Citrix Usage Collector（Version 1.0および1.0.1）について

Apr 03, 2015

Citrix Usage Collectorは、Citrix Service Providerによる請求対象ライセンスの使用状況データを収集して、Citrixに直接レポートします。

マシンの追加方法

- 使用状況データをポーリングするライセンスサーバー（コレクションポイント）を指定します。
- 課金対象から除外するユーザーを一覧します。
- ユーザーやグループを指定して、レポートを表示するための読み取り専用権限または構成を変更するための管理者権限を付与します。
- フレンドリ名を変更します。
- 現在または過去のレポートを表示します。
- アラートを表示します。
- ポートを変更します。

注意事項

My Accountの資格情報はUsage Collectorのユーザーインターフェイスで再登録できますが、カスタマーIDが変更されたことが確実でなければ、再登録しないでください。カスタマーIDが変更されていない場合にMy Accountの資格情報を変更すると、データ伝送に失敗するおそれがあります。

解決された問題

- この修正により、脆弱性の問題CVE-2014-0160（Heartbleed）が解決されます。詳しくは、Knowledge CenterのCTX140605を参照してください。[#0479792]（Version 1.0.1）
- 次のいずれかのシナリオでライセンスサーバーが構成されている場合、使用状況データが表示されないことがありました[#0460627]（Version 1.0.1）。
  - 複数のライセンスの種類（たとえば、XDT_PLTおよびXDT_ENT）と1つのライセンスの種類に1つのSubscription Advantage日しかない場合。
  - 1つのライセンスの種類（たとえば、XDT_PLT）に複数のSubscription Advantage日がある場合。
- プロキシが構成されるとライセンスサーバーがUsage Collectorと通信できない場合。[#0460624]（Version 1.0.1）

既知の問題

- 複製した仮想マシンのoutboxフォルダーにデータが存在する場合、そのデータが複製後のサーバーでも表示される可能性があります。回避策：サーバーを複製する前にoutboxフォルダーを空にしてください。[#0426508]
- ユーザーとグループを構成するとき、無効なユーザー名またはグループ名を入力してもエラーメッセージが表示されず、追加できてしまう可能性があります。新しいユーザーがシステムにログオンできない場合は、ユーザーおよびグループの名前が有効であることと、ユーザーがCitrix Usage Collectorサーバー上のActive Directoryのメンバーであることを確認してください。[#0416751]

Citrix Usage Collectorのシステム要件

Apr 03, 2015

Citrix Usage Collectorを使用するために必要なハードウェアは、各オペレーティングシステムでのハードウェア要件と同じです。ハードウェアを追加する必要はありません。

要件

- Version 11.9～11.12の、1台または複数のCitrixライセンスサーバー。
- 1台または複数のライセンスサーバーにインストール済みの、Citrix Service Provider対応のユーザー/デバイスライセンス。
- citrix.comのMy Account資格情報。
- 各Usage Collectorサーバーで使用状況をレポートするために登録する、一意のカスタマーID。My Accountを使用して資格情報を取得します。

オペレーティングシステム	Usage Collectorは、以下のMicrosoftオペレーティングシステムが動作するサーバーにインストールできます。 • Windows Server 2008 R2 • Windows Server 2012
空きディスク容量	• 37～40MB
Webブラウザー	• Internet Explorer Version 9および10 • Mozilla Firefox Version 14.0および15.0 • Chrome Version 14.0および15.0

Citrix Usage Collectorの概要

Apr 03, 2015

Citrix Usage Collectorを使用する前に：

1. citrix.comのMy Account資格情報を使用して、一意のカスタマーIDを取得します。各Usage Collectorサーバーで使用状況をレポートするために、このIDを登録します。
2. 要件を確認します。
3. Usage Collectorをダウンロードしてインストールします。
4. Usage Collectorを構成します。
5. 証明書を手動でインストールします（オプション）。

インストール

Apr 02, 2014

1. citrix.comの［My Account］にログオンして、https://www.citrix.com/downloads/licensing/components/citrix-usage-collector.htmlでCtx_UsageCollector.msiをダウンロードします。
2. Ctx_UsageCollector.msiを実行します。
3. デフォルトのポート（8084）をそのまま使用することも、ポートの手動構成を選択することもできます。
4. ［Citrix Usage Collectorの起動］をクリックします。 この画面が閉じてWebベースのユーザーインターフェイスが開きます。 初期構成およびさらに高度な構成を実行できます。

