANCES ="longterm;tokenkeys"
HSM_ENABLED	Cet attribut ne doit jamais être défini sur *true* pour la prise en charge d'HSM.
HSM_PRNG_ALGORITHM	Si HSM_ENABLED est défini sur *true*, la valeur d'attribut doit être *PKCS11DeviceRNG*.
HSM_CONFIG_FILE_LOCATION	Si HSM_ENABLED est défini sur *true* la valeur d'attribut doit être définie sur l'emplacement du fichier de configuration IBMPKCS11

2. Mettez à jour ou créez le fichier de configuration nécessaire à la configuration d'HSM en fonction du type d'HSM.

   Selon le type d'HSM, vous pouvez trouver le fichier de configuration du périphérique comme expliqué ci-après ou bien vous pouvez demander le fichier de configuration au support IBM. Vous pouvez mettre à jour n'importe lequel des paramètres par défaut, le cas échéant. Vous devez éditer la valeur *library* si votre emplacement est différent de l'emplacement par défaut.

   ```
   Pour le périphérique SafeNet Luna :

   lunasa_5_0_jsse.cfgname = B2Bi
   library=/usr/safenet/lunaclient/lib/libCryptoki2_64.so
   description=Luna SA 5.0 IBM SSP config - JSSE

   publickeyimportonly=false
   slotListIndex = 0
   disabledMechanisms = {
      CKM_MD5
      CKM_SHA_1
      CKM_MD5_HMAC
      CKM_SHA_1_HMAC
      CKM_DES_CBC
      CKM_DES_CBC_PAD
      CKM_DES_ECB
      CKM_DES3_CBC
      CKM_DES3_ECB
      CKM_DES3_CBC_PAD
   ```

```
   CKM_AES_CBC
   CKM_AES_ECB
   CKM_AES_CBC_PAD
   CKM_RC4
   CKM_SSL3_MASTER_KEY_DERIVE
   CKM_SSL3_KEY_AND_MAC_DERIVE
   CKM_SSL3_PRE_MASTER_KEY_GEN
   CKM_TLS_PRE_MASTER_KEY_GEN
   CKM_TLS_MASTER_KEY_DERIVE
   CKM_TLS_KEY_AND_MAC_DERIVE
   CKM_TLS_MASTER_KEY_DERIVE_DH
   CKM_TLS_PRF
   CKM_SHA256_HMAC
   CKM_SHA384_HMAC
   CKM_SHA512_HMAC
   CKM_EC_KEY_PAIR_GEN
   CKM_ECDSA_KEY_PAIR_GEN
   CKM_ECDH1_DERIVE
   CKM_ECDH1_COFACTOR_DERIVE
   CKM_ECMQV_DERIVE
   CKM_DH_PKCS_KEY_PAIR_GEN
   CKM_DH_PKCS_PARAMETER_GEN
   CKM_DH_PKCS_DERIVE
}
attributes (*, CKO_PRIVATE_KEY, *) = {
CKA_SENSITIVE = true
CKA_SIGN = true
CKA_DECRYPT = true
CKA_DERIVE=true}
attributes (*, CKO_PUBLIC_KEY, *) = {
CKA_VERIFY = true
CKA_ENCRYPT = true
CKA_DERIVE = true}
attributes (*, CKO_SECRET_KEY, *) = {
CKA_SENSITIVE = true
CKA_ENCRYPT = true
CKA_DECRYPT = true
CKA_SIGN = true
CKA_VERIFY = true}
```

Pour le périphérique nCipher :

```
======= ncipher_gen2.cfg.jsse
#nCipher nShield, nForce - Generation 2 cards
name =B2Bi
library=/opt/nfast/toolkits/pkcs11/libcknfast.so
description= IBM SSP NCIPHER HSM ADAPTER config for JSSE

slotListIndex =  1
disabledMechanisms = {
   CKM_MD5
   CKM_SHA_1
   CKM_MD5_HMAC
   CKM_SHA_1_HMAC
   CKM_SHA256_HMAC
   CKM_SHA384_HMAC
   CKM_SHA512_HMAC
   CKM_EC_KEY_PAIR_GEN
   CKM_ECDSA_KEY_PAIR_GEN
   CKM_ECDSA
   CKM_ECDSA_SHA1
   CKM_ECDH1_DERIVE
   CKM_ECDH1_COFACTOR_DERIVE
   CKM_ECMQV_DERIVE
}
attributes(*, CKO_SECRET_KEY, *) = {
   CKA_ENCRYPT=true
   CKA_DECRYPT=true}
```

```
attributes (*, CKO_PRIVATE_KEY, *) = {
   CKA_TOKEN=false
   CKA_SIGN=true
   CKA_SENSITIVE=false}
attributes(GENERATE, CKO_PRIVATE_KEY, CKK_RSA) = {
   CKA_DECRYPT=true
   CKA_UNWRAP=true
   CKA_EXTRACTABLE=true}
attributes(GENERATE, CKO_PUBLIC_KEY, *) = {
   CKA_TOKEN=false
   CKA_VERIFY=true}
attributes(*, CKO_PUBLIC_KEY, CKK_RSA) = {
   CKA_ENCRYPT=true
   CKA_WRAP=true
   CKA_VERIFY=true}
attributes(IMPORT, CKO_PRIVATE_KEY, CKK_RSA) = {
   CKA_EXTRACTABLE=true
   CKA_DECRYPT=true
   CKA_UNWRAP=true
   CKA_DERIVE=true}
```

