# CA Performance Center

## Manuel de l'utilisateur de l'authentification unique

2.4

# Produits CA Technologies référencés

Ce document fait référence aux produits CA Technologies suivants :

- CA Performance Center
- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor

# Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

# Table des matières

# Chapitre 1: Personnalisation de l'authentification dans CA Performance Center

Ce chapitre traite des sujets suivants :



## CA Single Sign-On

L'*authentification unique* est le schéma d'authentification de CA Performance Center et de toutes les sources de données prises en charge. Une fois authentifiés sur CA Performance Center, les utilisateurs peuvent naviguer à travers la console et les sources de données enregistrées sans avoir à se connecter une seconde fois.

En assurant une navigation transparente entre des interfaces de produit distinctes et divers niveaux de données, l'authentification unique optimise et facilite le travail des opérateurs qui analysent les données de performance et de statut. Ainsi, un utilisateur qui se connecte à CA Performance Center, puis accède à un niveau plus détaillé de l'interface de source de données, n'a pas à se reconnecter.

CA Performance Center utilise une architecture distribuée. Une instance du site Web d'authentification unique est installée automatiquement sur tous les serveurs où une source de données prise en charge ou CA Performance Center est installé. L'architecture distribuée permet aux utilisateurs d'accéder à des produits de source de données CA spécifiques en se connectant aux serveurs où ces produits sont installés.

## Authentification de CA Performance Center et sécurité

L'authentification unique fournit des services d'authentification à CA Performance Center et aux sources de données prises en charge. Elle prend également en charge des schémas d'authentification externes, tels que LDAP et SAML 2.0. Cette prise en charge vous permet d'intégrer CA Performance Center et d'autres produits de source de données CA au même schéma d'authentification, à l'échelle de l'entreprise.

La fonction d'audit de sécurité de l'authentification unique consigne des informations sur qui se connecte et à quelle heure de la journée. Sur des serveurs Linux, le journal est enregistré à l'emplacement suivant :
`[répertoire_installation]/PerformanceCenter/sso/logs`

Et sur les serveurs Windows sur lesquels les sources de données sont installées, le journal est enregistré dans le répertoire suivant :
`[répertoire_installation]\Portal\SSO\logs`

## Méthodes d'authentification

Le composant d'authentification unique fournit la page de connexion qui prend en charge l'authentification des utilisateurs dans CA Performance Center et dans les produits de source de données. L'authentification unique prend en charge les méthodes d'authentification suivantes :

- L'authentification Produit, qui est basée sur les comptes d'utilisateurs
- LDAP
- SAML (Security Assertion Markup Language) 2.0

L'administrateur de CA Performance Center peut modifier les paramètres d'une instance particulière de l'authentification unique. Vous pouvez par exemple définir l'authentification LDAP dans l'authentification unique. Vous pouvez également configurer le chiffrement facultatif avec le protocole SSL (Secure Sockets Layer) ou modifier le répertoire virtuel par défaut.

**Remarque** : Puisque nous sommes dans une architecture distribuée, toute mise à jour du site Web d'authentification unique affecte seulement les produits de source de données qui s'exécutent sur le même serveur.

## Prise en charge des sources de données

CA Single Sign-On prend en charge toutes les sources de données suivantes :

- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor

L'outil de configuration de l'authentification unique a été conçu pour s'exécuter sur des systèmes Linux. Toutefois, vous pouvez également le déployer sur les serveurs Windows sur lesquels les sources de données sont installées. Si vous lancez cet outil à partir d'un serveur Windows, connectez-vous en tant qu'administrateur sur ce serveur.

Vous pouvez également exécuter l'outil de configuration sous Linux et envoyer des instructions de configuration aux sources de données s'exécutant sous Windows à l'aide de l'option Valeur distante.

L'outil de configuration est installé à suivant sous Linux :
`[répertoire_installation]/CA/PerformanceCenter`

Et sur les serveurs Windows sur lesquels les sources de données sont installées, l'outil de configuration est installé dans le répertoire suivant :
`[répertoire_installation]\Portal\SSO\bin\SsoConfig.exe`

## Outil de configuration de l'authentification unique

L'outil de configuration de l'authentification unique est une application de ligne de commande qui permet aux administrateurs de définir les paramètres du site Web d'authentification unique et les produits de source de données CA associés.

**Remarque :** L'option Valeur distante de l'outil de configuration propage les paramètres pour chaque source de données enregistrée. Utilisez l'option Substitution locale pour remplacer les paramètres propagés sur un serveur sélectionné.

L'outil de configuration de l'authentification unique a été conçu pour s'exécuter sur des systèmes Linux. Toutefois, vous pouvez également le déployer sur les serveurs Windows sur lesquels les sources de données sont installées. Si vous lancez cet outil à partir d'un serveur Windows, connectez-vous en tant qu'administrateur sur ce serveur.

L'outil de configuration de l'authentification unique permet d'effectuer les tâches suivantes :

- Configurer des produits de source de données pour utiliser l'authentification LDAP.

  Tous les paramètres LDAP de chaque produit sont mis à jour à l'aide de cet outil. Vous pouvez également tester la configuration LDAP actuelle pour vérifier les paramètres.

- Configurer des produits de source de données pour utiliser l'authentification SAML 2.0.

  Outre l'outil de configuration, l'administrateur doit également procéder à certaines étapes au niveau du fournisseur d'identités pour configurer l'authentification SAML 2.0.

- Mettre à jour le répertoire virtuel d'authentification unique référencé par chaque produit.

  Si vous avez ajouté un schéma de chiffrement ou modifié le répertoire virtuel d'authentification unique, vous pouvez utiliser cet outil pour synchroniser les produits de source de données. Par exemple, les sources de données du serveur modifié ont besoin d'instructions pour savoir où rediriger les utilisateurs dont l'authentification a échoué.

- Activez la communication entre les serveurs exécutant des logiciels CA à l'aide du protocole HTTPS.

  Cette modification affecte aussi bien le schéma que le port de l'URL d'authentification unique. L'outil de configuration de l'authentification unique permet aux administrateurs de mettre facilement à jour ces valeurs dans tous les produits de source de données voulus.

## Sauvegarde des fichiers de configuration de l'authentification unique

Les paramètres que vous modifiez à l'aide de l'outil de configuration sont enregistrés dans des fichiers de configuration. Nous vous recommandons de créer régulièrement des copies de sauvegarde de ces fichiers pour éviter de perdre vos paramètres d'authentification unique. Utilisez rsync ou une autre méthode préférée (un script par exemple) pour sauvegarder ces fichiers automatiquement ou avant une mise à niveau.

Ajoutez les fichiers suivants à vos procédures de sauvegarde :

*répertoire_installation*/CA/PerformanceCenter/sso/start.ini
*répertoire_installation*/CA/PerformanceCenter/PC/start.ini

Sauvegardez également les répertoires suivants :

*répertoire_installation*/CA/PerformanceCenter/sso/webapps/sso/configuration
*répertoire_installation*/CA/PerformanceCenter/sso/etc
*répertoire_installation*/CA/PerformanceCenter/sso/conf
*répertoire_installation*/CA/PerformanceCenter/PC/etc
*répertoire_installation*/CA/PerformanceCenter/PC/conf

**Remarque** : Le répertoire d'installation par défaut est /opt/CA.

# Mise à jour des paramètres du site Web d'authentification unique

L'outil de configuration de l'authentification unique vous permet de modifier les paramètres par défaut du site Web d'authentification unique. Vous pouvez par exemple modifier le répertoire virtuel de ce dernier. Le répertoire virtuel doit utiliser un schéma de chiffrement pour les communications entre les serveurs CA.

Vous pouvez modifier d'autres paramètres qui affectent le comportement d'authentification unique lorsque les utilisateurs essayent de se connecter. Certains paramètres affectent également le comportement de l'interface utilisateur, par exemple le délai après lequel l'utilisateur est automatiquement déconnecté après une période d'inactivité.

**Important :** Les mises à jour du site Web d'authentification unique affectent uniquement les produits de source de données CA qui s'exécutent sur le même serveur, car l'architecture du logiciel est distribuée.

**Procédez comme suit:**

1. Connectez-vous au serveur où CA Performance Center ou un produit de source de données CA est installé.

   Connectez-vous en tant qu'utilisateur root ou à l'aide de la commande sudo.

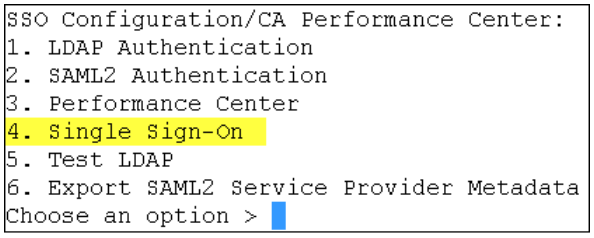
2. Lancez l'outil de configuration de l'authentification unique en exécutant la commande ./SsoConfig dans le répertoire suivant :

   `[répertoire_installation]/CA/PerformanceCenter`

   Vous êtes invité à sélectionner une option. Les options disponibles correspondent à des applications CA s'exécutant sur le serveur local.

3. Lors de la sélection des paramètres, utilisez les commandes suivantes :
   - q (quitter)
   - b (revenir au menu précédent)
   - u (mettre à jour)
   - r (réinitialiser)
4. Entrez 1 pour configurer CA Performance Center.

   Vous êtes invité à sélectionner une option.




5. Entrez 4 pour l'authentification unique.

   Vous êtes invité à définir la priorité.

   Le paramètre de priorité s'applique uniquement à CA Performance Center.
6. Entrez l'une des options ci-après :

   **1. Valeur distante**

   Se rapporte à des paramètres que seuls les administrateurs peuvent modifier. Ces paramètres sont appliqués à tous les autres produits CA enregistrés sur cette instance de CA Performance Center. Les paramètres de valeur distante sont utilisés uniquement s'il n'y a pas de valeur de substitution locale correspondante.

   **2. Substitution locale**

   Se rapporte à des paramètres pouvant être modifiés pour tous les produits. La valeur de substitution locale a priorité sur la valeur distante et sur les paramètres par défaut.

   Vous êtes invité à sélectionner une propriété à configurer.

7. Sélectionnez au moins une des propriétés ci-dessous. Lorsque vous y êtes invité, entrez u pour mettre à jour la valeur et en indiquer une nouvelle :

   **1. Utilisateur anonyme activé**

   Indique si la page de connexion s'affiche lorsque les utilisateurs essayent de se connecter à une interface de source de données. Si ce paramètre est activé, vous devrez renseigner le champ du paramètre ID d'utilisateur anonyme. L'utilisateur ne voit pas la page de connexion lorsqu'il tente de se connecter. Il est connecté en tant qu'utilisateur associé au paramètre ID d'utilisateur anonyme.

   Le paramètre Activer la connexion pour l'utilisateur de l'hôte local est prioritaire lorsque les conditions suivantes sont remplies :

   - L'utilisateur se connecte à partir du serveur d'authentification unique.
   - Les paramètres Activer la connexion pour l'utilisateur de l'hôte local et Utilisateur anonyme activé sont tous deux activés.

   **Valeur par défaut** : Désactivé.

   **Remarque** : La connexion Utilisateur anonyme a priorité sur l'authentification Windows.

   **2. ID d'utilisateur anonyme**

   Indique le nom d'utilisateur qui est utilisé pour l'authentification automatique de l'utilisateur, sans passer par la page de connexion. Ce paramètre est uniquement utilisé si le paramètre Utilisateur anonyme activé est activé Sélectionnez l'une des valeurs ci-dessous.

   - **1** - Le nom d'utilisateur associé au compte d'administrateur par défaut (administration).
   - **2** - Le nom d'utilisateur associé au compte d'utilisateur par défaut (utilisateur).
   - Un autre nom d'utilisateur présent dans la base de données de CA Performance Center.

**3. Activer la page de connexion pour l'utilisateur de l'hôte local**

Indique si la page de connexion s'affiche lorsque l'utilisateur se connecte à partir du serveur où l'authentification unique est installée.

Si ce paramètre est activé, la page de connexion s'affiche, même si l'utilisateur se connecte à partir du serveur d'authentification unique.

Si ce paramètre est désactivé, les règles suivantes s'appliquent :

- Le paramètre Activer la connexion pour l'utilisateur de l'hôte local doit être activé.
- La valeur du paramètre ID de l'utilisateur de l'hôte local doit contenir un nom d'utilisateur de produit valide. Cette valeur est utilisée pour connecter l'utilisateur à l'interface du logiciel, sans passer par la page de connexion.

**Valeur par défaut** : Désactivé.

**4. Activer la connexion pour l'utilisateur de l'hôte local**

Indique si les utilisateurs sont connectés automatiquement, c'est-à-dire sans passer par la page de connexion, lorsqu'ils se connectent à partir du serveur d'authentification unique. Si ce paramètre est activé, vous devrez renseigner le champ du paramètre ID de l'utilisateur de l'hôte local.

- Si le paramètre Activer la page de connexion pour l'utilisateur de l'hôte local est activé, ce paramètre est utilisé lorsque l'utilisateur clique sur l'option permettant de se connecter sans entrer de nom d'utilisateur ni de mot de passe. L'utilisateur est alors connecté au logiciel en tant qu'utilisateur associé au paramètre ID de l'utilisateur de l'hôte local.
- Si l'utilisateur fournit un nom d'utilisateur et un mot de passe, ces informations d'identification sont utilisées pour l'authentification.
- Si ce paramètre est activé mais que le paramètre Activer la page de connexion pour l'utilisateur de l'hôte local est désactivé, l'utilisateur ne passe pas par la page de connexion. Il est connecté à l'interface à l'aide de la valeur du paramètre ID de l'utilisateur de l'hôte local.
- Si l'utilisateur se connecte à partir du serveur d'authentification unique et que les paramètres Activer la connexion pour l'utilisateur de l'hôte local et Utilisateur anonyme activé sont tous deux activés, le paramètre Activer la connexion pour l'utilisateur de l'hôte local a priorité.

**Valeur par défaut** : Désactivé.

**5. ID de l'utilisateur de l'hôte local**

Indique l'ID d'utilisateur qui est utilisé pour authentifier les utilisateurs automatiquement, c'est-à-dire sans passer par la page de connexion, lorsqu'ils se connectent au serveur d'authentification unique. Ce paramètre est utilisé uniquement si le paramètre Activer la connexion pour l'utilisateur de l'hôte local est activé. Entrez l'une des valeurs ci-dessous.

