

À propos de Citrix Usage Collector (versions 1.0 et 1.0.1)

Apr 03, 2015

Citrix Usage Collector recueille et rend compte de la consommation de licences facturable aux Citrix Service Provider directement à Citrix.

Vous pouvez :

- Spécifier les serveurs de licences (points de collecte) à interroger pour les données d'utilisation.
- Dresser la liste des utilisateurs à exclure de la facturation.
- Spécifier les utilisateurs et groupes qui sont uniquement autorisés à consulter les rapports en lecture seule ou qui disposent d'autorisations d'administrateur leur permettant de modifier les configurations.
- Modifier le nom convivial.
- Afficher les rapports actuels ou des rapports antérieurs.
- Afficher des alertes.
- Changer le port.

Notions importantes

Vous pouvez réenregistrer vos informations d'identification My Account dans l'interface Usage Collector, mais ne le faites pas à moins d'être sûr que votre ID client a été modifié. La modification de vos informations d'identification My Account alors que votre ID client n'a pas été modifié peut compromettre la transmission de vos données.

Problèmes résolus

- Cette correction résout la faille de sécurité CVE-2014-0160 (Heartbleed). Pour obtenir davantage d'informations, veuillez consulter l'article [CTX140605](#) du centre de connaissances. [#0479792] (Version 1.0.1)
- Les données d'utilisation peuvent ne pas s'afficher lorsque le serveur de licences est configuré dans l'un ou l'autre de ces scénarios [#0460627] (Version 1.0.1) :
 - Types de licence multiples (par exemple, XDT_PLT et XDT_ENT) et un type ne dispose que d'une seule date Subscription Advantage.
 - Un seul type de licence (par exemple, XDT_PLT) avec de multiples dates Subscription Advantage.
- Le serveur de licences ne peut pas communiquer avec Usage Collector lorsqu'un proxy est configuré. [#0460624] (Version 1.0.1)

Problèmes connus

- Lorsque vous clonez une VM contenant des données dans le dossier de boîte d'envoi, ces données peuvent apparaître sur le serveur cloné. Solution : videz le dossier de boîte d'envoi avant de cloner le serveur. [#0426508]
- Lors de la configuration d'utilisateurs et de groupes, vous pouvez ajouter un nom d'utilisateur ou nom de groupe non valide ou les saisir incorrectement sans recevoir de message d'erreur. Si un nouvel utilisateur ne peut pas ouvrir de session sur le système, vérifiez que le nom d'utilisateur et de groupe sont valides et que l'utilisateur est membre d'Active Directory sur le serveur Citrix Usage Collector. [#0416751]

Configuration système requise pour Citrix Usage Collector

Apr 03, 2015

Citrix Usage Collector est compatible avec le même matériel que celui nécessaire à la prise en charge des systèmes d'exploitation compatibles. Aucun matériel supplémentaire n'est requis.

Configuration requise

- Un ou plusieurs serveurs de licences Citrix, version 11.9 à 11.12.
- Une installation existante de licences utilisateur/machine activées pour Citrix Service Provider sur un ou plusieurs serveurs de licences.
- Les informations d'identification My Account (Se connecter) pour l'accès à citrix.com.
- Un ID client unique doté d'informations d'identification enregistrées à des fins de rapport d'utilisation pour chaque serveur Usage Collector. Utilisez My Account pour obtenir des informations d'identification.

Systèmes d'exploitation	<p>Vous pouvez installer Usage Collector sur des serveurs exécutant les systèmes d'exploitation Microsoft suivants.</p> <ul style="list-style-type: none">• Windows Server 2008 R2• Windows Server 2012
Besoins en espace disque	<ul style="list-style-type: none">• 37 à 40 Mo
Navigateurs	<ul style="list-style-type: none">• Internet Explorer version 9 et 10• Mozilla Firefox version 14.0 et 15.0• Chrome version 14.0 et 15.0

Prise en main de Citrix Usage Collector

Apr 03, 2015

Avant d'utiliser Citrix Usage Collector :

1. Utilisez vos informations d'identification My Account sur citrix.com pour obtenir un ID client unique doté d'informations d'identification enregistrées à des fins de rapport d'utilisation pour chaque serveur Usage Collector.
2. Vérifiez la configuration requise.
3. Téléchargez et installez Usage Collector.
4. Configurez Usage Collector.
5. Installez un certificat manuellement (facultatif).