1. citrix.comの［My Account］にログオンして、https://www.citrix.com/downloads/licensing/components/citrix-usage-collector.htmlでCtx_UsageCollector.msiをダウンロードします。
2. コマンドラインから以下のコマンドを実行してインストーラーをサイレント実行します。
   msiexec /i Ctx_UsageReportingTool.msi /quiet parameters

   次の表は、コマンドパラメーターの一覧です。

オプション	説明
INSTALLDIR =	コンポーネントのインストール先として既存の空ディレクトリを指定します。デフォルトのインストールディレクトリである%ProgramFiles%\Citrix\Licensing\UsageCollectorを上書きします。
CTX_UC_PORT=	デフォルトのポート番号を上書きします。デフォルトのポートは8084です。
CTX_UC_PORT_AUTO_CONFIG=	自動ポート（ファイアウォール）構成を設定します。1はオン（デフォルト）、0はオフです。

Usage Collectorをインストールしたら、［スタート］、［すべてのプログラム］、［Citrix］、［Citrix UsageCollector］の順に選択して構成のユーザーインターフェイスを開きます。

Citrix Usage Collectorの構成

Jan 23, 2017

Usage Collectorをインストールした後で、［初回構成］のユーザーインターフェイスを使用します。

インストールウィザードの最後に［Citrix Usage Collectorの起動］をクリックすると、構成のユーザーインターフェイスが開きます。［スタート］、［すべてのプログラム］、［Citrix］、［Citrix Usage Collector］の順に選択して、初回構成を開始することもできます。

1. My Accountの資格情報を入力します。
2. コレクションポイントとしてのライセンスサーバーの名前およびWebポートを入力します。 Version 11.9より前のライセンスサーバーは、コレクションポイントとして追加できません。

単一のライセンスサーバー上で複数のテナントをホストする場合は、以下の手順に従って、ライセンスサーバーで「@domain.com」の部分が切り捨てられないように設定します。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. 以下のレジストリキーを検索します。
   32ビットマシンの場合：HKLM\Software\citrix\licenseserver

   64ビットマシンの場合：HKLM\Software\Wow6432Node\citrix\licenseserver

   値の名前：UDUseDomain

2. 値のデータとして、1を設定します。

データ	説明
0	ドメイン名が切り捨てられます（デフォルト）
1	ドメイン名が切り捨てられません

Usage Collectorをインストールして初回構成を実行した後は、以下の項目を構成および変更できます。

- コレクションポイント - 使用状況データをポーリングするライセンスサーバー
- 構成を変更できるユーザー
- レポートの読み取り専用権限を持つユーザー
- 管理者権限またはレポートの読み取り専用権限を持つグループ

1. ［スタート］、［すべてのプログラム］、［Citrix］、［Citrix Usage Collector］の順に選択して、Usage Collectorのユーザーインターフェイスを開きます。
2. ［構成］タブをクリックしてボックスの一覧から機能を選択します。

目的	手順
一般的な構成の編集： ● フレンドリ名 ● Citrix Service Provider（CSP）情報 - カスタマー名およびID ● Webポート My Account資格情報の再登録 - カスタマーIDが変更されたことが確実でなければ、再登録しないでください。登録情報に不一致が発生すると、データ伝送に失敗するおそれがあります。	［構成］タブの［一般］をクリックします。
Usage Collectorでライセンスの使用状況データを取得するコレクションポイントの構成。コレクションポイントは追加または削除できます。 少なくとも1つ構成済みのコレクションポイントが必要です。	［構成］タブの［コレクションポイント］をクリックします。 ● ［接続テスト］をクリックすると接続要求がライセンスサーバーに送信され、Citrix Licensingサービスが実行中であり Version 11.9以降であることが確認されます。 ● ［状態］ボックスに、ライセンスサーバーが動作しているかどうかが表示されます。
個人およびグループの追加、編集、または削除、および個人およびグループの役割の指定。	［構成］タブの［ユーザー］をクリックします。
例外の追加および削除。例外とは、Usage Collectorの対象から除外されるユーザーを指します。 デフォルトでは、例外は特定のライセンスサーバー上のライセンスをチェックアウトしたユーザーです。単一のライセンスサーバー上で複数のクライアントをホストする場合は、「user@domain.com」形式を使用し、ライセンスサーバーで「@domain.com」の部分が切り捨てられないように設定してください。 例外名はライセンスサーバーの設定と文字列の長さに基づいて切り捨てられる可能性があるため、udamin.exeで表示されるユーザー名に基づいて例外を作成することをお勧めします。 Citrixに連絡して例外の内容について合意してください。	［構成］タブの［例外］をクリックします。