**1** - Le nom d'utilisateur associé au compte d'administrateur par défaut (administration).

**2** - Le nom d'utilisateur associé au compte d'utilisateur par défaut (utilisateur).

**6. Délai d'expiration de cookie en minutes**

Indique le nombre de minutes après lequel un cookie d'authentification unique expire. Chaque fois qu'un utilisateur effectue une action dans une interface de source de données, le délai d'expiration de cookie se réinitialise. Si le délai expire, l'utilisateur est déconnecté et doit à nouveau s'authentifier.

**Par défaut** : 20 minutes

**7. Clé de chiffrement/déchiffrement**

Indique la clé qui est utilisée pour chiffrer et déchiffrer le cookie d'authentification unique.

**8. Algorithme de chiffrement**

Indique l'algorithme de chiffrement qui est utilisé pour chiffrer et déchiffrer le cookie d'authentification unique. La valeur doit être DES (Data Encryption Standard) ou AES (Advanced Encryption Standard).

**9. Délai en secondes après échec**

Indique le nombre de secondes qui s'écoulent après l'échec d'une tentative de connexion via l'application d'authentification unique.

**10. Activer Mémoriser mes informations**

Indique si la case à cocher Mémoriser mes informations est affichée sur la page de connexion. Le paramètre Mémoriser mes informations détermine si l'utilisateur est automatiquement déconnecté lorsque le délai du cookie expire.

**Par défaut** : Activé

**11. Délai d'expiration en jours de l'option Mémoriser mes informations**

Définit le nombre de jours après lequel un utilisateur qui a sélectionné Mémoriser mes informations sur la page de connexion doit à nouveau s'authentifier. Ce paramètre est uniquement utilisé si le paramètre Activer Mémoriser mes informations est activé La valeur 0 indique que le paramètre Mémoriser mes informations n'expire pas ; l'utilisateur doit cliquer sur le lien de déconnexion de l'interface du produit de source de données.

**12. Schéma**

Définit le schéma d'URL que les produits de source de données peuvent utiliser pour accéder à l'application d'authentification unique. Si vous utilisez SSL, la valeur est https.

**13. Port**

Définit le port d'URL que les produits de source de données peuvent utiliser pour accéder à l'application d'authentification unique.

**14. Répertoire virtuel**

Indique le nom du répertoire virtuel de l'authentification unique.

**Valeur par défaut** : SingleSignOn

**Remarque** : Si vous modifiez la valeur de l'un des paramètres précédents, la valeur par défaut n'est pas remplacée, mais la nouvelle valeur a désormais priorité. La nouvelle valeur est en fait une substitution locale.

8. Une fois les paramètres par défaut modifiés, entrez b.
9. Vous retournez à l'ensemble d'options précédent.
10. Entrez à nouveau b pour retourner au premier ensemble d'options.
11. Entrez q pour fermer l'outil de configuration d'authentification unique.

    L'outil de configuration d'authentification unique se ferme.

    CA Performance Center dirige tous les utilisateurs non authentifiés sur le site Web d'authentification unique à l'aide des nouvelles valeurs que vous avez indiquées.

# Mise à jour des paramètres du site Web de CA Performance Center

L'outil de configuration d'authentification unique vous permet de modifier les paramètres par défaut du site Web et du service Web de CA Performance Center. Vous pouvez par exemple définir un hôte ou un numéro de port différent pour le service Web de CA Performance Center. Ces paramètres indiquent à l'application d'authentification unique comment se connecter à CA Performance Center.

**Procédez comme suit:**

1. Connectez-vous au serveur où CA Performance Center ou un produit de source de données CA est installé.

   Connectez-vous en tant qu'utilisateur root ou à l'aide de la commande sudo.

2. Lancez l'outil de configuration de l'authentification unique en exécutant la commande ./SsoConfig dans le répertoire suivant :

   `[répertoire_installation]/CA/PerformanceCenter`

   Vous êtes invité à sélectionner une option. Les options disponibles correspondent à des applications CA s'exécutant sur le serveur local.

3. Lors de la sélection des paramètres, utilisez les commandes suivantes :

   - q (quitter)
   - b (revenir au menu précédent)
   - u (mettre à jour)
   - r (réinitialiser)

4. Entrez 1 pour configurer CA Performance Center.

   Vous êtes invité à sélectionner une option de configuration.

   ```
   SSO Configuration/CA Performance Center:
   1. LDAP Authentication
   2. SAML2 Authentication
   3. Performance Center
   4. Single Sign-On
   5. Test LDAP
   6. Export SAML2 Service Provider Metadata
   Choose an option >
   ```

5. Entrez 3 pour Performance Center.

   Vous êtes invité à définir la priorité.

   Le paramètre de priorité s'applique uniquement à CA Performance Center.

6. Entrez l'une des options ci-après :

   **1. Valeur distante**

   Se rapporte à des paramètres que seuls les administrateurs peuvent modifier. Ces paramètres sont appliqués à tous les autres produits CA enregistrés sur cette instance de CA Performance Center. Les paramètres de valeur distante sont utilisés uniquement s'il n'y a pas de valeur de substitution locale correspondante.

   **2. Substitution locale**

   Se rapporte à des paramètres pouvant être modifiés pour tous les produits. La valeur de substitution locale a priorité sur la valeur distante et sur les paramètres par défaut.

   Vous êtes invité à sélectionner une propriété à configurer.

7. Sélectionnez au moins une des propriétés ci-dessous. Lorsque vous y êtes invité, entrez u pour mettre à jour la valeur et en indiquer une nouvelle :

   **1. Schéma du service Web**

   Indique le schéma d'URL que l'application d'authentification unique peut utiliser pour accéder au service Web de CA Performance Center. Cette valeur doit être https si vous utilisez SSL pour le chiffrement.

   **2. Hôte du service Web**

   Indique l'URL de l'hôte à partir duquel l'application d'authentification unique peut accéder au service Web de CA Performance Center.

   **3. Port du service Web**

   Indique le port d'URL que l'application d'authentification unique peut utiliser pour accéder au service Web de CA Performance Center.

   **4. Inventaire du service Web**

   Indique le chemin d'URL que l'application d'authentification unique peut utiliser pour accéder au service Web Inventaire de CA Performance Center.

   **5. Demande de produit du service Web**

   Indique le chemin d'URL que l'application d'authentification unique peut utiliser pour accéder au service Web Demande de produit de CA Performance Center.

   **6. Schéma du site Web**

   Indique le schéma d'URL que l'application d'authentification unique peut utiliser pour accéder à CA Performance Center. Si vous avez configuré SSL, utilisez https.

   **7. Hôte du site Web**

   Indique l'hôte de l'URL d'URL que l'application d'authentification unique peut utiliser pour accéder à CA Performance Center.

   **8. Port du site Web**

   Indique le port d'URL que l'application d'authentification unique peut utiliser pour accéder à CA Performance Center.

   **9. Chemin du site Web**

   Indique le chemin d'URL que l'application d'authentification unique peut utiliser pour accéder à CA Performance Center.

   **10. SMTP activé**

   Indique si le protocole SMTP (Simple Mail Transfer Protocol) est activé afin de permettre aux opérateurs de CA Performance Center d'envoyer par courriel des rapports et des notifications d'événement.

   **Valeur par défaut** : Désactivé.

**11. Adresse du serveur SMTP**

Indique l'adresse IP du serveur SMTP.

**Valeur par défaut** : Désactivé.

**12. Ports SMTP**

Spécifie le port à utiliser pour les demandes SMTP.

**Valeur par défaut** : Port 25.

**13. SMTP SSL**

Indique s'il convient d'utiliser le chiffrement SSL lors de l'envoi de courriels depuis CA Performance Center ou depuis d'autres produits de source de données CA. Avant d'activer cette option, vérifiez que SSL est correctement configuré sur votre système.

**Valeur par défaut** : Désactivé.

**14. Adresse électronique de réponse**

Indique l'adresse à laquelle sont envoyées les réponses aux courriels générés par CA Performance Center. Entrez u pour mettre la valeur à jour et indiquer une adresse électronique. Utilisez le format username@mydomain.com.

**15. Format du courriel**

Définit le format des courriels envoyés par CA Performance Center. Entrez u pour mettre la valeur à jour et indiquer HTML ou texte.

**16. Nom d'utilisateur SMTP**

Indique le nom d'utilisateur à utiliser lorsque le serveur de messagerie défie une demande SMTP. Entrez un nom d'utilisateur ou indiquez une chaîne vide pour désactiver l'authentification côté client.

**17. Mot de passe SMTP**

Indique le nom d'utilisateur à utiliser lorsque le serveur de messagerie défie une demande SMTP. Entrez un mot de passe valide. Le champ du paramètre Nom d'utilisateur SMTP doit être renseigné.

8. Une fois les paramètres par défaut modifiés, entrez b.

   Vous retournez à l'ensemble d'options précédent.

9. Entrez à nouveau b pour retourner au premier ensemble d'options.

10. Entrez q pour quitter le programme.

    L'outil de configuration d'authentification unique se ferme.

    CA Performance Center dirige tous les utilisateurs sur le site Web d'authentification unique en utilisant les nouvelles valeurs que vous avez indiquées.

# Chapitre 2: Configuration de l'authentification LDAP

Ce chapitre traite des sujets suivants :



## Prise en charge de LDAP

L'authentification unique intégrant LDAP, les opérateurs peuvent s'authentifier sur un serveur LDAP (Lightweight Directory Access Protocol) s'exécutant dans votre environnement. Une fois authentifiés, ils sont mappés vers un compte d'utilisateur que l'administrateur peut définir : un compte d'utilisateur prédéfini ou un compte personnalisé.

L'outil de configuration d'authentification unique vous permet de définir précisément la manière dont le serveur d'authentification unique se connecte au serveur LDAP. Vous pouvez également mapper des utilisateurs de CA Performance Center particuliers vers les comptes d'utilisateurs qui prennent en charge leur flux de travaux tout en protégeant les données sensibles.

**Remarque** : Les modifications apportées dans l'outil de configuration de l'authentification unique affectent uniquement les utilisateurs LDAP nouvellement créés. Elles ne s'appliquent pas aux utilisateurs LDAP déjà enregistrés dans CA Performance Center.

Les paramètres LDAP disponibles dans l'outil de configuration de l'authentification unique vous permettent d'intégrer CA Infrastructure Management et toutes les sources de données enregistrées, dans un schéma d'authentification existant. Par exemple, le serveur LDAP peut autoriser l'accès à des groupes d'utilisateurs qui sont mappés vers un compte d'utilisateur personnalisé unique dans CA Performance Center. Vous pouvez personnaliser à votre guise les noms de compte et groupes LDAP existants. Les paramètres Etendue de la recherche vous permettent de déterminer les modalités de la recherche dans les annuaires. Vous pouvez en outre sélectionner les propriétés de compte d'utilisateur qui sont examinées lors de la validation des utilisateurs.

# Activation de l'authentification LDAP sans mécanisme d'authentification

Utilisez l'outil de configuration d'authentification unique pour indiquer aux sources de données enregistrées d'utiliser le même schéma LDAP pour l'authentification des utilisateurs. Avec l'outil de configuration d'authentification unique vous pouvez définir des paramètres qui permettent au serveur CA de se connecter au serveur LDAP de façon sécurisée. Vous pouvez également associer des utilisateurs figurant dans le catalogue LDAP à des comptes d'utilisateurs prédéfinis ou personnalisés dans CA Performance Center.

Les opérations à effectuer pour activer l'authentification LDAP sont légèrement différentes si vous utilisez un mécanisme d'authentification (page 26), comme GSSAPI. Sans un mécanisme d'authentification, vous devez utiliser un compte de service et le lier au serveur LDAP. Ce compte requiert un accès en lecture au serveur LDAP et des droits de recherche. Vous devez fournir le nom unique complet de l'utilisateur de la connexion et activer le paramètre Liaison utilisateur.

L'application d'authentification unique établit une liaison au serveur LDAP à l'aide des informations d'identification que vous fournissez pour les paramètres Utilisateur de la connexion et Mot de passe de connexion. Une recherche de répertoire est effectuée en fonction de la chaîne saisie pour le paramètre Chaîne de recherche. Les résultats de la recherche incluent le nom unique de l'utilisateur. L'application d'authentification unique établit une seconde liaison au serveur LDAP à l'aide du nom unique et du mot de passe.

**Important :** Dans les cas où aucun mécanisme d'authentification n'est utilisé, il est fortement recommandé d'établir une connexion SSL au serveur LDAP. Si le mode SSL n'est pas utilisé, les mots de passe sont transmis au serveur LDAP en texte clair.

**Procédez comme suit:**

1. Connectez-vous au serveur où CA Performance Center ou un produit de source de données CA est installé.

   Connectez-vous en tant qu'utilisateur root ou à l'aide de la commande sudo.

2. Lancez l'outil de configuration de l'authentification unique en exécutant la commande ./SsoConfig dans le répertoire suivant :

   *répertoire_installation*/CA/PerformanceCenter

   Vous êtes invité à sélectionner une option. Les options disponibles correspondent à des applications CA s'exécutant sur le serveur local.

3. Lors de la sélection des paramètres, utilisez les commandes suivantes :
   - q (quitter)
   - b (revenir au menu précédent)
   - u (mettre à jour)
   - r (réinitialiser)
4. Entrez 1 pour configurer CA Performance Center.

   Vous êtes invité à sélectionner une option.
5. Entrez 1 pour l'authentification LDAP.

   Vous êtes invité à définir la priorité.

   Le paramètre de priorité s'applique uniquement à CA Performance Center.
6. Entrez l'une des options ci-après :

   **1. Valeur distante**

   Se rapporte à des paramètres que seuls les administrateurs peuvent modifier. Ces paramètres sont appliqués à tous les autres produits CA enregistrés sur cette instance de CA Performance Center. Les paramètres de valeur distante sont utilisés uniquement s'il n'y a pas de valeur de substitution locale correspondante.

   **2. Substitution locale**

   Se rapporte à des paramètres pouvant être modifiés pour tous les produits. La valeur de substitution locale a priorité sur la valeur distante et sur les paramètres par défaut.

