Session Recording 2210

Contents

Session Recording 2210

May 1, 2023

> 重要:
>
> 最新リリース（CR）および長期サービスリリース（LTSR）の製品ライフサイクル戦略は、「Lifecycle Milestones」で説明しています。

Session Recording により録画、カタログ化、およびアーカイブされるセッションを、後で取得して再生することができます。

アプリケーションおよびデスクトップセッションの録画を自動的に起動する、柔軟性の高いポリシーが提供されます。また、動的なセッションの録画がサポートされます。この機能により、IT 担当者はユーザーアクティビティを監視および確認できます。このように Session Recording は、企業が法規制順守やセキュリティ監視に関する内部統制を行ううえで役に立ちます。同様に、技術サポート部門でこの機能を使用すれば、問題の特定と解決までの時間を短縮することができます。

長所

ログと監視によるセキュリティの強化。Session Recording により、機密情報を取り扱うアプリケーションで、エンドユーザーの画面上での操作を録画できるため、仮想セッションからの機密情報の漏えいについて監視および防止できます。機密情報の漏えいの防止は、医療や金融などの規制の厳しい業界では、特に重要な機能です。

高機能アクティビティ監視。マウスのクリックおよび目に見えるキーボード入力などの画面の更新をキャプチャしてアーカイブすることで、特定のエンドユーザー、アプリケーション、およびサーバーの操作を録画できます。

Session Recording は、法的手続きの証拠収集を目的に開発されてはいません。ただし組織は、Session Recording を他の手法（一般的な動画録画とテキストベースの電子証拠開示ツールの組み合わせなど）とともに使用して、証拠の収集を行うことができます。

迅速な問題解決。再現が難しい問題についてユーザーが問い合わせをしたときに、ヘルプデスクのサポートスタッフはユーザーセッションを録画できます。問題が再発したら、発生時刻が記録されているエラーの録画を使用して、より迅速に問題のトラブルシューティングができます。

新機能

December 22, 2022

2210 の新機能

このリリースは、次の新機能が含まれ問題に対応しているため、より優れたユーザーエクスペリエンスを提供します。

セッション **0** でのインストールのサポート

セッション 0 での Session Recording Administration コンポーネントのインストールを自動化するために、このリリースでは **AllowSession0Install** 引数が導入されています。詳しくは、「インストールの自動化」を参照してください。

以前のリリースの新機能

1912 LTSR～2209 最新リリース（CR）の後に出荷されたリリースの新機能については、「新機能の履歴」を参照してください。

解決された問題

December 22, 2022

Session Recording 2209 との比較

Session Recording 2210 には、以下の修正が追加されています：

- アクセス制限を変更するために一度に 40 を超える録画を選択すると、タイムアウトエラーが発生することがあります。[SRT-8496]

既知の問題

April 3, 2024

このリリースでは、次の問題が確認されています：

- CVE-2021-44228 の脆弱性を部分的に緩和するために Citrix Web App Firewall（WAF）シグネチャを使用している場合、Session Recording が正常に機能しない可能性があります。この問題を解決するには、Session Recording サーバーの IP アドレスを NetScaler 側の **mitigate_cve_2021_44228** ポリシーから除外します。[CVADHELP-24365]

- Session Recording ポリシーコンソールでローカル管理者権限を持つドメインユーザーは、ローカルユーザーとドメインユーザーをポリシー規則のアクションの適用対象として追加できます。ただし、ローカル管理者権限を持つローカルユーザーは、ローカルユーザーのみを追加でき、ドメインユーザーは追加できません。[SRT-5769]
- バージョン 2009 以前からアップグレードすると、Web Player が正しく機能しないことがあります。この問題を回避するには、Web ブラウザーのキャッシュをクリアします。[SRT-5624]
- カスタムポリシーの規則は、Session Recording を XenApp and XenDesktop 7.6 LTSR に含まれるバージョンから最新バージョンに更新すると、失われることがあります。この問題を回避するには、XenApp and XenDesktop 7.15 LTSR の最新 CU に含まれるバージョンに更新してから、最新リリースに更新します。[SRT-4546]
- Machine Creation Services（MCS）または Citrix Provisioning（PVS）で、インストール済みの Microsoft Message Queuing（MSMQ）を使用して複数の VDA を作成すると、これらの VDA の`QMId`が同じになる可能性があります。この状態は、次のようなさまざまな問題を引き起こす可能性があります：
  - 録画の同意が得られていても、セッションが録画されない場合があります。
  - セッションのログオフ信号が Session Recording サーバーによって受信されず、セッションのステータスが常に［ライブ］になってしまう場合があります。

  回避策について詳しくは、「インストール、アップグレード、およびアンインストール」を参照してください。[#528678]

サードパーティ製品についての通知

February 20, 2024

Session Recording バージョン 2210（PDF のダウンロード）

Session Recording のこのリリースには、次のドキュメントで定義された条件の下でライセンスが有効になったサードパーティのソフトウェアが含まれている可能性があります。

システム要件

March 1, 2023

Session Recording は、Session Recording Administration コンポーネント、Session Recording Agent、および Session Recording Player から構成されています。Session Recording Administration コンポーネント（Session Recording データベース、Session Recording サーバー、Session Recording ポリシーコンソール）

は、1 台のサーバーにインストールすることも、異なるサーバーにインストールすることも可能です。ここでは、各 Session Recording コンポーネントの要件について詳しく説明します。

長期サービスリリース（LTSR）環境でのこの最新リリース（CR）の使用について、およびその他のよくある質問については、Knowledge Centerの記事を参照してください。

Session Recording データベース

以下のオペレーティングシステムがサポートされています：

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

サポートされている Microsoft SQL Server のバージョン：

- Microsoft SQL Server 2019 Enterprise、Express、および Standard Edition
- Microsoft SQL Server 2017 Enterprise、Express、および Standard Edition
- Microsoft SQL Server 2016 SP2 Enterprise、Express、および Standard Edition
- Microsoft SQL Server 2016 SP1 Enterprise、Express、および Standard Edition
- Microsoft SQL Server 2014 SP2 Enterprise、Express、および Standard Edition
- Microsoft SQL Server 2012 SP3 Enterprise、Express、および Standard Edition
- Microsoft SQL Server 2008 R2 SP3 Enterprise、Express、および Standard Edition

サポートされている Azure SQL データベースサービス：

- Azure SQL Managed Instance
- Azure 仮想マシン（VM）上の SQL Server
  （前述のサポートされているバージョンの Microsoft SQL Server を使用します。）

サポートされている AWS RDS データベースサービス：

- SQL Server

要件：.NET Framework 4.7.2

Session Recording サーバー

以下のオペレーティングシステムがサポートされています：

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

そのほかの要件:

- インターネットインフォメーションサービス（IIS）10、8.5、8.0 または 7.5
- .NET Framework Version 4.7.2
- Session Recording サーバーで、通信プロトコルとして HTTPS、および有効な証明書を使用する場合。Session Recording では、デフォルトで Citrix の推奨プロトコルである HTTPS が使用されます。
- Active Directory 統合を無効にし、MSMQ HTTP サポートを有効にした Microsoft Message Queuing（MSMQ）。
- 管理者ログの場合：Chrome、Firefox、または Internet Explorer 11 の最新バージョン

Session Recording ポリシーコンソール

以下のオペレーティングシステムがサポートされています:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

要件：.NET Framework 4.7.2

Session Recording Agent

Session Recording Agent は、セッションを録画するすべての Windows Virtual Delivery Agent（VDA）にインストールします。

以下のオペレーティングシステムがサポートされています:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 11
- Windows 10、最小バージョン 1607
- Windows 10 Enterprise for Virtual Desktops

要件:

- Citrix Virtual Apps and Desktops 7 2203 Premium ライセンス
- Citrix Virtual Apps and Desktops 7 1912 LTSR CU4 以降の Platinum ライセンス
- XenApp および XenDesktop 7.15 LTSR CU8 Platinum ライセンス
- .NET Framework 4.7.2
- Active Directory 統合を無効にし、MSMQ HTTP サポートを有効にした Microsoft Message Queuing（MSMQ）

> 注:
>
> Session Recording は現在、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の Advanced、Advanced Plus、Premium、Premium Plus などのエディションをサポートしています。

Session Recording Player

以下のオペレーティングシステムがサポートされています:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 11
- 64 ビット版 Windows 10、最小バージョン 1607

要件：.NET Framework 4.7.2

> 注:
>
> 32 ビット版 Windows 10 で、SessionRecordingPlayer.msi ファイルを使用してのみ Player をインストールできます。msi ファイルは、**\layout\image-full\x86\Session Recording** の Citrix Virtual Apps and Desktops ISO で見つけることができます。

最適なパフォーマンスを得るには、Session Recording Player を以下の条件のワークステーションにインストールします:

- 1024 X 768 の画面解像度
- 32 ビット以上の色数
- 2GB RAM（最小）。グラフィックが多用されている録画を再生する場合、特に録画にアニメーションが多く含まれる場合には、RAM および CPU/GPU リソースを追加すると、パフォーマンスが向上します。

シークの応答速度は、録画のサイズやマシンのハードウェア仕様によって異なります。

開始

February 20, 2024

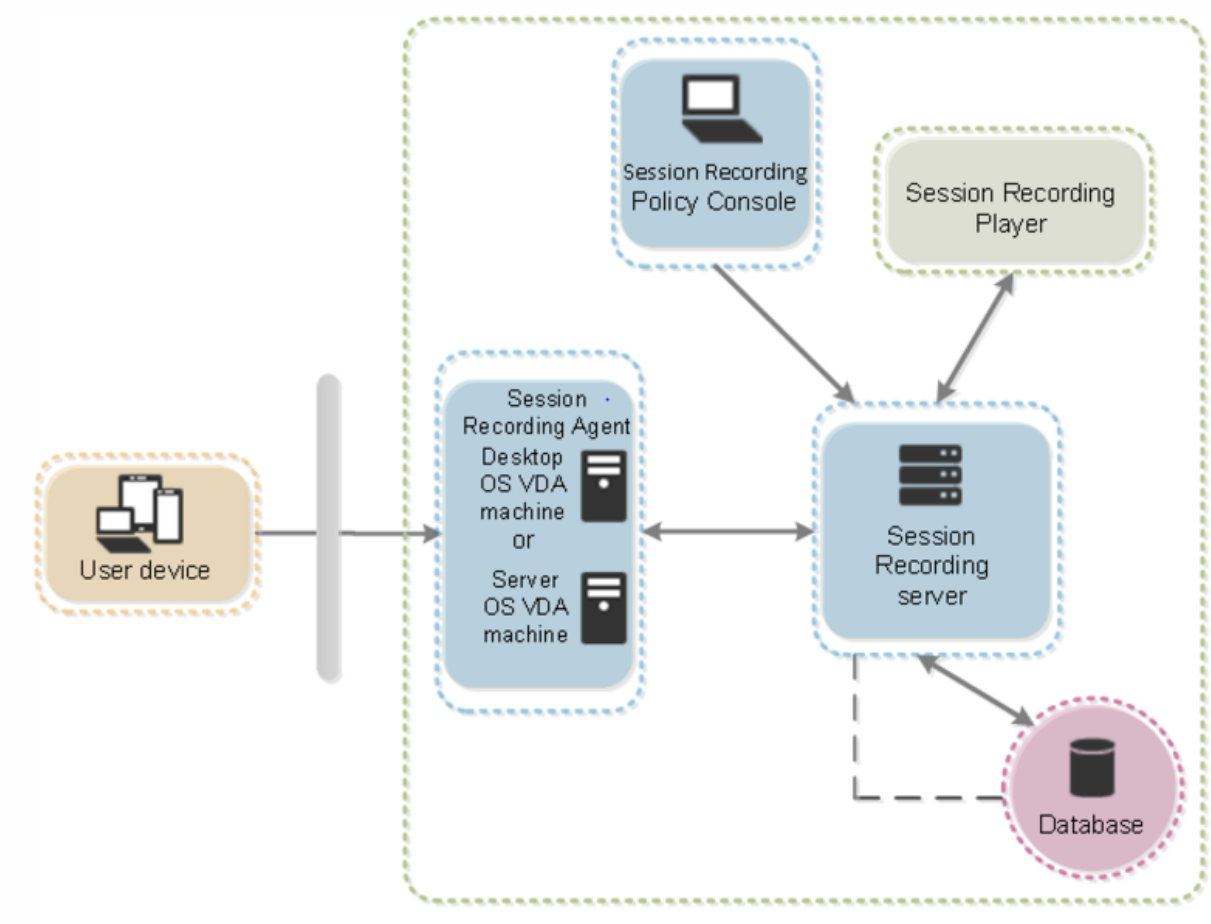
Session Recording は 5 つのコンポーネントから構成されます:

- **Session Recording Agent**。マルチセッション OS またはシングルセッション OS 対応 VDA にインストールされる、録画処理を有効にするコンポーネントです。これによりセッションデータが録画されます。
- **Session Recording** サーバー。次のサービスをホストするサーバーです。

  - ブローカー：以下の目的に役立つ IIS 6.0 以降でホストされる Web アプリケーション：
    * Session Recording Player と Web Player からの検索クエリとファイルダウンロード要求の処理。
    * Session Recording ポリシーコンソールからのポリシー管理要求の処理。
    * Citrix Virtual Apps and Desktops または Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の各セッションの録画ポリシーの評価。
  - ストレージマネージャー：Windows サービスです。これにより、Session Recording が有効な VDA から受信する、セッションの録画ファイルが管理されます。
  - 管理者ログ：Session Recording サーバーでインストールされる、管理アクティビティをログに記録するための任意のサブコンポーネントです。ログデータはすべて、デフォルトで **CitrixSessionRecordingLogging** という名前の個別の SQL Server データベースに格納されます。データベース名はカスタマイズすることができます。

- **Session Recording Player**。セッションのファイルを調査するユーザーが、録画を再生するためにワークステーションでアクセスするユーザーインターフェイスです。
- **Session Recording** データベース。セッションの録画データを格納するための SQL データベースを管理するコンポーネントです。このコンポーネントがインストールされていると、デフォルトで **CitrixSessionRecording** という名前のデータベースが作成されます。データベース名はカスタマイズすることができます。
- **Session Recording** ポリシーコンソール。録画するセッションを指定するポリシーを作成するコンソールです。

ここに示す展開例では、すべての Session Recording コンポーネントがセキュリティファイアウォールの背後にあります。Session Recording Agent は、マルチセッション OS またはシングルセッション OS の VDA にインストールされます。第 2 のサーバーは Session Recording ポリシーコンソールをホストし、第 3 のサーバーは Session Recording サーバーとして機能します。そして、第 4 のサーバーは Session Recording データベースをホストします。Session Recording Player はワークステーションにインストールされます。ファイアウォール外部のクライアントデバイスは、Session Recording Agent がインストールされている VDA に接続します。ファイアウォール内では、Session Recording Agent、ポリシーコンソール、Player、およびデータベースはすべて Session Recording サーバーに接続します。



展開計画

February 20, 2024

制限事項

Session Recording では、デスクトップコンポジションのリダイレクト (DCR) の表示モードはサポートされません。デフォルトでは、Session Recording は、録画されるセッションの DCR を無効化します。この動作は、[**Session Recording Agent** のプロパティ] で設定できます。

Internet Explorer のブラウザーコンテンツのリダイレクトポリシーに設定されている URL を参照すると、グラフィックスアクティビティが録画されません。

Session Recording では、Framehawk の表示モードはサポートされません。このため、Framehawk の表示モードのセッションを正しく録画および再生することはできません。Framehawk の表示モードで録画されたセッションには、セッションアクティビティが含まれない可能性があります。

HDX RealTime Optimization Pack を使用している場合、Session Recording で Lync Web カメラの映像を録画することはできません。

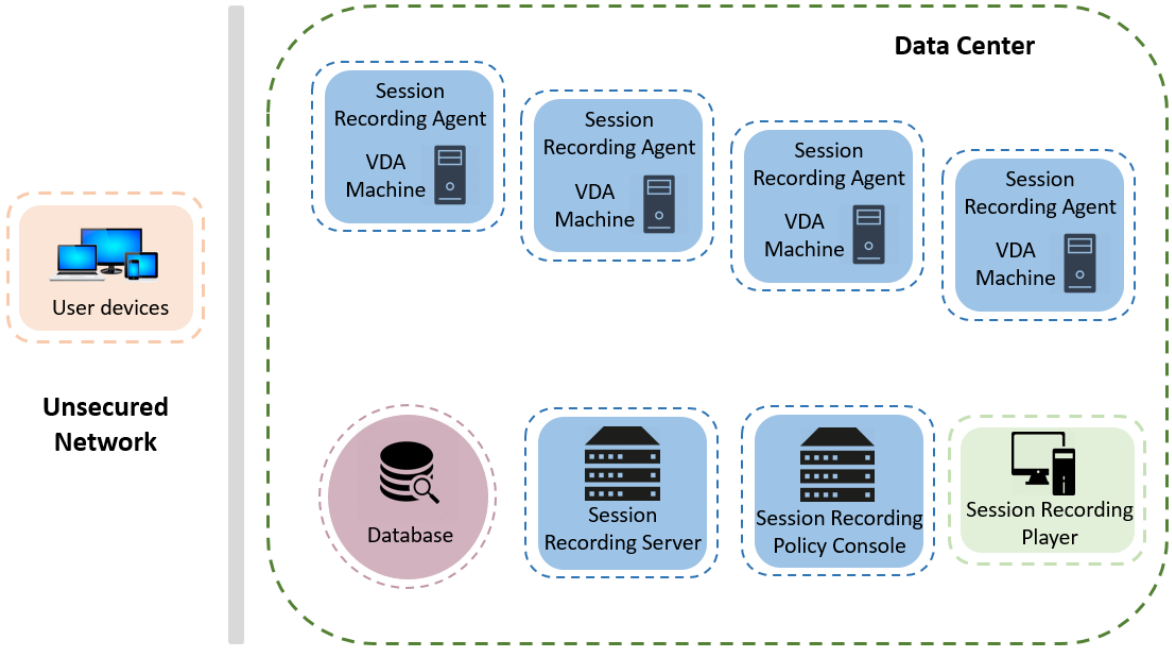
環境に応じ、異なるシナリオに基づいて Session Recording コンポーネントを展開できます。

Session Recording を単一のサイトのみに限って展開するという制限はありません。Session Recording Agent 以外はすべて、サーバーサイトに依存しないコンポーネントです。たとえば、複数のサイトで単一の Session Recording サーバーを使用するように設定できます。

単一の Session Recording サーバーで高いパフォーマンスが要求される場合があります。たとえば、多数のエージェントが関わる大規模なサイトで、多数のセッションや、AutoCAD などのグラフィックを多用するアプリケーションをいくつも録画することを計画している場合などです。パフォーマンスの問題を軽減するために、複数の Session Recording サーバーをインストールし、負荷分散を構成できます。

提案されたサーバーサイトの構成

1 つまたは複数のサイトのセッションを録画する場合は、この構成を使用します。Session Recording Agent はサイト内の各 VDA にインストールされます。サイトはセキュリティファイアウォール内のデータセンターにあります。Session Recording Administration コンポーネントは他のサーバーにインストールされ、Session Recording Player はワークステーションにインストールされます。これらはすべてファイアウォールの背後にあります。



展開に関する重要な注意事項

- Session Recording コンポーネントを有効にして各コンポーネント間で通信できるようにするには、同じドメイン内か、推移的な信頼関係を持つ信頼されているドメイン間にインストールします。ワークグループまた

は外部の信頼関係を持つドメイン間にはインストールできません。

- 映像を処理するアプリケーションであり、サイズの大きな録画を再生するときは多くのメモリが使用されるため、Session Recording Player を公開アプリケーションとしてインストールすることはお勧めしません。
- デフォルトでは、Session Recording は TLS/HTTPS を使用して通信するように設定されます。Session Recording サーバーに証明書をインストールします。ルート認証機関（CA）が Session Recording コンポーネントで信頼されていることを確認します。
- SQL Server を実行しているスタンドアロンサーバー上の Session Recording サーバーの場合、TCP/IP プロトコルを有効にし、SQL Server ブラウザーサービスを実行します。これらの設定はデフォルトでは無効になっていますが、Session Recording サーバーとデータベースとの間で通信を行うために有効にする必要があります。詳しくは、Microsoft 社の記事「SQL Server の TCP/IP ネットワークプロトコルの有効化」と「SQL Server Browser サービス」を参照してください。
- Session Recording の展開を計画するときは、セッション共有の影響を考慮します。公開アプリケーションのセッションを共有すると、Session Recording の公開アプリケーションの録画ポリシー規則と競合する可能性があります。Session Recording では、アクティブなポリシーとユーザーが最初に開いた公開アプリケーションを照合します。ユーザーが最初のアプリケーションを開いた後で、同じセッション上で次のアプリケーションを開くと、最初のアプリケーションに対して有効なポリシーが、次のアプリケーションにも適用されます。たとえば、ポリシーが Microsoft Outlook での操作のみを録画する設定になっている場合、ユーザーが Outlook を開くと録画が始まります。Microsoft Outlook の実行中に公開アプリケーションの Word をユーザーが開くと、Word での操作も録画されます。逆に、アクティブなポリシーが Word での操作を録画する設定になっていない場合、ユーザーが Outlook の前に Word を開くと、Outlook での操作が録画されません。
- Session Recording サーバーを Delivery Controller にインストールすることはできますが、パフォーマンスの問題があるため、この操作はお勧めしません。
- Session Recording ポリシーコンソールを Delivery Controller にインストールできます。
- Session Recording サーバーと Session Recording ポリシーコンソールは同じシステムにインストールできます。
- Session Recording サーバーの NetBIOS 名が 15 文字を超えないようにしてください。Microsoft にはホスト名長に 15 文字の制限があります。
- カスタムイベントログを記録するには、PowerShell 5.1 以降が必要です。PowerShell 4.0 がインストールされている Windows Server 2012 R2 に Session Recording Agent をインストールする場合は、PowerShell をアップグレードします。アップグレードしなかった場合、API 呼び出しが失敗する可能性があります。

セキュリティの推奨事項

February 20, 2024

Session Recording は、セキュアなネットワーク上に展開され管理者によりアクセスされそのことを前提にセキュリティを維持するコンポーネントです。デフォルトの構成はシンプルなシステムです。デジタル署名や暗号化などの

セキュリティ機能はオプションで設定できます。

Session Recording コンポーネント間の通信は、インターネットインフォメーションサービス（IIS）と Microsoft メッセージキュー（MSMQ）を通じて実現されます。IIS により、各 Session Recording コンポーネント間の Web サービスの通信リンクが提供されます。MSMQ は、Session Recording Agent から Session Recording サーバーへセッションの録画データを送信するための、信頼できるデータ伝送メカニズムを提供します。

> 警告：
>
> 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、オペレーティングシステム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。

展開計画を立てるときに、セキュリティに関する次の推奨事項について検討します：

- Microsoft インターネットインフォメーションサービス（IIS）を構成します。

  制限された IIS 構成で Session Recording を構成できます。各 Session Recording サーバーで、IIS マネージャーを開き、IIS アプリケーションプールごとに次のリサイクル制限を設定します：

  - 仮想メモリの制限：値を 4,294,967,295 に設定します。
  - プライベートメモリの制限：値を Session Recording サーバーの物理メモリに設定します。たとえば、物理メモリが 4GB の場合、値を 4,194,304 に設定します。
  - 要求の制限：この設定は指定しないでおくことをお勧めします。または、値を 4,000,000,000 に設定できます。

  > ヒント：
  >
  > 上記の設定にアクセスするには、各アプリケーションプールを強調表示し、［**Actions**］ウィンドウで［**Advanced Settings**］を選択してから、［**Advanced Settings**］ダイアログボックスの［**Recycling**］セクションまでスクロールします。

- 社内ネットワーク、Session Recording、または個々のマシンで各種管理者の役割を適切に分離する。このようにしないと、セキュリティ上の脅威にさらされ、システム機能が影響を受けたり、システムが不正利用されたりする可能性があります。ユーザーやアカウントごとに異なる管理者の役割（ロール）を割り当てることをお勧めします。一般のセッションユーザーに VDA システムの管理者権限を持たせないようにしてください。

  - VDA ローカル管理者の役割を、公開アプリまたはデスクトップのユーザーに付与しないでください。ローカル管理者の役割が必要な場合は、Windows のメカニズムまたはサードパーティ製のソリューションを使用して、Session Recording Agent コンポーネントを保護します。
  - Session Recording データベース管理者と Session Recording ポリシー管理者を別々に割り当てます。
  - VDA 管理者権限を一般的なセッションユーザーに（特にリモート PC アクセスを使用している場合には）割り当てないでください。

  - Session Recording サーバーのローカル管理者アカウントは、厳格に保護する必要があります。
  - Session Recording Player がインストールされたマシンへのアクセスを制御します。ユーザーが Session Recording Player の役割を許可されていない場合、そのユーザーにはどの Session Recording Player マシンのローカル管理者の役割も付与しないようにしてください。匿名アクセスを無効にしてください。
  - Session Recording のストレージサーバーには、物理マシンを使用することをお勧めします。

- Session Recording では、データの機密性にかかわらず、セッショングラフィックスアクティビティが録画されます。特定の状況においては、機密データ（ユーザーの資格情報、プライバシー情報、サードパーティの画面など。ただしこれらに限定されるものではありません）が誤って録画される場合があります。このリスクを回避するには、以下の措置を講じます：

  - 特定のトラブルシューティングの場合を除き、VDA のコアメモリダンプを無効にします。
    コアメモリダンプを無効にするには、以下の手順に従います。

    1. ［マイコンピューター］を右クリックし、［プロパティ］を選択します。
    2. ［詳細設定］タブをクリックし、［起動と回復］の ［設定］をクリックします。
    3. ［デバッグ情報の書き込み］で ［(なし)］を選択します。
       Microsoft の記事（https://support.microsoft.com/en-us/kb/307973）を参照してください。

  - セッションの所有者は、デスクトップセッションが録画されている場合は、オンライン会議と Microsoft Remote Assistance ソフトウェアが録画される可能性があることを出席者に知らせます。
  - ログオン資格情報またはセキュリティ情報が、社内で公開または使用されるすべてのローカルアプリケーションと Web アプリケーションに表示されないようにします。そうしない場合、そのような情報が Session Recording で録画されます。
  - リモート ICA セッションに切り替える前に、機密情報を公開する可能性のあるアプリケーションをすべて閉じます。
  - 公開デスクトップまたは Software as a Service（SaaS）アプリケーションへのアクセスには、自動認証方法（シングルサインオン、スマートカードなど）のみをお勧めします。

- Session Recording は、正常に機能し、セキュリティニーズを満たす上で、特定のハードウェアとハードウェアインフラストラクチャ（社内ネットワークデバイス、オペレーティングシステムなど）に依存しています。インフラストラクチャレベルで対策を講じることでこうしたインフラストラクチャの損傷と不正利用を防ぎ、Session Recording 機能の安全性と信頼性を確保します。

  - Session Recording をサポートするネットワークインフラストラクチャを適切に保護し、利用可能な状態を維持します。
  - サードパーティ製のセキュリティソリューションまたは Windows のメカニズムを使用して、Session Recording コンポーネントを保護することをお勧めします。Session Recording コンポーネントには以下が含まれます：

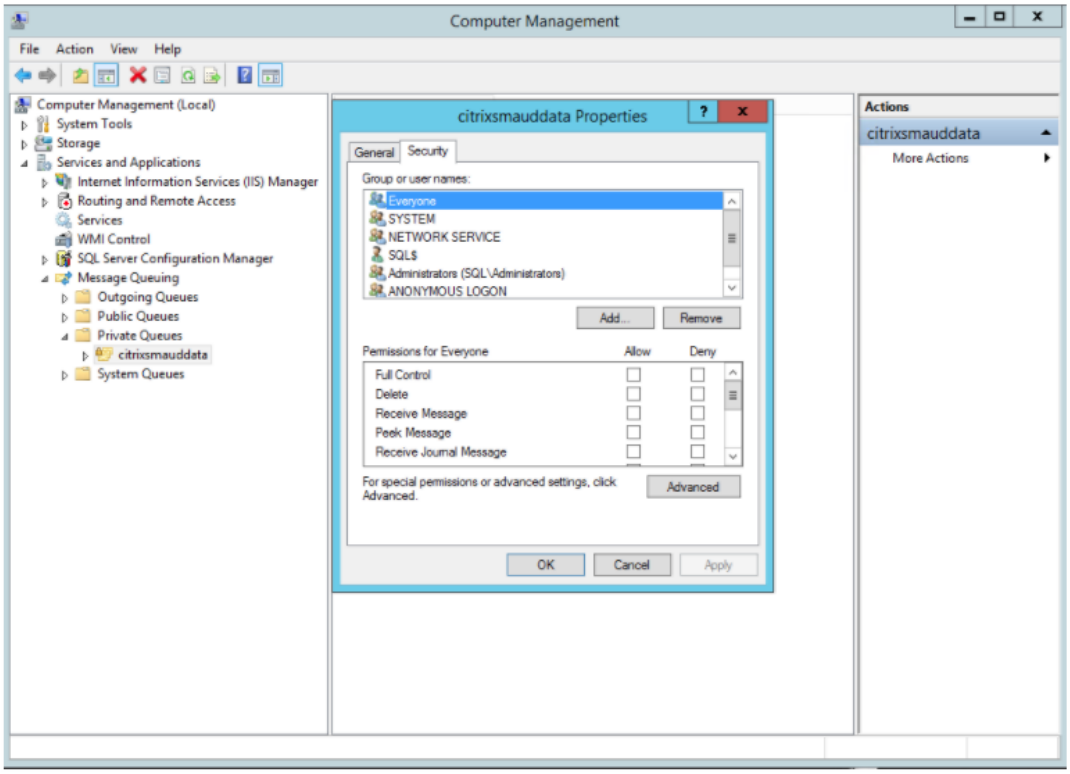
    * Session Recording サーバー上
      - プロセス：SsRecStoragemanager.exe および SsRecAnalyticsService.exe

- サービス：CitrixSsRecStorageManager および CitrixSsRecAnalyticsService
- Session Recording サーバーのインストールフォルダーにあるすべてのファイル
- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server にあるレジストリ値

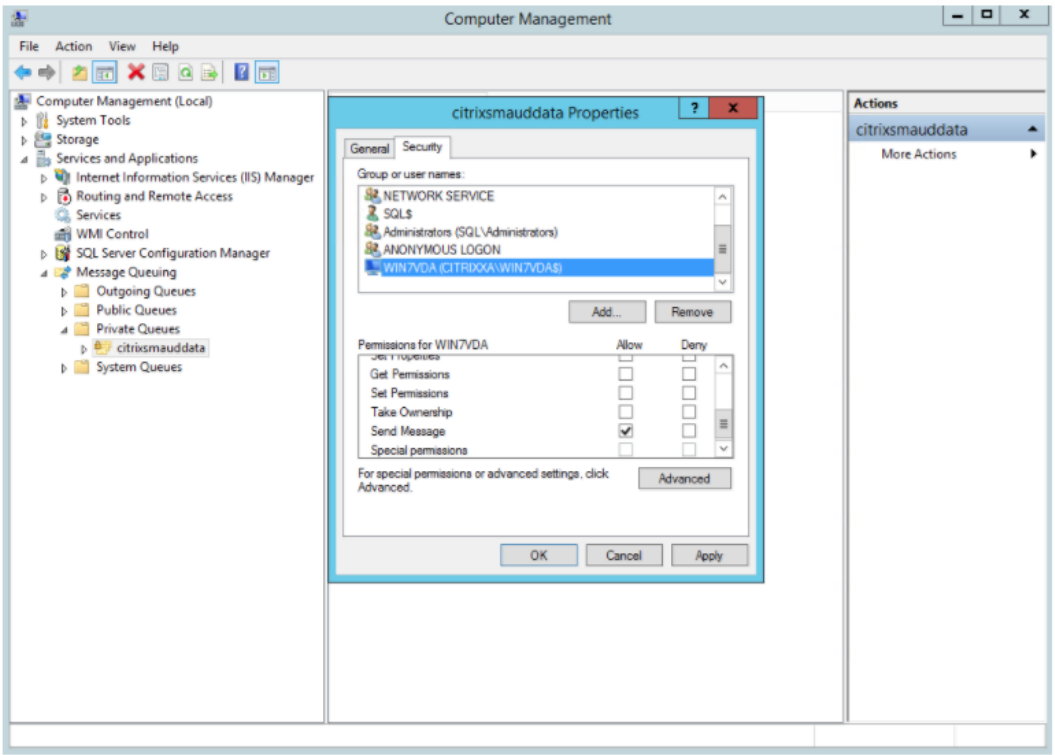
* Session Recording Agent 上
  - プロセス：SsRecAgent.exe
  - サービス：CitrixSmAudAgent
  - Session Recording Agent のインストールフォルダーにあるすべてのファイル
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent下のレジストリ値

- Session Recording サーバーで Message Queuing（MSMQ）のアクセス制御リスト（ACL）を設定することで、MSMQ データを Session Recording サーバーに送信できる VDA または VDI マシンを制限し、許可のないマシンがデータを Session Recording サーバーに送信できないようにします。

  1. 各 Session Recording サーバー、および Session Recording が有効になっている VDA または VDI マシンに、サーバー機能の Directory Service Integration をインストールします。次に Message Queuing サービスを再起動します。
  2. 各 Session Recording サーバーの Windows の ［スタート］メニューから、［管理ツール］ > ［コンピューターの管理］の順に開きます。
  3. ［サービスとアプリケーション］ > ［メッセージキュー］ > ［専用キュー］の順に開きます。
  4. **citrixsmauddata** 専用キューをクリックして ［プロパティ］ページを開き、［セキュリティ］タブをクリックします。



5. MSMQ データをこのサーバーに送信する VDA のコンピューターまたはセキュリティグループを追加し、メッセージを送信する権限を付与します。



- Session Recording サーバーと Session Recording Agent のイベントログを適切に保護する。Windows

またはサードパーティ製のリモートログソリューションを使用してイベントログを保護するか、イベントログをリモートサーバーにリダイレクトすることが推奨されます。

- Session Recording コンポーネントが動作するサーバーを物理的に保護する。可能であれば、権限を持つ人のみが入室できる安全なサーバー室にコンピューターを設置します。
- Session Recording コンポーネントが動作するサーバーを別のサブネットまたはドメインに分離する。
- Session Recording サーバーとほかのサーバーの間にファイアウォールを設置し、ほかのサーバーにアクセスするユーザーからセッションの録画データを保護する。
- Microsoft からの最新のセキュリティアップデートにより、Session Recording Administration サーバーおよび SQL データベースを最新に保ちます。
- 管理者以外の人が管理マシンにログオンできないように制限する。
- 録画ポリシーの変更およびセッションの録画ファイルの表示を行う権限を持つユーザーを厳しく制限する。
- デジタル証明書をインストールし、Session Recording のファイル署名機能を使用し、IIS で TLS 通信をセットアップする。
- MSMQ の通信で HTTPS が使用されるように設定する。そのためには、[**Session Recording Agent** のプロパティ] に表示される MSMQ プロトコルを HTTPS に設定します。詳しくは、「MSMQ のトラブルシューティング」を参照してください。
- TLS 1.1 または TLS 1.2（推奨）を使い SSLv2、SSLv3、および TLS 1.0 を Session Recording サーバーと Session Recording データベースで無効にします。
- Session Recording サーバーと Session Recording データベースで、TLS 用の RC4 暗号スイートを無効にします:

  1. Microsoft のグループポリシーエディターを使用して、[コンピューターの構成] **>** [管理用テンプレート] **>** [ネットワーク] **>** [**SSL** 構成設定] に移動します。
  2. [**SSL** 暗号の順位] ポリシーを [有効] に設定します。デフォルトでは、このポリシーは [未構成] に設定されています。
  3. RC4 暗号スイートをすべて削除します。

- 再生データの保護機能を使用する。再生データの保護は Session Recording の機能の 1 つで、これにより、Session Recording Player にダウンロードされる前に、セッションの録画ファイルが暗号化されます。このオプションは [**Session Recording** サーバーのプロパティ] にあり、デフォルトで有効に設定されます。
- 暗号化キー長および暗号化アルゴリズムの NSIT ガイダンスに従います。
- TLS 1.2 の Session Recording サポートを構成します。

  Session Recording コンポーネントのエンドツーエンドセキュリティを確実にするためには、通信プロトコルとして TLS 1.2 を使用されることをお勧めします。

  TLS 1.2 の **Session Recording** サポートを構成するには:

1. Session Recording サーバーをホストするマシンにログオンします。適切な SQL Server クライアントコンポーネントとドライバーをインストールし、.NET Framework（バージョン 4 以降）に対して強固な暗号を設定します。
   a) Microsoft ODBC Driver for SQL Server バージョン 11 以降をインストールします。
   b) .NET Frameworkの最新のホットフィックスロールアップを適用します。
   c) 使用している.NET フレームワークのバージョンに基づいてADO.NET - SqlClientをインストールします。詳しくは、https://support.microsoft.com/en-us/kb/3135244を参照してください。
   d) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NetFramework\v4.0.30319 および HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319 の下に、DWORD 値 SchUseStrongCrypto=1 を追加します。
   e) マシンを再起動してください。
2. Session Recording ポリシーコンソールをホストするマシンにログオンします。.NET Framework の最新のホットフィックスロールアップを適用し、.NET Framework（バージョン 4 以上）に対して強固な暗号を設定します。強固な暗号を設定する方法は、下位手順 1-4 および 1-5 と同じです。Session Recording サーバーと同じコンピューターで Session Recording ポリシーコンソールをインストールするように選択している場合は、これらの手順を実行する必要はありません。

2016 より前のバージョンの SQL Server に対する TLS 1.2 サポートを構成するには、https://support.microsoft.com/en-us/kb/3135244を参照してください。TLS 1.2 を使用するには、HTTPS を、Session Recording コンポーネントのための通信プロトコルとして構成します。

スケーラビリティに関する注意事項

February 20, 2024

Session Recording は、数千の、または数万のセッションを処理する高スケーラブルなシステムです。Session Recording のインストールと実行のために、Citrix Virtual Apps and Desktops または Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）の実行に必要なハードウェア要件を超えて、さらにリソースを追加する必要はほとんどありません。ただし、多くのセッションを録画する場合は、システムのパフォーマンスを考慮することをお勧めします。または、録画する予定のセッションによって、セッションファイルが大きくなることがあります（たとえば、グラフィックを多用するアプリケーション）。

ここでは、Session Recording によって高いスケーラビリティを実現し、最低限のコストで録画システムを最大限に活用できる方法について説明します。

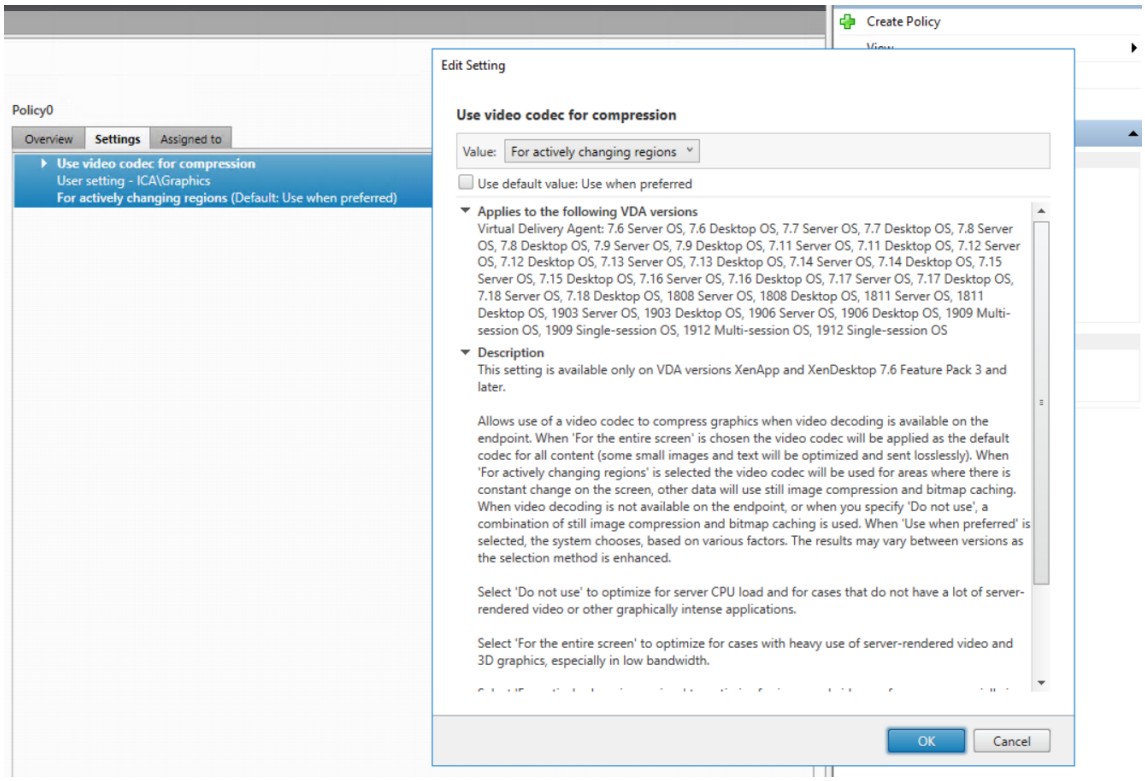
Session Recording のスケーラビリティが高い理由

Session Recording が同様の他社製品と比べて高いスケーラビリティを提供できるのには、主に 2 つの理由があります:

- 小さなファイルサイズ

  Session Recording で作成されたセッションの録画ファイルは比較的小さなサイズです。スクリーンスクレイピングによるソリューションで作成された同様のビデオ録画に比べると、けた外れに小さなサイズです。セッションの録画ファイルを転送/格納するのに必要なネットワーク帯域幅、ディスクスペース、ディスク IOPS は通常、同様のビデオファイルの 10 分の 1 以下です。

  セッションの録画ファイルのサイズが小さいと、ビデオフレームのレンダリングもより高速かつスムースになります。また、録画は無損失で、大半の小さなサイズのビデオ形式で発生しがちな表示の滑らかさの問題もありません。録画の中のテキストは、再生中でも元のセッションと同じくらい読み取りやすい状態です。ファイルサイズの小ささを維持するために、Session Recording はファイル内でキーフレームを録画しません。Session Recording では、ビデオを実行するセッションの録画中に H.264 パッケージをドロップできるため、録画ファイルのサイズを小さくすることができます。この機能を使用するには、Session Recording Agent で`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\DropH264Enabled`を1に設定し、[圧縮にビデオコーデックを使用する] の値を ［領域をアクティブに変更］ に設定します。



- ファイルの生成に必要な処理が少ない

  セッションの録画ファイルには、実質的には本来の形式で抽出されたセッションの ICA プロトコルデータが含

まれます。ファイルは Citrix Workspace アプリと通信していた ICA プロトコルデータストリームをキャプチャします。リアルタイムでデータを変換するために高価なトランスコードやエンコード用のソフトウェアコンポーネントを実行する必要はありません。VDA のスケーラビリティでは、処理の量を抑えることも重要です。これによって、同じ VDA から多くのセッションが録画された場合でも、エンドユーザーエクスペリエンスが維持されます。

また、再生が可能な ICA 仮想チャネルのみが録画されるため、さらに最適化が促進されます。たとえば、プリンターとクライアントドライブマッピングのチャネルは録画されません。これらのチャネルは、ビデオの再生に何のメリットもなく、大量のデータを生成する可能性があります。

データの入力速度および処理速度の推定

Session Recording サーバーは、セッションの録画ファイルを一元的に収集する場所です。マルチセッション OS VDA を実行している各マシンで Session Recording を有効にすると、セッションの録画データを Session Recording サーバーに送信します。Session Recording は、大量のデータを処理でき、バーストや障害に対応できます。ただし、1 つのサーバーが処理できるデータ量には物理的な限界があります。

各 Session Recording サーバーに送信するデータ量について検討してください。サーバーがデータを処理および保存できる速度を見積もります。受信データを格納する速度がデータ入力速度より高速である必要があります。

データ入力速度を見積もるには、次の計算を行います:

1. 録画されたセッションの数に平均セッションサイズを掛けます。
2. その計算結果を、セッションを録画する時間で割ります。

たとえば、5,000 件の Microsoft Outlook のセッションの平均サイズが 20MB として、毎営業日に 8 時間録画するとします。この場合、データの入力速度は約 3.5Mbps です（5,000 セッション ×20MB÷8 時間 ÷3,600 秒）。通常、100Mbps LAN に接続され、録画済みデータを格納する十分なディスクスペースがある Session Recording サーバーは、データを約 5.0Mbps で処理できます。この速度は、ディスクおよびネットワーク IOPS による物理的な制限に基づく処理速度です。この例では、処理速度（5.0Mbps）は入力速度（3.5Mbps）より高い値であるため、5,000 件の Outlook セッションを録画することが可能です。

セッションあたりのデータ量は、録画内容によって大きく異なります。画面の解像度、色深度、グラフィックモードなどの他の要素も影響します。CAD が実行されているセッションでは、ユーザーが Outlook でメールを送受信するセッションよりも、大幅に大きなサイズの録画データが生成されることが予想できます。したがって、同じ数でも CAD セッションは高い入力速度を必要とし、Session Recording サーバーの使用率も高くなります。

バーストや障害

前述の例では、シンプルで均一なデータのスループットを想定しましたが、短い時間に高いアクティビティが発生するバーストといわれる状態をシステムが処理する方法については、また異なります。バーストは、すべてのユーザーが朝の同じ時間に一斉にログオンするとき（9 時台のラッシュ）に発生する可能性があります。また、Outlook

の受信トレイで同じ電子メールを一度に受信した場合にも発生する可能性があります。このような急激な需要には、Session Recording サーバーの 5.0Mbps という処理速度では対応が不十分になります。

各 VDA で実行されている Session Recording Agent は、Microsoft メッセージキュー（MSMQ）を使用して録画済みデータを Session Recording サーバーに送信します。データは、ストアアンドフォワード方式で送信されます。これは、メールが送信者、メールサーバー、受信者との間で送受信される方法と似たような方式です。Session Recording サーバーやネットワークがバースト時の大量のデータを処理できない場合、録画データは一時的に保存されます。ネットワークが混雑している場合、データメッセージは VDA の送信キューに一時的に保存されることがあります。もう 1 つのケースは、データがネットワークを通過したが、ストレージマネージャーが他のメッセージの処理でビジー状態である場合です。この場合、データメッセージは Session Recording サーバーの受信キューに保存されます。

MSMQ はフォールトトレランスメカニズムとしても機能します。Session Recording サーバーがダウンするかリンクが破損している場合、録画済みデータは各 VDA の発信キューにとどまります。障害が解消されると、キューのすべてのデータが一度に送信されます。MSMQ により、セッション録画を中断したりデータを失ったりすることなく、サーバーをオフラインでアップグレードやメンテナンスすることもできます。

MSMQ の主な制限は、データメッセージの一時ストレージとしてのディスクスペースが限られていることです。この制限のため、バースト、障害、またはメンテナンスイベントが長引く場合、最終的にデータが失われることがあります。データ損失後も総合的なシステムは機能し続けますが、この状況では個別の録画内でデータの一部が失われます。データが失われたファイルは再生可能ですが、最初に失われたデータの箇所まで進むと再生が停止します。以下の点に注意してください：

- 各サーバー、特に Session Recording サーバーにディスクスペースを追加して MSMQ で使用できるようにすると、バーストや障害時の許容値が上昇します。
- 各 Session Recording Agent でメッセージの有効期間を適切なレベルに設定することが重要です（[Session Recording Agent のプロパティ］の ［接続］タブ）。デフォルト値は、7,200 秒（2 時間）です。つまり、記録された各データメッセージは、ストレージマネージャーに到達するまでに 2 時間かかり、その後、ストレージマネージャーがそのメッセージを破棄して録画ファイルに損傷を与えます。利用可能なディスクスペースが増えると（または録画するセッションを削減すると）、この値を増やすことを選択できます。最大値は 365 日です。

MSMQ のその他の制限は、データのバックログが作成されると、データメッセージの読み取りと書き込みのために追加のディスク IOPS が発生するということです。通常、ストレージマネージャーはネットワークから直接データを受信して処理し、データメッセージがディスクに書き込まれることはありません。データを格納するためには、セッションの録画ファイルを追加するためにディスクへの一度の書き込み操作が必要になります。データのバックログが作成された場合、ディスク IOPS が 3 倍になります。これは、各メッセージがディスクに書き込まれ、ディスクから読み取られ、ファイルに書き込まれる必要があるためです。ストレージマネージャーは IOPS に大幅に影響を受けるため、Session Recording サーバーの処理速度はメッセージのバックログが消去されるまで低下します。この追加の IOPS の影響を緩和するため、以下の推奨事項を採用します：

- MSMQ がメッセージを格納するディスクは、録画ファイル格納フォルダーとは異なるディスクを使用してください。IOPS バストラフィックが 3 倍になっても、実際の処理率の低下は深刻なものにはなりません。

- 停止はピーク時以外にだけ計画します。予算の制限によっては、高可用性サーバーの構築で実証済みのアプローチを使用します。このアプローチには、無停電電源装置（UPS）、デュアル NIC、冗長化されたスイッチ、ホットスワップ可能なメモリとディスクの使用が含まれます。

処理能力を重視した設計

セッションの録画データが均一であることは少なく、バーストや障害が発生する可能性があり、メッセージのバックログの消去は IOPS を増加させます。このため、各 Session Recording サーバーは処理能力に余裕をもって設計します。後のセクションで説明するように、サーバーを追加するか既存のサーバーの仕様を改善することで、より多くの処理能力を獲得できます。一般的な目安は、各 Session Recording サーバーを合計処理能力の最大 50% で実行することです。前述の例のように、サーバーが 5.0Mbps で処理することができる場合、システムは 2.5 Mbps で実行することを目標にします。1 つの Session Recording サーバーで 5,000 件の Outlook セッションの録画では 3.5Mbps ですが、3,500 件のセッションに抑えると約 2.5Mbps になります。

バックログとライブ再生

ライブ再生とは、セッションがアクティブなときに閲覧者がセッションの録画を開いて再生することです。ライブ再生中に、Session Recording Agent がそのセッションのストリーミングモードに切り替わります。録画データは、内部バッファリングなしで、すぐにストレージマネージャーに送信されます。録画ファイルは常に更新され、Player は引き続きライブセッションからの最新データを取得します。Agent からストレージマネージャーに送信されたデータは MSMQ を経由し、前述のキューの規則が適用されます。このシナリオでは、問題が発生する可能性があります。MSMQ のバックログが作成されると、ライブ再生で利用可能な新しい録画データは、他のすべてのデータメッセージのようにキューに登録されます。閲覧者がファイルを再生することはできますが、ライブで録画された最新のデータの閲覧には遅延が発生します。ライブ再生が閲覧者にとって重要な機能である場合は、バックログの確率が低くなるように設計してください。環境で処理能力やフォールトトレランスを設計できます。

システムのスケーラビリティ

Session Recording がセッションのパフォーマンスを低下させたり、録画済みデータのバックログへの応答でセッションを停止させたりすることは決してありません。エンドユーザーエクスペリエンスや単一サーバーのスケーラビリティを維持することが、Session Recording システムの設計において何よりも優先されます。録画システムが不可逆的に過負荷になった場合、録画されたセッションのデータは破棄されます。ICA セッションの録画が VDA のパフォーマンスとスケーラビリティに与える影響は大きくありません。影響の大きさは、プラットフォーム、利用可能なメモリ、録画されたセッションの画像の性質によって異なります。以下の構成では、単一サーバーのスケーラビリティへの影響は 1 ～ 5% 程度と予想されます。つまり、Session Recording をインストールしない場合に 100 ユーザーをホストできるサーバーの場合、インストール後は 95～99 人のユーザーをホストすることができます:

- マルチセッション OS VDA を実行している 8GB RAM の 64 ビットサーバー
- Office 業務アプリケーション（Outlook や Excel）を実行しているすべてのセッション

- アプリケーションの使用が可能で維持される
- すべてのセッションが Session Recording ポリシーの構成に従って録画される

録画されているセッションの数が少ないか、維持されるセッションアクティビティが少なく散発的であれば、影響は大きくありません。多くの場合、スケーラビリティへの影響は無視できる範囲で、サーバーあたりのユーザー密度に変化はありません。前述したように、影響が少ないのは各 VDA の Session Recording コンポーネントの処理要件がシンプルであるためです。録画済みのデータは、ICA セッションスタックから抽出され、そのまま MSMQ 経由で Session Recording サーバーに送信されます。コストがかかるデータのエンコードは発生しません。

セッションが録画されていない場合でも、Session Recording の使用には多少のオーバーヘッドが発生します。特定のサーバーからのセッションを録画しない場合は、そのサーバーでの録画を無効にすることができます。Session Recording を削除する方法もあります。より影響の少ないアプローチは、［**Session Recording Agent** のプロパティ］の ［**Session Recording**］タブで ［この **VDA** マシンでセッションを録画する］チェックボックスをオフにすることです。あとからセッションの録画が必要になった場合、このチェックボックスを再度オンにします。

スループットの測定

セッションの録画データを VDA から送信して Session Recording サーバーで受信する場合のスループットを測定できます。録画ファイルのサイズ、および Session Recording サーバーでディスクスペースが消費される速度を測定するのが、シンプルで効果的なアプローチです。ディスクに書き込まれるデータの量は、生成されるネットワークトラフィックの量をほぼ反映しています。Session Recording で提供されるカウンターに加えて、Windows パフォーマンスモニターツール（perfmon.exe）には、監視可能な標準システムカウンターがあります。カウンターは、スループットの測定だけでなく、ボトルネックやシステムの問題を特定するために使用できます。次の表では、最も有用なパフォーマンスカウンターの一部をまとめました。

パフォーマンスオブジェクト	カウンター名	説明
Citrix Session Recording Agent	`Active Recording Count`	現在、特定の VDA に録画されているセッションの数。
Citrix Session Recording Agent	`Bytes read from the Session Recording Driver`	セッションデータ取得に必要なカーネルコンポーネントからの読み取りバイト数です。そのサーバーで録画されているすべてのセッションで単一 VDA が生成するデータ量を決定するために役立ちます。
Citrix Session Recording ストレージマネージャー	`Active Recording Count`	Session Recording サーバーを除いては Citrix Session Recording Agent のカウンターと同様です。現在、すべてのサーバーで録画されているセッションの合計数を示します。

パフォーマンスオブジェクト	カウンター名	説明
Citrix Session Recording ストレージマネージャー	Message bytes/sec	すべての録画されたセッションのスループット。ストレージマネージャーがデータを処理する速度を決定するために使用できます。MSMQ でメッセージのバックログが作成されている場合は、ストレージマネージャーはフルスピードで動作します。この値は、ストレージマネージャーの最大処理速度を示すために使用することができます。
LogicalDisk	Disk Write Bytes/sec	ディスクのライトスループットを測定するために使用できます。これは、Session Recording サーバーの高スケーラビリティを実現するために重要です。個々のドライブのパフォーマンスも測定することができます。
MSMQ キュー	Bytes in Queue	CitrixSmAudData メッセージキュー内でバックログが作成されたデータの量を決定するために使用できます。時間の経過とともにこの値が増加した場合、ネットワークから録画データを受信する速度は、ストレージマネージャーがデータを処理できる速度よりも大きくなります。このカウンターは、データバーストや障害の影響を測定するために有用です。
MSMQ キュー	Message in Queue	キュー内のバイト数カウンターとほぼ同じですが、メッセージの数を測定します。

パフォーマンスオブジェクト	カウンター名	説明
ネットワークインターフェイス	Bytes Total/sec	リンクの両側で、セッションの録画時に生成されるデータの量を測定するために使用できます。Session Recording サーバーで測定すると、このカウンターは受信データを受け取る速度を示します。データの処理速度を測定する Citrix Session Recording ストレージマネージャーのMessage bytes/secカウンターとは、対照的なカウンターです。ネットワークの速度がこの値よりも大きい場合は、メッセージがメッセージキューに構築されます。
プロセッサ	% Processor Time	CPU がボトルネックになる可能性が低い場合でも、この値を監視することは役に立ちます。

Session Recording サーバーのハードウェア

Session Recording サーバーのハードウェアを慎重に選択することで、展開の処理能力を拡大できます。選択肢は、スケールアップ（各サーバーの処理能力を増やす）かスケールアウト（さらにサーバーを追加する）の 2 つです。最低限のコストでスケーラビリティを増やすことを念頭に、どちらかを選択します。

スケールアップ

単一の Session Recording サーバーの場合、予算内で最適なパフォーマンスを確保する次のベストプラクティスを検討してください。このシステムは、ネットワークからディスクへ、録画済みデータの高スループットを確保できる IOPS に依存します。そのため、適切なネットワークやディスクのハードウェアに投資することが重要です。高いパフォーマンスの Session Recording サーバーの場合、デュアル CPU またはデュアルコア CPU をお勧めしますが、これを超える仕様にしてもさほどパフォーマンスは上昇しません。64 ビットプロセッサをお勧めしますが、x86 プロセッサでも問題ありません。4GB の RAM をお勧めしますが、これを超える仕様にしてもパフォーマンスに大幅な変化はありません。

スケールアウト

スケールアップのベストプラクティスを使用しても、多くのセッションを録画する場合、1 つの Session Recording サーバーではパフォーマンスとスケーラビリティに限度があります。負荷に対応するために、追加のサーバーが必要

な場合があります。複数の Session Recording サーバーを異なるマシンにインストールすることで、負荷分散プールとして機能させることができます。このタイプの展開では、Session Recording サーバーはストレージとデータベースを共有します。負荷を分散するには、Session Recording Agent を負荷分散を担当するロードバランサーに割り当てます。

ネットワークの性能

Session Recording サーバーに接続するには 100Mbps のネットワークリンクが適しています。ギガビットイーサネット接続ではパフォーマンスが向上するかもしれませんが、100Mbps のリンクの 10 倍のパフォーマンスが得られるわけではありません。実際には、スループットの増加量は低下します。

Session Recording で使用するネットワークスイッチを、使用できるネットワーク帯域幅を求めて競合する可能性のあるサードパーティ製のアプリケーションと共有しないようにします。Session Recording サーバー専用のネットワークスイッチを用意することが理想的です。ネットワークの混雑がボトルネックであると判明した場合、ネットワークのアップグレードはシステムのスケーラビリティを向上させるうえで比較的安価な方法です。

ストレージ

ディスクとストレージハードウェアへの投資は、サーバーのスケーラビリティにおいて単独で最も重要な要因です。ディスクへのデータの書き込み速度が速いほど、システム全体のパフォーマンスが向上します。ストレージソリューションを選択する場合、読み取りパフォーマンスよりも書き込みパフォーマンスに重点を置いてください。

RAID または SAN にデータを保存します。

> 注:
>
> SMB や NFS などのファイルベースのプロトコルで NAS にデータを格納すると、パフォーマンスとセキュリティ上の問題が発生する可能性があります。最新バージョンのプロトコルを使用してセキュリティ上の問題を回避し、スケールテストを実行して適切なパフォーマンスを確保します。

ローカルドライブを使用する場合、キャッシュメモリが組み込まれたディスクコントローラーを検討してください。キャッシュによって、コントローラーはライトバック中に昇順に並べ替えることができます。これにより、ディスクヘッドの動きを最小限にとどめ、物理ディスクの操作が完了するのを待たずに書き込み操作を完了できます。このため、最小限の追加コストで大幅に書き込みパフォーマンスを向上させることができます。ただしキャッシュを使用する場合、停電時にデータ損失が発生する問題を検討する必要もあります。データとファイルシステムの整合性を確保するために、キャッシュ機能付きディスクコントローラーにバッテリーバックアップ機能を使用することを検討してください。

適切な RAID ストレージソリューションを使用するようにしてください。パフォーマンスと冗長性の要件に対応した、多くの RAID レベルがあります。次の表は、各 RAID レベルと各標準が Session Recording にどのように適用されるかを示します。

RAID レベル	種類	最小ディスク数	説明
RAID 0	パリティなしのストライピング設定	2	冗長性なしの高いパフォーマンスを提供します。いずれかのディスクが失われるとアレイが破損します。RAID 0 は、セッションの録画ファイルを格納する低コストソリューションであり、データ損失の影響も抑えられます。さらにディスクを追加することで、簡単にパフォーマンスをスケールアップできます。
RAID 1	パリティなしのミラーリング設定	2	1 つのディスクではパフォーマンスの向上が見られず、比較的コストの高いソリューションです。高いレベルの冗長性が必要な場合にのみ、このソリューションを使用します。
RAID 3	専用パリティありのストライピング設定	3	RAID 5 に類似した冗長性傾向で、高い書き込みパフォーマンスを提供します。RAID 3 は、ビデオ制作やライブストリーミングアプリケーションで推奨されます。Session Recording は、この種類のアプリケーションであるため、RAID 3 が最も推奨されますが、一般的な選択肢ではありません。

RAID レベル	種類	最小ディスク数	説明
RAID 5	分散パリティありのストライピング設定	3	冗長性のある高い読み取りパフォーマンスを提供しますが、書き込み速度が遅くなります。RAID 5 は、汎用用途で最も一般的です。ただし書き込みパフォーマンスが遅いため、Session Recording には推奨されません。RAID 3 は、同程度のコストかつ良好なパフォーマンスで展開できます。
RAID 10	ミラーリング設定とストライピング設定	4	RAID 0 のパフォーマンス特性と RAID 1 の冗長性のメリットを提供します。コストの高いソリューションで、Session Recording には推奨されません。

RAID 0 と RAID 3 が、最も推奨される RAID レベルです。RAID 1 と RAID 5 は一般的な標準ですが、Session Recording には推奨されません。RAID 10 は、パフォーマンス上のいくつかのメリットを提供していますが、コストパフォーマンスは低くなります。

ディスクドライブの種類や仕様を決定します。IDE/ATA ドライブや外付け USB または FireWire ドライブは、Session Recording での使用に適していません。主な選択肢は、SATA か SCSI です。SATA ドライブは SCSI ドライブと比較して、MB 単位のコストが抑えられた十分高い転送速度を提供します。ただし、SCSI ドライブはより優れたパフォーマンスを提供し、サーバー展開でより一般的です。サーバー RAID ソリューションは、主に SCSI ドライブをサポートしますが、一部の SATA RAID 製品も利用可能になりました。ディスクドライブ製品の仕様を評価する場合、ディスクの回転速度および他のパフォーマンス特性を考慮してください。

一日あたり数千のセッションの録画は、相当量のディスクスペースを消費する可能性があるため、総合的な処理能力とパフォーマンスのどちらかを選択する必要があります。前述の例では、毎営業日に 8 時間、5,000 件の Outlook セッションを録画すると、約 100GB の記憶域を消費します。10 日間の録画（50,000 件のセッションの録画ファイル）を格納するには、1,000GB（1TB）が必要です。ディスクスペースに対するこうしたプレッシャーは、古い録画をアーカイブまたは削除する前の保有期間を短縮することで緩和できます。1TB のディスクスペースが利用でき、7 日間の保有期間が適切な場合、ディスクスペースの使用は約 700GB 程度にして、300GB は多忙な日のバッファとして確保します。Session Recording では、ファイルのアーカイブや削除が ICLDB ユーティリティでサポートされています。最短保有期間は 2 日間です。バックグラウンドタスクをスケジュール設定して、ピーク時以外に 1 日に 1 回

実行できます。**ICLDB** コマンドおよびアーカイブについて詳しくは、「データベースレコードの管理」を参照してください。

ローカルドライブやコントローラーを使用する代わりに、ブロックレベルのディスクアクセスベースの SAN ストレージソリューションを使用できます。Session Recording サーバーには、ディスクアレイはローカルドライブとして表示されます。SAN はセットアップにコストがかかりますが、ディスクアレイが共有されると、管理が簡易化され一元化されというメリットがあります。SAN には、ファイバチャネルと iSCSI という 2 つの主な種類があります。iSCSI は基本的に TCP/IP を介した SCSI で、ギガビットイーサネットの導入以来ファイバチャネルよりも一般的になっています。

データベースのスケーラビリティ

Session Recording データベースには録画されたセッションのメタデータのみが格納されるため、このデータベースに送信されるデータ量は少なくなります。セッションの録画ファイル自体は別のディスクに書き込まれます。Session Recording イベント API を使用してセッションに検索可能なイベントを挿入するのでなければ、セッション録画 1 件につきデータベースに必要な容量は通常 1KB のみです。

Microsoft SQL Server 2019、Microsoft SQL Server 2017、Microsoft SQL Server 2016、Microsoft SQL Server 2014、Microsoft SQL Server 2012、および Microsoft SQL Server 2008 R2 の Express Edition では、データベースサイズの上限は 10GB です。1 件のセッション録画あたり 1KB のデータが書き込まれるとすれば、この制限があっても、4 百万件のセッションをデータベースでカタログ化できます。Microsoft SQL Server のほかのエディションではデータベースサイズの制限はなく、使用できるディスク容量によってのみ上限が決定されます。データベース内のセッション数が増加するにつれて、データベースのパフォーマンスと検索速度はごくわずかに低下します。

Session Recording イベント APIによるカスタマイズを行わない場合は、録画セッションそれぞれについて、録画開始時に 2 件、ユーザーがセッションにログオンするときに 1 件、および録画終了時に 1 件の、合わせて 4 件のデータベーストランザクションが生成されます。Session Recording イベント API を使用してセッションをカスタマイズする場合は、検索可能な録画イベントそれぞれについて 1 件のトランザクションが生成されます。最も基本的な方式で展開したデータベースで、1 秒あたり何百件というトランザクションを制御できるため、データベースの処理負荷が高くなる可能性はほとんどありません。影響が十分に小さいため、Citrix Virtual Apps and Desktops のデータストアデータベースを含めたほかのデータベースと同じ SQL Server で、Session Recording データベースを実行できます。

Session Recording のデータベースで何百万というセッション録画をカタログ化する必要がある場合は、SQL Server のスケーラビリティに関する Microsoft 社のガイドラインに従います。

インストール、アップグレード、およびアンインストール

February 20, 2024

> 注:
>
> 負荷分散によりサーバーの高可用性を構成する方法については、「既存の環境での負荷分散の構成」および「Azure での Session Recording の展開と負荷分散」を参照してください。

この記事は、次のセクションで構成されています。

- インストールチェックリスト
- Citrix スクリプトを使用した Windows の役割と機能の前提条件のインストール
- Session Recording Administration コンポーネントのインストール
  - Session Recording データベースのインストール
  - Session Recording サーバーのインストール
- Session Recording Agent のインストール
- Session Recording Player と Web Player のインストール
- インストールの自動化
- Session Recording のアップグレード
- Session Recording のアンインストール
- Citrix Analytics for Security との統合

インストールチェックリスト

次のファイルを使用して、Session Recording コンポーネントをインストールします:

- `Broker_PowerShellSnapIn_x64.msi`
- `SessionRecordingAdministrationx64.msi`
- `SessionRecordingAgentx64.msi`
- `SessionRecordingPlayer.msi`
- `SessionRecordingWebPlayer.msi`

インストールを始める前に、以下のリストに記載されている作業を行います:

☒	手順
	インストールを開始する前に、前提条件をインストールします。「システム要件」および「Citrix スクリプトを使用した Windows の役割と機能の前提条件のインストール」を参照してください。 Session Recording の各コンポーネントをインストールするマシンを選択します。各マシンがインストールするコンポーネントのハードウェアおよびソフトウェアの要件を満たしていることを確認してください。 Citrix アカウント資格情報を使用して、Citrix Virtual Apps and Desktops のダウンロードページにアクセスして、製品ファイルをダウンロードします。ファイルを解凍します。 Session Recording コンポーネント間の通信に TLS プロトコルを使用するには、正しい証明書を環境にインストールします。 Session Recording コンポーネントに必要な Hotfix をインストールします。Hotfix はCitrix サポートから入手できます。 Director を構成して、Session Recording ポリシーを作成およびアクティブ化します。詳しくは、「Director を構成して Session Recording サーバーを使用する」を参照してください。

注:

- 録画ポリシーに基づいて、公開アプリケーションを個別のデリバリーグループに分割することをお勧めします。公開アプリケーションのセッション共有は、同じデリバリーグループ内のアクティブなポリシーと競合する可能性があります。Session Recording では、アクティブなポリシーとユーザーが最初に開いた公開アプリケーションを照合します。バージョン 7.18 リリース以降、動的なセッションの録画機能を使用して、セッション中いつでもセッションの録画を開始または停止できます。詳しくは、「動的なセッションの録画」を参照してください。
- Machine Creation Services（MCS）または Citrix Provisioning を使用する計画がある場合は、一意な`QMId`を準備します。この手順の実行に失敗すると、録画データが損失する可能性があります。
- SQL Server では TCP/IP を有効にする必要があり、SQL Server Browser サービスが実行中で、また Windows 認証の使用が必要です。
- HTTPS を使用するには、TLS/HTTPS のサーバー証明書を構成します。
- `Local Users and Groups > Groups > Users`のユーザーが`C:\windows\Temp`

> フォルダーへの書き込み権限があることを確認してください。

Citrix スクリプトを使用した Windows の役割と機能の前提条件のインストール

以下の Citrix スクリプトを使用して、Session Recording が正しく動作するために必要な Windows の役割および機能の前提条件をインストールしてから
Session Recording をインストールします:

- InstallPrereqsforSessionRecordingAdministration.ps1

```
<#
.Synopsis
    Installs Prereqs for Session Recording Administration
.Description
    Supports Windows Server 2022, Windows Server 2019 and Windows
        Server 2016.
    Install below windows feature on this machine:
    -Application Development
    -Security - Windows Authentication
    -Management Tools - IIS 6 Management Compatibility
        IIS 6 Metabase Compatibility
        IIS 6 WMI Compatibility
        IIS 6 Scripting Tools
        IIS 6 Management Console
    -Microsoft Message Queuing (MSMQ), with Active Directory
       integration disabled, and MSMQ HTTP support enabled.
#>
function AddFeatures($featurename)
{

    try
    {

        $feature=Get-WindowsFeature | ? {
$\_.DisplayName -eq $featurename -or $\_.Name -eq $featurename }

        Add-WindowsFeature $feature
     }

    catch
    {

        Write-Host "Addition of Windows feature $featurename
            failed"
        Exit 1
     }

    Write-Host "Addition of Windows feature $featurename
       succeeded"
 }

```



```
38
39  $system= gwmi win32_operatingSystem | select name
40
41  if (-not (($system -Like '\*Microsoft Windows Server 2022\*') -or
        ($system -Like '\*Microsoft Windows Server 2019\*') -or (
       $system -Like '\*Microsoft Windows Server 2016\*')))
42  {
43
44      Write-Host("This is not a supported server platform.
           Installation aborted.")
45      Exit
46   }
47
48
49  # Start to install Windows feature
50  Import-Module ServerManager
51
52  AddFeatures('Web-Asp-Net45') #ASP.NET 4.5
53  AddFeatures('Web-Mgmt-Console') #IIS Management Console
54  AddFeatures('Web-Windows-Auth') # Windows Authentication
55  AddFeatures('Web-Metabase') #IIS 6 Metabase Compatibility
56  AddFeatures('Web-WMI') #IIS 6 WMI Compatibility
57  AddFeatures('Web-Lgcy-Scripting')#IIS 6 Scripting Tools
58  AddFeatures('Web-Lgcy-Mgmt-Console') #IIS 6 Management Console
59  AddFeatures('MSMQ-HTTP-Support') #MSMQ HTTP Support
60  AddFeatures('web-websockets') #IIS Web Sockets
61  AddFeatures('NET-WCF-HTTP-Activation45') #http activate
62  <!--NeedCopy-->
```

- InstallPrereqsforSessionRecordingAgent.ps1

```
1   <#
2   .Synopsis
3       Installs Prereqs for Session Recording Agent
4   .Description
5       Supports  Windows Server 2022, Windows Server 2019, Windows
           Server 2016, windows 11, and Windows 10.
6       Install below windows feature on this machine:
7       -Microsoft Message Queuing (MSMQ), with Active Directory
           integration disabled, and MSMQ HTTP support enabled.
8   #>
9   function AddFeatures($featurename)
10  {
11
12      try
13      {
14
15          $feature=Get-WindowsFeature | ? {
16  $\_.DisplayName -eq $featurename -or $\_.Name -eq $featurename }
17
18          Add-WindowsFeature $feature
19       }
20
```



```
21      catch
22      {
23
24          Write-Host "Addition of Windows feature $featurename
                failed"
25          Exit 1
26       }
27
28      Write-Host "Addition of Windows feature $featurename
            succeeded"
29   }
30
31
32   # Start to install Windows feature
33   $system= gwmi win32_operatingSystem | select name
34
35   if (-not (($system -Like '\*Microsoft Windows Server 2022\*') -or
         ($system -Like '\*Microsoft Windows Server 2019\*') -or (
        $system -Like '\*Microsoft Windows Server 2016\*') -or (
        $system -Like '\*Microsoft Windows 11\*') -or ($system -Like '
        \*Microsoft Windows 10\*')))
36   {
37
38      Write-Host("This is not a supported platform. Installation
            aborted.")
39      Exit
40   }
41
42
43   if ($system -Like '\*Microsoft Windows Server\*')
44   {
45
46      Import-Module ServerManager
47      AddFeatures('MSMQ') #Message Queuing
48      AddFeatures('MSMQ-HTTP-Support')#MSMQ HTTP Support
49   }
50
51   else
52   {
53
54      try
55      {
56
57          dism /online /enable-feature /featurename:MSMQ-HTTP /all
58       }
59
60      catch
61      {
62
63          Write-Host "Addition of Windows feature MSMQ HTTP Support
                failed"
64          Exit 1
65       }
```



```
66
67        write-Host "Addition of Windows feature MSMQ HTTP Support
              succeeded"
68    }
69
70   <!--NeedCopy-->
```

Windows の役割と機能の前提条件をインストールするには、次の手順を完了します:

1. Session Recording Administration コンポーネントをインストールする予定のマシンで以下を行います:

   a) PowerShell の実行ポリシーが **RemoteSigned** か **Unrestricted** に設定されていることを確認してください。

   ```
   1  Set-ExecutionPolicy RemoteSigned
   2  <!--NeedCopy-->
   ```

   b) コマンドプロンプトを管理者として起動し、`powershell.exe -file InstallPrereqsforSession.ps1`コマンドを実行します。

   正常に追加されている機能が表示され、スクリプトは停止します。

   c) スクリプトの実行後、実行ポリシーが社内ポリシーに基づく適切な値に設定されていることを確認します。

2. Session Recording Agent コンポーネントをインストールする予定のマシンで以下を行います:

   a) PowerShell の実行ポリシーが **RemoteSigned** か **Unrestricted** に設定されていることを確認してください。

   ```
   1  Set-ExecutionPolicy RemoteSigned
   2  <!--NeedCopy-->
   ```

   b) コマンドプロンプトを管理者として起動し、`powershell.exe -file InstallPrereqsforSession.ps1`コマンドを実行します。

   正常に追加されている機能が表示され、スクリプトは停止します。

   c) スクリプトの実行後、実行ポリシーが社内ポリシーに基づく適切な値に設定されていることを確認します。

Session Recording Administration コンポーネントのインストール

> 注:
>
> 2110 以降、TLS 1.0 が無効になっている Windows Server 2016 に Session Recording Administration コンポーネントをインストールする前に、次の手順を実行します。
>
> 1. OLE DB Driver for SQL Server をインストールします。

> 2. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 レジストリキーで、SchUseStrongCrypto DWORD（32 ビット）値を追加して、値を 1 に設定します。
> 3. 再起動します。

Session Recording Administration、Session Recording Agent、および Session Recording Player の各コンポーネントを別々のサーバーにインストールすることをお勧めします。

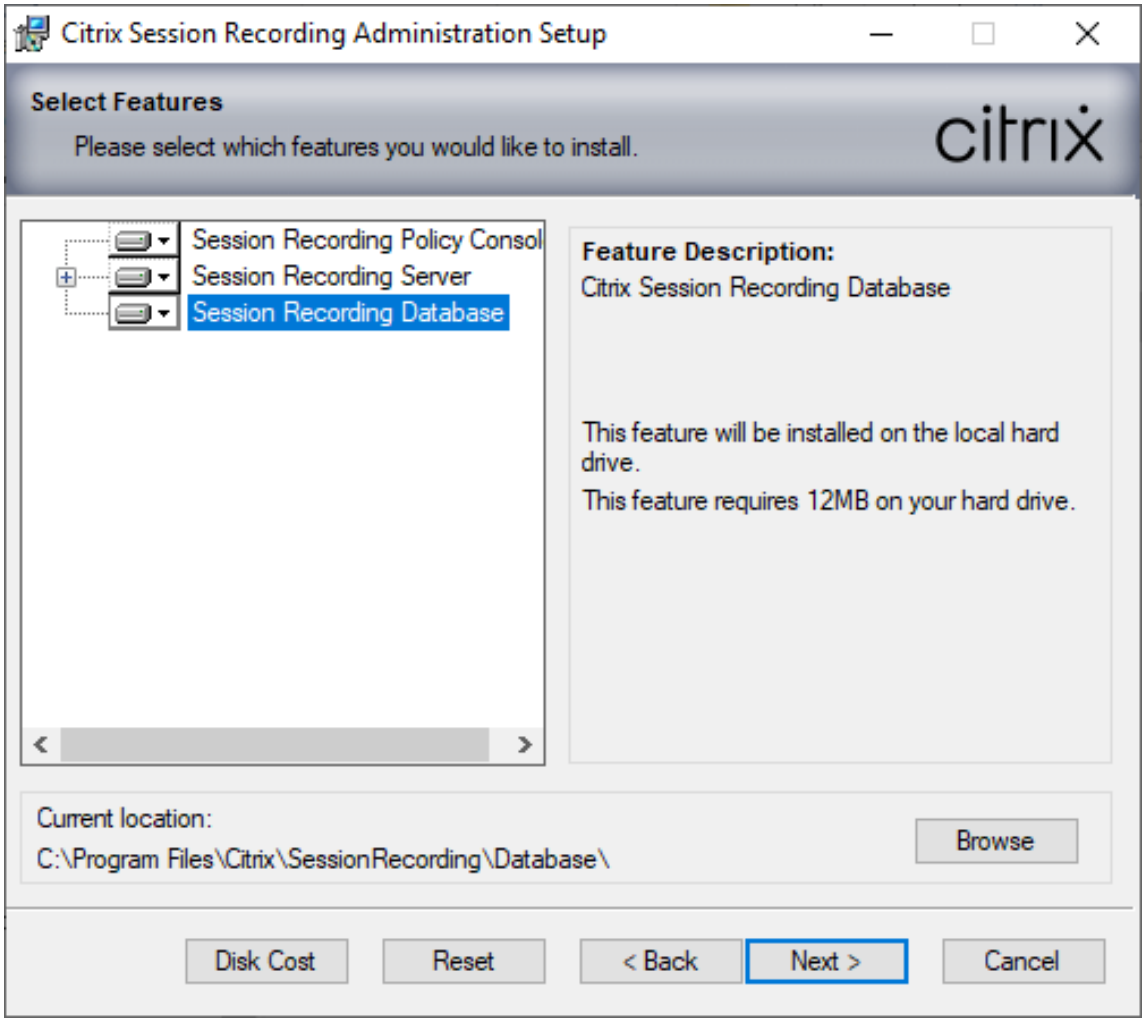
Session Recording Administration コンポーネントは、Session Recording データベース、Session Recording サーバー、および Session Recording ポリシーコンソールから構成されています。コンポーネントを選択してサーバーにインストールできます。

> 注:
>
> 2110 以降、TLS 1.0 が無効になっている Windows Server 2016 に Session Recording Administration コンポーネントをインストールする前に、次の手順を実行します。
>
> 1. OLE DB Driver for SQL Server をインストールします。
> 2. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 レジストリキーで、SchUseStrongCrypto DWORD（32 ビット）値を追加して、値を 1 に設定します。
> 3. Windows Server 2016 を再起動します。

1. **Broker_PowerShellSnapIn_x64.msi** をインストールします。

   > 重要:
   >
   > Session Recording ポリシーコンソールを使用するには、Broker PowerShell スナップイン（Broker_PowerShellSnapIn_x64.msi）を手動でインストールします。Citrix Virtual Apps and Desktops の ISO（\layout\image-full\x64\Citrix Desktop Delivery Controller）でスナップインを検索し、インストール手順に従います。従わない場合、エラーが発生する可能性があります。

2. Windows コマンドプロンプトを管理者として起動し、msiexec /i SessionRecordingAdministrationx.msi コマンドを実行するか、この.msi ファイルをダブルクリックします。
3. インストール UI で ［次へ］を選択して、ライセンス契約に同意します。
4. **Session Recording Administration Setup** 画面で、インストールする Session Recording Administration コンポーネントを選択します。



注:

概念実証では、すべての Session Recording Administration コンポーネントを 1 つのサーバーにインストールしても構いません。ただし、大規模な実稼働環境の場合は、Session Recording ポリシーコンソールをインストールしたサーバーとは別のサーバーに、Session Recording サーバー、Session Recording 管理者ログ、および Session Recording データベースをインストールすることをお勧めします。Session Recording 管理者ログは、Session Recording サーバーのオプションのサブ機能です。Session Recording 管理者ログを選択する前に、Session Recording サーバーを選択します。

Session Recording データベースのインストール

注:

- Session Recording データベースは実際のデータベースではありません。Microsoft SQL Server インスタンスに必要なデータベースを作成して構成する役割のコンポーネントです。Session Recording では、Microsoft SQL Server に基づくデータベースの高可用性のための 3 つのソリューションをサポー

> トしています。詳しくは、「データベースの高可用性」を参照してください。
>
> - Session Recording データベースは、Azure SQL Managed Instance、Azure 仮想マシン（VM）上の SQL Server、AWS RDS に展開できます。詳しくは、「Azure SQL Managed Instance または AWS RDS での Session Recording データベースの展開」および「Azure VM 上の SQL Server での Session Recording データベースの展開」を参照してください。

Session Recording データベースと Microsoft SQL Server の展開には、通常以下の 3 種類があります:

- 展開 1: Session Recording サーバーと Session Recording データベースを同じマシンにインストールし、Microsoft SQL Server をリモートマシンにインストールする（推奨）。
- 展開 2: Session Recording サーバー、Session Recording データベース、および Microsoft SQL Server を同じマシンにインストールする。
- 展開 3: Session Recording サーバーをあるサーバーにインストールし、Session Recording データベースと Microsoft SQL Server の両方を、Session Recording サーバーをインストールしたマシンとは別のマシンにインストールする（推奨されません）。

1. ［データベースおよびサーバーの構成］ページで、Session Recording データベースのインスタンス名とデータベース名、および Session Recording サーバーのコンピューターアカウントを指定します。［次へ］をクリックします。

    - インスタンス名: データベースインスタンスが名前付きインスタンスでない場合、SQL Server のコンピューター名のみを使用できます。名前付きインスタンスがある場合は、データベースインスタンス名として「コンピューター名\インスタンス名」を使用します。使用中のサーバーインスタンス名を確認するには、SQL Server で **select @@servername** を実行します。戻り値は、正確なデータベースインスタンス名です。SQL Server がカスタムポート（デフォルトポート 1433 以外）でリスンする場合は、インスタンス名にコンマを追加してカスタムリスナーポートを設定します。たとえば、［インスタンス名］テキストボックスで「**DXSBC-SRD-1,2433**」と入力します。コンマの後の「2433」は、カスタムリスナーポートを示します。
    - データベース名: ［データベース名］テキストボックスで任意のデータベース名を入力するか、またはテキストボックスに事前設定されているデフォルトのデータベース名を使用します。［接続のテスト］をクリックして、SQL Server インスタンスへの接続とデータベース名の有効性をテストします。

        > 重要:
        >
        > 任意のデータベース名に使用できる文字は、A～Z、a～z、0～9、アンダースコアのみで、123 文字を超えてはなりません。

        - データベースのサーバーの役割権限である **securityadmin** および **dbcreator** が必要です。権限がない場合は、次を行います:

            * データベース管理者にインストールの権限を割り当ててもらいます。インストールの完了後は、**securityadmin** および **dbcreator** サーバー役割権限は不要になり、安全に削除できます。

* または、msi のインストール中、**securityadmin** および **dbcreator** サーバー役割権限とともに、データベース管理者の資格情報を求めるダイアログボックスが表示されます。資格情報を正確に入力して、[**OK**] をクリックし、インストールを続行します。

インストールにより Session Recording データベースが作成され、Session Recording サーバーのマシンアカウントが **db_owner** として追加されます。

- **Session Recording** サーバーのコンピューターアカウント:
  - 展開 **1** と展開 **2**:[**Session Recording** サーバーのコンピューターアカウント] テキストボックスで、「**localhost**」と入力します。
  - 展開 **3**: Session Recording サーバーをホストするマシンの名前を、「ドメイン\コンピューター名」の形式で入力します。Session Recording サーバーのコンピューターアカウントは、Session Recording データベースにアクセスするためのユーザーアカウントです。

> 注:
>
> [**Session Recording** サーバーのコンピューターアカウント] テキストボックスにドメイン名が設定されているときに、Session Recording Administration コンポーネントをインストールしようとすると、エラーコード 1603 で失敗することがあります。回避策として、**localhost** または NetBIOS ドメイン\マシン名を [**Session Recording** サーバーのコンピューターアカウント] テキストボックスに入力してください。NetBIOS ドメイン名を取得するには、Session Recording サーバーをインストールしたマシンの PowerShell で「`$env:userdomain`」を実行するか、コマンドプロンプトで「`echo %UserDomain%`」を実行します。