1. コマンドラインで、**/opt/citrix/licensing/LS/conf/ud_settings.conf**ファイルを開きます。
2. **vi**エディターを使用して、**CTX_UD_USERDOMAIN**を**1**に設定します。
3. ライセンスサーバーVPXまたはCitrixライセンスサーバーデーモンを再起動します。

設定	説明
CTX_UD_USERDOMAIN=1	ユーザープロファイルのユーザードメインを使用します。 ドメイン名切り捨ては無効化されます。
CTX_UD_USERDOMAIN=0	ユーザープロファイルのユーザードメインを使用しません。 （デフォルト）

データ
0
1

データ
0
1

ドメインに属しているUsage Collectorで使用する証明書の手動インストール

Nov 06, 2013

ドメインに属しているUsage Collectorで使用する証明書を、ドメインに属しているライセンスサーバーに手動でインストールできます。

Citrix Usage Collectorサーバーにログオンして MMCを開き、次の手順に従います。

1. ［ファイル］、［スナップインの追加と削除］、［証明書］、［コンピューターアカウント］、［ローカルコンピューター］の順に選択して、証明書スナップインを追加します。
2. 左ペインの［証明書］の下の［個人］を右クリックし、［すべてのタスク］、［新しい証明書の要求］の順に選択して［次へ］をクリックします。
3. 証明書の登録ポリシーウィザードで［Active Directory登録ポリシー］を選択して［次へ］をクリックし、［コンピューター］の隣のチェックボックスをオンにして右側の［詳細］をクリックします。
4. 表示されるボックス内の［プロパティ］をクリックし、［全般］タブのボックスにフレンドリ名と説明を入力して［適用］をクリックします。
5. ［サブジェクト］タブをクリックし、［サブジェクト名］の下の［種類］ボックスの一覧から［共通名］を選択し、［値］ボックスにフレンドリ名を入力して［追加］、［適用］の順にクリックします。
6. ［拡張機能］タブをクリックし、［キー使用法］セクションの［選択されたオプション］ボックスに［デジタル署名］および［キーの暗号化］を追加します。
7. ［拡張キー使用法（アプリケーションポリシー）］セクションの［選択されたオプション］ボックスに［サーバー認証］および［クライアント認証］を追加して、［適用］をクリックします。
8. ［秘密キー］タブをクリックし、［キーのオプション］セクションの［キーのサイズ］が2048で［秘密キーをエクスポート可能にする］チェックボックスがオンになっていることを確認して、［適用］をクリックします。
9. ［証明機関］タブをクリックし、証明機関のチェックボックスがオンになっていることを確認して、［OK］、［登録］、［完了］の順にクリックします。
10. ［証明書］コンソールで［個人］、［証明書］の順に選択し、作成した証明書を右クリックして［すべてのタスク］、［エクスポート］、［次へ］の順に選択します。［はい、秘密キーをエクスポートします］をクリックして［次へ］をクリックします。
11. ［Personal Information Exchange – PKCS #12(.PFX)］の下の［証明のパスにある証明書を可能であればすべて含む］チェックボックスをオンにして［次へ］をクリックし、パスワードを作成して［次へ］をクリックします。
12. ［参照］をクリックしてC:\program files (x86)\citrix\licensing\UsageCollector\Apache\conf\に移動し、「<filename>.PFX」と入力します。ウィザードの指示に従って完了します。