   Vous êtes invité à sélectionner une propriété à configurer.
7. Sélectionnez au moins une des propriétés ci-dessous. Lorsque vous y êtes invité, entrez u pour mettre à jour la valeur et en indiquer une nouvelle :

   **1. Utilisateur de la connexion**

   Définit l'ID d'utilisateur (ici, l'ID d'utilisateur du compte de service) utilisé par le serveur de connexion pour se connecter au serveur LDAP. Ce nom d'utilisateur LDAP est utilisé pour assurer la liaison avec le serveur.

   **Important :** Un compte de service disposant d'un accès en lecture au serveur LDAP et de droits de recherche est requis pour ce paramètre, si vous n'utilisez aucun mécanisme d'authentification, comme GSSAPI.

   **2. Mot de passe de connexion**

   Définit le mot de passe utilisé par le serveur de connexion pour se connecter au serveur LDAP.

   **Exemple** : Si le serveur de connexion utilise un compte fixe, entrez un texte conforme à l'exemple suivant :

   ```
   SomePassword
   ```

**3. Domaine de recherche**

Identifie le serveur LDAP et le port de connexion pour CA Single Sign-On. Identifie également l'emplacement de recherche des utilisateurs dans l'arborescence des répertoires lors de la vérification des informations d'identification des comptes d'utilisateur. Si vous n'indiquez aucun numéro de port après le serveur dans la chaîne, le port 389 est utilisé.

Utilisez le format suivant pour le domaine de recherche :

LDAP://*serveur_ldap*:*port*/*chemin_recherche*

**Remarque :** Le chemin de recherche est *obligatoire*.

**4. Chaîne de recherche**

Spécifie les critères utilisés pour localiser l'enregistrement adéquat de l'utilisateur. Fonctionne avec le paramètre Etendue de la recherche. Si seul un sous-ensemble d'utilisateurs LDAP est autorisé à se connecter, vous pouvez utiliser la chaîne de recherche pour rechercher plusieurs propriétés dans l'enregistrement. Ce paramètre peut prendre pour valeur tout critère de recherche LDAP valide.

**Exemple** :

```
(saMAccountName={0})
```

**5. Etendue de la recherche**

Spécifie les critères utilisés pour localiser l'enregistrement adéquat de l'utilisateur. Il est utilisé avec le paramètre Chaîne de recherche. Délimite la recherche effectuée par le serveur LDAP pour le compte d'utilisateur. Entrez l'une des valeurs ci-dessous.

**niveau 1**

Inclut le répertoire actuel dans la recherche. Limite la recherche au répertoire actuel, en excluant les objets des sous-répertoires.

**sous-arborescence**

Inclut tous les sous-répertoires dans la recherche. Recommandé pour la plupart des installations.

**base**

Limite la recherche à l'objet de base.

**6. Liaison utilisateur**

Indique s'il convient d'effectuer une étape d'authentification supplémentaire (liaison) à l'aide du nom unique et du mot de passe de l'utilisateur pour valider les informations d'identification fournies.

**Important :** Ce paramètre doit être défini sur Activé si vous avez entré un compte de service aux étapes 1 et 2.

**Valeur par défaut** : Désactivé.

**7. Chiffrement**

Spécifie le mécanisme d'authentification à utiliser lors de la seconde liaison au serveur LDAP.

**Valeur par défaut :** Simple.

**Valeurs acceptées :** Simple, GSSAPI, DIGEST-MD5.

**8. Utilisateur de compte**

Spécifie le compte par défaut de CA Performance Center vers lequel mapper des utilisateurs LDAP validés n'appartenant pas à un groupe. Fonctionne avec le paramètre Mot de passe du compte. Si un utilisateur valide ne correspond à aucune définition de groupe, l'utilisateur est connecté via l'ID d'utilisateur par défaut spécifié pour ce paramètre.

Pour permettre à tous les utilisateurs de se connecter avec leur propre nom d'utilisateur, entrez :

- {saMAccountName}
- {saMAccountName} or {CN}

**Remarque** : Le paramètre Utilisateur de compte correspond au champ d'une entrée de répertoire de cet utilisateur. Généralement, la valeur correspond à votre filtre de recherche.

**9. Clone par défaut de l'utilisateur de compte**

Définit le compte d'utilisateur à cloner si les utilisateurs LDAP validés appartiennent à un groupe non spécifié pour le paramètre Groupe.

**Exemple** : Entrez "utilisateur" si vous voulez attribuer des droits minimaux à ces utilisateurs.

**Remarque** : Un compte d'utilisateur est requis.

**10. Group (Groupe)**

Permet de déterminer la gestion de compte par défaut des comptes d'utilisateurs ou groupes de comptes sélectionnés.

**Exemple** : Pour permettre à tous les membres d'un groupe de se connecter à l'aide d'un compte d'administrateur, entrez :

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}" passwd=""
userClone="admin"/></LDAPGroups>
```

**11. Temporisation**

Spécifie la durée d'attente qu'observe CA Performance Center lors de la vérification des autorisations auprès du serveur LDAP. Lorsque le délai de vérification des autorisations expire, les utilisateurs qui tentent de se connecter se voient refuser l'accès. Pour afficher les erreurs, ouvrez le fichier SSOService.log. Le délai d'expiration par défaut est 10000.

8. Vérifiez que le statut du protocole LDAP est Activé. Si le statut du protocole LDAP est Désactivé, l'authentification utilise le référentiel d'utilisateurs interne de CA Performance Center.
9. Entrez q pour quitter le programme.

   L'outil de configuration se ferme.

### Exemple de configuration

1. Utilisateur de la connexion : CN=********,OU=Role-Based,OU=North America,DC=ca,DC=com  [nom unique complet du compte de service]
2. Mot de passe de connexion : ******* [mot de passe du compte de service]
3. Domaine de recherche : LDAP://******.ca.com/DC=ca,DC=com
4. Chaîne de recherche : (sAMAccountName={0})
5. Limite de recherche : sous-arborescence
6. Liaison d'utilisateur : Activé
7. Chiffrement : False
8. Utilisateur de compte : {sAMAccountName}
9. Clone par défaut de l'utilisateur de compte : user
10. Groupe : All employees
11. Krb5ConfigFile : krb5.conf

# Chiffrement de la connexion au serveur LDAP à l'aide de GSSAPI

CA Single Sign-On prend en charge les connexions chiffrées à l'aide de DIGEST-MD5 ou de GSSAPI. Lorsque vous utilisez une connexion chiffrée sur le serveur d'annuaire, aucun compte de service n'est requis pour la liaison au serveur LDAP (le paramètre UserBind défini dans l'outil de configuration d'authentification unique).

Pour utiliser GSSAPI pour le chiffrement, vous devez changer certains paramètres dans un fichier de configuration.

**Procédez comme suit:**

1. Connectez-vous au serveur où CA Performance Center ou un produit de source de données CA est installé.

   Connectez-vous en tant qu'utilisateur root ou à l'aide de la commande sudo.
2. Accédez au répertoire suivant :
   `[répertoire_installation]/webapps/sso/Configuration/`

3. Ouvrez le fichier krb5.conf dans ce répertoire pour le modifier.
4. Définissez les paramètres requis suivants :

```
[libdefaults]
        default_realm = CA.COM
[realms]
        CA.COM  = {
                kdc = EXAMPLE.CA.COM
                default_domain = CA.COM
}

[domain_realm]
       .CA.COM = CA.COM
}
```

   où :

   **[libdefaults]**

   Contient des valeurs par défaut pour la bibliothèque Kerberos V5.

   **default_realm**

   Mappe les noms de sous-domaines et de domaines vers les noms de domaines Kerberos. Permet aux programmes de déterminer le domaine pour un hôte, d'après son nom de domaine complet. Dans cet exemple, le domaine par défaut est CA.COM.

   **realms**

   Contient des informations concernant les noms de domaine Kerberos, qui décrivent l'emplacement de serveurs Kerberos et incluent d'autres informations spécifiques de domaine.

   **kdc**

   Est-ce que le centre de distribution clé Kerberos doit prendre en charge les services d'authentification. Par exemple, EXAMPLE.CA.COM.

   **default_domain**

   Domaine IP par défaut. Par exemple, CA.COM.

   **Remarque :** Votre administrateur Active Directory ou LDAP peut probablement vous fournir un fichier krb5.conf ou vous aider à en créer un.

5. Enregistrez vos modifications.
6. Suivez les étapes décrites dans la section Activation de l'authentification LDAP à l'aide d'un mécanisme de chiffrement (page 28) pour configurer l'authentification LDAP avec CA Single Sign-On.

# Activation de l'authentification LDAP à l'aide d'un mécanisme de chiffrement

Utilisez l'outil de configuration d'authentification unique pour indiquer aux sources de données enregistrées d'utiliser le même schéma LDAP pour l'authentification des utilisateurs. Avec l'outil de configuration d'authentification unique vous pouvez définir des paramètres qui permettent au serveur CA de se connecter au serveur LDAP de façon sécurisée. Lorsque vous utilisez Digest-MD5 ou GSSAPI pour chiffrer la connexion au serveur LDAP, une opération de liaison unique a lieu (spécifiée par l'utilisateur).

Vous pouvez également associer des utilisateurs figurant dans le catalogue LDAP à des comptes d'utilisateurs prédéfinis ou personnalisés dans CA Performance Center.

**Procédez comme suit:**

1. Connectez-vous au serveur où CA Performance Center ou un produit de source de données CA est installé.

   Connectez-vous en tant qu'utilisateur root ou à l'aide de la commande sudo.

2. Lancez l'outil de configuration de l'authentification unique en exécutant la commande ./SsoConfig dans le répertoire suivant :

   *répertoire_installation*/CA/PerformanceCenter

   Vous êtes invité à sélectionner une option. Les options disponibles correspondent à des applications CA s'exécutant sur le serveur local.

3. Lors de la sélection des paramètres, utilisez les commandes suivantes :
   - q (quitter)
   - b (revenir au menu précédent)
   - u (mettre à jour)
   - r (réinitialiser)

4. Entrez 1 pour configurer CA Performance Center.

   Vous êtes invité à sélectionner une option.

5. Entrez 1 pour l'authentification LDAP.

   Vous êtes invité à définir la priorité.

   Le paramètre de priorité s'applique uniquement à CA Performance Center.

6. Entrez l'une des options ci-après :

   **1. Valeur distante**

   Se rapporte à des paramètres que seuls les administrateurs peuvent modifier. Ces paramètres sont appliqués à tous les autres produits CA enregistrés sur cette instance de CA Performance Center. Les paramètres de valeur distante sont utilisés uniquement s'il n'y a pas de valeur de substitution locale correspondante.

   **2. Substitution locale**

   Se rapporte à des paramètres pouvant être modifiés pour tous les produits. La valeur de substitution locale a priorité sur la valeur distante et sur les paramètres par défaut.

   Vous êtes invité à sélectionner une propriété à configurer.

7. Sélectionnez au moins une des propriétés ci-dessous. Lorsque vous y êtes invité, entrez u pour mettre à jour la valeur et en indiquer une nouvelle :

   **1. Utilisateur de la connexion**

   Définit l'ID d'utilisateur utilisée par le serveur de connexion pour se connecter au serveur LDAP. Ce nom d'utilisateur LDAP est utilisé pour assurer la liaison avec le serveur. Un compte de service n'est généralement pas requis pour une connexion utilisant un mécanisme d'authentification, tel que GSSAPI.

   **Exemple** : Si le serveur de connexion utilise un compte fixe, entrez le texte en respectant la syntaxe suivante :

   ```
   CN=Utilisateur,cn=Utilisateurs,dc=domaine,dc=com
   ```

   Vous pouvez également entrer la valeur suivante, car la connexion utilise un mécanisme d'authentification :

   ```
   {0}
   ```

   Les configurations complexes ont besoin du nom d'utilisateur principal pour identifier l'utilisateur. Entrez {0} et utilisez l'adresse électronique comme nom de domaine. Par exemple :

   ```
   {0}@domaine.com
   ```

   Le serveur LDAP ne requiert généralement pas de nom unique complet pour une connexion chiffrée.

   **Remarque** : Pour des raisons de sécurité, ne créez pas de compte statique pour l'utilisateur de la connexion. L'authentification LDAP vérifie uniquement le mot de passe lors de la liaison avec le serveur. Si vous utilisez un compte statique, tout utilisateur figurant dans l'arborescence LDAP pourra se connecter à l'aide d'un quelconque mot de passe.

**2. Mot de passe de connexion**

Définit le mot de passe utilisé par le serveur de connexion pour se connecter au serveur LDAP.

**Exemple** : Si le serveur de connexion utilise un compte fixe, entrez un texte conforme à l'exemple suivant :

```
SomePassword
```

Vous pouvez également entrer la valeur suivante, car la connexion utilise un mécanisme d'authentification :

```
{1}
```

**3. Domaine de recherche**

Identifie le serveur LDAP et le port de connexion pour CA Single Sign-On. Identifie également l'emplacement de recherche des utilisateurs dans l'arborescence des répertoires lors de la vérification des informations d'identification des comptes d'utilisateur. Si vous n'indiquez aucun numéro de port après le serveur dans la chaîne, le port 389 est utilisé.

Utilisez le format suivant pour le domaine de recherche :

LDAP://*serveur_ldap*:*port*/*chemin_recherche*

**Remarque :** Le chemin de recherche est *obligatoire*.

**4. Chaîne de recherche**

Spécifie les critères utilisés pour localiser l'utilisateur correct dans l'annuaire. Fonctionne avec le paramètre Etendue de la recherche. Si seul un sous-ensemble d'utilisateurs LDAP est autorisé à se connecter, vous pouvez utiliser la chaîne de recherche pour rechercher plusieurs propriétés dans l'enregistrement. Ce paramètre peut prendre pour valeur tout critère de recherche LDAP valide.

**Exemple** :