2. 手順に従ってインストールを完了します。

Session Recording サーバーのインストール

1. [機能] ページで、[**Session Recording** サーバー] と [**Session Recording** 管理者ログ] を選択します。

> 注:
>
> - Session Recording 管理者ログは、Session Recording サーバーのオプションのサブ機能です。Session Recording 管理者ログを選択する前に、Session Recording サーバーを選択します。
> - Session Recording 管理者ログと Session Recording サーバーを同時にインストールすることをお勧めします。管理者ログ機能を有効にしない場合は、後のページで無効にできます。

2. [データベースおよびサーバーの構成] ページで、設定を指定します。
   - インスタンス名:[インスタンス名] に SQL Server の名前を入力します。名前付きインスタンスを使用している場合は、「コンピューター名\インスタンス名」を入力します。使用していない場合は、「コンピューター名」だけを入力します。SQL Server がカスタムポート（デフォルトポート 1433 以外）でリスンする場合は、インスタンス名にコンマを追加してカスタムリスナーポートを設定します。たと

えば、［インスタンス名］テキストボックスで「**DXSBC-SRD-1,2433**」と入力します。コンマの後の「2433」は、カスタムリスナーポートを示します。

- データベース名：［データベース名］テキストボックスで任意のデータベース名を入力するか、またはテキストボックスに事前設定されているデフォルトのデータベース名 **CitrixSessionRecording** を使用します。
  データベースのサーバーの役割権限である **securityadmin** および **dbcreator** が必要です。権限がない場合は、次を行います：
  - データベース管理者にインストールの権限を割り当ててもらいます。インストールの完了後は、**securityadmin** および **dbcreator** サーバー役割権限は不要になり、安全に削除できます。
  - または、msi のインストール中、**securityadmin** および **dbcreator** サーバー役割権限とともに、データベース管理者の資格情報を求めるダイアログボックスが表示されます。資格情報を正確に入力して、［**OK**］をクリックし、インストールを続行します。
- 正しいインスタンス名とデータベース名を入力したら、［接続のテスト］をクリックして Session Recording データベースへの接続をテストします。
- Session Recording サーバーのコンピューターアカウントを入力して、［次へ］をクリックします。

3. ［管理者ログの構成］ページで、管理者ログ機能の構成を指定します。

   - ログデータベースは **SQL Server** インスタンスにインストールされます：このテキストボックスは編集できません。管理者ログデータベースの SQL Server インスタンス名は、［データベースおよびサーバーの構成］ページで入力したインスタンス名が自動的に適用されます。
   - ログデータベース名：このテキストボックスで管理者ログデータベースの任意のデータベース名を入力するか、またはテキストボックスに事前設定されたデフォルトのデータベース名 **CitrixSessionRecordingLogging** を使用します。

     > 注：
     >
     > 管理者ログデータベース名は ［データベースとサーバーの構成］ページの ［データベース名］テキストボックスで設定した Session Recording データベース名と異なるものにする必要があります。

   - デフォルトのデータベース名を使用します：このオプションを選択すると、デフォルトのログデータベース名が使用されます。
   - ロギングサービスを有効にする：デフォルトでは、管理者ログ機能は有効になっています。チェックボックスをオフにしてこの機能を無効にできます。
   - 強制ブロッキングを有効にする：デフォルトでは強制ブロッキングが有効になっているため、ログが失敗すると通常の機能がブロックされることがあります。チェックボックスをオフにして強制ブロッキング（必須のブロック）を無効にできます。

4. ［次へ］をクリックしてインストールを完了します。

> 注:
>
> Session Recording サーバーのデフォルトのインストールでは、通信をセキュリティで保護するため HTTPS/TLS を使用します。Session Recording サーバーのデフォルトのインターネットインフォメーションサービス（IIS）サイトで TLS が構成されていない場合は、HTTP を使用します。これを行うには、IIS 管理コンソールで SSL の選択をキャンセルします。Session Recording Broker サイトに移動し、SSL 設定を開き、［**Require SSL**］チェックボックスをオフにします。

Session Recording Agent のインストール

Session Recording Agent は、セッションを録画する VDA または VDI マシンにインストールします。

1. ［**Session Recording Agent** 構成］ページで、次の作業を行います：Session Recording サーバーを事前にインストールしている場合は、Session Recording サーバーをインストールしたマシンのコンピューター名を入力します。Session Recording サーバーとの接続のプロトコルとポート情報を入力します。Session Recording のインストールが済んでいない場合は、後で ［**Session Recording Agent** のプロパティ］でこれらの情報を変更できます。
2. 手順に従ってインストールを完了します。

> 注:
>
> Machine Creation Services（MCS）または Citrix Provisioning Services（PVS）で、インストール済みの Microsoft Message Queuing（MSMQ）を使用して VDA を作成すると、一定の状況下において、これらの VDA の`QMId`が同じになる可能性があります。この場合、次のようなさまざまな問題が発生する可能性があります:
>
> - 録画の同意が得られていても、セッションが録画されない場合があります。
> - セッションのログオフ信号が Session Recording サーバーによって受信されず、セッションのステータスが常に［ライブ］になってしまう可能性があります。
>
> 解決策は VDA ごとに固有の`QMId`を作成することですが、方法は展開方法によって異なります。
>
> 静的デスクトップモードで PVS 7.7 以降および MCS 7.9 以降を使用して作成されたシングルセッション OS VDA には、追加のアクションは必要ありません。
>
> MCS または PVS を使用して作成されたマルチセッション OS VDA と、ユーザーがログオフするとすべての変更が削除されるように構成されているシングルセッション OS VDA は、`GenRandomQMID.ps1`スクリプトを使用してシステム起動時に`QMId`を変更します。電源管理方法を変更して、ユーザーがログインする前に十分な数の VDA が実行されているようにします。
>
> GenRandomQMID.ps1 スクリプトを使用するには、以下の手順に従ってください:
>
> 1. PowerShell の実行ポリシーが **RemoteSigned** か **Unrestricted** に設定されていることを確認してください。


```
Set-ExecutionPolicy RemoteSigned
```

2. スケジュールされたタスクを作成し、トリガーを［システム起動時］に設定して、PVS または MCS マスターイメージマシンで SYSTEM アカウントを使って実行します。

3. スタートアップタスクとしてコマンドを追加します。

```
powershell .exe -file C:\\GenRandomQMID.ps1
```

GenRandomQMID.ps1 スクリプトの概要:

1. レジストリから現在の`QMId`を削除します。
2. `SysPrep = 1`を`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters`に追加します。
3. CitrixSmAudAgent や MSMQ などの関連サービスを停止します。
4. ランダムな`QMId`を生成するために、先ほど停止したサービスを開始します。

例 **GENRANDOMQMID.PS1**:

```
# Remove old QMId from registry and set SysPrep flag for MSMQ

Remove-Itemproperty -Path >HKLM:Software\Microsoft\MSMQ\Parameters\
    MachineCache -Name QMId -Force

Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -
    Name >"SysPrep" -Type DWord -Value 1

# Get dependent services

$depServices = Get-Service -name MSMQ -dependentservices | Select -
    Property Name

# Restart MSMQ to get a new QMId

Restart-Service -force MSMQ

# Start dependent services

if ($depServices -ne $null) {


    foreach ($depService in $depServices) {


        $startMode = Get-WmiObject win32_service -filter "NAME = '$
    ($depService.Name)'" | Select -Property StartMode

        if ($startMode.StartMode -eq "Auto") {


```



```
28                Start-Service $depService.Name
29            }
30
31    }
32
33
34    }
35
36  <!--NeedCopy-->
```

Session Recording Player と Web Player のインストール

Session Recording サーバーまたはドメイン内のワークステーションに Session Recording Player をインストールします。Session Recording サーバーでのみ Web Player をインストールします。

SessionRecordingPlayer.msiとSessionRecordingWebPlayer.msiをダブルクリックし、手順に従ってインストールを完了します。

インストールの自動化

Session Recording は、オプションを使用するサイレントインストールをサポートしています。サイレントインストールを使用するスクリプトを記述し、関連するコマンドを実行します。

Session Recording Administration コンポーネントのインストールを自動化する

単一のコマンドを使用して **Session Recording Administration** コンポーネントの完全なセットをインストールする　たとえば、次のいずれかのコマンドを実行すると、Session Recording Administration コンポーネントの完全なセットをインストールし、インストール情報を取得するためにログファイルを作成します。

```
1  msiexec /i "c:\SessionRecordingAdministrationx64.msi" AddLocal="
       SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
       DatabaseInstance="WNBIO-SRD-1" DatabaseName="CitrixSessionRecording"
        LoggingDatabaseName="CitrixSessionRecordingLogging" DatabaseUser="
       localhost" AllowSession0Install="1" /q /l*vx "YourInstallationLog"
2  <!--NeedCopy-->
```

```
1  msiexec /i "SessionRecordingAdministrationx64.msi" AddLocal="
       SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
       DatabaseInstance="CloudSQL" DatabaseName="CitrixSessionRecording"
       LoggingDatabaseName="CitrixSessionRecordingLogging"
       AzureSQLServiceSupport="1" AzureUsername="CloudSQLAdminName"
       AzurePassword="CloudSQLAdminPassword" AllowSession0Install="1" /q /l
       *vx "c:\WithLogging.log"
2  <!--NeedCopy-->
```


> 注:
>
> SessionRecordingAdministrationx64.msiファイルは\layout\image-full\x64\Session Recordingの Citrix Virtual Apps and Desktops ISO にあります。

各項目の意味は次のとおりです:

- **AddLocal** は選択する機能です。複数のオプションを選択できます。**SsRecServer** は、Session Recording サーバーです。**PolicyConsole** は、Session Recording ポリシーコンソールです。**SsRecLogging** は、管理者ログ機能です。**StorageDatabase** は、Session Recording データベースです。Session Recording 管理者ログは、Session Recording サーバーのオプションのサブ機能です。Session Recording 管理者ログを選択する前に、Session Recording サーバーを選択します。
- **DatabaseInstance** は、Session Recording データベースのインスタンス名です。たとえば、Azure SQL Managed Instance を使用している場合は.\SQLEXPRESS,computer-name\SQLEXPRESS,computer-nameまたはtcp:srt-sql-support.**public**.ca7b16b60789.database.windows.net,3342です。
- **DatabaseName** は、Session Recording データベースのデータベース名です。
- **LoggingDatabaseName** は、管理者ログデータベース名です。
- **AzureSQLServiceSupport** によって、クラウド SQL がサポートされるかどうかが決まります。クラウド SQL を使用するには、これを1に設定します。
- **DatabaseUser** は、Session Recording サーバーのコンピューターアカウントです。
- **AzureUsername** は、クラウド SQL の管理者名です。
- **AzurePassword** は、クラウド SQL 管理者のパスワードです。
- **AllowSession0Install** は、Session Recording Administration コンポーネントをセッション 0 でインストールするかどうかを決定します。Session Recording Administration コンポーネントをセッション 0 でインストールするには、この引数をコマンドに追加して 1 に設定します。コマンドを実行する前に、SQL Server で使用するコンピューターアカウントをログインとして追加し、**sysadmin** ロールを割り当てるようにしてください。
- **/q** は、サイレントモードを指定します。
- **/l*v** スイッチにより詳細モードでログが記録されます。
- **YourInstallationLog** は、インストールログを作成する場所です。

Session Recording サーバーを展開するためのマスターイメージを作成する Session Recording データベースおよび管理者ログデータベースが既存の展開に存在する可能性があります。このような場合は、SessionRecordingAdministrationx64.msi を使用して Session Recording Administration コンポーネントをインストールするときに、データベースチェックを省略できるようになりました。マスターイメージを作成することで、Session Recording サーバーを他の多くのマシン上で簡単に作成できます。マスターイメージを使用してターゲットマシンにサーバーを展開後、各マシンでコマンドを実行して、既存の Session Recording データベースと管理者ログデータベースに接続します。このマスターイメージのサポートにより展開が容易になり、人的エラーによって影響を受ける可能性が最小限に抑えられます。これは新規インストールにのみ適用され、次の手順で実行します:

1. コマンドプロンプトを起動し、次のようなコマンドを実行します:

```
msiexec /i "SessionRecordingAdministrationx64.msi" AddLocal="
    SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
    DatabaseInstance="sqlnotexists" DatabaseName="
    CitrixSessionRecording2" LoggingDatabaseName="
    CitrixSessionRecordingLogging2" DatabaseUser="localhost" /q /l*
    vx "c:\WithLogging.log" IgnoreDBCheck="True"
<!--NeedCopy-->
```

   このコマンドは、Session Recording データベースおよび管理者ログデータベースへの接続を構成およびテストせずに、Session Recording Administration コンポーネントをインストールします。

   IgnoreDBCheck パラメーターを **True** に設定し、**DatabaseInstance**、**DatabaseName**、**LoggingDatabaseName** でランダムな値を使用します。

2. 操作しているマシン上にマスターイメージを作成します。
3. Session Recording サーバーを展開するために、マスターイメージを他のマシンに展開します。
4. 各マシンで、次のようなコマンドを実行します:

```
.\SsRecUtils.exe -modifydbconnectionpara DATABASEINSTANCE
    DATABASENAME LOGGINGDATABASENAME

iisreset /noforce
<!--NeedCopy-->
```

   このコマンドは、以前にインストールされた Session Recording サーバーを既存の Session Recording データベースおよび管理者ログデータベースに接続します。

   `SsRecUtils.exe`ファイルは、`\Citrix\SessionRecording\Server\bin\`に保存されます。必要に応じて、**DatabaseInstance**、**DatabaseName**、および **LoggingDatabaseName** パラメーターを設定します。

Session Recording Administration コンポーネントのアンインストール時にデータベースを保持　**KeepDB** を **True** に設定すると、Session Recording Administration コンポーネントのアンインストール時に次のコマンドで Session Recording データベースおよび管理者ログデータベースを保持します。

```
msiexec /x "SessionRecordingAdministrationx64.msi" KeepDB="True"
<!--NeedCopy-->
```

Session Recording Player および **Web Player** のインストールを自動化する

たとえば、次のコマンドはそれぞれ Session Recording Player と Web Player をインストールします。

```
msiexec /i "c:\SessionRecordingPlayer.msi" /q /l*\vx "
    yourinstallationlog"
<!--NeedCopy-->
```



```
msiexec /i "c:\SessionRecordingWebPlayer.msi" /q /l*vx "
    yourinstallationlog"
<!--NeedCopy-->
```

> 注:
>
> SessionRecordingPlayer.msiファイルは\layout\image-full\x86\Session Recordingの Citrix Virtual Apps and Desktops ISO にあります。
>
> SessionRecordingWebPlayer.msiファイルは\layout\image-full\x64\Session Recordingの Citrix Virtual Apps and Desktops ISO にあります。

各項目の意味は次のとおりです:

- **/q** は、サイレントモードを指定します。
- **/l*v** スイッチにより詳細モードでログが記録されます。
- **yourinstallationlog** は、インストールログを作成する場所です。

Session Recording Agent のインストールを自動化する　たとえば、次のコマンドでは、Session Recording Agent をインストールし、インストール情報を取得するためにログファイルを作成します。

```
msiexec /i SessionRecordingAgentx64.msi /q /l*vx yourinstallationlog
    SESSIONRECORDINGSERVERNAME=yourservername
SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol
    SESSIONRECORDINGBROKERPORT=yourbrokerport
<!--NeedCopy-->
```

> 注:
>
> SessionRecordingAgentx64.msiファイルは\layout\image-full\x64\Session Recordingの Citrix Virtual Apps and Desktops ISO にあります。

各項目の意味は次のとおりです:

- **yourservername** は、Session Recording サーバーをホストするマシンの NetBIOS 名または FQDN です。指定しない場合のデフォルト値は **localhost** です。
- **yourbrokerport** は、Session Recording Broker との通信に Session Recording Agent で使用されるポートを表す HTTP または HTTPS です。指定しない場合のデフォルト値は HTTPS です。
- **yourbrokerport** は、Session Recording Broker との通信に Session Recording Agent で使用されるポートを表す整数です。指定しない場合のデフォルト値は 0 で、選択したプロトコルのデフォルトのポート番号を使用するよう Session Recording Agent に指示します。具体的には、HTTP では 80、HTTPS では 443 です。
- **/q** は、サイレントモードを指定します。
- **/l*v** スイッチにより詳細モードでログが記録されます。
- **yourinstallationlog** は、インストールログを作成する場所です。

Session Recording のアップグレード

新しいバージョンのマシンやサイトをセットアップせずに、一部の環境をアップグレードすることができます。Session Recording 7.15 LTSR の最新の CU および以降のバージョンから Session Recording の最新バージョンにアップグレードできます。

> 注:
>
> Session Recording Administration を 7.6 から 7.13 以降にアップグレードし、［変更］を選択して管理者ログサービス追加した場合、［管理者ログの構成］ページに SQL Server インスタンスの名前が表示されません。［次へ］をクリックすると次のエラーメッセージが表示されます:「データベース接続テストに失敗しました。正しいデータベースインスタンス名を入力してください。」回避策として、localhost ユーザーの読み取り権限を次の SmartAuditor サーバーレジストリフォルダーに追加します: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`。
>
> Technical Preview バージョンからはアップグレードできません。

要件、準備、および制限

- Session Recording コンポーネントのアップグレードは、Session Recording インストーラーのグラフィカルインターフェイスまたはコマンドラインを使用します。
- アップグレードを開始する前に、SQL Server インスタンスで CitrixSessionRecording という名前のデータベースをバックアップします。これにより、データベースのアップグレード後に問題が発生した場合に元の状態に復元することができます。
- Session Recording コンポーネントをアップグレードするには、ドメインユーザーであることに加えて、そのマシンのローカル管理者である必要があります。
- Session Recording サーバーと Session Recording データベースが同じサーバーにインストールされていない場合、Session Recording データベースをアップグレードするには、データベースの役割権限が必要です。それ以外の場合、次のことができます:
  - データベース管理者に頼んで、アップグレードのために **securityadmin** および **dbcreator** サーバー役割権限を割り当ててもらいます。アップグレードの完了後は、**securityadmin** および **dbcreator** サーバー役割権限は不要になり、安全に削除できます。
  - または、`SessionRecordingAdministrationx64.msi`ファイルを使用してアップグレードします。msi のアップグレード中、**securityadmin** および **dbcreator** サーバー役割権限を持つデータベース管理者の資格情報を求めるダイアログボックスが表示されます。資格情報を正確に入力して、［**OK**］をクリックし、アップグレードを続行します。
- Session Recording Agent 7.6.0 以降は最新バージョンの Session Recording サーバーと互換性があります。ただし、一部の新機能やバグ修正は反映されない可能性があります。
- Session Recording サーバーのアップグレード中に開始されたセッションは録画されません。
- デスクトップコンポジションリダイレクトモードとの互換性を維持するために、新規インストールまたはアップグレード後に ［**Session Recording Agent** のプロパティ］の ［グラフィック調整］オプションがデフォ

ルトで有効になっています。このオプションは、新規インストールまたはアップグレード後に手動で無効にできます。

- 管理者ログ機能は、この機能を使用できない以前のバージョンから Session Recording をアップグレードした後はインストールされません。この機能を追加するには、アップグレード後にインストールを修正します。
- アップグレードプロセスの開始時にライブ録画セッションが実行されていた場合、録画を完了できる可能性はほとんどありません。
- サイトが停止する場合に備えて影響を軽減するために、以下のアップグレードの順序を確認してください。

アップグレードの順序

1. Session Recording データベースと Session Recording サーバーが別々のサーバーにインストールされている場合、Session Recording サーバーで Session Recording ストレージマネージャーサービスを手動で停止します。次に、まず Session Recording データベースをアップグレードします。
2. インターネットインフォメーションサービス（IIS）マネージャーで、Session Recording Broker が実行されていることを確認します。Session Recording サーバーをアップグレードします。Session Recording データベースと Session Recording サーバーが同じサーバーにインストールされている場合、Session Recording データベースもアップグレードされます。
3. Session Recording サーバーのアップグレードが完了すると、Session Recording サービスは自動的にオンラインに戻ります。
4. （マスターイメージの）Session Recording Agent をアップグレードします。
5. Session Recording サーバーと一緒に、または Session Recording サーバーの後に、Session Recording ポリシーコンソールをアップグレードします。
6. Session Recording Player をアップグレードします。

クラウド **SQL** データベースサービスでの **Session Recording** データベースの展開

ここでは、Azure SQL Managed Instance、AWS RDS、Azure VM 上の SQL Server に、Session Recording データベースを展開する方法について説明します。

Azure SQL Managed Instance または **AWS RDS** での **Session Recording** データベースの展開

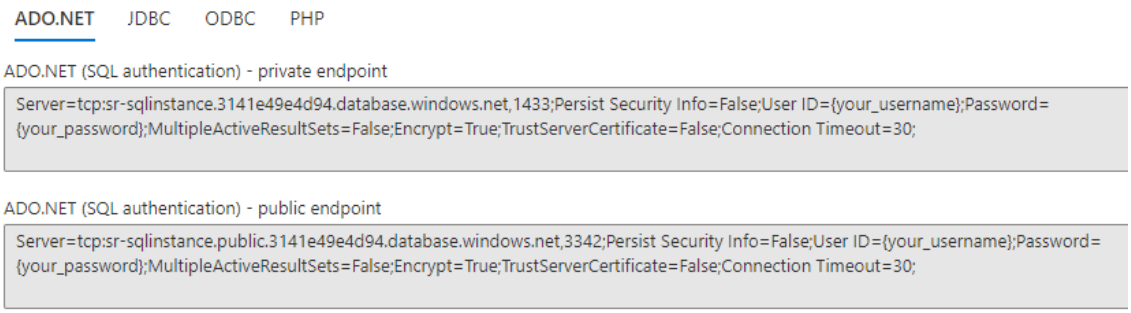
> ヒント：
>
> 次のような単一のコマンドを実行して、Azure SQL Managed Instance または AWS RDS に Session Recording データベースを展開することもできます。詳しくは、この記事の「インストールの自動化」セクションを参照してください。

```
msiexec /i "SessionRecordingAdministrationx64.msi" AddLocal="
    SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
    DatabaseInstance="CloudSQL" DatabaseName="CitrixSessionRecording
    " LoggingDatabaseName="CitrixSessionRecordingLogging"
```

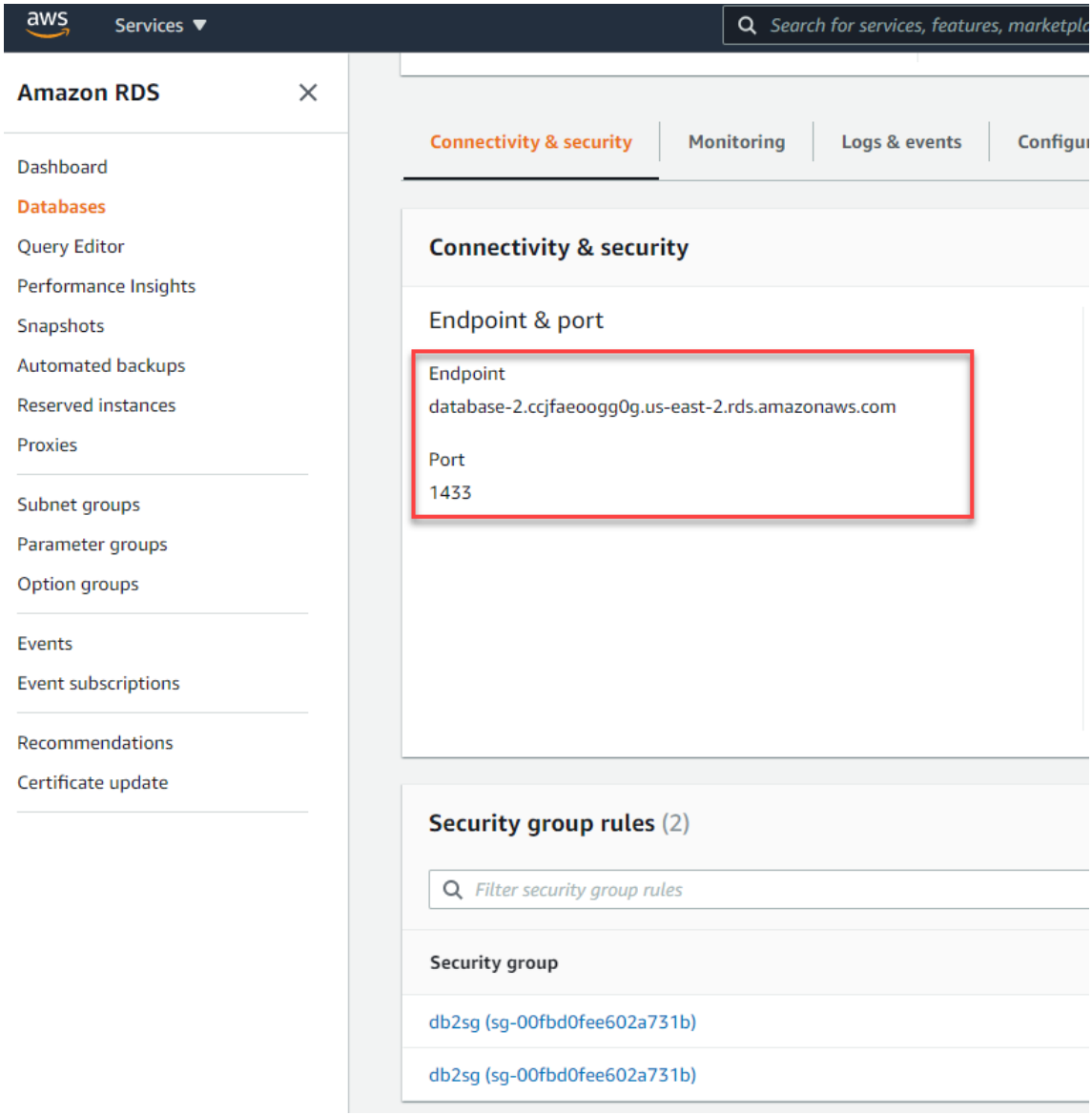


```
        AzureSQLServiceSupport="1" AzureUsername="CloudSQLAdminName"
        AzurePassword="CloudSQLAdminPassword" /q /l*vx "c:\WithLogging.
        log"
2   <!--NeedCopy-->
```

1. Azure SQL Managed Instance を作成するか、Amazon RDS コンソールから SQL Server インスタンスを作成します。
2. （Azure SQL の場合のみ）プロパティパネルに表示される **Server** の文字列を記録しておきます。この文字列は、Session Recording データベースのインスタンス名です。例として、以下のスクリーンショットを参照してください。

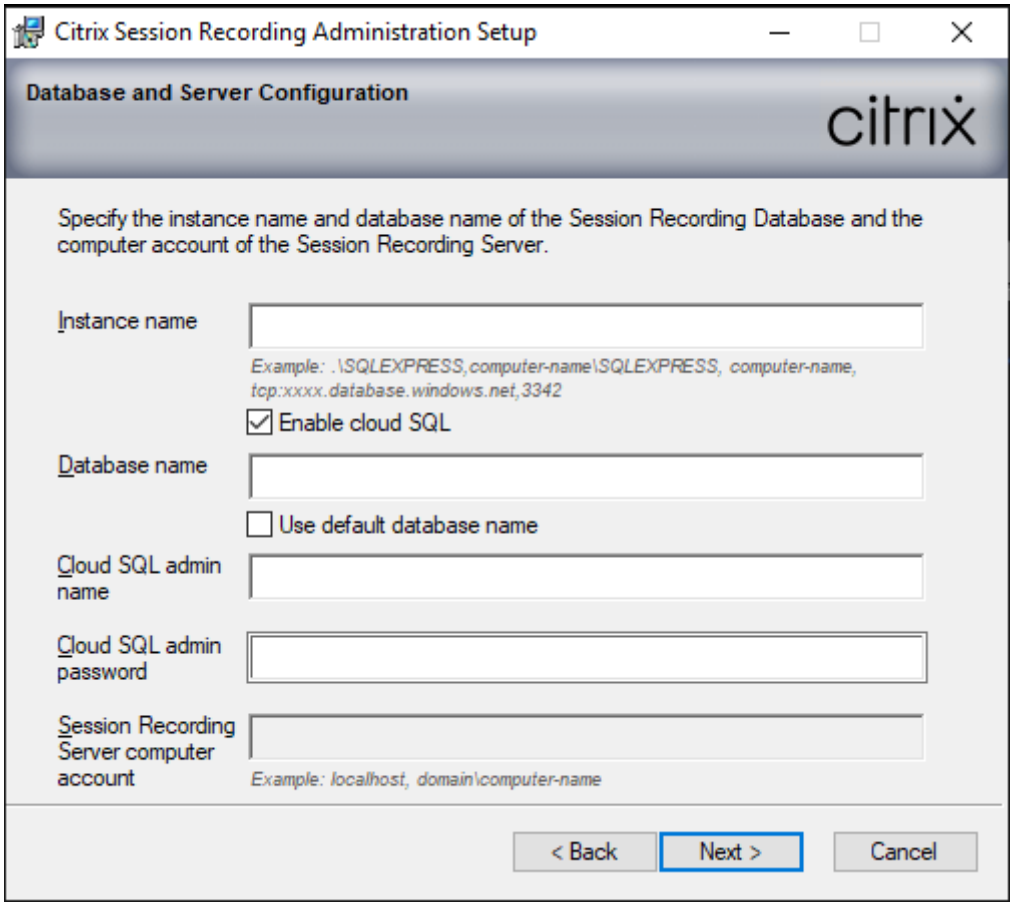


3. （AWS RDS の場合のみ）エンドポイントとポートの情報を記録します。これはデータベースのインスタンス名として、**<** エンドポイント**,** ポート **>** という形式で使用します。



4. SessionRecordingAdministrationx64.msi を実行して、Session Recording データベースをインストールします。

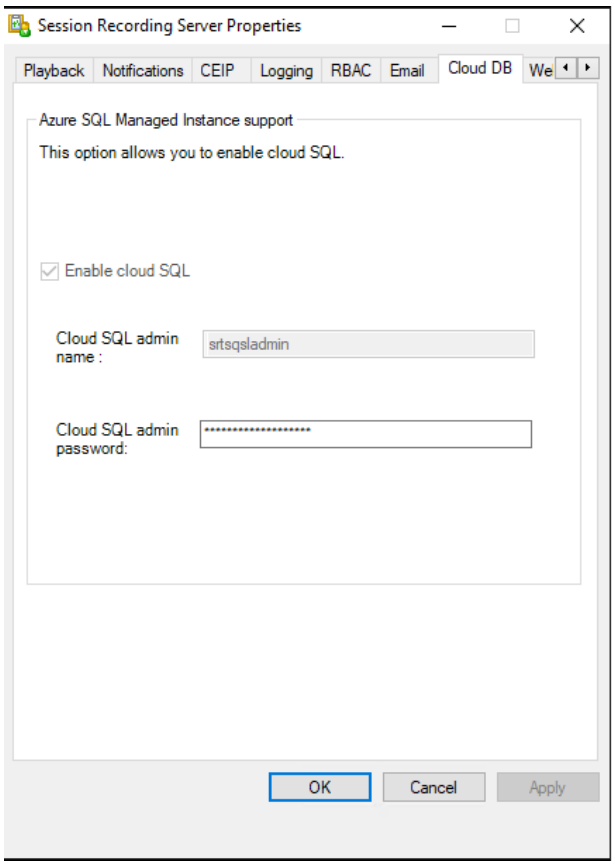
   ［クラウド **SQL** を有効にする］チェックボックスをオンにして、クラウド SQL の管理者名とパスワードを入力します。その他の必要な構成を行います。



注:

クラウド SQL の管理者パスワードを変更する場合は、[**Session Recording** サーバーのプロパティ] でパスワードを更新する必要があります。[**Session Recording** サーバーのプロパティ] を開くと、エラーメッセージが表示されます。[**OK**] をクリックして続行し、[クラウド **DB**] タブを選択します。次に、クラウド SQL の新しい管理者パスワードを入力します。Citrix Session Recording Analytics サービス、Citrix Session Recording ストレージマネージャーサービス、および IIS サービスを再起動します。

Azure AD 認証はサポートされていません。



クラウド **SQL Managed Instance** へのオンプレミスデータベースの移行

1. https://docs.microsoft.com/en-us/data-migration/またはhttps://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-microsoft-sql-server-database-to-amazon-rds-for-sql-server.htmlに従って、オンプレミスデータベースを移行します。
2. 移行後に Session Recording を正しく機能させるには、Session Recording サーバーで`SsRecUtils.exe`を実行します。

   ```
   C:\Program Files\Citrix\SessionRecording\Server\bin\SsRecUtils.exe -modifyazuredbconnectionpara { Database Instance } { Session Recording Database Name } { Session Recording Logging Database Name } { AzureAdminName } { AzureAdminPassword } iisreset /noforce
   ```

3. Session Recording サーバーで、Citrix Session Recording Analytics サービス、Citrix Session Recording ストレージマネージャーサービス、および IIS サービスを再起動します。

Azure SQL Managed Instance からオンプレミスデータベースへの実稼働データベースの移行

1. https://docs.microsoft.com/en-us/data-migration/に従って、データベースを移行します。
2. 移行後に Session Recording を正しく機能させるには、Session Recording サーバーで`SsRecUtils.exe`を実行します。

   ```
   C:\Program Files\Citrix\SessionRecording\Server\bin\SsRecUtils.exe -modifydbconnectionpara { Database Instance } { Session Recording Database Name } { Session Recording Logging Database Name } iisreset /noforce
   ```

3. Session Recording サーバーで、Citrix Session Recording Analytics サービス、Citrix Session Recording ストレージマネージャーサービス、および IIS サービスを再起動します。

Azure VM 上の **SQL Server** での **Session Recording** データベースの展開

Azure VM 上の SQL Server で Session Recording データベースを展開できます。

1. Azure SQL VM を確認します。
2. VM を構成し、Session Recording コンポーネントをインストールするドメインに追加します。
3. Session Recording データベースのインストール時に、VM の FQDN をインスタンス名として使用します。
   注：インストールに SessionRecordingAdministrationx64.msi を使用している場合は、［クラウド **SQL** を有効にする］チェックボックスをオフにします。
4. 手順に従ってインストールを完了します。

Session Recording のアンインストール

サーバーやワークステーションから **Session Recording** コンポーネントを削除するには、**Windows** のコントロールパネルのプログラムのアンインストールまたは削除オプションを使用します。Session Recording データベースを削除するには、インストール時と同じ SQL Server の役割権限 **securityadmin** および **dbcreator** が必要です。

セキュリティ上の理由により、コンポーネントがアンインストールされた後には管理者ログデータベースは削除されません。

Citrix Analytics for Security との統合

Session Recording サーバーを構成して、ユーザーイベントを Citrix Analytics for Security に送信できます。Citrix Analytics for Security は、このユーザーイベントを処理して、ユーザーの動作に関する実用的な分析情報を提供します。

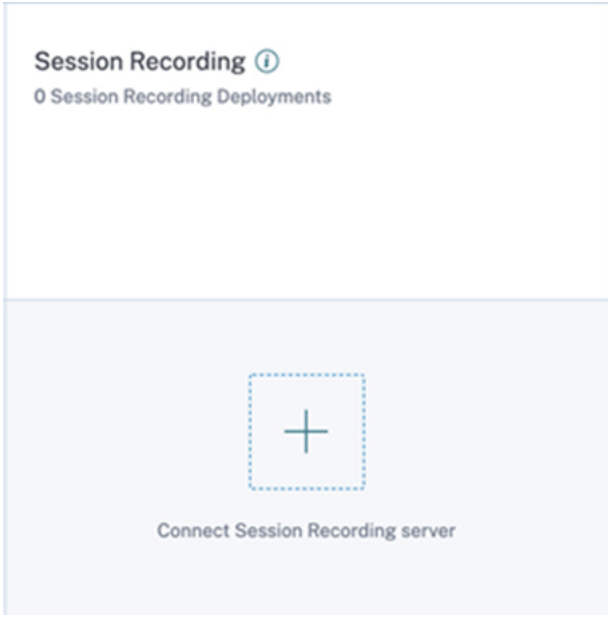
前提条件

開始前に、次の前提条件が満たされていることを確認してください:

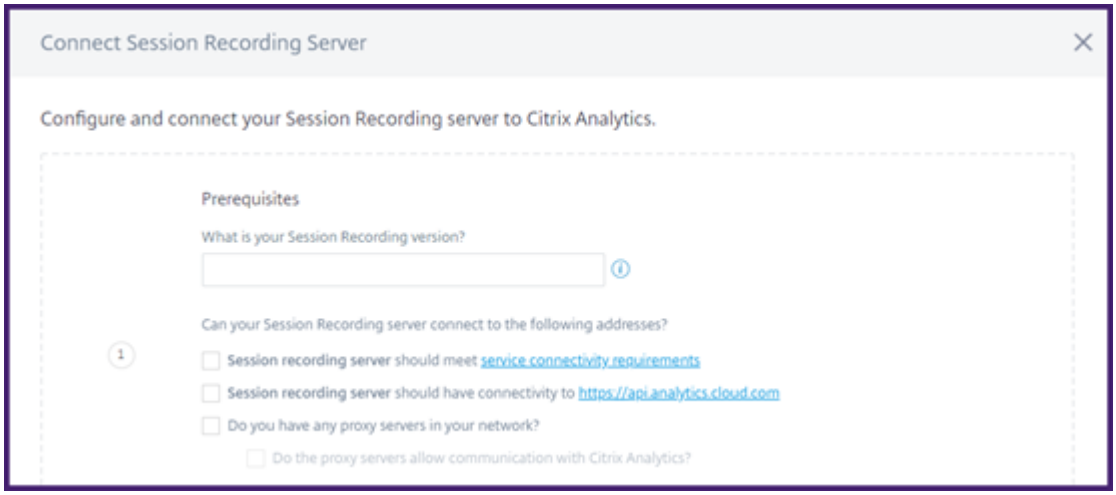
- Session Recording サーバーが、次のアドレスに接続できます:
  - https://*.cloud.com
  - https://*.citrixdata.com
  - https://api.analytics.cloud.com
- Session Recording 展開では、送信インターネット接続用にポート 443 が解放されています。ネットワーク上のすべてのプロキシサーバーは、この Citrix Analytics for Security との通信を許可する必要があります。
- Citrix Virtual Apps and Desktops 7 1912 LTSR を使用している場合、サポートされている Session Recording のバージョンは 2103 以降です。

Session Recording サーバーを **Citrix Analytics for Security** に接続する

1. Citrix Cloud にサインインします。
2. Citrix Analytics for Security を見つけて、[**Manage**] をクリックします。
3. トップバーから [**Settings**] > [**Data Sources**] をクリックします。
4. [**Virtual Apps and Desktops- Session Recording**] サイトカードで、[**Connect Session Recording server**] をクリックします。



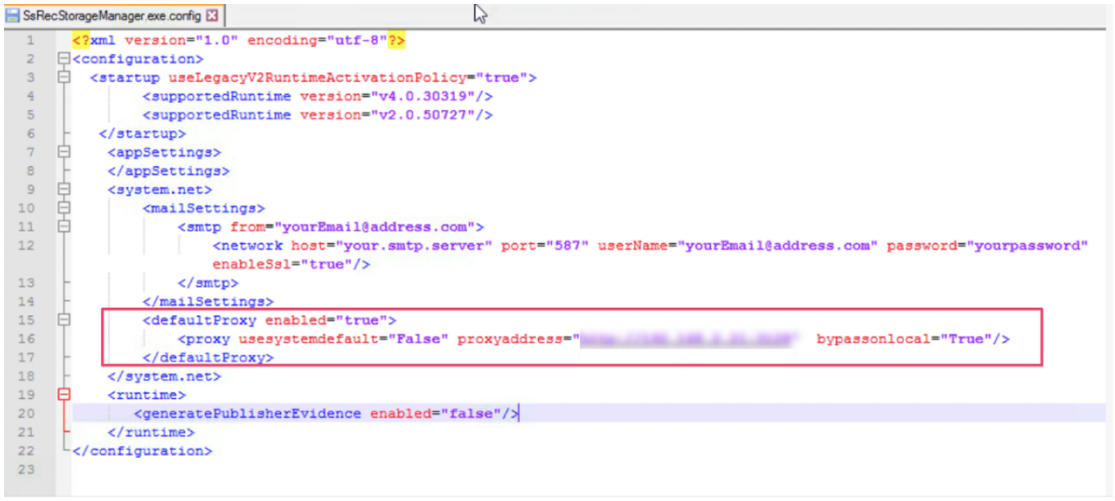
5. [**Connect Session Recording Server**] ページで、チェックリストを確認し、すべての必須要件を選択します。必須要件を選択しない場合、[**Download File**] オプションは無効になります。



6. ネットワークにプロキシサーバーがある場合は、Session Recording サーバーの *SsRecStorageManager.exe.config* ファイルにプロキシアドレスを入力します。

   構成ファイルは次の場所にあります: `<Session Recording server installation path>\bin\SsRecStorageManager.exe.config`

   たとえば、次のようになります: `C:\Program Files\Citrix\SessionRecording\Server\Bin\SsRecStorageManager.exe.config`



7. [**Download File**] をクリックして、*SessionRecordingConfigurationFile.json* ファイルをダウンロードします。

   > 注:
   >
   > このファイルには機密情報が含まれています。ファイルを安全な場所に保存します。

8. Citrix Analytics for Security に接続する Session Recording サーバーにファイルをコピーします。

   展開に複数の Session Recording サーバーがある場合は、接続する各サーバーにファイルをコピーし、手順に従って各サーバーを構成する必要があります。

9. Session Recording サーバーで、次のコマンドを実行して設定をインポートします:

```
<Session Recording server installation path>\bin\SsRecUtils.exe -Import_SRCasConfigurations <configuration file path>
<!--NeedCopy-->
```

例:

```
C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.exe -Import_SRCasConfigurations C:\Users\administrator \Downloads\SessionRecordingConfigurationFile.json
<!--NeedCopy-->
```

10. 次のサービスを再起動します:

    - Citrix Session Recording Analytics サービス
    - Citrix Session Recording ストレージマネージャー

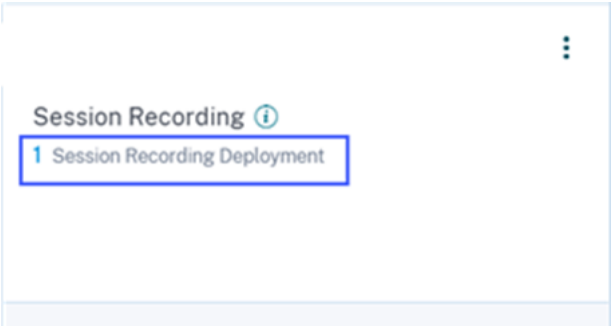
11. 構成が正常に完了したら、Citrix Analytics for Security に移動して、接続されている Session Recording サーバーを表示します。[**Turn On Data Processing**] クリックして、Citrix Analytics for Security がデータを処理できるようにします。

    > 注:
    >
    > Session Recording サーバーバージョン 2103 または 2104 を使用している場合は、最初に Virtual Apps and Desktops セッションを起動して、Citrix Analytics for Security で接続されている Session Recording サーバーを表示する必要があります。こうしないと、接続されている Session Recording サーバーが表示されません。この要件は、Session Recording サーバーバージョン 2106 以降には適用されません。

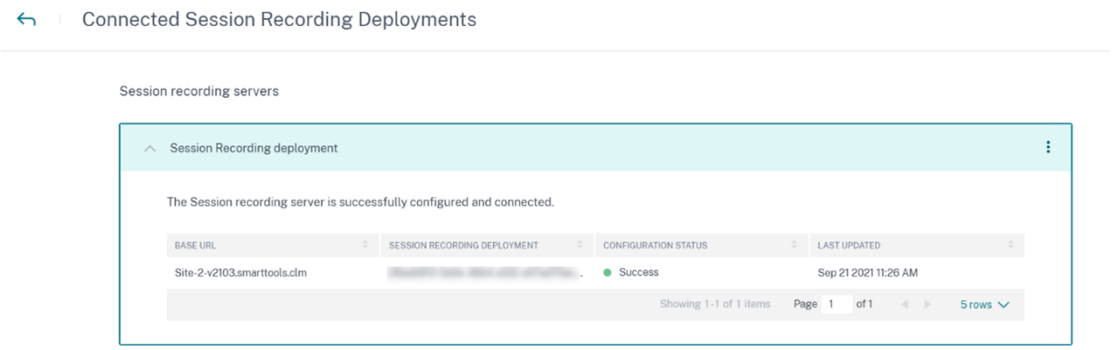
接続された展開を表示する

サーバーの展開は、構成が成功した場合にのみ Session Recording サイトカードに表示されます。サイトカードには、Citrix Analytics for Security との接続を確立した構成済みサーバーの数が表示されます。

構成が成功した後も Session Recording サーバーが表示されない場合は、「構成済み Session Recording サーバーが接続に失敗する」のトラブルシューティングのセクションを参照してください。



サイトカードで展開の数をクリックして、Citrix Analytics for Security で接続されているサーバーグループを表示します。たとえば、**1 Session Recording Deployment** をクリックして、接続されている 1 つまたは複数のサーバーグループを表示します。各 Session Recording サーバーは、ベース URL と ServerGroupID で表示されます。



受信したイベントを表示する

サイトカードには、接続された Session Recording 展開と、これらの展開から過去 1 時間に受信したイベントが表示されます。これは、デフォルトの時間の選択肢です。1 週間（1 W）を選択して、データを表示することもできます。受信したイベントの数をクリックして、セルフサービス検索ページにイベントを表示します。

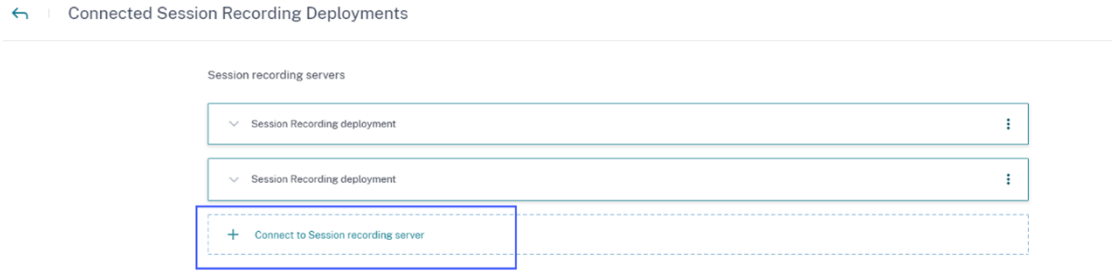
データ処理を有効にすると、サイトカードに **No data received** ステータスが表示される場合があります。このステータスは、次の 2 つの理由で表示されます:

1. 初めてデータ処理をオンにした場合、イベントが Citrix Analytics のイベントハブに到達するまでに時間がかかります。Citrix Analytics がイベントを受信すると、ステータスが **Data processing on** に変わります。しばらく経ってもステータスが変わらない場合は、[Data Sources] ページを更新してください。
2. Citrix Analytics は、過去 1 時間にデータソースからイベントを受信していません。

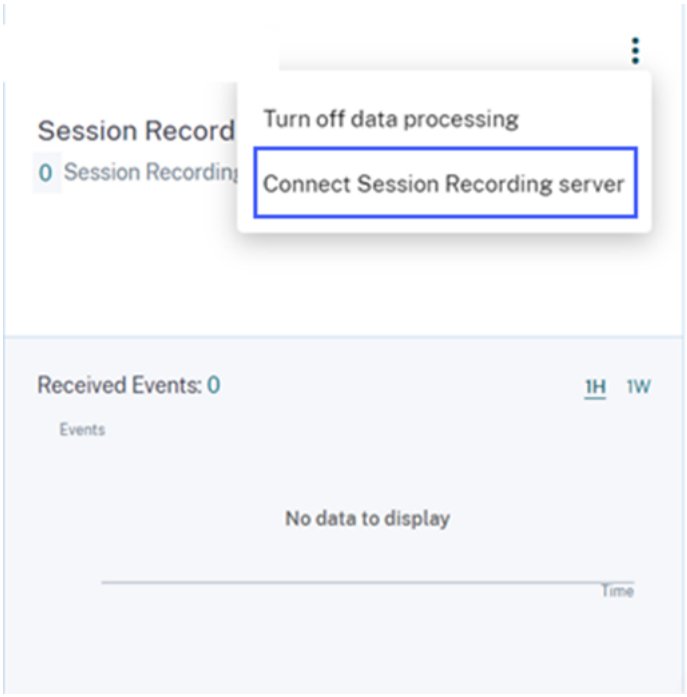
Session Recording サーバーを追加する

Session Recording サーバーを追加するには、次のいずれかを実行します:

- [**Connected Session Recording Deployments**] ページで、[**Session Recording Server** への接続] をクリックします。



- [**Virtual Apps and Desktops- Session Recording**] サイトカードで、縦の省略記号（⋮）をクリックして［**Session Recording Server** への接続］を選択します。

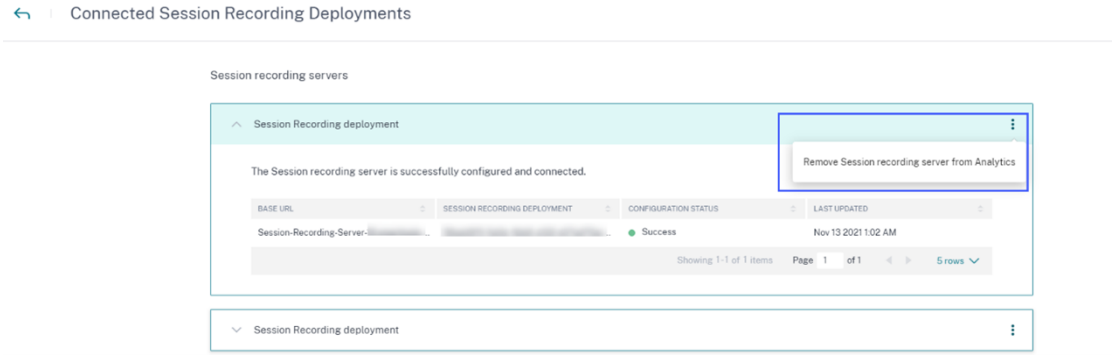


手順に従って構成ファイルをダウンロードし、Session Recording サーバーを構成します。

Session Recording サーバーを削除する

Session Recording サーバーを削除するには:

1. Citrix Analytics for Security で、［**Connected Session Recording Deployments**］ページに移動し、削除するサーバー展開を選択します。
2. 縦の省略記号（⋮）をクリックし、［**Remove Session Recording server from Analytics**］を選択します。



3. Citrix Analytics から削除した Session Recording サーバーで、次のコマンドを実行します:


```
<Session Recording server installation path>\bin\SsRecUtils.exe -
    Remove_SRCasConfigurations
<!--NeedCopy-->
```

例:

```
C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.
    exe -Remove_SRCasConfigurations
<!--NeedCopy-->
```

データソースのデータ処理をオンまたはオフにする

特定のデータソース（Director および Workspace アプリ）のデータ処理をいつでも停止できます。データソースのサイトカードで縦の省略記号（⋮）をクリックし、[**Turn off data processing**] を選択します。Citrix Analytics は、そのデータソースのデータの処理を停止します。Virtual Apps and Desktops サイトカードからデータ処理を停止することもできます。このオプションは、Director と Workspace アプリの両方のデータソースで使用できます。
データ処理を再度有効にするには、[**Turn On Data Processing**] をクリックします。

構成された **Session Recording** サーバーが接続に失敗する

構成後、Session Recording サーバーが Citrix Analytics に接続できません。したがって、**Session Recording** サイトカードに構成済みのサーバーが表示されません。

この問題のトラブルシューティングを行うには、次の手順を実行します:

1. 構成済みの Session Recording サーバーで、次の PowerShell コマンドを実行してクライアントマシンの ID（CMID）を確認します:

   ```
   Get-WmiObject -class SoftwareLicensingService | select Clientmachineid
   ```

2. CMID が空の場合は、指定したパスに次のレジストリファイルを追加します:

レジストリ名	レジストリのパス	キー型	値
AuditorUniqueID	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\	文字列	UUID を入力します。
EnableCASUseAuditorUniqueID	Computer\HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/SmartAuditor/Server/	REG_DWORD	1

3. 次のサービスを再起動します:
    - Citrix Session Recording Analytics サービス
    - Citrix Session Recording ストレージマネージャー

動的なセッションの録画

February 20, 2024

これまでセッションの録画は、録画ポリシーに合致したセッションの開始時に厳密に開始され、セッションが終了すると厳密に停止しました。

7.18 リリース以降、Citrix では動的なセッションの録画機能が導入されています。この機能を使用すると、セッション中いつでも、特定のユーザーが起動する特定のセッションまたは複数のセッションの録画を開始または停止できます。

> 注:
>
> 機能が正常に動作するために、Session Recording、VDA、Delivery Controller をバージョン 7.18 以降にアップグレードしてください。

動的なセッションの録画を無効または有効にする

Session Recording Agent に、機能を有効または無効にするためのレジストリ値が追加されています。このレジストリ値はデフォルトで **1** に設定されています。つまり、この機能はデフォルトで有効になっています。

この機能を有効または無効にするには、次の手順を実行します:

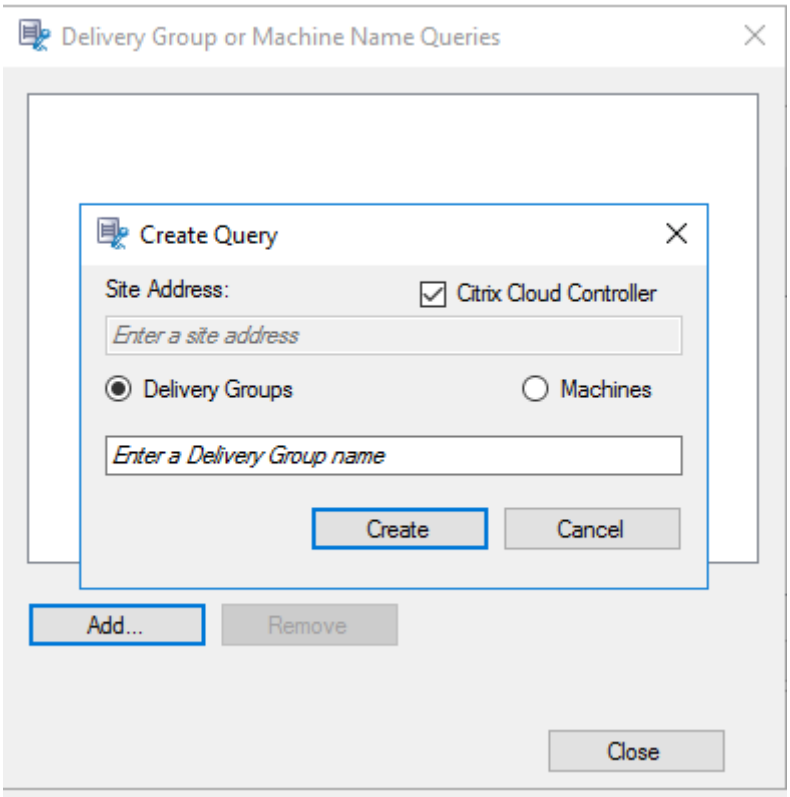
1. Session Recording のインストールを完了後、Session Recording Agent をインストールしたマシンの管理者としてログオンします。
2. レジストリエディターを開きます。
3.「HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor」を参照します。
4. **DynamicControlAllowed** の値を **0** に設定するか、デフォルト値の **1** を使用します。
   1: 動的な録画を有効にする
   0: 動的な録画を無効にする
5. Session Recording Agent を再起動して、設定を機能させます。
   MCS または PVS を使用して展開している場合は、マスターイメージで設定を変更し、更新を実行して変更を有効にします。

> 警告:
>
> レジストリエディターの編集を誤ると、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、シトリックス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。

Citrix SDK で **PowerShell** コマンドを使用して動的に録画を開始または停止する

この動的なセッション録画機能は、オンプレミス環境と Citrix Cloud 環境の両方で使用できます。オンプレミス環境でこの機能を使用するには、Citrix Virtual Apps and Desktops の PowerShell SDK を使用します。Citrix Cloud 環境でこの機能を使用するには、Citrix DaaS Remote PowerShell SDK（旧称 Citrix Virtual Apps and Desktops Remote PowerShell SDK）を使用します。

インストールして使用する SDK を決定するには、録画ポリシーを作成するときに指定した Delivery Controller に注意してください。Citrix Cloud 環境でセッションを録画するために［**Citrix Cloud Controller**］チェックボックスをオンにした場合は、Citrix Cloud 資格情報を検証する必要があります。



> 注:
>
> Citrix DaaS Remote PowerShell SDK を Citrix Cloud Connector マシンにインストールしないでください。同じリソースの場所内のドメイン参加済みマシンには、Remote PowerShell SDK をインストールできます。この SDK のコマンドレットは、Cloud Connector では実行しないことをお勧めします。これは、SDK の操作に Cloud Connector は関係しないためです。

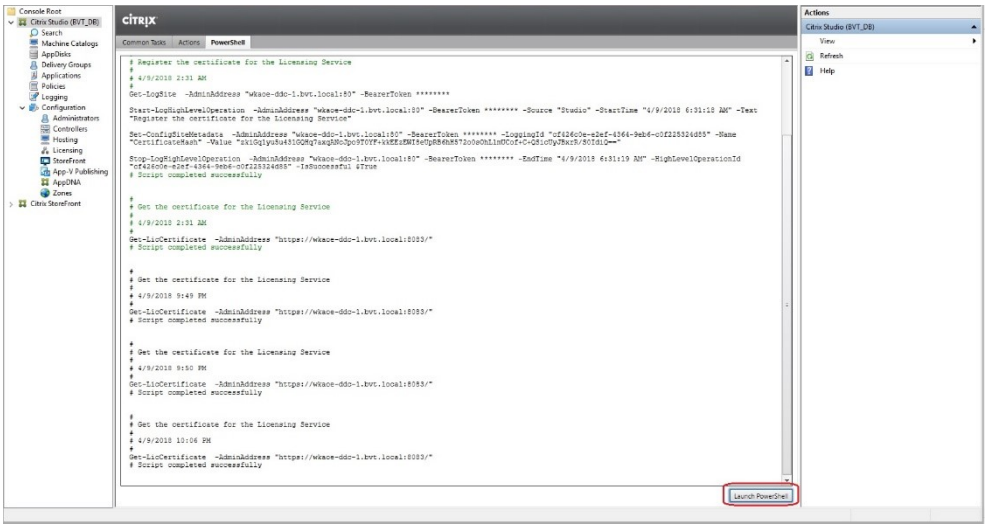
次の表は、動的なセッションの録画のために両方の Citrix SDK で使用できる 3 つの PowerShell コマンドです。

コマンド	説明
Start-BrokerSessionRecording	特定のアクティブなセッション、アクティブなセッション一覧、または特定のユーザーによって開始されたセッションの録画を開始できます。詳しくは、`Get-Help Start-BrokerSessionRecording`を実行してコマンドのオンラインヘルプを参照してください。
Stop-BrokerSessionRecording	特定のアクティブなセッション、アクティブなセッション一覧、または特定のユーザーによって開始されたセッションの録画を停止できます。詳しくは、`Get-Help Stop-BrokerSessionRecording`を実行してコマンドのオンラインヘルプを参照してください。

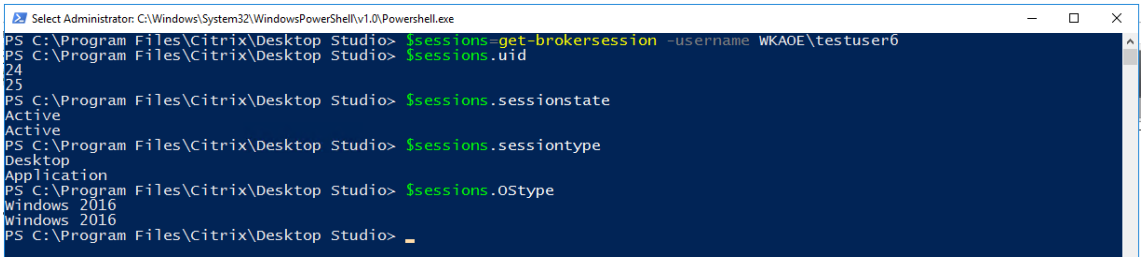
コマンド	説明
Get-BrokerSessionRecordingStatus	特定のアクティブなセッションの録画状態を取得できます。詳しくは、`Get-Help Get-BrokerSessionRecordingStatus`を実行してコマンドのオンラインヘルプを参照してください。

たとえば、ユーザーが問題を報告し、タイムリーなサポートが必要な場合は、この機能を使用して動的にユーザーのアクティブなセッションの録画を開始できます。ライブ録画を再生して、詳細なトラブルシューティングを実行できます。以下の操作を実行できます:

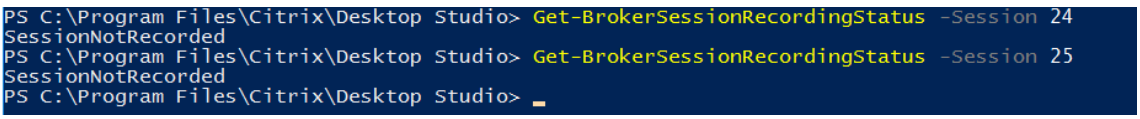
1. (Citrix Virtual Apps and Desktops PowerShell SDK の場合のみ) Citrix Studio コンソールから PowerShell を起動します。



2. ターゲットユーザーのすべてのアクティブなセッションを取得するには、`Get-BrokerSession`コマンドを使用します。



3. `Get-BrokerSessionRecordingStatus`コマンドを使用して、指定したセッションの録画状態を取得します。



> 注:
>
> **-Session** パラメーターには、一度に 1 つのセッション UID のみを使用できます。

4. Start-BrokerSessionRecordingコマンドを使用して、録画を開始します。デフォルトでは、録画操作を通知するメッセージがユーザーに表示されます。

   次の表は、Start-BrokerSessionRecordingコマンドを使用する一般的な例を示しています。

コマンド	説明
`Start-BrokerSessionRecording -User DomainA \ UserA`	DomainA という名前のドメイン内のユーザー（UserA）のすべてのセッションの録画を開始し、UserA に通知します。
`Start-BrokerSessionRecording -User DomainA \ UserA -NotifyUser $false`	DomainA という名前のドメイン内のユーザー UserA のすべてのセッションの録画を開始し、UserA に通知しません。
`Start-BrokerSessionRecording -Sessions $SessionObject`	$SessionObject という名前のオブジェクトのすべてのセッションの録画を開始し、ユーザーに通知します。オブジェクト $SessionObject を取得するには、`$SessionObject=Get-BrokerSession -username UserA`を実行します。オブジェクト名の前にはドル記号（$）が付きます。詳しくは、手順 2 およびコマンドのオンラインヘルプを参照してください。
`Start-BrokerSessionRecording -Sessions uid1,uid2,…,uidn`	セッション（UID1, UID2, …, UIDn）の録画を開始し、ユーザーに通知します。

5. Get-BrokerSessionRecordingStatusコマンドを使用して、各ターゲットセッションの録画状態を取得します。状態は **SessionBeingRecorded** となっているはずです。
6. ライブ録画または完全録画を再生し、詳細なトラブルシューティングを実行します。

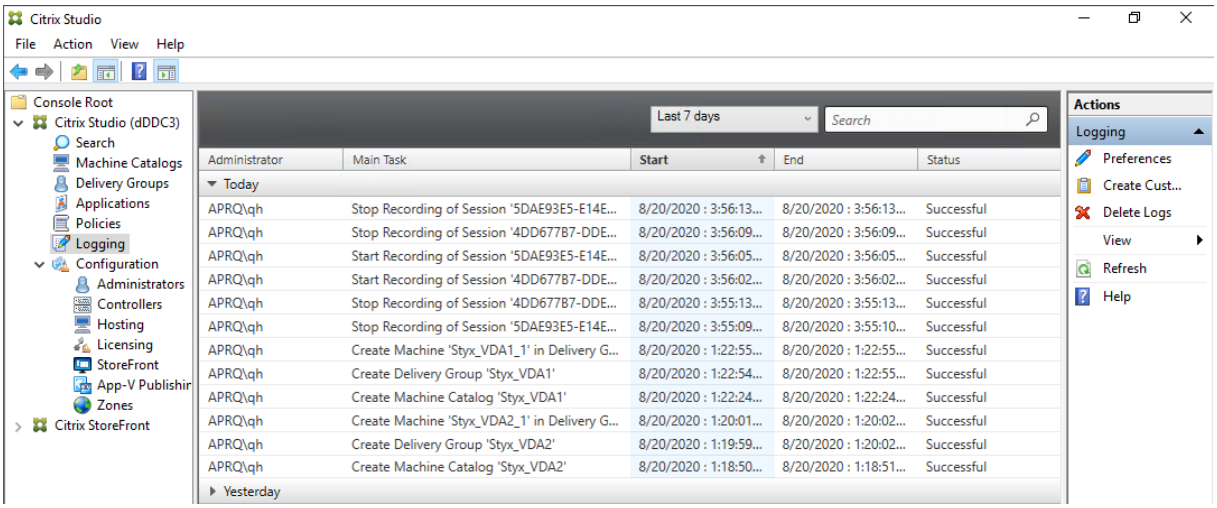
   > 注:
   >
   > Stop-BrokerSessionRecordingコマンドで終了した完全録画を再生すると、Player の進行状況バーでタイムラインの最後のセクションが灰色表示になることがあります。そして、録画されたセッションの最後のセクションがアイドル状態になっています。録画されたセッションに一定のアクティビティがある場合は、明らかではありません。

7. 報告された問題が処理されたか解決された場合、Stop-BrokerSessionRecordingコマンドを使用して録画を停止します。

   次の表は、このコマンドを使用する一般的な例を示しています:

コマンド	説明
`Stop-BrokerSessionRecording -User DomainA\UserA`	DomainA という名前のドメイン内のユーザー（UserA）のすべてのセッションの録画を停止します。
`Stop-BrokerSessionRecording -Sessions $SessionObject`	$SessionObject のすべてのセッションの録画を停止します。
`Stop-BrokerSessionRecording -Sessions uid1,uid2,…,uidn`	セッション（UID1,UID2,…,UIDn）の録画を停止します。

Citrix Studio のログ画面では、`Start-BrokerSessionRecording`コマンドと`Stop-BrokerSessionRecordi`コマンドの結果ログを表示できます。



構成

December 22, 2022

このセクションでは、次の設定を構成するための手順を説明します：

- Session Recording Agent の設定
  - 録画の有効化または無効化
  - Session Recording サーバーとの接続の構成
  - 通信プロトコルの構成
- Session Recording サーバーの設定
  - ユーザーの承認

  - 通知メッセージのカスタマイズ
  - 録画の保存場所の指定
  - 録画のファイルサイズの指定
  - デジタル署名の有効化または無効化
  - CEIP の構成

- ポリシー
  - Session Recording ポリシーの構成
  - 録画の閲覧ポリシーの構成
  - イベント検出ポリシーの構成
  - イベント応答ポリシーの構成

- 高可用性と負荷分散
  - Session Recording サーバーの負荷分散
  - データベース高可用性の構成

Session Recording Agent の設定の構成

December 22, 2022

このセクションでは、次の設定について説明します:

- 録画の有効化または無効化
- Session Recording サーバーとの接続の構成
- 通信プロトコルの構成

録画の有効化または無効化

December 22, 2022

Session Recording Agent は、セッションを録画するマルチセッション OS VDA にインストールします。インストール先の VDA で録画を有効にするかどうかの設定は、Session Recording Agent で行います。録画を有効にすると、Session Recording によりアクティブな録画ポリシーが評価されます。このポリシーにより録画対象のセッションが決定されます。

録画対象以外の VDA ではセッションの録画を無効にすることをお勧めします。録画が行われなくても、パフォーマンスに影響を与えます。

VDA での録画の無効化または有効化

1. Session Recording Agent がインストールされているサーバーにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording Agent** のプロパティ］を選択します。
3. ［**Session Recording**］で ［この **VDA** マシンでセッションを録画する］チェックボックスをオンまたはオフにし、この VDA でセッションを録画できるようにするかを指定します。
4. 確認メッセージが表示されるので、Session Recording Agent サービスを再起動して変更を受け入れます。

> 注:
>
> Session Recording をインストールしたときにアクティブになっているポリシーは「録画しない」ポリシーです。どのサーバーのセッションも録画されません。録画を開始するには、Session Recording ポリシーコンソールを使用して別のポリシーをアクティブにします。

カスタムイベントの記録の有効化

Session Recording では、サードパーティ製のアプリケーションを使用して、イベントとして知られるカスタムデータを録画されたセッションに挿入することができます。これらのイベントは、録画されたセッションが再生されるときに表示されます。イベントはセッションの録画ファイルの一部であり、セッションの録画後に変更することはできません。

たとえば、イベントに「ユーザーが Web ブラウザーを開きました」というテキストが含まれることがあります。セッションの録画中、ユーザーがブラウザーを開くたびに、このテキストが録画に挿入されます。閲覧者は録画されたセッションを再生するときにマーカーの数をメモしておくと、ユーザーがブラウザーを開いた回数を数えることができます。

サーバー上の録画にカスタムイベントを挿入するには:

- ［**Session Recording Agent** のプロパティ］を使用して、カスタムイベントを挿入する各サーバーで設定を有効にします。サーバーは個別に有効にします。サイト内のすべてのサーバーをまとめて有効にすることはできません。
- イベント API に基づくアプリケーションを開発します。このアプリケーションを各エンドユーザーの仮想セッションで実行し、録画にデータを挿入します。

Session Recording のインストールにはイベント録画 COM アプリケーション（API）が含まれており、サードパーティ製のアプリケーションからテキストを録画に挿入することができます。Visual Basic、C++、または C# を含む、多くのプログラミング言語で API を使用できます。詳しくは、Knowledge Center の記事CTX226844を参照してください。Session Recording イベント API の DLL は Session Recording の一部としてインストールされます。DLL は`C:\rogram Files\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll`で見つけることができます。

サーバーでカスタムイベントの録画を有効にするには、以下の手順を実行します:

1. Session Recording Agent がインストールされているサーバーにログオンします。

2. ［スタート］ボタンをクリックし、［**Session Recording Agent** のプロパティ］を選択します。
3. ［**Session Recording Agent** のプロパティ］で、［録画］タブをクリックします。
4. ［カスタムイベントの記録］で ［このサーバーでサードパーティ製アプリケーションによるカスタムデータの記録を許可する］チェックボックスをオンにします。

Session Recording サーバーとの接続の構成

December 22, 2022

Session Recording Player から **Session Recording** サーバーへの接続の構成

Session Recording Player でセッションを再生する前に、録画されたセッションを格納する Session Recording サーバーとの接続を構成します。Player ごとに複数の Session Recording サーバーとの接続を構成できますが、同時に複数の Session Recording サーバーに接続することはできません。Player を複数の Session Recording サーバーと接続できるように構成する場合、ユーザーは Player の接続先の Session Recording サーバーを変更できます。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. Session Recording Player を起動します。
3. Session Recording Player のメニューバーで、［ツール］**>**［オプション］の順に選択します。
4. ［接続］タブで ［追加］をクリックします。
5. ［ホスト名］フィールドに、Session Recording サーバーをホストするマシンの名前か IP アドレスを入力し、プロトコルを選択します。デフォルトでは、セキュリティで保護された通信のため HTTPS/SSL を使用するように Session Recording が構成されます。SSL が構成されていない場合は、HTTP を選択します。
6. Session Recording Player が複数の Session Recording サーバーと接続できるように構成するには、Session Recording サーバーごとに手順 4 および 5 を繰り返します。
7. 接続する Session Recording サーバーのチェックボックスがオンになっていることを確認します。

Session Recording Agent から **Session Recording** サーバーへの接続の構成

接続は通常、Session Recording Agent をインストールするときに構成されます。Session Recording Agent をインストールした後でこの接続を設定するには、［**Session Recording Agent** のプロパティ］を使用します。

1. Session Recording Agent がインストールされているサーバーにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording Agent** のプロパティ］を選択します。
3. ［接続］タブをクリックします。

4. [**Session Recording** サーバー] フィールドで、Session Recording サーバーの完全修飾ドメイン名 (FQDN) を入力します。

   > 注:
   >
   > HTTPS 接続でメッセージキューを使用するには、[**Session Recording** サーバー] フィールドに完全修飾ドメイン名を入力します (デフォルトでは TCP を使用)。入力しない場合、Session Recording は失敗します。

5. [**Session Recording** ストレージマネージャーメッセージのキュー] で、Session Recording ストレージマネージャーが通信に使用するプロトコルを選択し、必要であればデフォルトのポート番号を変更します。

   > 注:
   >
   > HTTP および HTTPS 経由でメッセージキューを使用するには、IIS 推奨機能をすべてインストールします。

6. [メッセージの有効期間] フィールドで、通信エラーが発生したときにキューに各メッセージを保持する秒数として、デフォルトの 7,200 秒 (2 時間) を受け入れるか、新しい値を入力します。この期間が経過すると、メッセージは削除され、ファイルを再生できるのはデータが失われた時点までになります。
7. [**Session Recording Broker**] で、Session Recording Broker が通信に使用するプロトコルを選択し、必要であればデフォルトのポート番号を変更します。
8. 確認メッセージが表示されるので、**Session Recording Agent** サービスを再起動して変更を受け入れます。

通信プロトコルの変更

December 22, 2022

セキュリティ上の理由から、HTTP を通信プロトコルに使用することは Citrix ではお勧めしません。デフォルトでは、Session Recording は HTTPS を使用して通信するように設定されます。HTTPS ではなく HTTP を使用する場合は、いくつかの設定を変更する必要があります。

HTTP を通信プロトコルに使用する

1. Session Recording サーバーをホストするマシンにログオンし、IIS で Session Recording Broker との接続に使用しているセキュリティで保護された接続を無効にします。
2. Session Recording Agent がインストールされている各サーバーの [**Session Recording Agent** のプロパティ] でプロトコル設定を HTTPS から HTTP に次の手順に従って変更します:

   a) Session Recording Agent がインストールされている各サーバーにログオンします。
   b) [スタート] ボタンをクリックし、[**Session Recording Agent** のプロパティ] を選択します。

c) [**Session Recording Agent** のプロパティ] で、[接続] タブを選択します。
d) [**Session Recording Broker**] で [プロトコル] ボックスの一覧から [**HTTP**] を選択し、[**OK**] をクリックして変更を受け入れます。サービスの再起動を促すメッセージが表示されたら、[はい] をクリックします。

3. Session Recording Player の設定で、プロトコルを HTTPS から HTTP に変更します:

a) Session Recording Player がインストールされている各ワークステーションにログオンします。
b) [スタート] メニューの [**Session Recording Player**] を選択します。
c) [**Session Recording Player**] メニューバーで [ツール] > [オプション] > [接続] の順に選択し、サーバーを選択して [変更] をクリックします。
d) [プロトコル] ボックスの一覧から [**HTTP**] を選択し、[**OK**] を 2 回クリックして、変更を受け入れてダイアログボックスを閉じます。

4. Session Recording ポリシーコンソールの設定で、プロトコルを HTTPS から HTTP に変更します:

a) Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
b) [スタート] ボタンをクリックし、[**Session Recording** ポリシーコンソール] を選択します。
c) [プロトコル] ボックスの一覧から [**HTTP**] を選択し、[**OK**] をクリックして接続します。接続が確立するとこの設定が保存され、次に Session Recording ポリシーコンソールを起動するときにも使用されます。

通信プロトコルを **HTTPS** に戻す

1. Session Recording サーバーをホストするマシンにログオンし、IIS で Session Recording Broker との接続に使用しているセキュリティで保護された接続を有効にします。
2. Session Recording Agent がインストールされている各サーバーの [**Session Recording Agent** のプロパティ] でプロトコル設定を HTTP から HTTPS に変更します:

a) Session Recording Agent がインストールされている各サーバーにログオンします。
b) [スタート] ボタンをクリックし、[**Session Recording Agent** のプロパティ] を選択します。
c) [**Session Recording Agent** のプロパティ] で、[接続] タブを選択します。
d) [**Session Recording Broker**] で [プロトコル] ボックスの一覧から [**HTTPS**] を選択し、[**OK**] をクリックして変更を受け入れます。サービスの再起動を促すメッセージが表示されたら、[はい] をクリックします。

3. Session Recording Player の設定で、プロトコルを HTTP から HTTPS に変更します:

a) Session Recording Player がインストールされている各ワークステーションにログオンします。
b) [スタート] メニューの [**Session Recording Player**] を選択します。
c) [**Session Recording Player**] メニューバーで [ツール] > [オプション] > [接続] の順に選択し、サーバーを選択して [変更] をクリックします。
d) [プロトコル] ボックスの一覧から [**HTTPS**] を選択し、[**OK**] を 2 回クリックして、変更を受け入れてダイアログボックスを閉じます。

4. Session Recording ポリシーコンソールの設定で、プロトコルを HTTP から HTTPS に変更します:

   a) Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
   b) [スタート] ボタンをクリックし、[**Session Recording** ポリシーコンソール] を選択します。
   c) [プロトコル] ボックスの一覧から [**HTTPS**] を選択し、[**OK**] をクリックして接続します。接続が確立するとこの設定が保存され、次に Session Recording ポリシーコンソールを起動するときにも使用されます。

Session Recording サーバーの設定の構成

December 22, 2022

このセクションでは、次の設定について説明します:

- ユーザーの承認
- 通知メッセージのカスタマイズ
- 録画の保存場所の指定
- 録画のファイルサイズの指定
- デジタル署名の有効化または無効化
- CEIP の構成

ユーザーの承認

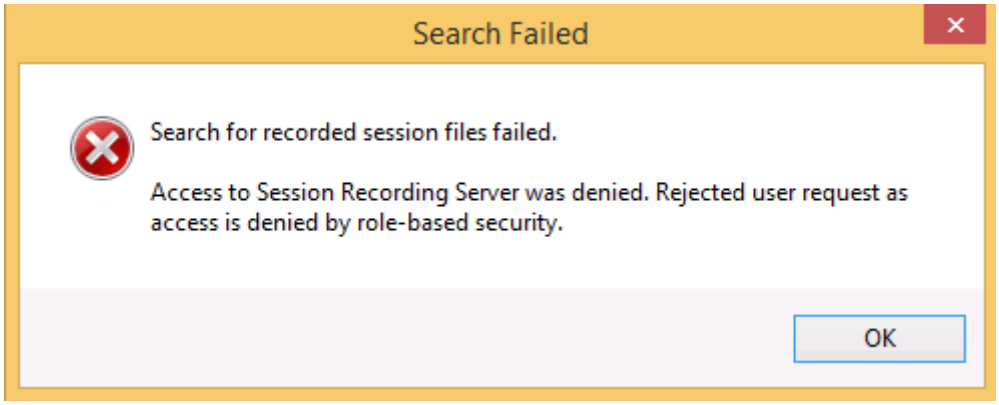
February 20, 2024

ユーザーに権限を付与するには、Session Recording サーバーをホストするコンピューターで Session Recording 承認コンソールを使用して役割（ロール）を割り当てます。5 つのロールがあります:

> 重要:
>
> セキュリティ上の理由から、セッションの録画の表示など、特定の機能を実行するために必要な権限のみをユーザーに付与します。

- **PolicyAdministrator**。録画ポリシーの表示、作成、編集、削除、および有効化を実行できます。デフォルトでは、Session Recording サーバーをホストするマシンの管理者がこのロールのメンバーです。
- **PolicyQuery**。Session Recording Agent をホストするサーバーで録画ポリシーの評価を要求できます。デフォルトでは、認証ユーザーがこのロールのメンバーです。
- **LoggingWriter**。管理者ログを書き込む権限を付与します。デフォルトでは、ローカル管理者および Network Service グループがこのロールのメンバーです。デフォルトの **LoggingWriter** メンバーシップを変更すると、ログの書き込みが失敗する原因となる可能性があります。

- **LoggingReader**。管理者ログを照会する権限を付与します。デフォルトでこのロールのメンバーになるユーザーはありません。
- **PrivilegedPlayer**。録画のアクセス制限を設定および削除する権限と、録画をアーカイブおよび削除する権限を付与します。
- **Player**。録画した Citrix Virtual Apps and Desktops および Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）セッションを表示する権限を付与します。デフォルトでこのロールのメンバーになるユーザーはありません。Session Recording のデフォルト設定では、どのユーザーにも録画したセッションを再生する権限はありません。録画したセッションを再生する権限がないユーザーが録画したセッションを再生しようとすると次のエラーメッセージが表示されます：



ユーザーをロールに割り当てるには、次の手順を実行します：

1. Session Recording サーバーをホストするマシンに管理者としてログオンします。
2. Session Recording 承認コンソールを起動します。
3. ユーザーを割り当てるロールを選択します。
4. メニューバーで、［操作］**>**［ユーザーとグループの割り当て］の順に選択します。
5. ユーザーとグループを追加します。

Session Recording では、Active Directory で定義されるユーザーおよびグループがサポートされます。

管理コンソールで加えた変更は、1 分間隔の更新時に有効になります。また 1906 リリース以降、Session Recording ポリシーコンソールで録画の閲覧ポリシーを作成できます。詳しくは、「録画の閲覧ポリシー」を参照してください。

Citrix カスタマーエクスペリエンス向上プログラム（**CEIP**）の構成

April 3, 2024

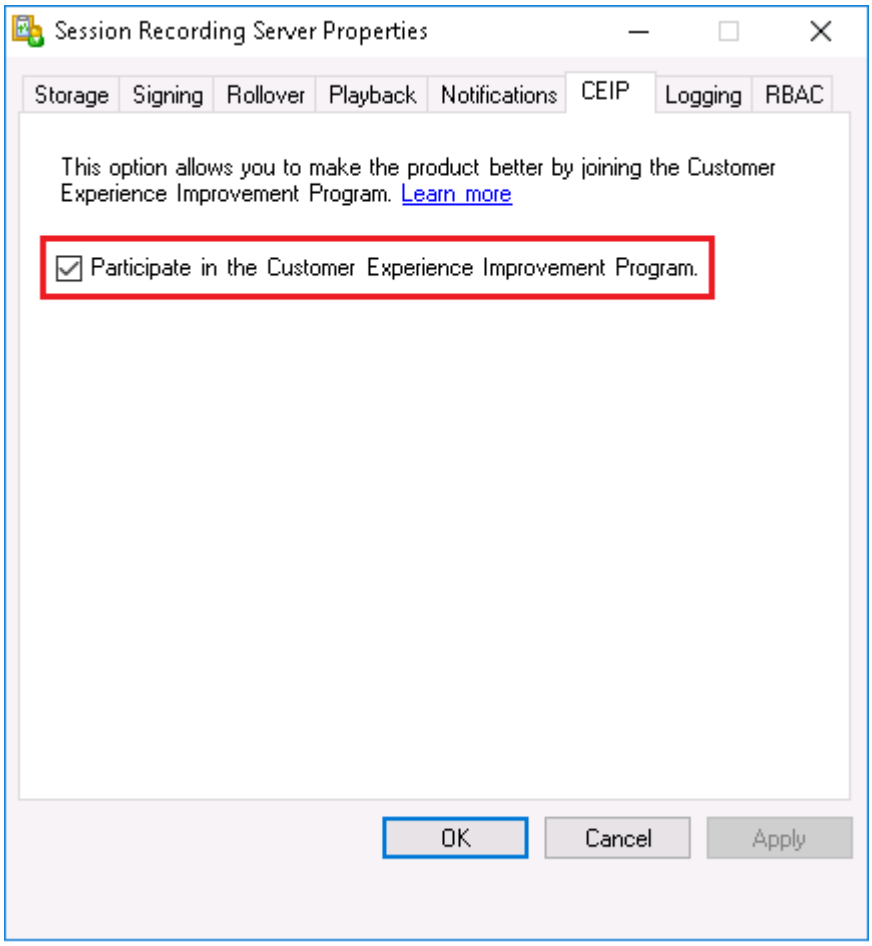
Citrix カスタマーエクスペリエンス向上プログラム（CEIP）に参加すると、匿名の構成データおよび使用状況データが収集および送信されます。データは、製品の品質とパフォーマンスの向上に役立ちます。この匿名データのコピーは、より迅速かつ効率的に分析するために Google Analytics にも送信されます。

設定

CEIP の設定

デフォルトでは、ユーザーは Session Recording のインストール時に CEIP に自動で参加します。Session Recording のインストールからおよそ 7 日後に、初回データアップロードが行われます。CEIP のサブスクリプションを解除するには、以下を実行します:

1. Session Recording サーバーをホストするマシンにログオンします。
2. [スタート] ボタンをクリックし、[**Session Recording** サーバーのプロパティ] を選択します。
3. [**Session Recording** サーバーのプロパティ] で、[**CEIP**] タブをクリックします。
4. [カスタマーエクスペリエンス向上プログラムに参加する] チェックボックスをオフにします。
5. **Citrix Session Recording Analytics** サービスを再起動して、設定を有効にします。



Google Analytics の設定

Google Analytics を有効にすると、Google Analytics と Session Recording サーバーとの間のハートビートデータが 5 時間ごとに収集されます。Web Player のユーザー行動データも Google Analytics に送信されます。ユーザー行動には、Web Player を開く、Web Player で録画を再生および検索するなどのアクティビティが含まれます。