Remarque : SafeNet Luna ne vous permet pas d'importer une clé privée créée en externe. Vous devez les créer et les stocker sur le périphérique HSM.

Remarques

Le présent document peut être proposé par IBM dans plusieurs langues différentes. Toutefois, il peut être nécessaire de posséder une copie du produit ou de la version du produit dans cette langue pour pouvoir y accéder.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7 Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet (DBCS) peuvent être obtenues auprès du Département de la propriété intellectuelle IBM de votre pays ou par demande écrite envoyée à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

LE PRÉSENT DOCUMENT EST LIVRE EN L'ÉTAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DÉCLINE NOTAMMENT TOUTE RESPONSABILITÉ RELATIVE A CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DÉFAUT D'APTITUDE A L'EXÉCUTION

© Copyright IBM Corp. 2000, 2015

D'UN TRAVAIL DONNÉ. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites dans certaines transactions, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performances et les exemples de clients ne sont présentés qu'à des fins d'illustration. Les performances réelles peuvent varier en fonction des configurations et des conditions d'exploitation spécifiques.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes et de sociétés serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. IBM ne peut donc pas garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les exemples de programmes sont fournis "en l'état", sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable des dommages liés à l'utilisation de ces programmes exemples.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme indiqué dans la colonne suivante.

© 2015.
Des segments de code sont dérivés des Programmes exemples d'IBM Corp.
© Copyright IBM Corp. 2015.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Adobe, le logo Adobe, PostScript et le logo PostScript sont des marques d'Adobe Systems Incorporated aux États-Unis et/ou dans certains autres pays.

IT Infrastructure Library est une marque de The Central Computer and Telecommunications Agency qui fait désormais partie de The Office of Government Commerce.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium et Pentium sont des marques d'Intel Corporation ou de ses filiales aux États-Unis et/ou dans certains autres pays.

Linux est une marque de Linus Torvalds aux États-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux États-Unis et/ou dans certains autres pays.

ITIL est une marque de The Office of Government Commerce et est enregistrée au bureau américain Patent and Trademark Office.

UNIX est une marque enregistrée de The Open Group aux États-Unis et/ou dans certains autres pays.

Java™ ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Cell Broadband Engine est une marque de Sony Computer Entertainment, Inc. aux États-Unis et/ou dans certains autres pays et est utilisée sous licence.

Linear Tape-Open, LTO, le logo LTO, Ultrium et le logo Ultrium sont des marques de HP, IBM Corp. et Quantum aux États-Unis et/ou dans certains autres pays.

Connect Control Center, Connect:Direct, Connect:Enterprise, Gentran, Gentran:Basic, Gentran:Control, Gentran:Director, Gentran:Plus, Gentran:Realtime, Gentran:Server, Gentran:Viewpoint, Sterling Commerce, Sterling Information Broker et Sterling Integrator sont des marques de Sterling Commerce, Inc., une filiale d'IBM Company.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Termes et conditions applicables à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes :

Applicabilité

Les présentes dispositions viennent s'ajouter à toute autre condition d'utilisation applicable au site Web IBM.

Usage personnel :

Vous pouvez reproduire ces publications pour un usage personnel et non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez distribuer ou publier tout ou partie de ces publications ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

Utilisation commerciale

Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient

conservées. Vous ne pouvez reproduire, distribuer, afficher ou publier tout ou partie de ces publications en dehors de votre entreprise, ou en faire des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits

Sauf autorisation expresse, aucun autre droit, autorisation ou licence n'est accordé de façon explicite ou implicite aux publications ou à toute information, donnée ou tout logiciel ou autre propriété intellectuelle contenu dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVRÉES EN L'ÉTAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DÉCLINE NOTAMMENT TOUTE RESPONSABILITÉ RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DÉFAUT D'APTITUDE A L'EXÉCUTION D'UN TRAVAIL DONNÉ.

Numéro de programme :

Imprimé en France