```
(saMAccountName={0})
```

**5. Etendue de la recherche**

Spécifie les critères utilisés pour localiser l'enregistrement adéquat de l'utilisateur. Il est utilisé avec le paramètre Chaîne de recherche. Délimite la recherche effectuée par le serveur LDAP pour le compte d'utilisateur. Entrez l'une des valeurs ci-dessous.

**niveau 1**

Inclut le répertoire actuel dans la recherche. Limite la recherche au répertoire actuel, en excluant les objets des sous-répertoires.

**sous-arborescence**

Inclut tous les sous-répertoires dans la recherche. Recommandé pour la plupart des installations.

**base**

Limite la recherche à l'objet de base.

**6. Liaison utilisateur**

Indique s'il convient d'effectuer une étape d'authentification supplémentaire (liaison) à l'aide du nom unique et du mot de passe de l'utilisateur pour valider les informations d'identification fournies.

**Valeur par défaut** : Désactivé. Cette valeur est acceptable avec une connexion chiffrée.

**7. Chiffrement**

Spécifie le mécanisme d'authentification à utiliser lors de la liaison au serveur LDAP.

Dans ce cas (c'est-à-dire, avec un mécanisme d'authentification), entrez GSSAPI ou DIGEST-MD5, en fonction des mécanismes de votre serveur LDAP.

**Valeur par défaut :** Simple.

**Valeurs acceptées :** Simple, GSSAPI, DIGEST-MD5.

**8. Utilisateur de compte**

Spécifie le compte par défaut de CA Performance Center vers lequel mapper des utilisateurs LDAP validés n'appartenant pas à un groupe. Fonctionne avec le paramètre Mot de passe du compte. Si un utilisateur valide ne correspond à aucune définition de groupe, l'utilisateur est connecté via l'ID d'utilisateur par défaut spécifié pour ce paramètre.

Pour permettre à tous les utilisateurs de se connecter avec leur propre nom d'utilisateur, entrez :

- {saMAccountName}
- {saMAccountName} or {CN}

**Remarque** : Le paramètre Utilisateur de compte correspond au champ d'une entrée de répertoire de cet utilisateur. Généralement, la valeur correspond à votre filtre de recherche.

**9. Clone par défaut de l'utilisateur de compte**

Définit le compte d'utilisateur à cloner si les utilisateurs LDAP validés appartiennent à un groupe non spécifié pour le paramètre Groupes.

**Exemple** : Entrez "utilisateur" si vous voulez attribuer des droits minimaux à ces utilisateurs.

**Remarque** : Un compte d'utilisateur est requis.

**10. Group (Groupe)**

Permet de déterminer la gestion de compte par défaut des comptes d'utilisateurs ou groupes de comptes sélectionnés.

**Exemple** : Pour permettre à tous les membres d'un groupe de se connecter à l'aide d'un compte d'administrateur, entrez :

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}" passwd=""
userClone="admin"/></LDAPGroups>
```

**11. Temporisation**

Spécifie la durée d'attente qu'observe CA Performance Center lors de la vérification des autorisations auprès du serveur LDAP. Lorsque le délai de vérification des autorisations expire, les utilisateurs qui tentent de se connecter se voient refuser l'accès. Pour afficher les erreurs, ouvrez le fichier SSOService.log. Le délai d'expiration par défaut est 10000.

8. Vérifiez que le statut du protocole LDAP est Activé. Si le statut du protocole LDAP est Désactivé, l'authentification utilise le référentiel d'utilisateurs interne de CA Performance Center.
9. Entrez q pour quitter le programme.

   L'outil de configuration se ferme.

### Exemple de configuration

1. Configuration du service d'authentification unique/CA Performance Center/Authentification LDAP/Valeur distante :
2. Utilisateur de la connexion : {0}
3. Mot de passe de connexion : {1}
4. Domaine de recherche : LDAP://******.ca.com/DC=ca,DC=com
5. Chaîne de recherche : (sAMAccountName={0})
6. Limite de recherche : sous-arborescence
7. Liaison d'utilisateur : Désactivé
8. Chiffrement : DIGEST-MD5
9. Utilisateur de compte : {sAMAccountName}
10. Clone par défaut de l'utilisateur de compte : user
11. Groupe : All employees
12. Krb5ConfigFile : krb5.conf

**Informations complémentaires :**

Chiffrement de la connexion au serveur LDAP à l'aide de GSSAPI (page 26)

# Activation de l'authentification LDAPS

Utilisez l'outil de configuration de l'authentification unique pour indiquer aux sources de données enregistrées d'utiliser une connexion LDAPS (LDAP over SSL) pour l'authentification d'utilisateur sécurisée. Par défaut, le trafic LDAP est transmis sans garantie. Activez les connexions LDAPS en installant un certificat à partir d'une autorité de certification. Avec CA Single Sign-On, vous devez importer votre certificat dans le référentiel de clés approuvé Java.

Avec l'outil de configuration d'authentification unique vous pouvez définir des paramètres qui permettent au serveur CA de se connecter au serveur LDAP de façon sécurisée. Vous pouvez également associer des utilisateurs figurant dans le catalogue LDAP à des comptes d'utilisateurs prédéfinis ou personnalisés dans CA Performance Center.

**Procédez comme suit:**

1. Connectez-vous au serveur où CA Performance Center ou un produit de source de données CA est installé.

   Connectez-vous en tant qu'utilisateur root ou à l'aide de la commande sudo.

2. Pour obtenir votre certificat, suivez les instructions de la rubrique Importation du certificat LDAP (page 38) et importez-le dans le référentiel de clés Java.

3. Lancez l'outil de configuration de l'authentification unique en exécutant la commande ./SsoConfig dans le répertoire suivant :

   *répertoire_installation*/CA/PerformanceCenter

   Vous êtes invité à sélectionner une option. Les options disponibles correspondent à des applications CA s'exécutant sur le serveur local.

4. Lors de la sélection des paramètres, utilisez les commandes suivantes :

   - q (quitter)
   - b (revenir au menu précédent)
   - u (mettre à jour)
   - r (réinitialiser)

5. Entrez 1 pour configurer CA Performance Center.

   Vous êtes invité à sélectionner une option.

6. Entrez 1 pour l'authentification LDAP.

   Vous êtes invité à définir la priorité.

   Le paramètre de priorité s'applique uniquement à CA Performance Center.

7. Entrez l'une des options ci-après :

   **1. Valeur distante**

   Se rapporte à des paramètres que seuls les administrateurs peuvent modifier. Ces paramètres sont appliqués à tous les autres produits CA enregistrés sur cette instance de CA Performance Center. Les paramètres de valeur distante sont utilisés uniquement s'il n'y a pas de valeur de substitution locale correspondante.

   **2. Substitution locale**

   Se rapporte à des paramètres pouvant être modifiés pour tous les produits. La valeur de substitution locale a priorité sur la valeur distante et sur les paramètres par défaut.

   Vous êtes invité à sélectionner une propriété à configurer.

8. Sélectionnez au moins une des propriétés ci-dessous. Lorsque vous y êtes invité, entrez u pour mettre à jour la valeur et en indiquer une nouvelle :

   **1. Utilisateur de la connexion**

   Définit l'ID d'utilisateur utilisée par le serveur de connexion pour se connecter au serveur LDAP. Ce nom d'utilisateur LDAP est utilisé pour assurer la liaison avec le serveur. Un compte de service n'est généralement pas requis pour une connexion utilisant un mécanisme d'authentification, tel que GSSAPI.

   **Exemple** : Si le serveur de connexion utilise un compte fixe, entrez le texte en respectant la syntaxe suivante :

   ```
   CN=Utilisateur,cn=Utilisateurs,dc=domaine,dc=com
   ```

   Vous pouvez également entrer la valeur suivante, car la connexion utilise un mécanisme d'authentification :

   ```
   {0}
   ```

   Les configurations complexes ont besoin du nom d'utilisateur principal pour identifier l'utilisateur. Entrez {0} et utilisez l'adresse électronique comme nom de domaine. Par exemple :

   ```
   {0}@domaine.com
   ```

   Le serveur LDAP ne requiert généralement pas de nom unique complet pour une connexion chiffrée.

   **Remarque** : Pour des raisons de sécurité, ne créez pas de compte statique pour l'utilisateur de la connexion. L'authentification LDAP vérifie uniquement le mot de passe lors de la liaison avec le serveur. Si vous utilisez un compte statique, tout utilisateur figurant dans l'arborescence LDAP pourra se connecter à l'aide d'un quelconque mot de passe.

**2. Mot de passe de connexion**

Définit le mot de passe utilisé par le serveur de connexion pour se connecter au serveur LDAP.

**Exemple** : Si le serveur de connexion utilise un compte fixe, entrez un texte conforme à l'exemple suivant :

```
SomePassword
```

Vous pouvez également entrer la valeur suivante, car la connexion utilise un mécanisme d'authentification :

```
{1}
```

**3. Domaine de recherche**

Identifie le serveur LDAP et le port de connexion pour CA Single Sign-On. Identifie également l'emplacement de recherche des utilisateurs dans l'arborescence des répertoires lors de la vérification des informations d'identification des comptes d'utilisateur. Si vous n'indiquez aucun numéro de port après le serveur dans la chaîne, le port 389 est utilisé.

Utilisez le format suivant pour le domaine de recherche :
LDAPS://*serveur_ldap*:*port*/*chemin_recherche*

**Remarque :** Le chemin de recherche est *obligatoire*.

Pour établir une connexion SSL au serveur LDAP, utilisez le port 636 ou un autre port de connexion SSL pour votre serveur LDAP :

LDAPS://*Serveur_LDAP*:636/OU=Users,OU=North America,DC=ca,DC=com

**4. Chaîne de recherche**

Spécifie les critères utilisés pour localiser l'utilisateur correct dans l'annuaire. Fonctionne avec le paramètre Etendue de la recherche. Si seul un sous-ensemble d'utilisateurs LDAP est autorisé à se connecter, vous pouvez utiliser la chaîne de recherche pour rechercher plusieurs propriétés dans l'enregistrement. Ce paramètre peut prendre pour valeur tout critère de recherche LDAP valide.

**Exemple** :

```
(saMAccountName={0})
```

**5. Etendue de la recherche**

Spécifie les critères utilisés pour localiser l'enregistrement adéquat de l'utilisateur. Il est utilisé avec le paramètre Chaîne de recherche. Délimite la recherche effectuée par le serveur LDAP pour le compte d'utilisateur. Entrez l'une des valeurs ci-dessous.

**niveau 1**

Inclut le répertoire actuel dans la recherche. Limite la recherche au répertoire actuel, en excluant les objets des sous-répertoires.

**sous-arborescence**

Inclut tous les sous-répertoires dans la recherche. Recommandé pour la plupart des installations.

**base**

Limite la recherche à l'objet de base.

**6. Liaison utilisateur**

Indique s'il convient d'effectuer une étape d'authentification supplémentaire (liaison) à l'aide du nom unique et du mot de passe de l'utilisateur pour valider les informations d'identification fournies.

**Valeur par défaut** : Désactivé. Cette valeur est acceptable avec une connexion chiffrée.

**7. Chiffrement**

(Facultatif) Spécifie le mécanisme d'authentification à utiliser lors de la liaison au serveur LDAP.

La valeur par défaut (authentification simple) est prise en charge par le protocole LDAPS.

**8. Utilisateur de compte**

Spécifie le compte par défaut de CA Performance Center vers lequel mapper des utilisateurs LDAP validés n'appartenant pas à un groupe. Fonctionne avec le paramètre Mot de passe du compte. Si un utilisateur valide ne correspond à aucune définition de groupe, l'utilisateur est connecté via l'ID d'utilisateur par défaut spécifié pour ce paramètre.

Pour permettre à tous les utilisateurs de se connecter avec leur propre nom d'utilisateur, entrez :

- {saMAccountName}
- {saMAccountName} or {CN}

**Remarque** : Le paramètre Utilisateur de compte correspond au champ d'une entrée de répertoire de cet utilisateur. Généralement, la valeur correspond à votre filtre de recherche.

**9. Clone par défaut de l'utilisateur de compte**

Définit le compte d'utilisateur à cloner si les utilisateurs LDAP validés appartiennent à un groupe non spécifié pour le paramètre Groupes.

**Exemple** : Entrez "utilisateur" si vous voulez attribuer des droits minimaux à ces utilisateurs.

**Remarque** : Un compte d'utilisateur est requis.

**10. Group**

Permet de déterminer la gestion de compte par défaut des comptes d'utilisateurs ou groupes de comptes sélectionnés.

**Exemple** : Pour permettre à tous les membres d'un groupe de se connecter à l'aide d'un compte d'administrateur, entrez :