Google Analytics を有効または無効にするレジストリ設定（デフォルトは 0）:

場所：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\

名前：CeipHeartBeatDisable

値のデータ：1 = 無効、0 = 有効

未指定の場合、Google Analytics は有効です。

Google Analytics を無効にするには:

1. Session Recording サーバーをホストするマシンにログオンします。
2. レジストリエディターを開きます。
3. 「HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\」を参照します。
4. レジストリ値を追加して「**CeipHeartBeatDisable**」という名前を指定します。
5. **CeipHeartBeatDisable** の値を 1 に設定します。
6. Citrix Session Recording Analytics サービスを再起動して、設定を有効にします。

Session Recording サーバーから収集されるデータ

次の表では、収集される匿名の情報の種類の例を紹介します。データでは、お客様を特定するすべての詳細は含まれません。

データポイント	キー名	説明
マシンのグローバル一意識別子	machine_guid	データの発生元のマシンを識別。Google Analytics を有効にすると、CEIP が有効になっていなくてもハートビートデータが Google Analytics に送信されます。

データポイント	キー名	説明
オペレーティングシステムのバージョン	OS_version	マシンのオペレーティングシステムを示すテキスト文字列。Google Analytics を有効にすると、CEIP が有効になっていなくてもハートビートデータが Google Analytics に送信されます。
Session Recording サーバーのバージョン	SRS_version	インストールされている Session Recording サーバーのバージョンを示すテキスト文字列。Google Analytics を有効にすると、CEIP が有効になっていなくてもハートビートデータが Google Analytics に送信されます。
アプリケーションの録画数	application-recording-number	アプリケーションの録画ファイルの数を示す整数。Google Analytics と CEIP の両方が有効な場合、データが送信されます。
録画数	recording-number	アプリケーションとデスクトップ両方の録画ファイルの数を示す整数。Google Analytics と CEIP の両方が有効な場合、データが送信されます。
動的な録画の数	dynamic-recording-number	動的に録画されたファイルの数を示す整数。Google Analytics と CEIP の両方が有効な場合、データが送信されます。
録画されたセッションをホストするエージェントの数	recorded-agent-number	録画されたセッションをホストする VDA の数を示す整数。Google Analytics と CEIP の両方が有効な場合、データが送信されます。
(ログ記録されたイベントを含む）録画されたセッションをホストするエージェントの数	event-logging-enabled-agent-number	(ログ記録されたイベントを含む）録画されたセッションをホストする VDA の数を示す整数。Google Analytics と CEIP の両方が有効な場合、データが送信されます。

データポイント	キー名	説明
（ログ記録されたイベントを含む）録画の数	event-logging-recording-number	（ログ記録されたイベントを含む）録画ファイルの数を示す整数。Google Analytics と CEIP の両方が有効な場合、データが送信されます。
管理者ログの有効化	admin-logging-status	管理者ログの有効化を示す数字。「1」は有効を「0」は無効を意味します。Google Analytics と CEIP の両方が有効な場合、データが送信されます。
ログ記録されたイベントの数	collected-events-number	ログ記録されたイベントの数を示す整数。Google Analytics と CEIP の両方が有効な場合、データが送信されます。
カスタムポリシーの数	customized-policies-number	カスタム Session Recording ポリシーおよびイベントログポリシーの数を示す整数。Google Analytics と CEIP の両方が有効な場合、データが送信されます。
負荷分散の有効化	load-balancing-status	負荷分散の有効化を示す数字。「1」は有効を「0」は無効を意味します。Google Analytics と CEIP の両方が有効な場合、データが送信されます。
録画の閲覧ポリシーの有効化	rbac-status	録画の閲覧ポリシーの有効化を示す数字。「1」は有効を「0」は無効を意味します。Google Analytics と CEIP の両方が有効な場合、データが送信されます。

通知メッセージのカスタマイズ

April 3, 2024

アクティブな録画ポリシーが通知オンの状態でセッションを録画する場合、ユーザーは資格情報を入力した後に録画通知を受け取ります。デフォルトの通知メッセージは「現在開始しているデスクトップまたはプログラムでの操作

を録画しています。この条件に不服である場合は、デスクトップまたはプログラムを閉じてください。ユーザーが［**OK**］をクリックすると、ウィンドウが閉じセッションを続行できます。

デフォルトの通知メッセージは、VDA のオペレーティングシステムの言語で表示されます。

選択した言語でカスタム通知を作成できます。ただし、作成できる通知メッセージは言語ごとに 1 つのみです。ユーザーには、ユーザーが選択したローカル設定の言語で通知メッセージが表示されます。

通知メッセージの作成

1. Session Recording サーバーをホストするマシンにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** サーバーのプロパティ］を選択します。
3. ［**Session Recording** サーバーのプロパティ］で、［通知］タブをクリックします。
4. ［追加］をクリックします。
5. メッセージで使用する言語を選択し、新しいメッセージを入力します。1 つの言語につき作成できるメッセージは 1 つです。

新しいメッセージを受け入れてアクティブにすると、
［言語特有の通知メッセージ］ボックスに表示されます。

デジタル署名の有効化または無効化

December 22, 2022

Session Recording サーバーと Session Recording Player をインストールしたマシンに、証明書をインストールできます。証明書をインストールすることで、Session Recording にデジタル署名を割り当て、環境のセキュリティを強化できます。

デフォルトで、デジタル署名は無効になっています。録画に署名する証明書を選択すると、Session Recording から Session Recording ストレージマネージャーサービスに読み取り権限が付与されます。

デジタル署名の有効化

1. Session Recording サーバーをホストするマシンにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** サーバーのプロパティ］を選択します。
3. ［**Session Recording** サーバーのプロパティ］で、［署名］タブをクリックします。
4. Session Recording コンポーネントをインストールしたマシンの間で保護された通信を有効にする証明書を参照します。

デジタル署名の無効化

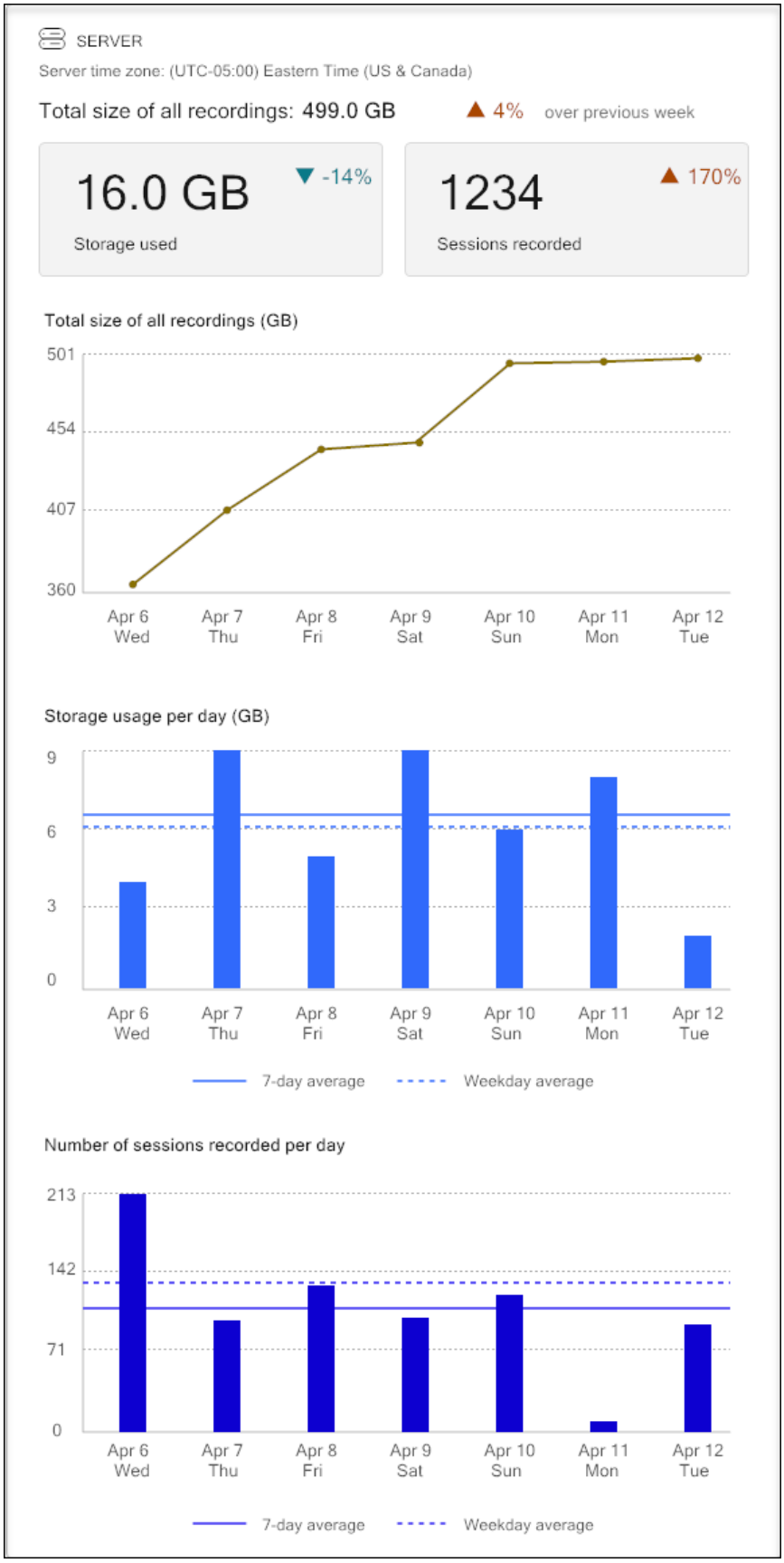
1. Session Recording サーバーをホストするマシンにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** サーバーのプロパティ］を選択します。
3. ［**Session Recording** サーバーのプロパティ］で、［署名］タブをクリックします。
4. ［消去］をクリックします。

Session Recording ストレージレポート

February 20, 2024

概要

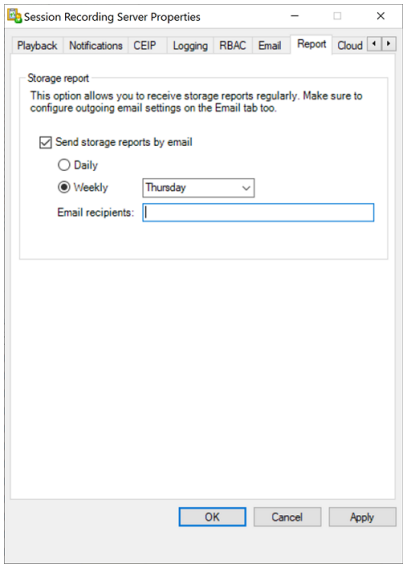
Session Recording ストレージレポートは、単一または複数の負荷分散された Session Recording サーバーの画面記録に関して、週次統計を提供します。メールで受信するこのレポートには、次のようなダイジェストチャートが含まれます:



構成

メールで送信された Session Recording ストレージレポートを日次または週次で受信するには、Session Recording サーバーのプロパティを使用してレポートをスケジュールします。[**Email**] タブでも送信メール設定を構成してください。

> 注:
>
> Session Recording サーバーが負荷分散方式で構成されている場合は、サーバーの 1 つでレポートをスケジュールします。それ以外の場合は、各 Session Recording サーバーでスケジュールを作成します。



録画のファイルサイズの指定

February 20, 2024

録画ファイルのサイズが大きくなるにつれて、ダウンロードに時間がかかり、再生中にシークスライダーを使用して再生箇所を変更するときに反応が遅くなります。ファイルサイズを制御するにはファイルのしきい値を指定します。録画ファイルがこの限界に達すると、Session Recording によってファイルが閉じられ、録画を続行するために追加のファイルが作成されます。この操作をロールオーバーと呼びます。

ロールオーバーのため、2 つのしきい値を指定できます:

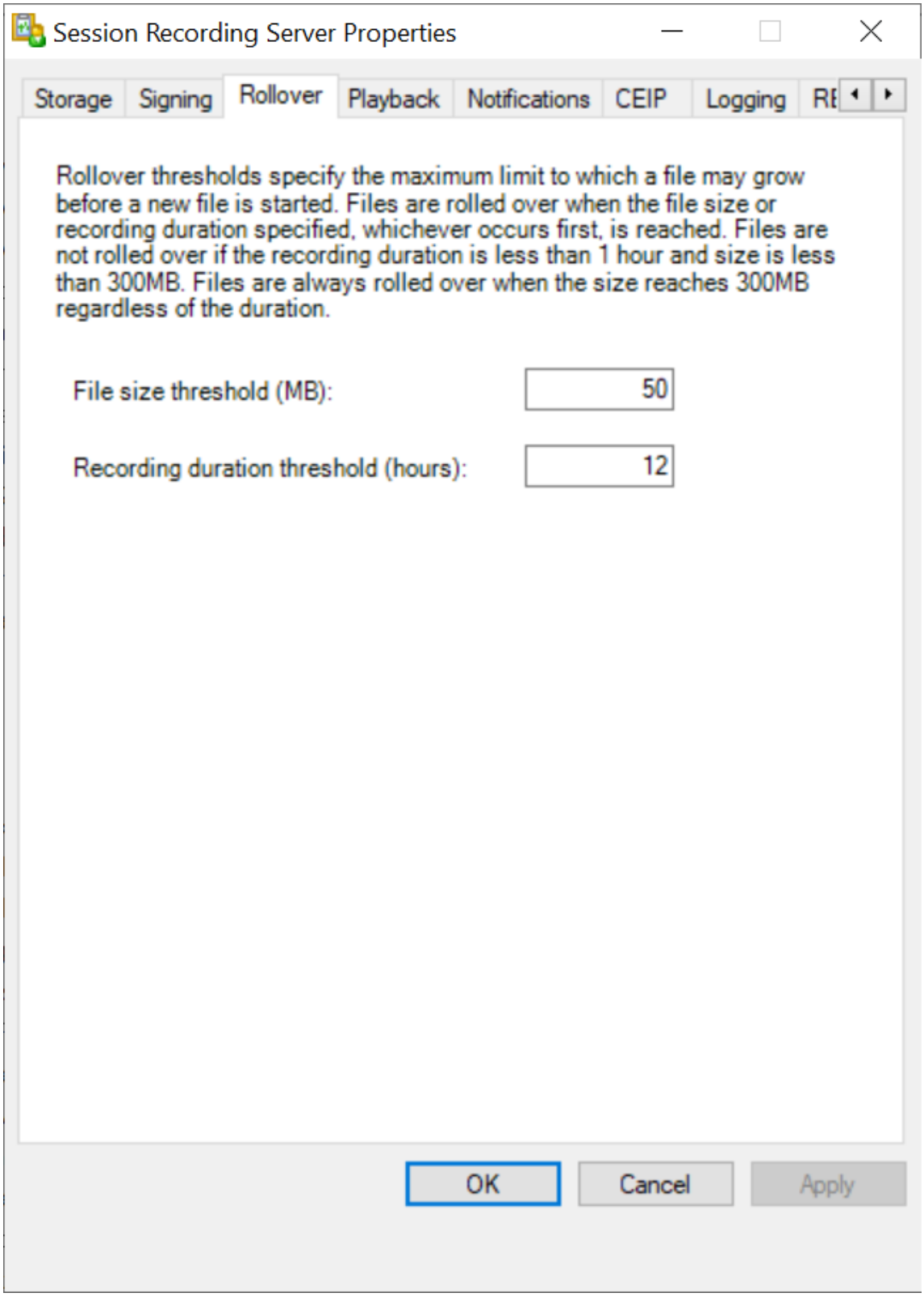
- ファイルサイズ。このサイズに達すると現在のファイルが閉じ、新しいファイルが開きます。デフォルトでは、ロールオーバーはサイズが 50MB を超えると発生します。サポートされる値は、0〜300 です。
- 時間。この時間に達すると、現在のファイルが閉じ、新しいファイルが開きます。デフォルトでは、セッションが 12 時間録画されるとロールオーバーが発生します。サポートされる値は、1〜24 です。

ロールオーバーは、上記の 2 つの条件の最初の 1 つが満たされたときに発生します。たとえば、サイズとして 17MB、時間として 6 時間を指定したとします。録画ファイルが 3 時間で 17MB に達すると、Session Recording によりファイルが閉じられ、新しいファイルが開きます。

多くの小さなファイルが作成されないように、ファイルサイズに指定された値にかかわらず、少なくとも 1 時間が経過するまでロールオーバーは起こりません。この規則の例外は、ファイルサイズが 300MB を超えた場合です。

録画の最大ファイルサイズの指定

1. Session Recording サーバーをホストするマシンにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** サーバーのプロパティ］を選択します。
3. ［**Session Recording** サーバーのプロパティ］で、［ロールオーバー］タブをクリックします。



4. 10 から 300 の間の整数を入力して、ファイルサイズの上限を MB 単位で指定します。
5. 1 から 24 の間の整数を入力して、録画時間の上限を時間単位で指定します。

録画の保存場所の指定

February 20, 2024

［**Session Recording** サーバーのプロパティ］を使用して、録画の格納先とアーカイブされた録画の再生時の復元先を指定します。

ローカルドライブ、SAN ボリューム、および UNC ネットワークパスで指定する場所に録画を格納できます。バージョン 2103 以降、録画を Azure ファイル共有に格納できます。詳しくは、後述の「録画を保存するための Azure ファイル共有を構成する」を参照してください。

> 注:
>
> - SMB や NFS などのファイルベースのプロトコルで NAS にデータを格納すると、パフォーマンスとセキュリティ上の問題が発生する可能性があります。最新バージョンのプロトコルを使用してセキュリティ上の問題を回避し、スケールテストを実行して適切なパフォーマンスを確保します。
> - ファイルをアーカイブする、または削除されたファイルを復元するには、ICLDBコマンドを使用します。

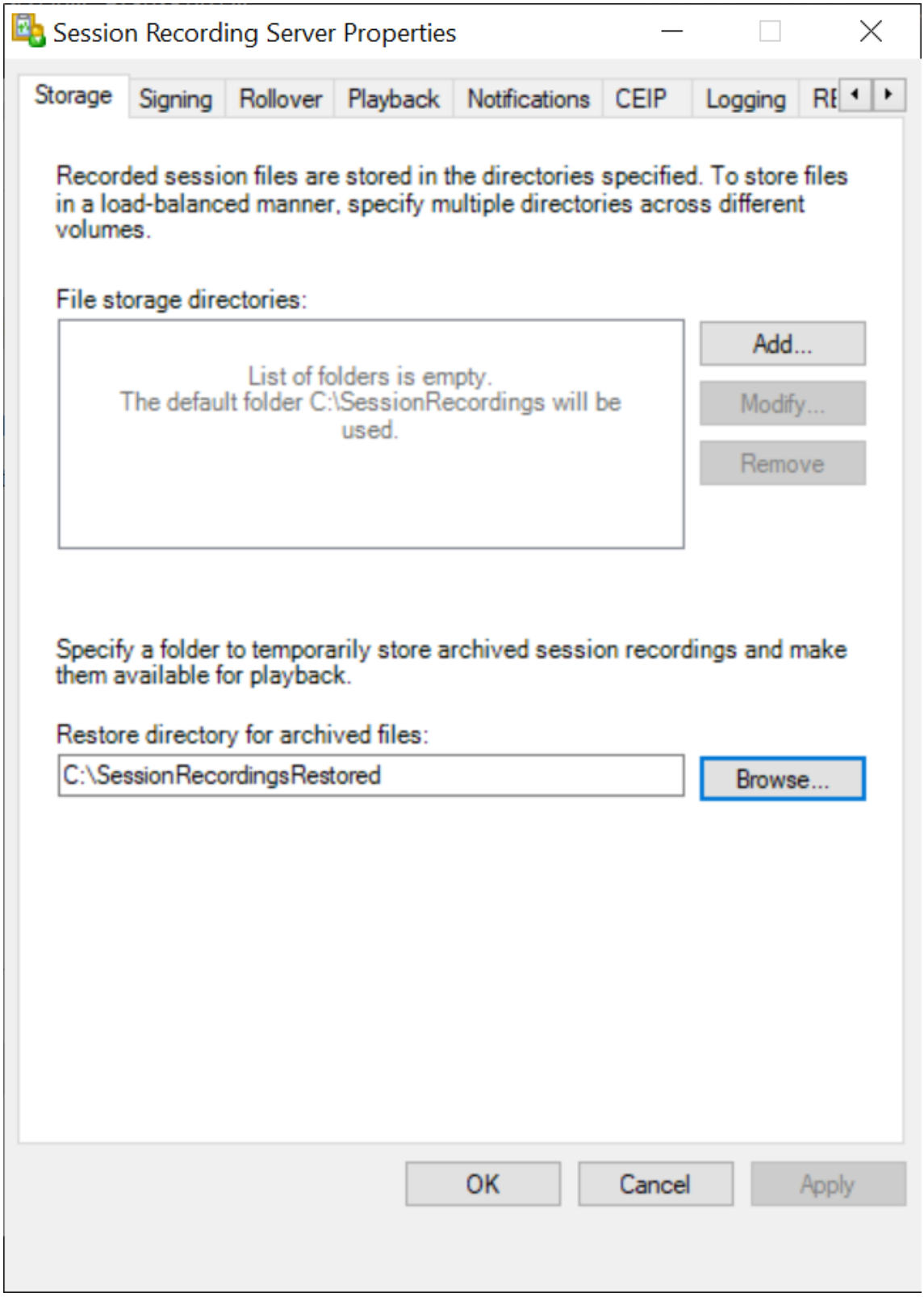
録画を格納するための **1** つまたは複数のフォルダーと、アーカイブされた録画を復元するためのフォルダーを **1** つ指定する

1. Session Recording サーバーをホストするマシンにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** サーバーのプロパティ］を選択します。
3. ［**Session Recording** サーバーのプロパティ］で、［格納場所］タブをクリックします。
4. ［ファイル格納フォルダー］ボックスの一覧を使用して、録画を格納するフォルダーを管理します。

   フォルダーを選択すると、それらのフォルダーにフルコントロール権限のサービスが付与されます。

   デフォルトでは、録画は Session Recording サーバーをホストするマシンの「**<drive>:SessionRecordings**」フォルダーに格納されます。録画を保存するフォルダーを変更したり、複数のボリューム間で負荷分散をするため、またはより多くの容量を活用するために、フォルダーを追加したりできます。複数のフォルダーが一覧にある場合は、録画がフォルダー間で負荷分散されていることを示します。負荷分散は各フォルダーを循環して行われます。
5. ［アーカイブ済みファイルの復元フォルダー］ボックスに、アーカイブ済み録画を復元するフォルダーを入力します。

   デフォルトでは、アーカイブ済み録画は Session Recording サーバーをホストするマシンの「**<drive>:SessionRecordingsRestore**」フォルダーに復元されます。フォルダーを変更できます。



録画を保存するための **Azure** ファイル共有を構成する

録画を保存するための Azure ファイル共有を作成するには、次の手順を実行します:

1. Azure Portalで、ストレージアカウントを作成してから、Azure ファイル共有を作成します。

   クイックスタートガイドについては、Azure Portal を使用したAzure ファイル共有の作成および管理を参照してください。次の表は、検討すべきお勧めの構成です。

録画ファイルサイズ（MB/時間）	セッション数	ファイル共有タイプ	ファイル共有クォータ（TB）	Session Recording サーバーの数	Session Recording サーバーのサイズ
< 6.37	< 1,000	HDD Standard (StorageV2)	2	1	Standard D4as_v4
< 6.37	1,000～2,000	SSD Premium	3	1	Standard D4as_v4
< 6.37	2,000～3,000	SSD Premium	5	1	Standard D4as_v4
< 6.37	3,000～4,000	SSD Premium	6	1	Standard D4as_v4
約 10	< 1,000	HDD Standard (StorageV2)	3	1	Standard D4as_v4
約 10	1,000～2,500	SSD Premium	6	1	Standard D4as_v4
約 10	2,500～4,000	SSD Premium	10	2	Standard D4as_v4

   ファイル共有クォータは、1 日あたり 8 時間、1 か月あたり 23 営業日、各録画ファイルの 1 か月の保有期間に基づいて計算されます。

2. Session Recording サーバーをインストールしたホストに、Azure ファイル共有の資格情報を追加します。

   a) 管理者としてコマンドプロンプトを起動し、ドライブを **<Session Recording** サーバーのパス **>\Bin** フォルダーに変更します。

      デフォルトでは、Session Recording サーバーは`C:\Program Files\Citrix\SessionRecording\Server`にインストールされています。

   b)「**SsRecUtils.exe -AddAzureFiles <storageAccountName> <fileShareName> <accesskey>**」コマンドを実行します。

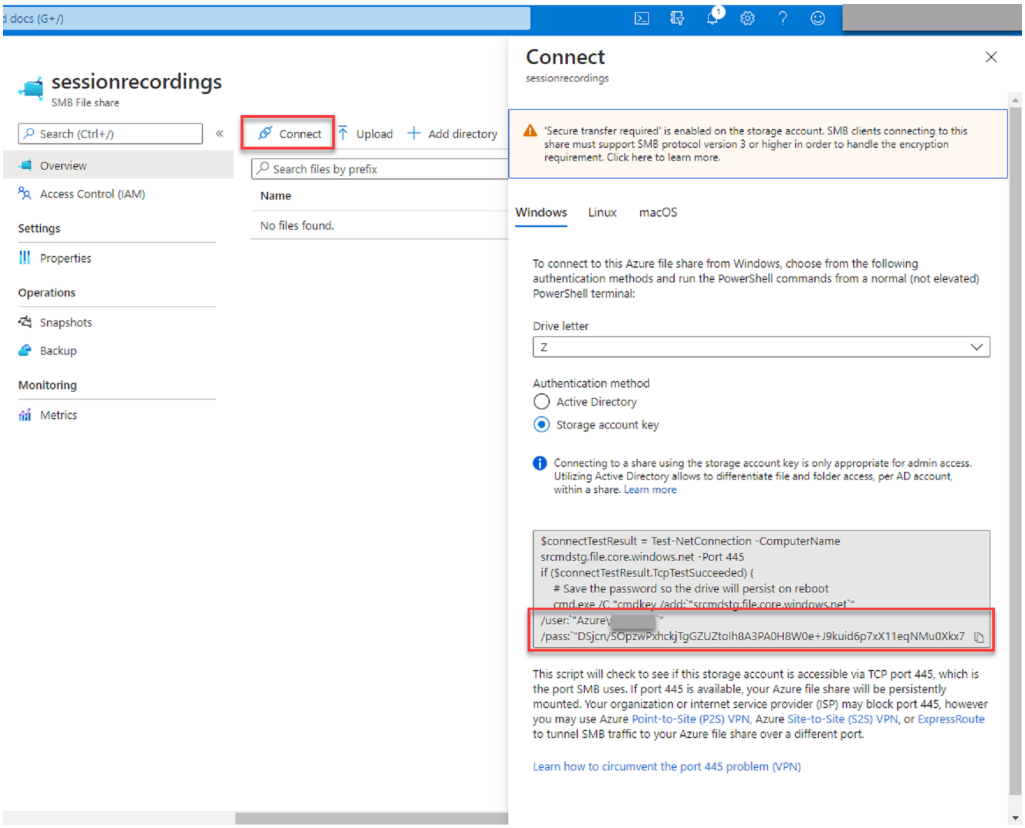
      各項目の意味は次のとおりです。

      - **<storageaccountname>** は、Azure のストレージアカウントの名前です。

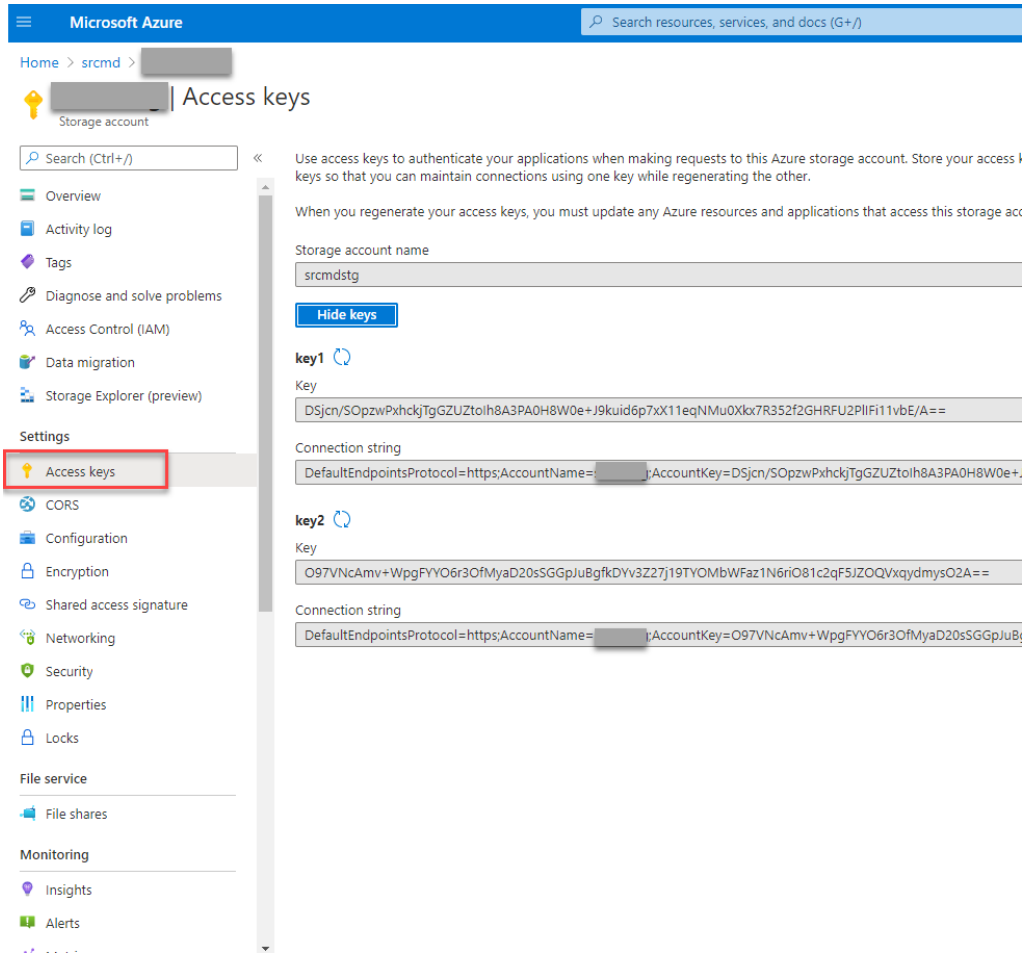
- **<filessharename>** は、ストレージアカウントに含まれるファイル共有の名前です。
- **<accesskey>** は、ファイル共有へのアクセスに使用できるストレージアカウントキーです。

ストレージアカウントキーを取得するには、次の 2 つの方法があります:

- ストレージアカウントキーは、ファイル共有ページの ［**Connect**］アイコンをクリックしたときに表示される接続文字列から取得できます。



- ストレージアカウントページの左側のナビゲーションにある ［**Access keys**］をクリックして、ストレージアカウントキーを取得することもできます。



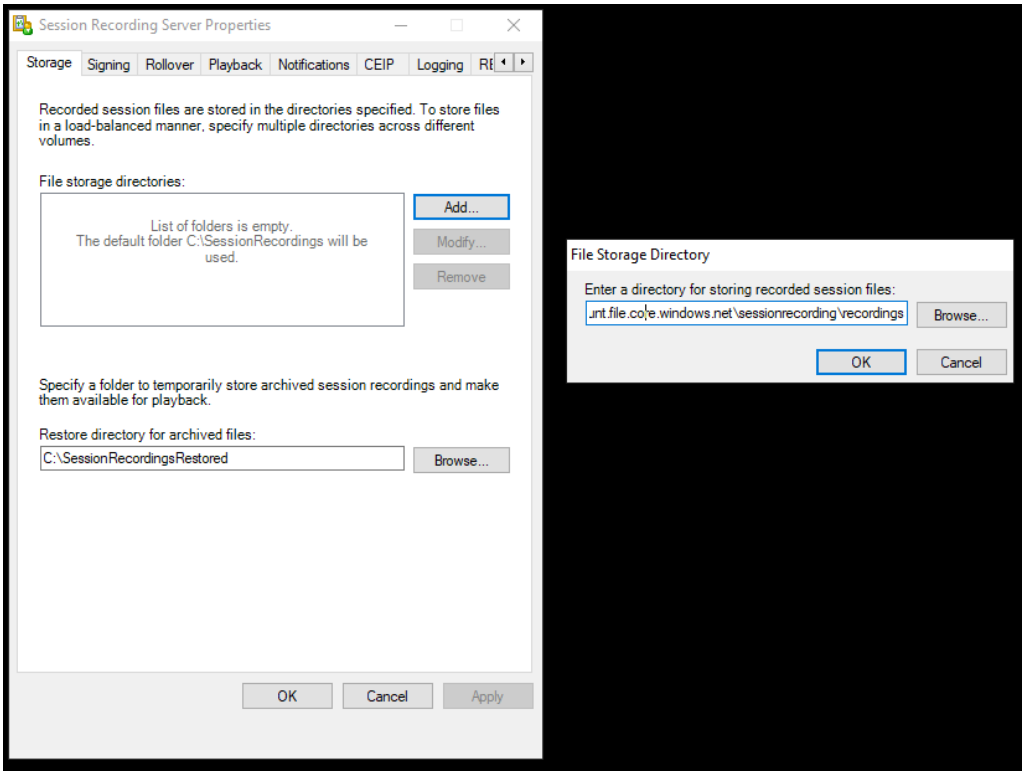
c) Session Recording サーバーをインストールしたホストに、Azure ファイル共有をマウントします。

i. [**Session Recording** サーバーのプロパティ] を開きます。

ii. [格納場所] タブで [追加] をクリックします。

iii. 次の形式で UNC パスを入力します: **\\<storageaccountname>.file.core.windows.net\\<filessharena**

録画ファイルを保存する場所として、ファイル共有の下にあるサブフォルダーを指定します。そうすると、Session Recording サーバーが自動的にサブフォルダーを作成します。

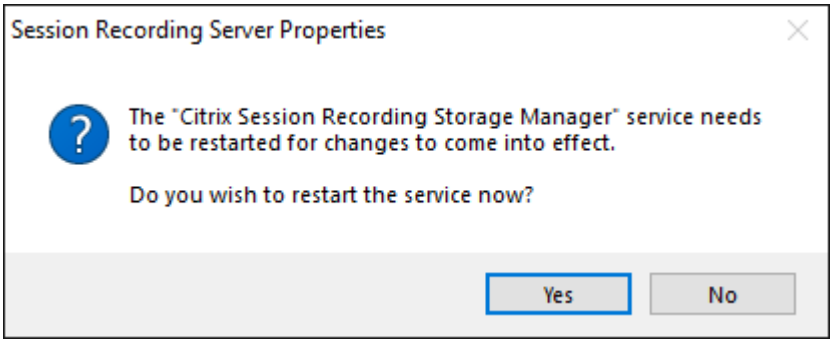


iv. ［ファイル格納フォルダー］ダイアログボックスで ［**OK**］をクリックします。

v. ［**Session Recording** サーバーのプロパティ］ウィンドウで ［適用］をクリックします。

vi. ［適用］がグレー表示になったら、［**OK**］をクリックします。

vii. Session Recording ストレージマネージャーサービスを再起動するよう求められたら、［はい］をクリックします。



ポリシー

April 3, 2024

Session Recording ポリシーコンソールを使用して、録画ポリシー、イベント検出ポリシー、イベント応答ポリシー、および録画の閲覧ポリシーを作成します。ポリシーの作成時は、Citrix Cloud とオンプレミス環境の両方から Delivery Controller を指定できます。

> 重要:
>
> Session Recording ポリシーコンソールを使用するには、Broker PowerShell スナップイン（Broker_PowerShellSnapIn_x64.msi）または Citrix DaaS Remote PowerShell SDK（CitrixPoshSdk.exe）を手動でインストールする必要があります。Citrix Virtual Apps and Desktops ISO（`\layout\image-full\x64\Citrix Desktop Delivery Controller`）で Broker PowerShell スナップインを検索します。または、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）のダウンロードページから、Citrix DaaS Remote PowerShell SDKをダウンロードします。
>
> ヒント:
>
> レジストリを編集して、Session Recording サーバーに予期しない障害が発生した場合にファイルが失われるのを防ぐことができます。Session Recording Agent をインストールしたマシンに管理者としてログオンし、レジストリエディターを開いて、`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent`の下に DWORD 値`DefaultRecordActionOnError` =1を追加します。

ポリシーのアクティブ化

1. Session Recording ポリシーコンソールをインストールしたマシンに管理者としてログオンします。
2. Session Recording ポリシーコンソールを起動します。
3. [**Session Recording** サーバーへの接続] ウィンドウが開いたら、Session Recording サーバーの名前、プロトコル、およびポートが正しいことを確認します。[**OK**] をクリックします。
4. Session Recording ポリシーコンソールで、対象のポリシーの種類を開きます。
5. アクティブ化するポリシーを選択 します。
6. メニューバーで ［ポリシーのアクティブ化］ を選択します。

ポリシーの変更

1. Session Recording ポリシーコンソールをインストールしたマシンに管理者としてログオンします。
2. Session Recording ポリシーコンソールを起動します。
3. [**Session Recording** サーバーへの接続] ウィンドウが開いたら、Session Recording サーバーの名前、プロトコル、およびポートが正しいことを確認します。[**OK**] をクリックします。
4. Session Recording ポリシーコンソールで、対象のポリシーの種類を開きます。
5. 変更するポリシーを選択します。ポリシーの規則が右ペインに表示されます。
6. 規則を追加、変更、または削除するには:

    - メニューバーで ［新しい規則の追加］ を選択します。ポリシーがアクティブな場合はポップアップウィ

ンドウが開き、操作の確認を促すメッセージが表示されます。規則ウィザードを使用して新しい規則を作成します。

- 変更する規則を選択し、右クリックして ［プロパティ］を選択します。規則ウィザードを使用して規則を変更します。
- 削除する規則を選択し、右クリックして ［規則の削除］を選択します。

ポリシーの削除

> 注:
>
> システム定義のポリシーまたはアクティブなポリシーは削除できません。

1. Session Recording ポリシーコンソールをインストールしたマシンに管理者としてログオンします。
2. Session Recording ポリシーコンソールを起動します。
3. ［**Session Recording** サーバーへの接続］ウィンドウが開いたら、Session Recording サーバーの名前、プロトコル、およびポートが正しいことを確認します。［**OK**］をクリックします。
4. Session Recording ポリシーコンソールで、対象のポリシーの種類を開きます。
5. 左ペインで削除するポリシーを選択します。ポリシーがアクティブな場合は、ほかのポリシーをアクティブにする必要があります。
6. メニューバーで ［ポリシーの削除］を選択します。
7. ［はい］をクリックして操作を確定します。

Session Recording ポリシーの構成

February 20, 2024

システム定義の録画ポリシーをアクティブにすることも、独自のカスタム録画ポリシーを作成してアクティブにすることもできます。システム定義の録画ポリシーにより、セッション全体に単一の規則を適用します。カスタム録画ポリシーにより、録画するセッションを指定します。

アクティブな録画ポリシーによって録画するセッションが決定されます。一度にアクティブにできる録画ポリシーは 1 つだけです。

システム定義の録画ポリシー

Session Recording には、次のシステム定義の録画ポリシーがあります:

- 録画しない。デフォルトのポリシーです。ほかのポリシーを指定しなければ、セッションは録画されません。
- イベントのみを録画する（全ユーザー、通知あり）。このポリシーは、イベント検出ポリシーで指定されたイベントのみを録画します。画面は録画されません。ユーザーは事前に録画通知を受け取ります。

- イベントのみを録画する（全ユーザー、通知なし）。このポリシーは、イベント検出ポリシーで指定されたイベントのみを録画します。画面は録画されません。ユーザーは録画通知を受け取りません。
- セッション全体を録画する（全ユーザー、通知あり）。このポリシーは、セッション全体（画面とイベント）を録画します。ユーザーは事前に録画通知を受け取ります。
- セッション全体を録画する（全ユーザー、通知なし）。このポリシーは、セッション全体（画面とイベント）を録画します。ユーザーは録画通知を受け取りません。

システム定義の録画ポリシーは変更または削除できません。

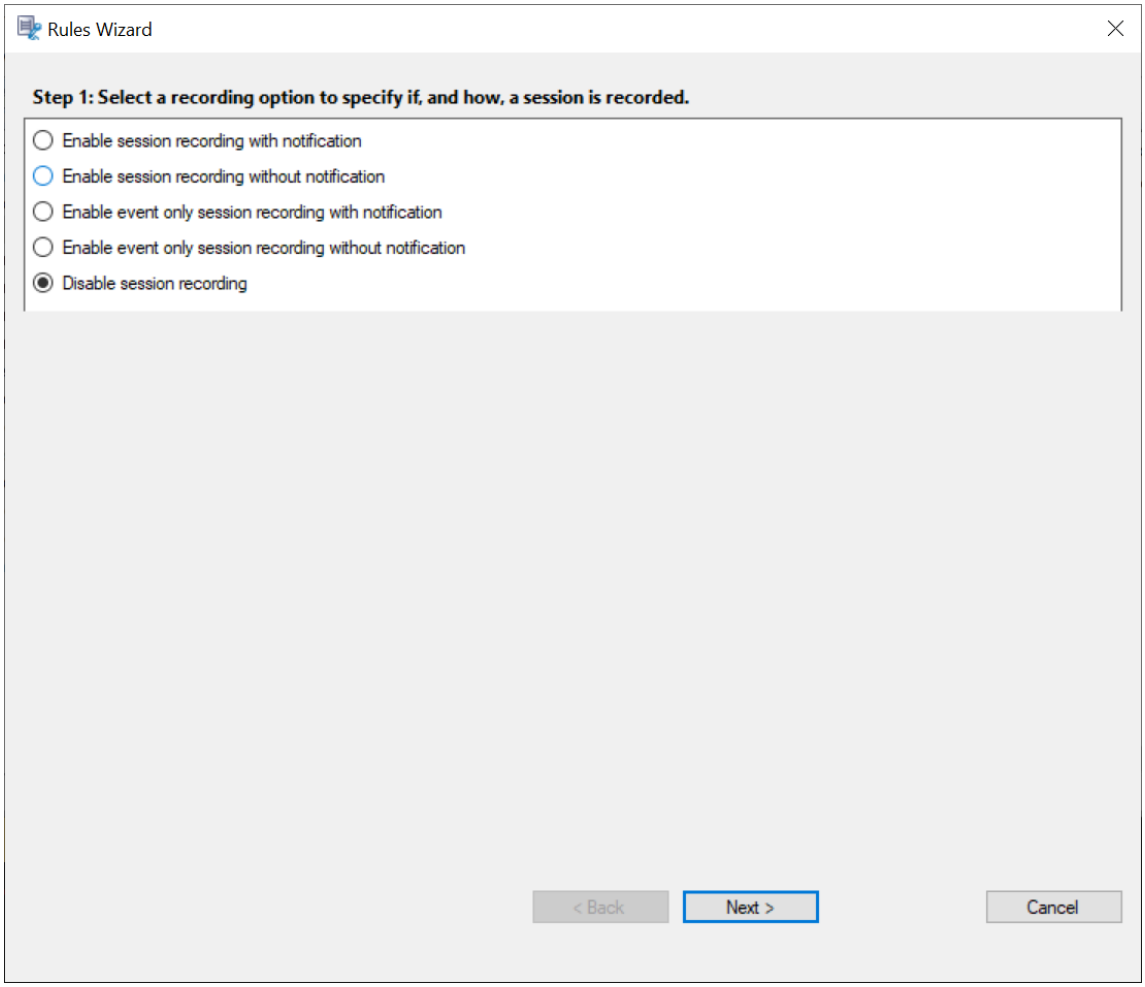
カスタム録画ポリシーの作成

ユーザーまたはグループ、公開アプリケーションまたはデスクトップ、デリバリーグループまたは VDA マシン、および Citrix Workspace アプリクライアントの IP アドレスを指定すれば、そのセッションを録画できます。Session Recording ポリシーコンソールにはウィザードが用意されており、このウィザードに従って規則を作成します。公開されているアプリケーションまたはデスクトップや、デリバリーグループまたは VDA マシンの一覧を取得するには、サイト管理者の読み取り権限が必要です。サイトの Delivery Controller で管理者の読み取り権限を構成します。

作成する規則ごとに録画操作および規則条件を指定します。録画操作は規則条件を満たすセッションに適用されます。

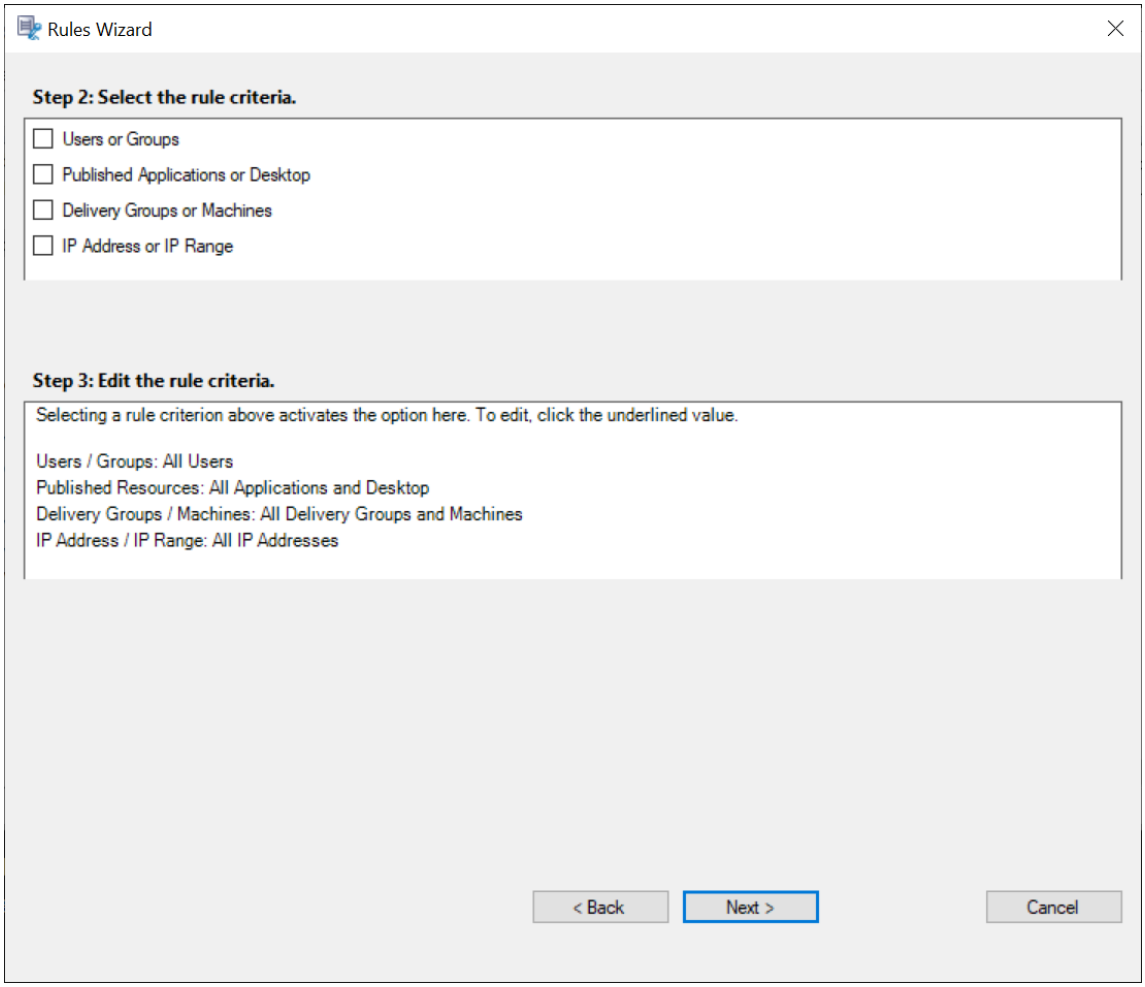
規則ごとに録画操作を 1 つ選択します:

- 通知してセッションを録画する。このオプションは、セッション全体（画面とイベント）を録画します。ユーザーは事前に録画通知を受け取ります。
- 通知しないでセッションを録画する。このオプションは、セッション全体（画面とイベント）を録画します。ユーザーは録画通知を受け取りません。
- 通知してイベントのみのセッションを録画する。このオプションは、セッションを通してイベント検出ポリシーで指定されたイベントのみを録画します。画面は録画されません。ユーザーは事前に録画通知を受け取ります。
- 通知しないでイベントのみのセッションを録画する。このオプションは、セッションを通してイベント検出ポリシーで指定されたイベントのみを録画します。画面は録画されません。ユーザーは録画通知を受け取りません。
- セッションを録画しない。このオプションは、セッションが録画されないことを意味します。



規則ごとに次の項目のいずれかを少なくとも 1 つ選択して、規則条件を作成します:

- ユーザーまたはグループ。規則の操作を適用するユーザーまたはグループの一覧を作成します。Session Recording によってActive Directory グループおよびユーザーのホワイトリスト化を使用できます。
- 公開アプリケーションまたはデスクトップ。規則の操作を適用する公開アプリケーションまたはデスクトップの一覧を作成します。規則ウィザードで、アプリケーションまたはデスクトップを使用できる Citrix Virtual Apps and Desktops または Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）を選択します。
- デリバリーグループまたはマシン。規則の操作を適用するデリバリーグループまたはマシンの一覧を作成します。規則ウィザードで、デリバリーグループまたはマシンの場所を選択します。
- **IP** アドレスまたは **IP** 範囲。規則の操作を適用する IP アドレスまたは IP アドレスの範囲の一覧を作成します。［**IP** アドレスまたは **IP** の範囲の選択］画面で、録画が有効または無効になった有効な IP アドレスまたは IP 範囲を追加します。この IP アドレスは、Citrix Workspace アプリの IP アドレスです。



> 注:
>
> Session Recording ポリシーコンソールでは、1 つの規則内で複数の条件を構成できます。規則が適用される際には、「AND」と「OR」の両方の論理演算子が、最終的なアクションを計算するために使われます。一般的に、「OR」演算子は一定の条件内の項目に使われ、「AND」演算子は違った複数の条件に当てはまる項目に使われます。結果が true であれば、Session Recording ポリシーエンジンがその規則のアクションをとります。そうでなければ、次の規則に進み、処理を繰り返します。

録画ポリシーに複数の規則を作成する場合は、複数の規則条件に一致するセッションがある可能性があります。そのような場合は、優先順位が最も高い規則がセッションに適用されます。

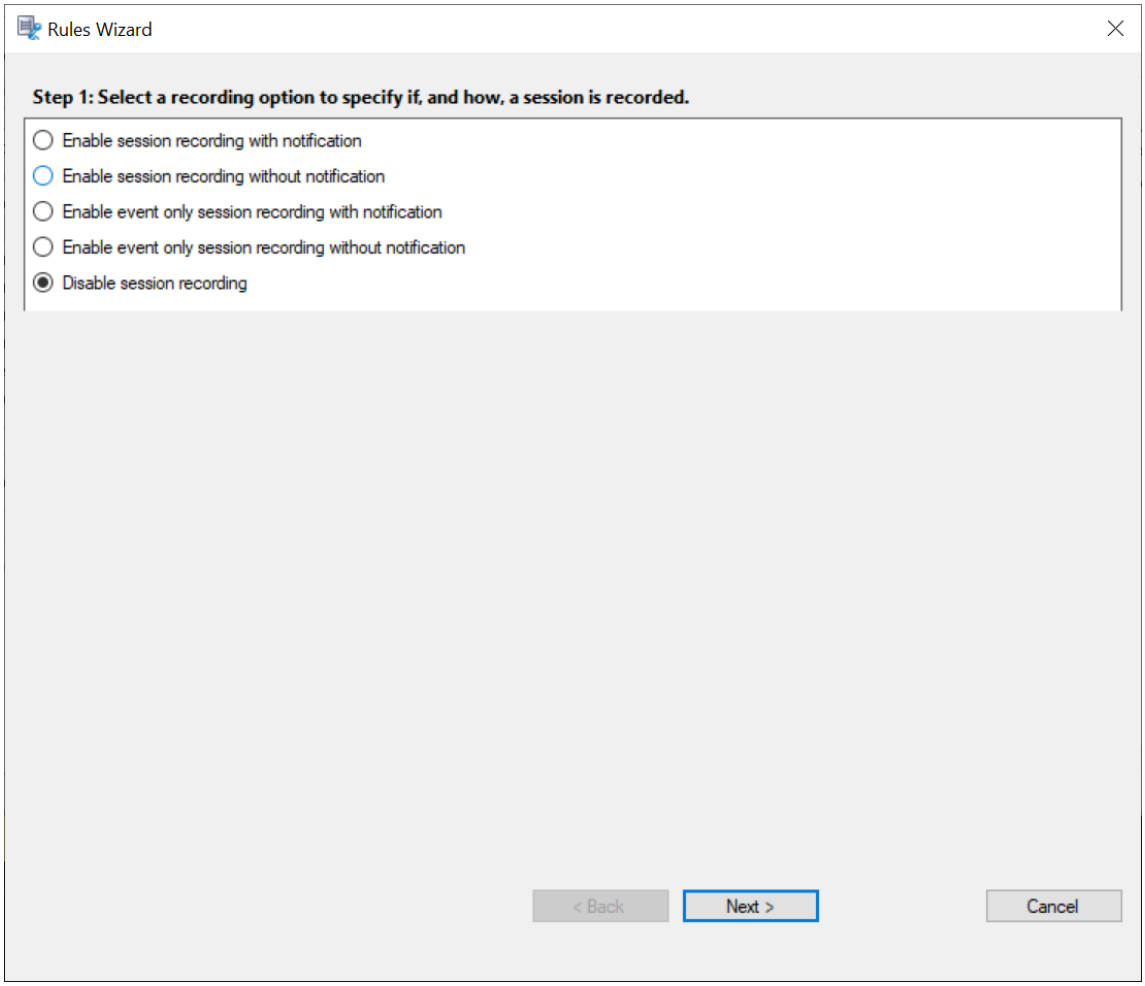
規則により実行される録画操作によってその優先順位が決まります。

- 「録画しない」規則の優先順位が最も高くなります。
- 「通知して録画する」規則の優先順位が次に高くなります。
- 「通知しないで録画する」規則の優先順位が最も低くなります。
- 「通知してイベントのみのセッションを録画する」規則の優先度は中程度です。
- 「通知しないでイベントのみのセッションを録画する」規則の優先度は最も低くなります。

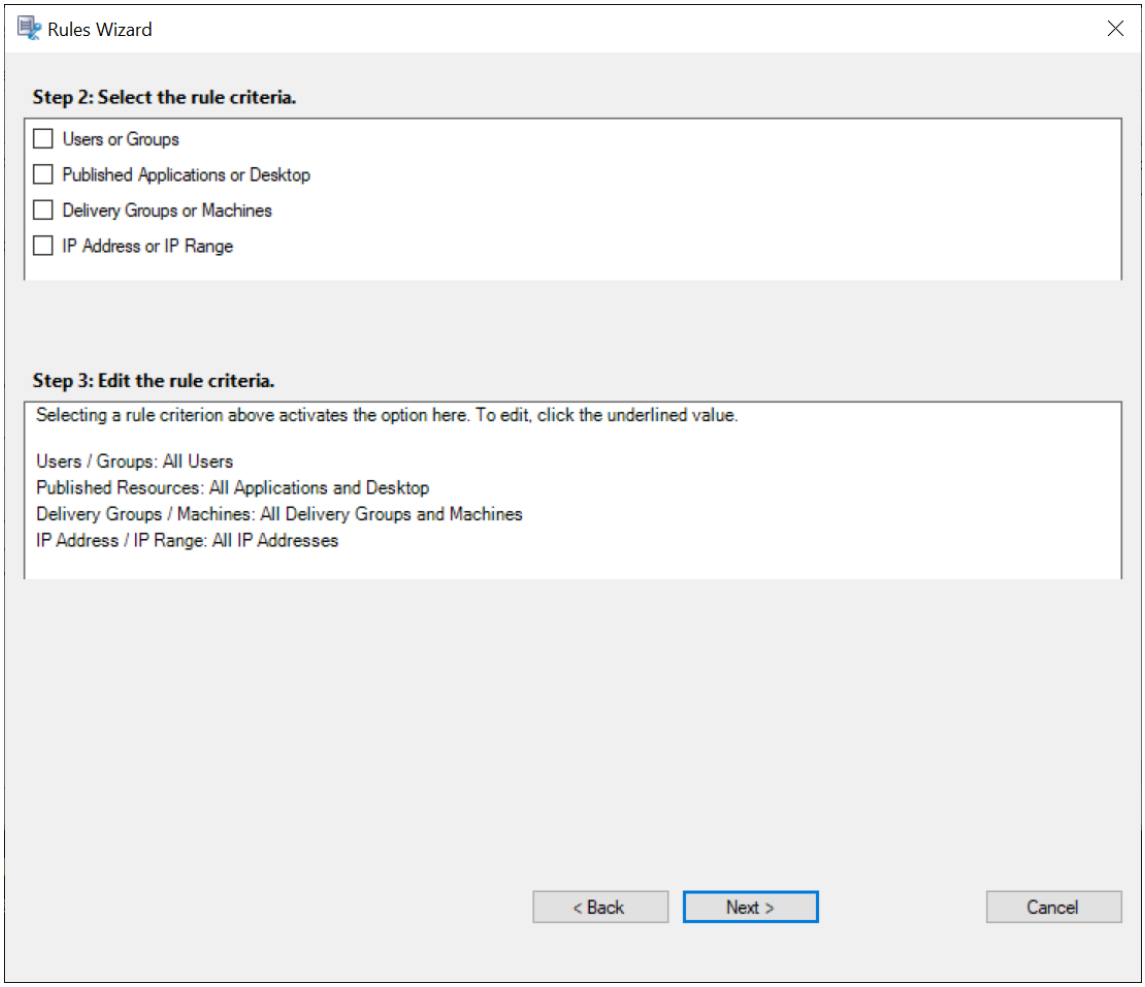
録画ポリシーの規則条件のいずれにも当てはまらないセッションがある可能性があります。そのようなセッションについては、フォールバック規則の操作が適用されます。フォールバック規則の操作は常に「録画しない」です。フォールバック規則は変更または削除できません。

カスタム録画ポリシーを作成するには:

1. 承認済みのポリシー管理者として、Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recording ポリシーコンソールを起動して、左側のペインで ［録画ポリシー］を選択します。メニューバーで ［新しいポリシーの追加］を選択します。
3. 新しいポリシーを右クリックして ［規則の追加］をクリックします。
4. 規則ウィザードで、録画オプションを選択し、［次へ］をクリックします。



5. 規則条件の選択 - 次の 1 つまたは複数の規則条件を選択することができます:
   ユーザーまたはグループ
   公開アプリケーションまたはデスクトップ
   デリバリーグループまたはマシン
   IP アドレスまたは **IP** の範囲

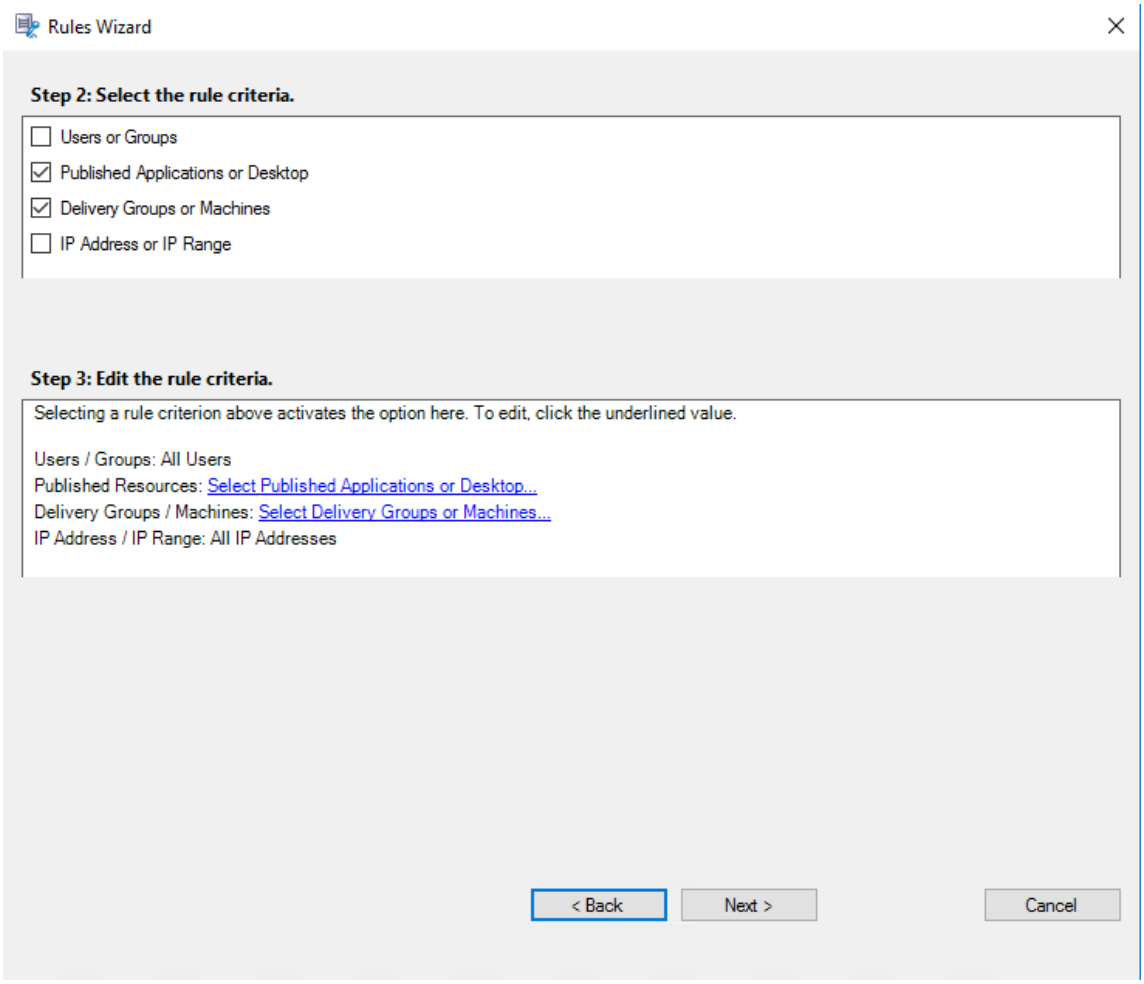


6. 規則条件の編集 - 編集するには、下線付きの値をクリックします。前の手順で選択した条件に基づき、値に下線が引かれます。

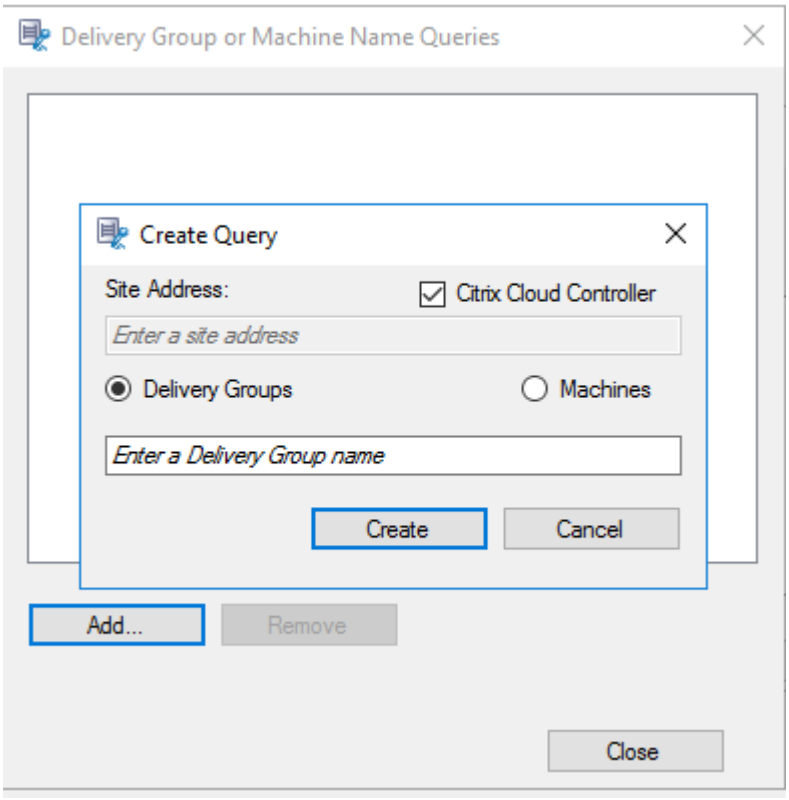
> 注:
>
> ［公開アプリケーションまたはデスクトップ］の下線付きの値を選択した場合、［サイトアドレス］は IP アドレス、URL、またはコントローラーがローカルネットワーク上にある場合はコンピューター名になります。［アプリケーションの名前］リストに表示名が表示されます。

［公開アプリケーションまたはデスクトップ］または ［デリバリーグループまたはマシン］を選択する場合、Session Recording ポリシーコンソールで通信に使用する Delivery Controller を指定します。

Session Recording ポリシーコンソールは、Citrix Cloud およびオンプレミス環境から Delivery Controller に通信する唯一のチャネルです。



たとえば、［デリバリーグループまたはマシン］を選択する場合、上のスクリーンショットの手順 3 で関連するハイパーリンクを選択して ［追加］をクリックし、Delivery Controller へのクエリを追加します。



以下の表は、オンプレミスおよび Citrix Cloud の Delivery Controller の使用例について説明しています:

使用例	必要な操作
オンプレミス Delivery Controller	a) Broker_PowerShellSnapIn_x64.msi をインストールする。2.［**Citrix Cloud Controller**］チェックボックスをオフにする。
Citrix Cloud Delivery Controller	a) Citrix DaaS Remote PowerShell SDK をインストールする。2. Citrix Cloud のアカウント資格情報を検証する。3.［**Citrix Cloud Controller**］チェックボックスをオンにする。
オンプレミス Delivery Controller から Citrix Cloud Delivery Controller に切り替える	a) Broker_PowerShellSnapIn_x64.msi をアンインストールしてマシンを再起動する。2. Citrix DaaS Remote PowerShell SDK をインストールする。3. Citrix Cloud のアカウント資格情報を検証する。4.［**Citrix Cloud Controller**］チェックボックスをオンにする。

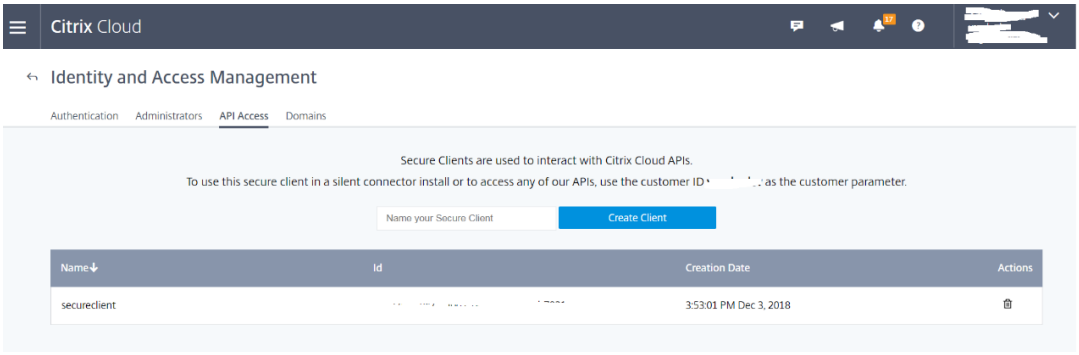
使用例	必要な操作
Citrix Cloud Delivery Controller からオンプレミス Delivery Controller に切り替える	a) Citrix DaaS Remote PowerShell SDK をアンインストールしてマシンを再起動する。2. Broker_PowerShellSnapIn_x64.msi をインストールする。3. [**Citrix Cloud Controller**] チェックボックスをオフにする。

Citrix Cloud の資格情報の検証

Citrix Cloud でホストされている Delivery Controller にクエリするには、Session Recording ポリシーコンソールがインストールされたマシンで手動で Citrix Cloud 資格情報を検証します。この作業を行わない場合、エラーが発生し Session Recording ポリシーコンソールが正常に機能しなくなることがあります。

手動で検証するには:

a) Citrix Cloud コンソールにログオンし、[**ID** およびアクセス管理] > [**API** アクセス] に移動します。API アクセス用セキュアクライアントを作成して、Citrix Cloud の認証プロンプトを省略できる認証プロファイルを取得します。セキュアクライアントをダウンロードし、名前を変更して安全な場所に保存します。デフォルトのファイル名は secureclient.csv です。



b) PowerShell セッションを開いて次のコマンドを実行し、(前の手順で取得した) 認証プロファイルを有効にします。

```
asnp citrix.*
Set-XDCredentials -CustomerId “citrixdemo” -SecureClientFile “c:\temp\secureclient.csv” -ProfileType CloudAPI -StoreAs “default”

<!--NeedCopy-->
```

必要に応じて、**CustomerId** と **SecureClientFile** を設定します。上記のコマンドで、顧客用のデフォルトの認証プロファイル`citrixdemo`が作成され、以降のすべての PowerShell セッションで認証プロンプトが省略されます。

7. ウィザードの指示に従って構成を終了します。

> 注：事前起動されたアプリケーションセッションに関する制限事項：
>
> - アクティブなポリシーがアプリケーション名との一致を試みた場合、事前起動されたセッションで開かれているアプリケーションとは一致しません。その結果、事前起動されたセッションは録画できません。
> - アクティブなポリシーがすべてのアプリケーションを録画していて、セッションの事前起動が有効になっている場合は、ユーザーが Windows 向け Citrix Workspace アプリにログオンしたときに、録画通知が表示されます。事前起動された（空の）セッションと、そのセッションで今後起動されるアプリケーションが録画されます。
>
> これを回避するには、録画ポリシーに従って別のデリバリーグループでアプリケーションを公開します。録画条件にアプリケーション名を使用しないでください。このアプローチによって、事前起動されたセッションを録画できます。ただし、通知は表示されます。

Active Directory グループの使用

Active Directory グループを使用して、Session Recording のポリシーを作成できます。個々のユーザーではなく Active Directory グループを使用すると、規則とポリシーを簡単に作成したり管理したりできます。たとえば、財務部門のユーザーが **Finance** という名前の Active Directory グループに含まれている場合は、
［規則］ウィザードで **Finance** グループを選択することで、このグループのすべてのメンバーに適用される規則を作成できます。

ユーザーのホワイトリスト化

組織内の一部のユーザーのセッションを確実に録画対象から除外する、Session Recording ポリシーを作成できます。これは
ユーザーのホワイトリスト化と呼ばれます。個人情報を取り扱う社員や特定の階層の従業員など、セッションを録画するべきではないユーザーをホワイトリストに登録すると便利です。

すべての上級管理職が **Executive** という名前の Active Directory グループのメンバーである場合、**Executive** グループのセッション録画を無効にする規則を作成して、それらのユーザーのセッションが決して録画されないように設定できます。この規則を含むポリシーがアクティブな間は、Executive グループのメンバーのセッションは録画されません。組織内のほかのメンバーのセッションは、アクティブなポリシーのほかの規則に基づいて録画されます。

Director を構成して **Session Recording** サーバーを使用する

Director コンソールを使用して、録画ポリシーを作成およびアクティブ化できます。

1. HTTPS 接続の場合は、Director サーバーの［信頼されたルート証明書］に Session Recording サーバーを信頼する証明書をインストールします。

2. Session Recording サーバーを使用するように Director サーバーを構成するには、`C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording` コマンドを実行します。
3. Director サーバーで、Session Recording サーバーの IP アドレスまたは FQDN、ポート番号、および Session Recording Agent が Session Recording Broker との接続に使用する接続の種類（HTTP または HTTPS）を入力します。

ロールオーバーの動作

ポリシーをアクティブにする場合、それまでアクティブだったポリシーはセッションの録画が終了するまで、またはセッションの録画ファイルが上限に達するまで効力を保ちます。ロールオーバーは、ファイルサイズが上限に達すると実行されます。録画ファイルのサイズの上限について詳しくは、「録画ファイルのサイズの指定」を参照してください。

次の表で、セッションの録画中に新しい録画ポリシーを適用してロールオーバーが起きたときに生じる現象について説明します:

以前の録画ポリシー:	新しい録画ポリシー:	ロールオーバーの後の録画ポリシー:
録画しない	ほかのポリシー	変更なし。ユーザーが新しいセッションにログオンするときのみに新しいポリシーが有効になります。
通知しないで録画する	録画しない	録画を停止します。
通知しないで録画する	通知して録画する	録画を続行し通知メッセージを表示します。
通知して録画する	録画しない	録画を停止します。
通知して録画する	通知しないで録画する	録画を続行します。ユーザーが次にログオンするときはメッセージが表示されません。

録画の閲覧ポリシーの構成

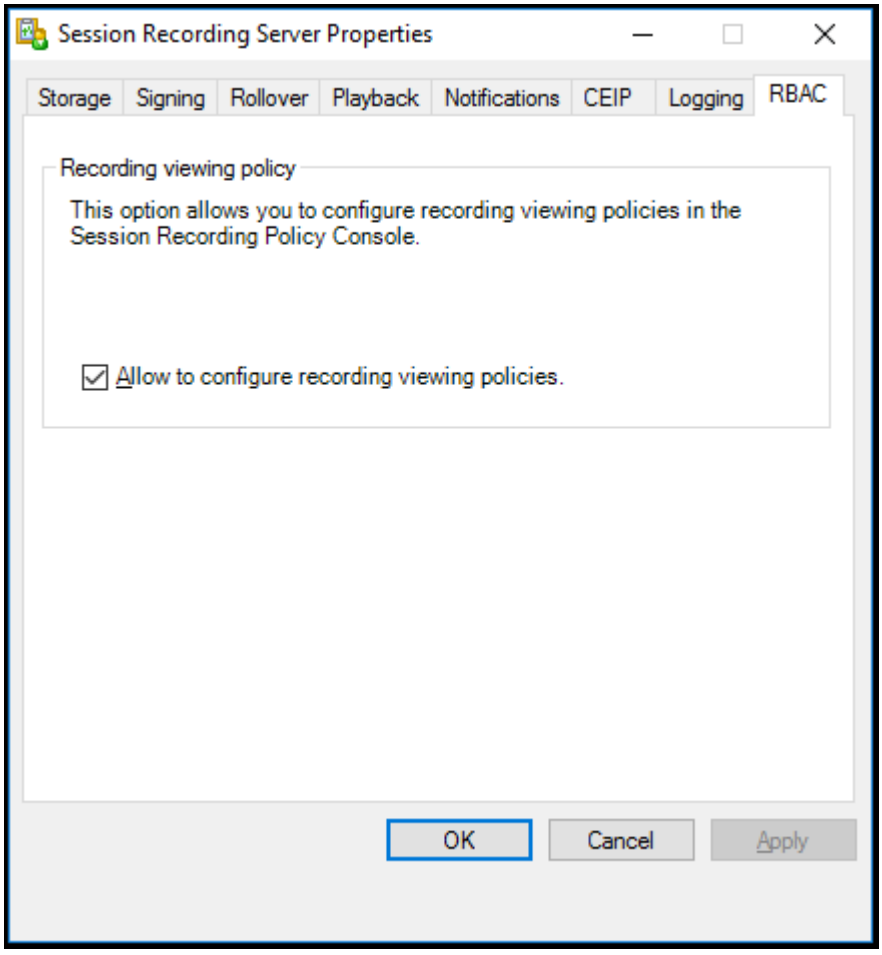
February 20, 2024

Session Recording では、役割ベースのアクセス制御がサポートされています。Session Recording ポリシーコンソールで録画の閲覧ポリシーを作成し、各ポリシーに複数の規則を追加できます。各規則は、録画の閲覧者としてユーザーまたはユーザーグループを選択し、だれの録画をその閲覧者が表示できるかを設定するのに役立ちます。

カスタム録画閲覧ポリシーの作成

録画の閲覧ポリシーを作成する前に、次の手順で機能を有効にします:

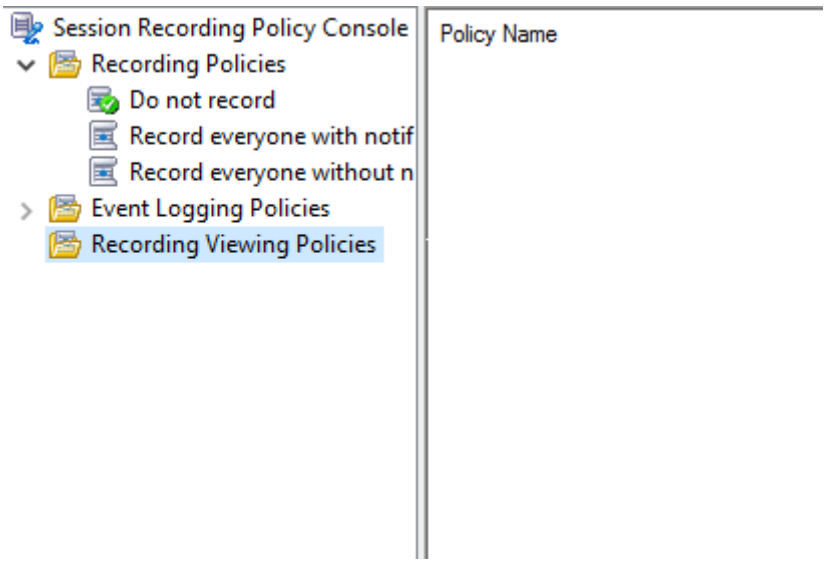
1. Session Recording サーバーをホストするマシンにログオンします。
2. [スタート] ボタンをクリックし、[**Session Recording** サーバーのプロパティ] を選択します。
3. [**Session Recording** サーバーのプロパティ] で、[**RBAC**] タブをクリックします。
4. [録画の閲覧ポリシーの構成を許可する] チェックボックスをオンにします。



カスタム録画閲覧ポリシーを作成するには:

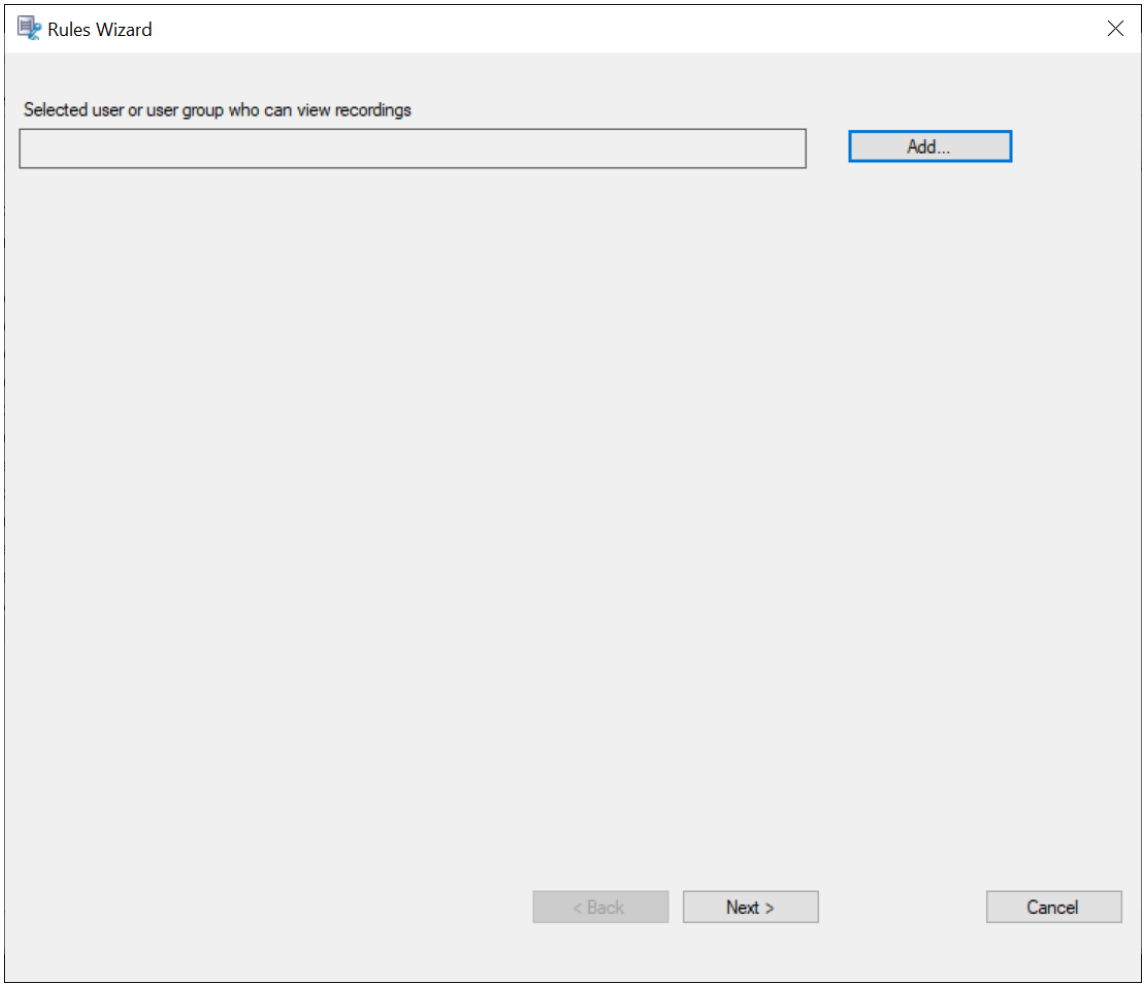
注: 録画ポリシーおよびイベント検出ポリシーとは異なり、録画の閲覧ポリシー（ポリシー内に追加したすべての規則を含む）は、作成すると直ちにアクティブになります。有効化する必要はありません。

1. 承認済みのポリシー管理者として、Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recording ポリシーコンソールを起動します。デフォルトでは、録画の閲覧ポリシーはありません。



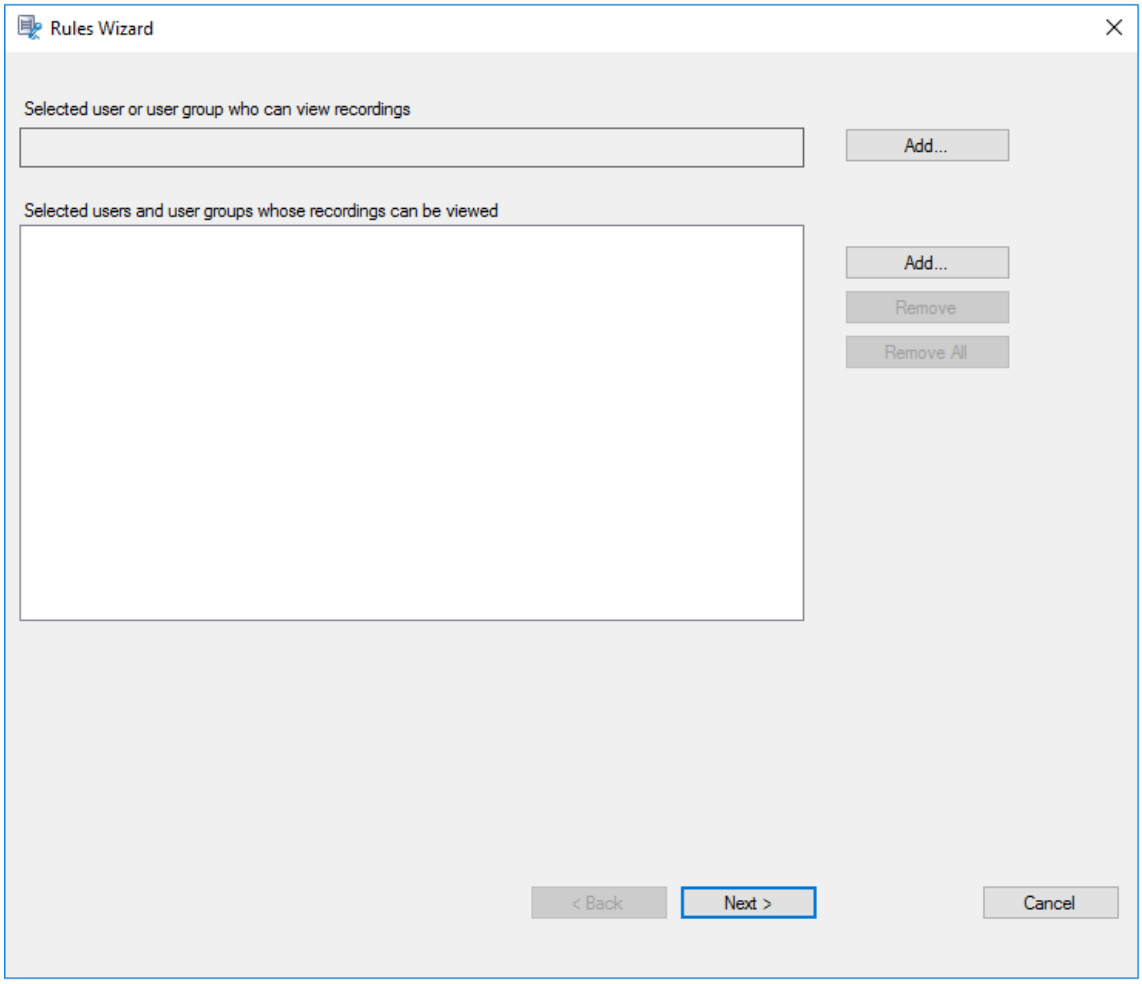
注：［録画の閲覧ポリシー］を使用できるようにするには、最初に ［**Session Recording** サーバーのプロパティ］でこの機能を有効にしてください。