管理者特権でのコマンドプロンプトを開き、次の手順に従います。

1. cd \program files (x86)\citrix\licensing\UsageCollector\Apache\conf\
2. ..\bin\openssl pkcs12 -in <server>.pfx -out server.crt –nokeys
3. エクスポート処理で作成したパスワードを入力します。
4. ..\bin\openssl pkcs12 -in <server>.pfx -out server.key -nocerts –nodes

5. エクスポート処理で作成したパスワードを入力します。
6. Usage Collectorを再起動します。

Usage Collectorで使用する証明書の手動インストール

Sep 02, 2014

証明書は、以下の3つの手順を行ってインストールします。

1. 証明書および秘密キーを含んでいるPFXファイルを入手します。後述する2つのいずれかの方法でこれを行います。
2. PFXファイルから証明書および秘密キーを抽出します。
3. 証明書および秘密キーをUsage Collector上にインストールします。

サーバーにログオンしてMMCを開き、次の手順に従います。

1. エクスポートしたPFXファイルを格納するためのc:\uc_certディレクトリを作成します。
2. ［ファイル］、［スナップインの追加と削除］、［証明書］、［コンピューターアカウント］、［ローカルコンピューター］の順に選択して、証明書スナップインを追加します。
3. 左ペインの［証明書］の下の［個人］を右クリックし、［すべてのタスク］、［新しい証明書の要求］の順に選択して［次へ］をクリックします。
4. 証明書の登録ポリシーウィザードで［Active Directory登録ポリシー］を選択して［次へ］をクリックし、［コンピューター］の隣のチェックボックスをオンにして右側の［詳細］をクリックします。
5. ［プロパティ］を選択して、［全般］タブにフレンドリ名と説明を入力します。
6. ［サブジェクト］タブの［サブジェクト名］の下の［種類］ボックスの一覧から［共通名］を選択し、ボックスにフレンドリ名を入力して［追加］、［適用］の順にクリックします。
7. ［拡張機能］タブで［キー使用法］のドロップダウンメニューを開き、［選択されたオプション］ボックスに［デジタル署名］および［キーの暗号化］を追加します。
8. ［拡張キー使用法］のドロップダウンメニューを開き、［選択されたオプション］ボックスに［サーバー認証］および［クライアント認証］を追加します。.
9. ［秘密キー］タブをクリックし、［キーのオプション］の［キーのサイズ］が2048で［秘密キーをエクスポート可能にする］チェックボックスがオンになっていることを確認して、［適用］をクリックします。
10. ［証明機関］タブをクリックし、証明機関のチェックボックスがオンになっていることを確認して、［OK］、［登録］、［完了］の順にクリックします。
11. ［証明書］コンソールで［個人］、［証明書］の順に選択し、作成した証明書を右クリックして［すべてのタスク］、［エクスポート］、［次へ］の順に選択します。［はい、秘密キーをエクスポートします］をクリックして［次へ］をクリックします。
12. ［Personal Information Exchange – PKCS #12(.PFX)］の下の［証明のパスにある証明書を可能であればすべて含む］チェックボックスをオンにして［次へ］をクリックし、パスワードを作成して［次へ］をクリックします。
13. ［参照］をクリックしてC:\uc_certを開き、「server.PFX」と入力します。後は、ウィザードの指示に従って完了します。

以下の手順は、使用する証明機関により異なる場合があります。

1. Usage Collectorにログオンして MMCを開き、次の手順に従います。
    1. ［ファイル］、［スナップインの追加と削除］、［証明書］、［コンピューターアカウント］、［ローカルコンピューター］の順に選択して、証明書スナップインを追加します。
    2. 左ペインの［証明書］の下の［個人］を右クリックし、［すべてのタスク］、［詳細設定操作］、［カスタム要求の作

成］の順に選択して［次へ］をクリックします。
3. ［カスタム要求］ページでボックスの一覧から［（テンプレートなし）CNGキー］を選択し、要求の形式として［PKCS #10］を選択して［次へ］をクリックします。
4. ［証明書情報］ページで［詳細］のドロップダウンメニューを開き、［プロパティ］をクリックします。
5. ［全般］タブにフレンドリ名と説明を入力します。
6. ［サブジェクト］タブの［サブジェクト名］の下で［共通名］を選択して、ボックスに値を入力します。
7. ［拡張機能］タブで［キー使用法］のドロップダウンメニューを開き、［デジタル署名］および［キーの暗号化］を追加します。
8. ［拡張機能］タブで［拡張キー使用法］のドロップダウンメニューを開き、［サーバー認証］および［クライアント認証］を追加します。
9. ［秘密キー］タブで［暗号化サービスプロバイダー］のドロップダウンメニューを開き、［RSA, Microsoft Software Key Storage Provider］（デフォルト）を選択します。また、［キーのオプション］でキーのサイズとして［2048］を選択し、［秘密キーをエクスポート可能にする］チェックボックスをオンにします。
10. 要求をREQファイル（*.req）として保存して、それを証明機関（CA）に送信し、CERファイルを保存します。