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}" passwd=""
userClone="admin"/></LDAPGroups>
```

9. Entrez q pour quitter le programme.

   L'outil de configuration se ferme.

### Exemple de configuration

1. Configuration du service d'authentification unique/CA Performance Center/Authentification LDAP/Valeur distante
2. Utilisateur de la connexion : {0}
3. Mot de passe de connexion : {1}
4. Domaine de recherche : LDAPS://******.ca.com:636/OU=Users,OU=North America,DC=ca,DC=com
5. Chaîne de recherche : (sAMAccountName={0})
6. Limite de recherche : sous-arborescence
7. Liaison d'utilisateur : Désactivé
8. Chiffrement : Simple
9. Utilisateur de compte : {sAMAccountName}
10. Clone par défaut de l'utilisateur de compte : user
11. Groupe : All employees
12. Krb5ConfigFile : krb5.conf

## Importation du certificat LDAP

Pour utiliser une connexion LDAPS, vous devez importer un certificat LDAP dans le référentiel de clés Java.

Si vous ne possédez pas encore de certificat SSL, vous pouvez en générer un à l'aide de la commande d'outil keytool. Cette procédure explique les opérations à effectuer pour importer un certificat à partir d'une autorité de certification et l'installer dans le référentiel de clés.

**Procédez comme suit:**

1. Obtenez le certificat auprès de l'administrateur du serveur LDAP.
2. Importez le certificat dans le référentiel de clés de certificats approuvés Java à l'aide de la commande suivante :

   `keytool -importcert -keystore` *`répertoire_installation`*`/jre/lib/security/cacerts -storepass` *`cacertspasswd`* `-alias` *`alias`* `-file` *`filename.cer`*

   **keystore**

   Emplacement du fichier de référentiel de clés (.ks).

   **cacertspasswd**

   Indique le mot de passe du référentiel de clés cacerts.

   **Valeur par défaut :** changeit

   **filename.cer**

   Nom de fichier du certificat.
3. Créez une sauvegarde du fichier cacerts.
4. (Facultatif) Pour plus de sécurité, modifiez le mot de passe du référentiel de clés de certificats approuvé par Java, à l'aide de la commande suivante :

   `keytool -storepasswd -keystore` *`répertoire_installation`*`/jre/lib/security/cacerts`

   Vous êtes invité à fournir le mot de passe existant et le nouveau mot de passe.
5. Vérifiez que le certificat importé est disponible. Utilisez la commande suivante :

   `keytool -list -keystore` *`répertoire_installation`*`/jre/lib/security/cacerts`

   **Important :** Pour activer les services Web, le certificat doit se trouver dans le référentiel de clés cacerts. Dans le cas contraire, une erreur sera enregistrée dans le journal pour signaler que PKIX n'a pas trouvé de certificat.

# Validation des paramètres LDAP

Les paramètres LDAP peuvent être testés à l'aide de l'outil de configuration d'authentification unique. Vous pouvez vérifier que l'authentification LDAP est correctement configurée. Un script de test LDAP vous invite à spécifier une combinaison nom d'utilisateur/mot de passe à tester, à l'aide des paramètres d'authentification LDAP actuels. Si vous n'avez encore jamais utilisé l'outil de configuration pour modifier les paramètres d'authentification LDAP, les valeurs par défaut sont utilisées.

**Procédez comme suit:**

1. Connectez-vous au serveur où CA Performance Center ou un produit de source de données pris en charge est installé.

   Connectez-vous en tant qu'utilisateur root ou à l'aide de la commande sudo.

2. Lancez l'outil de configuration de l'authentification unique en exécutant la commande ./SsoConfig dans le répertoire suivant :

   `[répertoire_installation]/CA/PerformanceCenter`

   Vous êtes invité à sélectionner une option. Les options disponibles correspondent à des applications CA s'exécutant sur le serveur local.

3. Lors de la sélection des paramètres, utilisez les commandes suivantes :
   - q (quitter)
   - b (revenir au menu précédent)
   - u (mettre à jour)
   - r (réinitialiser)

4. Entrez 1 pour configurer CA Performance Center.

   Vous êtes invité à sélectionner une option.

5. Entrez 5 pour l'option Tester LDAP.

   L'invite vous demande d'entrer un nom d'utilisateur.

6. Entrez un nom d'utilisateur et un mot de passe pouvant être authentifiés à l'aide de LDAP.

   L'authentification unique tente d'utiliser les paramètres définis lors de la configuration de l'authentification LDAP pour se connecter au serveur LDAP et valider le compte d'utilisateur. Si le test réussit, de nombreuses actions sont enregistrées.

   Un message indique si l'authentification a réussi ou échoué.

7. Entrez q pour quitter le programme.

# Chapitre 3: Configuration de la prise en charge de SAML 2.0

Ce chapitre traite des sujets suivants :



## A propos de SAML 2.0

*SAML* (Security Assertion Markup Language) est un protocole de sécurité basé sur XML. Le concept de base implique l'échange d'assertions de sécurité concernant un sujet (une personne ou un ordinateur) qui demande l'accès à un domaine sécurisé. Les assertions indiquent notamment si la personne ou l'ordinateur peut accéder à certaines ressources et si une source de données externe, tel qu'un magasin de stratégies, est utilisée.

L'authentification SAML est généralement utilisée dans un environnement fédéré, tel que les services cloud qui nécessitent une couche supplémentaire de sécurité dans un réseau d'entreprise. Toutefois, l'implémentation de SAML implique au moins trois acteurs qui ont des rôles distincts :

**Fournisseur de services**

Utilise des informations d'identités qui sont stockées sur un autre serveur pour permettre aux utilisateurs autorisés d'accéder au système. Il est aussi appelé "Relying Party" en anglais. CA Performance Center remplit ce rôle lorsque l'authentification unique est configurée pour utiliser SAML.

**Fournisseur d'identités (Asserting Party)**

Conserve les informations d'identité et de sécurité et les fournit dans le cadre de l'authentification. Le terme SAML pour désigner ce rôle est *fournisseur d'identités*. Ce rôle est par exemple rempli par le serveur CA SiteMinder.

**Sujet**

Il s'agit de l'utilisateur (ou ordinateur) associé aux informations d'identité stockées par le fournisseur d'identités.

# Prise en charge de SAML 2.0 dans l'authentification unique

CA Single Sign-On prend en charge l'authentification avec SAML (Security Assertion Markup Language), version 2.0. Le service d'authentification unique peut accepter et décoder des jetons SAML 2.0 et les présenter aux agents d'authentification conformes à la norme SAML.

La prise en charge de SAML 2.0 inclut la prise en charge de la déconnexion unique. Ainsi, un utilisateur connecté à plusieurs interfaces utilisateur peut se déconnecter simultanément de toutes les interfaces. Par exemple, un utilisateur qui se connecte à CA Performance Center et consulte plus tard les données de flux de CA Network Flow Analysis peut se déconnecter d'une interface et être automatiquement déconnecté de l'autre.

L'authentification unique utilise une bibliothèque normalisée pour SAML 2.0. Elle prend ainsi potentiellement en charge beaucoup plus de produits qui reposent sur les normes SAML 2.0. Toutefois, les produits CA ci-dessous sont les seuls fournisseurs d'identités à avoir été testés avec CA Single Sign-On.

- CA SiteMinder Federation Manager
- CA Arcot A-OK™ On-Demand

Dans un environnement SAML, plusieurs méthodes d'authentification sont proposées. Les utilisateurs de CA Performance Center peuvent se connecter à l'aide de la méthode d'authentification classique (Produit) ou utiliser un jeton SAML. La méthode Produit est activée par défaut pour tous les comptes d'utilisateurs actifs. Les utilisateurs accèdent à l'interface utilisateur de CA Performance Center à l'aide de l'URL standard de CA Single Sign-On.

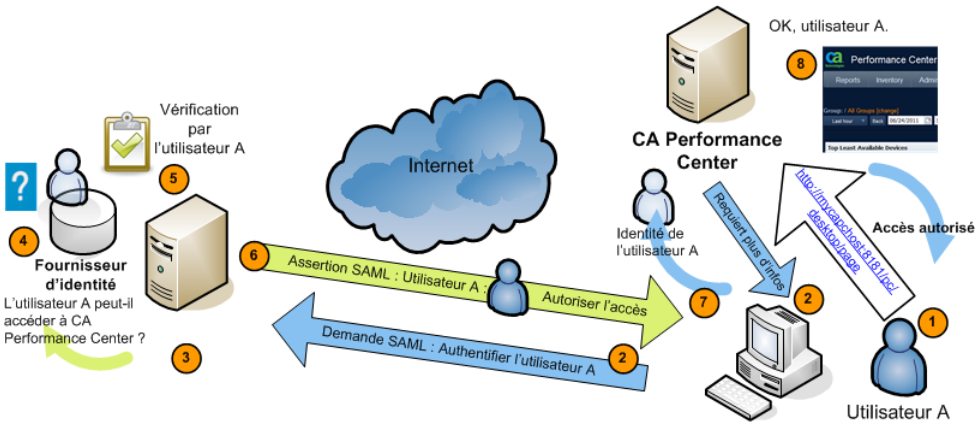
Pour permettre l'authentification des utilisateurs via SAML 2.0, l'administrateur doit modifier certains paramètres de l'authentification unique à l'aide de l'outil de configuration. Il doit également activer l'authentification externe pour tous les comptes d'utilisateurs et pour toutes les sources de données enregistrées qui prennent en charge SAML 2.0.

Les produits de source de données CA ne prennent pas tous en charge SAML 2.0. Si vous configurez SAML 2.0 pour l'authentification externe et que vous enregistrez une source de données qui ne prend pas en charge SAML, les utilisateurs de CA Performance Center doivent se réauthentifier lorsqu'ils effectuent une navigation descendante vers cette source de données.

## Fonctionnement de la prise en charge de SAML 2.0 par l'authentification unique

Le processus d'authentification unique classique de CA Performance Center à l'aide de l'authentification unique diffère de l'authentification avec SAML 2.0. Avec l'authentification SAML 2.0, les utilisateurs ne voient pas la page de connexion de CA Performance Center. Ils sont redirigés vers une interface fournie par le fournisseur d'identités. Toutes les autres méthodes d'authentification prises en charge utilisent une page de connexion.

Le schéma ci-dessous illustre le processus d'authentification SAML 2.0 avec l'authentification unique, CA Performance Center et un fournisseur d'identités qui prend en charge la norme SAML 2.0, tel que CA SiteMinder.




Le processus générique ci-après décrit la manière dont CA Performance Center prend en charge l'authentification SAML 2.0. Les options spécifiques à l'implémentation, telles que les certificats signés numériquement et la liaison d'acheminement, ont été ignorées.

1. Un utilisateur essaye d'accéder à CA Performance Center, en naviguant par exemple vers la page http://mycapchost:8181/pc/desktop/page.
2. CA Performance Center répond par une demande d'authentification SAML à partir du fournisseur d'identités.
3. Le navigateur traite la demande et contacte le logiciel d'authentification du serveur du fournisseur d'identités.
4. Le fournisseur d'identités détermine si l'utilisateur a déjà un contexte de connexion sécurisé, c'est-à-dire si l'utilisateur est déjà connecté.
5. S'il ne l'est pas, le fournisseur d'identités authentifie l'utilisateur à l'aide d'une méthode spécifique à l'implémentation.

   Le fournisseur d'identités peut par exemple interagir avec le navigateur pour demander à l'utilisateur de fournir des informations d'identification. Cette étape de l'authentification n'est pas pertinente pour CA Single Sign-On.

6. Le fournisseur d'identités crée, puis envoie au navigateur, une assertion SAML représentant le contexte de connexion sécurisé de l'utilisateur.

   L'assertion inclut un attribut requis, subjectNameId, et un attribut facultatif, ClonedUser.

   La valeur de subjectNameId correspond à l'utilisateur autorisé.

   Vous pouvez inclure le nom du compte d'utilisateur cloné dans l'assertion. Cet attribut définit le compte d'utilisateur vers lequel les utilisateurs SAML autorisés sont mappés.

7. Le navigateur envoie l'assertion SAML à CA Performance Center.

8. CA Performance Center reçoit l'assertion et la traite.

9. Si l'assertion est valide, CA Performance Center établit une session pour l'utilisateur. Le navigateur se redirige vers la page cible, la page d'accueil du tableau de bord de l'utilisateur.

# Configuration de l'authentification SAML

Pour activer l'authentification SAML 2.0 dans l'authentification unique, l'administrateur doit suivre les procédures ci-dessous.

1. En vous conformant aux directives spécifiques au fournisseur d'identités, créez un fichier de métadonnées qui établit l'accord entre le fournisseur d'identités et l'authentification unique.

   Pour plus d'informations, reportez-vous à la rubrique Préparation de l'accord avec le fournisseur d'identités (page 46).

2. (Facultatif) Créez un fichier de propriétés pour activer les signatures numériques et le chiffrement des communications entre le fournisseur d'identités et les serveurs où sont installés des logiciels CA.

   Pour plus d'informations, consultez la rubrique Préparation du fichier de propriétés de la sécurité (page 46).

3. Utilisez l'outil de configuration d'authentification unique pour définir les paramètres de l'authentification SAML.

   Pour plus d'informations, reportez-vous à la rubrique Configuration de la prise en Charge de SAML dans l'authentification unique (page 47).

4. Définissez les paramètres sur le serveur du fournisseur d'identités. Ajoutez par exemple tous les sites Web de produit de source de données qui prennent en charge SAML à la liste des sites de confiance.

   Pour plus d'informations, reportez-vous à la rubrique Configuration du fournisseur d'identités (page 51).

5. Mettez à jour les comptes d'utilisateurs dans la partie Administration de CA Performance Center afin d'ajouter une instruction pour utiliser l'authentification externe.

   Pour plus d'informations, reportez-vous à la rubrique Configuration de SAML (page 53).

## Préparation de l'accord avec le fournisseur d'identités

Un fichier de métadonnées au format XML est nécessaire pour établir l'accord entre le fournisseur d'identités et le fournisseur de services. Dans ce cas, CA Performance Center et toutes les sources de données enregistrées qui prennent en charge SAML 2.0 ont besoin de cet accord. Le fichier de métadonnées décrit le fournisseur d'identités et contient des informations sur les profils qu'il prend en charge. Ce fichier contient également des données sur les services qu'il exige du fournisseur de services.

L'authentification unique peut importer ce fichier pour configurer la relation avec le fournisseur d'identités.

Certains fournisseurs d'identités, comme CA SiteMinder, proposent des utilitaires pour vous aider à créer ces fichiers et à les exporter. Ils peuvent aussi créer l'accord automatiquement d'après les paramètres que vous avez définis.

Si vous souhaitez que votre fournisseur d'identités effectue cette tâche, consultez la documentation.

## Préparation du fichier de propriétés de la sécurité

Si vous envisagez d'utiliser le chiffrement et les certificats numériques pour les communications entre CA Performance Center et le fournisseur d'identités, un fichier de propriétés est requis. Dans ce fichier, vous devez spécifier le certificat à utiliser pour la signature et le chiffrement, ainsi que d'autres paramètres permettant d'activer le chiffrement.

Le fichier de propriétés SAML est enregistré dans le répertoire de base d'authentification unique :
`/opt/CA/PerformanceCenter/sso/webapps/sso`

Par exemple, un fichier comme celui-ci est requis :
`/opt/CA/PerformanceCenter/sso/webapps/sso/configuration/saml.properties`

Le fichier de propriétés doit inclure les paramètres suivants :

- Emplacement et nom de fichier du certificat de signature.
- Alias et mot de passe du certificat de vérification pour accéder au certificat.
- Nom d'hôte du serveur CA Performance Center.
- Emplacement et nom de fichier de l'accord que vous avez exporté à partir du fournisseur d'identités.
- Longueur du délai d'expiration défini sur le fournisseur d'identités. La valeur doit correspondre à celle du paramètre Délai d'expiration de la session IdP SAML2 de l'authentification unique.

Voici un exemple de la syntaxe :

```
# Emplacement du certificat utilisé pour signer des documents SAML
saml.sp.certificate.location=/opt/CA/saml2configuration/[nom_fichier_certificate]
saml.sp.certificate.password=[mot_de_passe]
saml.sp.certificate.alias=[alias]

saml.sp.metadata.hostname=[Nom_hôte_complet_serveur_CA Performance Center]
saml.sp.metadata.entityID=[Nom_serveur_CA Performance Center_sans_domaine_IP]
saml.sp.metadata.organizationName=[Nom_votre_organisation]
saml.sp.metadata.contactPerson=[Prénom_et_nom_administrateur]
saml.sp.metadata.email=[Adresse_électronique_personne_à_contacter]