3. 左側のペインで ［録画の閲覧ポリシー］を選択します。メニューバーで ［新しいポリシーの追加］を選択して録画の閲覧ポリシーを作成します。
4. （オプション）新しい録画の閲覧ポリシーを右クリックして、名前を変更します。
5. 新しいポリシーを右クリックして ［規則の追加］をクリックします。



6. [**Add**] をクリックします。
7. [ユーザーとグループの選択] ダイアログで、録画の閲覧者としてユーザーまたはユーザーグループを選択します。

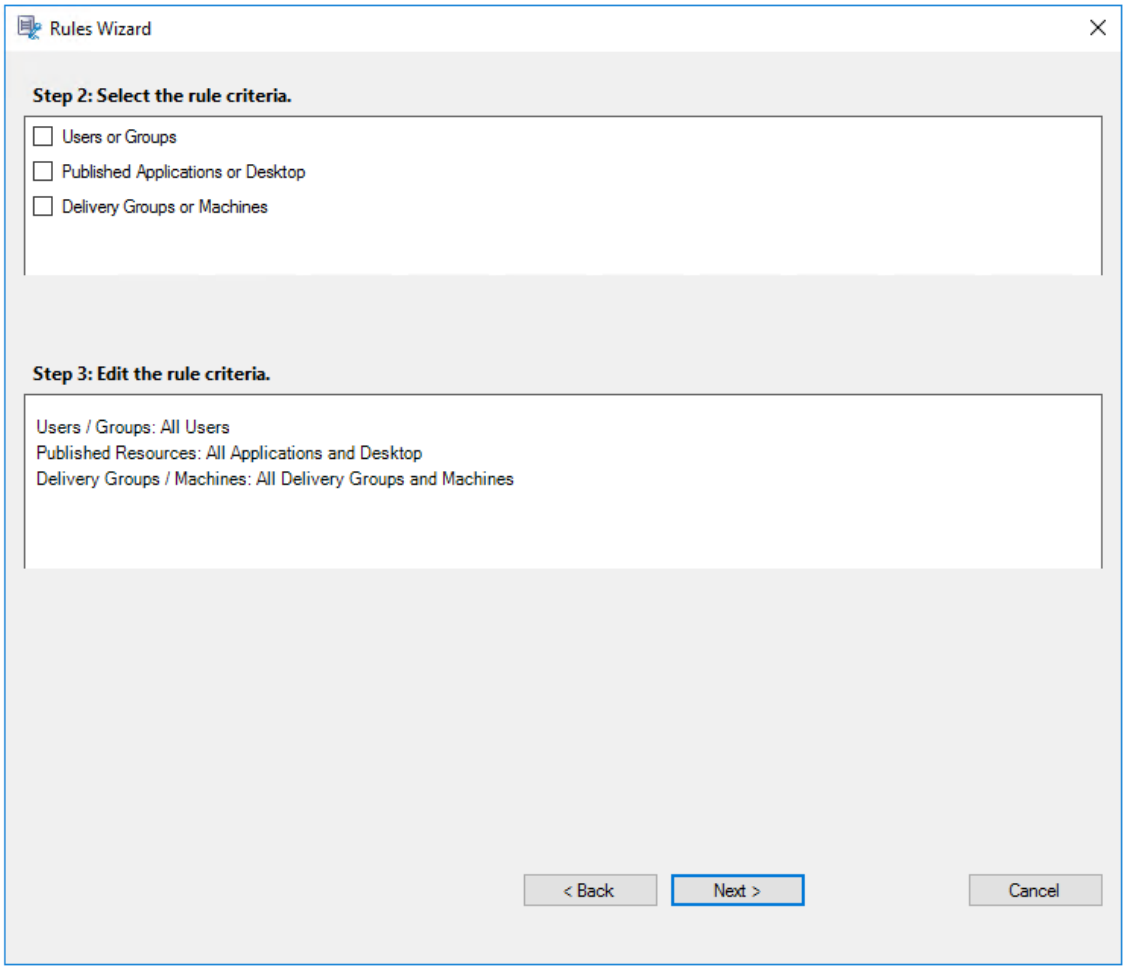
> 注:
>
> 録画したセッションを表示するには、ビューアーに Player の役割を割り当てる必要があります。詳しくは、「ユーザーの承認」を参照してください。



> 注:
>
> 各規則で、録画の閲覧者として選択できるのは 1 人のユーザーまたは 1 つのユーザーグループだけです。複数のユーザーまたはユーザーグループを選択した場合は、最新の選択のみが有効になり、テキストボックスに表示されます。
> 録画の閲覧者を指定するときは、閲覧者に Player のロールを割り当てていることを確認してください。録画されたセッションを再生する権限がないユーザーが、録画されたセッションを再生しようとするとエラーメッセージが表示されます。詳しくは、「ユーザーの承認」を参照してください。

8. [**OK**]、[次へ] をクリックします。規則条件を設定するダイアログが開きます。
9. 規則条件を選択して編集し、前述の閲覧者が閲覧できる録画を指定します。

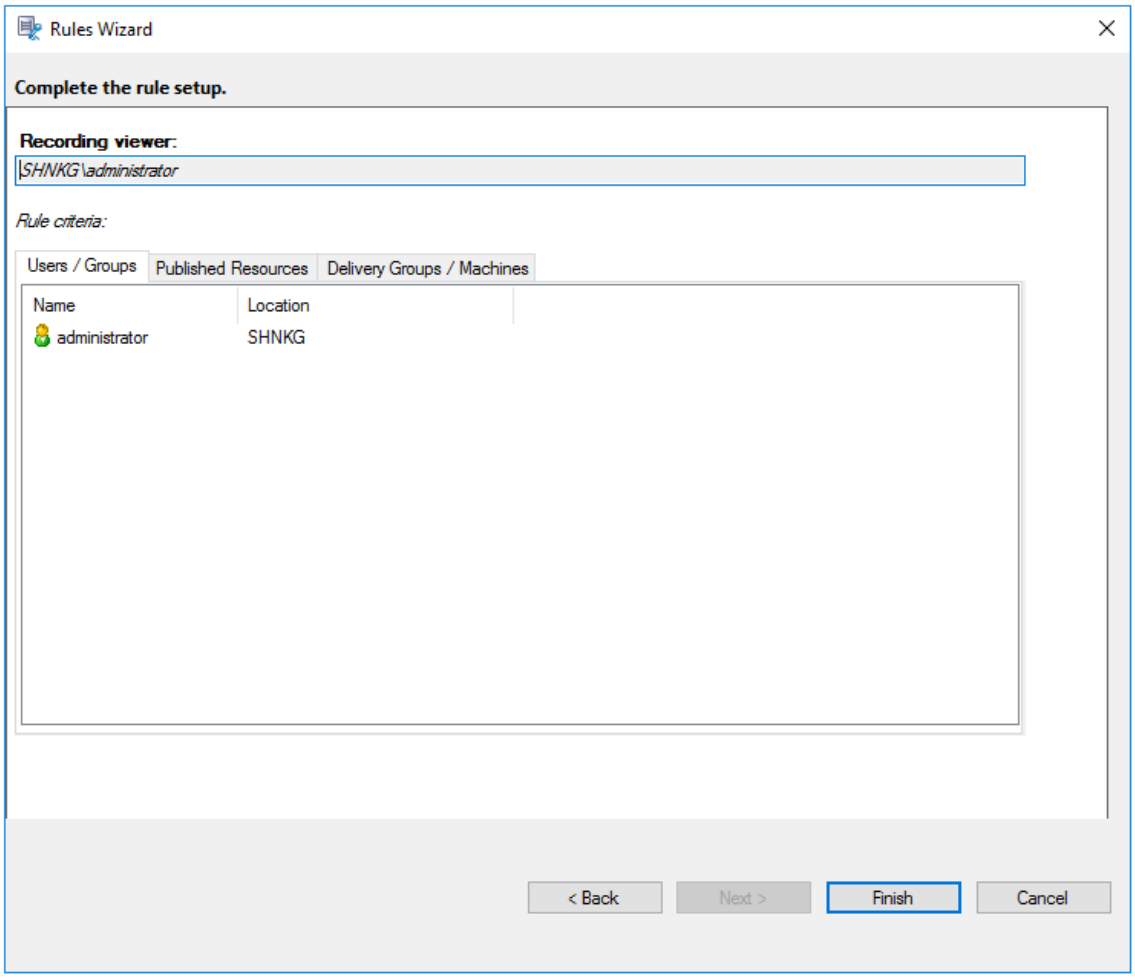
   - ユーザーまたはグループ
   - 公開アプリケーションまたはデスクトップ
   - デリバリーグループまたはマシン



> 注:
>
> 「OR」論理演算子は、規則条件内の項目間と個別の規則条件間の両方で使用されます。
>
> 規則条件を指定しないでおくと、前述の指定した閲覧者には閲覧用の録画が表示されません。

10. ウィザードの指示に従って構成を完了します。

    例:



イベント検出ポリシーの構成

February 20, 2024

Session Recording はイベント検出ポリシーの一元的な構成をサポートします。Session Recording ポリシーコンソールでポリシーを作成してさまざまなイベントをログ記録できます。

検出できるイベント

Session Recording では、対象のイベントを検出し、録画内でそのイベントにタグ付けして、後で検索および再生で使うことができます。大量の録画から関心のあるイベントを検索したり、再生時にそのイベントを見つけたりすることができます。

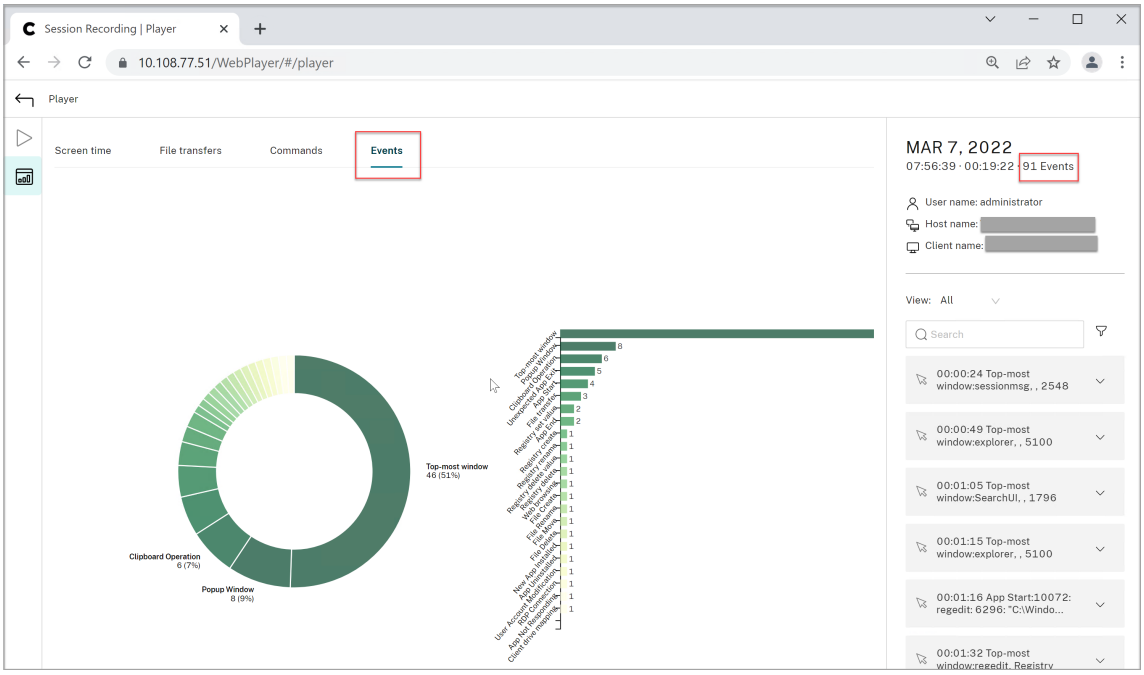
システム定義のイベント

Session Recording では、録画されたセッションで発生した次のシステム定義のイベントを検出してログに記録できます:

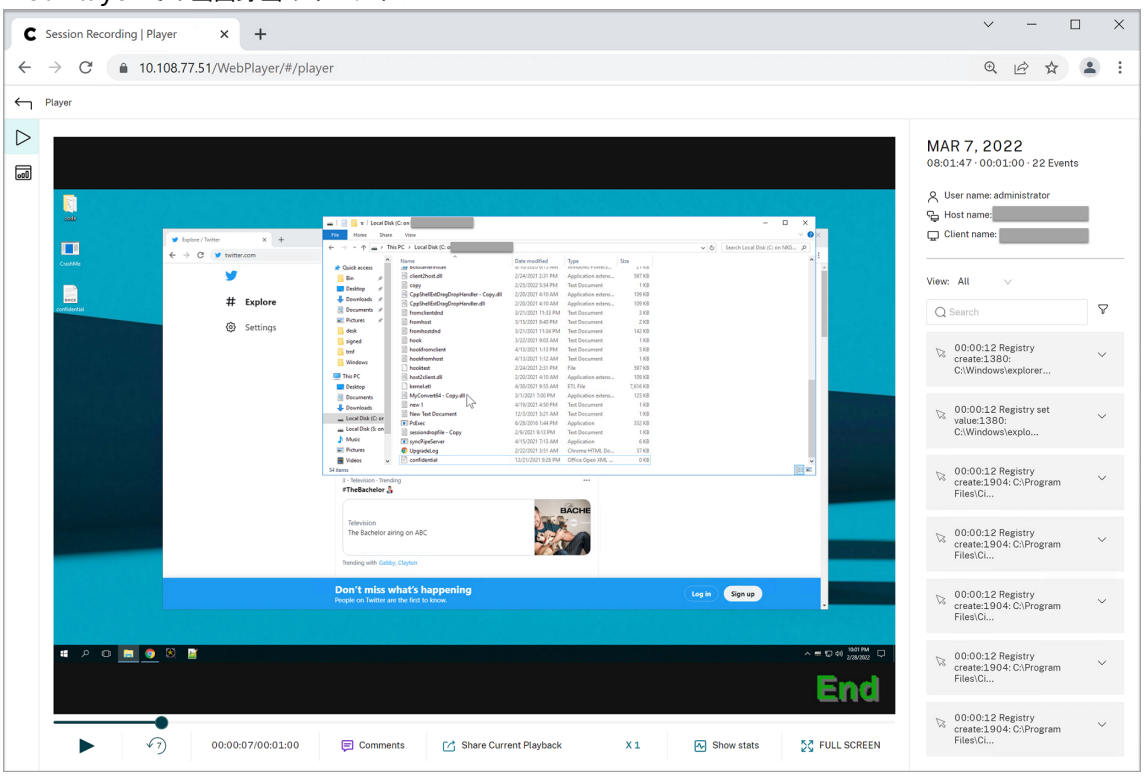
- USB 大容量記憶装置デバイスの挿入
- アプリケーションの起動と終了
- アプリエラー
- アプリのインストールとアンインストール
- ファイルの名前変更、作成、削除、移動のセッション内操作
- セッションホスト（VDA）とクライアントデバイス（マップされたクライアントドライブと汎用リダイレクトを使用した大容量記憶装置デバイスを含む）との間のファイル転送
- Web 閲覧アクティビティ
- 最前面のウィンドウのイベント
- クリップボードのアクティビティ
- Windows レジストリの変更
- ユーザーアカウントの変更
- RDP 接続
- パフォーマンスデータ（録画されたセッションに関連するデータポイント）
- ポップアップウィンドウイベント

例:

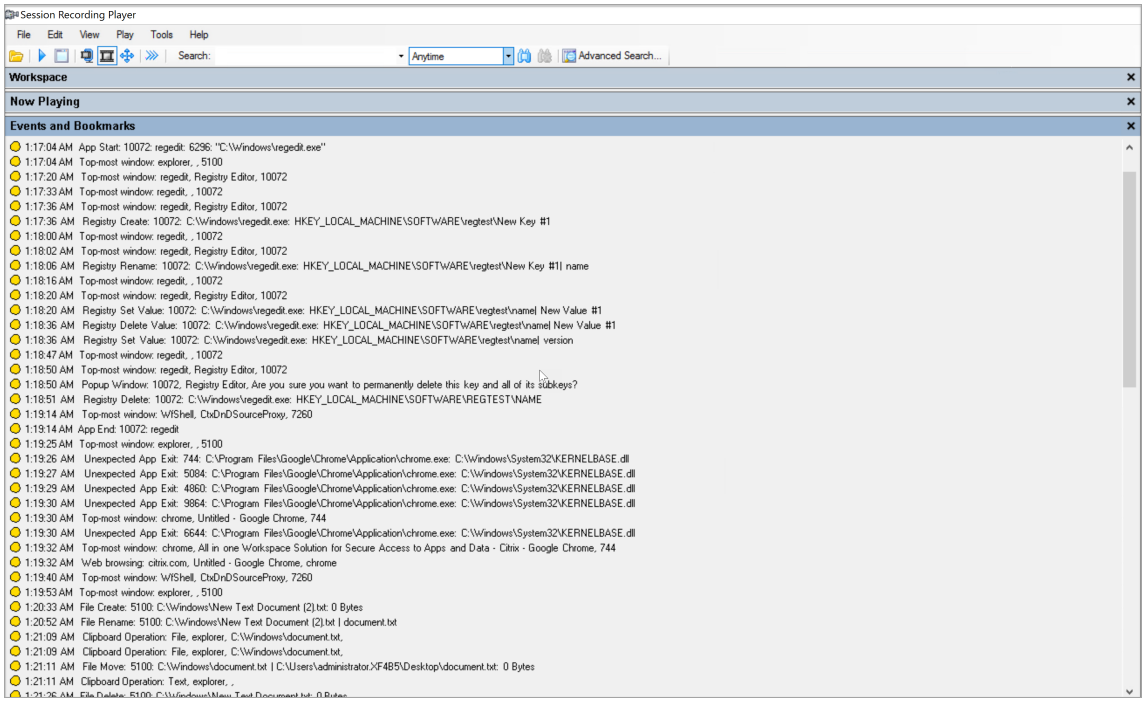
- Web Player でのイベントのみの録画のイベント:



- Web Player での画面録画のイベント:



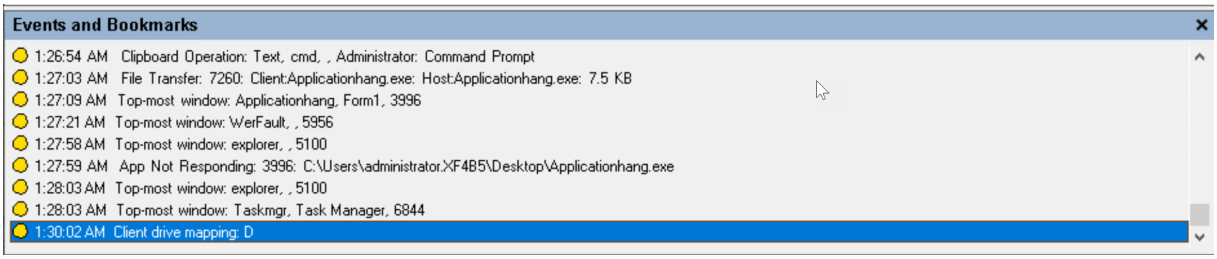
- Session Recording Player のイベント:



Session Recording Player のイベントについて詳しくは、この記事の後半にあるイベントの説明を参照してください。

> 注:
>
> Web 閲覧アクティビティと最前面のウィンドウのイベントを検出するアクティブなポリシーがある場合、PowerBuilder によって構築されたアプリケーションが予期せず終了することがあります。この問題を回避するには、PowerBuilder 2019 R3 を使用してアプリケーションを構築します。

USB 大容量記憶装置デバイスの挿入　Windows 向けまたは Mac 向け Citrix Workspace アプリがインストールされているクライアントで、クライアントドライブマッピング（CDM）でマッピングされた、または汎用リダイレクトを使用した、USB 大容量記憶装置デバイスが挿入されると、Session Recording により、そのデバイスが検出されます。Session Recording は、録画内のイベントにタグ付けします。



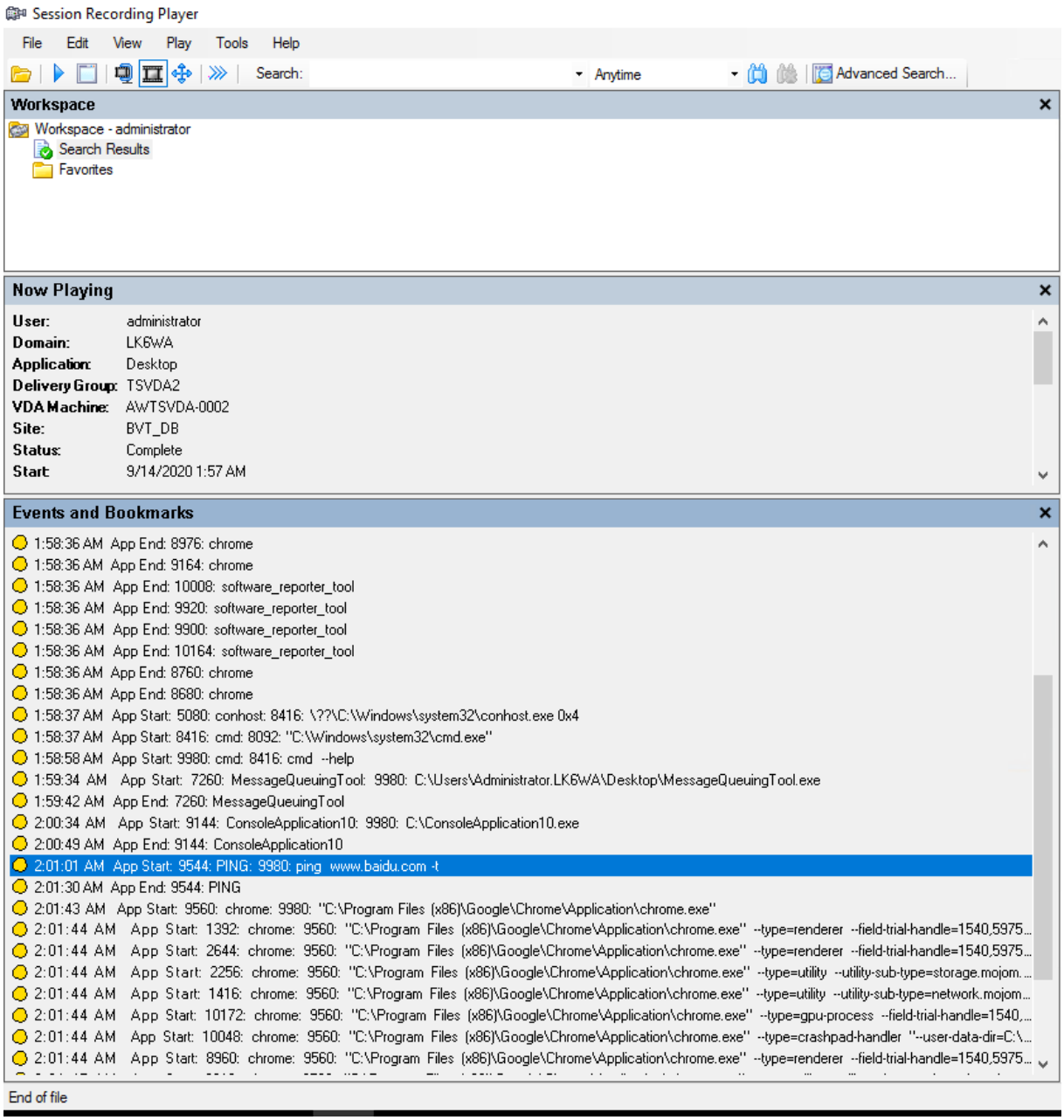
> 注:
>
> 挿入された USB 大容量記憶装置デバイスを使用して挿入イベントを検出するには、Citrix Studio で「クライアント **USB** デバイスリダイレクト」ポリシーを ［許可］ に設定します。

> 現在、USB 大容量記憶装置デバイス（USB Class 08）の挿入のみが検出されます。

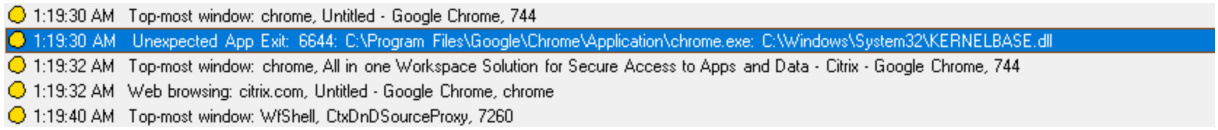
アプリケーションの起動と終了　Session Recording は、アプリケーションの起動と終了の両方の検出をサポートします。プロセスを ［アプリ監視一覧］ に追加すると、追加したプロセスとその子プロセスにより実行されるアプリが監視されます。Session Recording が実行される前に開始する親プロセスの子プロセスもキャプチャできます。

Session Recording はプロセス名`cmd.exe`、`powershell.exe`、`wsl.exe`を ［アプリ監視一覧］ にデフォルトで追加します。イベント検出ポリシーで ［アプリ起動イベントのログを記録する］ および ［アプリ終了イベントのログを記録する］ を選択すると、コマンドプロンプト、PowerShell、Windows Subsystem for Linux（WSL）アプリの起動および終了が、これらのプロセス名が手動で ［アプリ監視一覧］ に加えられているかどうかにかかわらず、ログに記録されます。デフォルトのプロセス名は、［アプリ監視一覧］ には表示されません。

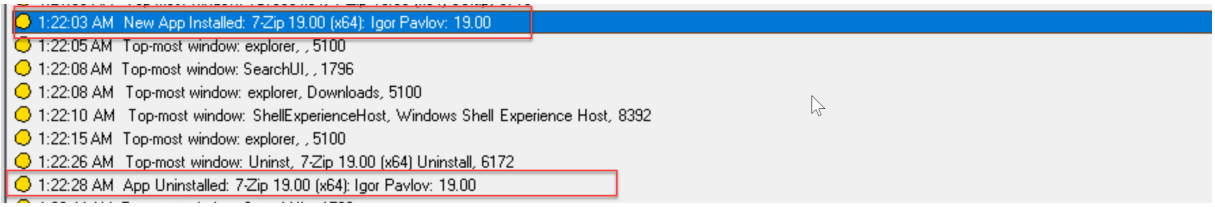
さらに、Session Recording は、ログに記録された各アプリ起動イベントの完全なコマンドラインを提供します。



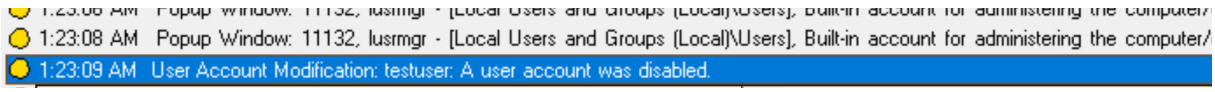
アプリケーションエラー　イベント検出ポリシーの作成時に、［アプリエラーをログに記録する］を選択すると、Session Recording はアプリの終了と応答しないアプリを検出します。［アプリエラーをログに記録する］規則は、すべてのアプリに適用されます。



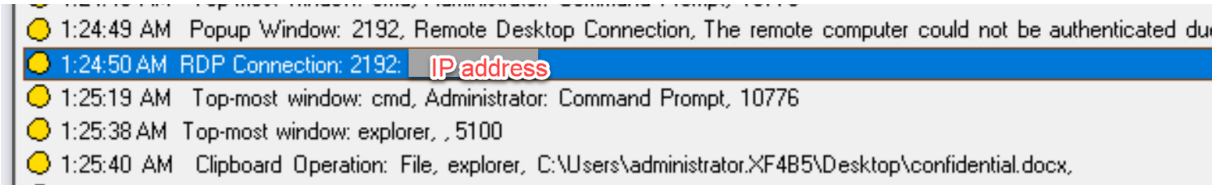
アプリのインストールとアンインストール　［アプリのインストールとアンインストール］規則は、すべてのアプリに適用されます。



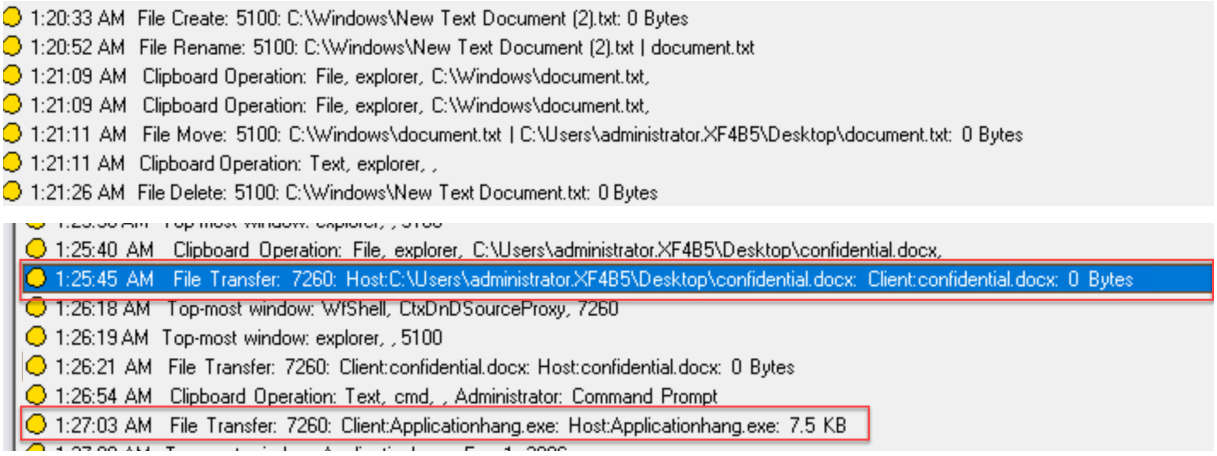
ユーザーアカウントの変更　Session Recording は、アカウントの作成、有効化、無効化、削除、名前の変更、およびパスワード変更の試行を検出できます。



RDP 接続　Session Recording は、録画されたセッションをホストしている VDA から開始された RDP 接続を検出できます。



セッション内でのファイルの名前変更、作成、削除、移動の操作、およびセッションホスト（**VDA**）とクライアントデバイスとの間のファイル転送　Session Recording は、［ファイル監視一覧］で指定したターゲットファイルおよびフォルダーの名前変更、作成、削除、および移動操作を検出できます。Session Recording は、セッションホスト(VDA）とクライアントデバイス（マップされたクライアントドライブと汎用リダイレクトを使用した大容量記憶装置デバイスを含む）との間のファイル転送を検出することもできます。［機密ファイルイベントのログを記録する］オプションを選択すると、［ファイル監視一覧］を指定するかに関係なく、ファイル転送の検出がトリガーされます。



> 注:
>
> ファイルのドラッグアンドドロップを有効にし、ドラッグアンドドロップイベントをキャプチャするには、Citrix Studio で「ドラッグアンドドロップ」ポリシーを ［有効］ に設定します。

Web 閲覧アクティビティ　Session Recording により、サポートされている Web ブラウザーでユーザーアクティビティを検出し、録画中にイベントにタグ付けできます。ブラウザー名、URL、ページタイトルがログに記録されます。例として、以下のスクリーンショットを参照してください。

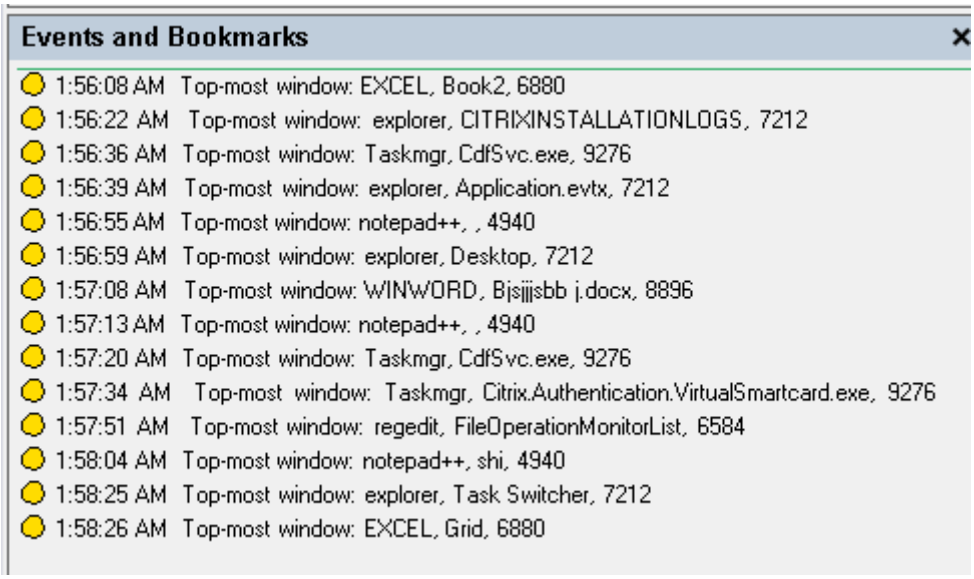
フォーカスのある Web ページからカーソルを動かすと、この Web ページの閲覧がタグ付けされますが、ブラウザー名は表示されません。この機能は、ユーザーが Web ページに滞在する時間を推定するために使用できます。例として、以下のスクリーンショットを参照してください。

サポートされているブラウザーの一覧:

ブラウザー	バージョン
Chrome	69 以降
Internet Explorer	11
Firefox	61 以降

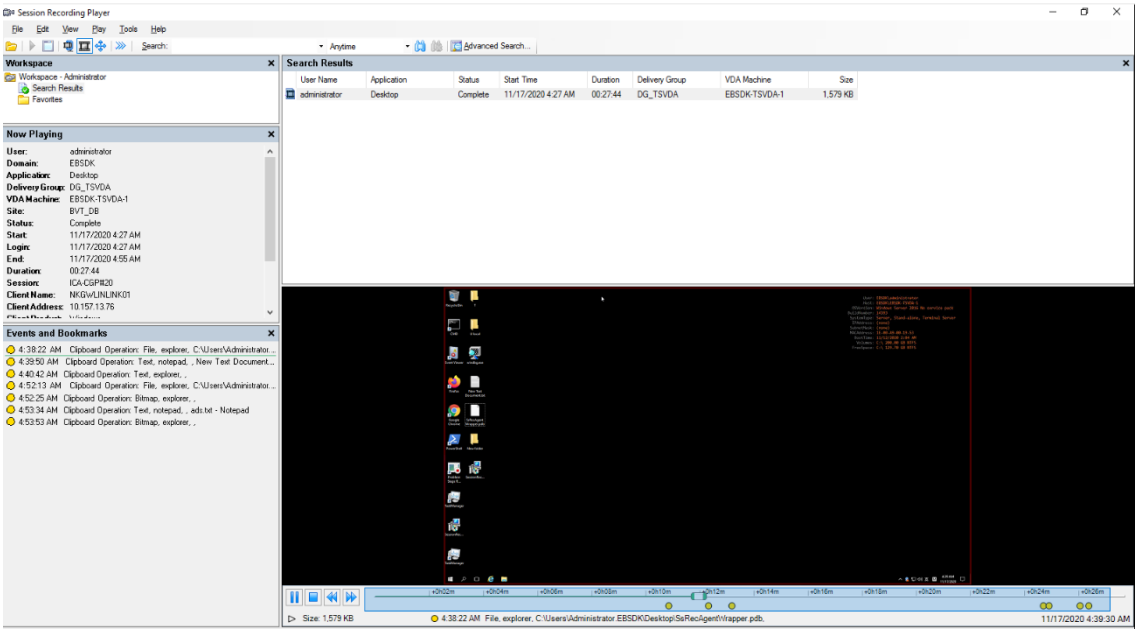
> 注:
>
> この機能には、Session Recording バージョン 1906 以降が必要です。

最前面のウィンドウのイベント　Session Recording では、アプリのウィンドウが他のすべてのウィンドウの前面にあるときにイベントを検出できます。プロセス名、タイトル、プロセス番号がログに記録されます。



クリップボードのアクティビティ　Session Recording では、クリップボードを使用した、テキスト、画像、ファイルのコピー操作を検出できます。プロセス名とファイルパスは、ファイルコピーのログとして記録されます。プロセス名とタイトルは、テキストコピーのログとして記録されます。プロセス名は、画像コピーのログとして記録されます。

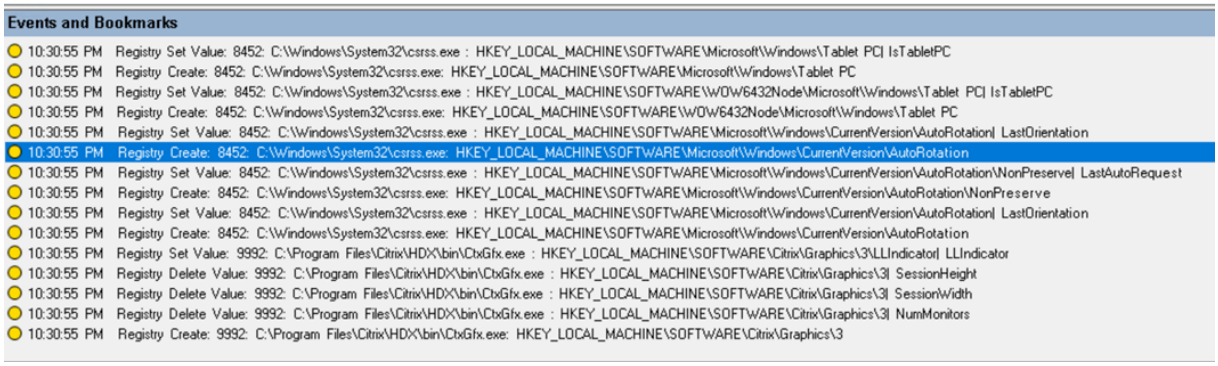
注：コピーされたテキストの内容は、デフォルトではログに記録されません。テキストの内容をログに記録するには、Session Recording Agent に移動し、`HKEY_LOCAL_MACHINE\SOFTWARE\ Citrix\SmartAuditor\Agent\CaptureClipboardContent`を1に設定します（デフォルト値は0です）。



Windows レジストリの変更　バージョン 2109 以降、Session Recording は、セッションの録画中に次のレジストリ変更を検出してログに記録できます:

レジストリ変更	対応するイベント
キーの追加	レジストリ - 作成
値の追加	レジストリ - 値の設定
キーの名前の変更	レジストリ - 名前の変更
値の名前の変更	レジストリ - 値の削除とレジストリ - 値の設定
既存の値の変更	レジストリ - 値の設定
キーの削除	レジストリ - 削除
値の削除	レジストリ - 値の削除

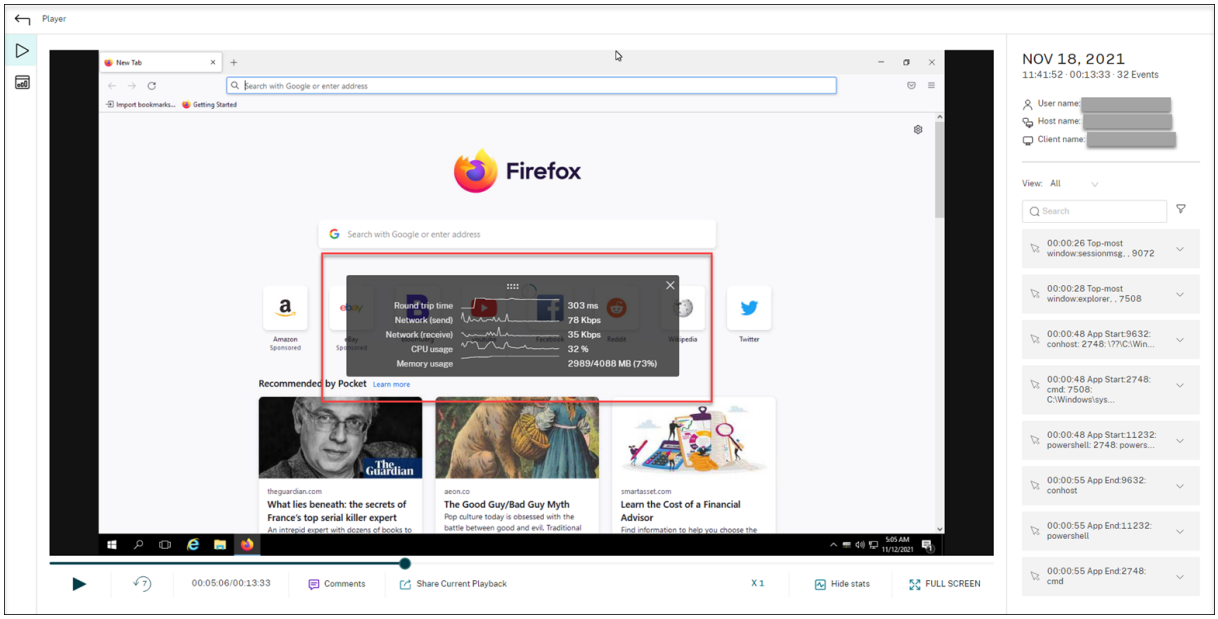
例:



このレジストリ監視機能を有効にするには、イベント検出ポリシーの ［レジストリの変更をログに記録する］オプションを選択します。

パフォーマンスデータ（録画されたセッションに関連するデータポイント）　イベント検出ポリシーを作成するときに、［パフォーマンスデータをログに記録する］を選択して、セッションデータオーバーレイ機能を有効にします。この機能では、Web Player でのセッション再生中に画面オーバーレイが導入されています。これは半透明のオーバーレイで、移動したり非表示にしたりできます。オーバーレイには、録画されたセッションに関連する次のデータポイントがあります:

- 往復時間
- ネットワーク（送信）
- ネットワーク（受信）
- CPU 使用率
- メモリ使用率



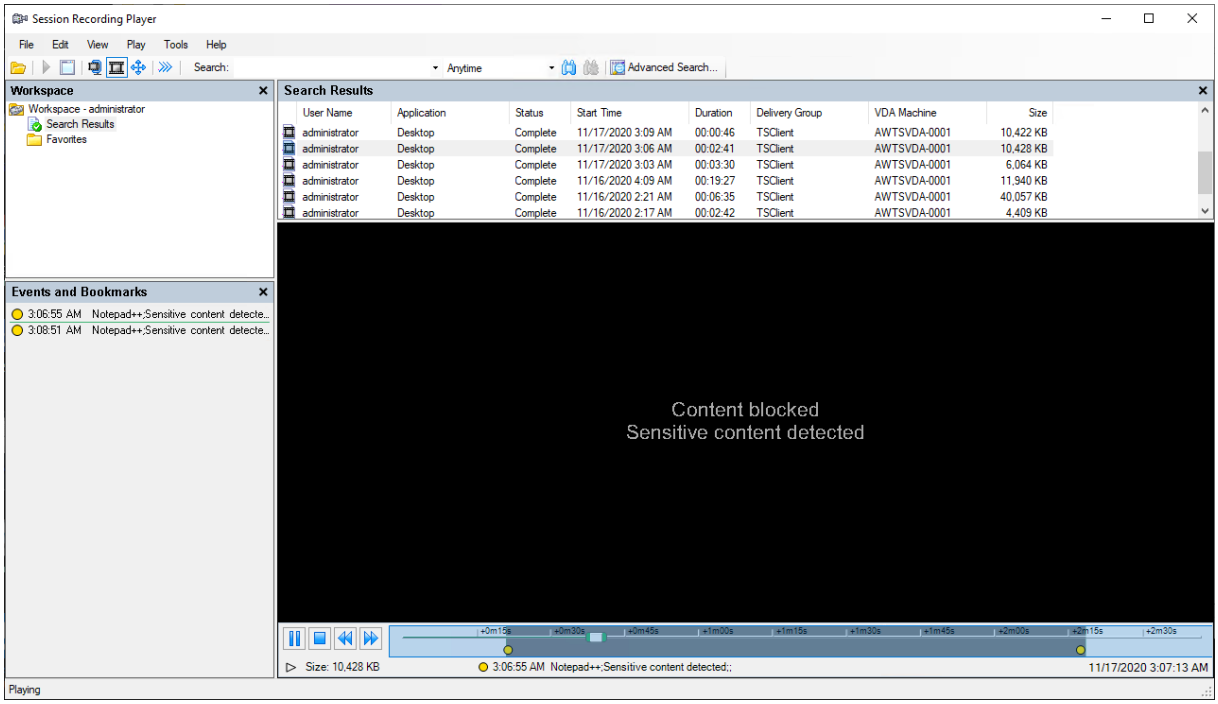
ポップアップウィンドウイベント　ユーザーが機密ファイルを開いたり閉じたり、フォルダにアクセスしたりすると、ポップアップウィンドウが表示され、プロンプトが表示されたり、パスワードの入力を求められたりする場合があります。Session Recording は、セッションの録画中にこのようなポップアップウィンドウイベントを監視できるようになりました。Web ブラウザのポップアップウィンドウは監視されないことに注意してください。

プロセス名やプロンプトの内容など、ポップアップウィンドウイベントの属性が録画されます。

カスタムイベント

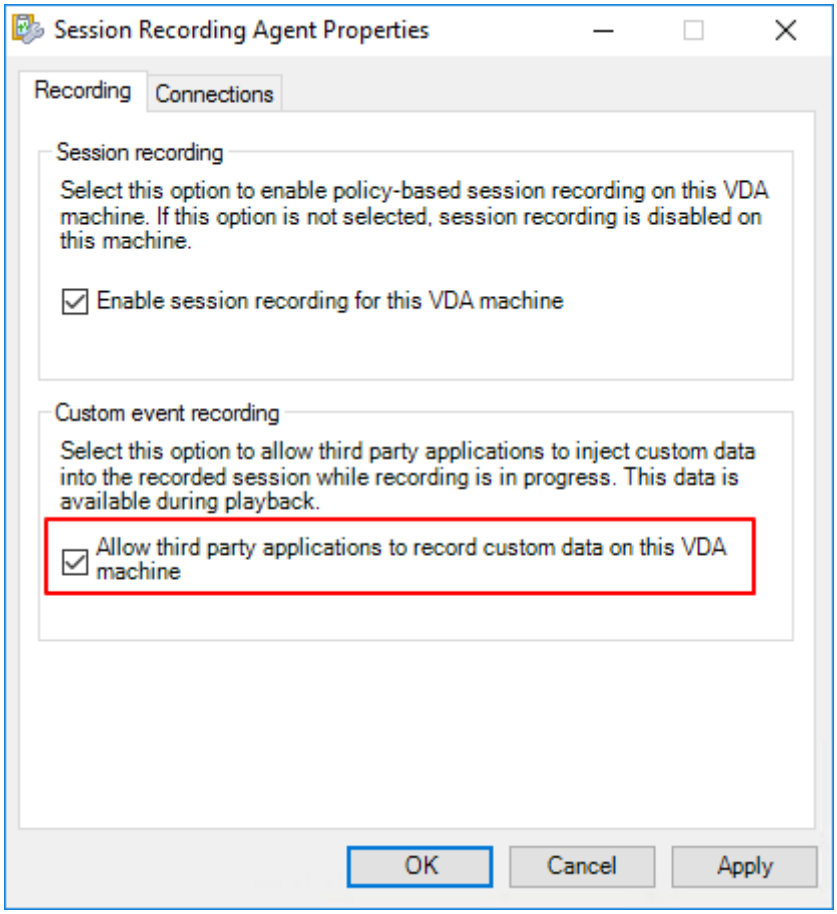
Session Recording Agent は、サードパーティアプリケーションがアプリケーション固有のイベントデータを、録画されたセッションに追加するときに使用できる IUserApi COM インターフェイスを提供します。イベントのカスタマイズに基づいて、Session Recording は機密情報をブロックしたり、セッションの一時停止イベントやセッション再開イベントをログに記録したりできます。

機密情報のブロック　Session Recording では、画面の録画時に特定の期間をスキップしたり、セッションの再生中に特定の期間の機密情報をブロックしたりすることができます。この機能を使用するには、Session Recording 2012 以降を使用します。



この機能を使用するには、次の手順を実行します:

1. [**Session Recording Agent** のプロパティ] で [この **VDA** マシンでサードパーティ製アプリケーションによるカスタムデータの記録を許可する] チェックボックスをオンにして、[適用] をクリックします。

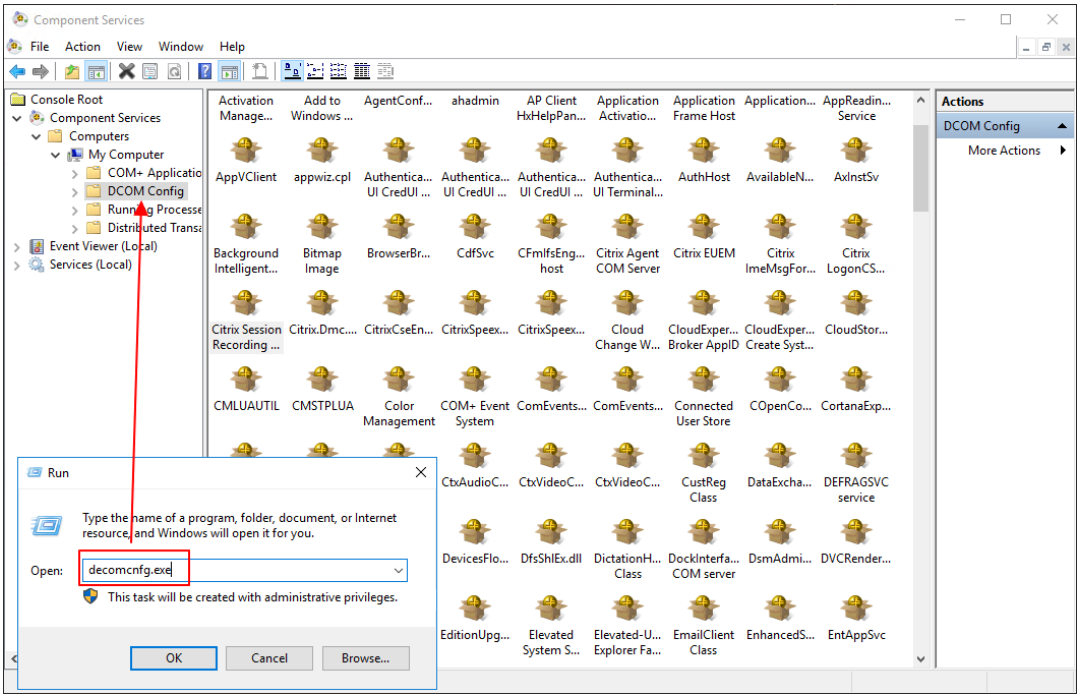


2. Session Recording イベント API（IUserApi COM インターフェイス）を呼び出す権限をユーザーに付与します。

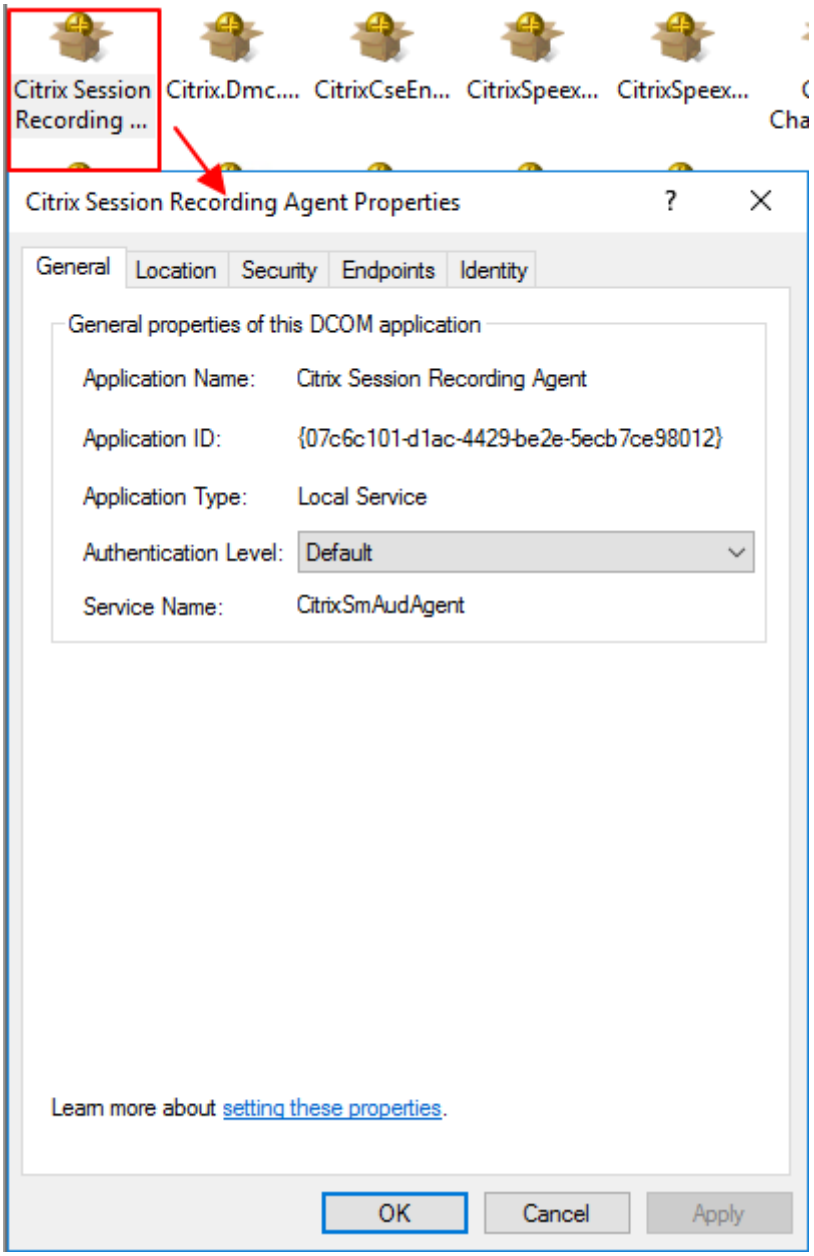
   Session Recording は、バージョン 7.15 でイベント API COM インターフェイスにアクセス制御を追加しました。許可されたユーザーのみが、イベントメタデータを録画に挿入する機能を呼び出すことができます。

   ローカル管理者には、デフォルトでこの権限が付与されています。他のユーザーにこのアクセス許可を付与するには、Windows の DCOM の構成ツールを使用します:

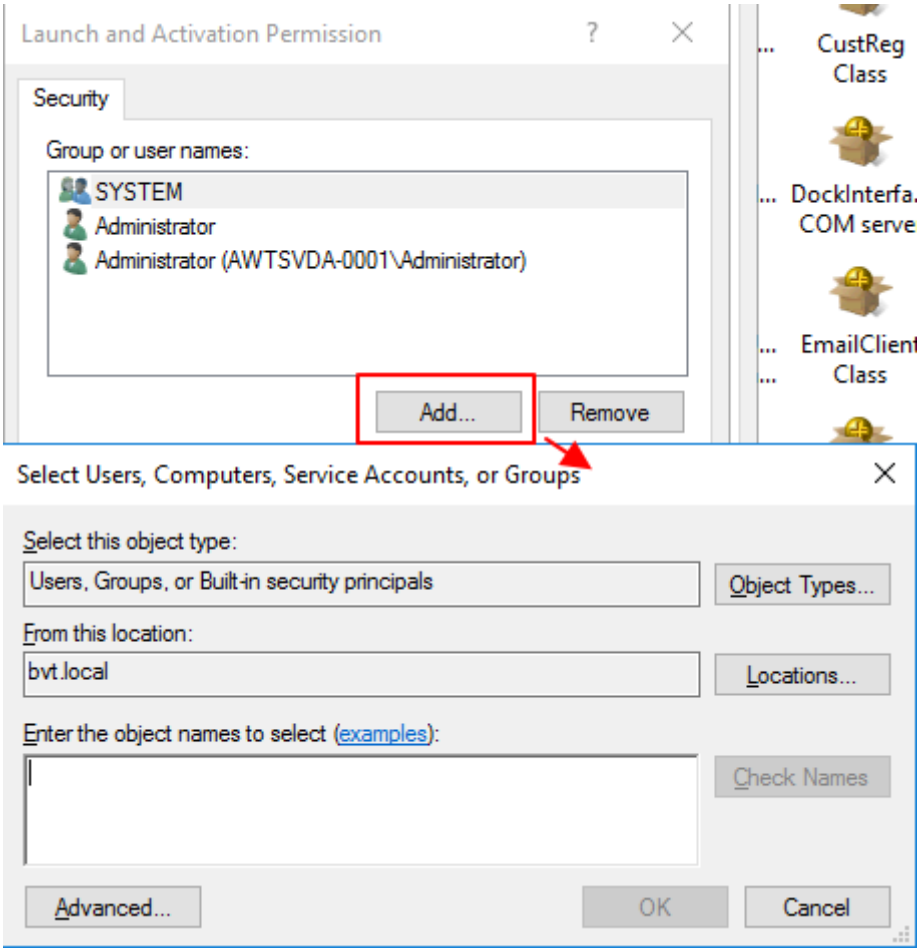
   a) `dcomcnfg.exe`を実行して、Session Recording Agent の Windows DCOM 構成ツールを開きます。

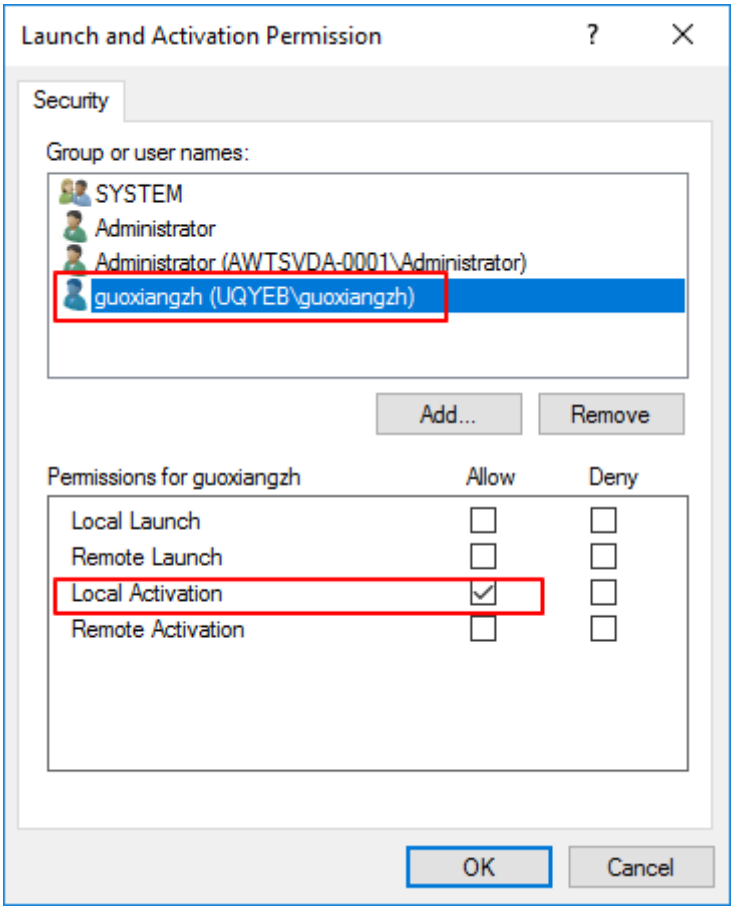


b) **Citrix Session Recording Agent** を右クリックし、［プロパティ］を選択します。



c) ［セキュリティ］タブを選択します。次に、［起動とアクティブ化のアクセス許可］セクションで ［編集］をクリックし、［ローカルからのアクティブ化］権限を持つユーザーを追加します。





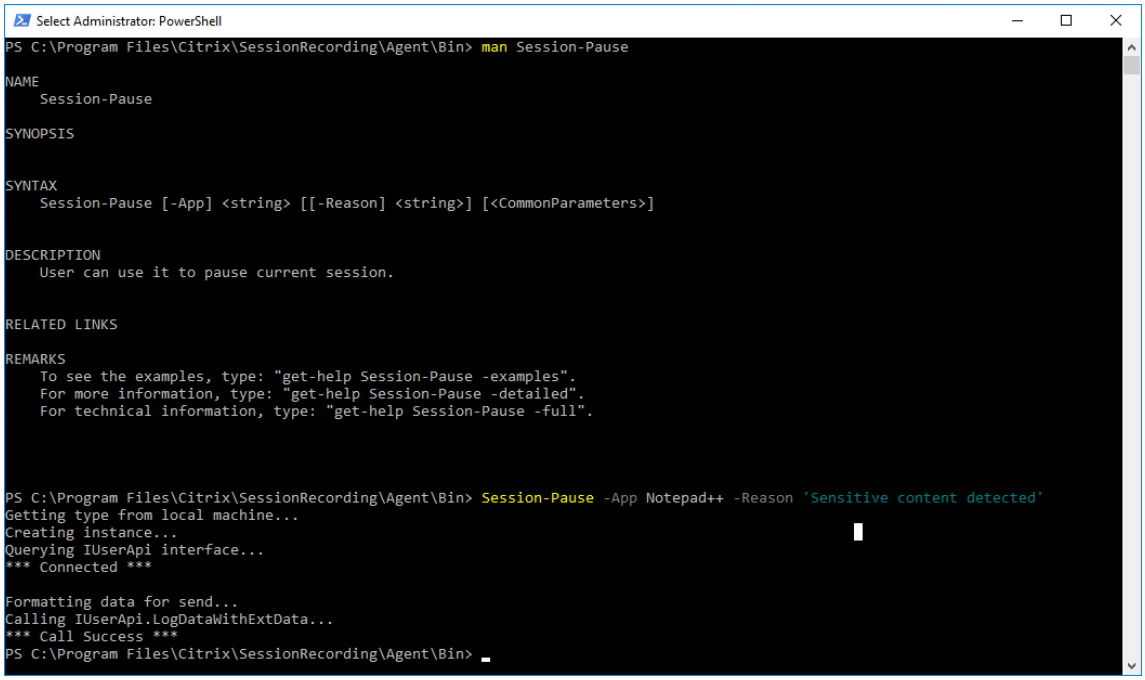
> 注:
>
> DCOM の構成はすぐに有効になります。サービスやマシンを再起動する必要はありません。

3. Citrix 仮想セッションを開始します。
4. PowerShell を起動して現在のドライブを **<Session Recording Agent** のインストールパス **>\Bin** フォルダーに変更し、SRUserEventHelperSnapin.dll モジュールをインポートします。
5. `Session-Pause`および`Session-Resume`コマンドレットを実行し、機密情報のブロックをトリガーするパラメーターを設定します。

パラメーター	説明	必須またはオプション
-APP	コマンドレットを呼び出すアプリ名。	必須

パラメーター	説明	必須またはオプション
-Reason	コンテンツがブロックされる理由。このパラメーターを指定しない場合は、コンテンツがブロックされていることおよび機密情報が存在し、ブロックされていることを示すデフォルト設定が表示されます。このパラメーターを設定すると、セッションの再生時にブロックされた期間に移動したときに、指定した理由が表示されます。	オプション

たとえば、次のようにSession-Pauseを実行できます:

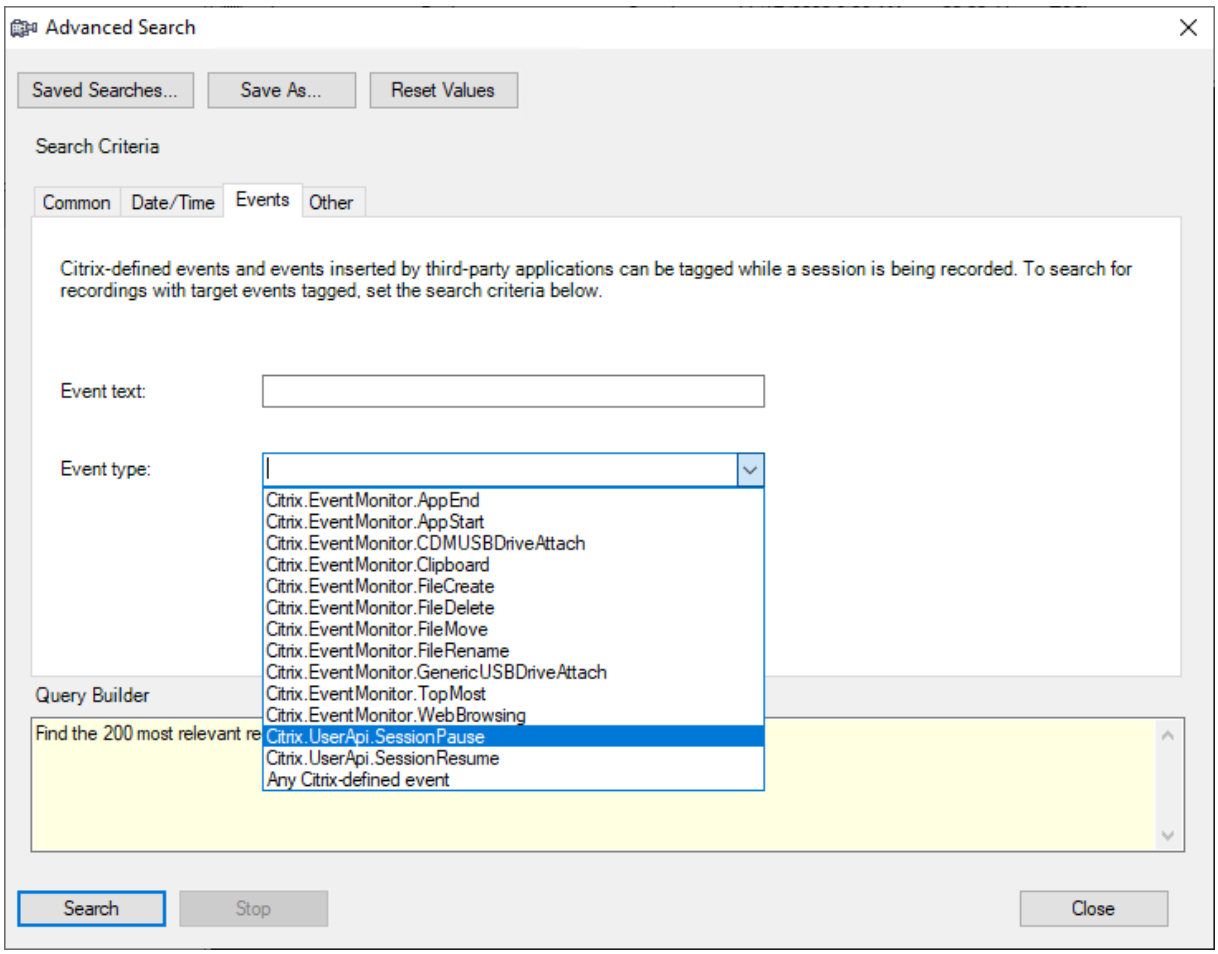


タグ付きイベントを使った録画の検索と再生

タグ付きイベントで録画を検索する　Session Recording Player を使用すると、タグ付きイベントの録画を詳細に検索できます。

1. [Session Recording Player] で、ツールバーの [高度な検索] をクリックするか、[ツール] > [高度な 検索] の順に選択します。
2. [高度な検索] ダイアログボックスで検索条件を定義します。

［イベント］タブでは、セッション内のタグ付きイベントをイベントテキストまたはイベントの種類別に、または両方を検索できます。［イベント］、［共通］、［日付/時刻］、［そのほか］の各フィルターを組み合わせて使用して、条件を満たす録画を検索できます。

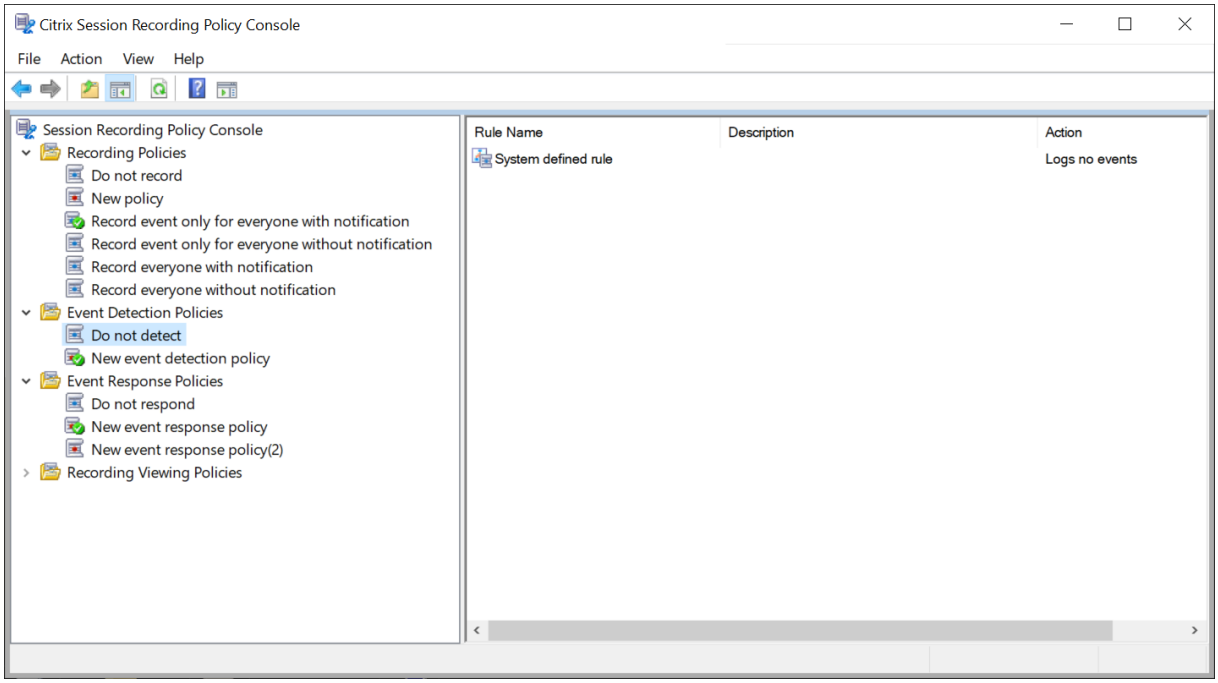


> 注:
>
> - ［イベントの種類］一覧には、すべてのイベントの種類が項目別に示されています。検索するイベントの種類を選択できます。［任意の **Citrix** 定義のイベント］を選択すると、イベントの種類にかかわらず Citrix Session Recording によってログに記録されたすべての録画を検索します。
> - イベントテキストフィルタは部分一致をサポートしています。ワイルドカードはサポートされません。
> - イベントテキストフィルターでは、照合時に大文字と小文字が区別されません。
> - イベントの種類の`App Start`、`App End`、`Client drive mapping`、`File Rename`という文字はイベントテキストで検索する場合、照合に使用されません。したがって、［イベントテキスト］ボックスに`App Start`、`App End`、`Client drive mapping`、または`File Rename`を入力すると、結果が見つかりません。

イベントを使用してセッションの録画内を移動したり、イベントがタグ付けされているポイントに飛ぶことができます。

システム定義のイベント検出ポリシー

システム定義のイベント検出ポリシーは「検出しない」です。デフォルトでは非アクティブです。アクティブの場合、イベントのログは記録されません。

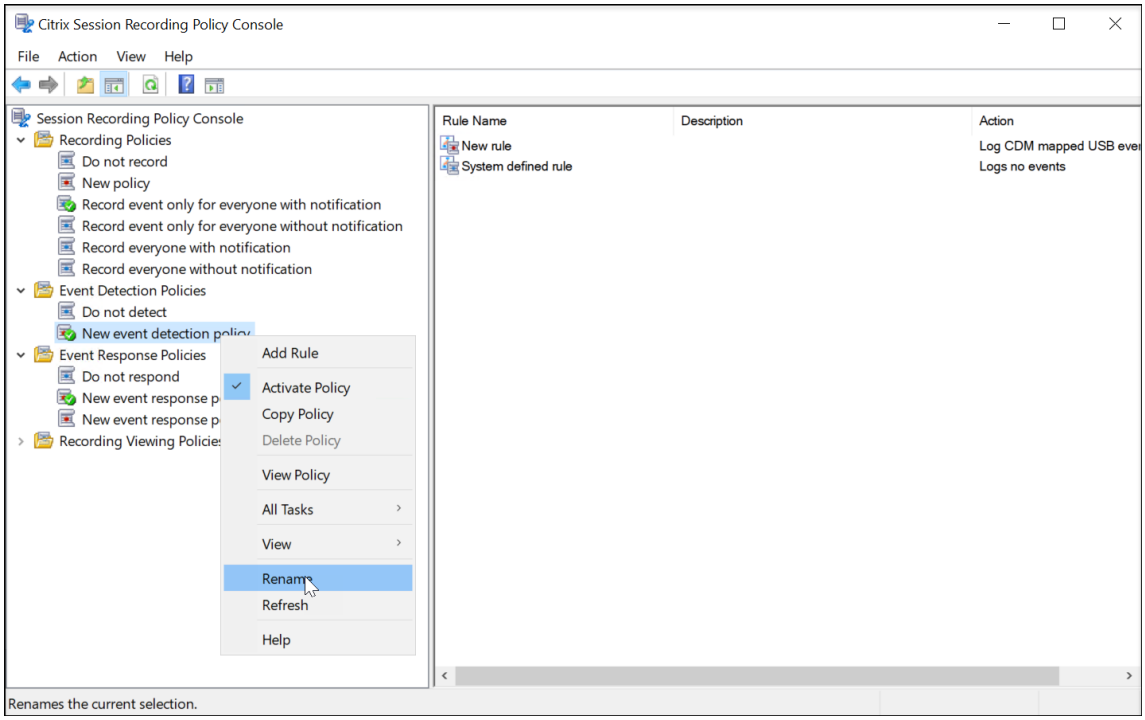


システム定義のイベント検出ポリシーは変更または削除できません。

カスタムイベント検出ポリシーの作成

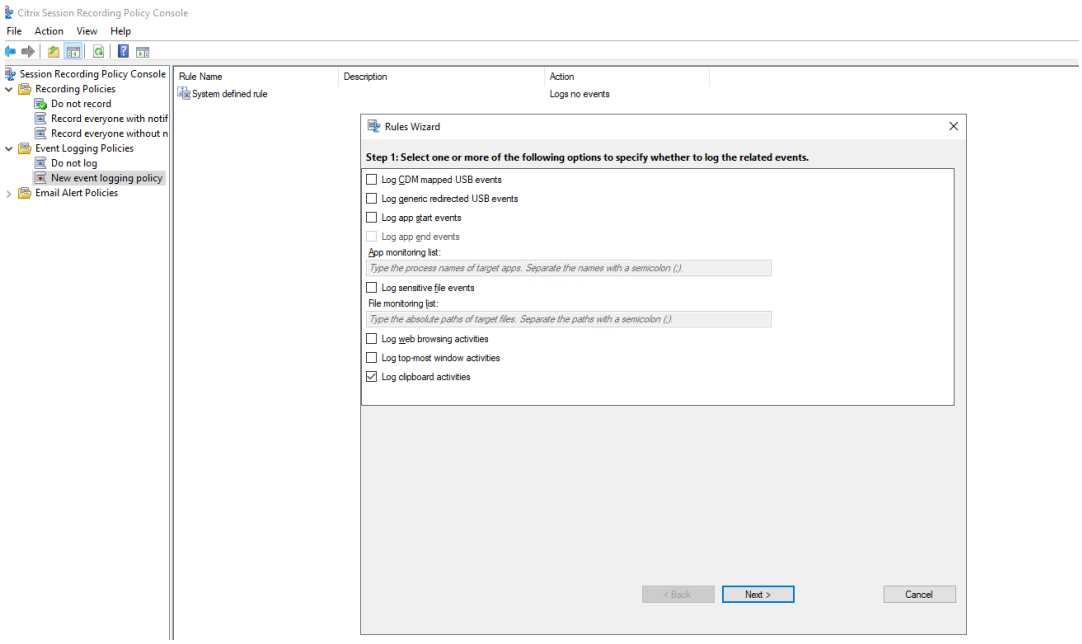
カスタムイベント検出ポリシーを作成するには:

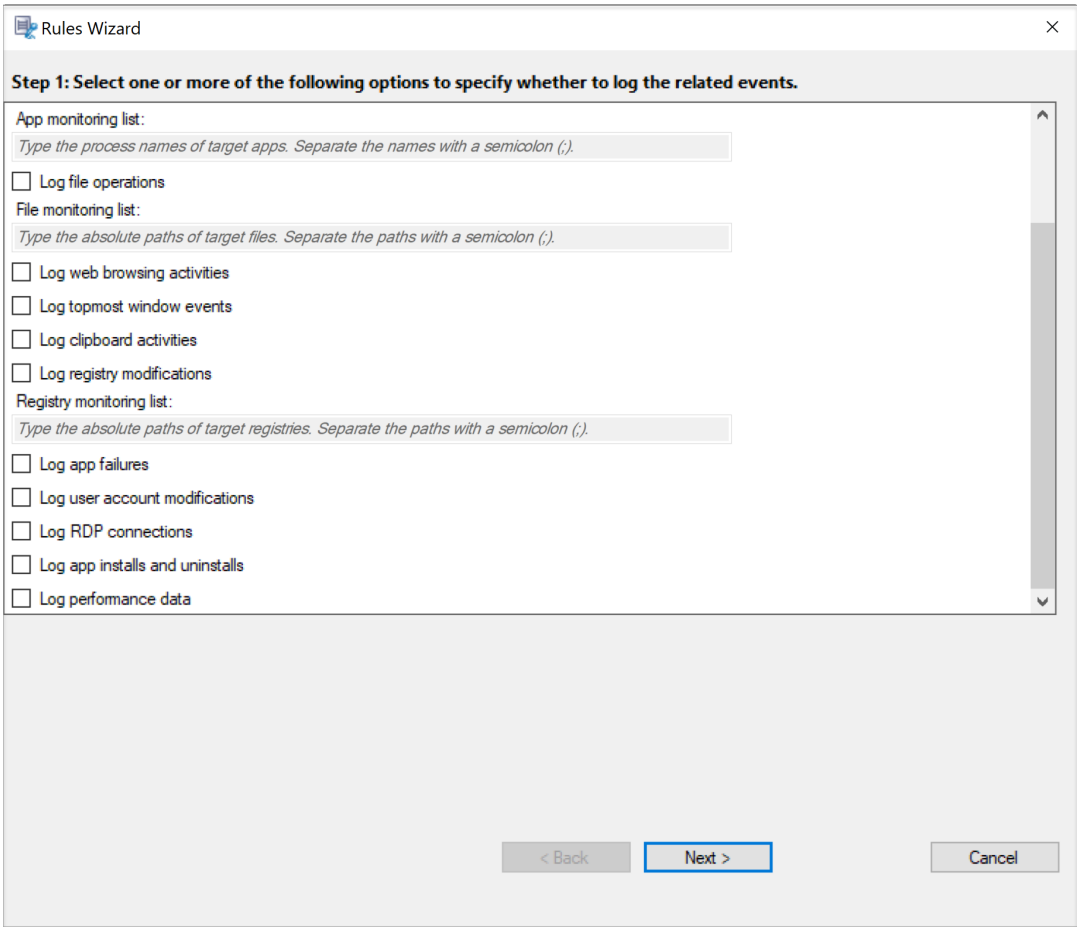
1. 承認済みのポリシー管理者として、Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recording ポリシーコンソールを起動します。
   デフォルトでは、アクティブなイベント検出ポリシーはありません。
3. 左ペインで ［イベント検出ポリシー］を選択します。メニューバーで ［新しいポリシーの追加］を選択してイベント検出ポリシーを作成します。
4. （オプション）新しいイベント検出ポリシーを右クリックして、名前を変更します。



5. 新しいイベント検出ポリシーを右クリックして ［規則の追加］をクリックします。

   a) 各イベントの種類のチェックボックスをオンにして、監視する 1 つまたは複数の対象イベントを指定します。ウィンドウを下方向にスクロールして、使用可能なすべてのイベントの種類を表示します。





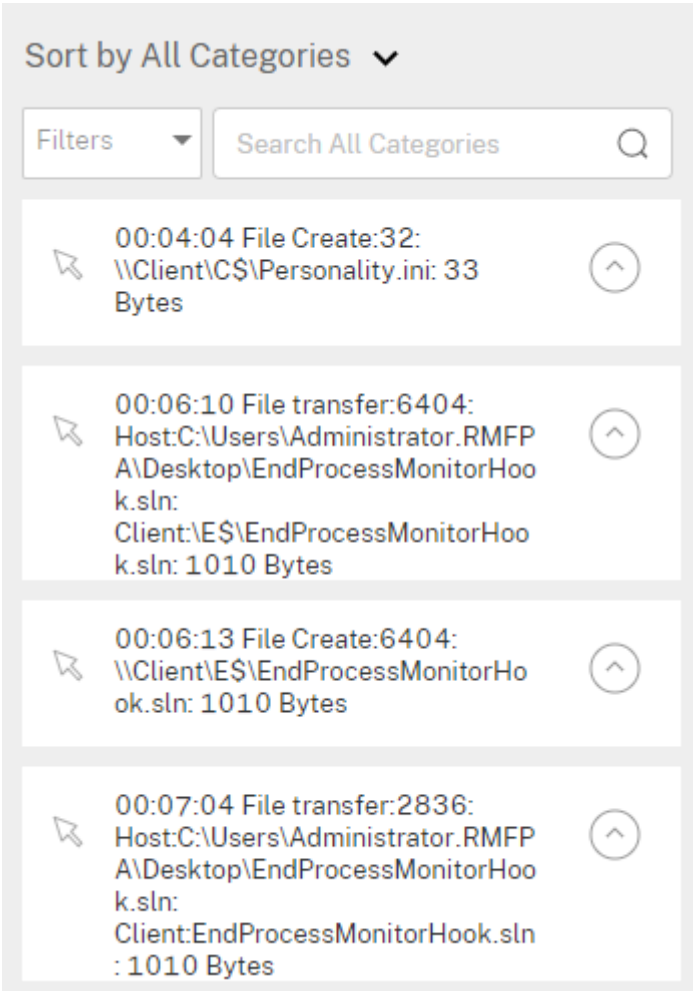
- **CDM** でマッピングされた **USB** イベントのログを記録する：Windows 向けまたは Mac 向け Citrix Workspace アプリがインストールされているクライアントで、クライアントドライブマッピング（CDM）を使用した大容量記憶装置デバイスが挿入されると、ログに記録します。
- 汎用 **USB** リダイレクトをログに記録する： Windows 向けまたは Mac 向け Citrix Workspace アプリがインストールされているクライアントで、汎用リダイレクトを使用した大容量記憶装置デバイスが挿入されると、ログに記録します。
- アプリ起動イベントのログを記録する：ターゲットアプリケーションの起動のログを記録します。
- アプリ終了イベントのログを記録する：ターゲットアプリケーションの終了のログを記録します。

  > 注：
  >
  > ［アプリ終了イベントのログを記録する］チェックボックスは、［アプリ起動イベントのログを記録する］の選択前は灰色表示になっています。

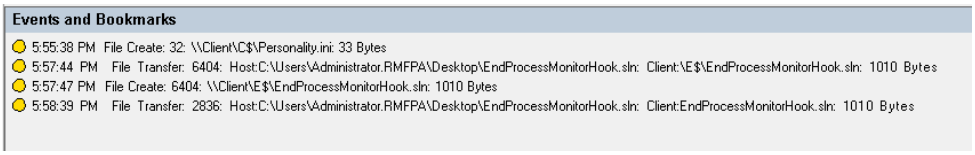
- アプリ監視一覧：［アプリ起動イベントのログを記録する］および ［アプリ終了イベントのログを記録する］を選択した場合、［アプリ監視一覧］でターゲットアプリケーションを指定して監視し、録画内に過剰にイベントを発生させないようにします。

> 注:
>
> - アプリケーションの起動と終了をキャプチャするには、[アプリ監視一覧]にアプリケーションのプロセス名を追加します。たとえば、リモートデスクトップ接続の起動イベントをキャプチャするには、プロセス名`mstsc.exe`を［アプリ監視一覧］に追加します。プロセスを ［アプリ監視一覧］に追加すると、追加したプロセスとその子プロセスにより実行されるアプリケーションが監視されます。Session Recording はプロセス名`cmd.exe`、`powershell.exe`、`wsl.exe`を ［アプリ監視一覧］にデフォルトで追加します。イベント検出ポリシーで ［アプリ起動イベントのログを記録する］および［アプリ終了イベントのログを記録する］を選択すると、コマンドプロンプト、PowerShell、Windows Subsystem for Linux（WSL）アプリの起動および終了が、これらのプロセス名が手動で ［アプリ監視一覧］に加えられているかどうかにかかわらず、ログ記録されます。デフォルトのプロセス名は、［アプリ監視一覧］には表示されません。
> - プロセス名はセミコロン（;）で区切ります。
> - 完全一致のみがサポートされています。ワイルドカードはサポートされません。
> - 追加するプロセス名では、大文字と小文字は区別されません。
> - 録画内に過剰にイベントを発生させないように、システムプロセス名（explorer.exe など）や Web ブラウザーをレジストリに追加しないでください。

- ファイル操作のログを記録する:［ファイル監視一覧］のターゲットファイルでの操作のログと、セッションホスト（VDA）とクライアントデバイス（マップされたクライアントドライブと汎用リダイレクトを使用した大容量記憶装置デバイスを含む）との間のファイル転送のログを記録します。このオプションを選択すると、［ファイル監視一覧］を指定するかに関係なく、ファイル転送のログ記録がトリガーされます。
  - Web Player に表示されるファイルイベント