Installer

Apr 02, 2014

1. Connectez-vous à My Account sur [citrix.com](https://www.citrix.com/downloads/licensing/components/citrix-usage-collector.html) et téléchargez le fichier Ctx_UsageCollector.msi depuis <https://www.citrix.com/downloads/licensing/components/citrix-usage-collector.html>.
2. Démarrez Ctx_UsageCollector.msi.
3. Vous pouvez accepter le port par défaut (8084) ou choisir de configurer un port manuellement.
4. Cliquez sur Lancer Citrix Usage Collector. Cet écran se ferme et une interface Web s'ouvre. Vous pouvez maintenant procéder à la configuration initiale et effectuer une configuration plus poussée si vous le souhaitez.

1. Connectez-vous à My Account sur [citrix.com](https://www.citrix.com/downloads/licensing/components/citrix-usage-collector.html) et téléchargez le fichier Ctx_UsageCollector.msi depuis <https://www.citrix.com/downloads/licensing/components/citrix-usage-collector.html>.
2. Exécutez le programme d'installation de manière silencieuse à partir de la ligne de commande à l'aide de :
msiexec /i Ctx_UsageReportingTool.msi /quiet paramètres

Le tableau suivant décrit les paramètres de commande.

Option	Description
INSTALLDIR =	Répertoire vide existant où les composants seront installés. Remplace le répertoire d'installation par défaut \Citrix\Licensing\UsageCollector.
CTX_UC_PORT=	Remplace le numéro de port par défaut. La valeur par défaut est 8084.
CTX_UC_PORT_AUTO_CONFIG=	Définit la configuration (pare-feu) automatique du port. 1 = activé (valeur par défaut), 0 = désactivé.

Après avoir installé Usage Collector, démarrez l'interface de configuration à partir de Démarrer > Tous les programmes > Citrix > Citrix Usage Collector.

Configurer Citrix Usage Collector

Feb 13, 2015

Utilisez l'interface Configuration initiale après l'installation de Usage Collector.

Si vous avez cliqué sur Lancer Citrix Usage Collector à la fin de l'assistant, l'interface de configuration s'affiche. Vous pouvez également démarrer la configuration initiale à partir de Démarrer > Tous les programmes > Citrix > Citrix Usage Collector.

1. Entrez vos informations d'identification My Account.
2. Entrez un nom de serveur de licences en tant que point de collecte et un port Web. Il n'est pas possible d'ajouter un serveur de licences antérieur à la version 11.9 en tant que point de collecte.

Si vous hébergez de multiples locataires sur le même serveur de licences, assurez-vous que le serveur de licences ne tronque pas @domaine.com.

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

1. Localisez la clé de registre :

Pour machines 32 bits : HKLM\Software\citrix\licenseserver

Pour machines 64 bits : HKLM\Software\Wow6432Node\citrix\licenseserver

Nom : UDUseDomain

2. Définissez la clé de registre sur 1.

Données	Description
0	Le champ de domaine est tronqué. (Défaut)
1	Le champ de domaine n'est pas tronqué.

Après avoir installé Usage Collector et effectué la configuration initiale, vous pouvez configurer et modifier les :

- Points de collecte - serveurs de licences à interroger pour les données d'utilisation
- Utilisateurs autorisés à modifier la configuration
- Utilisateurs uniquement autorisés à accéder aux rapports
- Groupes dotés d'autorisations d'administrateur ou d'accès aux rapports uniquement

1. Pour vous connecter à l'interface Usage Collector, cliquez sur Démarrer > Tous les programmes > Citrix > Citrix Usage Collector.
2. Cliquez sur l'onglet Configuration et choisissez l'une des fonctions dans le menu déroulant.