# Emplacement du fichier de métadonnées pour le site de connexion
saml.idp.metadata.file=/opt/CA/saml2configuration/[nom_fichier].xml
# Délai d'expiration de la session avec le fournisseur d'identités en minutes. Utilisez
cette valeur pour les demandes d'auto-réauthentification et de déconnexion
saml.idp.sessionTimeout=[Longueur_délai_expiration_minutes]
```

Après toute modification du fichier saml.properties, il convient d'exporter à nouveau le fichier de métadonnées (qui établit l'accord avec le fournisseur d'identités). Pour plus d'informations, reportez-vous à la rubrique Configuration de la prise en Charge de SAML 2.0 dans l'authentification unique (page 47). Vous devez également redémarrer l'authentification unique.

## Configuration de la prise en charge de SAML 2.0 dans l'authentification unique

L'administrateur de CA Performance Center doit définir les paramètres pour l'authentification SAML à l'aide de l'outil de configuration de l'authentification unique. Cette opération doit être réalisée sur tous les serveurs où est installée une source de données demandant aux utilisateurs de s'authentifier à l'aide de SAML 2.0.

**Remarque** : Plusieurs schémas d'authentification peuvent être utilisés simultanément. Par exemple, les utilisateurs d'une source de données CA Network Flow Analysis peuvent se connecter via LDAP, tandis que les utilisateurs de CA Infrastructure Management utilisent SAML 2.0.

**Procédez comme suit:**

1. Connectez-vous au serveur où CA Performance Center ou un produit de source de données CA est installé.

   Connectez-vous en tant qu'utilisateur root ou à l'aide de la commande sudo.

2. Lancez l'outil de configuration de l'authentification unique en exécutant la commande ./SsoConfig dans le répertoire suivant :

   `[répertoire_installation]/CA/PerformanceCenter`

   Vous êtes invité à sélectionner une option. Les options disponibles correspondent à des applications CA s'exécutant sur le serveur local.

3. Lors de la sélection des paramètres, utilisez les commandes suivantes :

   - q (quitter)
   - b (revenir au menu précédent)
   - u (mettre à jour)
   - r (réinitialiser)

4. Entrez la valeur qui correspond à la source de données que vous voulez configurer. Par exemple, entrez 1 pour configurer CA Performance Center.

   Vous êtes invité à sélectionner une option.

5. Entrez 2 pour l'authentification SAML.

   Vous êtes invité à définir la priorité.

   Le paramètre de priorité s'applique uniquement à CA Performance Center.

6. Entrez l'une des options ci-après :

   **1. Valeur distante**

   Se rapporte à des paramètres que seuls les administrateurs peuvent modifier. Ces paramètres sont appliqués à tous les autres produits CA enregistrés sur cette instance de CA Performance Center. Les paramètres de valeur distante sont utilisés uniquement s'il n'y a pas de valeur de substitution locale correspondante.

   **2. Substitution locale**

   Se rapporte à des paramètres pouvant être modifiés pour tous les produits. La valeur de substitution locale a priorité sur la valeur distante et sur les paramètres par défaut.

   Vous êtes invité à sélectionner une propriété à configurer.

   Pour indiquer les valeurs des propriétés SAML2, entrez u pour mettre à jour la valeur, puis entrez une nouvelle valeur.

7. Entrez 1 pour sélectionner le paramètre Activer l'authentification SAML2

   Vous êtes invité à sélectionner une option.

8. Entrez u pour modifier la valeur, puis 1 pour activer l'authentification SAML 2.0.
9. Entrez 2 pour définir le paramètre Cloner les comptes d'utilisateurs par défaut.

   **2. Cloner les comptes d'utilisateurs par défaut**

   Définit le compte d'utilisateur vers lequel les utilisateurs SAML autorisés sont mappés. Le rôle et les droits associés au compte d'utilisateur que vous spécifiez sont appliqués à tous les utilisateurs qui s'authentifient.

   **Valeur par défaut** : Vide.

   **Exemple** : Entrez "utilisateur" si vous voulez que tous les utilisateurs se connectent avec des droits d'utilisateur.

   **Remarque** : Un compte d'utilisateur est requis.

   Les comptes d'utilisateurs configurés sur le fournisseur d'identités sont envoyés à CA Performance Center lorsque l'accord est établi. Ils apparaissent sur la liste d'utilisateurs de la page d'administration Gérer les utilisateurs, où vous pouvez les modifier.

10. Entrez 3 pour activer les paramètres de sécurité.

    **3. Activer la signature SAML2 et le chiffrement**

    Active la sécurisation et le chiffrement des communications entre CA Performance Center et le fournisseur d'identités.

    **Valeur par défaut** : Désactivé.

    Vous êtes invité à sélectionner une option.

11. Entrez u pour modifier la valeur, puis entrer 1 pour l'activer.

    **Remarque** : Ce paramètre doit correspondre au paramètre du fournisseur d'identités.

12. Entrez 4 pour activer la réauthentification automatique.

    **4. Réauthentification automatique SAML2**

    Indique si les utilisateurs doivent se réauthentifier après l'expiration du délai. Activez ce paramètre pour permettre au fournisseur d'identités d'effectuer une réauthentification passive (réauthentification automatique), sans interaction de l'utilisateur.

    Le paramètre suivant vous permet de définir la durée du délai d'expiration.

    **Valeur par défaut** : Désactivé.

13. Entrez u pour modifier la valeur, puis entrer 1 pour l'activer.
14. Entrez 5 pour définir le délai d'expiration de la réauthentification.

    **5. Durée de la réauthentification automatique**

    Définit le laps de temps qui s'écoule avant qu'une réauthentification passive ne soit effectuée. Si le paramètre Réauthentification automatique SAML2 est désactivé, ce paramètre est ignoré.

    **Valeur** : Doit être inférieure à la valeur du paramètre Délai d'expiration de la session IdP.

    **Valeur par défaut** : Aucun.
15. Entrez u pour modifier la valeur, puis entrez une nouvelle valeur.
16. Entrez 6 pour définir un délai d'expiration de la session pour le fournisseur d'identités.

    **6. Délai d'expiration de la session IdP**

    Définit le laps de temps qui s'écoule avant que la session établie entre CA Performance Center et le fournisseur d'identités ne soit automatiquement fermée. Par exemple, entrez 10 pour définir un délai d'expiration de 10 minutes.

    La valeur doit être supérieure à celle spécifiée pour le paramètre Durée de réauthentification. Si ce n'est pas le cas, il n'y aura pas de session pour effectuer la réauthentification. La valeur doit en outre correspondre à la valeur du paramètre saml.idp.sessionTimeout défini dans le fichier de propriétés de la sécurité. Pour plus d'informations, consultez la rubrique Préparation du fichier de propriétés de la sécurité (page 46).

    **Valeur par défaut** : Aucun.
17. Entrez u pour modifier la valeur, puis entrez une nouvelle valeur.
18. Entrez b deux fois pour retourner à l'invite initiale.
19. Entrez 6 pour exporter le fichier de métadonnées qui établit l'accord avec le fournisseur d'identités.

    Le fichier de métadonnées fournit au fournisseur d'identités les paramètres à utiliser lors de l'authentification des utilisateurs.

    Vous devez fournir un chemin d'accès au répertoire et un nom de fichier.
20. Entrez le nom de fichier. Par exemple, entrez la commande suivante :

    ```
    /tmp/CAPCMetadata.xml
    ```

    Le fichier est généré automatiquement, d'après les paramètres que vous avez sélectionnés dans l'outil de configuration.

    Vous obtenez une sortie sur imprimante du XML si l'opération d'exportation réussit. Si l'opération échoue, vous obtenez un message d'erreur.

21. Entrez q pour quitter le programme.

    L'outil de configuration se ferme.

## Configuration du IdP (Contrôleur local)

Pour pouvoir utiliser SAML 2.0 pour authentifier des utilisateurs dans CA Performance Center, vous devez définir des paramètres au niveau du fournisseur d'identités. Tous les fournisseurs d'identités prenant en charge la norme SAML 2.0 devraient fonctionner, mais CA a uniquement testé CA SiteMinder.

Vous pouvez configurer manuellement le fournisseur d'identités ou importer l'accord avec le fournisseur d'identités à partir du serveur d'authentification unique.

### Configuration manuelle du fournisseur d'identités

**Procédez comme suit:**

1. Activez le mode d'authentification SAML2 sur le fournisseur d'identités.
2. Entrez l'URL du service consommateur des assertions qui s'exécute sur les serveurs où l'authentification unique est installée. Par exemple :

   `http://nom_serveur:8381/sso/saml2/UserAssertionService`

   où 8381 est le port utilisé par l'authentification unique.
3. Définissez la méthode de liaison à HTTP-Redirect.

   **Remarque** : HTTP-Redirect est la seule méthode de liaison prise en charge par l'authentification unique.
4. Entrez les URL du service de déconnexion unique.

   Il faut indiquer l'emplacement du service de déconnexion et celui de la réponse. Ces services fonctionnent sur le serveur où l'authentification unique est installée.

   Utilisez les exemples ci-dessous :

   `http://nom_serveur:8381/sso/saml2/LogoutService`
   `http://nom_serveur:8381/sso/saml2/LogoutServiceResponse`
5. Ajoutez tous les sites Web de produit de source de données prenant en charge SAML 2.0 à la liste des sites de confiance.

   Cette étape peut impliquer l'ajout de ces sites Web à une liste d'entités d'association de fédération.
6. (*Facultatif*) Vérifiez les paramètres de signature numérique et de chiffrement. Ces derniers doivent également être configurés dans l'authentification unique.

### Importation du fichier de l'accord avec le fournisseur d'identités

**Procédez comme suit:**

1. Importez le fichier de l'accord avec le fournisseur d'identités à partir de son emplacement sur le serveur d'authentification unique.

   Vous avez exporté ce fichier après d'autres opérations de configuration à l'aide de l'outil de configuration de l'authentification unique. Pour plus d'informations, reportez-vous à la rubrique Configuration de la prise en Charge de SAML dans l'authentification unique (page 47).

2. Ajoutez tous les sites Web de produit de source de données prenant en charge SAML 2.0 à la liste des sites de confiance.

   Cette étape peut impliquer l'ajout de ces sites Web à une liste d'entités d'association de fédération.

3. (*Facultatif*) Vérifiez les paramètres de signature numérique et de chiffrement. Ces derniers doivent également être configurés dans l'authentification unique.

### Dépannage

**Problème :**

Le message d'erreur suivant s'affiche après la configuration de SAML :

```
RelayState is either null or a blank string. RelayState must be set for SSO to work correctly.

Invalid syntax, RelayState=<value>

RelayState does not have parameter SsoRedirectUrl, RelayState=<value>
```

**Raison :**

Certains fournisseurs d'identités ne renvoient pas la valeur du paramètre RelayState que CA Performance Center envoie au fournisseur d'identités pendant la vérification de l'authentification.

**Résolution :**

Configurez manuellement le paramètre RelayState pour votre fournisseur d'identités. Utilisez la syntaxe suivante :