  - Session Recording Player に表示されるファイルイベント



- ファイル監視一覧：［ファイル操作をログに記録する］を選択する場合、［ファイル監視一覧］を使用して監視対象のファイルを指定します。フォルダーを指定すると、フォルダー内のすべてのファイルをキャプチャできます。デフォルトでは、ファイルが指定されていないため、ファイルはキャプチャされません。

  > 注：
  >
  > - ファイルの名前変更、作成、削除、移動操作をキャプチャするには、［ファイル監視一覧］でファイルフォルダーのパス文字列（ファイル名やファイルフォルダーのルートパスではなく）を追加します。たとえば、`C:\User\File`の`sharing.ppt`ファイルの名前変更、作成、削除、移動操作をキャプチャするには、［ファイル監視一覧］でパス文字

> 列C:\User\Fileを追加します。
> - ローカルファイルパスおよびリモート共有フォルダーパスの両方を使用できます。たとえば、\\remote.address\Documentsフォルダーの RemoteDocument.txt ファイルで操作をキャプチャするには、[ファイル監視一覧] でパス文字列\\remote.address\Documentsを追加します。
> - セミコロン（;）で監視パスを区切ります。
> - 完全一致のみがサポートされています。ワイルドカードはサポートされません。
> - パス文字列は大文字と小文字を区別しません。

制限事項:

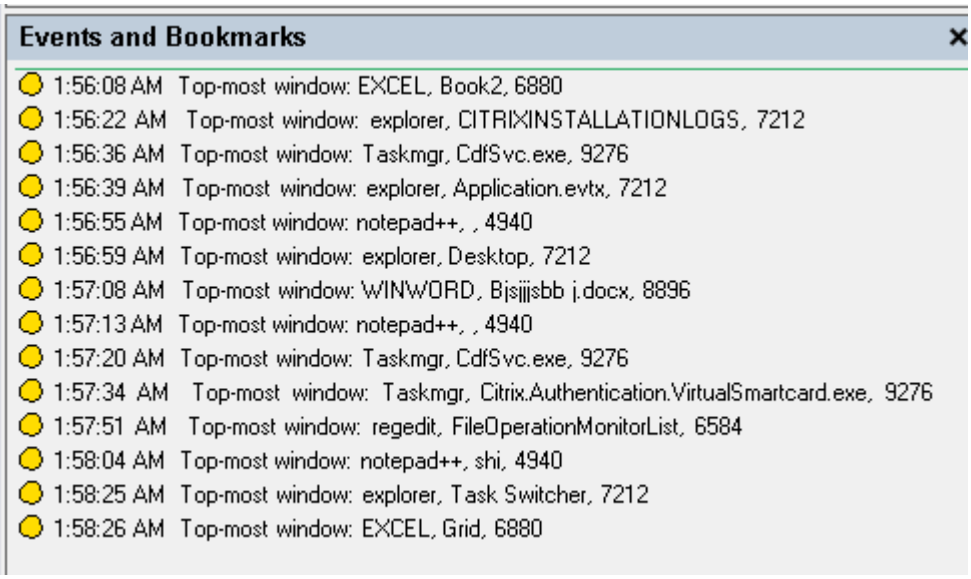
- 監視されているフォルダーから監視されていないフォルダーへのファイルまたはフォルダーのコピーはキャプチャされません。
- ファイルまたはフォルダーパスに、260 文字を超える名前のファイルまたはフォルダーが含まれている場合、ファイルまたはフォルダーの操作はキャプチャされません。
- データベースのサイズに注意してください。大量のイベントがキャプチャされないようにするには、定期的に「Event」テーブルをバックアップするか削除します。
- 短時間で大量のイベントがキャプチャされる場合、Player での表示およびデータベースへの格納は種類ごとに 1 つのイベントのみになり、ストレージの拡大を回避します。

- **Web** 閲覧アクティビティをログに記録する：サポートされているブラウザーでユーザーアクティビティをログ記録し、録画にブラウザー名、URL、ページタイトルのタグを付けます。

サポートされているブラウザーの一覧:

ブラウザー	バージョン
Chrome	69 以降
Internet Explorer	11
Firefox	61 以降

- 最前面のウィンドウイベントをログに記録する：最前面のウィンドウのイベントをログに記録して、録画にプロセス名、タイトル、プロセス番号のタグを追加します。



- クリップボードのアクティビティをログに記録する：クリップボードを使用した、テキスト、画像、ファイルのコピー操作をログに記録します。プロセス名とファイルパスは、ファイルコピーのログとして記録されます。プロセス名とタイトルは、テキストコピーのログとして記録されます。プロセス名は、画像コピーのログとして記録されます。
- レジストリの変更をログに記録する：Windows レジストリの変更（キーまたは値の追加、キーまたは値の名前の変更、既存の値の変更、キーまたは値の削除）をログに記録します。
- レジストリ監視リスト：［レジストリの変更をログに記録する］を選択する場合は、監視するターゲットレジストリの絶対パスを入力し、パスをセミコロンで区切ります。HKEY_USERS、HKEY_LOCAL_MACHINE、または HKEY_CLASSES_ROOT でパスを開始します。たとえば、次のように入力します：`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows;HKEY_CLASSES_ROOT\GuestStateVDev`。この一覧を指定しないままにすると、レジストリ変更はキャプチャされません。
- アプリエラーをログに記録する：予期しないアプリの終了や応答しないアプリをログに記録します。この規則はすべてのアプリに適用されます。
- ユーザーアカウントの変更をログに記録する：ユーザーアカウントの変更（アカウントの作成、有効化、無効化、削除、ロックアウト、名前の変更、パスワード変更の試行）をログに記録します。
- **RDP** 接続をログに記録する：録画されたセッションをホストしている VDA から開始された RDP 接続をログに記録します。
- アプリのインストールとアンインストールをログに記録する：録画されたセッション中のアプリのインストールとアンインストールをログに記録します。この規則はすべてのアプリに適用されます。
- パフォーマンスデータをログに記録する：セッションデータオーバーレイ機能を有効にします。録画されたセッションに関連するデータポイントを表示するには、このチェックボックスを選択しま

す。

- ポップアップウィンドウをログに記録する：ユーザーが機密ファイルを開いたり閉じたり、フォルダにアクセスしたりするときに表示されることがあるポップアップウィンドウをログに記録します。

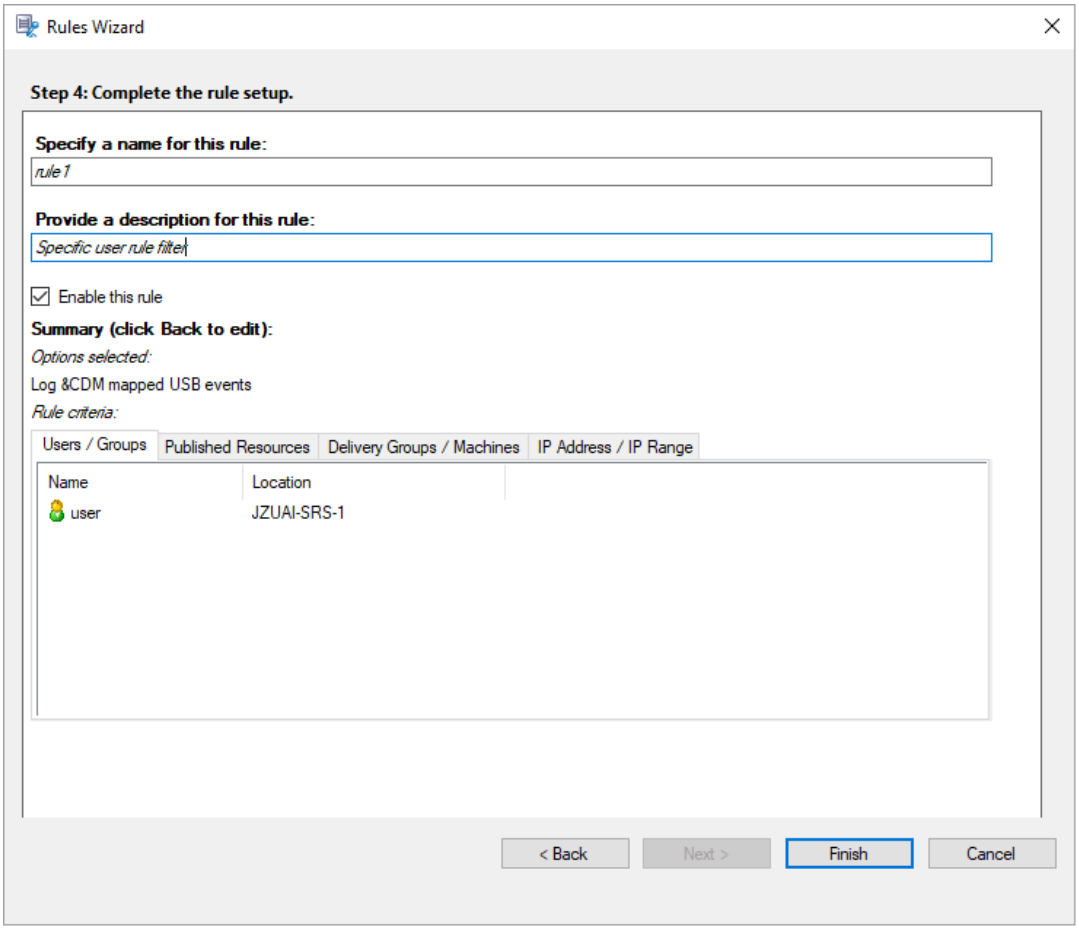
b) 規則条件を選択して編集します。

カスタム録画ポリシーの作成と同様、次の 1 つまたは複数の規則条件を選択できます：ユーザーまたはグループ、公開アプリケーションまたはデスクトップ、デリバリーグループまたはマシン、**IP** アドレスまたは **IP** の範囲。公開されているアプリケーションまたはデスクトップや、デリバリーグループまたは VDA マシンの一覧を取得するには、サイト管理者の読み取り権限が必要です。サイトの Delivery Controller で管理者の読み取り権限を構成します。

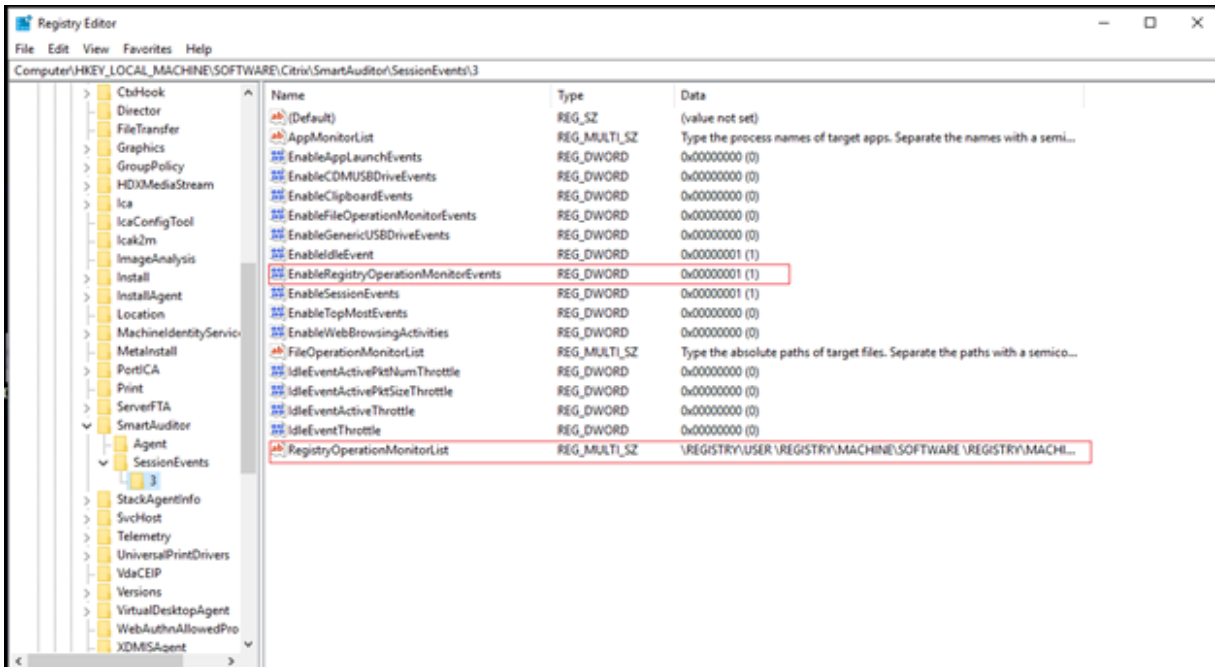
詳しくは、「カスタム録画ポリシーの作成」セクションで手順を参照してください。

> 注：
>
> イベント検出ポリシーの規則条件のいずれにも当てはまらないセッションがある可能性があります。これらのセッションの場合、フォールバック規則の操作（常に「検出しない」）が適用されます。フォールバック規則は変更または削除できません。

c) ウィザードの指示に従って構成を完了します。



イベント検出ポリシーに一致するセッションが開始されると、セッション ID とそのイベントレジストリ値が Session Recording Agent に表示されます。例:



レジストリ構成との互換性

Session Recording が新しくインストールされた場合、またはアップグレードされた場合、デフォルトで使用できるアクティブなイベント検出ポリシーはありません。この場合、Session Recording Agent は`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SessionEvents`のレジストリ値に従って特定イベントのログを記録するかどうかを決定します。レジストリ値の説明については、次の表を参照してください:

レジストリ値	説明
EnableSessionEvents	**1**: イベントの検出をグローバルに有効にする、**0**: イベントの検出をグローバルに無効にする（デフォルトの値のデータ）。
EnableAccountChangeEvents	**1**: ユーザーアカウントの変更の検出を有効にする、**0**: ユーザーアカウントの変更の検出を無効にする（デフォルト値のデータ）。
EnableAppChangeEvents	**1**: アプリのインストールとアンインストールの検出を有効にする、0: アプリのインストールとアンインストールの検出を無効にする（デフォルト値のデータ）。
EnableAppFaultEvents	**1**: アプリエラーの検出を有効にする、**0**: アプリエラーの検出を無効にする（デフォルト値のデータ）。
EnableAppLaunchEvents	**1**: アプリの起動のみの検出を有効にする、**2**: アプリの起動と終了の両方の検出を有効にする、**0**: アプリの起動と終了の検出を無効にする（デフォルトの値のデータ）。
AppMonitorList	監視するターゲットアプリを指定します。デフォルトでは、アプリが指定されていません。そのため、アプリのイベントはキャプチャされません。

レジストリ値	説明
EnableCDMUSBDriveEvents	**1**: CDM でマッピングされた USB 大容量記憶装置デバイスの挿入の検出を有効にする、**0**: CDM でマッピングされた USB 大容量記憶装置デバイスの挿入の検出を無効にする（デフォルトの値のデータ）。
EnableClipboardEvents	**1**: クリップボードのアクティビティの検出を有効にする、**0**: クリップボードのアクティビティの検出を無効にする（デフォルトの値のデータ）。
EnableFileOperationMonitorEvents	**1**: ファイル操作の検出を有効にする、**0**: ファイル操作の検出を無効にする（デフォルトの値のデータ）。
FileOperationMonitorList	監視するターゲットフォルダーを指定する。デフォルトでは、フォルダーが指定されていません。そのため、ファイル操作はキャプチャされません。
EnableGenericUSBDriveEvents	**1**: 汎用リダイレクトを使用した USB 大容量記憶装置デバイスの挿入の検出を有効にする、**0**: 汎用リダイレクトを使用した USB 大容量記憶装置デバイスの挿入の検出を無効にする（デフォルトの値のデータ）。
EnablePerfDataEvents	**1**: セッションデータオーバーレイ機能を有効にする、**0**: セッションデータオーバーレイ機能を無効にする（デフォルト値のデータ）。
EnablePopupWindowEvents	**1**: ポップアップウィンドウイベントの検出を有効にする、**0**: ポップアップウィンドウイベントの検出を無効にする（デフォルト値のデータ）。
EnableRDPConnectionEvents	**1**: RDP 接続の検出を有効にする、**0**: RDP 接続の検出を無効にする（デフォルトの値のデータ）。

レジストリ値	説明
EnableRegistryOperationMonitorEventTrig	**1**：Windows レジストリの変更の検出を有効にする、**0**：Windows レジストリの変更の検出を無効にする（デフォルト値のデータ）。
RegistryOperationMonitorList	監視するターゲットレジストリを指定する。デフォルトでは、レジストリが指定されていません。そのため、レジストリの変更のイベントはキャプチャされません。
EnableWebBrowsingActivities	**1**：Web 閲覧アクティビティの検出を有効にする、**0**：Web 閲覧アクティビティの検出を無効にする（デフォルトの値のデータ）。

以下は、互換性のあるシナリオです：

- Session Recording が新しくインストールされた場合、または、イベント検出（ログ記録）をサポートしない 1811 より前のリリースからアップグレードされた場合、各 Session Recording Agent の関連レジストリ値はデフォルト値です。デフォルトでは、アクティブなイベント検出ポリシーがないため、イベントのログは記録されません。
- Session Recording がイベントリリースをサポートする 1811 より前のリリースからアップグレードされた場合。アップグレード前にこの機能を無効にすると、各 Session Recording Agent の関連レジストリ値はデフォルトのままになります。デフォルトでは、アクティブなイベント検出ポリシーがないため、イベントのログは記録されません。
- Session Recording がイベント検出をサポートする 1811 より前のリリースからアップグレードされた場合。アップグレード前にこの機能を部分的にまたは完全に有効にすると、各 Session Recording Agent の関連レジストリ値は変更されません。デフォルトでは、アクティブなイベント検出ポリシーがないため、イベント検出の動作は変更されません。
- Session Recording が 1811 からアップグレードされた場合、ポリシーコンソールで構成されたイベント検出（ログ記録）ポリシーは引き続き使用されます。

> 注意：
>
> システム定義またはカスタムのイベント検出ポリシーをアクティブにすると、各 Session Recording Agent の関連レジストリ設定が無視されます。これを行うと、イベント検出にレジストリ設定を使用できなくなります。

イベント応答ポリシーの構成

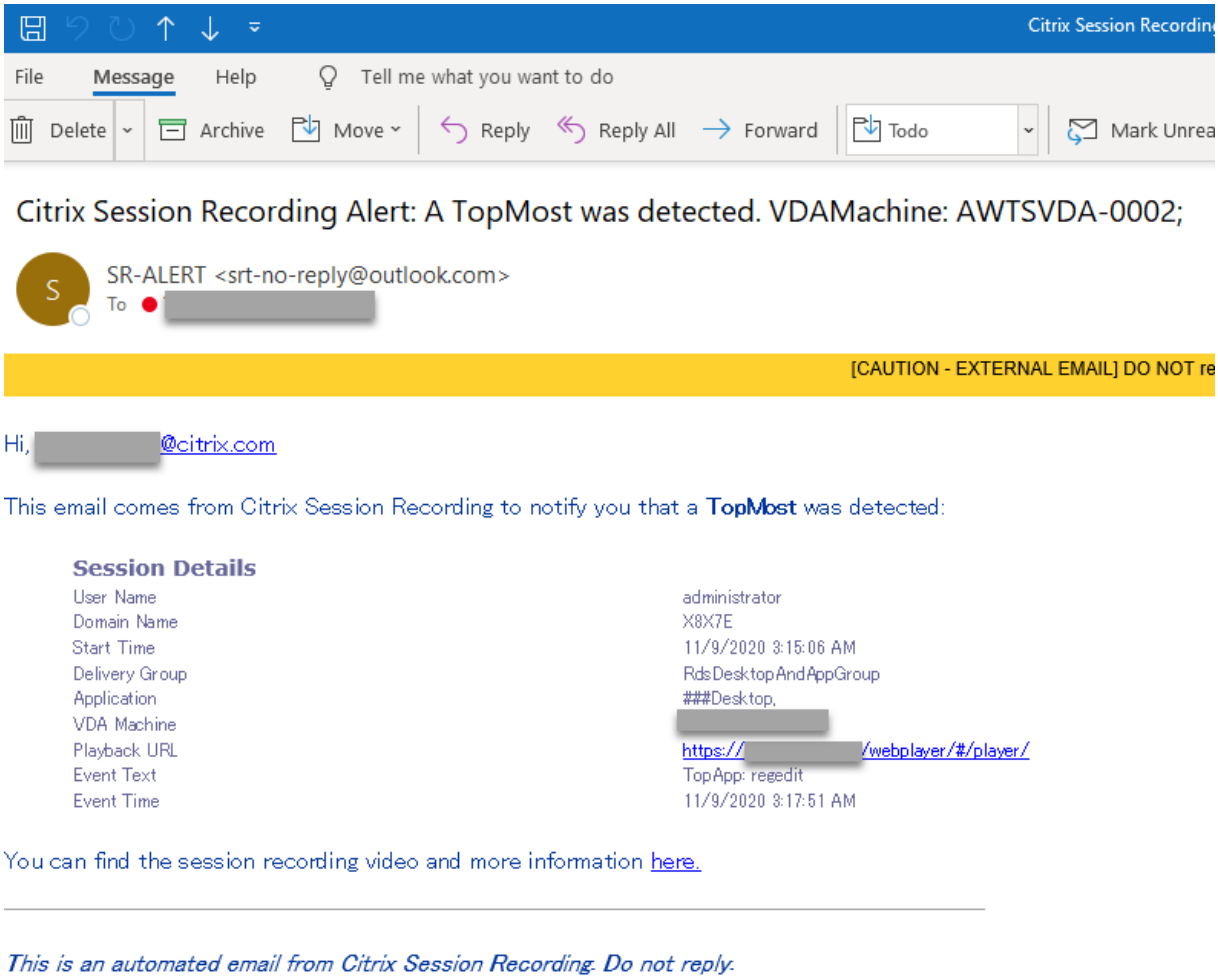
February 20, 2024

このポリシー設定を使用すると、録画されたセッションでログに記録されたイベントに応じて、次の操作を実行できます:

- メールアラートの送信
- 迅速な録画の開始
- セッションのロック
- セッションのログオフ
- セッションの切断

システム定義のイベント応答ポリシーは、「応答しない」のみです。必要に応じて、カスタムイベント応答ポリシーを作成できます。一度にアクティブにできるイベント応答ポリシーは 1 つだけです。

以下のスクリーンショットは、メールアラートの例です:



> ヒント：
>
> 再生 URL をクリックすると、Web Player で録画されたセッションの再生ページが開きます。ここをクリックすると、Web Player の ［すべての録画］ページが開きます。

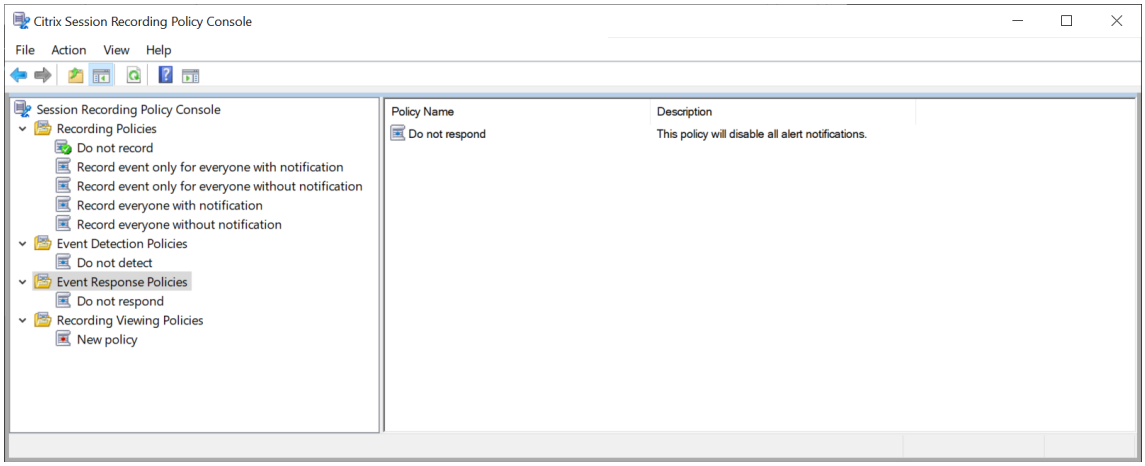
システム定義のイベント応答ポリシー

Session Recording は、1 つのシステム定義のイベント応答ポリシーを提供します。

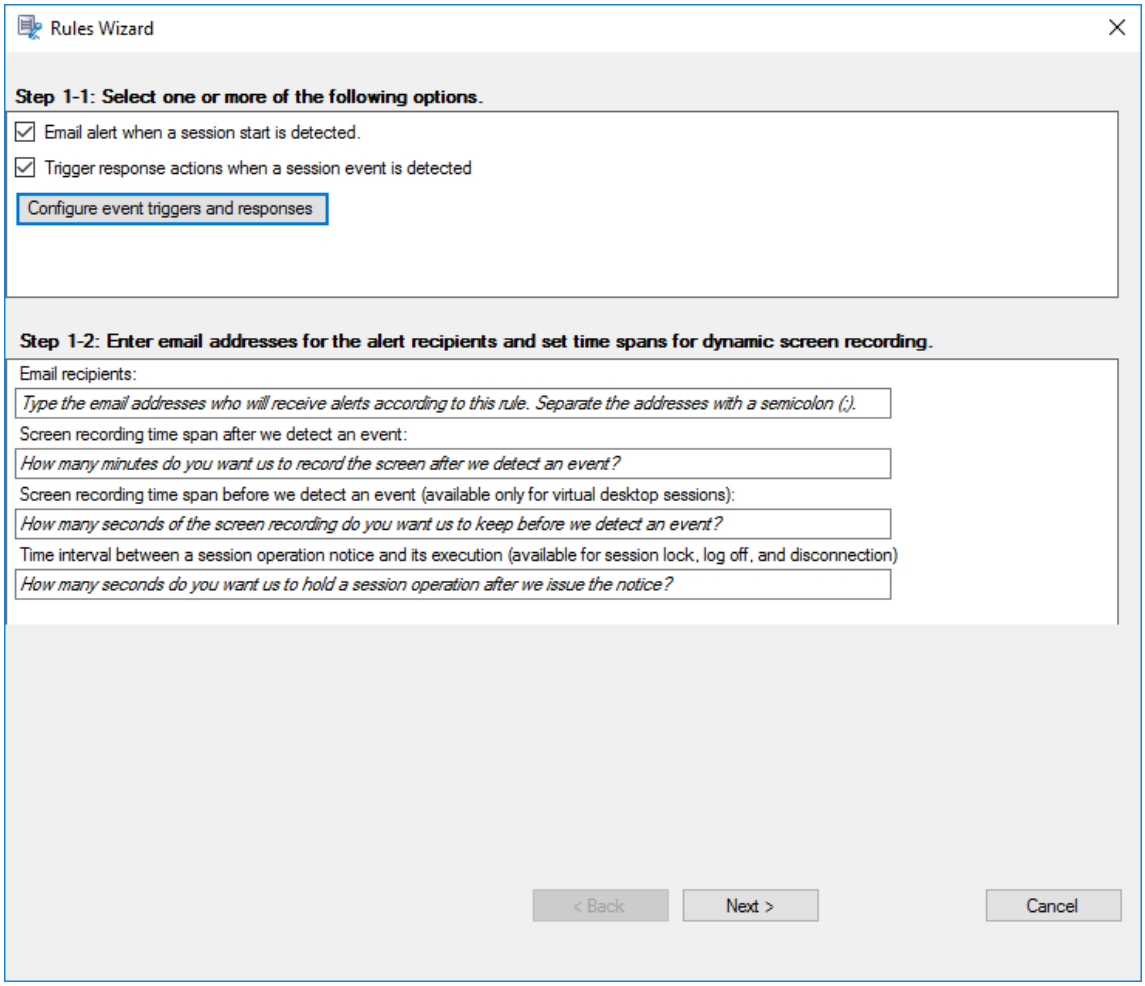
- 応答しない。デフォルトでは、録画でログ記録されたイベントに応じて操作が実行されることはありません。

カスタムイベント応答ポリシーの作成

1. 承認済みのポリシー管理者として、Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
2. Session Recording ポリシーコンソールを起動します。デフォルトでは、アクティブなイベント応答ポリシーはありません。



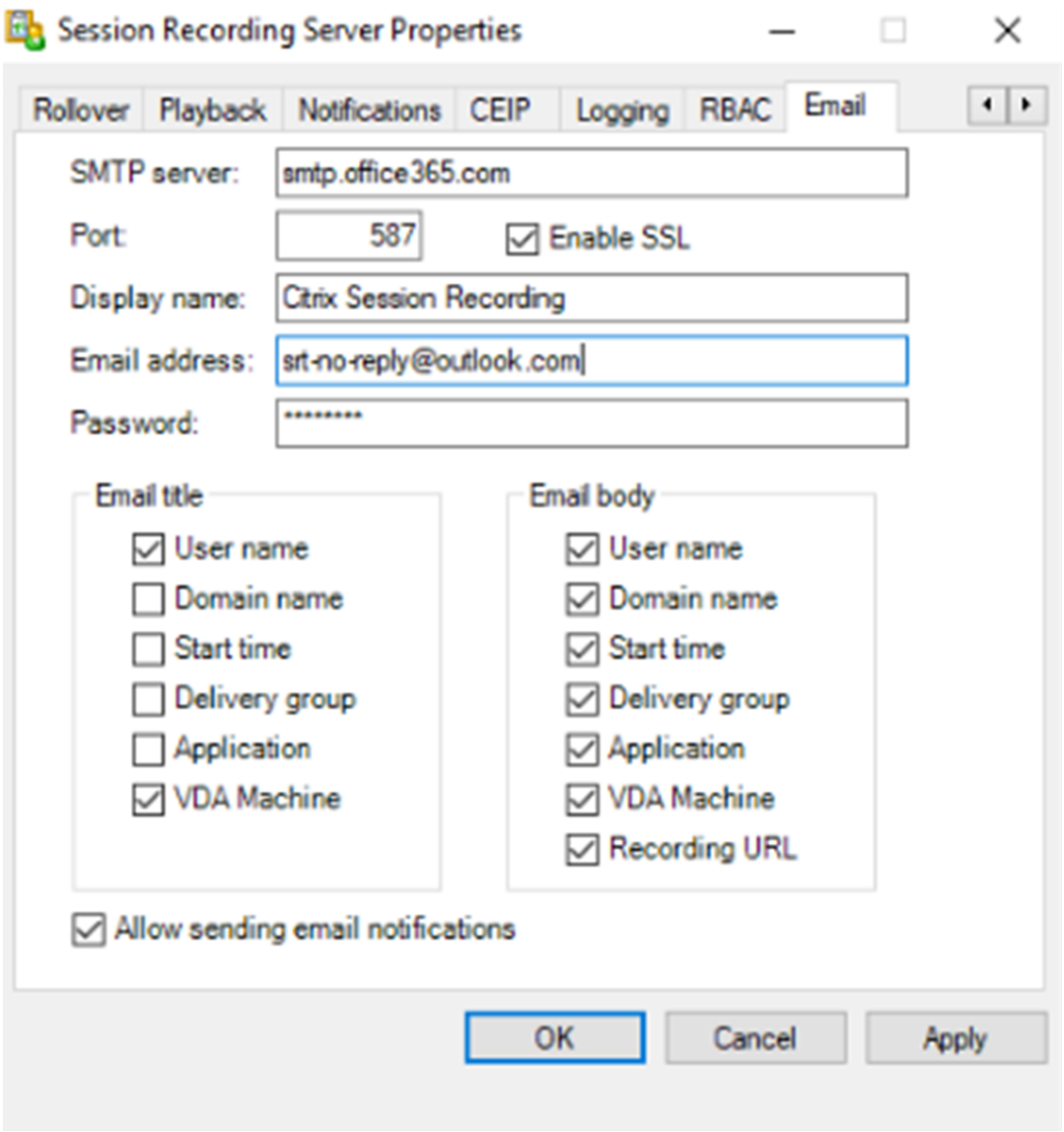
3. 左ペインで ［イベント応答ポリシー］を選択します。メニューバーで ［新しいポリシーの追加］を選択します。
4. （オプション）新しいイベント応答ポリシーを右クリックして、名前を変更します。
5. 新しいイベント応答ポリシーを右クリックして ［規則の追加］を選択します。
6. ［**Email alert when a session start is detected**］または ［**Use event triggers to specify how to respond when a session event is detected**］を選択します。



7.（オプション）メールの受信者と送信者のプロパティを設定します。

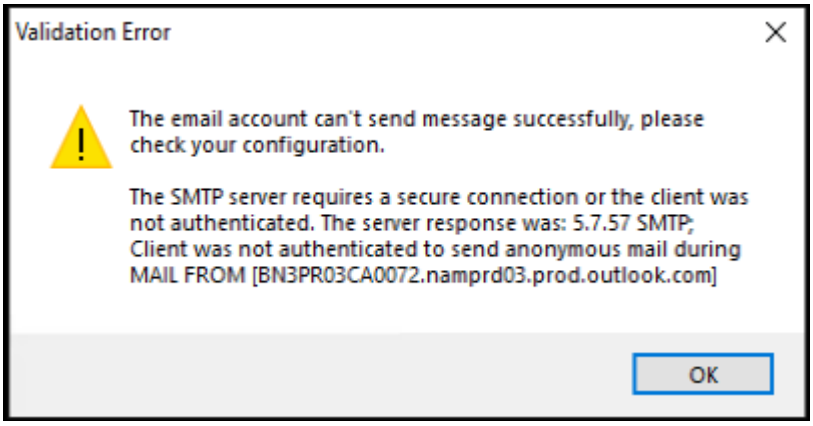
a)［規則］ウィザードで、アラート受信者のメールアドレスを入力します。

b)［**Session Recording** サーバーのプロパティ］で送信メールの設定を構成します。



注:

［メールタイトル］セクションで 3 つ以上のオプションを選択すると、メールの件名が長すぎる可能性があることを示す警告ダイアログが表示されます。［メール通知の送信を許可する］を選択して ［適用］をクリックすると、Session Recording はメールの設定を確認するメールを送信します。不正なパスワードやポートなど設定が正しくない場合、Session Recording はエラーの詳細を含むエラーメッセージを返します。



メール設定が有効になるまで約 5 分かかります。メール設定をすぐに有効にする場合、または設定に従ってメールが送信されない問題を修正する場合は、ストレージマネージャー（CitrixSsRecStorageManager）サービスを再起動します。また、バージョン 2006 以前から最新リリースにアップグレードする場合は、ストレージマネージャーサービスを再起動してください。

c) Web Player にアクセスするためのレジストリを編集します。

アラートメールの再生 URL を正常に機能させるには、HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Serverのレジストリキーを見つけて、次の手順を実行します:

- **LinkHost** の値データを、Web Player へのアクセスに使用するドメインの URL に設定します。たとえば、https://example.com/webplayer/#/player/の Web Player にアクセスするには、**LinkHost** の値データをhttps://example.comに設定します。
- 値 **EmailThreshold** を追加し、その値データを 1 から 100 の範囲の数値に設定します。値データは、メール送信アカウントが 1 秒以内に送信するアラートメールの最大数を決定します。この設定は、送信されるメールの数を抑え、CPU 使用率を削減するのに役立ちます。値データを指定しないままにするか、範囲外の数値に設定すると、値データは 25 にフォールバックします。

注:

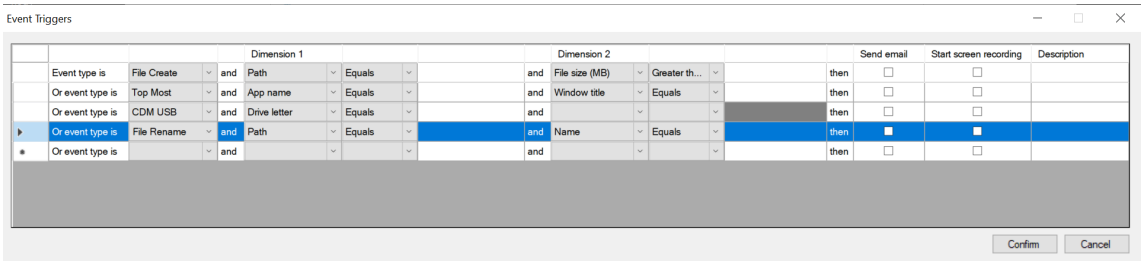
- メールサーバーは、メール送信アカウントをスパムボットとして扱い、メールの送信を阻止する可能性があります。アカウントでメールを送信できるようになる前に、そのアカウントが人間のユーザーによって使用されていることを確認するために、Outlook などのメールクライアントから要求がある場合があります。
- 一定期間内にメールを送信することに対する制限があります。たとえば、1 日の制限に達すると、翌日の開始までメールを送信できません。この場合、制限の数が期間内に録画されているセッションの数を超えていることを確認してください。

8.（オプション）イベントトリガーとイベント応答を構成します。

[**Trigger response actions when a session event is detected**] を選択すると、[**Configure event**

triggers and responses］ボタンが使用可能になります。これをクリックして、次の応答アクションをトリガーできるログ記録されたイベントを指定します：

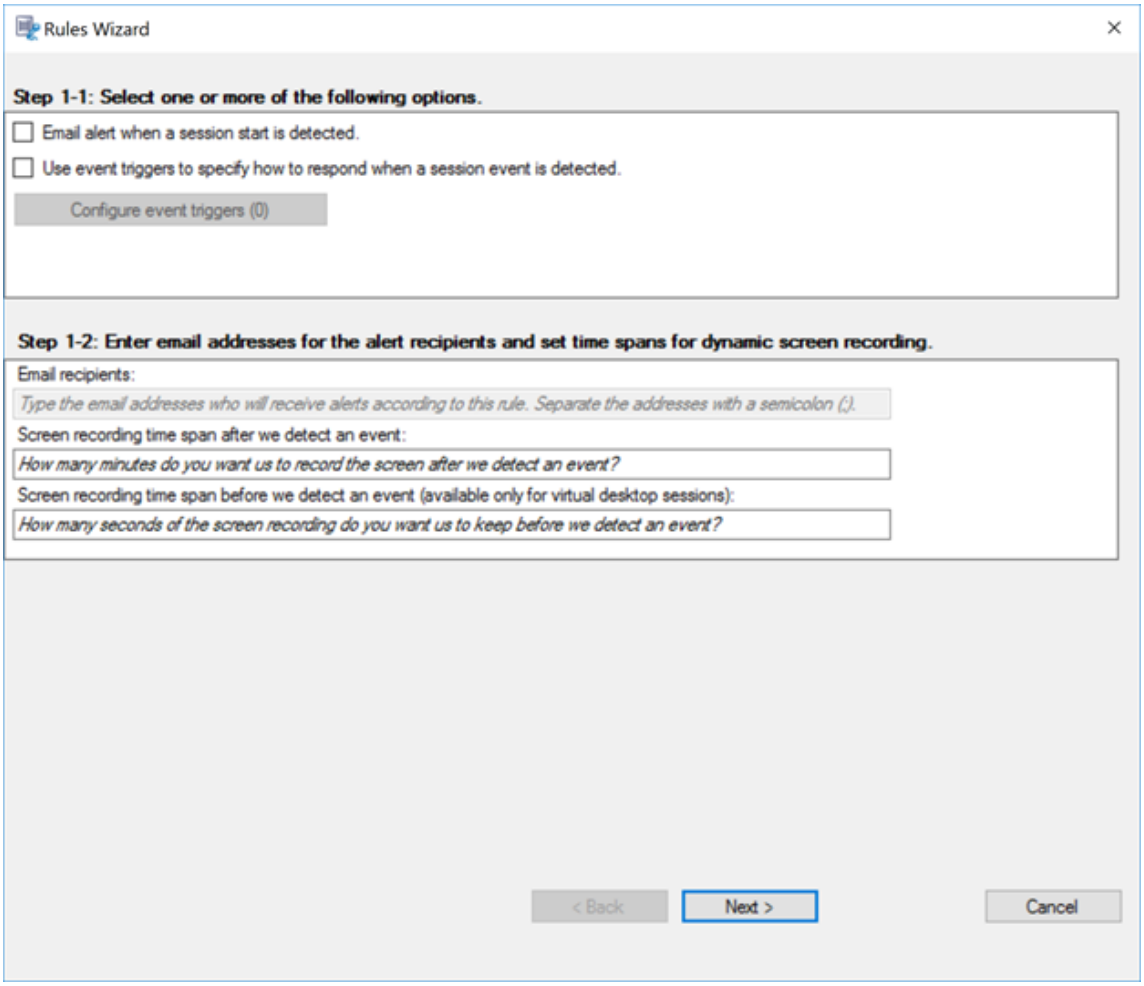
- メールアラートの送信
- 迅速な録画の開始
- セッションのロック
- セッションのログオフ
- セッションの切断



> 注：
>
> システム言語がドイツ語、フランス語、またはスペイン語の場合、マシンの水平方向の解像度が 1700 ピクセル以上であることを確認してください。そうしないと、テキストが切り捨てられ、イベントトリガーテーブルの列が完全に表示されません。
>
> アクティブなイベント検出ポリシーがログに記録するイベントの種類を選択する必要があります。操作が終了したら、［確認］をクリックします。

ドロップダウンリストからイベントの種類を選択し、論理積演算子を使用して結合される 2 つのディメンションを介してイベント規則を設定します。ポリシー規則ごとに最大 7 つのイベントトリガーを設定できます。また、［説明］列にイベントトリガーを定義したり、この列を空のままにしたりすることもできます。定義したイベントトリガーの説明は、［メールの送信］を選択しその種類のイベントがログに記録された場合に、アラートメールで提供されます。［画面の録画を開始する］を選択している場合、イベントのみの録画中に特定のイベントが発生すると、動的画面録画が自動的に開始されます。動的画面録画の期間を設定します：

- セッションイベントが検出された後の画面録画の期間：イベントが検出された後、画面を録画する分数を構成できます。値を指定しないままにすると、録画されたセッションが終了するまで画面の録画が続行されます。
- セッションイベントが検出される前の画面録画の期間：イベントが検出される前に保持する画面録画秒数を構成できます。この機能は、仮想デスクトップセッションでのみ使用できます。値の範囲は 1～120 です。値を 1 から 10 のいずれかに設定すると、値 10 が有効になります。値を指定しないままにすると、機能は有効になりません。Session Recording が保持する画面録画の実際の長さは、構成より少し長くなる場合があります。



サポートされているイベントの種類の全一覧については、次の表を参照してください。

イベントの種類	ディメンション	オプション
アプリ開始		
		アプリ名
		フルコマンドライン
アプリ終了		
		アプリ名
最上位		
		アプリ名
		ウィンドウのタイトル
Web 閲覧		
		URL

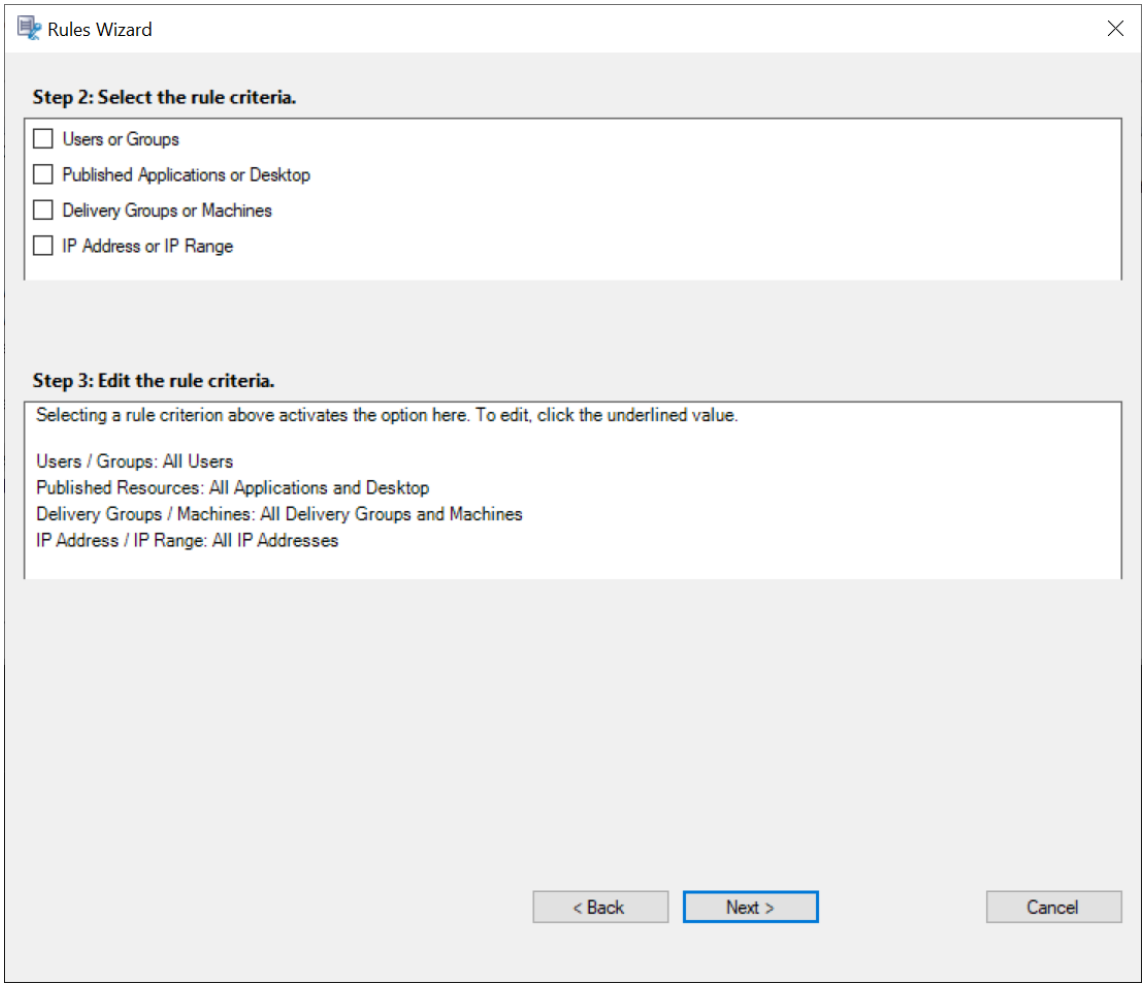
イベントの種類	ディメンション	オプション
		タブのタイトル
		ブラウザー名
ファイルの作成		
		Path
		ファイル サイズ (MB)
ファイル名の変更		
		Path
		名前
ファイルの移動		
		ソースパス
		ターゲット パス
		ファイル サイズ (MB)
ファイルの削除		
		Path
		ファイル サイズ (MB)
CDM USB		
		ドライブ文字
汎用 USB		
		デバイス名
アイドル状態		
		アイドル時間 (時間)
ファイル転送		
		ファイルソース
		ファイル サイズ (MB)
		ファイル名
レジストリ - 作成		
		キー名
レジストリ - 削除		
		キー名

イベントの種類	ディメンション	オプション
レジストリ - 値の設定		
		キー名
		値の名前
レジストリ - 値の削除		
		キー名
		値の名前
レジストリ - 名前の変更		
		キー名
ユーザーアカウントの変更		
		ユーザー名
予期しないアプリ終了		
		アプリ名
アプリ非応答		
		アプリ名
新しいアプリのインストール		
		アプリ名
アプリのアンインストール		
		アプリ名
RDP 接続		
		IP アドレス
ポップアップウィンドウ		
		プロセス名
		ウィンドウコンテンツ
パフォーマンスデータ		
		CPU 使用率（%）
		メモリ使用率（%）
		ネット送信速度（MB）
		ネット受信速度（MB）
		RTT（ミリ秒）

イベントの種類	ディメンション	オプション
クリップボード操作		
		データの種類
		プロセス名
		コンテンツ

9. ［次へ］をクリックして、規則条件を選択および編集します。

   カスタム録画ポリシーの作成と同様、次の 1 つまたは複数の規則条件を選択できます：ユーザーまたはグループ、公開アプリケーションまたはデスクトップ、デリバリーグループまたはマシン、**IP** アドレスまたは **IP** の範囲。詳しくは、「カスタム録画ポリシーの作成」セクションで手順を参照してください。



> 注:
>
> セッションまたはイベントが単一のイベント応答ポリシーで複数の規則を満たしている場合、最も古い

> 規則が有効になります。

10. ウィザードの指示に従って構成を完了します。
11. 新しいイベント応答ポリシーをアクティブにします。

高可用性と負荷分散

December 22, 2022

このセクションでは、次の設定について説明します:

- Session Recording サーバーの負荷分散
- データベース高可用性の構成

Session Recording サーバーの負荷分散

December 23, 2022

Session Recording は、Session Recording サーバー間の負荷分散をサポートします。この記事では、Citrix ADC を例として使用した負荷分散構成を説明しています。詳しくは、「既存の環境での負荷分散の構成」および「Azure での Session Recording の展開と負荷分散」を参照してください。

すべての Session Recording サーバー間で、負荷分散構成を同期できます。

> 注:
>
> この負荷分散機能を使用するには、Session Recording サーバーおよび Session Recording Agent のバージョン 7.16 以降が必要です。

負荷分散をサポートする場合の **Session Recording** の変更内容:

- すべての Session Recording サーバーが、録画ファイルを保存する 1 つのフォルダーを共有します。
- すべての Session Recording サーバーが、1 つの Session Recording データベースを共有します。
- (推奨) Session Recording ポリシーコンソールを 1 つだけインストールし、すべての Session Recording サーバーがこのコンソールを共有するようにしてください。

負荷分散の構成

この機能を使用するには、Citrix ADC とさまざまな Session Recording コンポーネントで以下の手順を行います:

負荷分散の構成（**Citrix ADC** 側）

負荷分散サーバーの構成　Citrix ADC 内の負荷分散サーバーに Session Recording サーバーを追加します。

負荷分散サービスの構成

1. それぞれの Session Recording サーバーで必要な各プロトコルに負荷分散サービスを追加します。
2. （推奨）各サービスモニターにバインドする、関連するプロトコルモニターを選択します。

負荷分散仮想サーバーの構成

1. 必要なプロトコルに基づいて、同じ Citrix ADC 仮想 IP アドレスを持つ仮想サーバーを作成し、それらの仮想サーバーを関連する負荷分散サービスにバインドします。
2. 各仮想サーバーでパーシステンスを構成します。
3. （推奨）負荷分散の方法には、デフォルトの方法（LEASTCONNECTION）ではなく、LEASTBANDWITH または LEASTPACKETS を選択します。
4. HTTPS 仮想サーバーを稼働させるための証明書を作成します。

負荷分散の構成（**Session Recording** 側）

Session Recording サーバーがインストールされた各サーバーで、以下を実行します

1. （推奨）Session Recording サーバーのインストール時に、同じ Session Recording データベース名を入力します。
2. 管理者ログ機能を選択した場合、各 Session Recording サーバーのインストール時に指定した管理者ログデータベース名と同じ名前を入力することをお勧めします。
3. ファイルストレージフォルダーの読み取り/書き込み権限を、すべての Session Recording サーバーマシンアカウントと共有します。その後、［**Session Recording** サーバーのプロパティ］で、ファイルストレージフォルダーを共有フォルダーとして使用するように変更します。詳しくは、「録画の復元先の指定」を参照してください。
4. `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`で Session Recording サーバーのレジストリキーに値を追加します。
   値の名前：**EnableLB**
   値のデータ：**1**（DWORD、つまり「有効」）
5. Session Recording ストレージマネージャーのメッセージキューに HTTP または HTTPS プロトコルを選択した場合、Citrix ADC 仮想 IP アドレスのホストレコードを作成し、`C:\Windows\System32\msmq\Mapping\sample_map`にリダイレクトを追加します。その後、Message Queuing サービスを再起動します。

   リダイレクトは以下のようにします：


```
<redirections xmlns="msmq-queue-redirections.xml">
        <redirection>
                    <from>http://<ADCHost>\*/msmq/private$/
                       CitrixSmAudData</from>
                    <to>http://<LocalFqdn>/msmq/private$/
                       CitrixSmAudData</to>
        </redirection>
        <redirection>
                    <from>https://<ADCHost>\*/msmq/private$/
                       CitrixSmAudData</from>
                    <to>https://<LocalFqdn>/msmq/private$/
                       CitrixSmAudData</to>
        </redirection>
</redirections>
<!--NeedCopy-->
```

<ADCHost> は作成された Citrix ADC 仮想 IP アドレスの FQDN で、**<LocalFqdn>** はローカルホストの FQDN です。

6. （推奨）1 つの Session Recording サーバーレジストリを構成後、スクリプト「**<Session Recording** サーバーのインストールパス **>\Scripts\SrServerConfigurationSync.ps1**」を使用して、このサーバーレジストリから構成をエクスポートして、他の Session Recording サーバーレジストリにインポートできます。スクリプト「**SrServerConfigurationSync.ps1**」を使用して、メッセージキューのリダイレクトマッピングを追加することもできます。

   a) 1 つの Session Recording サーバーで、**EnableLB** レジストリ値を構成後、管理者としてコマンドプロンプトを起動し、**powershell.exe -file SrServerConfigurationSync.ps1 -Action Export,AddRedirection -ADCHost <ADCHost>** コマンドを実行します。ここで、**<ADCHost>** は、作成した Citrix ADC 仮想 IP アドレスの FQDN です。

   b) スクリプトの実行後、**SrServerConfig.reg** というファイル名のエクスポート済みレジストリが生成され、**sr_lb_map.xml** が **C:\Windows\System32\msmq\Mapping** パスに追加されます。

   c) その他の Session Recording サーバーで、上の手順で生成された **SrServerConfig.reg** をコピーし、管理者としてコマンドプロンプトを起動し、**powershell.exe -file SrServerConfigurationSync.ps1 -Action Import,AddRedirection -ADCHost <ADCHost>** コマンドを実行します。ここで、**<ADCHost>** は、作成した Citrix ADC 仮想 IP アドレスの FQDN です。

   d) スクリプトの実行後、**EnableLB** 値が他の Session Recording サーバーレジストリキーに追加され、**sr_lb_map.xml** が **C:\Windows\System32\msmq\Mapping** パスに追加されます。

Session Recording Agent がインストールされたマシンの **Session Recording Agent** プロパティで以下を行います

- Session Recording ストレージマネージャーメッセージのキューに HTTP または HTTPS を選択した場合、［**Session Recording** サーバー］テキストボックスには Citrix ADC 仮想 IP アドレスの FQDN を入力します。

- Session Recording ストレージマネージャーメッセージのキューにデフォルトの TCP プロトコルを選択した場合、［**Session Recording** サーバー］テキストボックスには Citrix ADC 仮想 IP アドレスを入力します。

Session Recording Player がインストールされたマシンで以下を行います　Citrix ADC 仮想 IP アドレスまたはその FQDN を、接続された Session Recording サーバーとして追加します。

Session Recording データベースがインストールされた **SQL Server** で以下を行います　共有 Session Recording データベースにすべての Session Recording サーバーマシンアカウントを追加し、それらに **db_owner** 権限を割り当てます。

データベース高可用性の構成

December 22, 2022

Session Recording は、Microsoft SQL Server をベースとしたデータベースの高可用性に関する次のソリューションをサポートしています。プリンシパル SQL Server またはプライマリ SQL Server のハードウェアまたはソフトウェアに障害が発生した場合、データベースが自動的にフェールオーバーする可能性があります。

- Always On 可用性グループ

  Always On 可用性グループ機能は、高可用性および障害回復ソリューションで、データベースのミラーリングに取って代わるエンタープライズレベルのサービスです。これにより、企業の一連のユーザーデータベースの可用性が最大化されます。この機能では、Windows Server Failover Clustering（WSFC）ノード上に SQL Server インスタンスが存在する必要があります。詳しくは、「Always On 可用性グループ：高可用性および障害回復ソリューション」を参照してください。

- SQL Server クラスタリング

  Microsoft の SQL クラスタリングテクノロジーを使用して、任意のサーバーに障害が起きた場合に別のサーバーが自動的にタスクや実行内容を引き継ぐようにできます。ただし、このソリューションのセットアップは複雑で、SQL Server データベースミラーリングなどほかのソリューションよりも自動フェールオーバーには一般的に時間がかかります。詳しくは、「Always On フェールオーバークラスターインスタンス（SQL Server）」を参照してください。

- SQL Server データベースミラーリング

  データベースのミラーリングによって、アクティブなデータベースサーバーが停止しても数秒で自動的にフェールオーバーが実行されます。各データベースサーバー上に完全な SQL Server ライセンスが必要になるため、ほかの 2 つのソリューションよりも費用が高くつきます。SQL Server Express エディションを使用してデータベースをミラーリングすることはできません。詳しくは、「データベースミラーリング（SQL Server）」を参照してください。

Session Recording でデータベースの高可用性を構成する方法

Session Recording でデータベースの高可用性を構成するには、次のいずれかを実行します。

- 最初に Session Recording サーバーコンポーネントをインストールし、次に作成したデータベースのデータベース高可用性を構成します。
  準備した SQL Server インスタンスにデータベースがインストールされるように構成して、Session Recording Administration コンポーネントをインストールできます。次に、作成したデータベースのデータベース高可用性を構成できます。
  - Always On 可用性グループおよびクラスタリングの場合は、`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\SmAudDatabaseInstance`で、SQL Server インスタンス名を可用性グループのリスナーの名前、または SQL Server ネットワークの名前に変更します。
  - データベースのミラーリングの場合は、`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\DatabaseFailoverPartner`と`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\LoggingDatabaseFailoverPartner`で、データベースのフェールオーバーパートナーを追加します。
- 最初に空のデータベースのデータベース高可用性を構成し、次に Session Recording Administration コンポーネントをインストールします。
  想定したプライマリ SQL Server インスタンスに、Session Recording データベースおよび管理者ログデータベースとして空のデータベースを 2 つ作成し、高可用性を構成できます。次に、Session Recording サーバーコンポーネントをインストールするときに、SQL Server のインスタンス名を入力します。
  - Always On 可用性グループソリューションを使用するには、可用性グループのリスナーの名前を入力します。
  - データベースのミラーリングソリューションを使用するには、プリンシパル SQL Server の名前を入力します。
  - クラスタリングソリューションを使用するには、SQL Server のネットワーク名を入力します。

録画の表示

December 22, 2022

Session Recording Player または Session Recording Web Player を使用して、録画したセッションを表示、検索、およびブックマークすることができます。

ライブセッションの再生機能を有効にしてセッションを録画する場合は、進行中のセッションを 1〜2 秒遅れで表示できます。

時間やファイルサイズの上限を超えるセッションは、複数のセッションファイルに分けて表示されます。

> 注:
>
> 録画された VDA のセッションへのアクセス権をユーザーに付与してください。

Session Recording Player

December 23, 2022

Session Recording Player は、セッションの録画ファイルを調査するユーザーが、録画を再生するためにワークステーションでアクセスするユーザーインターフェイスです。このセクションでは、以下を実行する手順を説明します:

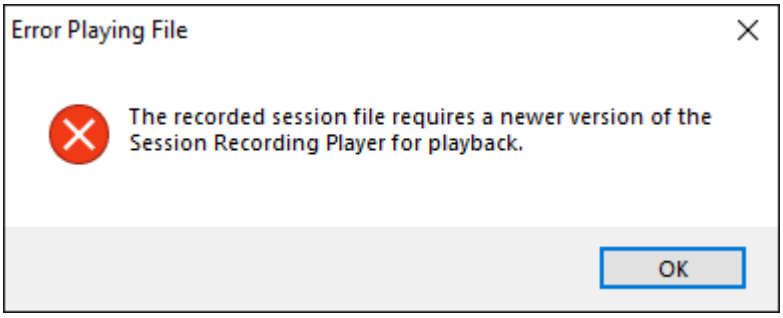
- Session Recording Player の起動
- ライブセッションの再生の有効化または無効化
- 再生データの保護の有効化または無効化
- 録画の検索
- 録画を開いて再生
- 録画のキャッシュ
- アイドル期間のハイライト
- イベントとブックマークの使用

Session Recording Player の起動

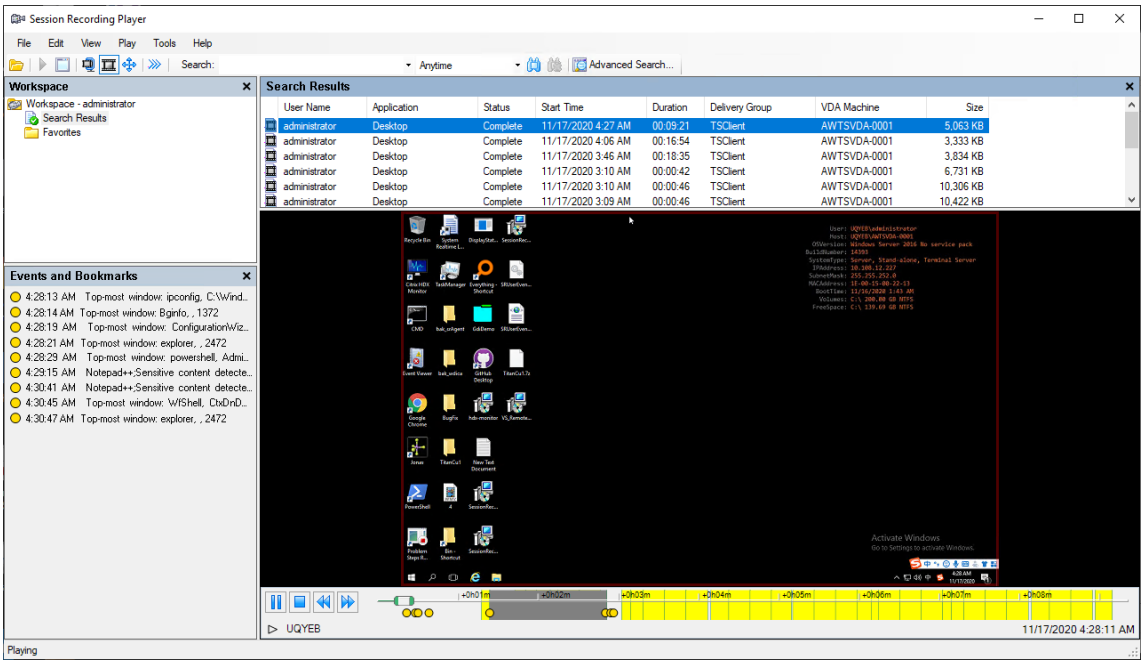
February 20, 2024

Session Recording Player の起動

> 注:
>
> - 録画にブロックされたコンテンツが含まれている場合、Session Recording はそれをスキップします。ただし、ブロックされた期間に移動した場合は、再生に黒い画面と、そのコンテンツがブロックされていることを示すメッセージが表示されます。この機能を使用するには、Session Recording 2012 以降を使用します。
> - Session Recording Player 2009 以前を使用して録画を再生している場合、次のエラーメッセージが表示されます。Web Player は影響を受けません。

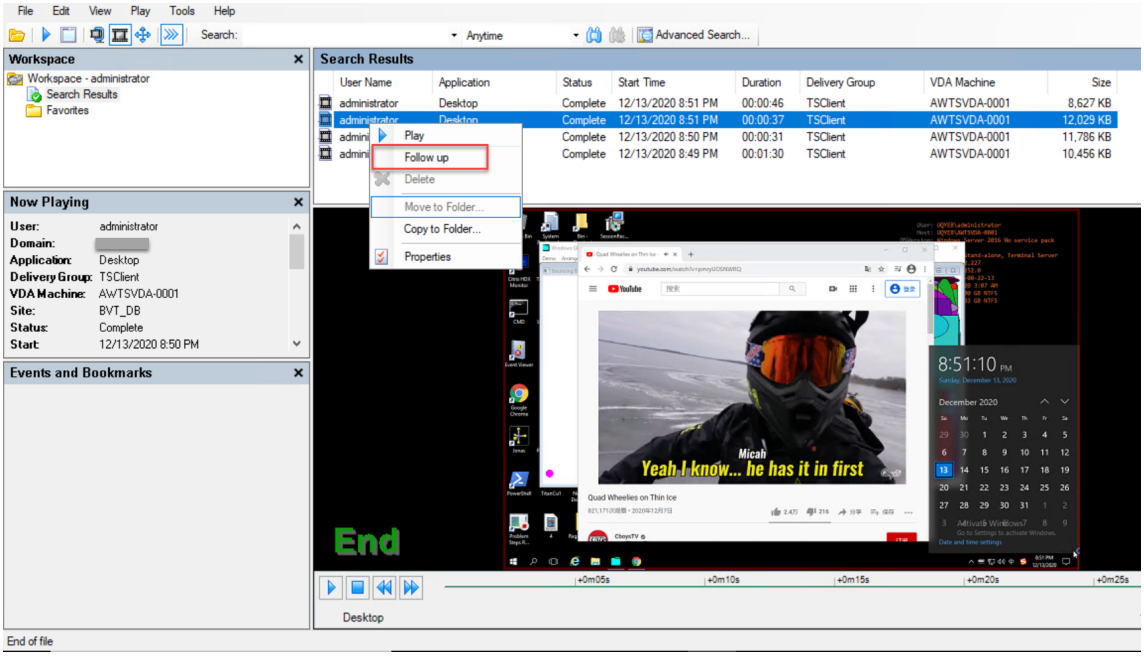


1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。Session Recording Player が表示されます。



ヒント：**EventOnly** 列は、画面録画またはイベントのみの録画を示します。

録画済みセッションのすべての録画ファイルを表示するには、リストで録画を右クリックし、［フォローアップ］を選択します。



ウィンドウ要素の表示または非表示

Session Recording Player には、表示するかどうかを切り替えるためのウィンドウ要素があります。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［表示］を選択します。
4. 表示する要素を選択します。選択するとすぐにその要素が表示されます。チェックマークはその要素が選択されていることを示します。

Session Recording サーバーへの接続

複数の Session Recording サーバーに接続するように Session Recording Player を設定してから、接続する Session Recording サーバーを選択できます。Session Recording Player から同時に複数の Session Recording サーバーに接続することはできません。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［ツール］**>**［オプション］**>**［接続］の順に選択します。
4. 接続する Session Recording サーバーを選択します。

ライブセッションの再生の有効化または無効化

December 22, 2022

ライブ再生機能を有効にしてセッションを録画すると、録画中または録画後にセッションを表示できます。セッションを録画しながら表示することは、ライブでセッションを見るようなものです。ただし、VDA からデータが送信されると実際には 1〜2 秒の遅延が発生します。

ライブ再生セッションを表示する場合、一部の機能は使用できません:

- 録画が完了するまでデジタル証明書を割り当てたり、証明書を表示することはできません。
- 録画が完了するまで、再生データの保護は適用できません。再生データの保護が有効な場合、ライブセッションを再生できます。ただし、セッションが完了するまでは暗号化されません。
- 録画が完了するまで、ファイルをキャッシュできません。

デフォルトで、ライブセッションの再生は有効になっています。

1. Session Recording サーバーをホストするコンピューターにログオンします。
2. [スタート] ボタンをクリックし、[**Session Recording** サーバーのプロパティ] を選択します。
3. [**Session Recording** サーバーのプロパティ] で、[再生] タブをクリックします。
4. [ライブセッションの再生を許可する] チェックボックスをオンまたはオフにします。

再生データの保護の有効化または無効化

December 22, 2022

セキュリティ上の安全のため、Session Recording では、Player で表示するためにダウンロードされた録画ファイルは自動的に暗号化されます。暗号化されたファイルは、ほかのワークステーションまたはユーザーアカウントではコピーまたは再生できません。暗号化されたファイルは`.icle`拡張子で識別されます。暗号化されていないファイルは`.icl`拡張子で識別されます。Player の`%localAppData%\Citrix\SessionRecording\Player\Cache`にある間、ファイルは、権限を持つユーザーがファイルを開くまで暗号化されたままです。

HTTPS を使用して転送データを保護することをお勧めします。

再生データの保護は、デフォルトで有効になります。

1. Session Recording サーバーをホストするマシンにログオンします。
2. [スタート] ボタンをクリックし、[**Session Recording** サーバーのプロパティ] を選択します。
3. [**Session Recording** サーバーのプロパティ] で、[再生] タブをクリックします。
4. [再生のためダウンロードされるセッションの録画ファイルを暗号化する] チェックボックスをオンまたはオフにします。

録画の検索

December 22, 2022

Session Recording Player では、クイック検索を実行することも、高度な検索を実行して検索に適用するオプションを指定することもできます。検索結果は Session Recording Player の検索結果の領域に表示されます。

> 注:
>
> Player のインストールでは、通常、Session Recording Player と Session Recording サーバーとの間の接続を設定できます。この接続の設定に失敗した場合は、初めてファイルを検索するときに、接続を設定するよう要求されます。
>
> 使用可能な録画されたセッションを 1 回の検索で表示できるセッション数の上限まですべて表示するには、検索パラメーターを指定せずに検索を実行します。

クイック検索の実行

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. 検索条件を定義します:
   - ［検索］ボックスに検索条件を入力します。
   - ［検索］ラベルの上にマウスポインターを移動すると、入力できるパラメーターの一覧が表示されます。
   - ［検索］ボックス右側の矢印をクリックすると、過去に使用した検索文字列が最新の 64 件まで表示されます。
   - ［検索］ボックス右側のドロップダウンリストを使用して、セッションが録画された日時を指定できます。
4. ドロップダウンリスト右側の双眼鏡のアイコンをクリックして、検索を開始します。

高度な検索の実行

高度な検索では、結果に 150,000 個を超えるエンティティが含まれている場合、返されるまでに最大 20 秒かかる場合があります。Citrix では日付範囲やユーザーなどのより厳密な検索条件を使用して、結果の数を減らすことをお勧めします。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. ［**Session Recording Player**］ウィンドウで、ツールバーの ［高度な検索］をクリックするか、メニューバーで ［ツール］>［高度な検索］の順に選択します。
4. ［高度な検索］ダイアログボックスのタブで検索条件を定義します:

- ［共通］タブでは、ドメインまたはアカウントの認証先、サイト、グループ、マルチセッション OS 対応 VDA、アプリケーション、またはファイル ID を使用して検索できます。
- ［日付/時刻］タブでは、日付、曜日、および時刻を使用して検索できます。
- ［イベント］タブでは、セッションに挿入された Citrix 定義イベントとカスタムイベントを検索できます。
- ［そのほか］タブでは、セッション名、クライアント名、クライアントアドレス、および録画時間を使用して検索できます。このタブでは、表示される検索結果数の上限およびアーカイブ済みのファイルを検索に含めるかどうかも指定できます。

  検索条件を指定するにつれて、作成しているクエリがダイアログボックス下部のペインに表示されます。

5. ［検索］をクリックして検索を開始します。

   高度な検索のクエリは、保存しておいて後で取得することができます。［高度な検索］ダイアログボックスの［保存］をクリックして、現在のクエリを保存します。保存したクエリを取得するには、［高度な検索］ダイアログボックスの ［開く］をクリックします。保存したクエリファイルの拡張子は `.isq` です。

検索オプションの設定

Session Recording Player の検索オプションにより、表示される検索結果数の上限およびアーカイブ済みのファイルを検索に含めるかどうかも指定できます。

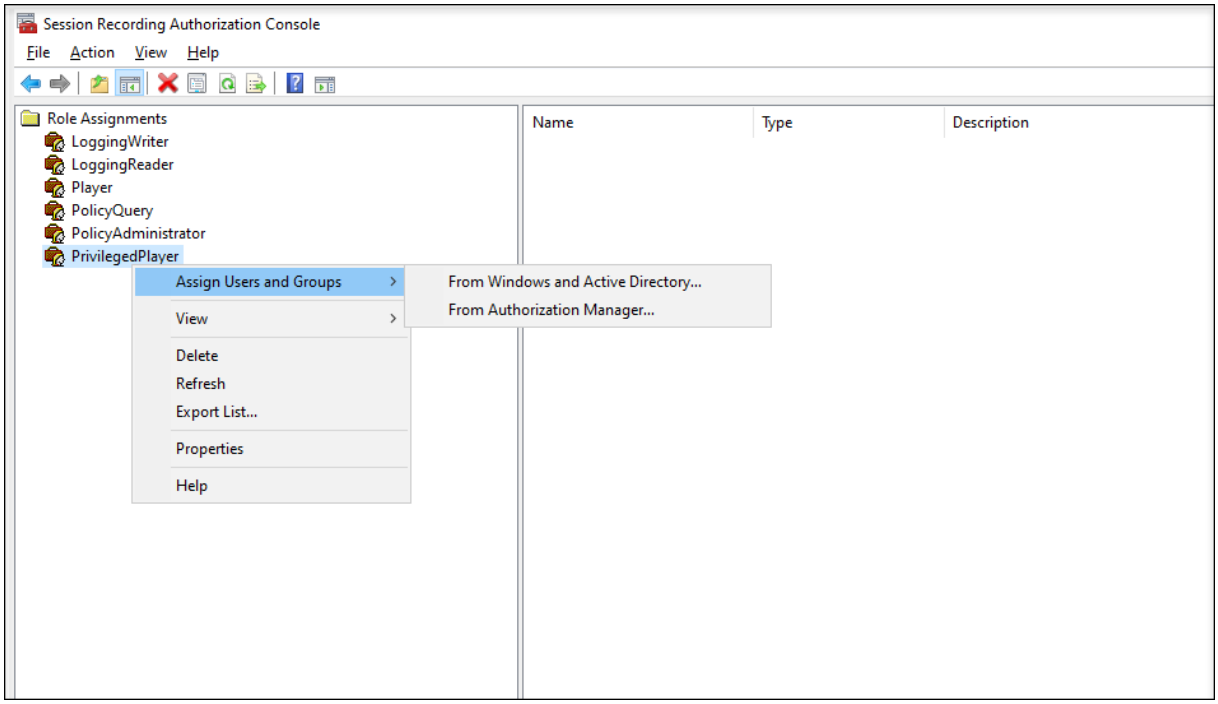
1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** メニューバーで、［ツール］**>** ［オプション］**>** ［検索］の順に選択します。
4. ［検索結果の表示件数の上限］ボックスに、表示する検索結果数を入力します。最大で 500 件の検索結果を表示できます。
5. アーカイブ済みのファイルを検索に含めるかどうかを設定するには、［アーカイブ済みファイルを含める］チェックボックスをオンまたはオフにします。

録画へのアクセス制限の設定

February 20, 2024

録画の閲覧ポリシーによる役割ベースのアクセス制御に加えて、対象の録画にアクセス制限を設定します。制限付き録画には、Citrix Session Recording 承認コンソールで **PrivilegedPlayer** の役割が割り当てられたユーザーおよびユーザーグループのみがアクセスできます。

> 注:
>
> ライブ録画へのアクセス制限はサポートされていません。

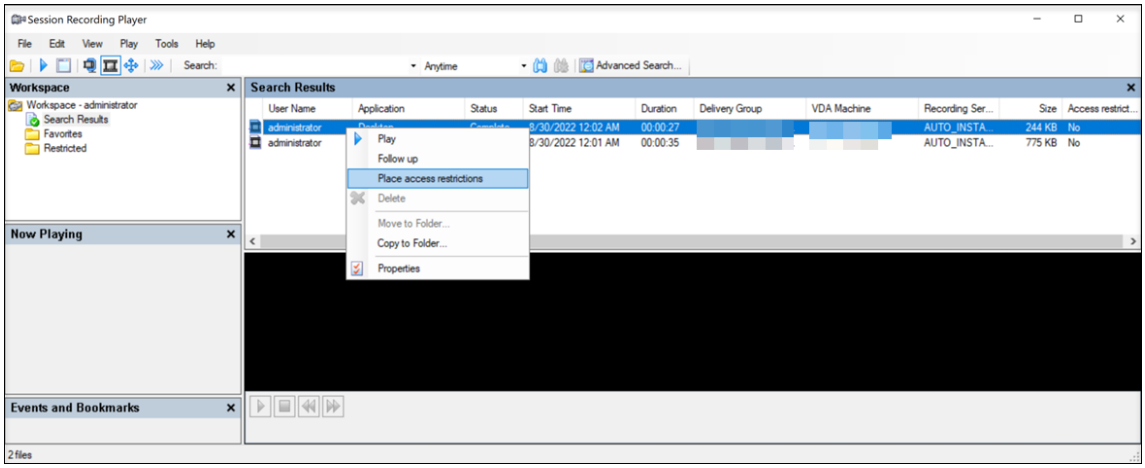


次のセクションでは、対象の録画に対するアクセス制限を設定および削除するプロセスについて説明します。

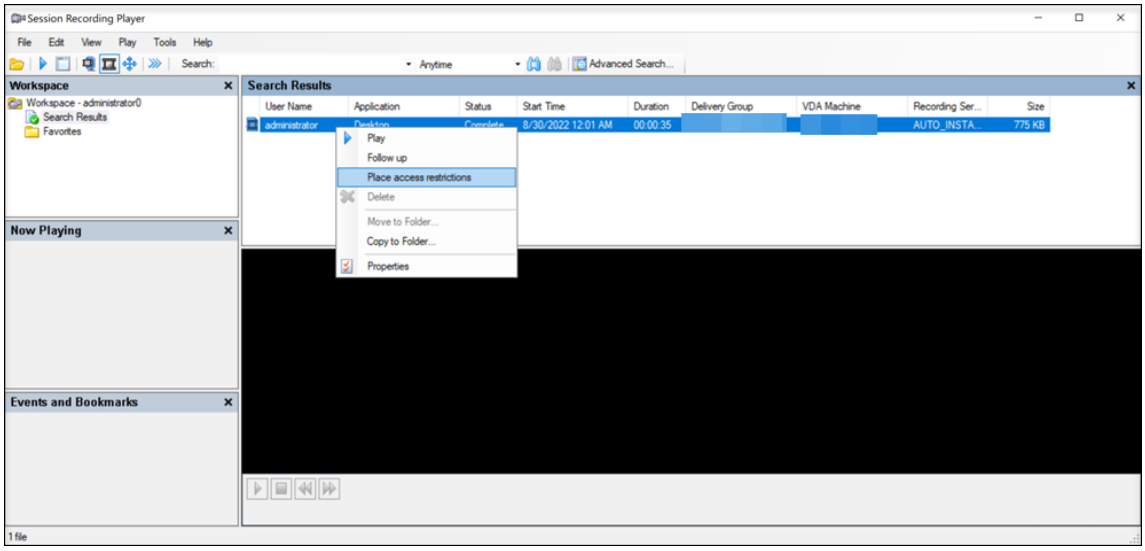
1. Session Recording Player がインストールされているマシンにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. ［ワークスペース］ペインで ［検索結果］を選択します。
4. ［検索結果］領域で、対象の録画を 1 つまたは複数個選択します。
5. 右クリックして ［アクセス制限を設定する］を選択します。

   Player または **PrivilegedPlayer** のいずれかの役割が割り当てられたユーザーおよびユーザーグループは、録画にアクセス制限を設定できます。［制限］メニューは、**PrivilegedPlayer** の役割が割り当てられたユーザーおよびユーザーグループのみが使用できます。

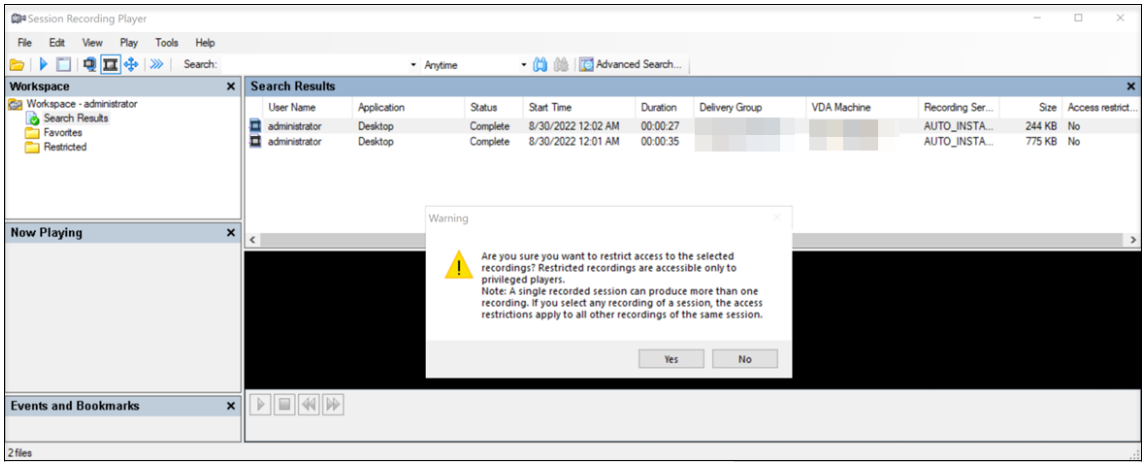
   PrivilegedPlayer の役割のビュー:



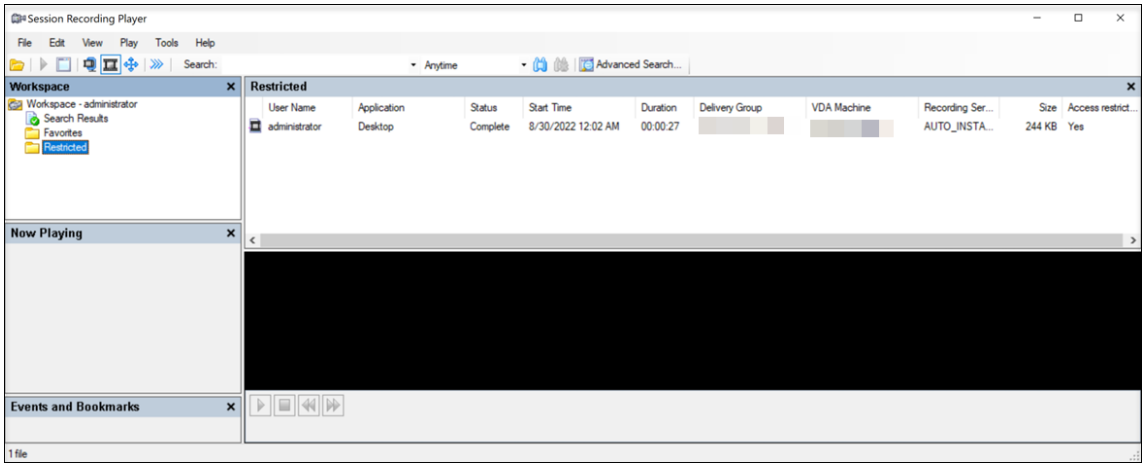
Player の役割のビュー：



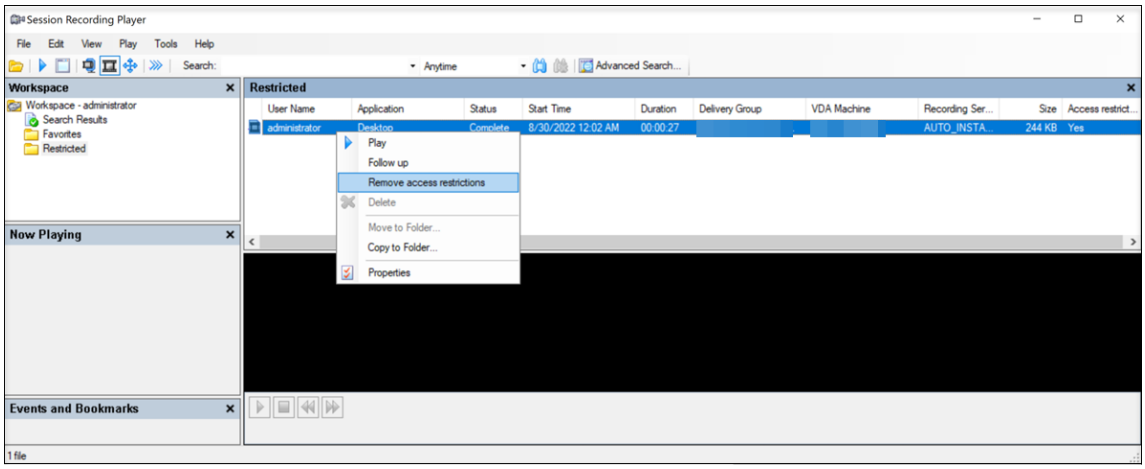
6. ［はい］をクリックします。



7. アクセス制限を設定した選択した録画が、［検索結果］領域から ［制限］領域に移動したことを確認します。



8. ［制限］領域で、必要に応じてアクセス制限を解除します。アクセス制限が解除されると、録画は ［検索結果］領域に戻ります。



録画を開いて再生

February 20, 2024

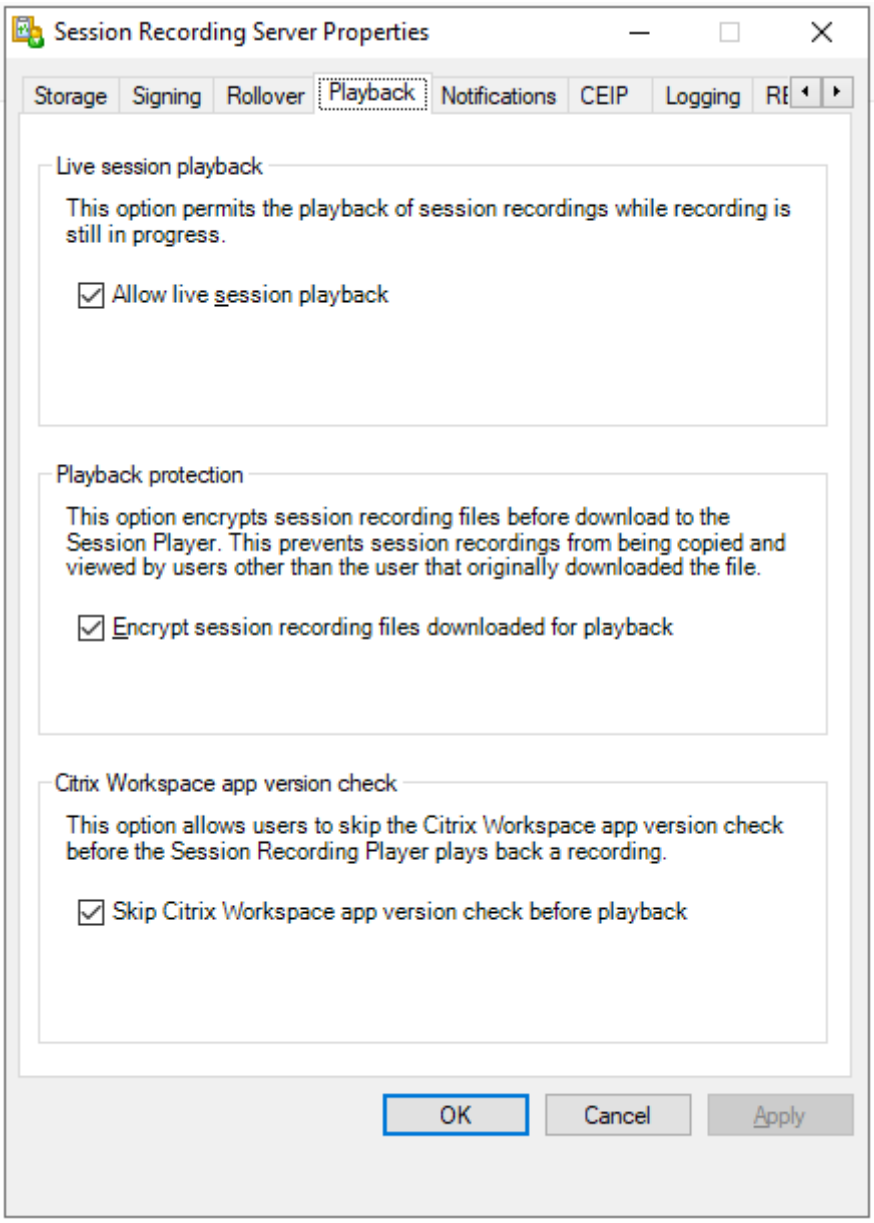
録画の開き方

Session Recording Player でセッションの録画を開くには、次の 3 つの方法があります:

- Session Recording Player を使用して検索を実行する。検索条件に一致するセッションの録画が、検索結果の領域に表示されます。
- ローカルディスクドライブまたは共有ドライブ上のセッションの録画ファイルに直接アクセスする。
- お気に入りフォルダーからセッションの録画ファイルにアクセスする。

デジタル署名なしで録画されたファイルを開くと、警告メッセージが表示されます。そのファイルの出所と整合性を確認できなかったと表示されます。ファイルの整合性について確信がある場合は、警告のポップアップウィンドウで［はい］をクリックしてファイルを開きます。

Session Recording Player が録画されたセッションを再生する前に、Citrix Workspace アプリのバージョンがチェックされます。Player がそのバージョンの Citrix Workspace アプリをサポートしていない場合、エラーが返されます。エラーを排除するには、［**Session Recording** サーバーのプロパティ］で［**Citrix Workspace** アプリバージョンチェックをスキップする］を選択します。



> 注:
>
> Session Recording の管理者ログ機能により、Session Recording Player の録画ダウンロードをログ記録

> できます。詳しくは、「管理者ログ」を参照してください。

検索結果の領域にある録画を開いて再生する

1. Session Recording Player がインストールされているマシンにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. 検索を実行します。
4. 検索結果ビューが表示されていない場合は、［ワークスペース］ペインで ［検索結果］を選択します。
5. 検索結果ビューで、再生するセッションを選択します。
6. 次のいずれかの操作を行います：
   - セッションをダブルクリックします。
   - 右クリックして ［再生］を選択します。
   - **Session Recording Player** のメニューバーで、［再生］**>** ［再生］の順に選択します。

ファイルにアクセスして録画を開く

録画ファイルの名前は、冒頭に`i_`が付く一意の英数字のファイル ID で、ファイル拡張子は`.icl`か`.icle`になります。`.icl`拡張子は、再生データの保護機能が適用されていない録画を示します。`.icle`拡張子は、再生データの保護機能が適用された録画を示します。セッションの録画ファイルは、セッションが録画された日付が組み込まれたフォルダに保存されます。たとえば、2014 年 12 月 22 日に録画されたセッションのファイルは、`2014\12\22`というフォルダーパスに保存されます。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. 次のいずれかの操作を行います：
   - **Session Recording Player** のメニューバーで、［ファイル］**>** ［開く］の順に選択し、ファイルを参照します。
   - Windows のエクスプローラーを使用してファイルを表示し、ファイルを **Player** ウィンドウにドラッグします。
   - Windows のエクスプローラーを使用してファイルを表示し、ダブルクリックします。
   - ［ワークスペース］ペインで「お気に入り」を作成した場合は、［お気に入り］を選択し、検索結果エリアからファイルを開くのと同じ方法で、［お気に入り］からファイルを開きます。

お気に入りの使用

お気に入りフォルダーを作成して、頻繁に表示する録画にすばやくアクセスすることができます。お気に入りフォルダーは、ワークステーションまたはネットワークドライブに格納されているセッションの録画ファイルを参照します。これらのファイルをほかのワークステーションにインポートおよびエクスポートし、ほかの Session Recording Player のユーザーと共有できます。

> 注:
>
> Session Recording Player へのアクセス権を持つユーザーのみが、お気に入りフォルダーに関連付けられているセッションの録画ファイルをダウンロードできます。アクセス権については、Session Recording Player 管理者に問い合わせてください。

お気に入りサブフォルダーを作成するには:

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** ウィンドウの［ワークスペース］ペインで ［お気に入り］フォルダーを選択します。
4. メニューバーで ［ファイル］**>**［フォルダー］**>**［新規フォルダー］の順に選択します。新しいフォルダが ［お気に入り］フォルダ配下に表示されます。
5. フォルダ名を入力し、**Enter** キーを押すか、新しい名前を反映する場所をクリックします。

［ファイル］**>**［フォルダー］の順に選択すると表示されるほかのオプションを使用して、フォルダーの削除、名前変更、移動、コピー、インポート、およびエクスポートを行います。

録画の再生

Session Recording Player で録画されたセッションを開いた後は、次の方法で録画されたセッション内を移動できます:

- Player ウィンドウのボタンを使用して、再生、停止、一時停止、および再生速度の変更を行います。
- シークスライダーを使用して、前後に移動します。

挿入されたマーカーとカスタムイベントに移動して、録画されたセッション内を移動することもできます。

> 注:
>
> - セッションの録画の再生時に、マウスポインターが 2 つ表示される場合があります。この問題は、ユーザーが Internet Explorer を使用中に、Internet Explorer により自動的に縮小表示されたイメージをユーザーがクリックすると発生します。セッション中は 1 つのマウスポインターしか表示されませんが、セッションの録画の再生時にのみ 2 つ目のマウスポインターが表示されます。
> - このバージョンの Session Recording は、SpeedScreen マルチメディアアクセラレーション機能や［Flash 品質の調整］ポリシー設定をサポートしません。この機能が有効の場合、再生画面が黒く表示されます。
> - 4096 x 4096 以上の解像度でセッションを録画すると、録画が断片化する場合があります。

Player ウィンドウのボタンの使用

Player ウィンドウのボタンを使用するか、**Session Recording Player** メニューバーの ［再生］の下のメニューアイテムを選択して、セッションの録画を操作します。

Player ウィンドウの制御	機能
	選択したセッションファイルを再生します。
	再生を一時停止します。
	再生を停止します。[停止] をクリックし、[再生] をクリックすると、ファイルの冒頭から録画が再開されます。
	現在の再生速度の半分に速度を変更します。最低で標準の 4 分の 1 にまで速度を下げます。
	現在の再生速度の 2 倍に速度を変更します。最高で標準の 32 倍にまで速度を上げます。

シークスライダーの使い方

Player ウィンドウの下部にあるシークスライダーを使用して、セッションの録画内の別の位置にジャンプします。シークスライダーを録画内の表示したいポイントまでドラッグすることも、スライダーバーの任意のポイントをクリックして移動することもできます。

また、次のキーボードキーを使用してシークスライダーを制御できます:

キーボードキー	機能
Home	冒頭へシークします。
End	末尾へシークします。
→	5 秒先へシークします。
←	5 秒前へシークします。
マウスホイールを 1 目盛り手前に動かす	15 秒先へシークします。
マウスホイールを 1 目盛り奥に動かす	15 秒前へシークします。
Ctrl+→	30 秒先へシークします。
Ctrl+←	30 秒前へシークします。
PgDn	1 分先へシークします。
PgUp	1 分前へシークします。
Ctrl キーを押しながらマウスホイールを 1 目盛り手前に動かす	90 秒先へシークします。
Ctrl キーを押しながらマウスホイールを 1 目盛り奥に動かす	90 秒前へシークします。

キーボードキー	機能
Ctrl+PageDown	6 分先へシークします。
Ctrl+PageUp	6 分前へシークします。

シークスライダーの速度を調整するには、**Session Recording Player** のメニューバーで、［ツール］**>**［オプション］**>**［**Player**］の順に選択し、スライダーをドラッグしてシークの応答速度を変更します。応答速度を上げると、より多くのメモリが消費されます。録画のサイズやマシンのハードウェアによって、応答速度が低下する場合があります。

再生速度の変更

標準の 4 分の 1 倍速から 32 倍速までの、指数的に増加する再生速度を設定できます。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［再生］**>**［再生速度］の順に選択します。
4. 速度を選択します。

すぐに速度が調節されます。この速度を示す緑色のテキストは、Player ウィンドウの下部に短時間表示されます。

録画されたセッションのアイドル期間のハイライト表示

録画されたセッションのアイドル期間とは、何も操作が行われていない部分です。Session Recording Player では、録画したセッションのアイドル期間を再生時にハイライトできます。このオプションは、デフォルトで ［オン］になっています。詳しくは、「アイドル期間のハイライト」を参照してください。

操作のない空白期間の省略

高速レビューモードを使用すると、録画されたセッション内で操作のない部分の再生を省略することができます。この設定により、再生時間を短縮できます。ただし、アニメーションを用いたマウスポインター、点滅するカーソル、秒針付きの時計など、動画による連続処理の再生は省略できません。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［再生］**>**［高速レビューモード］の順に選択します。

オプションがオンまたはオフに切り替わります。このオプションを選択するたびに、その状態が Player ウィンドウに短時間表示されます。

再生の表示形式の変更

以下を行うことで、Player ウィンドウの録画されたセッションの表示形式を変更できます:

- 表示領域や表示サイズを変更する
- 全画面で再生を表示する
- 独立ウィンドウで Player ウィンドウを表示する
- 録画されたセッションの周りに赤い境界線を表示して、Player ウィンドウの背景と区別する

全画面で **Player** ウィンドウを表示する

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［表示］**>**［全画面］の順に選択します。
4. 元のサイズに戻すには、**Esc** キーまたは **F11** キーを押します。

独立ウィンドウで **Player** ウィンドウを表示する

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［表示］**>**［独立ウィンドウ］の順に選択します。Player ウィンドウを含む新しいウィンドウが開きます。ドラッグしてウィンドウのサイズを変更することができます。
4. Player ウィンドウをメインウィンドウに埋め込むには、メニューバーで ［表示］**>**［独立ウィンドウ］の順に選択するか、**F10** キーを押します。

再生するセッションの画面サイズを **Player** ウィンドウのサイズに合わせる

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［再生］**>**［表示モード］**>**［ウィンドウに合わせる］の順に選択します。

    - ［ウィンドウに合わせる（高速描画）］を選択すると、十分な画質を維持しながら画像を縮小します。高画質オプションを使用する場合より描画が高速で行われますが、画像とテキストの明晰さは低下します。高画質モードでパフォーマンスに問題が生じる場合は、このオプションを使用します。
    - ［ウィンドウに合わせる（高画質）］を選択すると、明晰な画像とテキストを維持しながら画像を縮小します。このオプションを使用すると、高速描画オプションの場合より描画速度が遅くなることがあります。

再生するセッションの画面サイズを元のセッションのサイズに合わせる

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。

3. **Session Recording Player** のメニューバーで、［再生］**>**［表示モード］**>**［セッションに合わせる］の順に選択します。ポインタが手のひらの形に変わります。画面全体を表す小さなイメージが Player ウィンドウの右上に表示されます。
4. 画面をドラッグします。この小さなイメージで、画面のどこにいるかがわかります。
5. ［セッションに合わせる］を終了するには、表示モードのいずれかのオプションを選択します。

セッションの録画の周りに赤い枠線を表示する

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［ツール］**>**［オプション］**>**［**Player**］の順に選択します。
4. ［セッションの録画の周りに枠線を表示する］チェックボックスをオンにします。
   ［セッションの録画の周りに枠線を表示する］チェックボックスがオフの場合は、マウスポインターが Session Recording Player ウィンドウ内にあるときにマウスの左ボタンを押したままにすると、一時的に赤い枠線が表示されます。

録画のキャッシュ

December 22, 2022

Session Recording Player では、セッションの録画ファイルを開くたびに、録画が格納されている場所からファイルがダウンロードされます。同じファイルを頻繁にダウンロードする場合は、ファイルをワークステーションにキャッシュすることでダウンロード時間を節約できます。ワークステーションにキャッシュされるファイルは次のフォルダーに格納されます:

userprofile**AppData\Local\Citrix\SessionRecording\Player\Cache**

キャッシュに割り当てるディスク容量を指定できます。指定した容量まで録画ファイルが蓄積されると、最も古く使用されていない録画が削除され、新しい録画のための空き領域が作成されます。ディスク領域を解放するために、いつでもキャッシュを空にすることができます。

キャッシュの有効化

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［ツール］**>**［オプション］**>**［キャッシュ］の順に選択します。
4. ［ダウンロードしたファイルをローカルコンピューターにキャッシュする］チェックボックスをオンにします。
5. キャッシュに使用されるディスク容量を制限するには、［使用するディスク容量を制限する］チェックボックスをオンにして、使用する容量を MB 単位で指定します。

6. ［**OK**］をクリックします。

キャッシュを空にする

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［ツール］**>**［オプション］**>**［キャッシュ］の順に選択します。
4. ［ダウンロードしたファイルをローカルコンピューターにキャッシュする］チェックボックスをオンにします。
5. Session Recording Player で、［ツール］**>**［オプション］**>**［キャッシュ］の順に選択します。
6. ［キャッシュの削除］をクリックし、次に ［**OK**］をクリックして操作を確定します。

アイドル期間のハイライト

December 22, 2022

録画されたセッションのアイドル期間とは、何も操作が行われていない部分です。Session Recording Player では、録画したセッションのアイドル期間を再生時にハイライトできます。このオプションは、デフォルトで ［オン］になっています。

注： Session Recording Player でライブセッションを再生すると、アイドル期間がハイライトされない点に注意してください。

録画されたセッションのアイドル期間をハイライトするには、以下を実行します：

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. **Session Recording Player** のメニューバーで、［表示］>［アイドル期間］の順に選択し、チェックボックスをオンまたはオフにします。

イベントとブックマークの使用

December 22, 2022

イベントとブックマークを使用して、録画されたセッション内を簡単に移動できます。

セッションの録画中に、Citrix 定義のイベントがセッションに挿入されます。イベント API やサードパーティ製アプリケーションを使用してカスタムイベントを挿入することもできます。イベントはセッションファイルの一部として保存されます。Session Recording Player を使用して削除または変更することはできません。

ブックマークは、Session Recording Player で、セッション再生中に録画されたセッションに挿入されるマーカーです。ブックマークは、挿入すると、削除するまでは録画されたセッションに関連付けられます。セッションファイルの一部としては保存されませんが、Session Recording Player の **Bookmarks** キャッシュフォルダーに（たとえば C:\Users\SpecificUser\AppData\Local\Citrix\SessionRecording\Player\Bookmarks）`.iclb`ファイルとして、`.icl`形式の録画ファイルと同じファイル名で保存されます。別の Player でブックマークを使用して録画ファイルを再生する場合は、`.iclb`ファイルを Player 上の **Bookmarks** キャッシュフォルダーに移動します。各ブックマークのデフォルトのラベルテキストは「ブックマーク」ですが、最長 128 文字までの任意のコメントテキストに変更できます。

イベントは黄色の丸印、ブックマークは青い四角形として Player ウィンドウの下部に表示されます。これらの印にポインターを合わせると、関連付けられているテキストラベルが表示されます。イベントとブックマークは、Session Recording Player の ［イベントとブックマーク］の一覧にも表示できます。そのテキストラベルと録画されたセッションでの時刻と共に、時系列で一覧に表示されます。

イベントとブックマークを使用して、録画されたセッション内を簡単に移動できます。イベントまたはブックマークに移動することにより、それらが挿入されているポイントまでを省略して、録画されたセッション内を移動できます。

イベントとブックマークの一覧への表示

［イベントとブックマーク］の一覧には、現在再生中の録画されたセッションに挿入されているイベントとブックマークが表示されます。イベントのみ、ブックマークのみ、または両方を表示できます。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. ［イベントとブックマーク］の一覧にマウスポインターを移動し、右クリックしてメニューを表示します。
4. ［イベントのみ表示］、［ブックマークのみ表示］、または ［すべて表示］を選択します。

ブックマークの挿入

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. ブックマークを追加する録画セッションの再生を開始します。
4. ブックマークを挿入する位置までシークスライダーを動かします。
5. Player ウィンドウ内にマウスポインターを移動し、右クリックしてメニューを表示します。
6. 次の方法で、デフォルトのラベル 「ブックマーク」でブックマークを追加するか、コメントを作成します：
    - デフォルトのラベル「ブックマーク」でブックマークを追加するには、［ブックマークを追加］を選択します。
    - テキストラベル付きのブックマークを追加するには、［コメントの追加］を選択します。ブックマークに割り当てるテキストラベルを最長 128 文字で入力します。［**OK**］をクリックします。

コメントの追加または変更

ブックマークを作成した後でコメントを追加したり、コメントを変更したりできます。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. ブックマークを含む録画セッションの再生を開始します。
4. ［イベントとブックマーク］の一覧でブックマークが表示されていることを確認します。
5. ［イベントとブックマーク］の一覧でブックマークを選択し、右クリックしてメニューを表示します。
6. ［コメントの編集］を選択します。
7. ウィンドウが表示されたら、新しいコメントを入力して ［**OK**］をクリックします。

ブックマークの削除

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. ブックマークを含む録画セッションの再生を開始します。
4. ［イベントとブックマーク］の一覧でブックマークが表示されていることを確認します。
5. ［イベントとブックマーク］の一覧でブックマークを選択し、右クリックしてメニューを表示します。
6. ［削除］を選択します。

イベントまたはブックマークへの移動

イベントまたはブックマークに移動すると、それらが挿入されているポイントまで録画されたセッション内を移動できます。

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. ［スタート］メニューの ［**Session Recording Player**］を選択します。
3. イベントまたはブックマークを含む録画セッションの再生を開始します。
4. 次の方法で、イベントまたはブックマークに移動します：

   - Player ウィンドウの下部でイベントまたはブックマークを表す印をクリックし、イベントまたはブックマークに移動します。
   - ［イベントとブックマーク］の一覧で、イベントまたはブックマークをダブルクリックします。次のイベントまたはブックマークに移動するには、一覧からイベントまたはブックマークを選択し、右クリックしてメニューを表示し、［ブックマークへシーク］を選択します。

Session Recording Web Player

December 22, 2022

Web Player では、Web ブラウザーを使用して、録画されたセッションを表示および再生できます。Web Player を使用すると、以下を実行できます:

- フィルターを使用して録画を検索できます。
- 録画をライブで、または録画後に右ペインにタグ付きイベントを表示して再生できます。
- 再生中に録画を保存するためのキャッシュメモリを構成できます。
- アイドル期間をハイライトできます。
- 録画についてコメントを残し、コメントの重要度を設定できます。
- 録画の URL を共有できます。
- 各録画のグラフィカルなイベント統計を表示します。
- 録画された各セッションに関連するデータポイントを表示します。

Web Player にアクセスする

February 20, 2024

Web Player の Web サイトの URL は`http(s)://<FQDN of Session Recording server>/WebPlayer`です。HTTPS を確実に使用するには、IIS 上の Web サイトに SSL バインドを追加し、`SsRecWebSocketServer.config`構成ファイルを更新します。

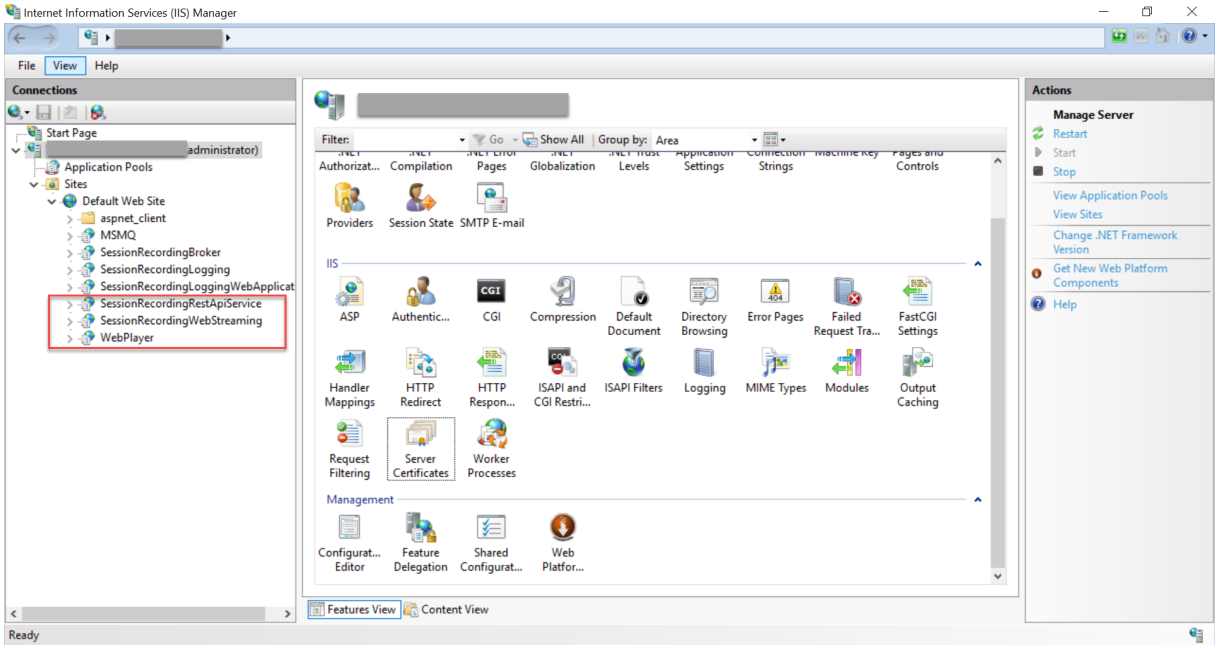
> 注:
>
> - Web Player の Web サイトにログオンする場合、ドメインユーザーは資格情報を入力する必要はありません。ドメインユーザー以外は入力が必要です。
> - サポートされているブラウザーは Google Chrome、Microsoft Edge、Firefox です。
> - Web Player を正しく機能させるには、Firefox で WebGL が有効になっていることを確認してください。

この記事では、Web Player をインストールして有効にするプロセスと、HTTPS を構成するプロセスについて説明します。

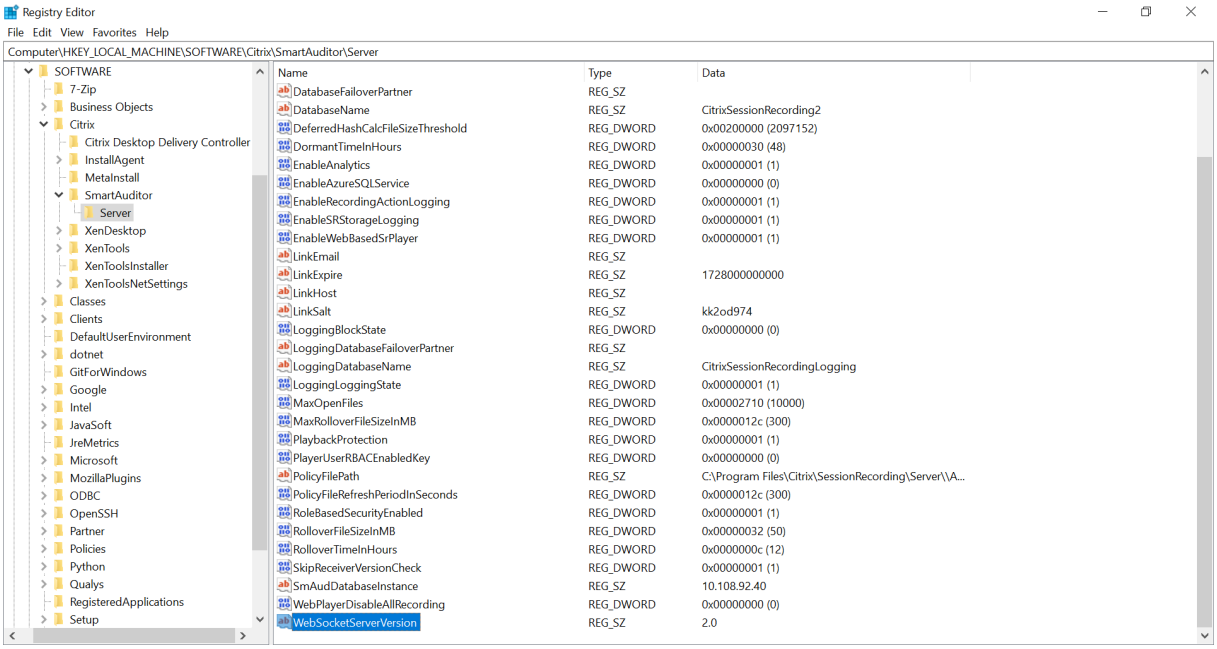
Web Player をインストールする

Session Recording サーバーでのみ Web Player をインストールします。SessionRecordingWebPlayer.msi をダブルクリックして、手順に従ってインストールを完了します。Session Recording のインストールについて詳しくは、「インストール、アップグレード、およびアンインストール」を参照してください。

バージョン 2103 以降、Session Recording は WebSocket サーバーを IIS に移行します。Web Player のインストール後、**SessionRecordingRestApiService**、**SessionRecordingWebStreaming**、**WebPlayer** アプリケーションが IIS に表示されます。



Session Recording 2103 以降を新規インストールすると、Web Player の Web サイトにアクセスしたとき、IIS でホストされている WebSocket サーバーに Web ブラウザーが接続されます。IIS でホストされている WebSocket サーバーはバージョン 2.0 であり、`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`にあるレジストリキーのレジストリ値 **WebSocketServerVersion** で示されています。



以前のバージョンから Session Recording 2103 以降にアップグレードインストールすると、Web ブラウザーが Python ベースの WebSocket サーバーに接続されます。IIS でホストされている WebSocket サーバーに接続するには、**<Session Recording** サーバーのインストールパス **>\Bin\SsRecUtils.exe -enablestreamingservice** コマンドを実行します。Python ベースの WebSocket サーバーに接続し直すには、**<Session Recording** サーバーのインストールパス **>\Bin\SsRecUtils.exe - disablestreamingservice** コマンドを実行します。Python ベースの WebSocket サーバーのバージョンは 1.0 です。

Web Player の有効化

Web Player はデフォルトで有効になっています。

- Web Player を無効にするには、Windows コマンドプロンプトを起動して<Session Recording Server installation path>\Bin\SsRecUtils.exe -disablewebplayerコマンドを実行します。
- Web Player を有効にするには、Windows コマンドプロンプトを起動して<Session Recording Server installation path>\Bin\SsRecUtils.exe -enablewebplayerコマンドを実行します。

HTTPS を構成する

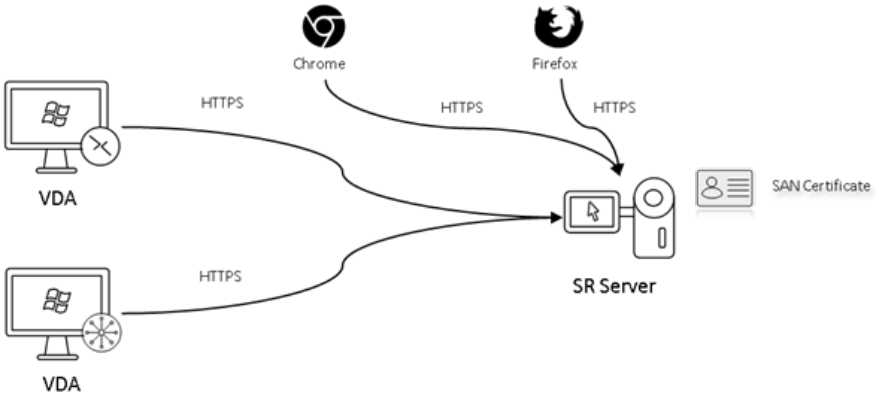
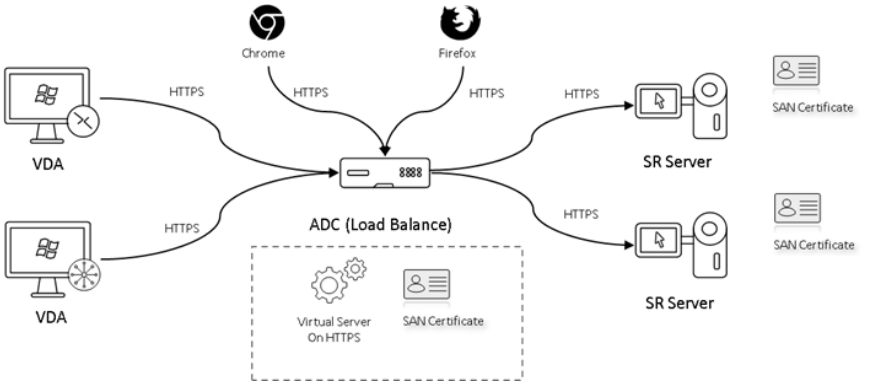
Web Player の Web サイトの URL はhttp(s)://<FQDN of Session Recording server >/WebPlayerです。HTTPS を確実に使用するには、IIS 上の Web サイトに SSL バインドを追加し、SsRecWebSocketServer.config構成ファイルを更新します。

> 注:
>
> Web Player の Web サイトにログオンする場合、ドメインユーザーは資格情報を入力する必要はありません。ドメインユーザー以外は入力が必要です。

HTTPS を使用して Web Player の Web サイトにアクセスするには、以下の手順を完了します:

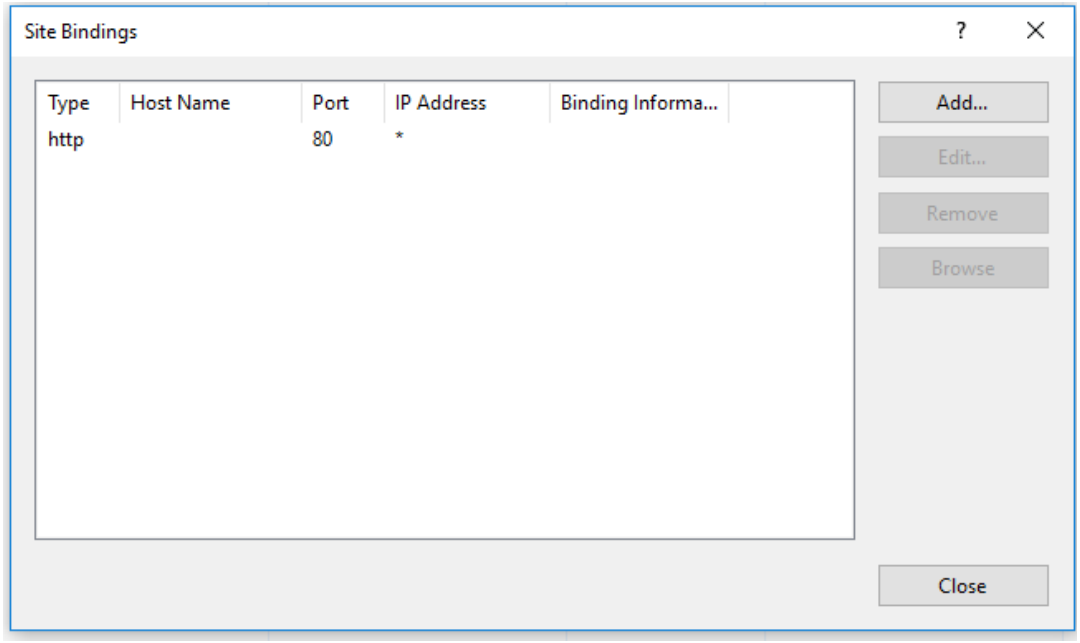
1. IIS に SSL バインドを追加します。

   a) 信頼できる認証機関（CA）から PEM 形式の SSL 証明書を取得します。

   > 注:
   >
   > Google Chrome や Firefox などのほとんどの一般的なブラウザーは、証明書署名要求（CSR）の共通名のサポートを停止しました。すべての信頼された機関からの証明書にはサブジェクトの別名（SAN）が適用されます。HTTPS 経由で Web Player を使用するには、状況に応じて次の操作を実行します:
   >
   > - 単一の Session Recording サーバーが使用されている場合、Session Recording サーバーの証明書を SAN 証明書に更新します。
   >
   > 
   >
   >
   > - 負荷分散を使用している場合は、Citrix ADC と各 Session Recording サーバーの両方で SAN 証明書が使用可能であることを確認してください。
   >
   > 
   >

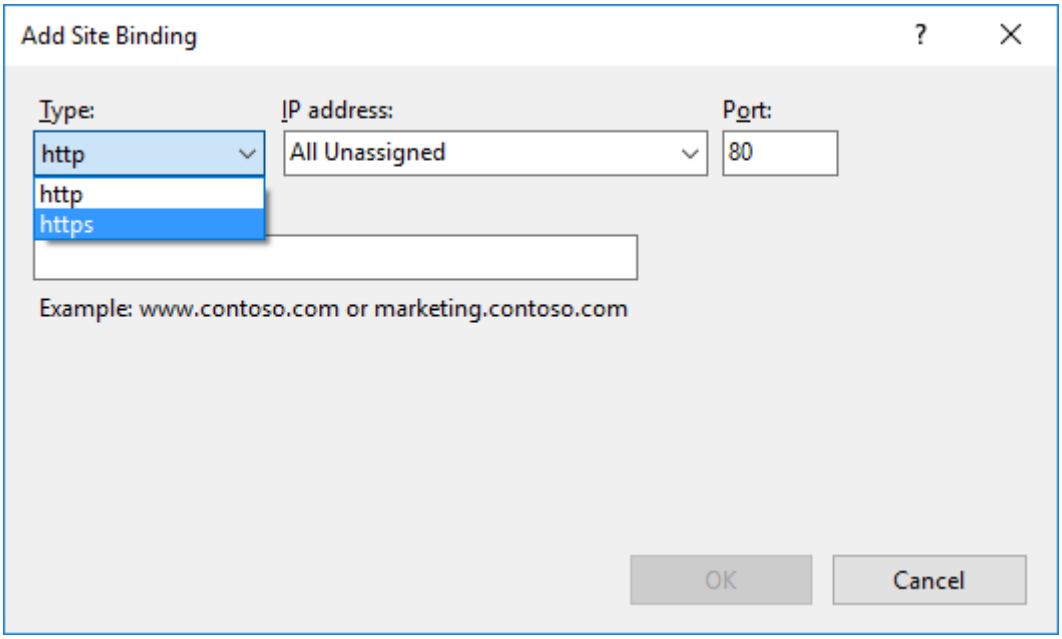
   b) IIS で Web サイトを右クリックして ［バインドの追加］を選択します。［サイトバインド］ダイアログ

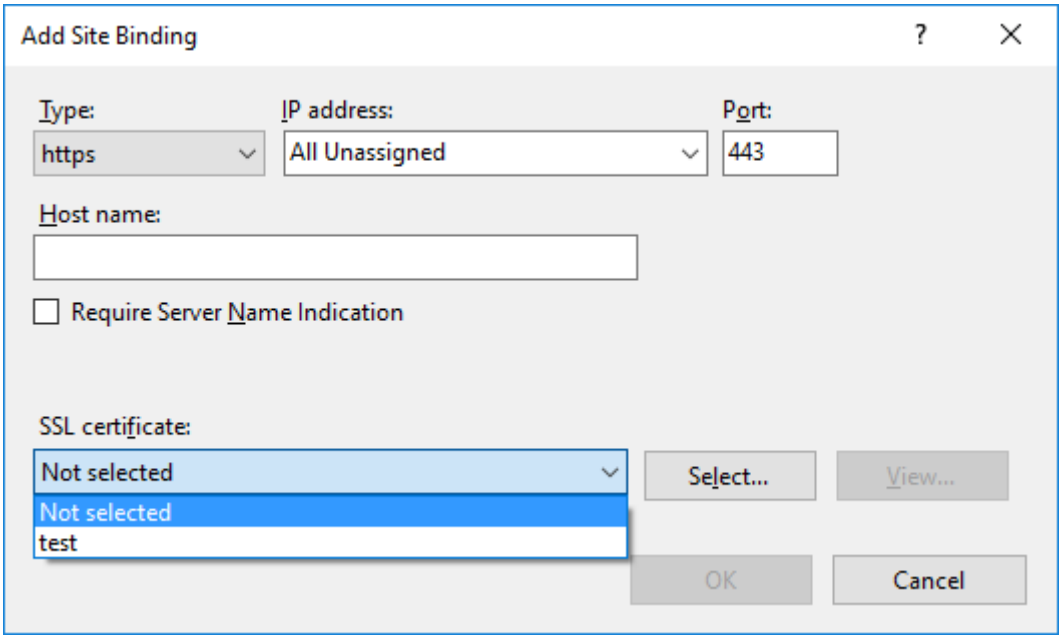
ボックスが表示されます。



c) 右上隅の ［追加］をクリックします。［サイトバインドの追加］ダイアログボックスが表示されます。

d) ［種類］ボックスの一覧から **https** を選択し、SSL 証明書を選択します。





e) [**OK**] をクリックします。

2. `SsRecWebSocketServer.config`構成ファイルを更新します。

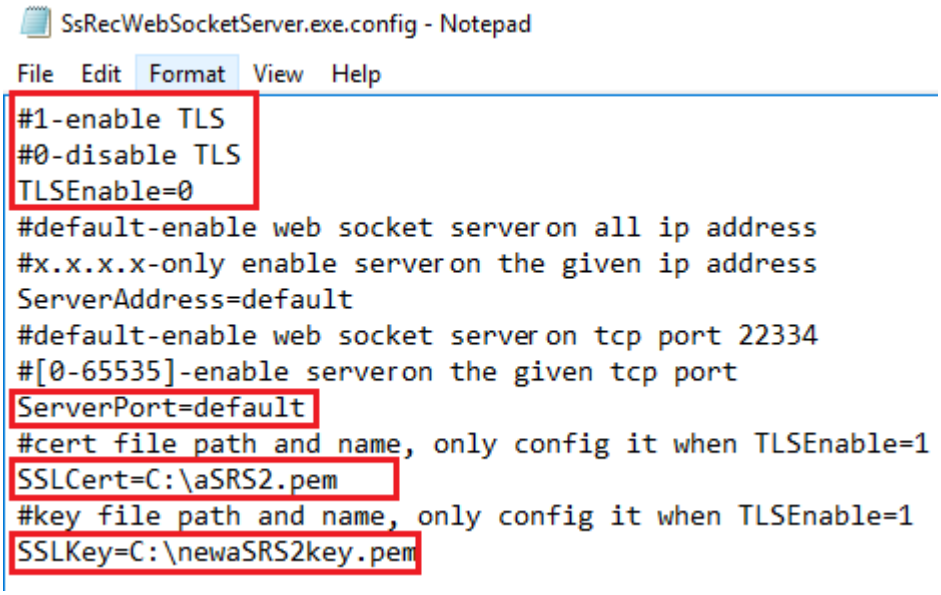
   a) `SsRecWebSocketServer.config`構成ファイルを見つけて開きます。

   `SsRecWebSocketServer.config`構成ファイルは通常`<Session Recording Server installation path>\Bin\`フォルダーにあります。

   b) (オプション) IIS で WebSocket サーバーをホストしている Session Recording 2103 以降の場合、TLSEnable=1 を編集して TLS を有効にし、[**ServerPort**]、[**SSLCert**]、[**SSLKey**] フィールドを無視します。

   c) (オプション) Session Recording 2012 以前の場合、TLSEnable=1 を編集して TLS を有効にし、SSL 証明書と証明書のキーへの各パスを入力します。

   > 注:
   >
   > PEM 形式の SSL 証明書とキーファイルのみがサポートされています。
   > **ServerPort** フィールドは、Web Player が録画ファイルを収集するために使用するポート番号を表示します。次のスクリーンショットでは、デフォルト値 (22334) に設定されています。



WebSocket サーバー構成で使用される個別の証明書とキーファイルを抽出するには:

i. SSL 証明書を含む Session Recording サーバーに OpenSSL がインストールされていることを確認してください。

ii. SSL 証明書を.pfx ファイルとしてエクスポートします。.pfx ファイルには、証明書と秘密キーの両方が含まれています。

iii. コマンドプロンプトを開き、.pfx ファイルを含むフォルダーに移動します。

iv. OpenSSL\bin フォルダーから OpenSSL を開始します。

v. 次のコマンドを実行して、証明書を抽出します:

```
openssl pkcs12 -in [yourfile.pfx] -clcerts -nokeys -out [
    aSRS2.pem]
<!--NeedCopy-->
```

.pfx ファイルをエクスポートするときに作成したインポートパスワードを入力します。

vi. 次のコマンドを実行して、秘密キーを抽出します:

```
openssl pkcs12 -in [yourfile.pfx] -nocerts -out [
    newaSRS2keyWithPassword.pem]
<!--NeedCopy-->
```

.pfx ファイルをエクスポートするときに作成したインポートパスワードを入力します。PEM パスフレーズの入力を求められたら、キーファイルを保護するための新しいパスワードを入力します。

vii. 次のコマンドを実行して、秘密キーの暗号化を解除します:

```
openssl rsa -in [newaSRS2keyWithPassword.pem] -out [
    newaSRS2key.pem]
<!--NeedCopy-->
```


d) 変更を保存します。

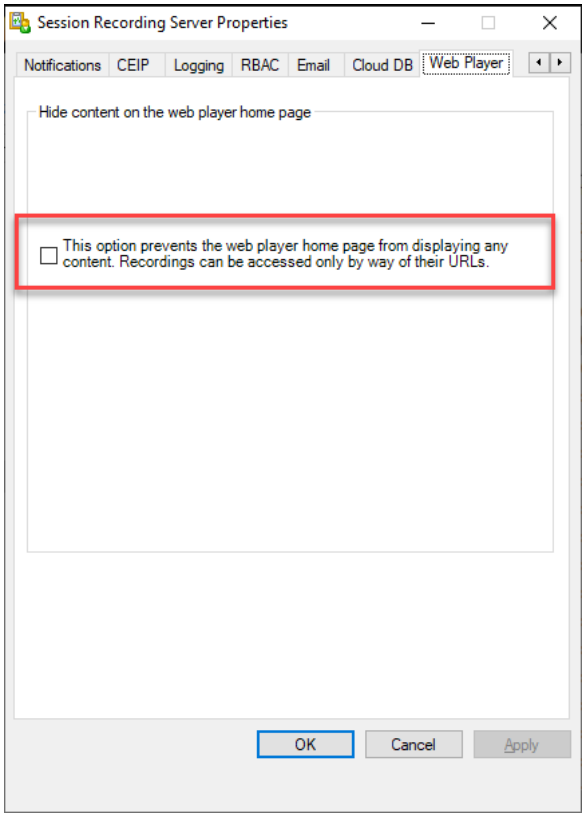
e) ファイアウォールの設定を確認します。SsRecWebSocketServer.exe が TCP ポート（デフォルトでは 22334）を使用できるようにし、Web Player の URL へのアクセスを許可します。

f) `SsRecUtils -stopwebsocketserver`コマンドを実行します。

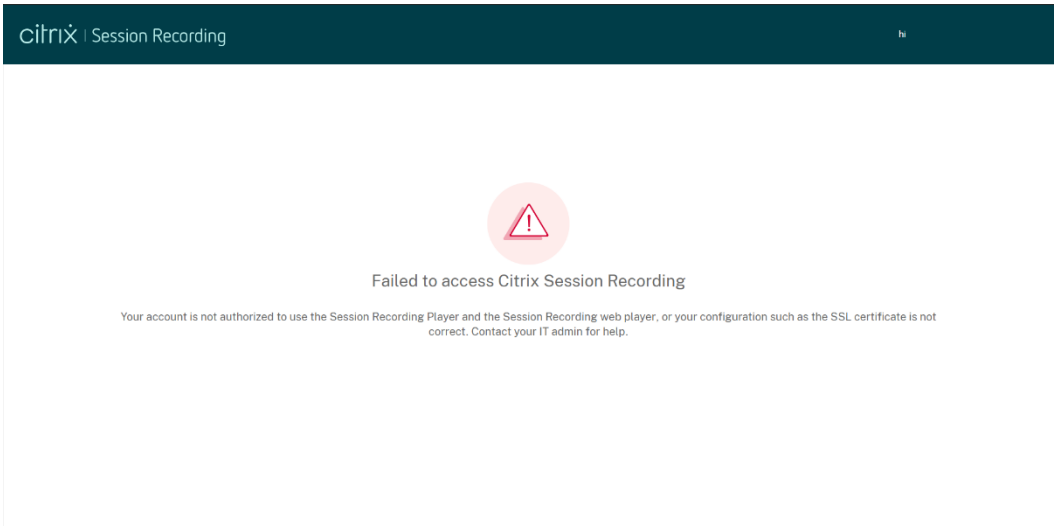
Web Player のホームページのコンテンツを非表示または表示する

February 20, 2024

ログオンした後、［**Session Recording** サーバーのプロパティ］で以下のオプションが選択されているかどうかに基づいて、Web Player のホームページでコンテンツが非表示または表示になる場合があります。

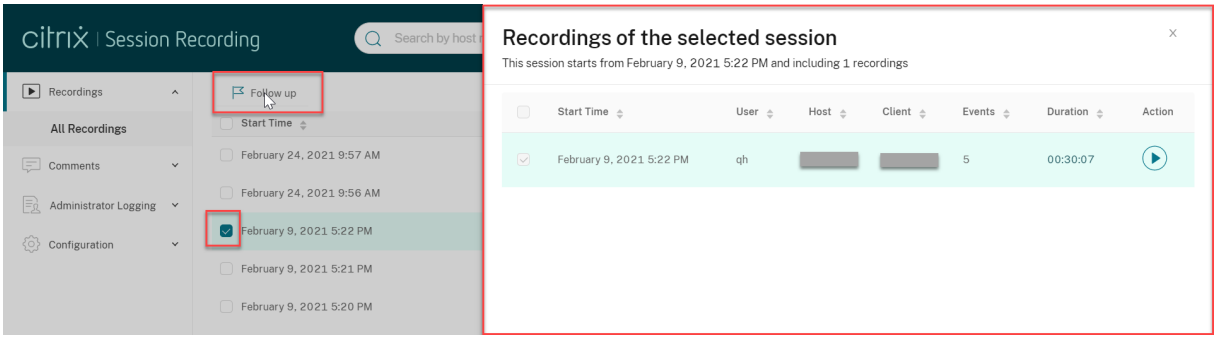


- オプションを選択すると、Web Player のホームページですべてのコンテンツが非表示になります。録画には、URL を介してのみアクセスできます。録画 URL は、指定された受信者に送信されるメールアラートで提供されます。メールアラートについて詳しくは、「イベント応答ポリシーの構成」を参照してください。録画再生ページの ［現在の再生を共有する］コントロールを使用して、録画 URL を共有することもできます。この記事の後半の説明を参照してください。



- オプションを選択しない場合、Web Player のホームページには、次のスクリーンショットのようなコンテンツが表示されます。左のナビゲーションバーで ［すべての録画］をクリックするとページが更新され、新しい録画が存在する場合は表示されます。Web ページを下にスクロールして、表示する録画を選択するか、フィルターを使用して検索結果をカスタマイズします。ライブ録画の場合、［継続時間］列に ［ライブ］と表示され、再生ボタンが緑に変わります。

録画済みセッションのすべての録画ファイルを表示するには、一覧で録画を選択し、［フォローアップ］アイコンを選択します。［フォローアップ］アイコンは、録画が選択されている場合にのみ使用できます。



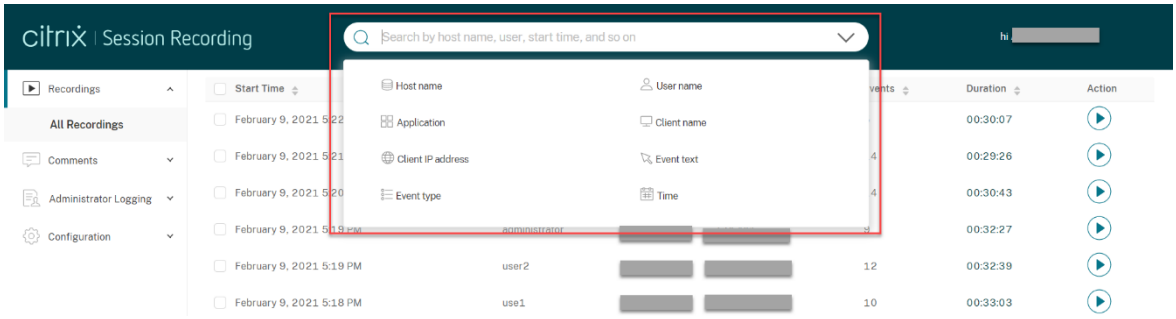
録画項目の説明については、次の表を参照してください。

項目	説明
開始日時	録画の開始時間。上矢印や下矢印をクリックして、録画を時系列順に表示できます。
ユーザー	セッションが録画されたユーザー。上矢印や下矢印をクリックして、ユーザーごとに録画をまとめて表示し、ユーザーをアルファベット順に並べることができます。
ホスト	録画されたセッションがホストされている VDA のホスト名。上矢印や下矢印をクリックして、VDA ホスト名をアルファベット順に並べることができます。
Client	セッションが実行されているクライアントデバイスの名前。上矢印や下矢印をクリックして、クライアントホスト名をアルファベット順に並べることができます。
イベント	録画内のイベントの量。上矢印や下矢印をクリックして、一覧の録画をイベントの量で並べることができます。
イベントのみ	画面録画またはイベントのみの録画を示します。Web Player で再生されるイベントのみの録画には、イベント統計の円グラフとヒストグラムが含まれます。円グラフとヒストグラムは、再生中は静的な状態です。
Recording サーバー	VDA から送信された録画データを処理する Session Recording サーバー。
継続時間	録画の時間の長さ。上矢印や下矢印をクリックして、一覧の録画を時間の長さで並べることができます。

録画の検索

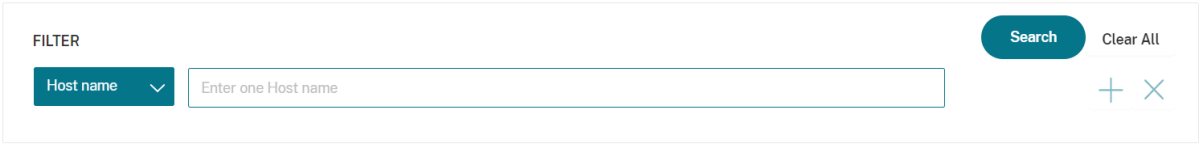
February 20, 2024

Web Player では、フィルターを使用して録画を検索できます。ホスト名、クライアント名、ユーザー名、アプリケーション、クライアント IP アドレス、イベントテキスト、イベントの種類、時刻などのフィルターを使用できます。

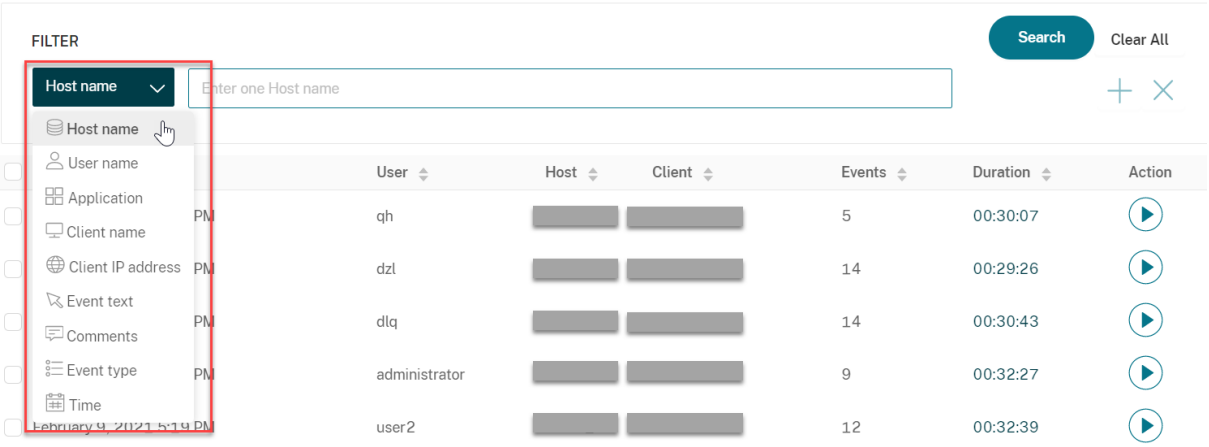


> ヒント：
>
> 録画を選択し、［フォローアップ］アイコンを選択して録画済みセッションのすべての録画を表示できます。

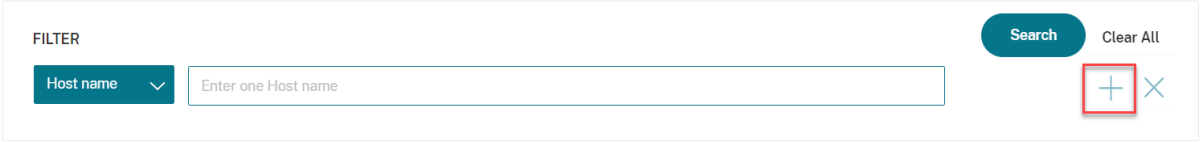
たとえば、ホスト名フィルターを選択すると、次のダイアログボックスが表示されます。録画されたセッションがホストされた VDA のホスト名を入力して ［検索］をクリックし、関連しない録画を検索結果から除外して関連する結果のみを表示します。



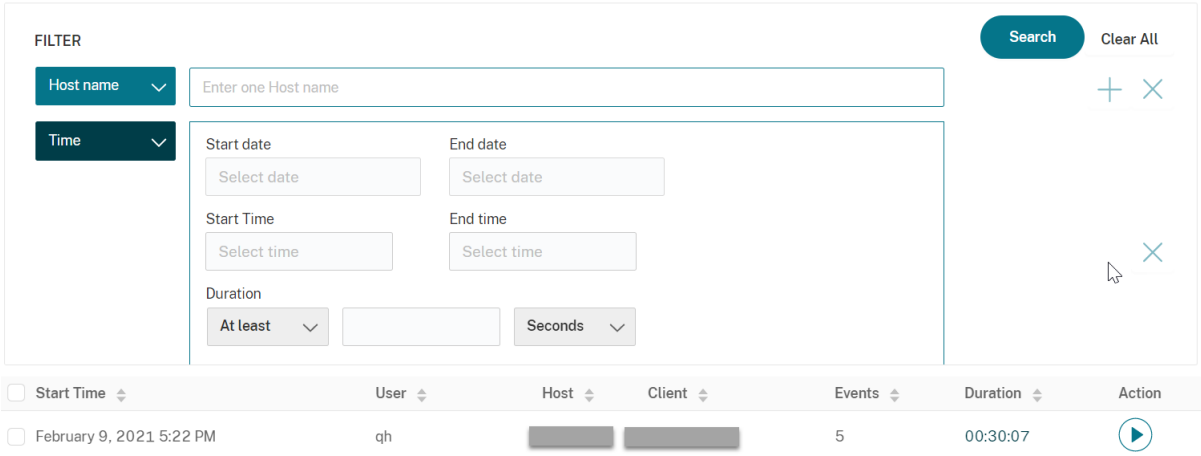
以下のスクリーンショットのように、現在選択されている ［ホスト名］をクリックすると、別のフィルターに変更できます。［ホスト名］のクリック後、すべてのフィルターが一覧表示されます。必要に応じてフィルターを選択します。



[+] をクリックしてフィルターを追加することもできます。



たとえば、［時間］フィルターを以下のスクリーンショットのように追加できます。



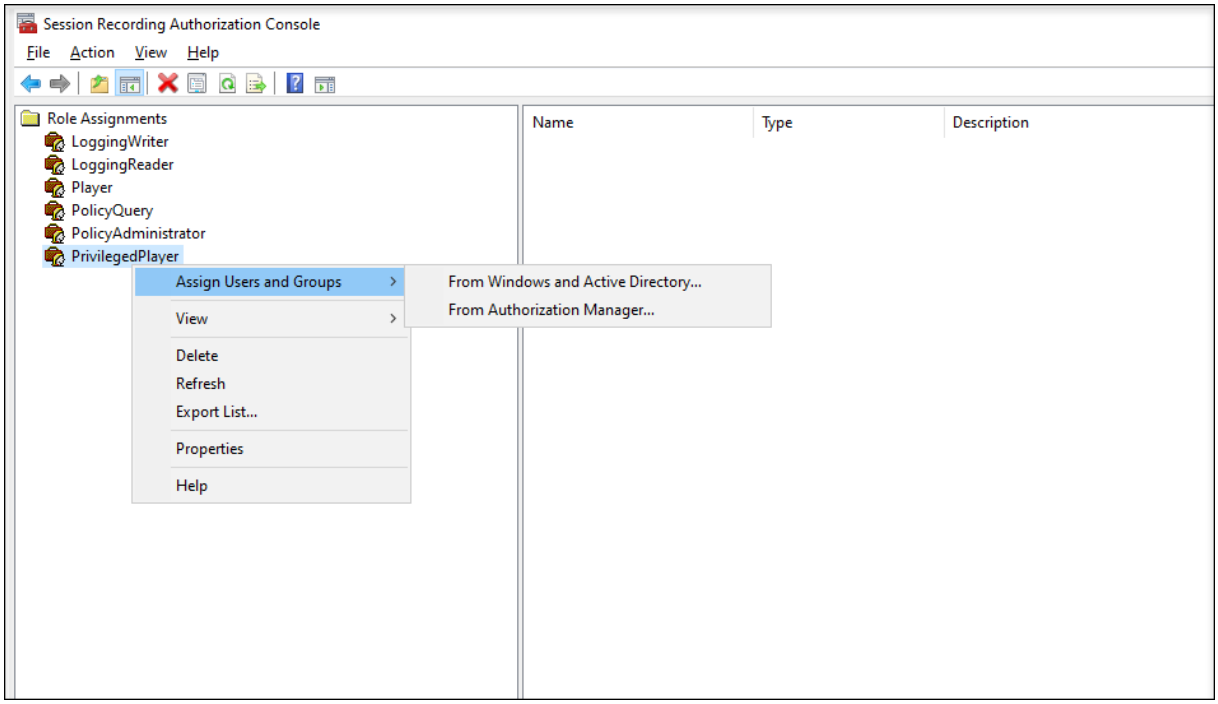
［時間］フィルターには録画の開始日、開始日時、経過時間があります。

録画へのアクセス制限の設定

February 20, 2024

録画の閲覧ポリシーによる役割ベースのアクセス制御に加えて、対象の録画にアクセス制限を設定します。制限付き録画には、Citrix Session Recording 承認コンソールで **PrivilegedPlayer** の役割が割り当てられたユーザーおよびユーザーグループのみがアクセスできます。

> 注:
>
> ライブ録画へのアクセス制限はサポートされていません。



次のセクションでは、対象の録画に対するアクセス制限を設定および削除するプロセスについて説明します。

1. サポートされているブラウザーのアドレスバーに、Web Player の Web サイトの URL を入力します。

   URL の形式は、**http(s)://<Session Recording** サーバーの **FQDN>/WebPlayer** です。

   サポートされているブラウザーは Google Chrome、Microsoft Edge、Firefox です。

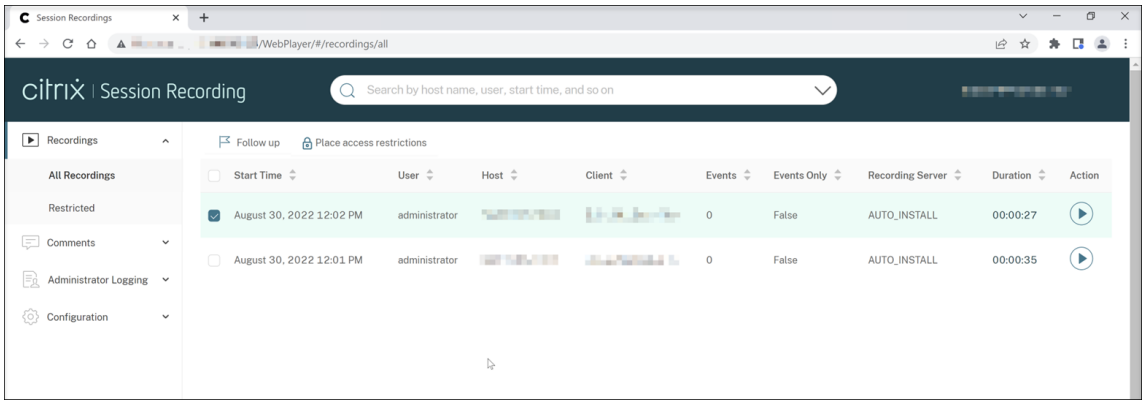
2. Web Player ページの左側のナビゲーションで、［録画］メニューを展開します。

3. ［すべての録画］ページで、1 つまたは複数の録画を選択します。

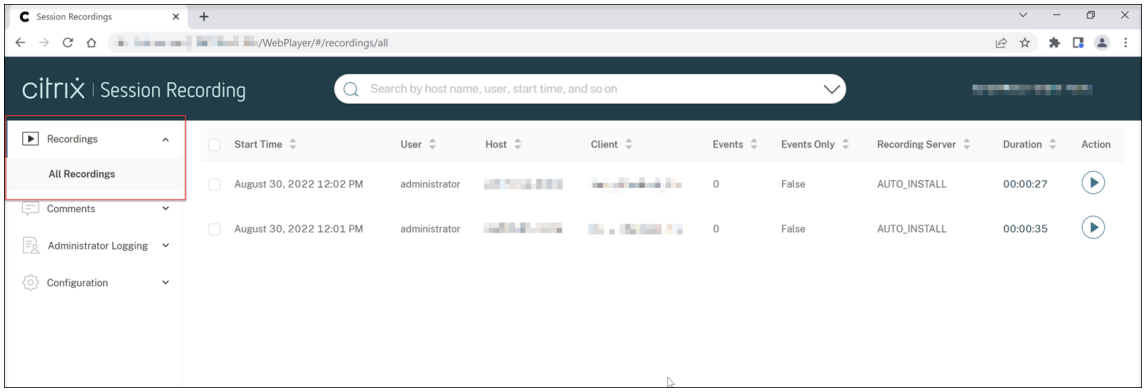
4. 録画一覧の上部にある ［アクセス制限を設定する］アイコンをクリックします。

   Player または **PrivilegedPlayer** のいずれかの役割が割り当てられたユーザーおよびユーザーグループは、録画にアクセス制限を設定できます。［制限］メニューは、**PrivilegedPlayer** の役割が割り当てられたユーザーおよびユーザーグループのみが使用できます。

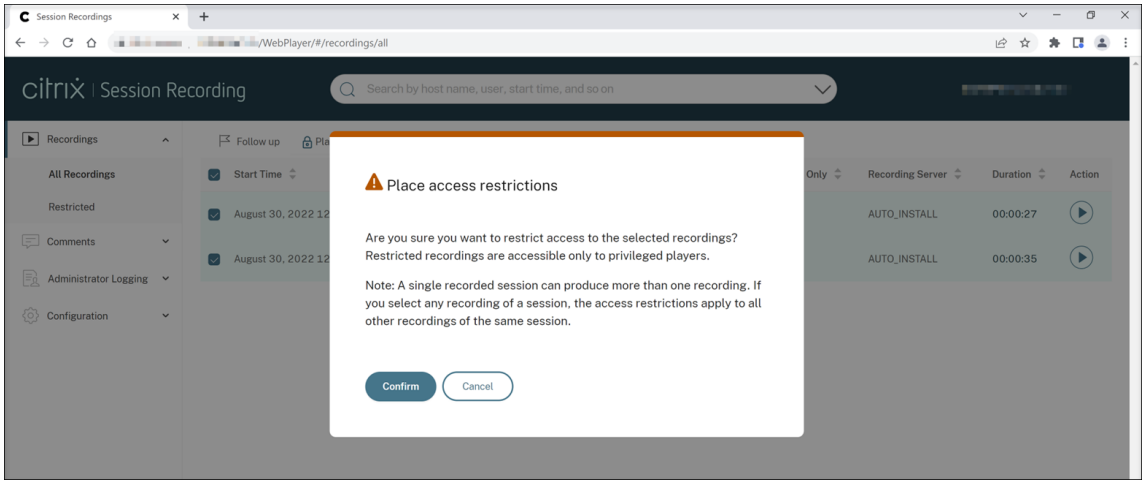
   PrivilegedPlayer の役割のビュー：



Player の役割のビュー：

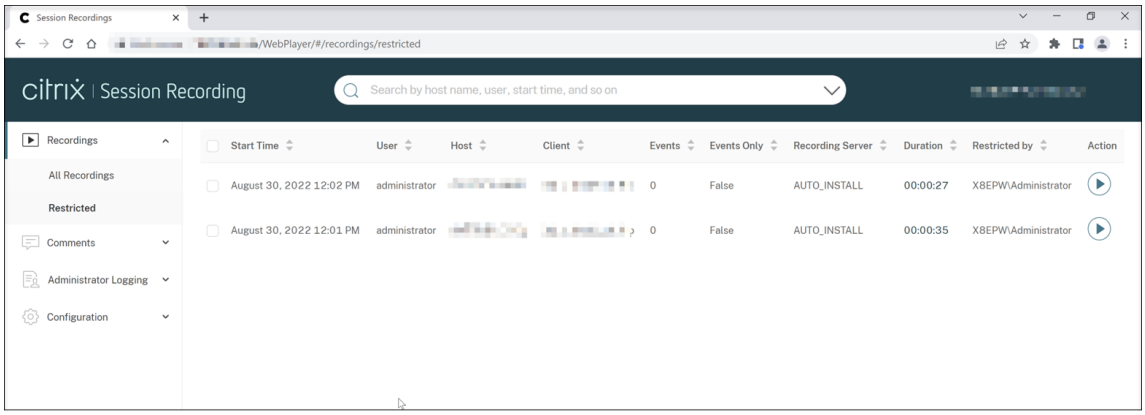


5. [確認] をクリックします。

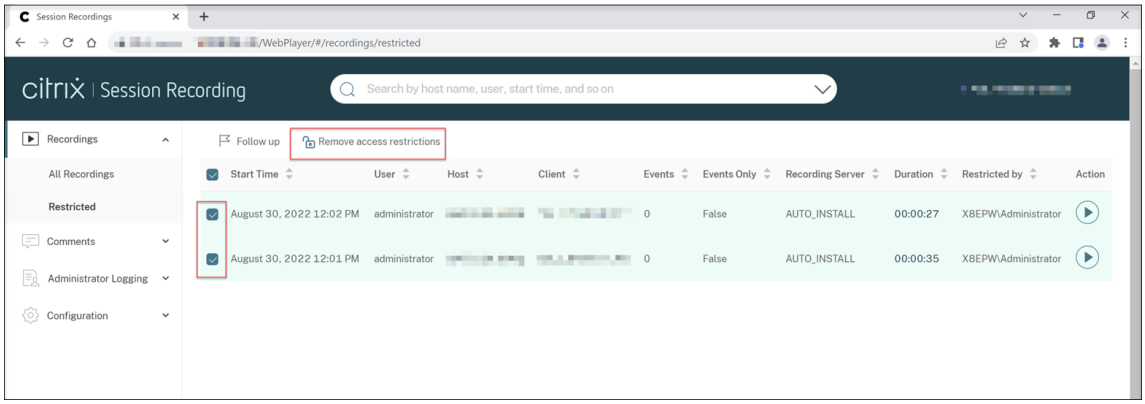


6. アクセス制限を設定した選択した録画が、[すべての録画] ページから [制限] ページに移動したことを確認します。

   [制限設定者] 列には、関連する録画にだれがアクセス制限を設定したかが表示されます。



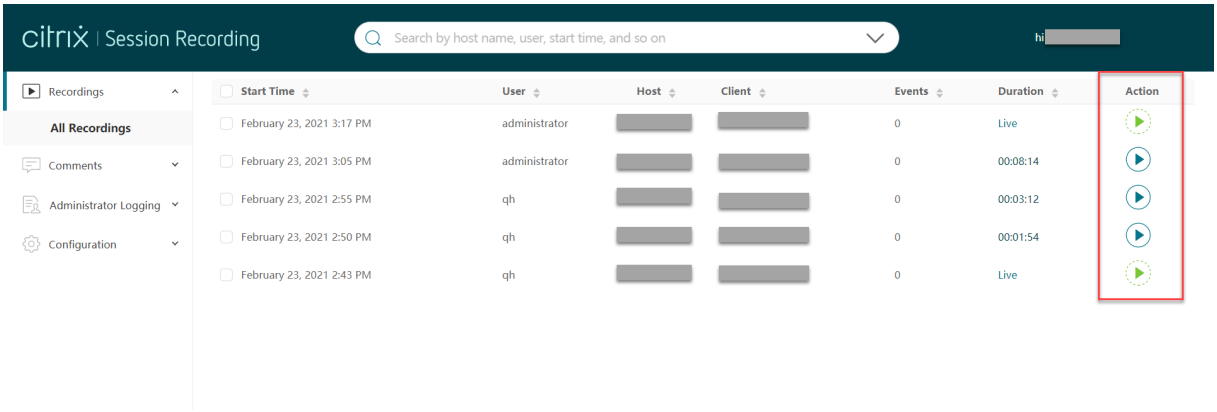
7. [制限] ページで、必要に応じてアクセス制限を解除します。アクセス制限が解除されると、録画は [すべての録画] ページに戻ります。



録画を開いて再生

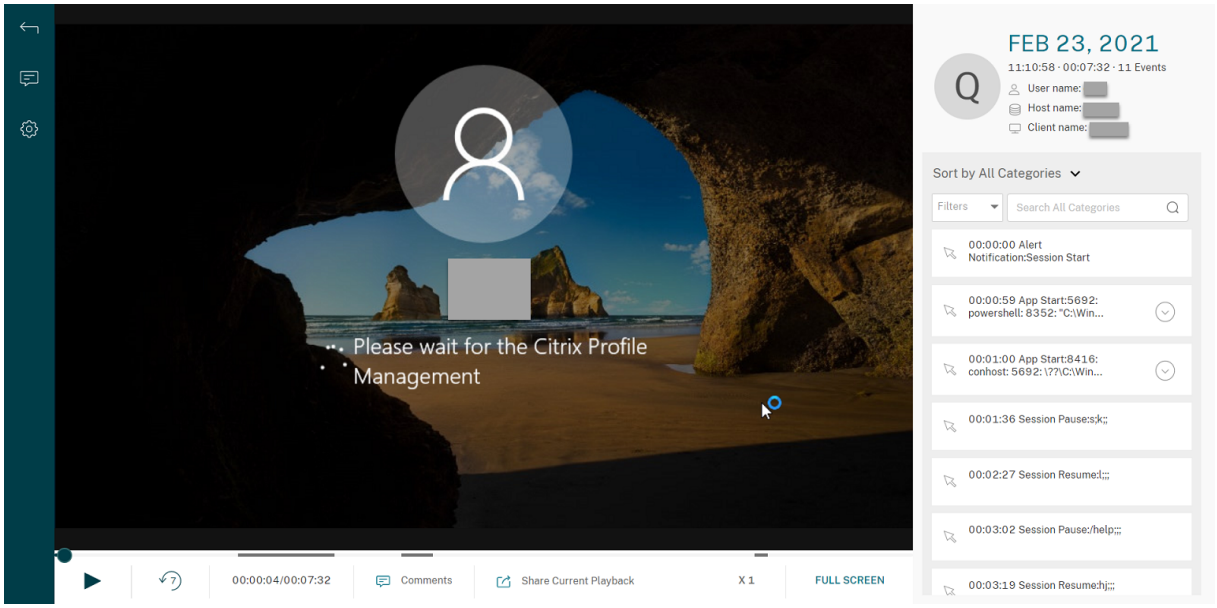
February 20, 2024

Web Player では、ライブと録画を再生できます。録画ページの各録画には ［経過時間］項目の右側に再生ボタンがあります。



> ヒント：
>
> **Player** の役割の場合、左側のナビゲーションの ［録画］メニューには ［すべての録画］サブメニューのみが表示されます。
>
> **PrivilegedPlayer** の役割の場合は、［録画］メニューには ［すべての録画］と ［制限］の両方のサブメニューが表示されます。

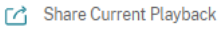
再生ボタンをクリックします。再生ページが表示されます。メモリキャッシュの後に再生が開始されます。

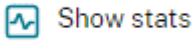
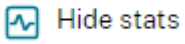


ヒント:

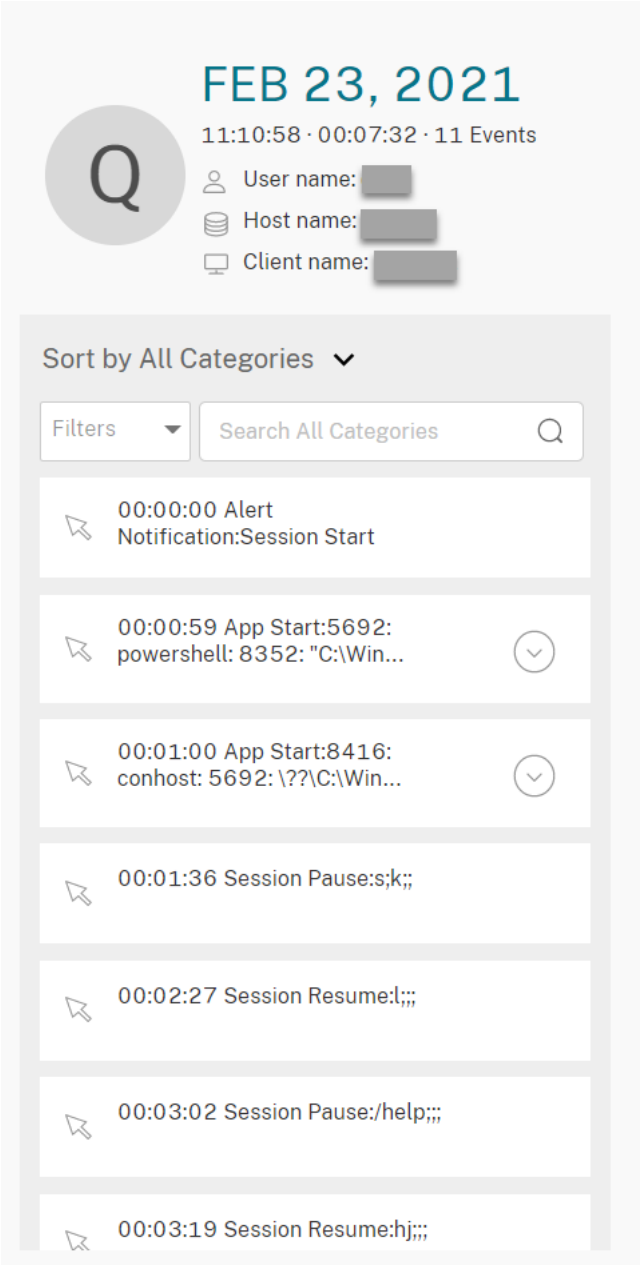
- セッションの進行時間をクリックすると、セッションが録画された絶対日時に切り替えることができます。
- イベントのみの録画の場合、左上隅の再生アイコンは使用できません。

Player ウィンドウの説明については、次の表を参照してください:

Player ウィンドウの制御	説明
	選択した録画ファイルを再生します。
	再生を一時停止します。
	再生中に進行状況バーをドラッグできます。録画されたセッションのアイドル期間は再生中にハイライトされます。
	7 秒前へシークします。
	録画再生の現在位置と合計録画時間を示します。時間の形式は HH:MM:SS です。
	録画の再生中にクリックしてコメントを追加することができます。
	現在の録画の URL をクリックしてクリップボードにコピーできます。

Player ウィンドウの制御	説明
	録画されたセッションに関連するデータポイントを持つオーバーレイを表示します。
	セッションデータオーバーレイを非表示にします。
	現在の再生速度を示します。アイコンをクリックして、X0.5、X1、X2、X4 などのオプションを切り替えます。
	全画面で再生を表示します。
	Web ページ内で再生を表示します。

再生ページの右ペインでは、イベントフィルターとコメントフィルター、クイック検索ボックス、一部の録画データを使用できます:



- Web Player マシンの日付と時刻。この例では、**AUG 20, 2021** と **18:50:50** です。
- 再生中の録画の時間。この例では、**01:37:00** です。
- 録画内のイベント数。この例では、**359 EVENTS** です。
- セッションが録画されたユーザー名。
- 録画されたセッションがホストされている VDA のホスト名。
- セッションが実行されているクライアントデバイスの名前。
- 検索結果を並べ替えるオプション：［すべて］、［イベント］または ［コメント］を選択して検索結果を並べ替えます。

- イベントフィルター。複数のフィルターを選択して、現在の録画内のイベントを検索できます。

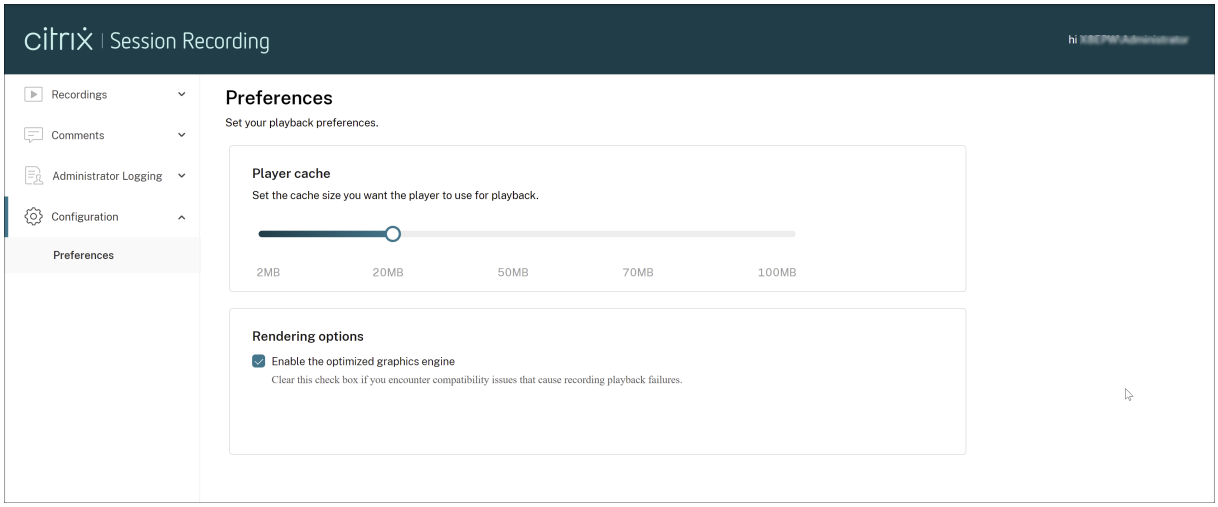
  アイコンをクリックして、イベントの表示を展開します。例:

- イベント一覧。一覧のイベントをクリックすると、録画内のイベントの位置に移動します。
- クイック検索ボックス。[イベントを検索] クイック検索ボックスによって、現在の録画でイベント一覧をすばやく絞り込むことができます。

基本設定を構成する

February 20, 2024

Web Player の基本設定を構成するには、Web Player ページで [構成] > [基本設定] に移動します。



Web Player の次の基本設定を構成できます:

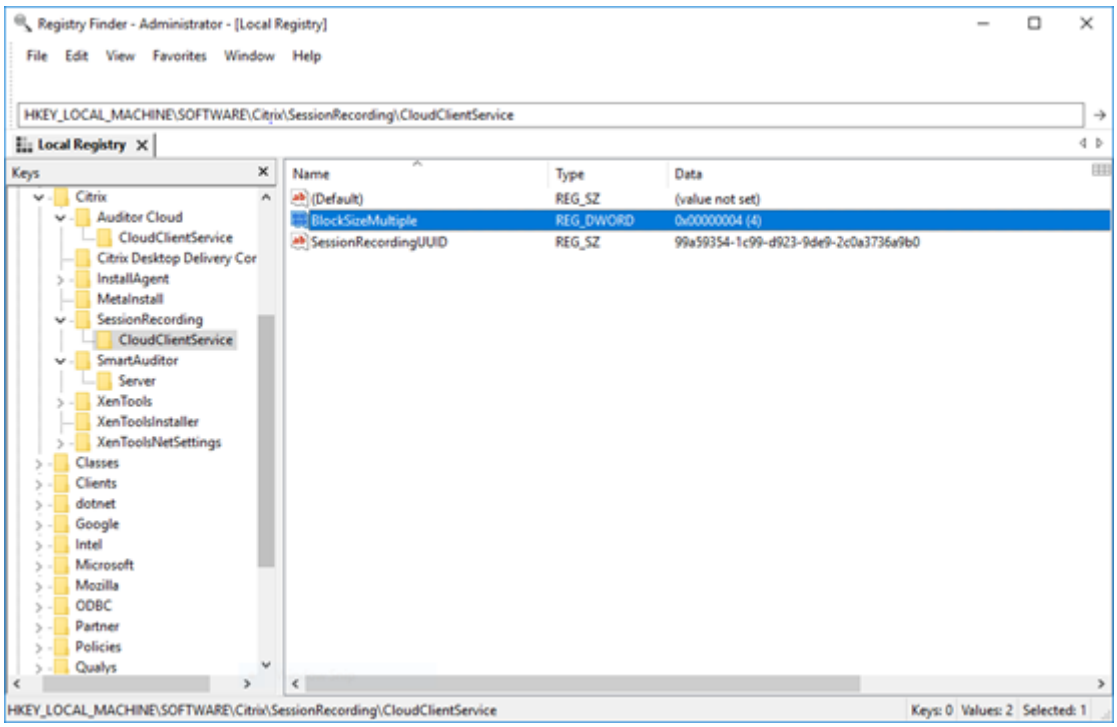
- **Player** キャッシュ。スライダーをドラッグして、Player が再生に使用するキャッシュサイズを設定します。
- 最適化されたグラフィックエンジン。グラフィックエンジンを最適化して、Web Player のパフォーマンスを向上させました。最適化されたエンジンはデフォルトで有効になっています。互換性やその他の問題が発生した場合は、チェックボックスをオフにすることで最適化されたエンジンを無効にできます。

Web Player の転送パケットサイズを増やす

December 22, 2022

1. <Session Recording installation path>/WebSocketServerにある **Web** 構成ファイルを見つけます。
2. **Web** 構成ファイルを開きます。
3. **BlockSizeMultiple** 値を編集します。

   デフォルト値は 1（4KB）です。値を 8（32KB）に設定することをお勧めします。



アイドル期間のハイライト

December 22, 2022

Session Recording はアイドルイベントを録画し、Web Player のアイドル期間をハイライトできます。

> ヒント：
>
> アイドルイベントは関連録画ファイル（.iclファイル）ではなく Session Recording データベースに保存されるため、Session Recording Player に表示されません。

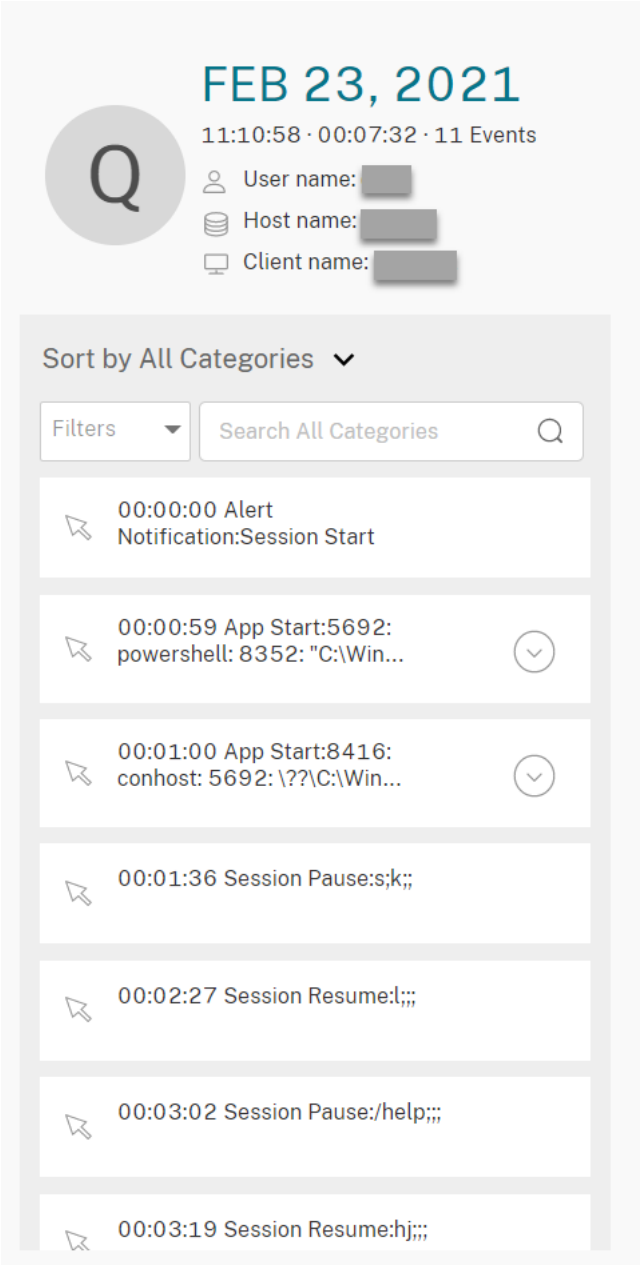
アイドルイベント機能をカスタマイズするには、HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SessionEventsにある以下のレジストリキーを設定します。