Tâche	Instructions
<p>Modifier la configuration générale :</p> <ul style="list-style-type: none"> • Nom convivial • Informations sur le programme Citrix Service Provider (CSP) - nom et ID client • Port Web <p>Ré-enregistrer les informations d'identification My Account — ne ré-enregistrez pas vos informations d'identification sauf si vous êtes sûr que votre ID client ID a été modifié ; cela pourrait compromettre la transmission de vos données.</p>	<p>Sur l'onglet Configuration, cliquez sur Général.</p>
<p>Configurer les points de collecte à partir desquels Usage Collector obtient les données d'utilisation de licence. Vous pouvez ajouter ou supprimer des points de collecte.</p> <p>Au moins un point de collecte doit être configuré.</p>	<p>Sur l'onglet Configuration, cliquez sur Points de collecte.</p> <ul style="list-style-type: none"> • Le bouton Tester la configuration envoie une demande de connexion au serveur de licences et vérifie que le service de licences Citrix fonctionne et qu'il exécute au minimum la version 11.9. • Le champ <u>Statut</u> indique si un serveur de licences est en cours d'exécution ou non.
<p>Ajouter, modifier ou supprimer des individus et des groupes et spécifier les rôles des individus et des groupes.</p>	<p>Sur l'onglet Configuration, cliquez sur Utilisateurs.</p>
<p>Ajouter ou supprimer des exceptions. Les exceptions sont des utilisateurs qui ne sont pas comptabilisés par Usage Collector.</p> <p>Par défaut, les exceptions sont des utilisateurs qui ont extrait une licence sur un serveur de licences spécifique. Si vous hébergez de multiples clients sur un seul serveur de licences, utilisez le format utilisateur@domaine.com et assurez-vous que le serveur de licences ne tronquera pas @domaine.com.</p> <p>Étant donné que les noms d'exception peuvent être tronqués en fonction des paramètres du serveur de licences et de la longueur des chaînes, Citrix recommande de créer des exceptions basées sur les noms d'utilisateur renvoyés par uadmin.exe.</p> <p>Contactez Citrix pour vous concerter sur une liste d'exceptions.</p>	<p>Sur l'onglet Configuration, cliquez sur Exceptions.</p>

Installer manuellement un certificat utilisé par Usage Collector associé à un domaine

Nov 06, 2013

Vous pouvez installer manuellement un certificat utilisé par Usage Collector associé à un domaine sur un serveur de licences membre d'un domaine.

Ouvrez une session sur le serveur Citrix Usage Collector, ouvrez la console MMC et suivez ces étapes.

1. Ajoutez le module enfichable pour les certificats en sélectionnant Fichier > Ajouter/supprimer un composant logiciel enfichable > Certificats > Compte d'ordinateur > Ordinateur local.
2. Dans le panneau de gauche sous Certificats, cliquez avec le bouton droit sur Personnel et choisissez Toutes les tâches > Demander un nouveau certificat, et cliquez sur Suivant.
3. Dans l'assistant Inscription de certificats, choisissez Stratégie d'inscription à Active Directory, cliquez sur Suivant, sélectionnez la case en regard de Ordinateur et sélectionnez Détails sur la droite.
4. Dans la zone qui s'affiche, sélectionnez Propriétés et entrez un nom et une description dans les zones de texte sous l'onglet Général et cliquez sur Appliquer.
5. Sélectionnez l'onglet Objet et dans la zone Type de sujet, choisissez Nom commun dans le menu déroulant Type, tapez le nom convivial dans la zone de texte Valeur, cliquez sur Ajouter puis sur Appliquer.
6. Sélectionnez l'onglet Extensions et dans le menu déroulant Utilisation de la clé, ajoutez les options Signature numérique et Chiffrement de la clé à la zone Sélectionnées.
7. Dans le menu déroulant Utilisation de clé étendue (stratégies d'application), ajoutez les options Authentification du serveur et Authentification du client à la zone Sélectionnées et cliquez sur Appliquer.
8. Sélectionnez l'onglet Clé privée et sous le menu déroulant des options de clé, assurez-vous que la taille de clé est de 2048 et que la case Clé exportable est sélectionnée et cliquez sur Appliquer.
9. Sélectionnez l'onglet Autorité de certification et assurez-vous que la case CA est sélectionnée et cliquez sur OK > Inscription > Terminer.
10. Dans la console Certificats, sélectionnez Personnel > Certificats, cliquez sur le certificat que vous avez créé, sélectionnez Toutes les tâches > Exporter > Suivant et sélectionnez le bouton radio Oui, exporter la clé privée et Suivant.
11. Sous Échange d'informations personnelles – PKCS #12 (.pfx), sélectionnez la case à cocher permettant d'inclure tous les certificats, cliquez sur Suivant, créez un mot de passe et cliquez sur Suivant.
12. Cliquez sur Parcourir et accédez à C:\program files (x86)\citrix\licensing\UsageCollector\Apache\conf\, tapez nomdefichier.PFX et suivez les instructions de l'assistant.

Ouvrez une invite de commandes élevée et suivez ces étapes.