```
SsoProductCode=pc&SsoRedirectUrl=http://CA Performance Center:8181/pc/desktop/page
```

**Remarque :** Pour des communications sécurisées, remplacez http par https et remplacez le numéro de port.

## Fin de la configuration de SAML 2.0

Pour activer l'authentification SAML 2.0, configurez les comptes d'utilisateurs de sorte qu'ils utilisent l'authentification externe. Les comptes d'utilisateurs créés dans CA Performance Center sont paramétrés pour utiliser par défaut l'authentification du centre de performance. L'administrateur doit mettre à jour les comptes de tous les opérateurs qui s'authentifient à l'aide de SAML 2.0.

Pendant la configuration de SAML2.0, vous devez spécifier un compte d'utilisateur CA Performance Center existant qui sera cloné dans le fournisseur d'identités. Tous les utilisateurs déjà définis dans le fournisseur d'identités reçoivent les mêmes droits du produit que le compte d'utilisateur désigné. Ces comptes sont également propagés à CA Performance Center, où ils apparaissent désormais dans la liste d'utilisateurs comme de nouveaux utilisateurs. Il est souvent nécessaire de modifier ces comptes pour assurer que les utilisateurs accèdent uniquement aux données dont ils ont besoin pour travailler.

**Procédez comme suit:**

1. Connectez-vous à CA Performance Center en tant qu'utilisateur avec des droits d'administrateur.
2. Sélectionnez Administration, Paramètres de l'utilisateur, puis cliquez sur Utilisateurs.

   La page Gérer les utilisateurs s'ouvre.
3. Sélectionnez un compte d'utilisateur à modifier.
4. Cliquez sur Modifier.

   L'assistant de modification d'un utilisateur s'ouvre.
5. Sélectionnez Externe comme type d'authentification.
6. Utilisez l'assistant pour apporter toute autre modification désirée au compte d'utilisateur. Par exemple, accédez à la troisième boîte de dialogue de l'assistant pour modifier les droits du produit pour cet utilisateur.
7. Cliquez sur Enregistrer.

   Les modifications apportées au compte d'utilisateur sont enregistrées.

# Chapitre 4: Utilisation de HTTPS avec l'authentification unique

Ce chapitre traite des sujets suivants :



## Chiffrement SSL (Secure Sockets Layer) : HTTPS

Par défaut, l'authentification unique utilise le protocole HTTP (Hyper Text Transfer Protocol) pour la communication entre le navigateur de l'utilisateur et CA Performance Center. Le protocole TLS (Transport Layer Security) et le protocole antérieur SSL (Secure Sockets Layer) sont des protocoles de chiffrement très utilisés pour la sécurisation de la transmission des données sur Internet. Vous pouvez utiliser les protocoles TLS ou SSL conjointement avec le protocole HTTP pour obtenir le protocole HTTPS (HTTP sécurisé). Dans ce manuel, le terme *SSL* est utilisé pour représenter TLS et SSL.

Vous pouvez améliorer la sécurité du système de surveillance en configurant le protocole HTTPS pour l'authentification unique au lieu du protocole HTTP.

La configuration de l'authentification unique de CA pour utiliser HTTPS est facultative. Pour pourvoir utiliser HTTPS sur le site Web d'authentification unique, vous devez vous procurer un certificat de serveur. L'équipe chargée de la création et de l'application des stratégies de sécurité de votre organisation peut sans doute vous aider dans ce processus.

# Procédure de configuration du protocole HTTPS pour CA Single Sign-On

Plusieurs étapes sont requises pour l'activation du protocole SSL. Vous devez tout d'abord installer les certificats de validation de l'identité du serveur. Vous devez ensuite modifier la base de données pour que CA Performance Center redirige les données vers le port et le schéma appropriés pour CA Single Sign-On. Finalement, vous devez modifier les services aussi bien pour CA Performance Center que pour CA Single Sign-On afin de refléter les nouveaux ports et schémas.

Deux ports sont importants pour ces étapes : le port CA Performance Center (port 8181 par défaut) et le port CA Single Sign-On (port 8381 par défaut). Le port 8181 est le port de connexion de CA Performance Center. Si les utilisateurs doivent s'authentifier, le serveur les redirige sur la page de connexion de CA Single Sign-On, sur le port 8381. Une fois un utilisateur connecté, le serveur le redirige vers l'URL d'origine sur le port 8181.

Vous ne pouvez pas donc pas utiliser le même port à chaque étape de configuration. Cela entraînerait un conflit entre CA Performance Center et CA Single Sign-On.

Pour activer le protocole HTTPS pour CA Performance Center et CA Single Sign-On, procédez comme suit :

1. Obtenez un certificat de serveur et installez-le dans le référentiel de clés du serveur Web (page 56).
2. A l'aide de l'outil de configuration de l'authentification unique, mettez à jour les propriétés requises (page 62).
3. Configurez le protocole HTTPS au niveau de la console CA Performance Center (page 63).
4. Configurez le protocole HTTPS dans CA Single Sign-On (page 65).
5. Arrêtez et redémarrez les services.

## Définition des certificats SSL

Pour pouvoir configurer le protocole HTTPS au niveau du site Web d'authentification unique, vous devez obtenir et installer une clé privée et le certificat public associé. Vous pouvez utiliser SSL avec un certificat autosigné ou avec un certificat signé par une autorité de certification approuvée. Ces procédures sont généralement spécifiques à une organisation et aux stratégies mises en oeuvre par l'équipe responsable de la sécurité. Toutefois, ces procédures fournissent des informations susceptibles de vous guider.

Reportez-vous à la procédure appropriée :

- Génération et importation d'un nouveau certificat (page 57).
- Importation d'un certificat SSL existant (page 60).

**Remarque :** Pour plus d'informations sur la commande d'outil keytool utilisée dans ces procédures, consultez la documentation Java sur le site Web d'Oracle.

## Génération et importation d'un nouveau certificat

Si vous ne possédez pas encore de certificat SSL, vous pouvez en générer un à l'aide de la commande d'outil keytool. Cette procédure explique les étapes à effectuer pour générer un certificat autosigné et l'installer dans le référentiel de clés.

**Procédez comme suit:**

1. Exécutez la commande suivante :

   ```
   cd répertoire_installation/PerformanceCenter/jetty/etc
   ```

2. Créez une sauvegarde du fichier de référentiel de clés jetty existant en le renommant à l'aide des commandes suivantes :

   ```
   mv répertoire_installation/PerformanceCenter/jetée/
   etc/keystore répertoire_installation/PerformanceCenter/
   jetty/etc/keystore.bak
   ```

   **Important :** Vous devez supprimer l'ancien référentiel de clés. Dans le cas contraire, une erreur "Keystore was tampered with, or password was incorrect" (le référentiel de clés a été falsifié ou mot de passe est incorrect) s'affiche pendant les étapes suivantes.

3. Générez une clé privée et un certificat autosigné public, à l'aide de la commande suivante :

   ```
   keytool -genkeypair -keystore keystore_file.ks -storepass storepasswd -keyalg
   RSA -keysize 2048 -keypass keypasswd -alias alias_name
   ```

   **storepasswd**

   Spécifie le mot de passe du référentiel de clés.

   **keypasswd**

   Spécifie le mot de passe de la clé privée dans le référentiel de clés.

   **Important :** Mémorisez ces mots de passe : ils sont irrécupérables.

4. Exportez le certificat autosigné à partir du référentiel de clés à l'aide de la commande suivante :

   `keytool -exportcert -keystore keystore_file.ks -storepass storepasswd -alias alias_name -file filename.cer`

   **alias**

   Spécifie un alias que vous pouvez utiliser pour référencer l'entrée du référentiel de clés qui sera créée pour contenir les clés.

   **filename.cer**

   Détermine le fichier vers lequel le certificat est exporté. Nous vous recommandons d'utiliser un chemin d'accès complet qui ne place pas le fichier dans le répertoire actuel.

   **Exemple** : /tmp/capcCert.cer.

   **Remarque :** Nous vous recommandons de sauvegarder le fichier cacerts avant de poursuivre.

5. Importez le certificat autosigné dans le référentiel de clés de certificats approuvés Java à l'aide de la commande suivante :

   `keytool -importcert -keystore installDirectory/jre/lib/security/cacerts -storepass cacertspasswd -alias capcSelfSigned -file filename.cer`

   **Remarque :** Le mot de passe par défaut du référentiel de clés cacerts est changeit.

   ***cacertspasswd***

   Indique le mot de passe du référentiel de clés cacerts.

   **Valeur par défaut :** changeit

   ***filename.cer***

   Fichier vers lequel le certificat a été exporté.

6. Sauvegardez le fichier cacerts.

7. (Facultatif) Pour plus de sécurité, modifiez le mot de passe du référentiel de clés de certificats approuvé par Java, à l'aide de la commande suivante :

   `keytool -storepasswd -keystore répertoire_installation/jre/lib/security/cacerts`

   Vous êtes invité à fournir le mot de passe existant et le nouveau mot de passe.

8. Vérifiez que le référentiel de clés importé est disponible. Utilisez la commande suivante :

   `keytool -list -keystore répertoire_installation/jre/lib/security/cacerts`

   **Important :** Pour activer les services Web, le certificat autosigné doit se trouver dans le référentiel de clés cacerts. Dans le cas contraire, une erreur sera enregistrée dans le journal pour signaler que PKIX n'a pas trouvé de certificat.

9. Redémarrez tous les services CA Performance Center à l'aide des commandes suivantes :

   ```
   /sbin/service caperfcenter_sso restart
   ```

   ```
   /sbin/service caperfcenter_devicemanager restart
   ```

   ```
   /sbin/service caperfcenter_console restart
   ```

   Le certificat SSL auto-signé est généré et installé dans le référentiel de clés.

Etapes suivantes :

- (Facultatif) Conversion d'un certificat autosigné en certificat SSL de l'autorité de certification (page 59)
- Configuration du port et du site Web pour la prise en charge du protocole HTTPS (page 62)

## Conversion d'un certificat autosigné en certificat SSL de l'autorité de certification

Le certificat autosigné affiche un message d'avertissement dans le navigateur lorsque les utilisateurs ouvrent CA Performance Center. Les utilisateurs peuvent ignorer l'avertissement et continuer. Toutefois, la signature du certificat par une autorité de certification approuvée évite l'affichage de ce genre d'avertissements dans le navigateur. La procédure suivante porte sur la conversion du certificat autosigné en certificat signé par une autorité de certification approuvée.

**Procédez comme suit:**

1. Exécutez la commande suivante :

   ```
   cd répertoire_installation/PerformanceCenter/jetty/etc
   ```

2. Exportez une demande de signature de certificat à l'aide de la commande suivante :

   ```
   keytool -certreq -keystore keystore_file.ks -storepass storepasswd -alias
   alias_name -keypass keypasswd -file requestFileName.csr
   ```

   **requestFileName.csr**

   Chemin et nom de fichier de la demande de signature exportée.

3. Envoyez le fichier généré (*requestFileName*.csr) à une autorité de signature qualifiée, avec toutes autres informations demandées.

   L'autorité de certification vous enverra ensuite un certificat signé (*signedCert*.cer). Elle vous enverra peut-être aussi un certificat racine de l'autorité de certification (*rootCA*.cer) pour l'authentification du certificat signé.

4. (*Facultatif*) Déterminez si le certificat racine de l'autorité de certification fait partie des autorités approuvées par défaut par Java à l'aide de la commande suivante :

   ```
   keytool -list -v -keystore répertoire_installation/jre/lib/security/cacerts
   -storepass cacertspasswd
   ```

5. (*Facultatif*) Dans la sortie, recherchez l'autorité de certification qui a signé votre certificat. Si l'autorité de certification n'est pas cataloguée, ajoutez-la à la liste d'autorités approuvées à l'aide de la commande suivante :

   ```
   keytool -importcert -keystore répertoire_installation/jre/lib/security/cacerts
   -storepass cacertspasswd -alias myRootCa -file rootCA.cer
   ```

6. Importez le certificat signé à l'aide de la commande suivante :

   ```
   keytool -importcert -trustcacerts -keystore keystore -storepass storepasswd
   -alias alias_name -keypass keypasswd -file signedCert.cer
   ```

7. Validez le contenu du référentiel de clés jetty à l'aide de la commande suivante :

   ```
   keytool -list -keystore
   répertoire_installation/PerformanceCenter/jetty/etc/keystore
   ```

   Le certificat unique que vous avez importé apparaît dans la liste.

8. Redémarrez tous les services CA Performance Center à l'aide des commandes suivantes :

   ```
   /sbin/service caperfcenter_sso restart
   ```

   ```
   /sbin/service caperfcenter_devicemanager restart
   ```

   ```
   /sbin/service caperfcenter_console restart
   ```

   Le certificat SSL de l'autorité de certification remplace votre certificat autosigné dans le référentiel de clés.

Etape suivante : Configuration du port et du site Web pour la prise en charge du protocole HTTPS (page 62)

## Importation d'une clé et d'un certificat existant

Vous pouvez utiliser une clé privée et un certificat public (un certificat auto-signé ou un de l'autorité de certification) provenant de sources différentes. Votre équipe de sécurité peut, par exemple, vous fournir un certificat SSL personnalisé pour satisfaire les besoins de votre organisation. Pour utiliser ce certificat SSL, importez la clé privée et le certificat signé.

**Procédez comme suit:**

1. Exécutez la commande suivante :

   ```
   cd /opt/CA/PerformanceCenter/jetty-version/etc
   ```

2. Supprimez l'ancien référentiel de clés à l'aide de la commande suivante :

   ```
   rm keystore
   ```

3. Créez un référentiel de clés PKCS#12 à partir de la clé privée et du certificat à l'aide de la commande suivante :

   `openssl pkcs12 -export -in certificate.pem -inkey privatekey.pem -name MyAlias -out keystore.pkcs12`

   ***certificate.pem***

   Indique le certificat qui vous a été fourni.

   ***privatekey.pem***

   Indique la clé privée qui vous a été fournie.

   **Remarque :** Cette commande fonctionne sous Linux uniquement.

4. Importez la clé et le certificat dans le référentiel de clés CA Performance Center à l'aide de la commande suivante :

   `keytool -importkeystore -destkeystore keystore_file -deststorepass storepasswd -srckeystore keystore.pkcs12 -srcstoretype pkcs12 -srcalias src_alias_name -destalias dest_alias_name -destkeypass keypasswd`

5. Redémarrez tous les services CA Performance Center à l'aide des commandes suivantes :

   `/sbin/service caperfcenter_sso restart`

   `/sbin/service caperfcenter_devicemanager restart`

   `/sbin/service caperfcenter_console restart`

   Votre certificat SSL existant est importé dans le référentiel de clés.

Etape suivante : Configuration du port et du site Web pour la prise en charge du protocole HTTPS (page 62)

**Remarque** : Si le certificat n'inclut aucune chaîne menant vers un certificat dans le référentiel de clés, importez-le dans le référentiel de clés cacerts de Java. Pour déterminer si le certificat inclut une telle chaîne, exécutez la commande suivante :

`keytool -printcert -file nom_fichier`

***nom_fichier***

Spécifie le nom du certificat.

Pour obtenir des instructions sur l'importation d'un certificat dans le référentiel de clés cacerts de Java, reportez-vous à la rubrique Génération et importation d'un certificat (page 57).

## Configuration du port et du site Web pour SSL

Par défaut, l'authentification unique utilise le port 8381. Pour configurer HTTPS, utilisez l'outil de configuration de l'authentification unique afin de mettre à jour le schéma et le port du site Web par défaut de sorte qu'ils correspondent aux paramètres de chiffrement.

Effectuez les tâches de cette procédure avec tous les serveurs sur lesquels une source de données est installée.

**Procédez comme suit:**

1. Lancez l'outil de configuration de l'authentification unique en exécutant la commande ./SsoConfig dans le répertoire suivant :

   `[répertoire_installation]/CA/PerformanceCenter`

   Vous êtes invité à sélectionner une option.

2. Utilisez les commandes suivantes pour modifier les paramètres :

   - q (quitter)
   - b (revenir au menu précédent)
   - u (mettre à jour)
   - r (réinitialiser)

3. Entrez 1 pour sélectionner CA Performance Center.

4. Entrez 4 pour configurer l'authentification unique.

   Vous êtes invité à définir la priorité.

5. Entrez l'une des options ci-après :

   **1. Valeur distante**

   Se rapporte à des paramètres que seuls les administrateurs peuvent modifier. Ces paramètres sont appliqués à tous les autres produits CA enregistrés sur cette instance de CA Performance Center. Les paramètres de valeur distante sont utilisés uniquement s'il n'y a pas de valeur de substitution locale correspondante.

   **2. Substitution locale**

   Se rapporte à des paramètres pouvant être modifiés pour tous les produits. La valeur de substitution locale a priorité sur la valeur distante et sur les paramètres par défaut.

   Vous êtes invité à sélectionner une propriété à configurer.

6. Entrez 12 pour la propriété du schéma.

7. Entrez u pour mettre à jour la valeur.

8. Indiquez la valeur https.

9. Entrez 13 pour la propriété du port.
10. Remplacez la valeur par 8382.
11. Entrez b deux fois pour revenir au menu Configuration/CA Performance Center de SSO.
12. Entrez 3 pour configurer le centre de performances.

    Vous êtes invité à définir la priorité.
13. Entrez 1 pour la valeur distante ou 2 pour la substitution locale.
14. Entrez 6 pour sélectionner le schéma de site Web.
15. Remplacez la valeur par https.
16. Entrez 8 pour sélectionner le port du site Web.
17. Remplacez la valeur par 8182.
18. Entrez q pour quitter le programme.

Vous devez à présent configurer les fichiers de CA Performance Center pour qu'ils utilisent HTTPS.

## Configuration de CA Performance Center pour utiliser HTTPS

Vous devez modifier certains fichiers de configuration pour refléter les nouveaux paramètres de site Web et de port. Modifiez les fichiers de configuration pour remplacer le connecteur HTTP par un connecteur HTTPS. Vous devez également redémarrer les services CA Performance Center pour que les modifications prennent effet.

**Procédez comme suit:**

1. Accédez au répertoire suivant :

   ```
   cd/[répertoire_installation]/CA/PerformanceCenter/PC
   ```
2. Ouvrez le fichier start.ini afin de le modifier.
3. Recherchez la ligne ci-dessous et supprimez le "#" pour l'activer :

   ```
   #/opt/CA/PerformanceCenter/PC/etc/jetty-ssl.xml
   ```

   où "/opt/CA" est le répertoire d'installation par défaut.
4. Enregistrez start.ini.
5. Accédez au répertoire suivant :

   ```
   cd/[répertoire_installation]/CA/PerformanceCenter/PC/etc
   ```

6. Créez un fichier nommé jetty-ssl.xml dans ce répertoire avec le contenu suivant :