2. MMCで［証明書］、［個人］、［証明書］の順に選択し、右クリックして［すべてのタスク］、［インポート］の順に選択します。 インポートウィザードでCERファイルを選択します。
3. エクスポートしたPFXファイルを格納するためのc:\uc_certディレクトリを作成します。
4. ［証明書］コンソールで［個人］、［証明書］の順に選択し、インポートした証明書を右クリックして［すべてのタスク］、［エクスポート］、［次へ］の順に選択します。［はい、秘密キーをエクスポートします］をクリックして［次へ］をクリックします。
5. ［Personal Information Exchange – PKCS #12（.PFX）］の下の［証明のパスにある証明書を可能であればすべて含む］チェックボックスをオンにして［次へ］をクリックし、パスワードを作成して［次へ］をクリックします。
6. ［参照］をクリックしてC:\uc_certを開き、「server.PFX」と入力します。後は、ウィザードの指示に従って完了します。

この手順を行うには、OpenSSLなど、PFXファイルから証明書や秘密キーを抽出するためのツールが必要です。

重要：Usage Collectorに付属のバージョンのOpenSSLでは、証明書や秘密キーを抽出できません。OpenSSL for Windowsは、https://www.openssl.org/related/binaries.htmlからダウンロードできます。ダウンロードしたOpenSSLをほかのワークステーション上にインストールして以下の手順を行うことをお勧めします。

1. <openssl directory>\binフォルダーを開きます。
2. 次のコマンドを実行します。openssl pkcs12 -in C:\uc_cert\server.pfx -out server.crt -nokeys
   注：Usage Collectorで使用できる証明書の形式は、CRTのみです。
3. エクスポート処理で作成したパスワードを入力します。
4. 次のコマンドを実行します。openssl pkcs12 -in C:\uc_cert\server.pfx -out server.key -nocerts –nodes
5. エクスポート処理で作成したパスワードを入力します。

1. 上記の手順で作成したserver.crtとserver.keyを以下のフォルダーにコピーします。cd \program files (x86)\citrix\licensing\UsageCollector\Apache\conf\
2. Usage Collectorを再起動します。

レポート

Sep 03, 2015

Citrix Usage Collectorのホームページには、Usage Collectorにより蓄積された結果が一覧表示されます。結果には以下の項目が含まれます。

- 製品名。
- 使用中のライセンス数。
- 例外数。例外とは、Usage Collectorの対象から除外されるユーザーを指します。これは、［構成］タブの下の［例外］画面で指定します。例外について詳しくは、「Citrix Usage Collectorの構成」を参照してください。
- 課金期間は月単位です。過去の月はもちろん、現在の月のレポートを表示できます。
- 通知。情報、警告、およびエラーのメッセージを表示します。メッセージは個別にまたは一括して削除できます。

   情報メッセージ

   警告メッセージ

   エラーメッセージ

レポートのエクスポート

Usage Collectorのホームページには課金レポートをエクスポートして保存するオプションが含まれています。

［レポートのエクスポート］をクリックするとき、.csvファイルを開くか保存するかを選択できます。ボタンが[レポートの保存］に変わり、同じレポートファイルを再度開くか保存できるようになります。新しいレポートをエクスポートするには、Webブラウザーの画面を更新します。［レポートのエクスポート］ボタンが再度表示されます。

ディスクスペースが限られている場合は、レポートを定期的に削除することをお勧めします。

Citrixは、現在の課金期間中は日次の使用状況レポートを維持します。当月最後のレポートが送信された後に、Citrixは日次レポートを削除して月次課金レポートのみを永久に保存します。