1. `cd \program files (x86)\citrix\licensing\UsageCollector\Apache\conf\`
2. `..\bin\openssl pkcs12 -in serveur.pfx -out server.crt -nokeys`
3. Entrez le mot de passe créé durant le processus d'exportation (password).
4. `..\bin\openssl pkcs12 -in serveur.pfx -out server.key -nocerts -nodes`
5. Entrez le mot de passe créé durant le processus d'exportation (password).

6. Redémarrez Usage Collector.

Installer manuellement un certificat utilisé par Usage Collector

Sep 02, 2014

L'installation d'un certificat comprend trois étapes :

1. Obtenez un fichier .pfx qui contient le certificat et la clé privée. Pour ce faire, vous pouvez utiliser l'une des deux méthodes suivantes.
2. Extrayez le certificat et la clé privée du fichier .pfx.
3. Installez le certificat et la clé privée sur Usage Collector.

Connectez-vous à un serveur du domaine, ouvrez la console MMC et procédez comme suit :

1. Créez un répertoire c:\uc_cert devant contenir le fichier .pfx exporté.
2. Ajoutez le module enfichable pour les certificats en sélectionnant Fichier > Ajouter/supprimer un composant logiciel enfichable > Certificats > Compte d'ordinateur > Ordinateur local.
3. Dans le panneau de gauche sous Certificats, cliquez avec le bouton droit sur Personnel et choisissez Toutes les tâches > Demander un nouveau certificat, puis cliquez sur Suivant.
4. Dans l'assistant Stratégie d'inscription de certificats, choisissez Stratégie d'inscription à Active Directory, cliquez sur Suivant, puis sélectionnez la case à cocher en regard de Ordinateur et sélectionnez Détails sur la droite.
5. Sélectionnez Propriétés et, dans l'onglet Général, entrez un nom convivial et une description.
6. Sur l'onglet Objet, sous Nom du sujet, choisissez Nom courant dans le menu déroulant Type, entrez un nom convivial dans la zone de texte et cliquez sur Ajouter, puis sur Appliquer.
7. Sur l'onglet Extensions, choisissez Utilisation de la clé dans le menu déroulant, ajoutez les options Signature numérique et Chiffrement de la clé à la zone Sélectionnées.
8. Dans le menu déroulant Utilisation de la clé étendue, ajoutez les options Authentification du serveur et Authentification du client à la zone Sélectionnées.
9. Sur l'onglet Clé privée et sous le menu déroulant des options de clé, assurez-vous que la taille de clé est 2048 et sélectionnez la case à cocher Clé exportable, puis cliquez sur Appliquer.
10. Sur l'onglet Autorité de certification, vérifiez que la case à cocher CA est sélectionnée et cliquez sur OK > Inscription > Terminer.
11. Dans la console Certificats, sélectionnez Personnel > Certificats, cliquez sur le certificat que vous avez créé, sélectionnez Toutes les tâches > Exporter > Suivant et sélectionnez le bouton radio Oui, exporter la clé privée et Suivant.
12. Sous Échange d'informations personnelles – PKCS #12 (.pfx), sélectionnez la case à cocher permettant d'inclure tous les certificats, cliquez sur Suivant, créez un mot de passe et cliquez sur Suivant.
13. Cliquez sur Parcourir, accédez à C:\uc_cert et tapez server.PFX, puis suivez les instructions de l'assistant pour terminer.

Ces étapes varient en fonction de votre autorité de certification.

1. Ouvrez une session sur Usage Collector, ouvrez la console MMC et suivez ces étapes :
 1. Ajoutez le module enfichable Certificat en sélectionnant Fichier > Ajouter/supprimer un composant logiciel enfichable