```
&lt;?xml version="1.0"?&gt;
<!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
"http://www.eclipse.org/jetty/configure.dtd">
<Configure id="Server" class="org.eclipse.jetty.server.Server">
  <Call name="addConnector">
    <Arg>
      <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
         <Set name="Port">8182</Set>
         <Set name="maxIdleTime">30000</Set>
        <Set name="Keystore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
        <Set name="Password">***PASSWORD***</Set>
         <Set name="KeyPassword">***PASSWORD***</Set>
        <Set name="truststore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
        <Set name="trustPassword">***PASSWORD***</Set>
        <Set name="allowRenegotiate">true</Set>
      </New>
    </Arg>
  </Call>
</Configure>
```

7. Remplacez toutes les instances de la valeur de "***PASSWORD***" par les mots de passe utilisés dans votre système.

8. Enregistrez le fichier.

9. Ouvrez le fichier jetty.xml pour le modifier.

10. Supprimez les lignes suivantes pour le connecteur HTTP par défaut :

```
<Call name="addConnector">
  <Arg>
      <New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
          <Set name="host"><Property name="jetty.host" /></Set>
            <!-- Changed: Used to be Property -->
           <Set name="port"><SystemProperty name="jetty.port"
default="8181"/></Set>
           <Set name="maxIdleTime">300000</Set>
           <Set name="Acceptors">2</Set>
           <Set name="statsOn">false</Set>
           <Set name="confidentialPort">8443</Set>
           <Set name="lowResourcesConnections">20000</Set>
           <Set name="lowResourcesMaxIdleTime">5000</Set>
      </New>
  </Arg>
 </Call>
```

11. Enregistrez jetty.xml.

12. Accédez au répertoire suivant :

    ```
    cd/[répertoire_installation]/CA/PerformanceCenter/PC/conf
    ```

13. Modifiez le fichier wrapper.conf. Dans la ligne suivante, remplacez "8181" par "8182" pour que cela corresponde au port défini dans le fichier jetty-ssl.xml décrit ci-dessus :

    ```
    wrapper.java.additional.2=-Djetty.port=8181
    ```

14. Enregistrez le fichier wrapper.conf.

15. Accédez au répertoire suivant :

    ```
    cd /[InstallationDirectory]/CA/PerformanceCenter/sso/webapps/
    sso/configuration
    ```

16. Modifiez le fichier CAPerformanceCenter.xml.

17. Remplacez les valeurs <Scheme> et <Port> par des paramètres appropriés pour SSL :

    ```
    <?xml version="1.0" encoding="utf-8" ?>
    <Configuration>
        <SingleSignOnEnabled>True</SingleSignOnEnabled>
        <SingleSignOnProductCode>pc</SingleSignOnProductCode>
        <SignInPageProductDefaultUrl>
            <Scheme>https</Scheme>
            <Port>8182</Port>
            <PathAndQuery>/pc/desktop/page</PathAndQuery>
        </SignInPageProductDefaultUrl>
        <SingleSignOnWebServiceUrl>
            <Scheme>https</Scheme>
            <Port>8182</Port>
            <PathAndQuery>/pc/center/webservice/sso</PathAndQuery>
        </SingleSignOnWebServiceUrl>
    </Configuration>
    ```

## Mise à jour de la configuration de l'authentification unique et redémarrage des services

Modifiez certains fichiers de démarrage pour prendre en charge le chiffrement SSL dans l'authentification unique. Vous devez également redémarrer tout les services CA Performance Center et les services d'authentification unique pour mettre à jour les paramètres.

**Procédez comme suit:**

1. Accédez au répertoire suivant :

   ```
   cd/[répertoire_installation]/CA/PerformanceCenter/sso
   ```

2. Ouvrez le fichier start.ini afin de le modifier.

3. Recherchez la ligne ci-dessous et supprimez le "#" pour l'activer :

   ```
   #/opt/CA/PerformanceCenter/sso/etc/jetty-ssl.xml
   ```

   où "/opt/CA" est le répertoire d'installation par défaut.

4. Enregistrez start.ini.

5. Accédez au répertoire suivant :

   ```
   cd/[répertoire_installation]/CA/PerformanceCenter/sso/etc
   ```

6. Créez un fichier nommé jetty-ssl.xml dans ce répertoire avec le contenu suivant :

   ```
   &lt;?xml version="1.0"?&gt;
   <!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
   "http://www.eclipse.org/jetty/configure.dtd">
   <Configure id="Server" class="org.eclipse.jetty.server.Server">
     <Call name="addConnector">
       <Arg>
         <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
            <Set name="Port">8382</Set>
            <Set name="maxIdleTime">30000</Set>
           <Set name="Keystore"><Property name="jetty.home" default="."
   />/etc/keystore</Set>
           <Set name="Password">***PASSWORD***</Set>
           <Set name="KeyPassword">***PASSWORD***</Set>
          <Set name="truststore"><Property name="jetty.home" default="."
   />/etc/keystore</Set>
           <Set name="trustPassword">***PASSWORD***</Set>
           <Set name="allowRenegotiate">true</Set>
         </New>
       </Arg>
     </Call>
   </Configure>
   ```

7. Remplacez toutes les instances de la valeur de "***PASSWORD***" par les mots de passe utilisés dans votre système.

8. Enregistrez le fichier jetty-ssl.xml.

9. Ouvrez le fichier jetty.xml.

10. Supprimez les lignes suivantes pour le connecteur HTTP par défaut :

```
<Call name="addConnector">
  <Arg>
      <New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
          <Set name="host"><Property name="jetty.host" /></Set>
            <!-- Changed: Used to be Property -->
           <Set name="port"><SystemProperty name="jetty.port"
default="8181"/></Set>
           <Set name="maxIdleTime">300000</Set>
           <Set name="Acceptors">2</Set>
           <Set name="statsOn">false</Set>
           <Set name="confidentialPort">8443</Set>
           <Set name="lowResourcesConnections">20000</Set>
           <Set name="lowResourcesMaxIdleTime">5000</Set>
      </New>
  </Arg>
 </Call>
```

11. Enregistrez jetty.xml.
12. Accédez au répertoire suivant :

    `[répertoire_installation]/CA/PerformanceCenter/sso/conf`

13. Modifiez le fichier wrapper.conf. Dans la ligne suivante, remplacez "8381" par "8382" pour que cela corresponde au port défini dans le fichier jetty-ssl.xml décrit précédemment :

    ```
    wrapper.java.additional.2=-Djetty.port=8381
    ```

14. Enregistrez le fichier wrapper.conf.
15. Arrêtez la console, le gestionnaire d'unités et les services d'authentification unique en entrant les commandes suivantes :

    ```
    service caperfcenter_console stop
    ```

    ```
    service caperfcenter_devicemanager stop
    ```

    ```
    service caperfcenter_sso stop
    ```

16. Redémarrez les services en entrant les commandes suivantes :

    ```
    service caperfcenter_sso start
    ```

    ```
    service caperfcenter_devicemanager start
    ```

    ```
    service caperfcenter_console start
    ```

# Chapitre 5: Dépannage

Ce chapitre traite des sujets suivants :



## Le navigateur indique une erreur

**Symptôme :**

Après avoir entré mon mot de passe sur la page de connexion, j'ai été redirigé sur une page du navigateur Web indiquant une erreur. Ai-je saisi un mot de passe incorrect ?

**Solution :**

Ce symptôme ne signifie pas que vous avez entré des informations d'identification SAML erronées. L'erreur du navigateur (401 ou 500) indique que l'authentification unique a redirigé le navigateur vers l'URL de connexion, mais que le serveur du fournisseur d'identités est hors service.

Procédez comme suit :

- Vérifiez que le serveur du fournisseur d'identités fonctionne.
- Testez la connexion réseau entre le serveur CA Performance Center et le serveur du fournisseur d'identités.

## Journaux

En vérifiant vos fichiers journaux de façon quotidienne ou hebdomadaire, vous pouvez résoudre les problèmes avant qu'ils n'aient un impact sur les opérations normales. Tous les journaux sont stockés dans des sous-dossiers correspondant à un service (ou démon). Trouvez des fichiers journaux dans le chemin d'accès suivant :

`CA/PerformanceCenter/nom_service/logs`

Remplacez le paramètre *nom_service* par un des noms de service suivants :

**DM**

Gestionnaire des unités

- DMService.log : fichier généré par le gestionnaire d'unités qui concerne essentiellement la synchronisation.
- wrapper.log : journalisation du processus caperfcenter_devicemanager.

**EM**

Gestionnaire d'événements.

- EMService.log : fichier généré par le gestionnaire d'événements ; inclut des informations sur les événements et alarmes.
- wrapper.log : journalisation du processus caperfcenter_eventmanager.

**PC**

Programme principal de la console.

- PCService.log : journalisation des données CA Performance Center ; inclut les composants de vues et de l'interface utilisateur.
- wrapper.log : journalisation du processus caperfcenter_console.

**SSO**

Logiciel d'authentification unique.

- SSOService.log : connexion à authentification unique, y compris les informations HTTPS (Secure Sockets Layer) lorsque HTTPS est configuré.
- wrapper.log : journalisation du processus caperfcenter_sso.

Pour des problèmes avec l'outil de configuration d'authentification unique, vérifiez le journal d'application dans l'emplacement suivant :

```
/opt/CA/PerformanceCenter/sso/logs/application.log
```

Les noms de fichier de journal incluent la date et l'heure pertinentes.

De nouveaux fichiers journaux sont générés automatiquement chaque jour. Les fichiers journaux plus anciens sont automatiquement supprimés au bout de 14 jours pour éviter la consommation d'un espace disque excessif.

Accédez au fichier journal le plus récent pour trouver les erreurs associées à la base de données ou la synchronisation de la source des données. Vous pouvez commencer par ouvrir le tableau de bord Evénements à partir de l'onglet Tableaux de bord et effectuer un tri par Statut. Si vous souhaitez examiner le fichier journal associé, notez le type de travail, ainsi que la date et l'heure de l'échec. Dans le répertoire des journaux, ouvrez le fichier journal présentant la date correspondante dans le nom de fichier.

# Examen du journal d'audit

L'authentification unique prend en charge les audits de sécurité en consignant quotidiennement dans un journal des détails relatifs à l'activité de connexion des utilisateurs à un fichier. Consultez le journal pour vérifier l'activité des utilisateurs.

**Procédez comme suit:**

1. Connectez-vous au serveur où est installé un produit de source de données CA.
2. Ouvrez une invite de commande et exécutez une commande cd pour accéder au répertoire suivant :

   `[répertoire_installation]/PerformanceCenter/sso/logs`

   **Remarque :** Le journal d'audit est enregistré à l'emplacement suivant sur les serveurs Windows :
   `[répertoire_installation]\Portal\SSO\logs.`
3. Entrez dir pour afficher le contenu du répertoire.

   Le nom de fichier du fichier journal est SingleSignOnAuditLogaaaa-mm-jj.log.
4. Entrez le nom du fichier d'audit que vous souhaitez examiner.

   Le fichier s'ouvre dans l'application d'éditeur de texte locale.

# Glossaire

**Authentification unique**

L'*authentification unique* est le schéma d'authentification de CA Performance Center et de toutes les sources de données prises en charge. Une fois authentifiés sur CA Performance Center, les utilisateurs peuvent naviguer à travers la console et les sources de données enregistrées sans avoir à se connecter une seconde fois.

**Fournisseur d'identités**

Le *fournisseur d'identités* stocke les informations d'identité et de sécurité et les fournit dans le cadre d'une authentification. Egalement connu en anglais sous le nom de "asserting party", c'est l'un des trois acteurs requis pour l'authentification SAML.

**LDAP**

*LDAP* (Lightweight Directory Access Protocol) est un protocole qui définit des méthodes pour effectuer des recherches dans des annuaires, pour les modifier et pour stocker les informations qu'ils contiennent sur des réseaux IP. En outre, LDAP est souvent utilisé pour sécuriser les accès réseau parce qu'il inclut une composante d'authentification. Les annuaires LDAP sont généralement organisés en groupes logiques d'unités. Microsoft Active Directory est un bon exemple d'application de services d'annuaire qui utilise LDAP.

**Outil de configuration**

L'*outil de configuration* est une application de ligne de commande qui permet aux administrateurs de définir les paramètres du site Web d'authentification unique et des produits de source de données CA associés.

**SAML**

*SAML* (Security Assertion Markup Language) est un protocole de sécurité basé sur XML. Le concept de base implique l'échange d'assertions de sécurité concernant un sujet (une personne ou un ordinateur) qui demande l'accès à un domaine sécurisé. Les assertions indiquent notamment si la personne ou l'ordinateur peut accéder à certaines ressources et si une source de données externe, tel qu'un magasin de stratégies, est utilisée.

**SSL (Secure Sockets Layer)**

*SSL* (Secure Sockets Layer) est un protocole de chiffrement pris en charge par de nombreux navigateurs Web pour la sécurité des données sur l'Internet. Les serveurs échangent des certificats SSL qui contiennent une clé publique pour chiffrer les données échangées, et une clé privée pour les déchiffrer. SSL permet au navigateur Web de spécifier le niveau de chiffrement à utiliser en fonction des capacités du navigateur, de l'ordinateur client et du serveur. Le niveau maximum de chiffrement est 256 bits, le plus difficile à déchiffrer.

**TLS**

Le protocole *TLS*, et le protocole antérieur SSL, sont les protocoles de chiffrement pris en charge pour sécuriser la transmission des données sur Internet.  Vous pouvez utiliser les protocoles SSL/TLS conjointement avec le protocole HTTP pour obtenir le protocole HTTPS (HTTP sécurisé).