- > Certificats > Compte d'ordinateur > Ordinateur local.
- 2. Dans le panneau de gauche sous Certificats, cliquez avec le bouton droit sur Personnel et choisissez Toutes les tâches > Opérations avancées > Créer une demande personnalisée, puis cliquez sur Suivant.
- 3. Sur l'écran Demande personnalisée, choisissez (Aucun modèle) Clé CNG dans le menu déroulant et PKCS#10 pour le format de la demande, puis cliquez sur Suivant.
- 4. Sur l'écran Informations sur le certificat, sélectionnez Détails et Propriétés.
- 5. Sur l'onglet Général, entrez un nom convivial et une description.
- 6. Sur l'onglet Objet, sous Nom du sujet, sélectionnez Nom commun et entrez une valeur dans la zone de texte.
- 7. Sur l'onglet Extensions, choisissez Utilisation de la clé dans le menu déroulant, ajoutez Signature numérique et Chiffrement de la clé.
- 8. Sur l'onglet Extensions, choisissez Utilisation de la clé étendue dans le menu déroulant et ajoutez Authentification du serveur et Authentification du client.
- 9. Sur l'onglet Clé privée, sélectionnez RSA, Microsoft Software Key Storage Provider (valeur par défaut) et dans le menu déroulant, sélectionnez Options de clé et 2048 pour la taille de la clé et Permettre l'exportation de la clé privée.
- 10. Enregistrez le fichier en tant que fichier .req. Ensuite, soumettez le fichier .req à une autorité de certification (CA) et enregistrez le fichier .cer.
- 2. Dans la console MMC, sélectionnez Certificats > Personnel > Certificats et cliquez avec le bouton droit sur Toutes les tâches > Importer. Dans l'assistant d'importation, sélectionnez le fichier .cer.
- 3. Créez un répertoire c:\uc_cert devant contenir le fichier .pfx exporté.
- 4. Dans la console Certificats, sélectionnez Personnel > Certificats, cliquez sur le certificat que vous avez importé, sélectionnez Toutes les tâches > Exporter > Suivant et sélectionnez le bouton radio Oui, exporter la clé privée et Suivant.
- 5. Sous Échange d'informations personnelles – PKCS #12 (.pfx), sélectionnez la case à cocher permettant d'inclure tous les certificats, cliquez sur Suivant, créez un mot de passe et cliquez sur Suivant.
- 6. Cliquez sur Parcourir, accédez à C:\uc_cert et tapez server.PFX, puis suivez les instructions de l'assistant pour terminer.

Cette étape requiert OpenSSL ou un autre outil permettant d'extraire le certificat et la clé privée d'un fichier .pfx.

Important : la version d'OpenSSL fournie avec Usage Collector ne prend pas en charge l'extraction de certificats et de clés privées. Vous pouvez télécharger OpenSSL pour Windows à l'adresse <https://www.openssl.org/related/binaries.html>. Citrix recommande d'installer OpenSSL sur un poste de travail distinct pour effectuer cette procédure :

1. Accédez au dossier <répertoire openssl>\bin.
2. Exécutez `openssl pkcs12 -in C:\uc_cert\server.pfx -out server.crt -nokeys`
Remarque : Usage Collector utilise uniquement le format de certificat .crt.
3. Entrez le mot de passe créé durant le processus d'exportation (password).
4. Exécutez `openssl pkcs12 -in C:\uc_cert\server.pfx -out server.key -nocerts -nodes`
5. Entrez le mot de passe créé durant le processus d'exportation (password).

1. Copiez les fichiers server.crt et server.key créés plus haut dans `cd \program files (x86)\citrix\licensing\UsageCollector\Apache\conf\`
2. Redémarrez Usage Collector.

Rapports

Apr 03, 2015

La page d'accueil de Citrix Usage Collector dresse la liste des résultats compilés par Usage Collector. Ces résultats comprennent :

- Nom du produit.
- Nombre de licences utilisées.
- Nombre d'exceptions. Les exceptions sont des utilisateurs qui ne sont pas comptabilisés par Usage Collector. Vous les spécifiez sur l'écran Exceptions sous l'onglet Configuration. Pour de plus amples informations sur les exceptions, veuillez consulter la section [Configurer Citrix Usage Collector](#).
- Les périodes de facturation sont mensuelles. Vous pouvez afficher les rapports du mois en cours ainsi que des mois précédents.
- Notifications. Permettent d'afficher des messages d'information, d'avertissement et d'erreur. Vous pouvez supprimer des messages individuels ou tous les messages.

 Message d'information

 Message d'avertissement

 Message d'erreur

Exporter des rapports

La page d'accueil Usage Collector contient une option permettant d'exporter et enregistrer des rapports de facturation.

Lorsque vous cliquez sur Exporter un rapport, vous pouvez au choix ouvrir ou enregistrer le fichier .csv et le bouton change en Enregistrer, ce qui vous permet d'ouvrir ou d'enregistrer de nouveau ce même fichier de rapport. Pour exporter un nouveau rapport, actualisez l'écran du navigateur et le bouton Exporter un rapport s'affiche de nouveau.

Citrix recommande de supprimer les rapports de façon périodique si l'espace disque est limité.

Citrix conserve des rapports d'utilisation quotidiens pour la période de facturation en cours. Une fois que le dernier rapport du mois a été transmis, Citrix supprime les rapports quotidiens et ne conserve que les rapports de facturation mensuels.