レジストリキー	デフォルト値	説明
DisableIdleEvent	0	アイドルイベント機能を無効にするには、値を **1** に設定します。アイドルイベント機能を有効にするには、値を **0** に設定します。
IdleEventThrottle	30 秒	レジストリキーで設定された期間のしきい値より長くユーザーアクティビティ（グラフィックの変更やキーボード/マウス入力を含む）がない場合、アイドルイベントが録画されます。録画されたセッションが Session Recording Web Player で再生されると、アイドル期間がハイライトされます。
IdleEventActiveThrottle	2 秒	指定された期間の指定された数のグラフィックの変更のみがユーザーアクティビティと見なされます。デフォルトでは、2 秒以内に少なくとも 3 つのパケットがユーザーアクティビティと見なされます。
IdleEventActivePktNumThrottle	3 つのパケット	指定された期間の指定された数のグラフィックの変更のみがユーザーアクティビティと見なされます。デフォルトでは、2 秒以内に少なくとも 3 つのパケットがユーザーアクティビティと見なされます。
IdleEventActivePktSizeThrottle	300 バイト	キー値よりも小さいグラフィックパケットは無視され、関連する期間はアイドル状態と見なされます。

イベントとコメントの使用

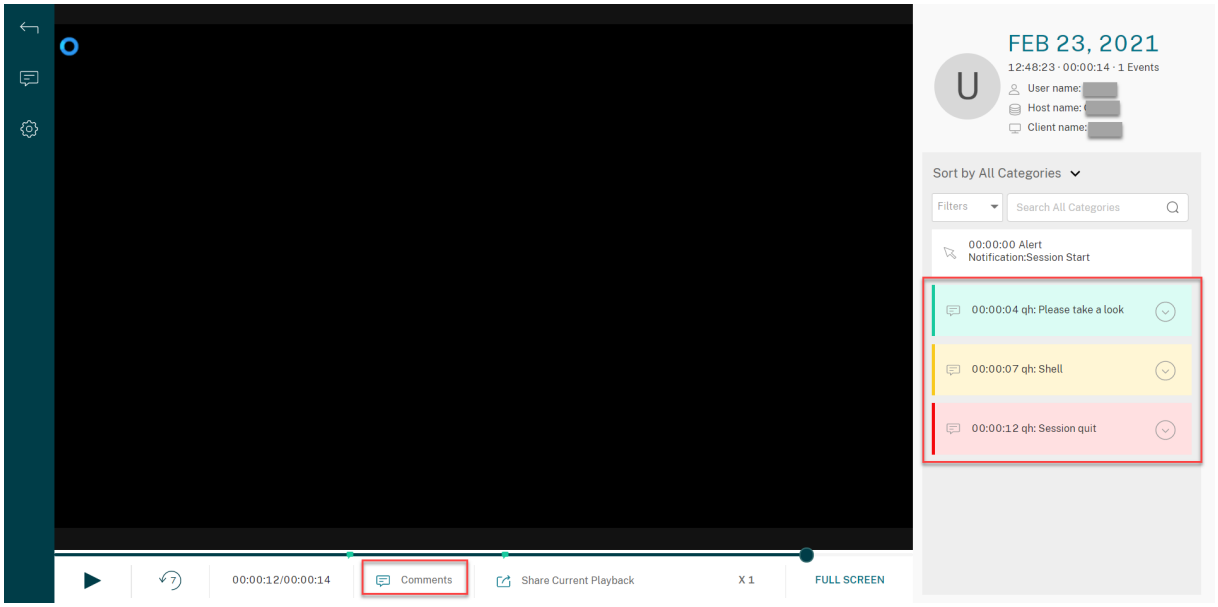
February 20, 2024

再生ページの右ペインでは、［イベント］フィルターと ［コメント］フィルターを使用できます。Web Player でイベントとコメントを使用して、録画されたセッション内を簡単に移動できます。

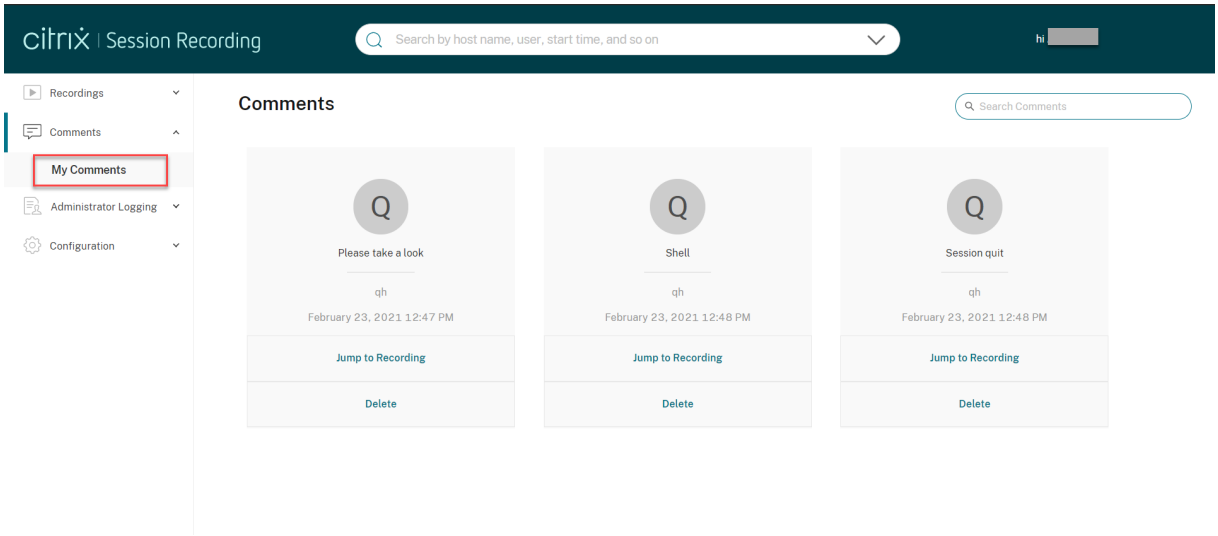


録画へのコメント

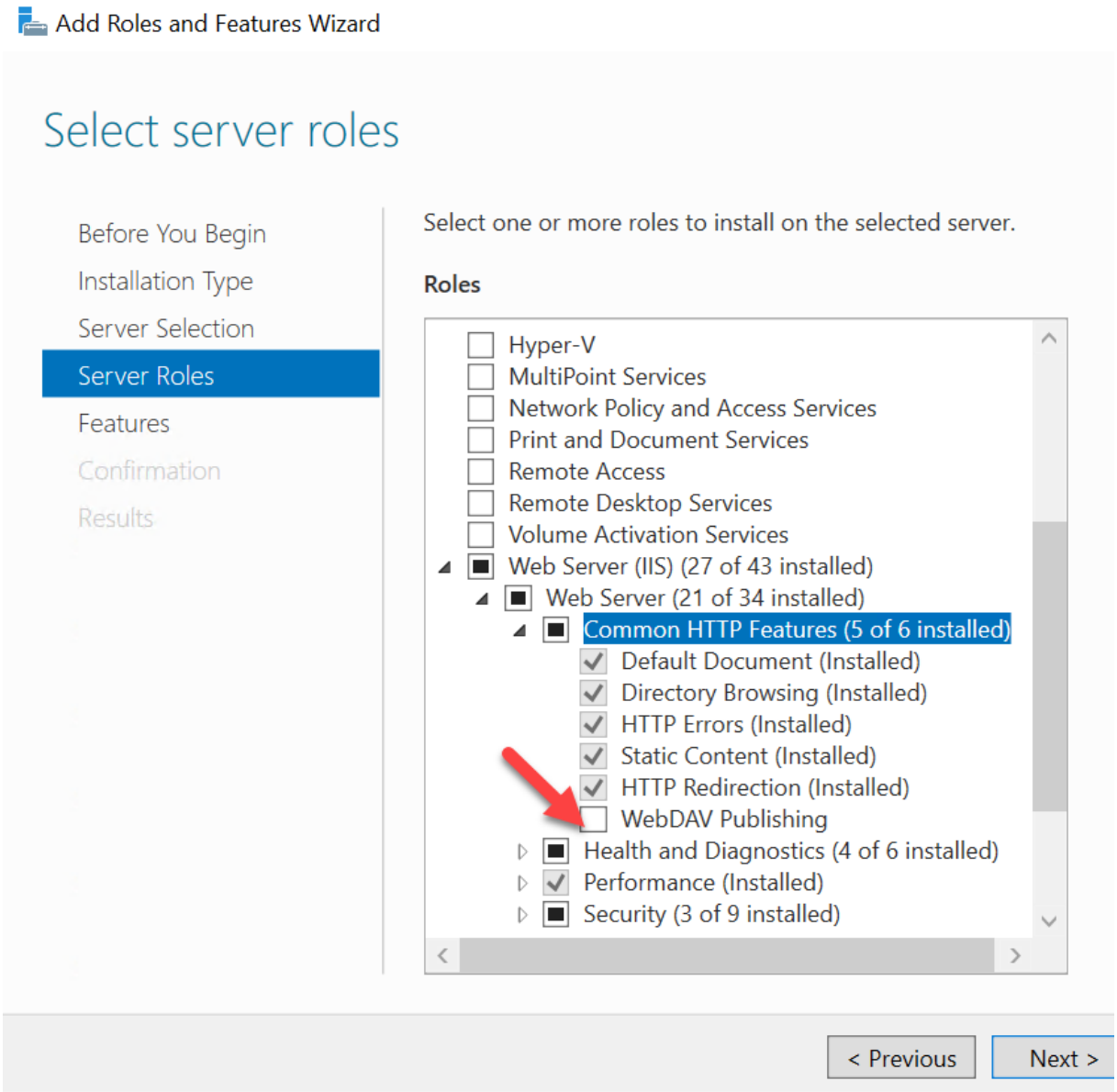
録画されたセッションが再生されると、［コメント］プレイヤーウィンドウをクリックしてコメントを追加し、コメントの重要度を設定できます。重要度には［通常］、［中］、［高］があります。［高］コメントと［中］コメントは、それぞれ赤とオレンジのドットで示されます。セッションの再生中、録画に関するすべてのコメントを表示できます。自分が追加したコメントを削除するには、Web ページを更新しコメントを展開して、［削除］をクリックします。



コメントをクリックすると、コメントが追加された場所にジャンプできます。[マイコメント] ページですべてのコメントを表示できます。



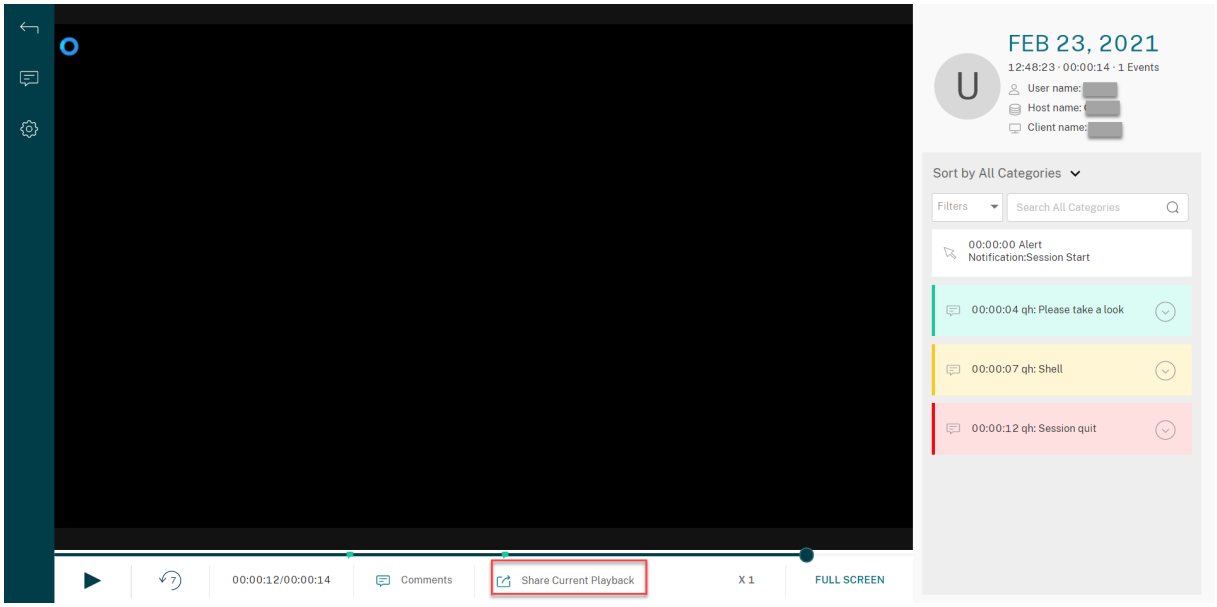
> 注:
>
> コメント機能を正常に動作させるには、Session Recording サーバー上の Server Manager の [役割と機能の追加] ウィザードで [**WebDAV Publishing**] チェックボックスをオフにします。



録画の **URL** の共有

February 20, 2024

録画の再生ページで ［現在の再生を共有する］をクリックすると、録画 URL をクリップボードにコピーします。他のユーザーと URL を共有できるため、ユーザーはすべての録画を検索することなく、URL から録画に直接アクセスできます。



［現在の再生を共有する］をクリックした後、次のメッセージのいずれかが表示され、操作が成功か失敗かが示されます：

- 共有された録画の **URL** がクリップボードにコピーされました
- 録画 **URL** の共有に失敗しました

共有 URL をアドレスバーに貼り付けると、URL がコピーされた場所にジャンプできます。

セキュアに共有するには、`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server` に次のレジストリ値を設定します：

レジストリ値	説明	デフォルト値	注釈
LinkExpire	共有 URL が期限切れになるまでの期間。10 マイクロ秒単位でカウントされます。	1,728,000,000,000（デフォルト値は 2 日です。）	-
LinkSalt	上記の URL の有効期限を保護するセキュリティメソッド	Kk2od974	デフォルト値を、数字で終わる（推奨）任意の文字列に変更します。

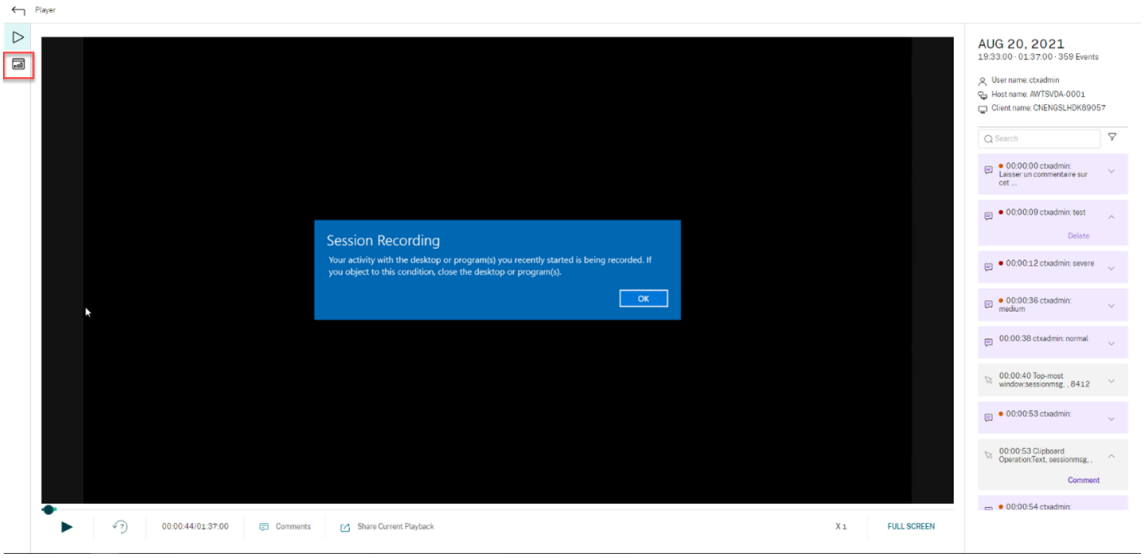
各録画のグラフィカルなイベント統計を表示する

February 20, 2024

イベントデータの視覚化は、Web Player で録画ごとに利用できます。グラフィカルなイベント統計により、録画に挿入されたイベントをすばやく把握できます。

グラフィカルなイベント統計を表示するには、次の手順を実行します:

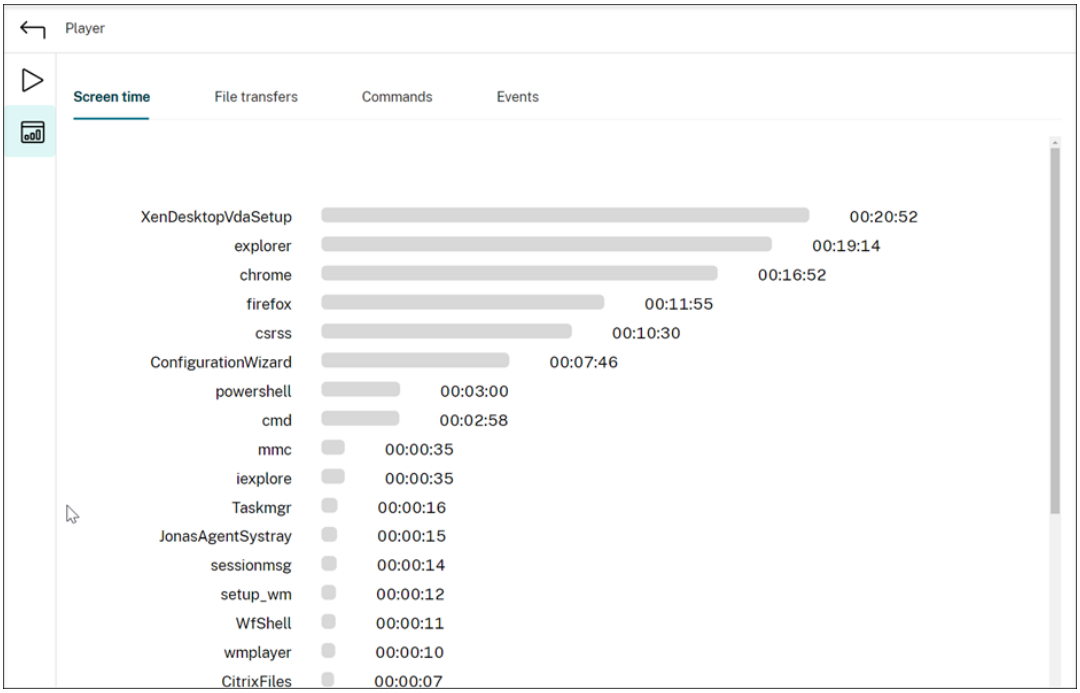
1. 録画を開いて再生します。
2. 再生ページの左上隅にある統計アイコンをクリックします。



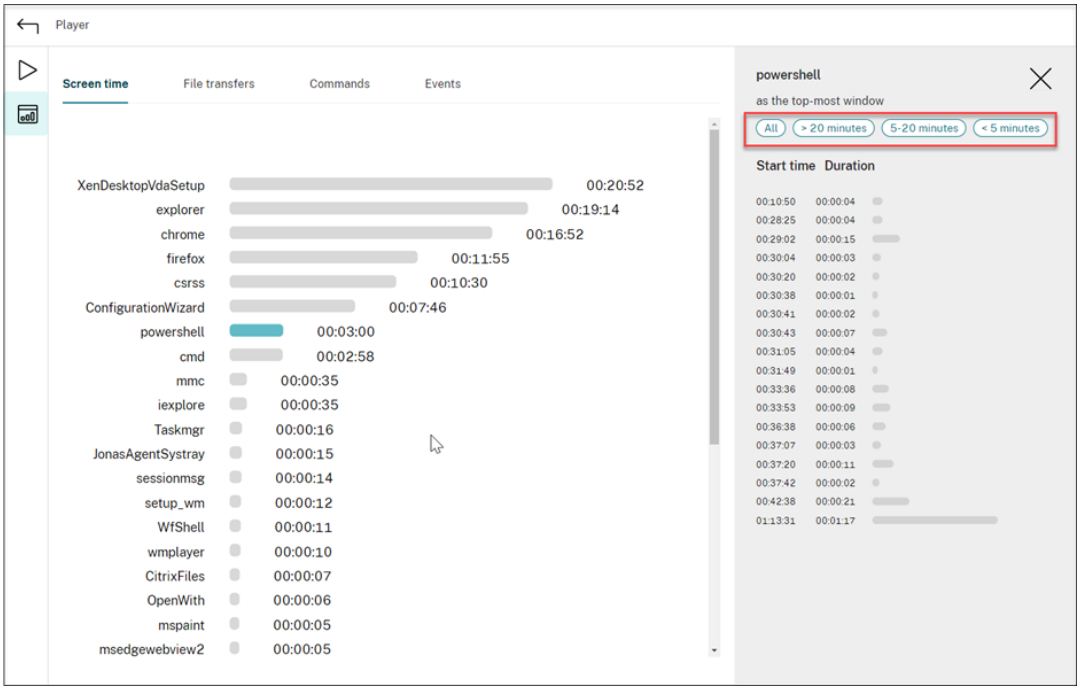
3. [画面表示時間]、[ファイル転送]、[コマンド]、[イベント] タブを切り替えて、さまざまな観点から統計を表示します。

    - スクリーンタイム

      [画面表示時間] タブでは、アプリケーションウィンドウがフォーカスされている累積時間を知ることができます（アクティブウィンドウ）。



各アプリケーションの横に水平のタイムバーがあります。バーをクリックすると、アプリケーションがフォーカスされるたびに開始時間とフォーカスの期間を表示できます。デフォルトの ［すべて］オプション以外の期間の範囲を指定することにより、検索範囲を絞り込むことができます。例:



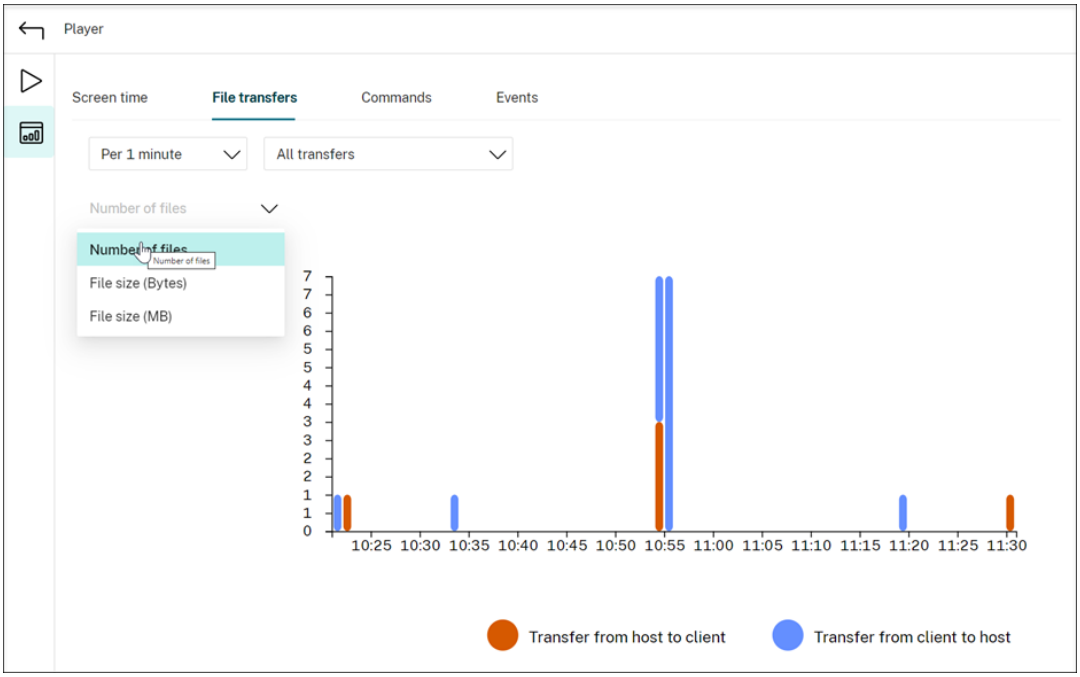
- ファイル転送

  ［ファイル転送］タブには、セッションの録画をホストしている VDA とセッションが実行されているクライアントデバイスとの間の双方向ファイル転送に関するグラフィカルな統計が表示されます。次の設

定を使用して、視覚化をカスタマイズできます:

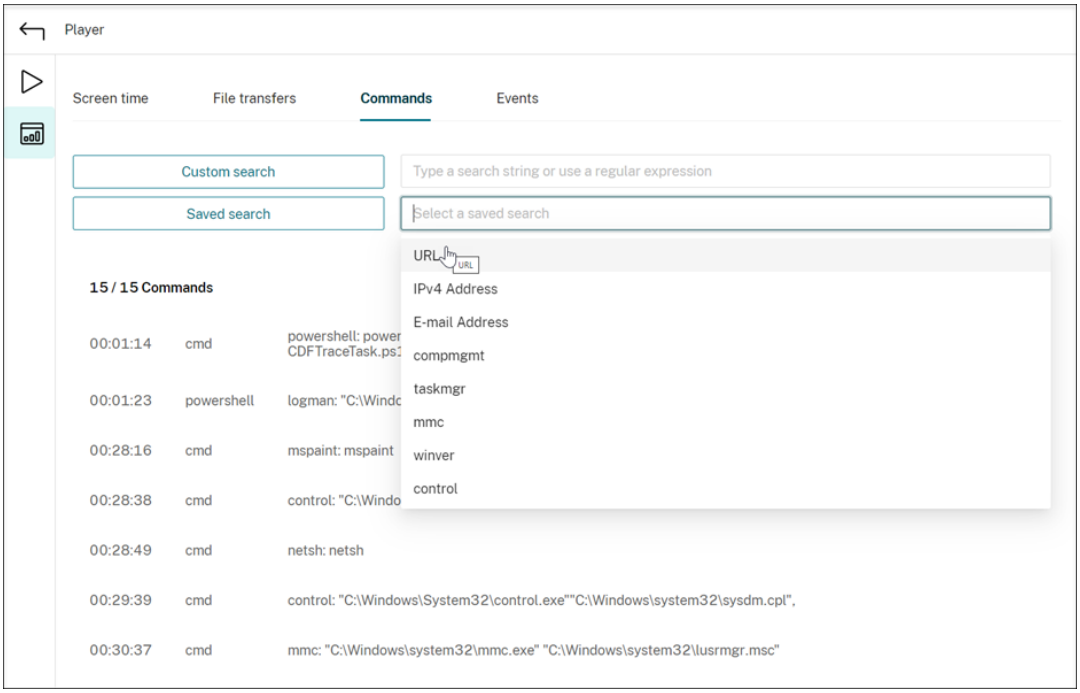
- 時間の単位:［**1** 分ごと］、［**10** 分ごと］、［**1** 時間ごと］
- ファイル転送先:［すべての転送］、［ホストからクライアントへの転送］、［クライアントからホストへの転送］
- 転送されたファイルの数またはサイズ（バイトまたは MB）

X 軸は、24 時間形式での絶対時間を表します。



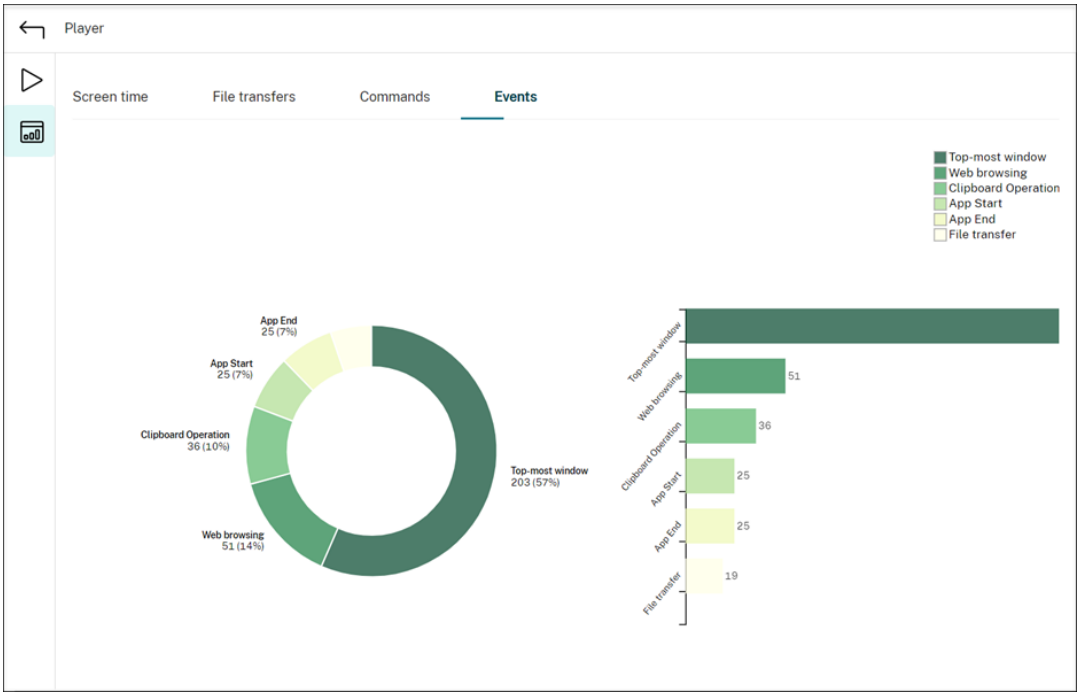
- **Commands**

［コマンド］タブには、録画されたセッション中に実行される CMD コマンドと PowerShell コマンドが表示されます。［カスタム検索］にカスタム検索を入力するか、［保存した検索］から保存した検索を選択することで、データの表示をカスタマイズできます。「OR」論理演算子は、最終アクションを計算するために使用されます。



- イベント

  ［イベント］タブには、録画されたセッションのすべての種類のイベントの割合と数が表示されます。

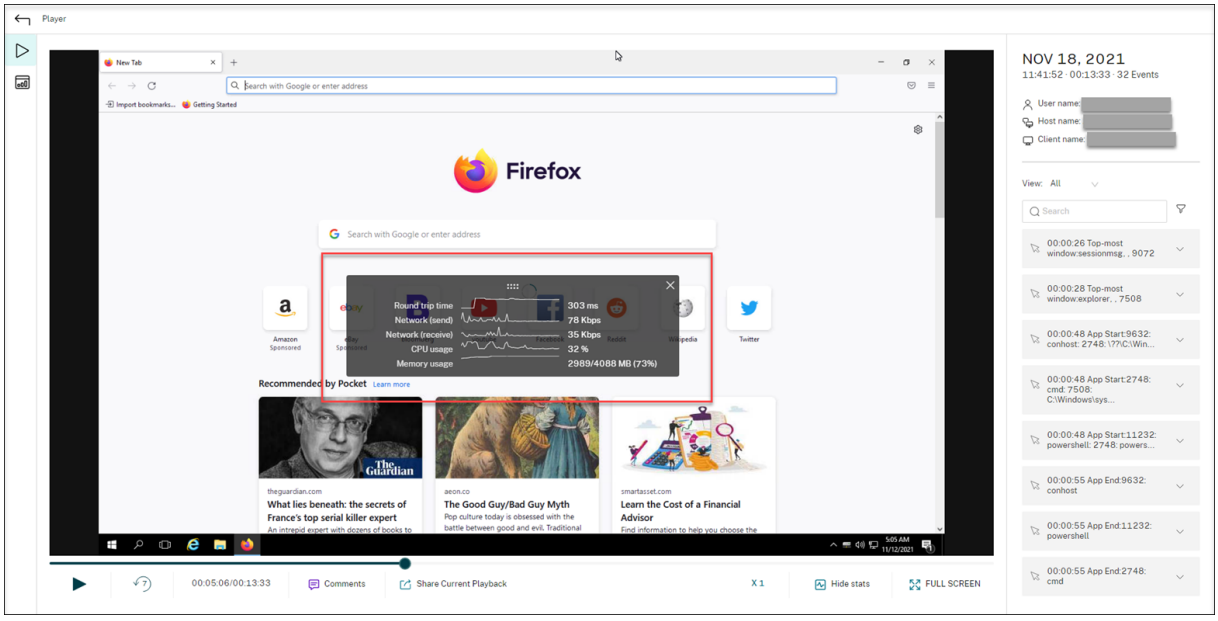


録画された各セッションに関連するデータポイントを表示する

February 20, 2024

再生中に、［統計を表示］コントロールをクリックすることで、録画されたセッションに関連する次のデータポイントをオーバーレイで表示できます:

- 往復時間
- ネットワーク（送信）
- ネットワーク（受信）
- CPU 使用率
- メモリ使用率



> 注:
>
> - Session Recording は、15 秒ごとに往復時間を収集し、残りのデータポイントを 1 秒ごとに収集します。
> - 理論的には、Session Recording は 5 秒ごとに往復時間のデータを更新します。ただし、往復時間データは、収集サイクルのため、実際には 15 秒ごとに更新されます。
> - Session Recording は、残りのデータポイントを 5 秒ごとに更新し、それらの平均値をオーバーレイに表示します。

オーバーレイは半透明です。移動したり、非表示にしたりすることができます。

- オーバーレイを移動するには、マウスを 8 つのドットの上に置いてから、ドラッグアンドドロップを実行します。
- オーバーレイを非表示にするには、［統計を非表示］をクリックします。

イベント検出ポリシーを作成するときに、［パフォーマンスデータをログに記録する］を選択すると、オーバーレイを有効にできます。詳しくは、「イベント検出ポリシーの構成」を参照してください。

録画の管理

December 23, 2022

ICA ログデータベース（ICLDB）は、データベース用のコマンドラインユーティリティで、セッションの録画のデータベースレコードを操作するために使用します。このユーティリティは、Session Recording サーバーをホストするサーバーの`\Program Files\Citrix\SessionRecording\Server\Bin`フォルダーに、Session Recording と合わせてインストールされます。

クイックリファレンス

次の表に、ICLDB ユーティリティで使用できるコマンドとオプションの一覧を示します。コマンドは次の形式で入力します。

```
icldb [version | locate | dormant | import | archive | remove |
removeall] command-options [/l] [/f] [/s] [/?]
```

> 注:
>
> 詳しくは、ユーティリティ関連のヘルプを参照してください。ヘルプにアクセスするには、コマンドプロンプトから`\Program Files\Citrix\SessionRecording\Server\Bin`フォルダー、`icldb /?`の順に入力します。特定のコマンドのオンラインヘルプにアクセスするには、「`icldb *command* /?`」と入力します。

コマンド	説明
`archive`	指定された保有期間を過ぎたセッションの録画ファイルをアーカイブします。このコマンドを使用して、録画と録画内のイベントをアーカイブします。イベントは`ArchivedEvent`データベーステーブルにアーカイブされます。

コマンド	説明
dormant	休止状態とみなされるセッションの録画ファイルの数またはファイル名を表示します。休止ファイルとは、データの損失のために不完全なセッションの録画ファイルです。このコマンドを使用してデータの損失があるかどうかを検証します。休止状態のセッションの録画ファイルの検索対象として、データベース全体を指定することも、日、時間、または分単位で、録画が行われた期間を指定することもできます。
import	セッションの録画ファイルを Session Recording データベースにインポートします。このコマンドを使用して、データベースレコードを失ったときにデータベースを再構築します。また、このコマンドを使用して、データベースをマージします。2 つのデータベースがある場合は、一方のデータベースからファイルをインポートできます。
locate	ファイル ID を条件として、セッションの録画ファイルを検索しフルパスを表示します。このコマンドを使用して、セッションの録画ファイルの格納場所を検索します。このコマンドは、特定のファイルを条件にデータベースが最新の状態かどうかを検証する手段としても使用できます。
remove	セッションの録画ファイルへの参照をデータベースから削除します。このコマンドを使用して、データベースをクリーンアップします。ただし、注意して使用してください。条件として使用する保有期間を指定します。関連付けられている物理ファイルを削除することもできます。
removeall	セッションの録画ファイルへのすべての参照を Session Recording データベースから削除し、データベースを元の状態に戻します。実際の物理ファイルは削除されません。ただし、Session Recording Player でファイルを検索することはできなくなります。このコマンドを使用して、データベースをクリーンアップします。ただし、注意して使用してください。削除された参照はバックアップから復元しない限り元に戻せません。
version	Session Recording データベースのスキーマバージョンを表示します。
/l	結果とエラーを Windows のイベントログに記録します。
/f	プロンプトを表示せずにコマンドを強制的に実行します。

コマンド	説明
/s	著作権のメッセージを非表示にします。
/?	コマンドのオンラインヘルプを表示します。

セッションの録画ファイルのアーカイブ

録画の格納場所に適切なレベルの空きディスク容量を維持するには、セッションの録画ファイルを定期的にアーカイブします。使用可能なディスク容量と標準的な録画ファイルのサイズに応じて、アーカイブ間隔は異なります。録画開始日から 2 日以上経過すると、セッションの録画ファイルはアーカイブ可能となります。この規則は、ライブ録画が完了する前にアーカイブされないようにするためのものです。

セッション録画をアーカイブするには、2 つの方法があります。録画ファイルが録画の格納場所にある間に、録画ファイルのデータベースレコードを更新してアーカイブ済みのステータスにすることができます。この方法を使用すると、Player での検索結果を減らすことができます。もう 1 つの方法は、録画ファイルのデータベースレコードをアーカイブ済みのステータスに更新し、そのファイルを録画の格納場所から別の場所に移して代替メディアにバックアップする方法です。ICLDB ユーティリティを使ってセッションの録画ファイルを移動する場合、それらのファイルは、年/月/日の元のファイルフォルダー構造のない指定されたディレクトリに移動します。

Session Recording データベースのセッションの録画レコードには、アーカイブに関連する 2 つのフィールド（アーカイブ日時とアーカイブメモ）が含まれています。アーカイブ日時は、録画がアーカイブされた最新の日時を表します。アーカイブメモは、アーカイブ中に追加できる任意のテキストメモです。この 2 つのフィールドは、録画がアーカイブされたこと、およびアーカイブの日時を示します。

Session Recording Player では、アーカイブされたセッションの録画にアーカイブ済みのステータスとアーカイブ日時が示されます。ファイルが移動していなくても、アーカイブされたセッション録画は再生されます。アーカイブ中にセッションの録画ファイルが移動した場合、「ファイルが見つかりません」というエラーが表示されます。セッションを再生するには、セッションの録画ファイルを復元する必要があります。セッションの録画ファイルを復元するには、録画ファイルのファイル ID とアーカイブ日時を指定します。アーカイブされたファイルの復元については、以下の「セッションの録画ファイルの復元」セクションで詳しく説明しています。

ICLDB ユーティリティの **archive** コマンドには、次のようなパラメーターがあります:

- **/RETENTION:<days>** - セッション録画の保有期間（日数）。指定された日数を超過した録画は、Session Recording データベースでアーカイブ済みにマークされます。保有期間は 2 日以上の整数とする必要があります。
- **/LISTFILES** - セッションの録画ファイルのアーカイブ時の完全なファイルパスとファイルを一覧表示します。このパラメーターはオプションです。
- **/MOVETO:<directory>** - アーカイブされたセッションの録画ファイルを物理的に移動する移動先ディレクトリ。あらかじめ存在するディレクトリを指定する必要があります。このパラメーターはオプションです。ディレクトリが指定されていない場合、ファイルは元の格納場所に残ります。

- **/NOTE:<note>** - データベースレコードに追加される、アーカイブされた各セッション録画のテキストを含むメモ。このメモは二重引用符で囲んでください。このパラメーターはオプションです。
- **/L** - Windows イベントログに、アーカイブされたセッションの録画ファイルの結果とエラーの数を記録します。このパラメーターはオプションです。
- **/F** - プロンプトを表示せずに archive コマンドを強制的に実行します。このパラメーターはオプションです。

Session Recording データベースにセッション録画をアーカイブし、セッションの録画ファイルを物理的に移動するには

1. Session Recording サーバーがインストールされているサーバーに、ローカル管理者としてログオンします。
2. コマンドプロンプトを開始します。
3. 現在の作業ディレクトリから、Session Recording サーバーのインストールパスの Bin ディレクトリ（<Session Recording server Installation Path>/Server/Bin）に変更します。
4. ICLDB ARCHIVE /RETENTION:<days> /LISTFILES /MOVETO:<directory> /NOTE:<note> /Lコマンドを実行します。ここで、**days** はセッションの録画ファイルの保有期間、**directory** はアーカイブされたセッションの録画ファイルの移動先ディレクトリ、**note** はデータベースレコードに追加された、アーカイブされた各セッションの録画ファイルに関するメモです。**Y** と入力してアーカイブを確定します。

Session Recording データベースでセッション録画のアーカイブのみを行うには

1. Session Recording サーバーがインストールされているサーバーに、ローカル管理者としてログオンします。
2. コマンドプロンプトを開始します。
3. 現在の作業ディレクトリから、Session Recording サーバーのインストールパスの Bin ディレクトリ（<Session Recording サーバーのインストールパス >/Server/Bin）に変更します。
4. ICLDB ARCHIVE /RETENTION:<days> /LISTFILES /NOTE:<note> /Lコマンドを実行します。ここで、**days** はセッション録画の保有期間、**note** はデータベースレコードに追加された、アーカイブされる各セッション録画に関するメモです。**Y** と入力してアーカイブを確定します。

セッションの録画ファイルの復元

Session Recording データベースにアーカイブされ、録画の格納場所から移動した録画ファイルを表示するには、ファイルを復元します。アーカイブ中に録画の格納場所から移動されなかったアーカイブ済みのセッション録画は、Session Recording Player で引き続きアクセスできます。

移動されたセッションの録画ファイルを復元するには、2 つの方法があります。必要なセッションの録画ファイルを、アーカイブ済みファイルの復元フォルダーにコピーします。または、ICLDB ユーティリティを使用して、必要なセッ

ションの録画ファイルを Session Recording データベースにインポートします。アーカイブされたセッションの録画ファイルの復元には、最初の方法をお勧めします。アーカイブ済みファイルの復元フォルダーにコピーしたファイルは、不要になった場合、削除します。

Session Recording Broker では、セッションの録画ファイルが元の格納場所に見つからない場合、アーカイブ済みファイルの復元フォルダーを利用します。このケースは、Session Recording Player からセッションの録画ファイルの再生が要求された場合に発生します。Session Recording Broker は最初に、元の格納場所でセッションの録画ファイルを探します。ファイルが元の格納場所に見つからない場合、Session Recording Broker は次に、アーカイブ済みファイルの復元フォルダーをチェックします。ファイルが復元フォルダーに存在する場合には、Session Recording Broker は再生するためにそのファイルを Session Recording Player に送信します。ファイルが見つからない場合は、Session Recording Broker は「ファイルが見つかりません」というエラーを Session Recording Player に送信します。

アーカイブ済みの録画ファイルをインポートすると、Session Recording データベースがこのファイルのセッション録画情報（新しい格納パスなど）で更新されます。アーカイブされたセッションの録画ファイルをインポートしても、ファイルはセッション録画時の元の格納場所には戻されません。

注：インポートされたセッションの録画ファイルには、Session Recording データベースで消去されたアーカイブ日時とアーカイブメモが含まれています。次に ICLDB の`archive`コマンドを実行したとき、インポートされたセッションの録画ファイルが再度アーカイブされることがあります。

ICLDB の**`import`**コマンドは、アーカイブされた多数の録画ファイルをインポートするのに役立ちます。これにより、Session Recording データベース内の誤った欠落しているセッション録画データを修復または更新できます。また、Session Recording サーバー上のある保管場所から別の保管場所にセッション録画ファイルを移動することもできます。ICLDB の **import** コマンドは、ICLDB の`removeall`コマンドの実行後、Session Recording データベースにセッション録画を再取り込みするのにも使用できます。

ICLDB ユーティリティの**`import`**コマンドには、次のようなパラメーターがあります：

- **/LISTFILES** - セッションの録画ファイルのインポート時の完全なファイルパスとファイル名を一覧表示します。このパラメーターはオプションです。
- **/RECURSIVE** - すべてのサブディレクトリでセッションの録画ファイルを検索します。このパラメーターはオプションです。
- **/L** - Windows イベントログに、インポートされたセッションの録画ファイルの結果とエラーの数を記録します。このパラメーターはオプションです。
- **/F** - プロンプトを表示せずに import コマンドを強制的に実行します。このパラメーターはオプションです。

アーカイブされたファイルの復元フォルダーを使用してセッションの録画ファイルを復元するには

1. Session Recording サーバーがインストールされているサーバーに、ローカル管理者としてログオンします。
2. Session Recording Player のプロパティで、アーカイブされたセッションの録画ファイルのファイル ID とアーカイブ時間を特定します。

3. Session Recording Player のプロパティで指定したファイル ID を使用して、バックアップ内のセッションの録画ファイルを探します。各セッション録画のファイル名は`i_<FileID>.icl`です。ここで、FileID はセッションの録画ファイルの ID です。
4. セッションの録画ファイルを、バックアップからアーカイブ済みファイルの復元フォルダーにコピーします。アーカイブ済みファイルの復元フォルダーを特定するには:

    a) ［スタート］メニューから、［スタート］> ［すべてのプログラム］> ［**Citrix**］> ［**Session Recording** サーバーのプロパティ］の順に選択します。

    b) ［**Session Recording** サーバーのプロパティ］で、［格納場所］タブを選択します。［アーカイブ済みファイルの復元フォルダー］フィールドに現在の復元ディレクトリが表示されます。

ICLDB import コマンドを使用してセッションの録画ファイルを復元するには

1. Session Recording サーバーがインストールされているサーバーに、ローカル管理者としてログオンします。
2. コマンドプロンプトを開始します。
3. 現在の作業ディレクトリから、Session Recording サーバーのインストールパスの Bin ディレクトリ（`<Session Recording server installation path>/Server/Bin`）に変更します。
4. 以下のいずれかを実行します:

    - `ICLDB IMPORT /LISTFILES /RECURSIVE /L <directory>`コマンドを実行します。ここで、**directory** はセッションの録画ファイルを含む 1 つ以上のディレクトリの（スペースで区切られた）名前です。**Y** と入力してインポートを確定します。
    - `ICLDB IMPORT /LISTFILES /L <file>`コマンドを実行します。ここで、**file** は 1 つ以上のセッションの録画ファイルの（スペースで区切られた）名前です。セッションの録画ファイルの指定には、ワイルドカード文字を使用することもできます。**Y** と入力してインポートを確定します。

管理者ログの管理と照会

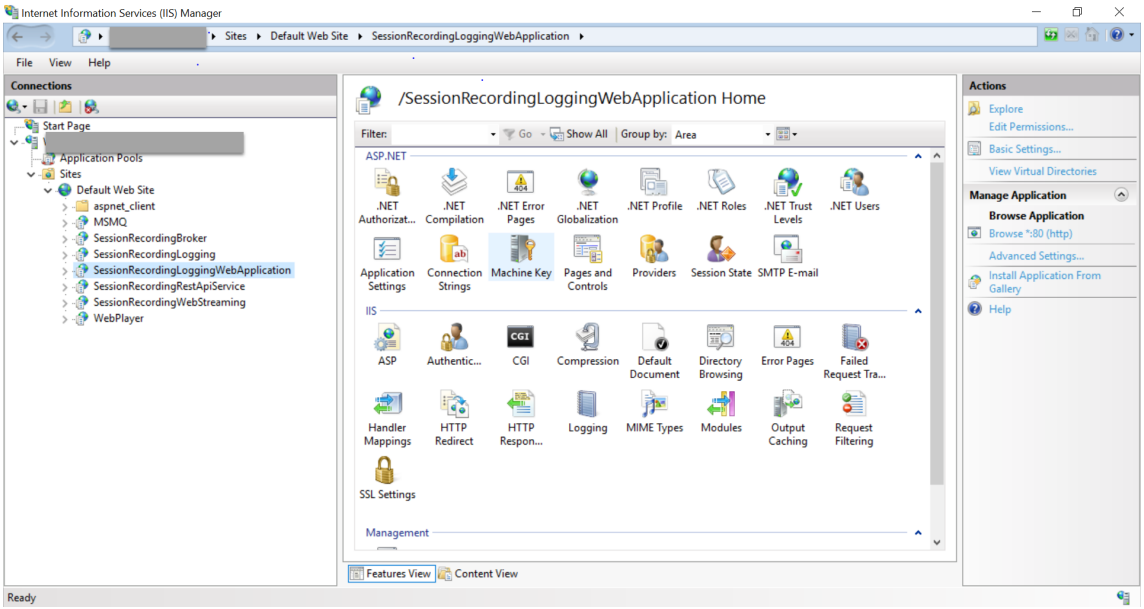
February 20, 2024

管理者ログデータの照会

要件

- **LoggingReader** と **Player** の両方の役割に割り当てられた管理者は、管理者ログを表示できます。ユーザーに役割を割り当てるには、Session Recording 承認コンソールに移動します。

- 管理者ログページは Web Player と統合されています。管理者ログを照会するには、Web Player をインストールする必要があります。インストールしない場合、404（ページが見つかりません）エラーが発生する可能性があります。
- Web Player ブラウザーに設定された言語は、Session Recording Administration コンポーネントをインストールしたときに選択した言語と一致している必要があります。
- IIS 上の SessionRecordingLoggingWebApplication サイトと Web Player の SSL 設定が同じであることを確認してください。同じではない場合、管理者ログデータへのアクセスを要求したときに 403 エラーが発生します。



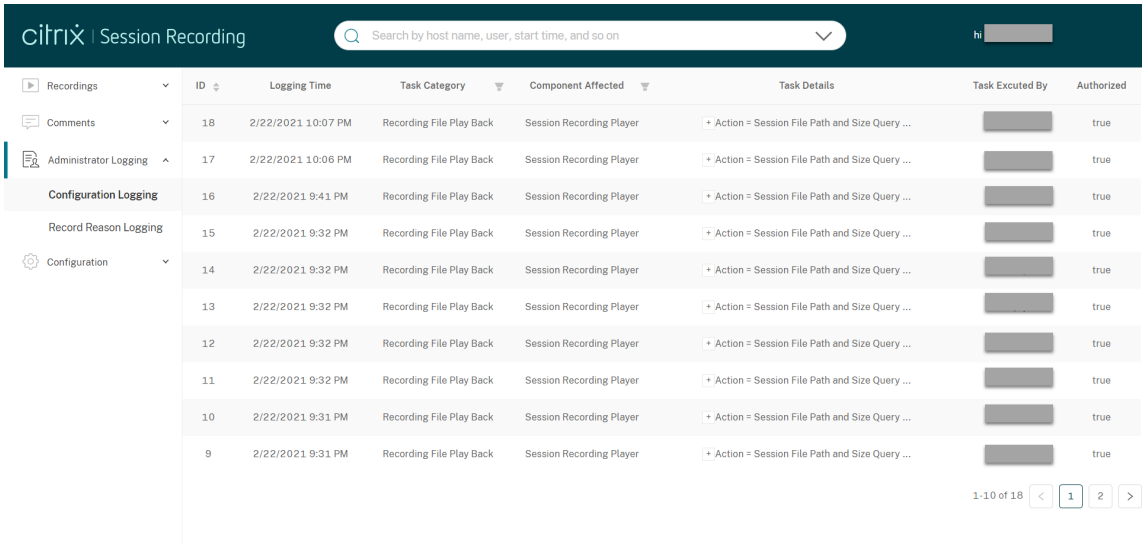
手順

サーバーをホストするマシンと他のマシンの両方から、Session Recording サーバーに関する管理者ログデータを照会できます:

対象の **Session Recording** サーバーをホストしているマシン上で

1. ［スタート］ボタンをクリックし、［**Session Recording** 管理者ログ］を選択します。
2. **LoggingReader** ユーザーの資格情報を入力します。

   Web Player と統合された管理者ログの Web ページが表示されます。

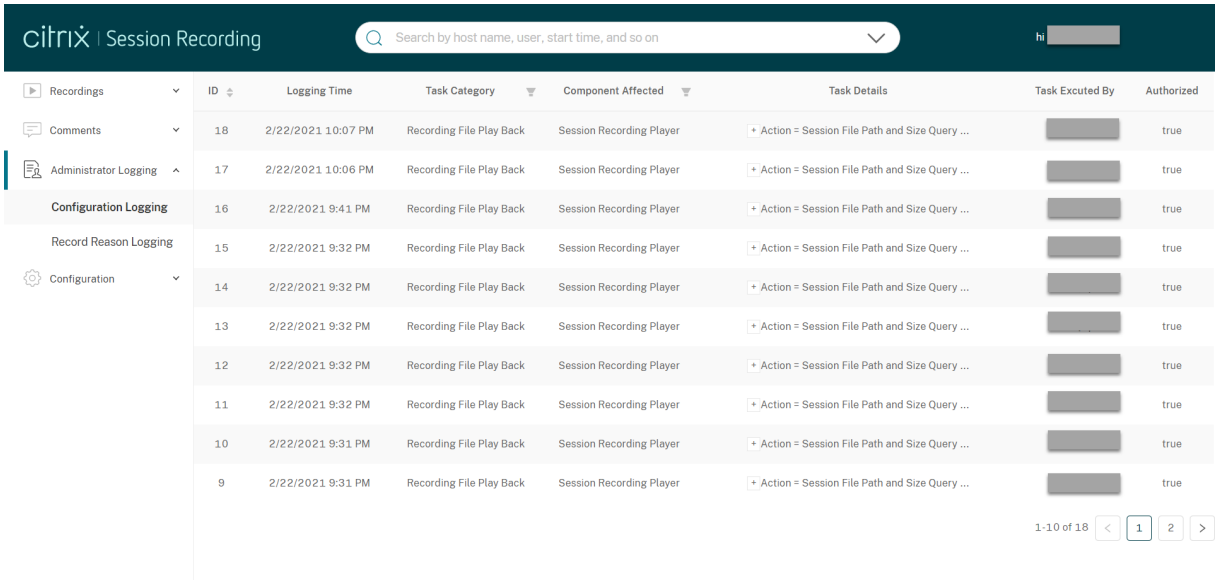


他のマシン上で

1. Web ブラウザーを開いて、管理者ログの Web ページにアクセスします。
   - **HTTPS** で接続する場合: `https://servername/WebPlayer/#/logging/config` `https://servername/WebPlayer/#/logging/record`(ここで、`servername`は Session Recording サーバーをホストするマシンの名前です)
   - **HTTP** で接続する場合: `http://servername/WebPlayer/#/logging/config` `http://servername/WebPlayer/#/logging/record`(ここで、`servername`は Session Recording サーバーをホストするマシンの名前です)
2. **LoggingReader** ユーザーの資格情報を入力します。

ログデータの概要

管理者ログデータは、構成ログと録画の理由のログの 2 つの部分で構成されます。



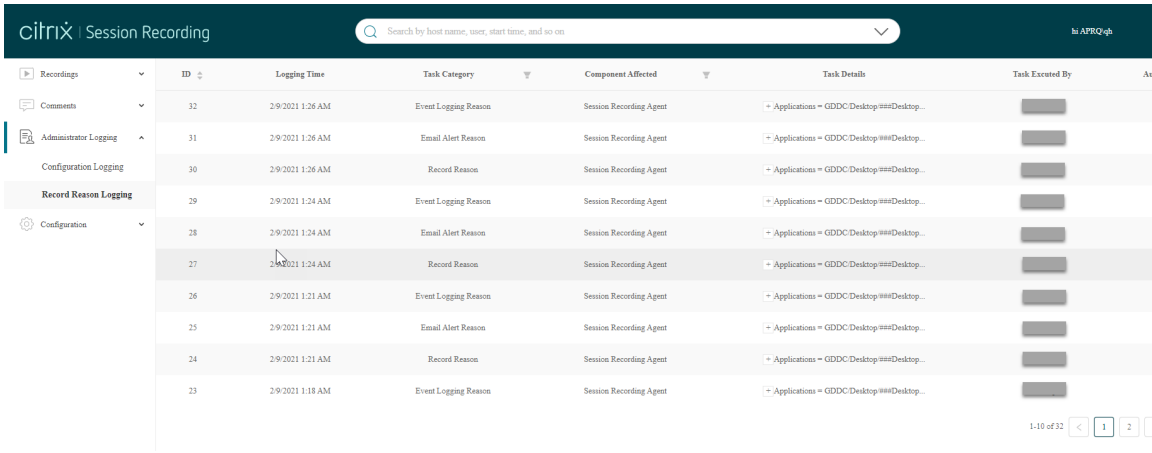
構成ログ

この部分は、次の管理者アクティビティをログに記録します:

- ポリシードキュメントの変更 - Session Recording ポリシーコンソールまたは Citrix Director でのポリシーへの変更
- サーバー設定の変更 - Session Recording サーバーのプロパティにおける変更
- 録画ファイルの再生 - 録画されたセッションの再生
- ログの読み取り - 権限のない管理者ログサービスへのアクセス試行

管理者アクティビティをログに記録するには、Session Recording サーバーで管理者ログを有効にします。詳しくは、「管理者ログの無効化または有効化」を参照してください。セキュリティを強化するために、管理者ログサービスアカウントを構成することもできます。

> ヒント:
>
> 管理者ログは、Session Recording サービスと Session Recording サーバーのプロパティの両方で有効にできます。



録画の理由のログ

この部分は、どのポリシーが録画をトリガーしたかをログに記録します。

この機能を有効にするには、Session Recording サーバーで管理者ログと録画の理由のログの両方を有効にします。管理者ログが無効になっている場合、録画の理由のログを有効にしても効果はありません。

管理者ログの無効化または有効化

インストール後、［**Session Recording** サーバーのプロパティ］で Session Recording 管理者ログ機能を無効または有効にできます。

1. Session Recording 管理者ログがインストールされているマシンに管理者としてログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording** サーバーのプロパティ］を選択します。
3. ［ログ］タブをクリックします。

Session Recording 管理者ログを無効にすると、新しいアクティビティはログに記録されません。既存のログを Web ベースの UI から照会できます。

［必須のブロック機能を有効にする］がオンの場合、ログが失敗すると以下のアクティビティがブロックされます。システムイベントもイベント ID 6001 でログに記録されます:

- Session Recording ポリシーコンソールまたは Citrix Director での録画ポリシーへの変更。
- Session Recording サーバーのプロパティにおける変更。

セッションの録画は必須のブロック設定による影響を受けません。

管理者ログサービスアカウントの構成

デフォルトでは、管理者ログはインターネットインフォメーションサービス（IIS）の Web アプリケーションとして実行されており、ID は Network Service です。セキュリティレベルを拡張するために、この Web アプリケーションの ID をサービスアカウントまたは特定のドメインアカウントに変更できます。

1. Session Recording サーバーをホストするマシンに管理者としてログオンします。

2. IIS マネージャーで、［アプリケーションプール］をクリックします。
3. ［アプリケーションプール］で、**SessionRecordingLoggingAppPool** を右クリックして ［詳細設定］を選択します。
4. 属性 **ID** を、使用する特定のアカウントに変更します。
5. **db_owner** 権限を、Microsoft SQL Server のデータベース **CitrixSessionRecordingLogging** のアカウントに付与します。
6. レジストリキー **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server** の読み取り権限をアカウントに付与します。

> 警告:
>
> 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、オペレーティングシステム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、シトリックス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。

録画の理由のログの無効化または有効化

デフォルトで、管理者ログではポリシークエリ完了後のすべての録画の理由がログに記録されます。この場合、大量のログが生成される可能性があります。パフォーマンスを向上させてストレージを確保するには、レジストリでこの種類のログを無効にします。

1. Session Recording サーバーをホストするマシンに管理者としてログオンします。
2. レジストリエディターを開きます。
3. **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server** に移動します。
4. **EnableRecordingActionLogging** の値として、以下を設定します:

   0: 録画の理由のログの無効化
   1: 録画の理由のログの有効化

ベストプラクティス

December 22, 2022

Session Recording の展開と負荷分散の構成については、次のベストプラクティスのドキュメントを参照してください:

- 既存の環境での負荷分散の構成
- Azure で Session Recording を展開して負荷分散する

既存の環境での負荷分散の構成

February 20, 2024

既存の Session Recording 環境で Citrix ADC を使用して負荷分散ノードを追加できます。例として、次のサーバーを使用します。Azure で Session Recording を展開して負荷分散することもできます。

- Session Recording

ホスト名	サーバーの役割	OS	IP アドレス
SRServer1	Session Recording サーバー	Windows Server	10.63.32.55
LBDC	ドメインコントローラー	Windows Server	10.63.32.82
TSVDA	Session Recording Agent	Windows Server	10.63.32.215
SRSQL	Session Recording データベースとファイルサーバー	Windows Server	10.63.32.91

すべての Session Recording コンポーネントとドメインコントローラーは、`lb.com`などのドメインを共有します。たとえば、ドメイン管理者アカウントの「lb\administrator」は サーバーログオン時に使用します。

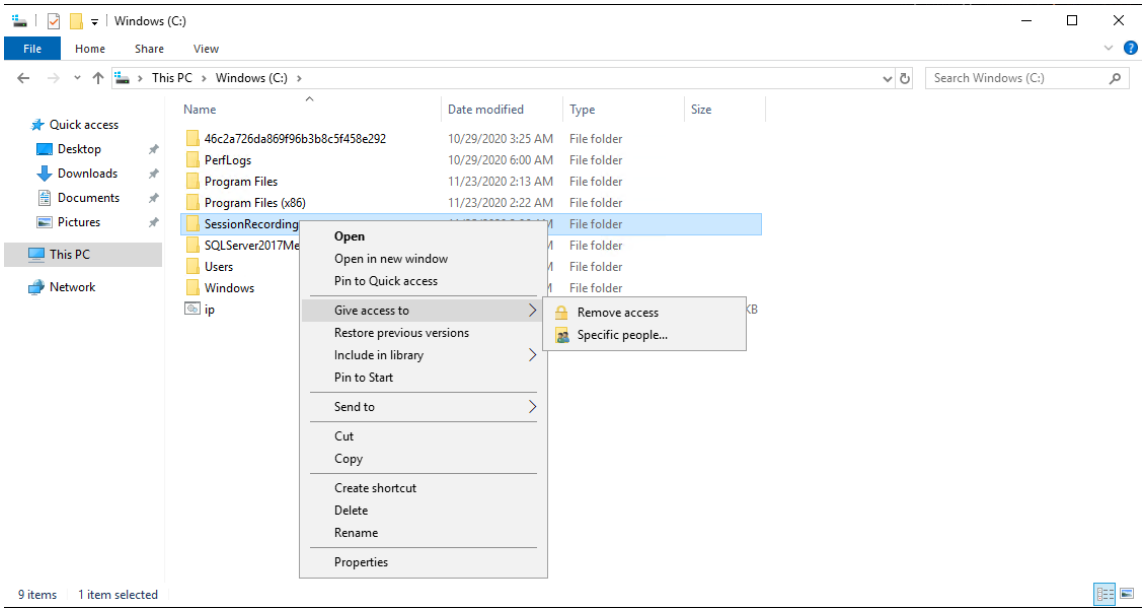
- Citrix ADC

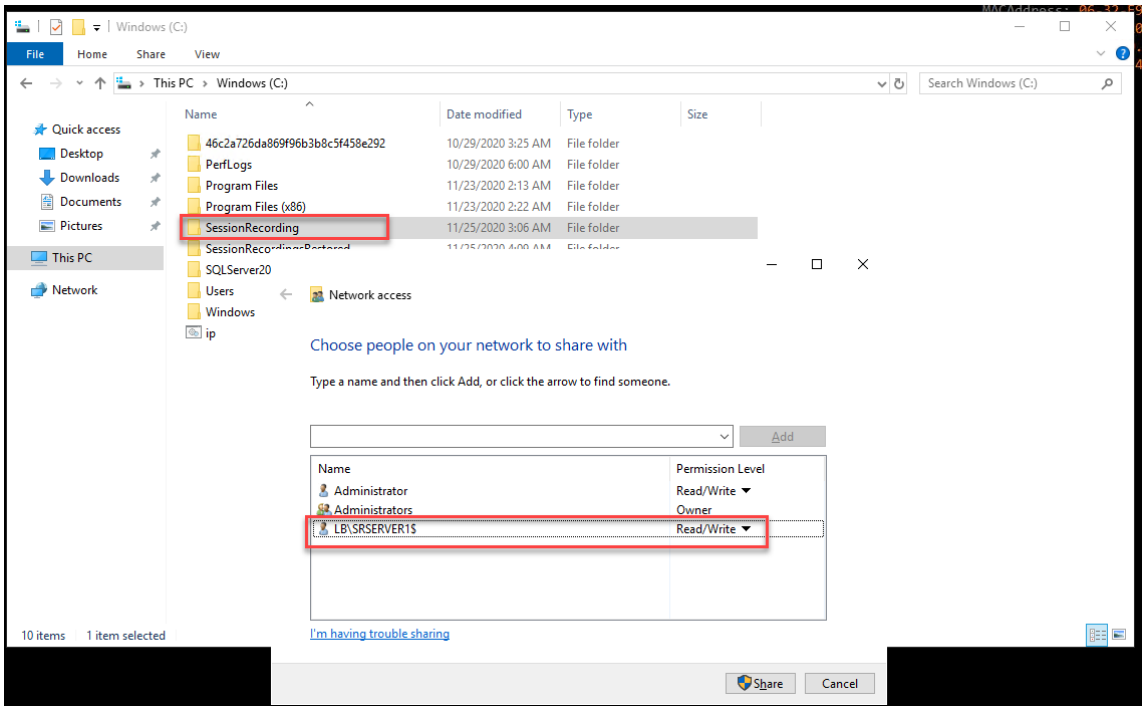
ホスト名	サーバーの役割	管理 IP アドレス（NSIP）	サブネット IP アドレス（SNIP）
NetScaler	Citrix ADC VPX インスタンス	10.63.32.40	10.63.32.109

詳しくは、「Citrix ADC VPX インスタンスを展開する」を参照してください。

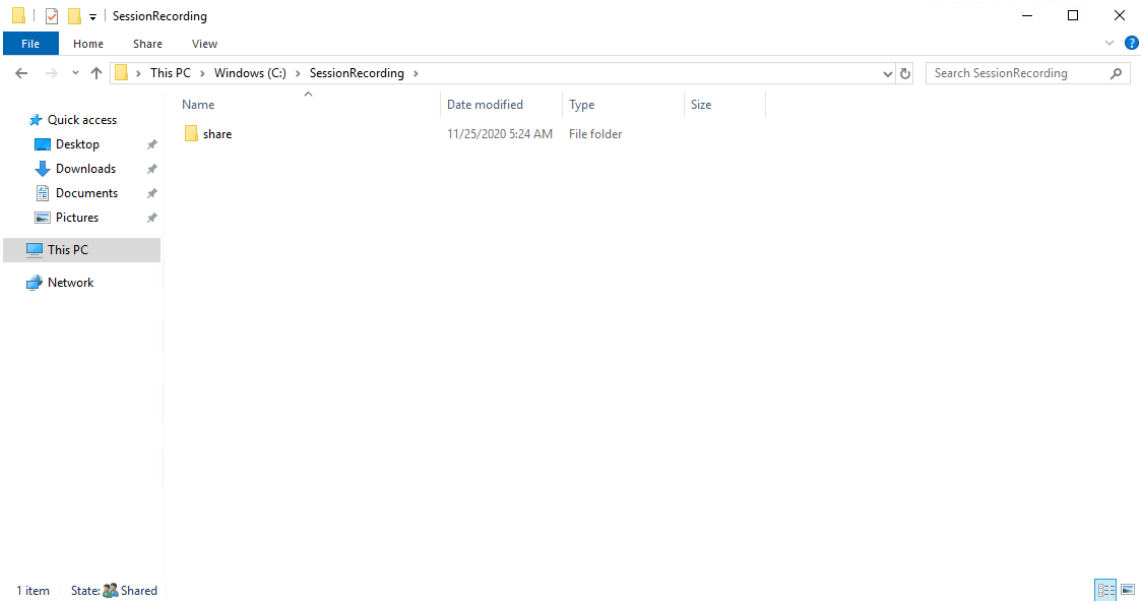
手順 **1**：ファイルサーバーに共有フォルダーを作成する

1. ドメイン管理者アカウント（例：`lb\administrator`）を使用してファイルサーバーにログオンします。
2. 録画を格納するフォルダーを作成し、`SessionRecording`という名前を付けます（例：`C:\SessionRecording`）フォルダーの読み取り/書き込み権限を Session Recording サーバーと共有します。例として`SRServer1`を使用し、「`LB\SRSERVER1$`」と入力します。ドル記号`$`は必要です。





3. SessionRecordingフォルダー内にサブフォルダーを作成し、shareという名前を付けます（例: C:\SessionRecording\share）。

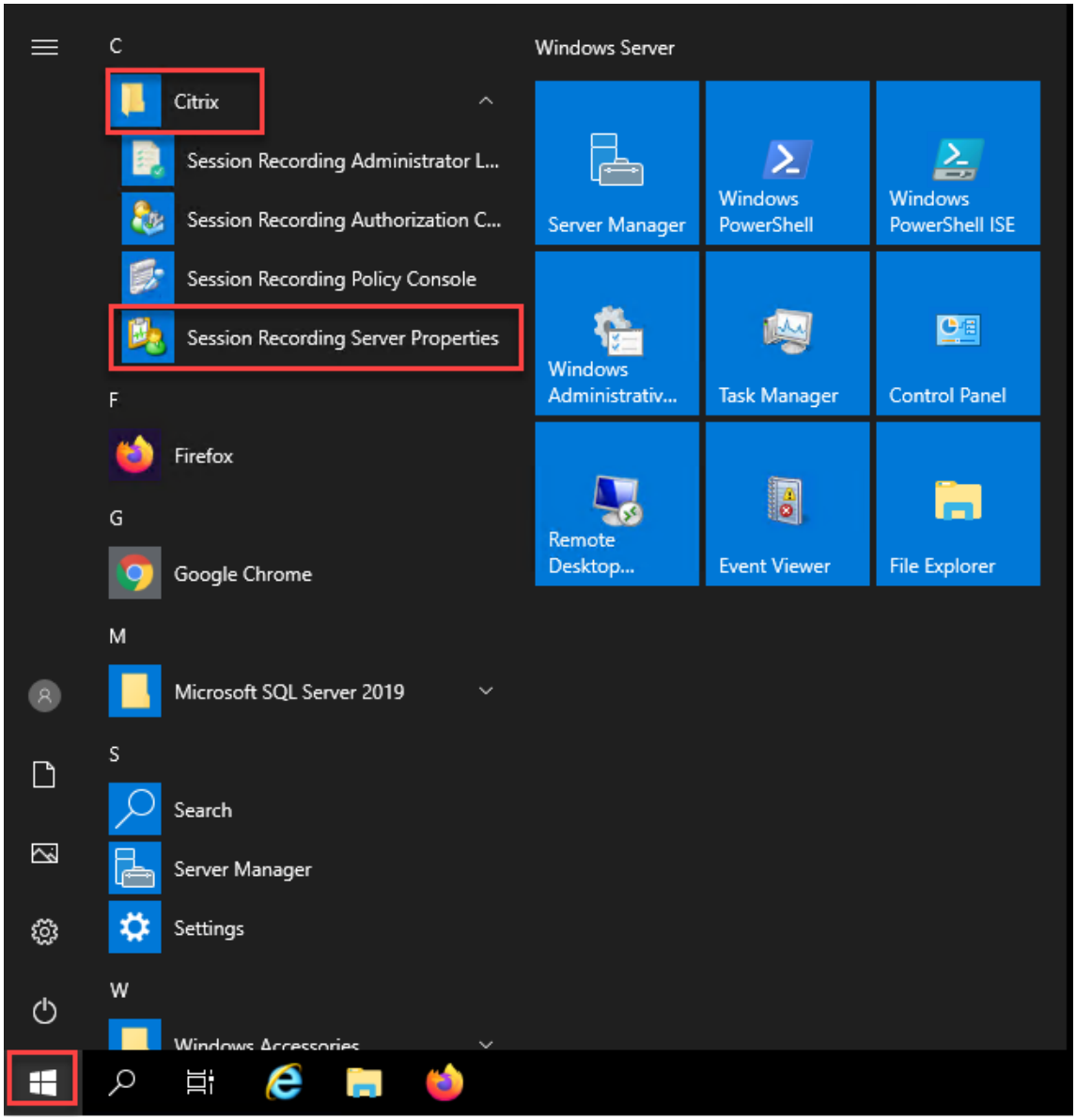


4. アーカイブされた録画を復元する別のフォルダーを作成し、SessionRecordingsRestoredという名前を付けます（例：C:\ SessionRecordingsRestored）。フォルダーの読み取り/書き込み権限を Session Recording サーバーと共有します。例としてSRServer1を使用し、「LB\SRSERVER1$」と入力します。ドル記号$は必要です。
5. SessionRecordingsRestoredフォルダー内にサブフォルダーを作成し、shareという名前を付けます（例：C:\SessionRecordingsRestored\share）。

手順 **2**：負荷分散をサポートするように既存の **Session Recording** サーバーを構成する

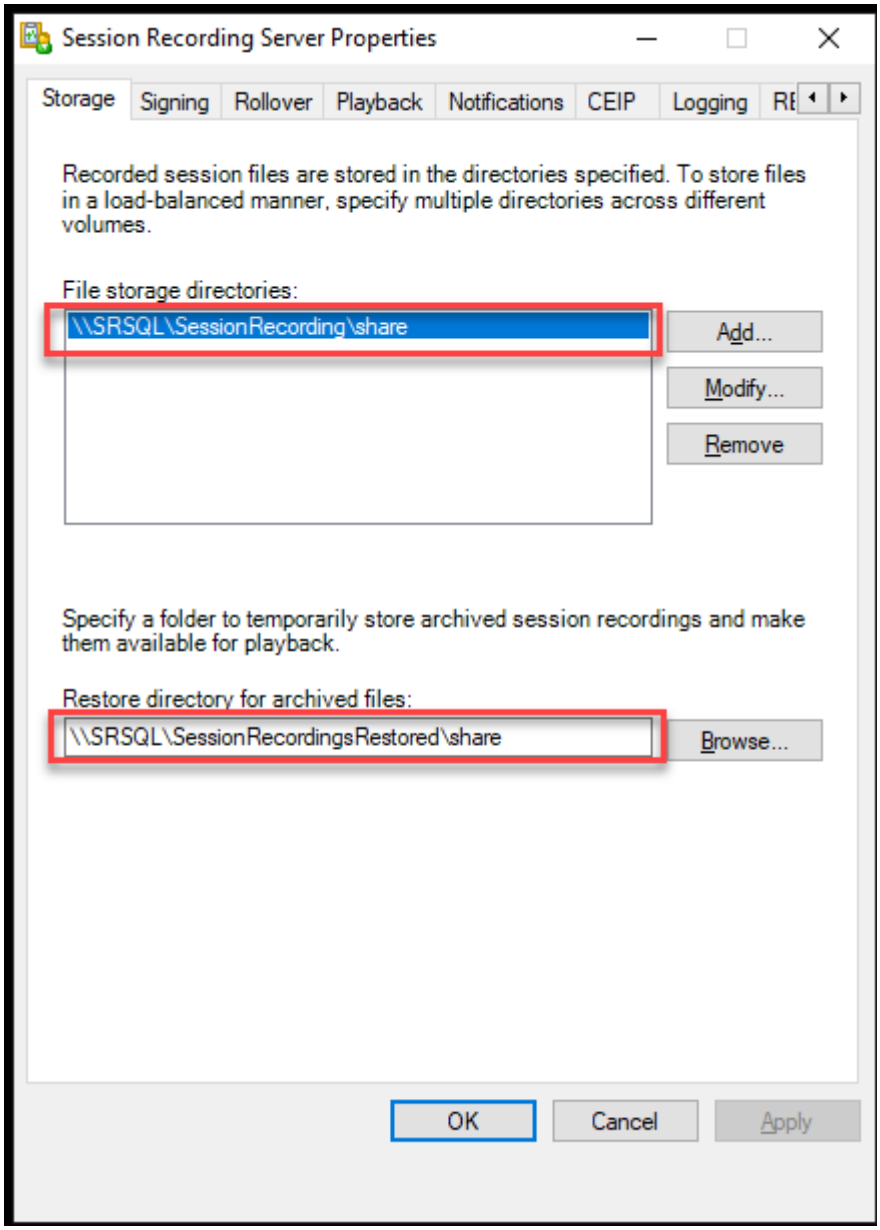
この手順では、負荷分散をサポートするように既存の Session Recording サーバーを構成する方法について説明します。手順 7では、既存の環境に Session Recording サーバーを追加する手順について詳しく説明します。

1. ドメイン管理者アカウントを使用して、Session Recording サーバーにログオンします。
2. [**Session Recording** サーバーのプロパティ] を開きます。



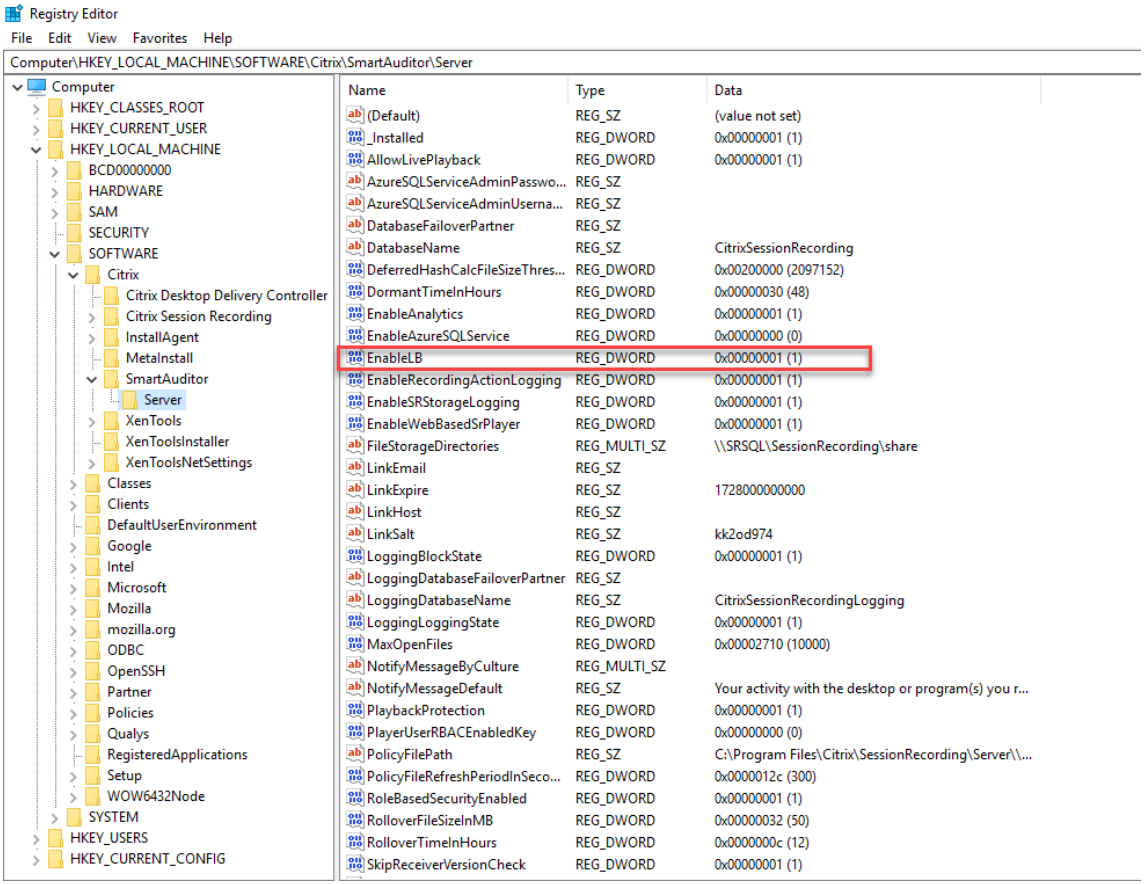
3. 録画ファイルを格納および復元するための、手順 1で作成した UNC（Universal Naming Convention：汎用名前付け規則）パスを追加します（この例では `\\SRSQL\SessionRecording\share`および`\\SRSQL\SessionRecordingRestored\share`）。`SRSQL`はファイルサーバーのホスト名です。

> 注:
>
> Session Recording Player は、ドライブ文字またはドル記号（$）を含むパスでファイルを再生できません。Session Recording Player と Session Recording サーバーを同じマシンにインストールする場合は例外です。



4. HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server で Session Recording サーバーのレジストリキーに値を追加します。

   値の名前：EnableLB
   値のデータ：1（D_WORD、つまり「有効」）



5. Citrix Session Recording ストレージマネージャーサービスを再起動します。

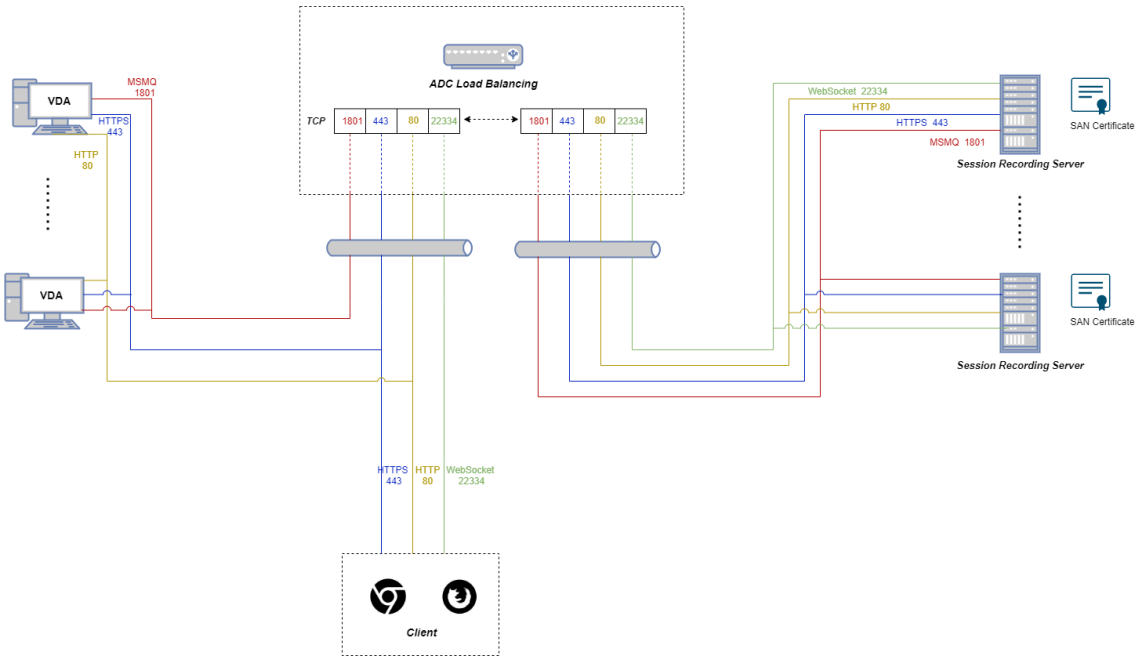
手順 **3**：**Citrix ADC** で負荷分散を構成する

Citrix ADC で負荷分散を構成する方法は 2 つあります。TCP パススルーと SSL オフロードです。

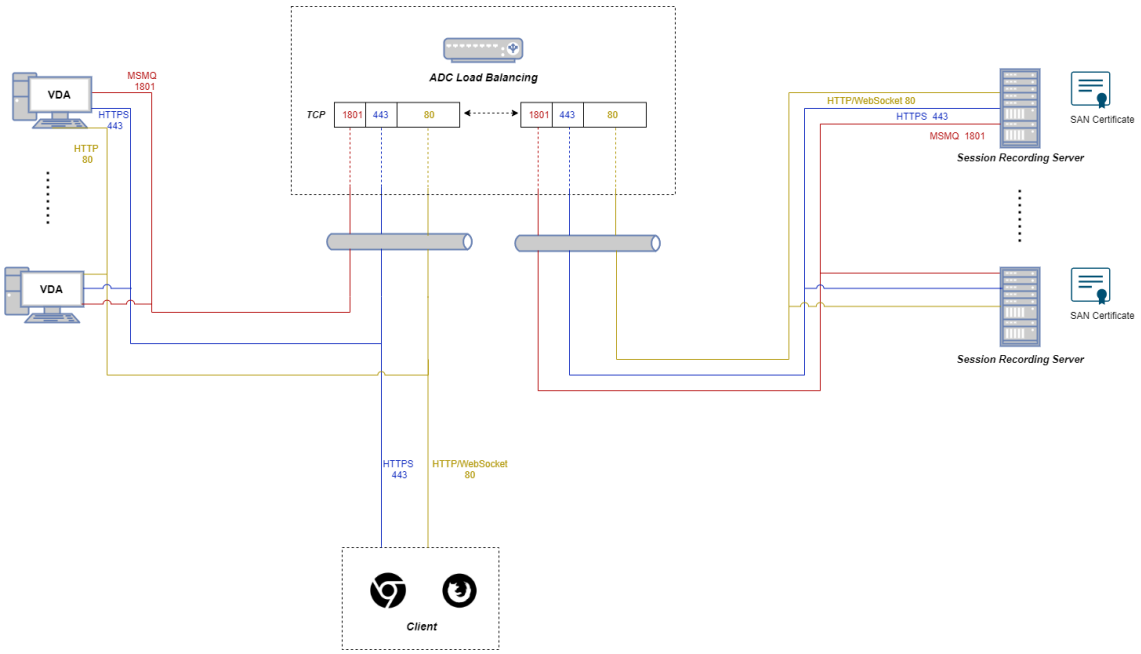
TCP パススルーを介して負荷分散を構成する

次のトポロジは、**TCP** パススルーを介して負荷分散を構成する方法を示しています。

- Python ベースの WebSocket サーバー（バージョン 1.0）を使用している場合：

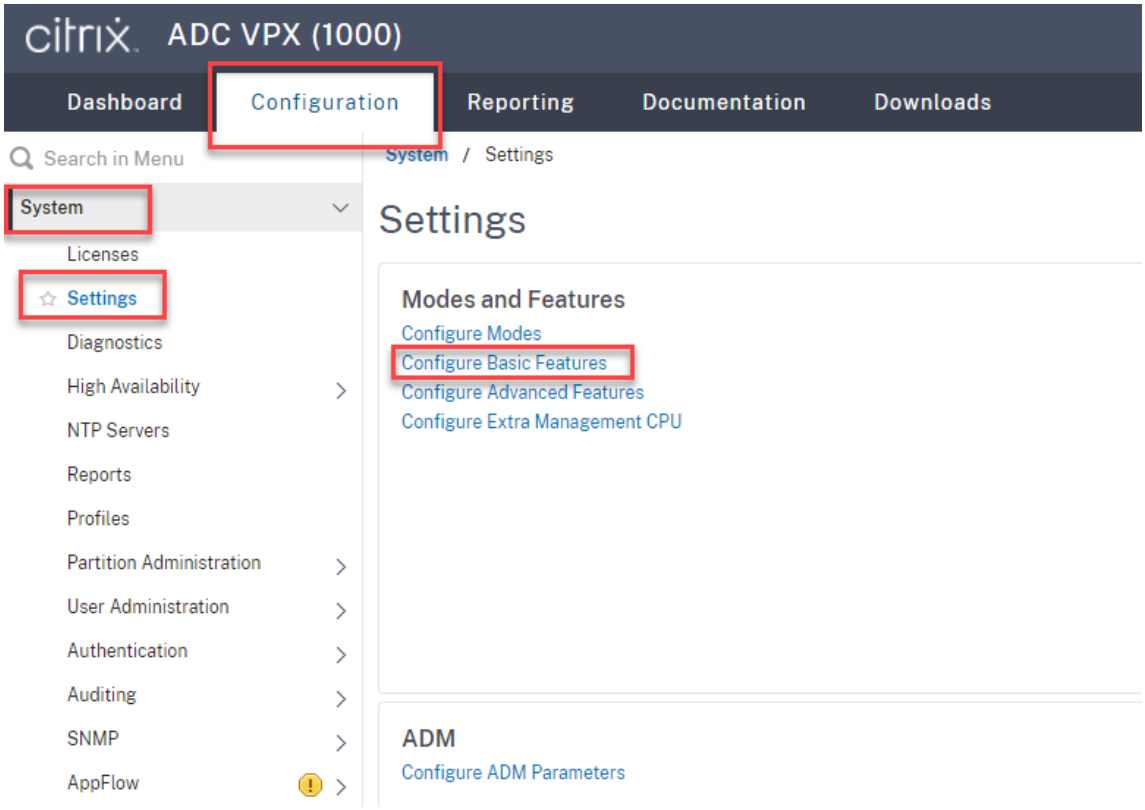


- IIS（バージョン 2.0）でホストされている WebSocket サーバーを使用している場合：

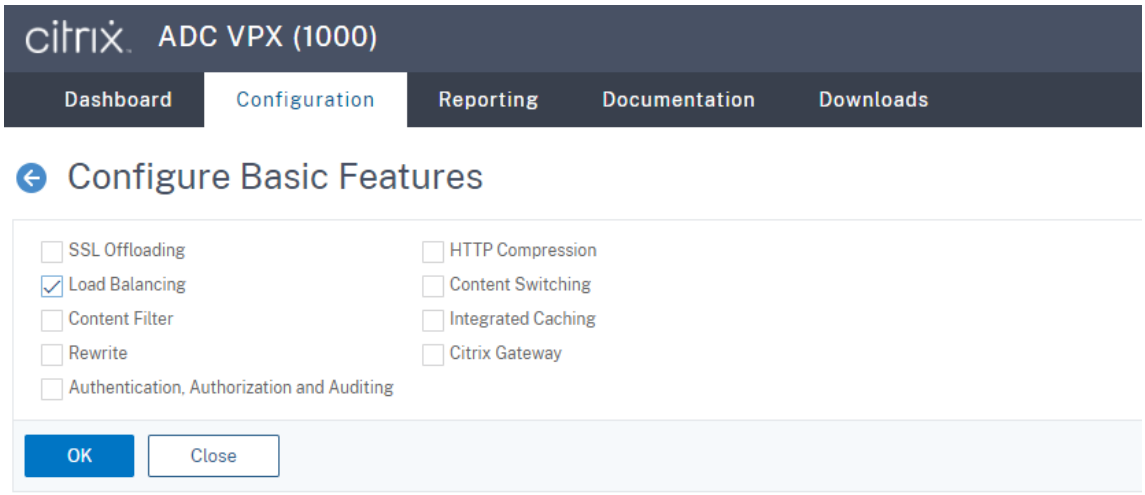


TCP パススルーを介して負荷分散を構成するには、次の手順を実行します：

1. Citrix ADC VPX インスタンスにログオンします。
2. ［**Configuration**］ > ［**System**］ > ［**Settings**］ > ［**Configure Basic Features**］の順に選択します。

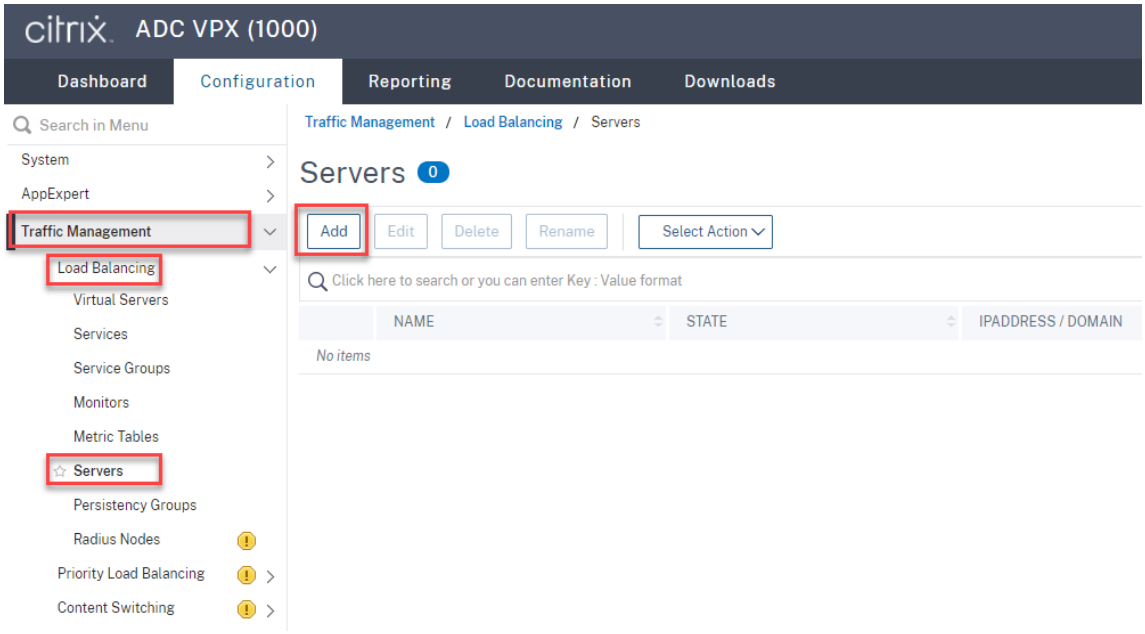


3. [**Load Balancing**] を選択し、[**OK**] をクリックします。

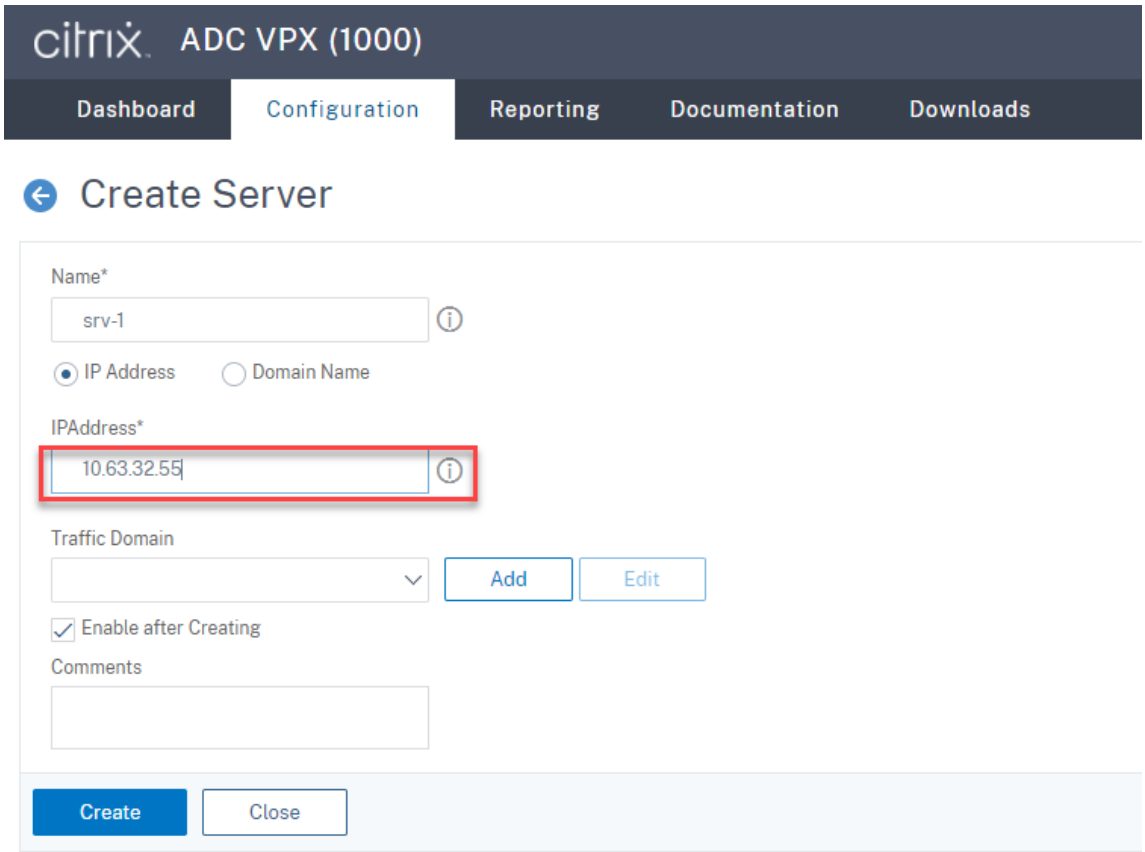


4. 負荷分散サーバーを追加します。

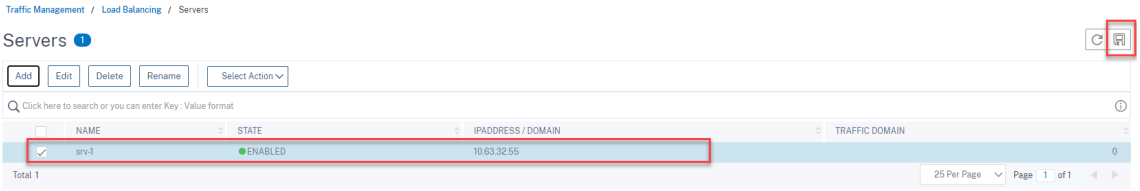
   [**Traffic Management**] > [**Load Balancing**] > [**Servers**] の順に選択し、[**Add**] をクリックします。



Session Recording サーバーの名前と IP アドレスを入力し、［**Create**］をクリックします。例:

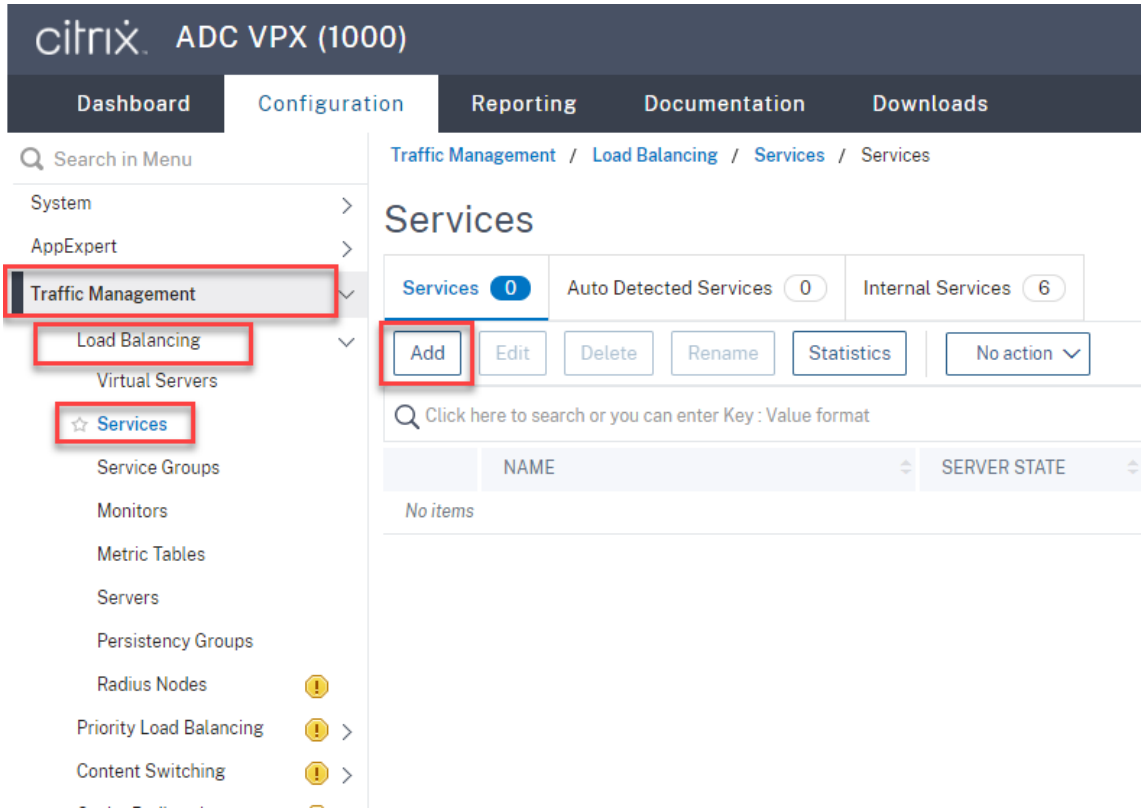


右上隅にある保存アイコンをクリックして、変更を保存します。

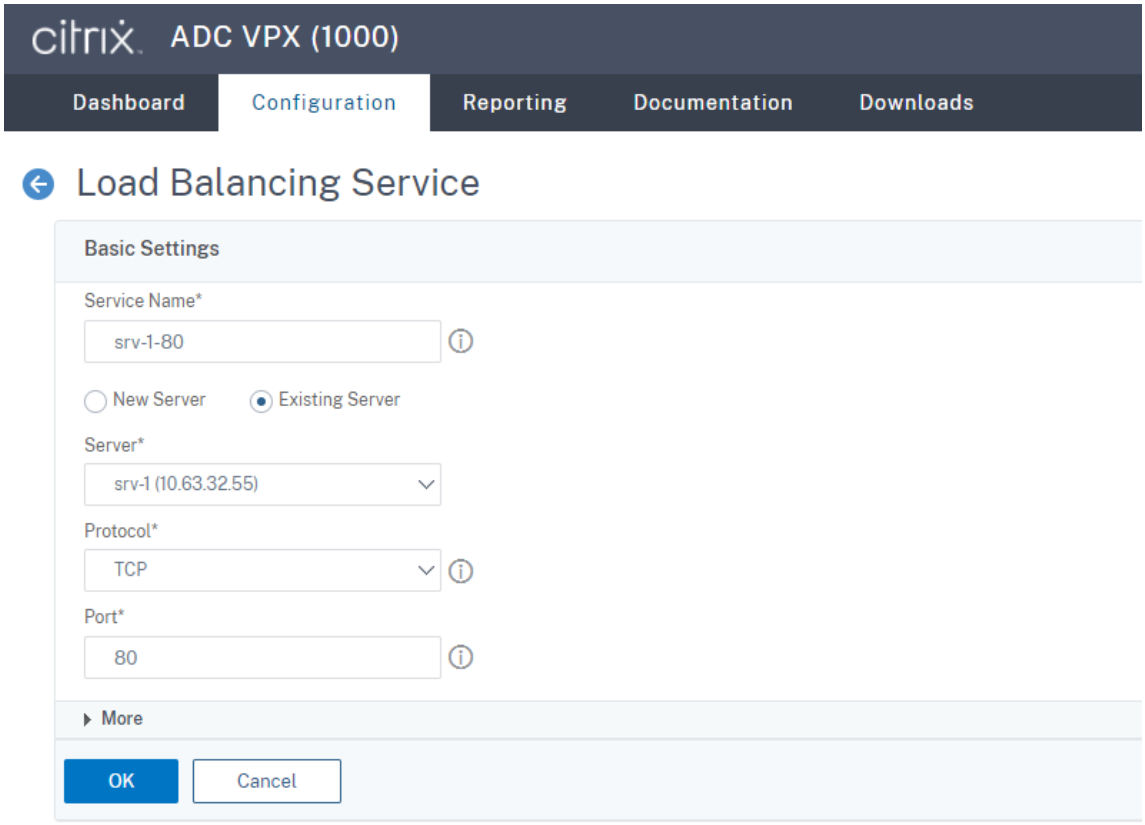


5. WebSocket サーバーバージョン 1.0 の場合、Session Recording サーバーごとにポート 80、1801、22334、443 の負荷分散サービスを追加します。WebSocket サーバーバージョン 2.0 の場合、Session Recording サーバーごとにポート 80、1801、443 の負荷分散サービスを追加します。

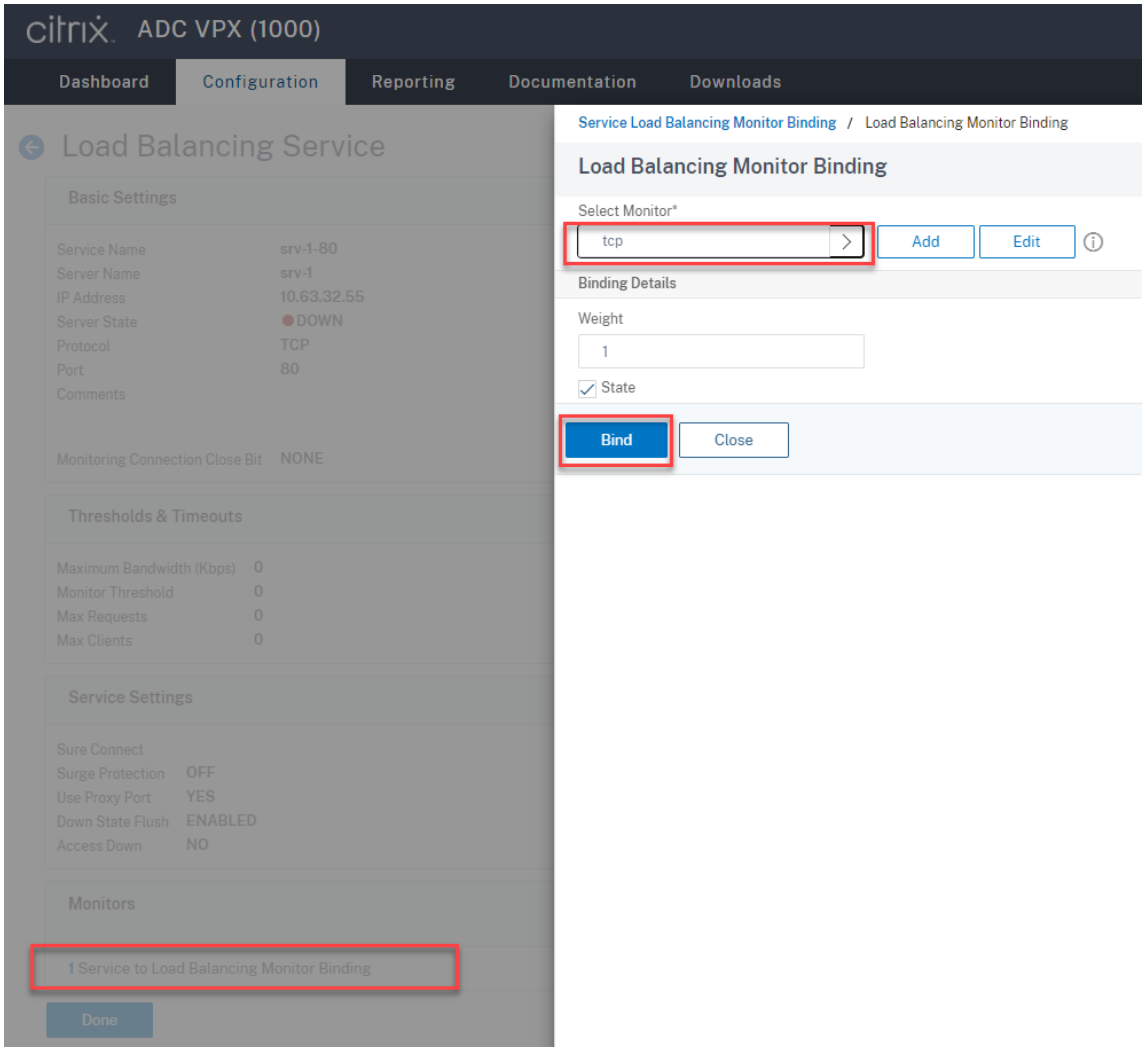
   [**Traffic Management**] > [**Load Balancing**] > [**Services**] の順に選択し、[**Add**] をクリックします。



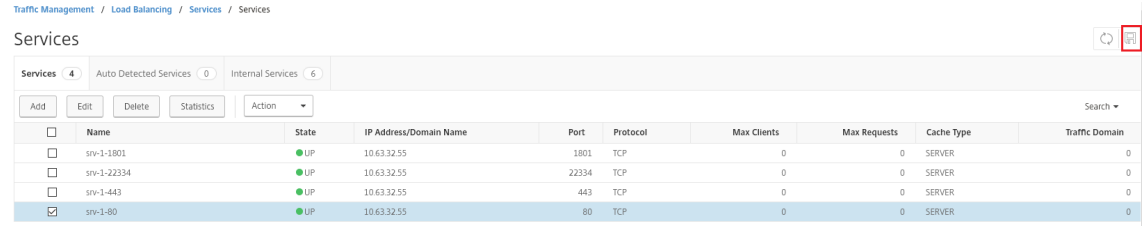
   追加する各負荷分散サービスの名前を入力します。[**Existing Server**] を選択し、ターゲットの Session Recording サーバーの IP アドレスを選択します。次に、サーバープロトコルとして [**TCP**] を選択し、ポート番号を入力します。[**OK**] をクリックします。



TCP プロトコルモニターを各負荷分散サービスにバインドします。



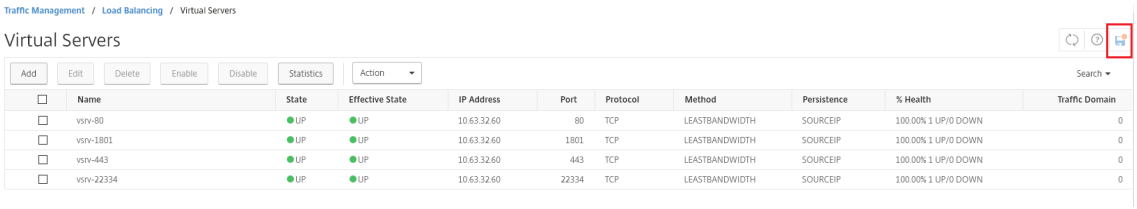
右上隅にある保存アイコンをクリックして、変更を保存します。



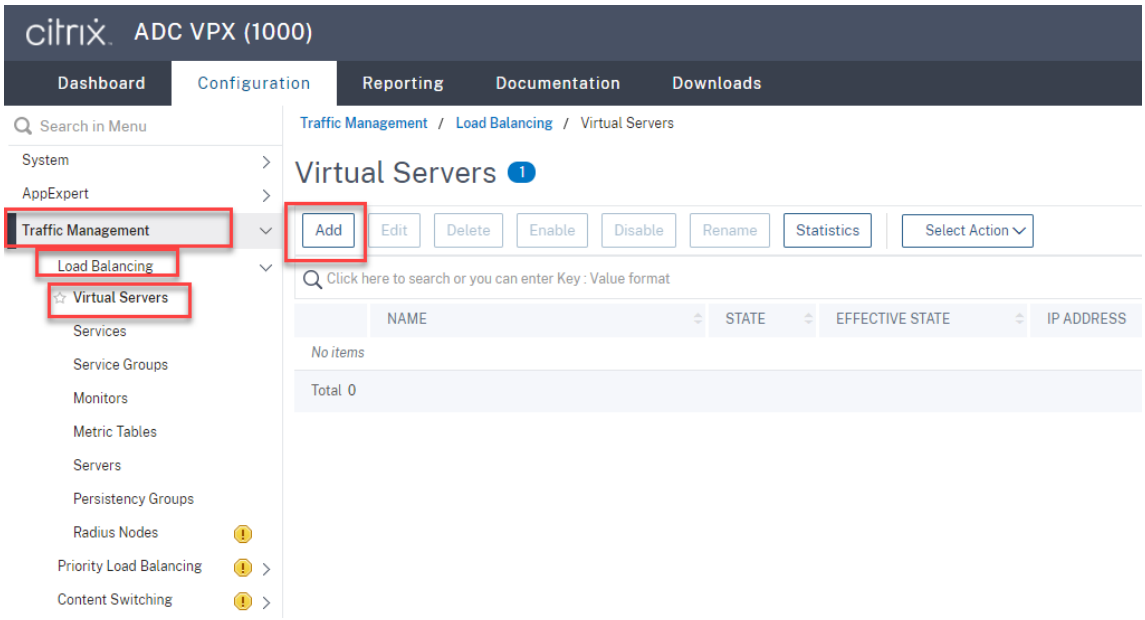
> ヒント：
>
> ポート 22334 の負荷分散サービスは、WebSocket サーバーバージョン 1.0 にのみ必要です。

6. 負荷分散仮想サーバーを追加します。

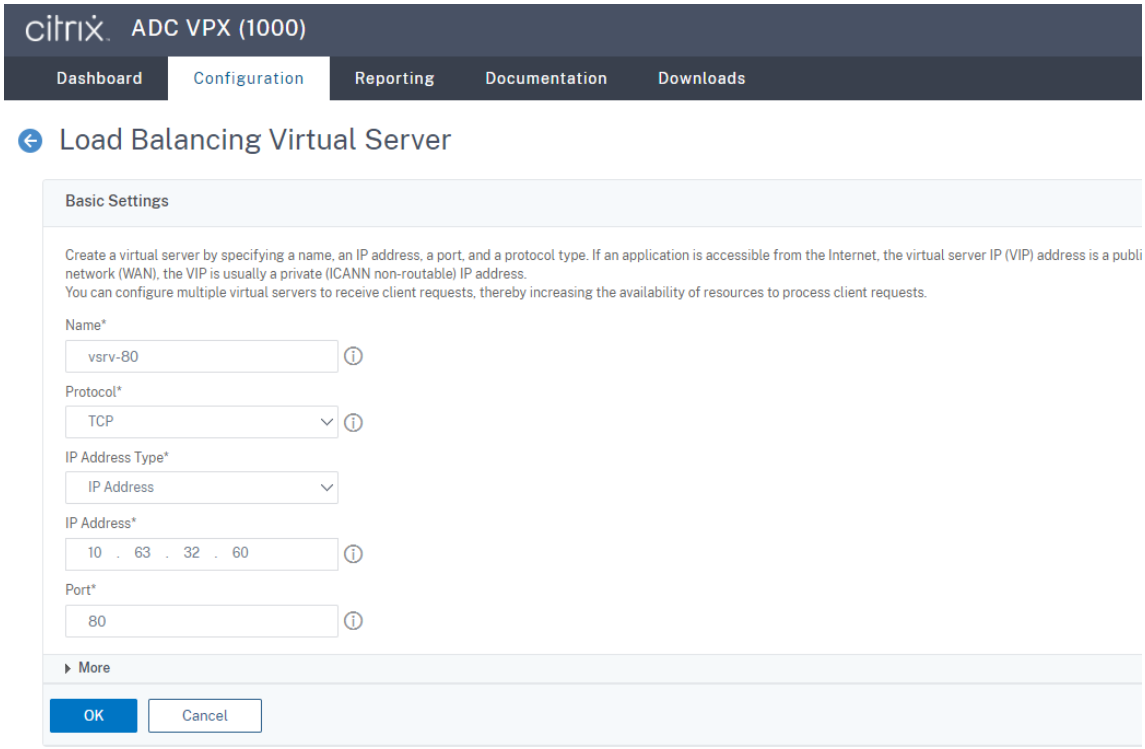
   WebSocket サーバーバージョン 1.0 の場合、次の手順を実行して、ポート 80、443、1801、22334 の負荷分散仮想サーバーを追加します。WebSocket サーバーバージョン 2.0 の場合、ポート 80、443、1801 の負荷分散仮想サーバーを追加します。例：



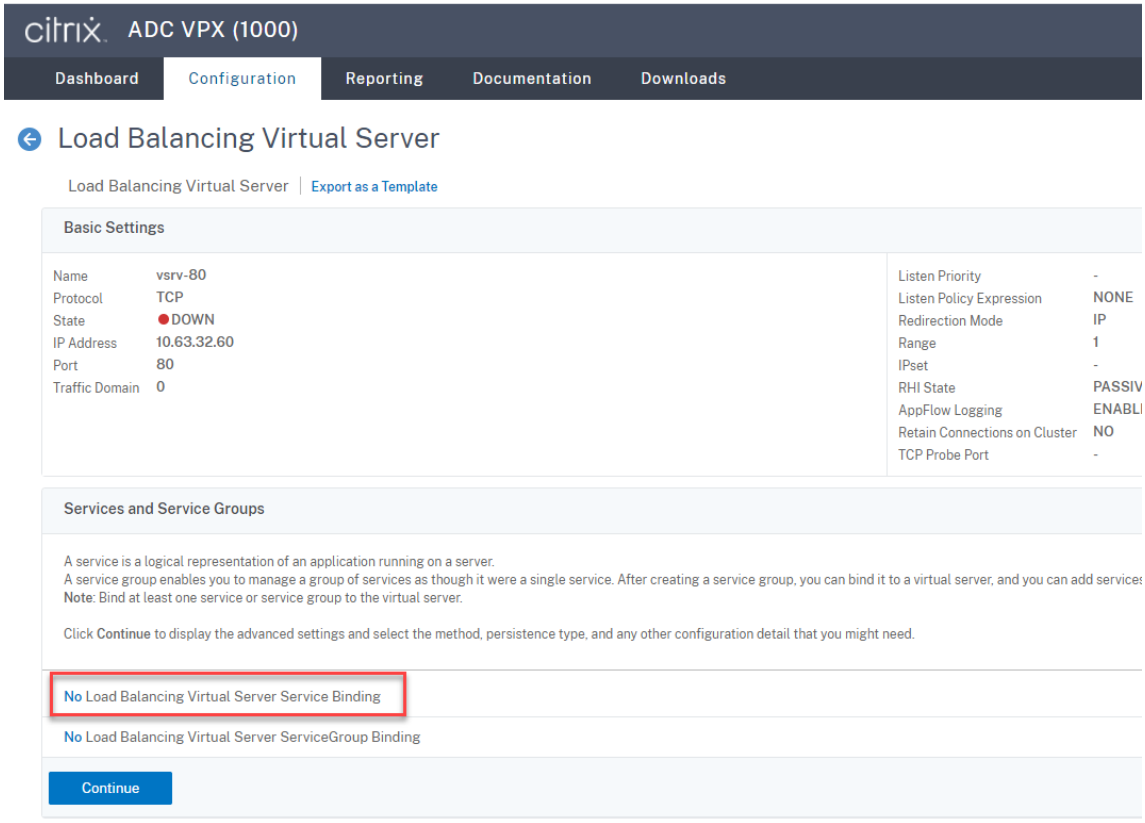
［**Traffic Management**］**>**［**Load Balancing**］**>**［**Virtual Server**］の順に選択し、［**Add**］をクリックします。

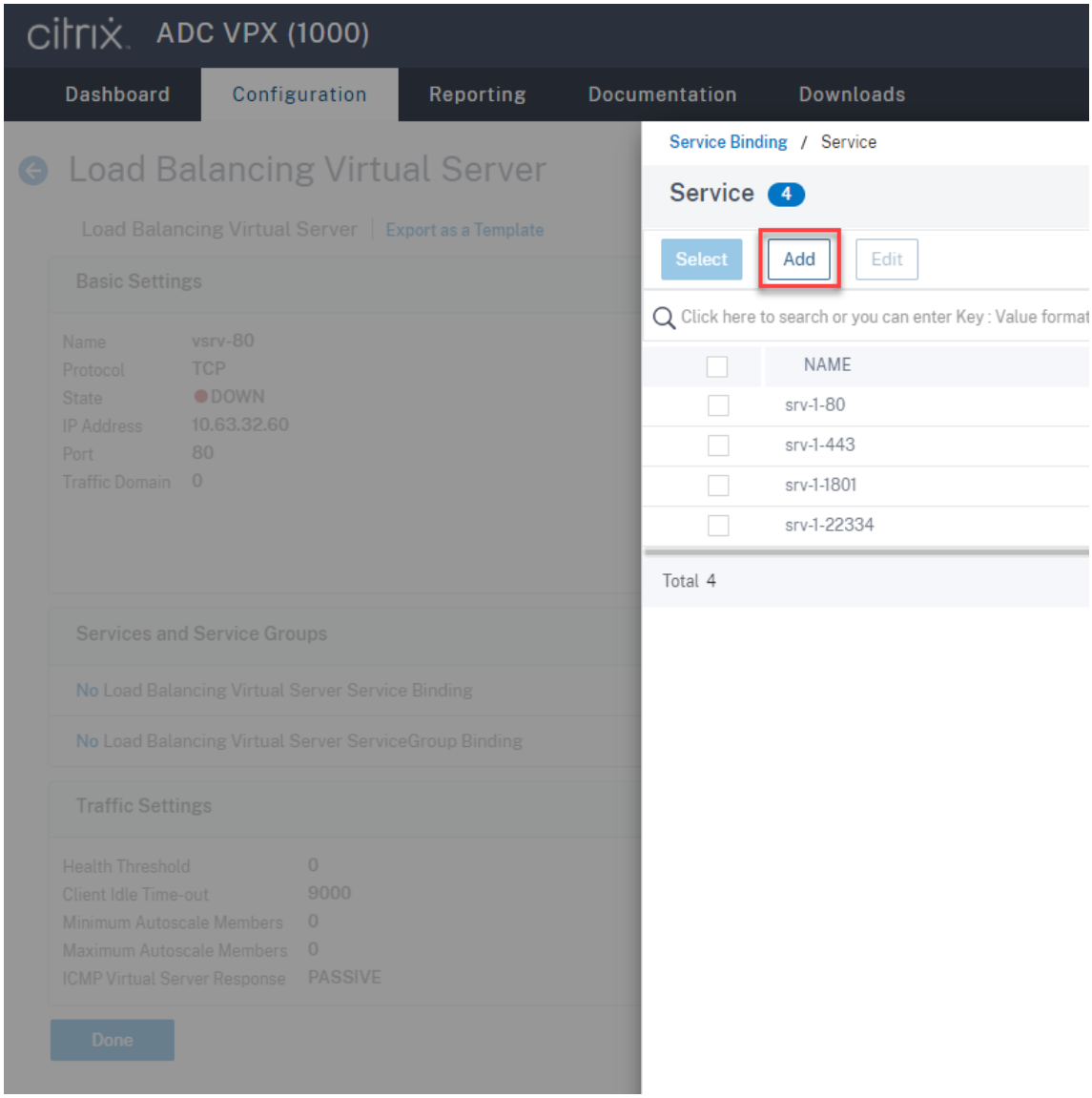


TCP プロトコルに基づいて Citrix ADC VIP アドレスで、仮想サーバーを追加します。

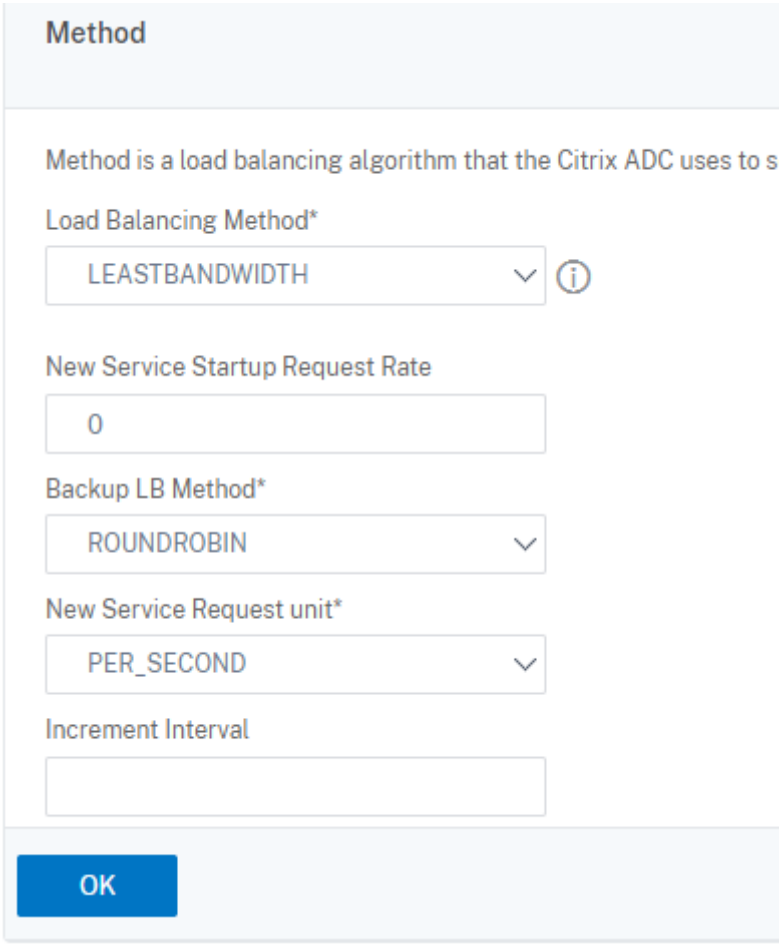


各仮想サーバーを同じポートの負荷分散サービスにバインドします。例:

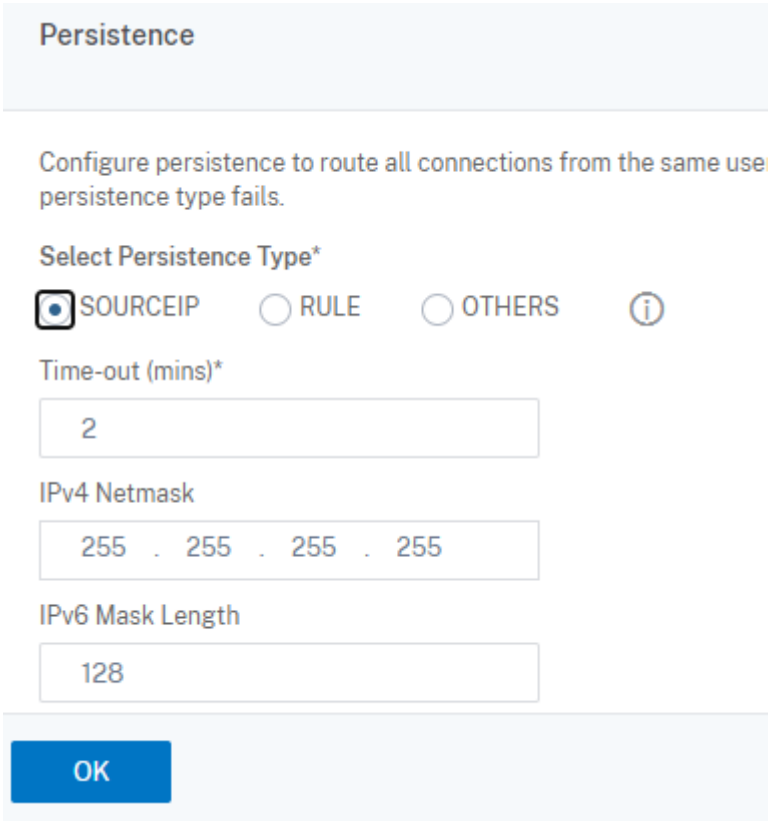




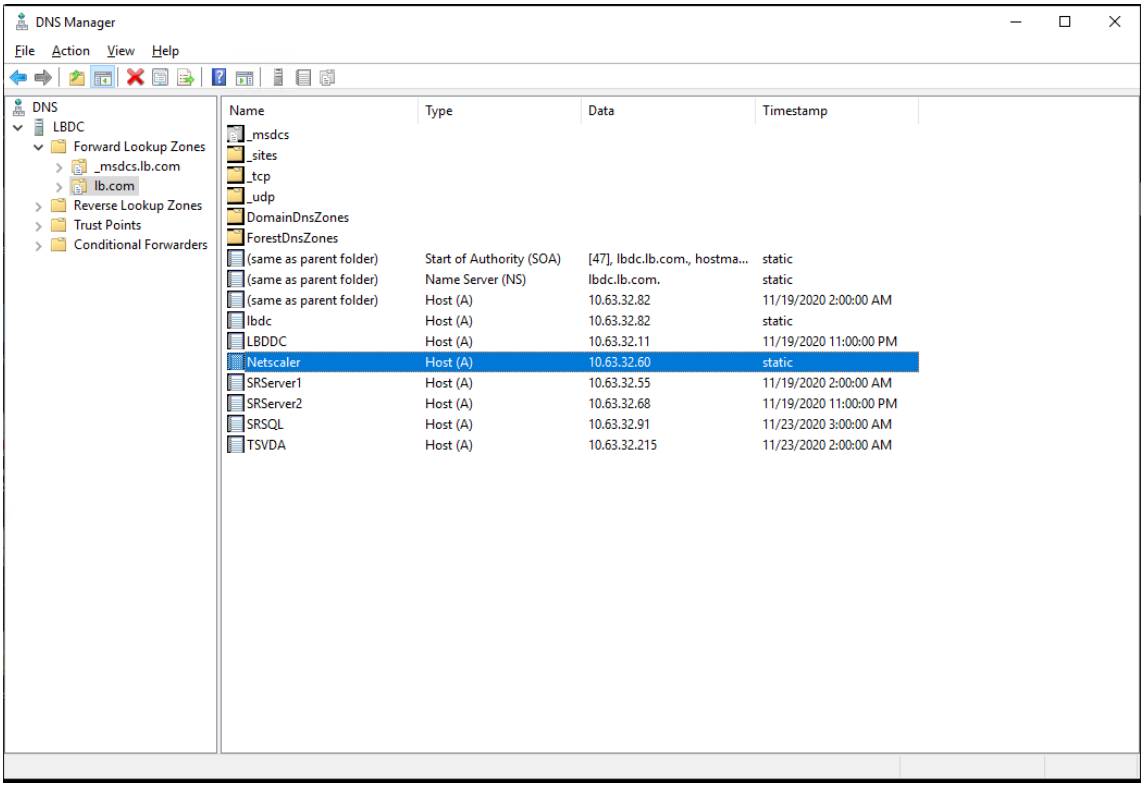
負荷分散の方法を選択します。



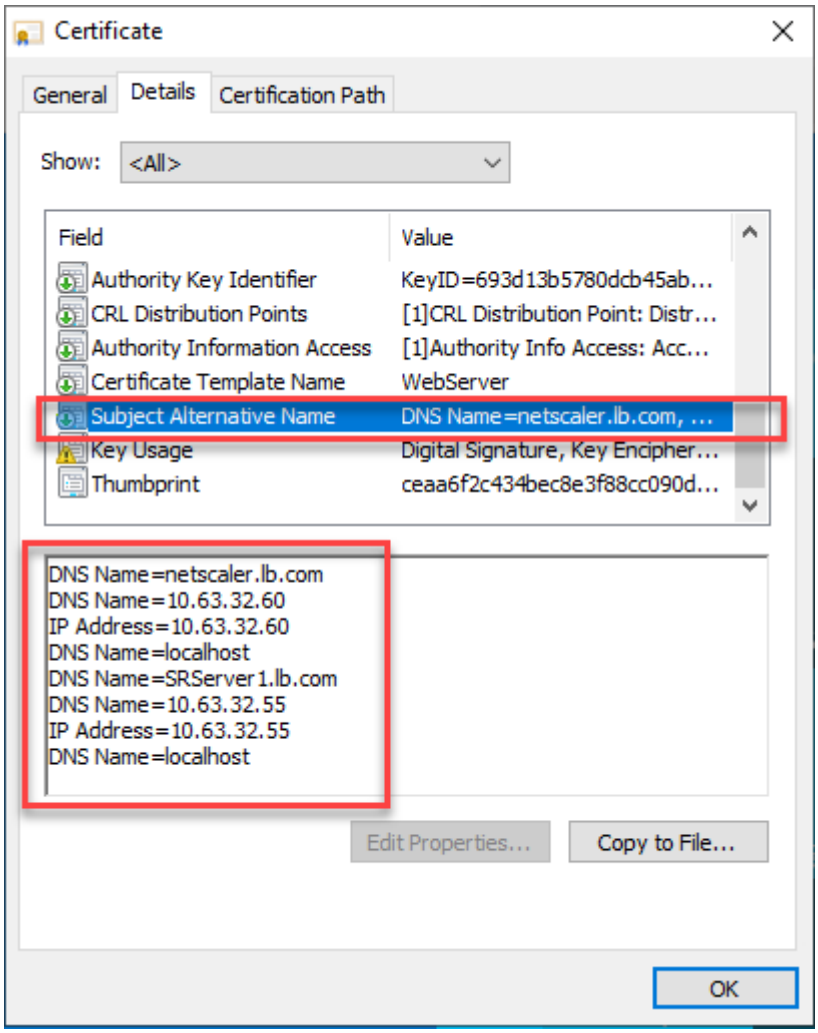
各仮想サーバーでパーシステンスを構成します。パーシステンスタイプとして **SOURCEIP** を選択することをお勧めします。詳しくは、「パーシステンスの設定」を参照してください。



7. ドメインコントローラーで Citrix ADC VIP アドレスのホストレコードを作成します。



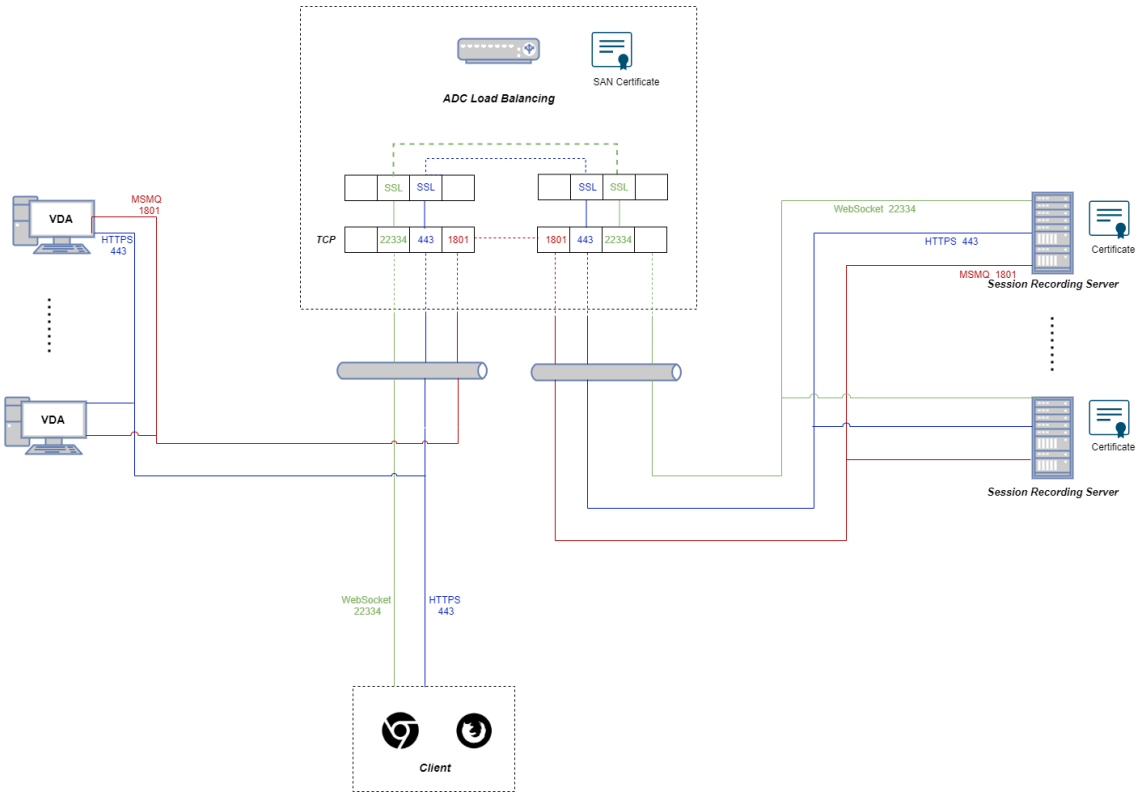
8. HTTPS 経由で Web Player にアクセスするには、Citrix ADC と各 Session Recording サーバーの両方で SAN 証明書が使用可能であることを確認してください。SAN 証明書には、Citrix ADC および各 Session Recording サーバーの完全修飾ドメイン名が含まれています。



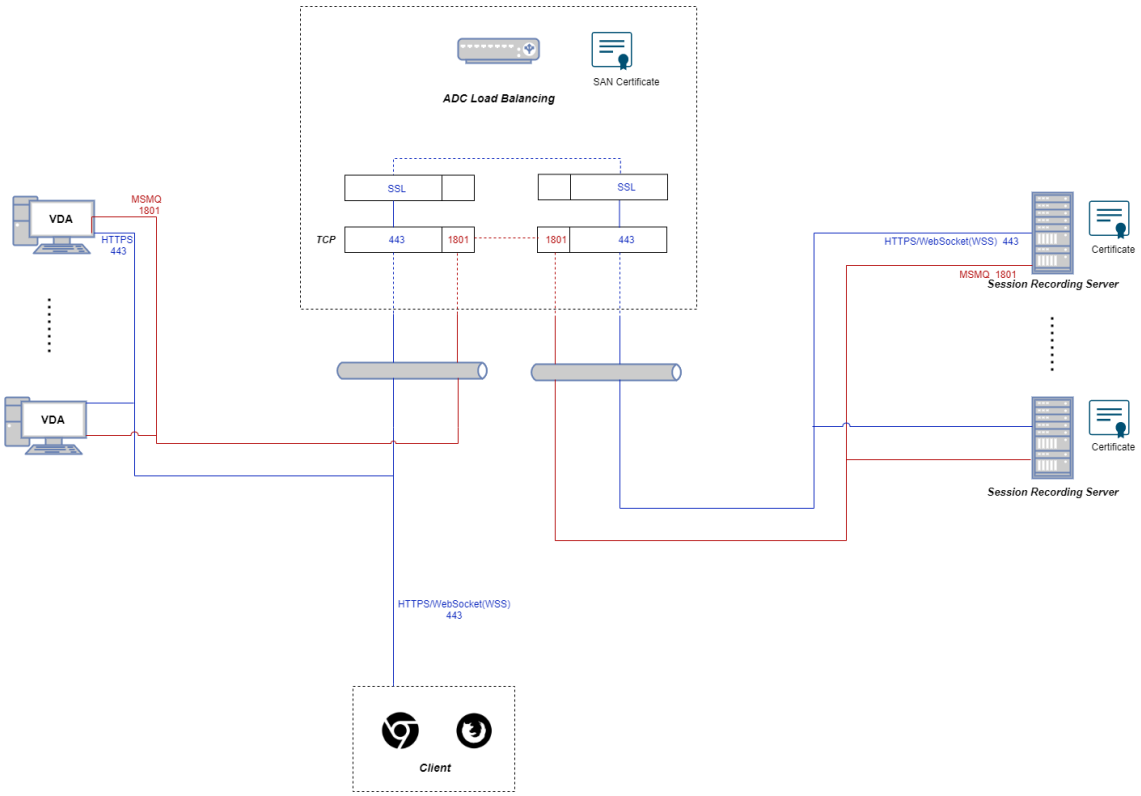
SSL オフロードで負荷分散を構成する

次のトポロジは、SSL オフロードで負荷分散を構成する方法を示しています。

- Python ベースの WebSocket サーバー（バージョン 1.0）を使用している場合:

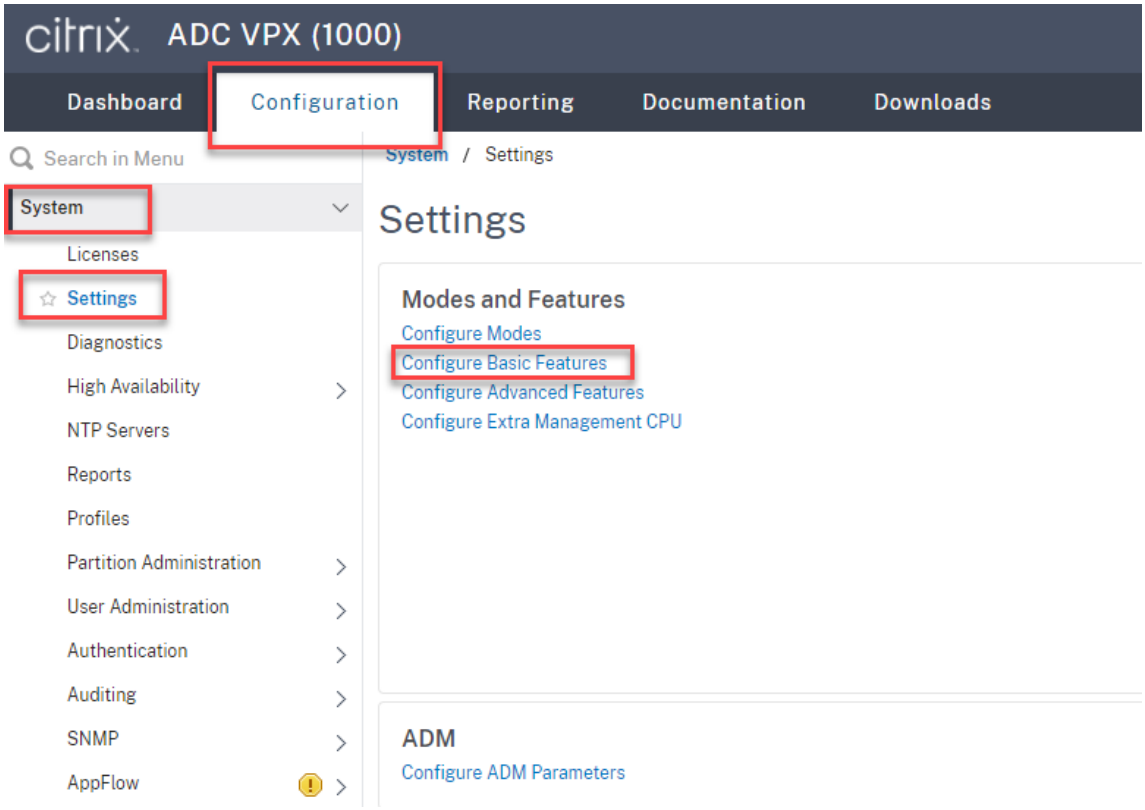


- IIS（バージョン 2.0）でホストされている WebSocket サーバーを使用している場合：

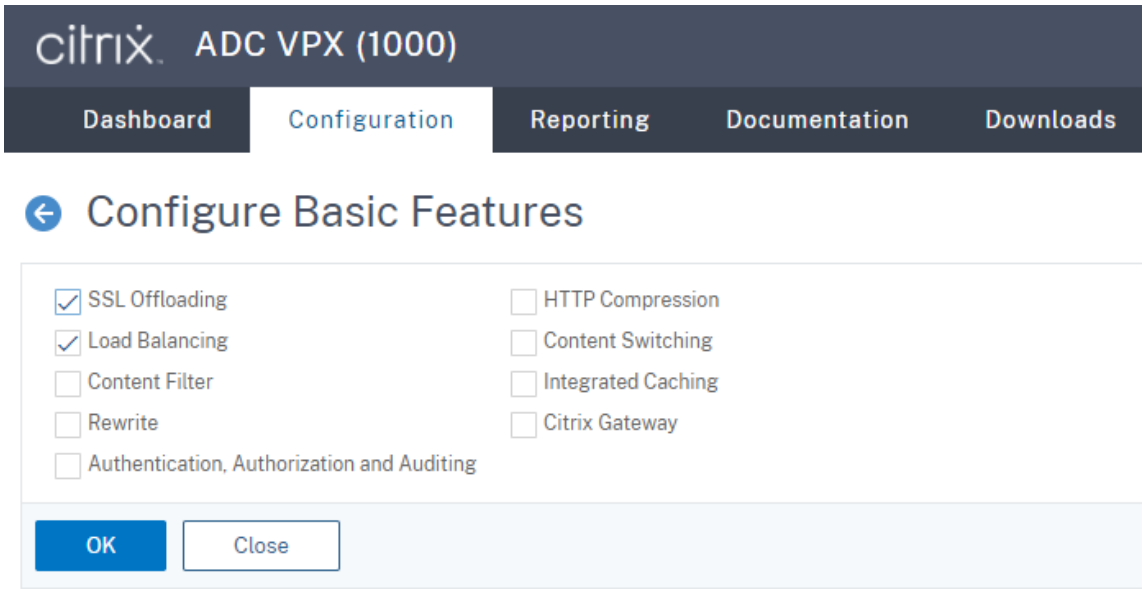


1. Citrix ADC VPX インスタンスにログオンします。

2. [**Configuration**] > [**System**] > [**Settings**] > [**Configure Basic Features**] の順に選択します。

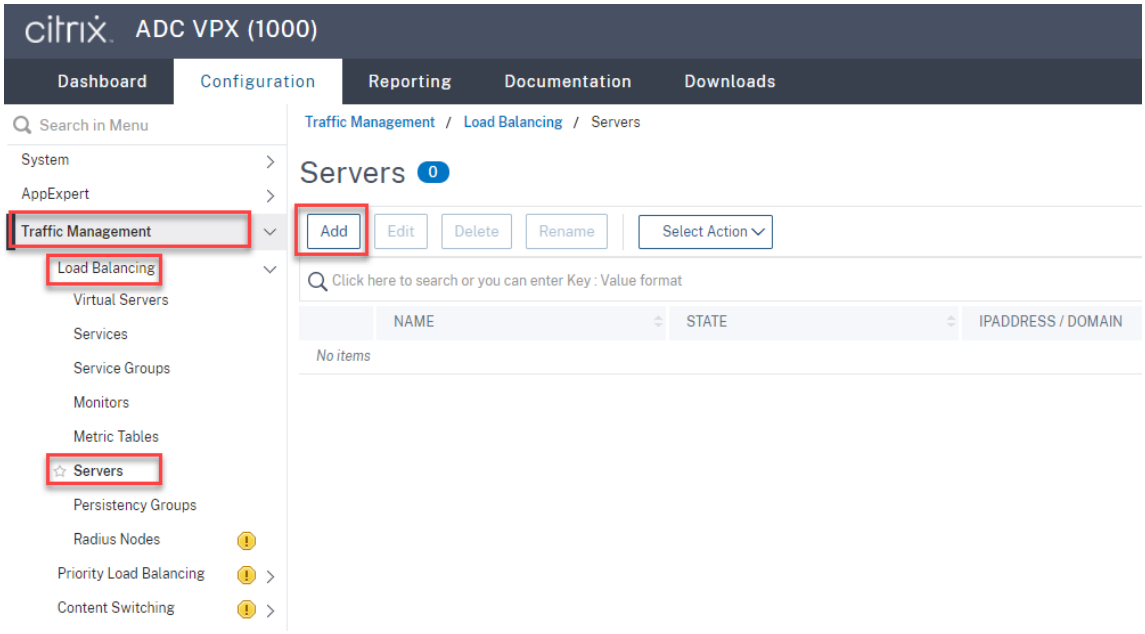


3. [**SSL Offloading**] と [**Load Balancing**] を選択し、[**OK**] をクリックします。

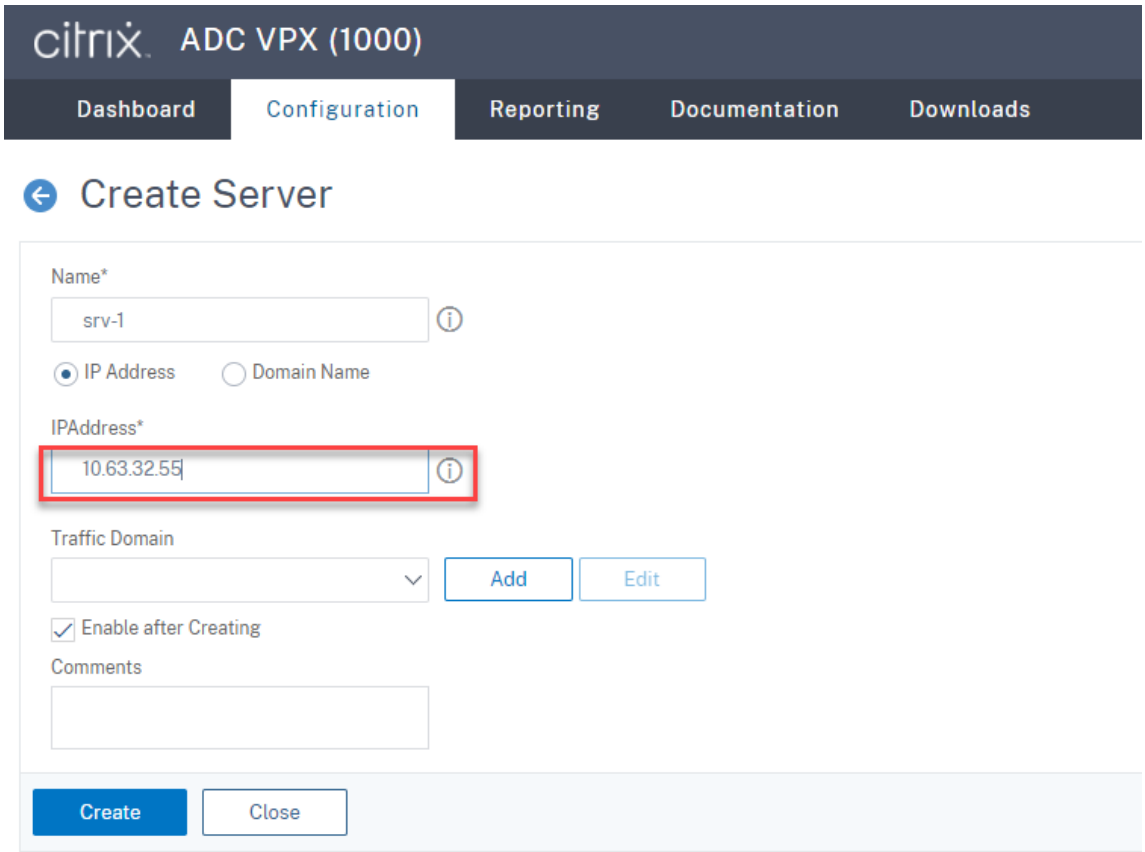


4. 負荷分散サーバーを追加します。

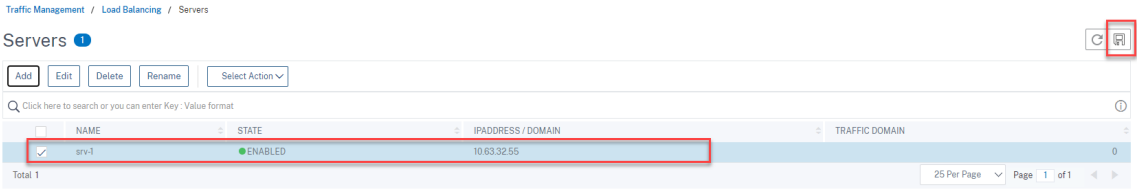
   [**Traffic Management**] > [**Load Balancing**] > [**Servers**] の順に選択し、[**Add**] をクリックします。



Session Recording サーバーの名前と IP アドレスを入力し、［**Create**］をクリックします。例:



右上隅にある保存アイコンをクリックして、変更を保存します。

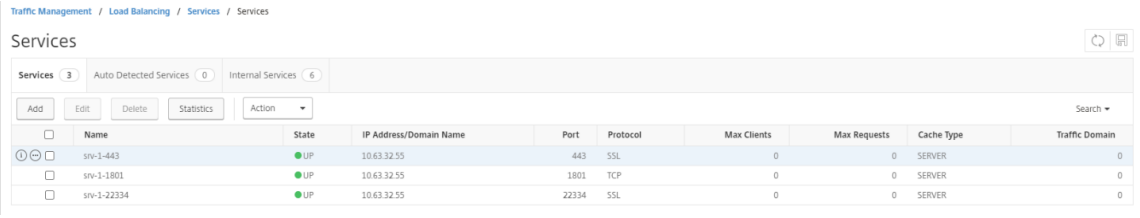


5. 前の手順で追加した各 Session Recording サーバーの負荷分散サービスを追加します。

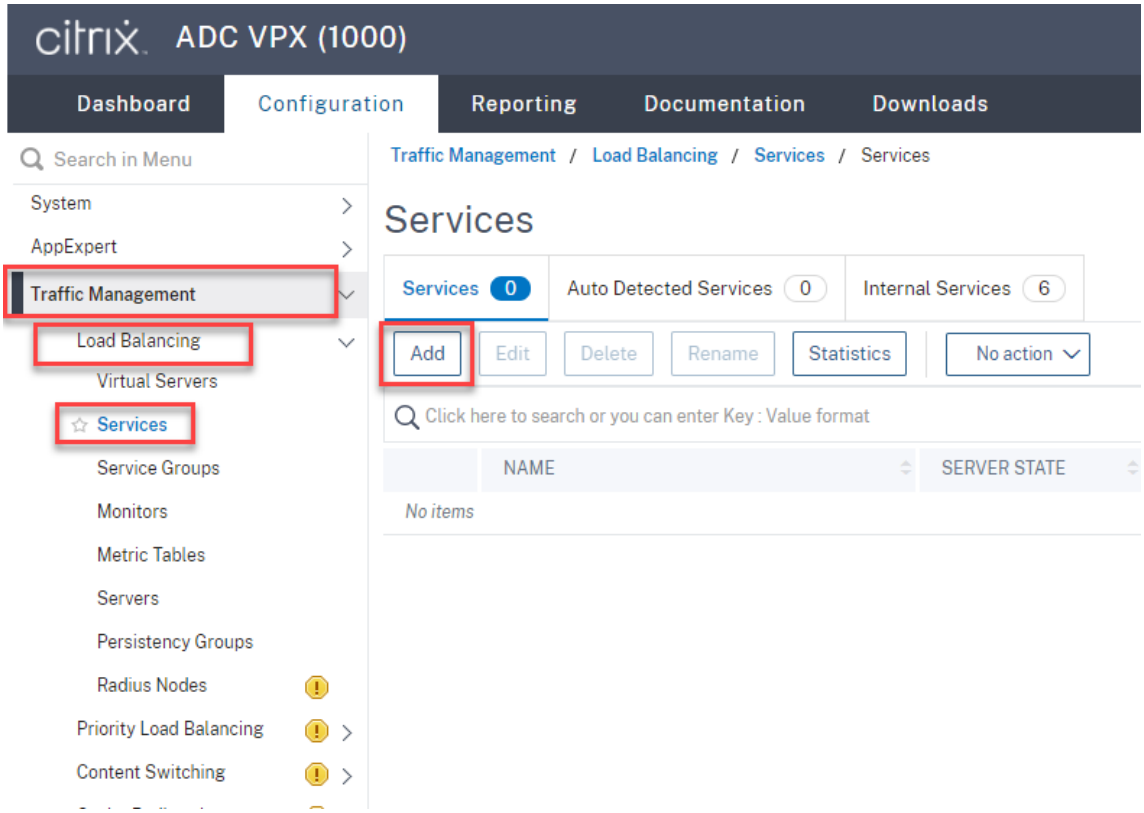
   各 Session Recording サーバーに次の負荷分散サービスを追加します:

   - (WebSocket サーバーバージョン 1.0 を使用している場合にのみ必要) TCP モニターにバインドするポート 22334 の **SSL** 負荷分散サービス
   - HTTPS モニターにバインドされたポート 443 の **SSL** 負荷分散サービス
   - TCP モニターにバインドされたポート 1801 の **TCP** 負荷分散サービス

   例:

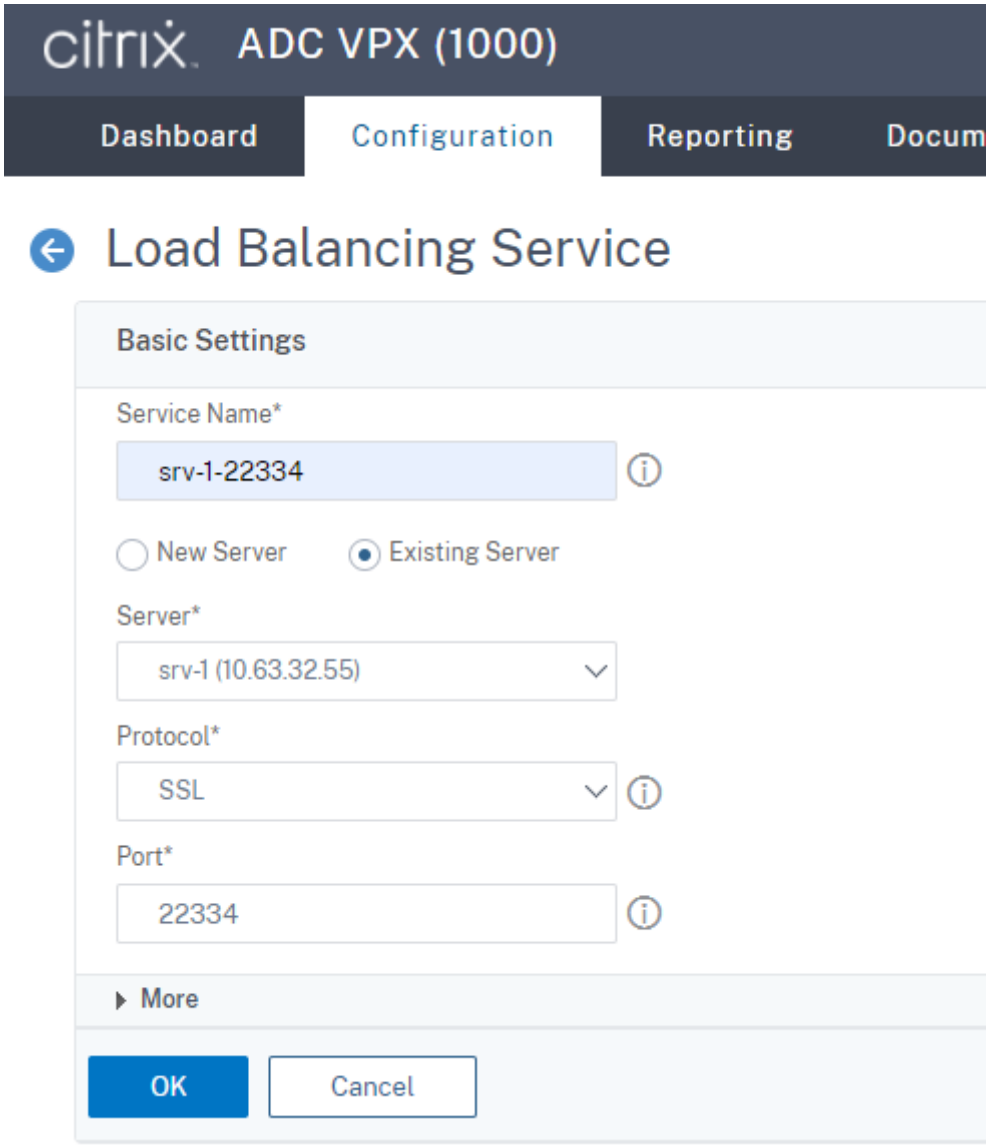


   [**Traffic Management**] > [**Load Balancing**] > [**Services**] の順に選択し、[**Add**] をクリックします。

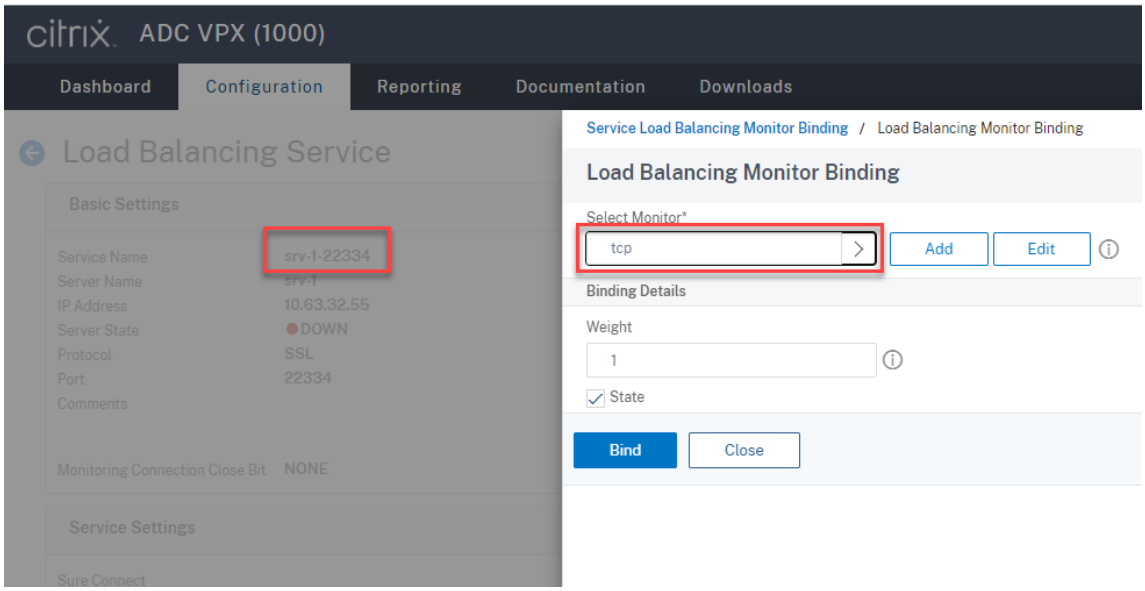


（**WebSocket** サーバーバージョン **1.0** を使用している場合にのみ必要）**Session Recording** サーバーごとにポート **22334** の **SSL** 負荷分散サービスを追加します。負荷分散サービスの名前を入力して ［**Existing Server**］を選択し、Session Recording サーバーの IP アドレスを選択します。次に、サーバープロトコルとして ［**SSL**］を選択し、ポート番号「**22334**」を入力して ［**OK**］をクリックします。

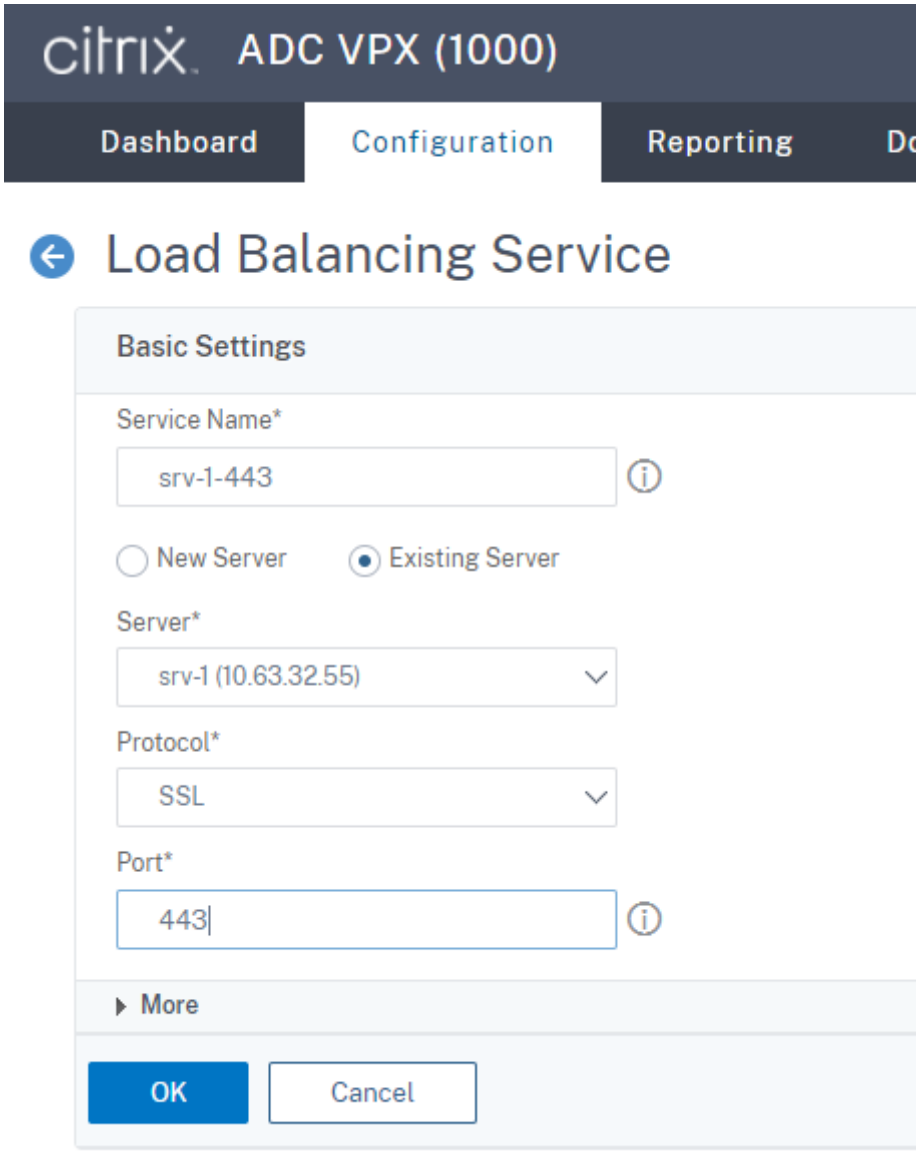
たとえば、以下のスクリーンショットを参照してください。



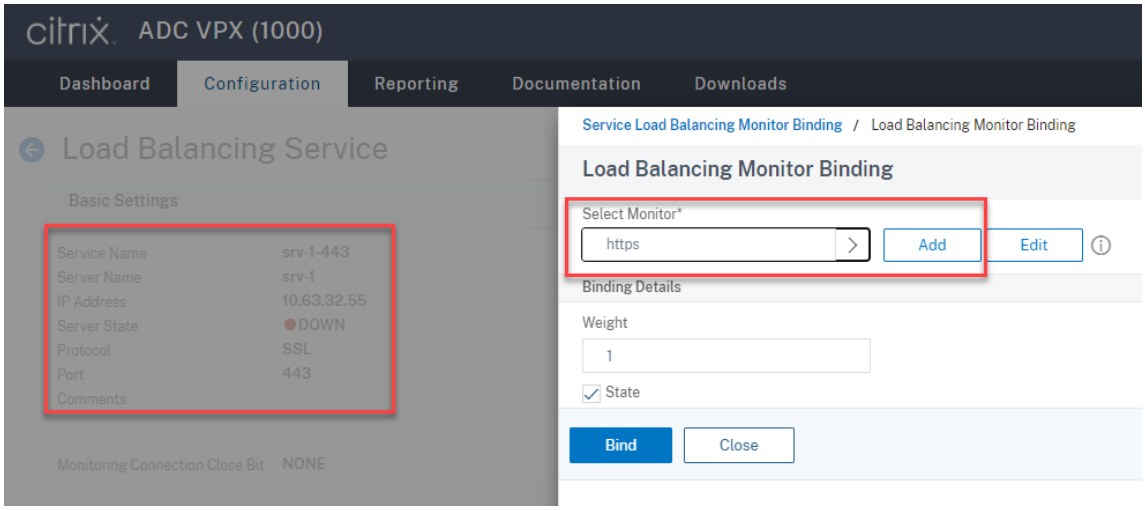
TCP モニターを、追加した **SSL** 負荷分散サービスにバインドします。



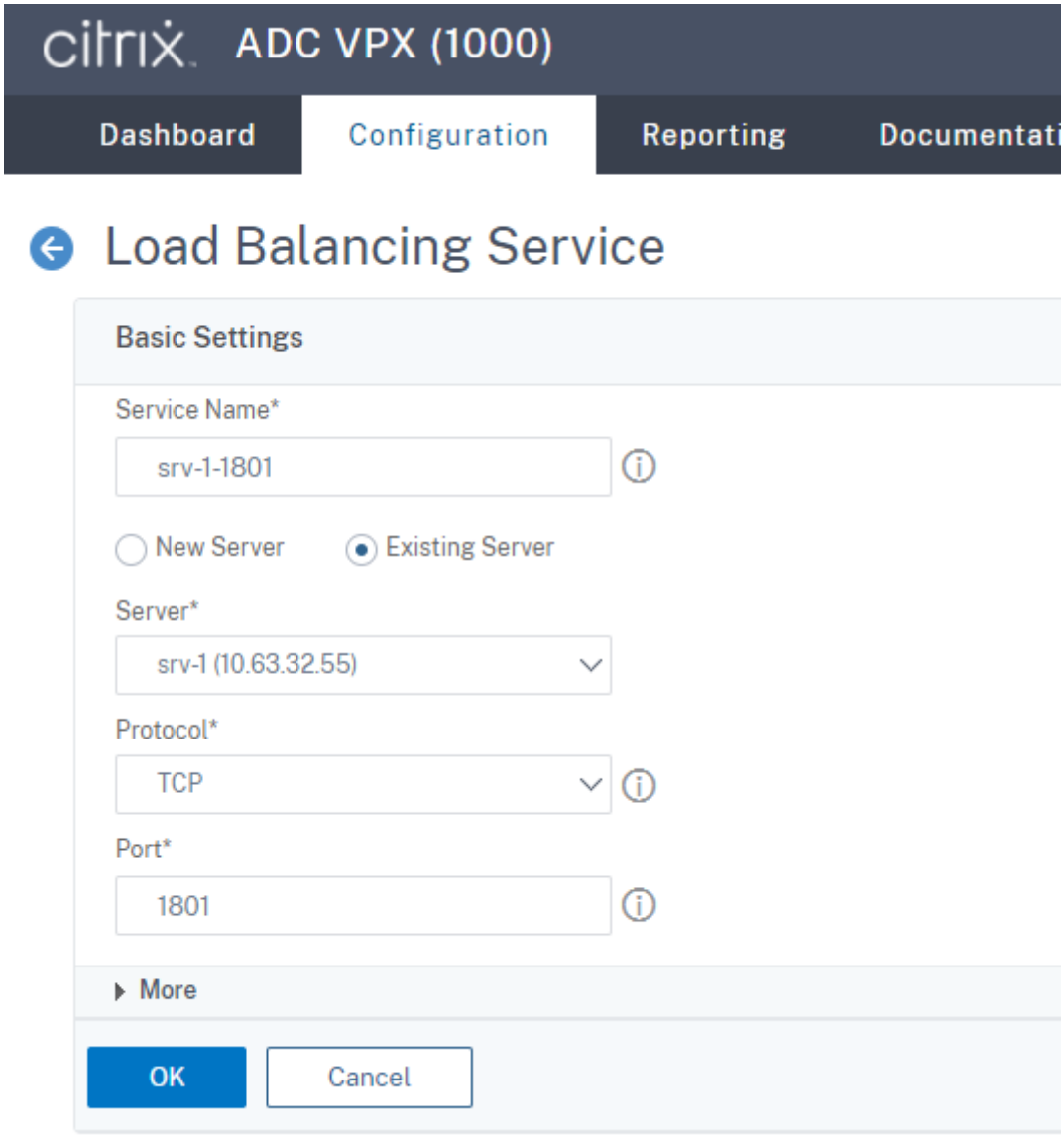
各 **Session Recording** サーバーにポート **443** の **SSL** 負荷分散サービスを追加します。負荷分散サービスの名前を入力して［**Existing Server**］を選択し、Session Recording サーバーの IP アドレスを選択します。次に、サーバープロトコルとして［**SSL**］を選択し、ポート番号「443」を入力して［**OK**］をクリックします。



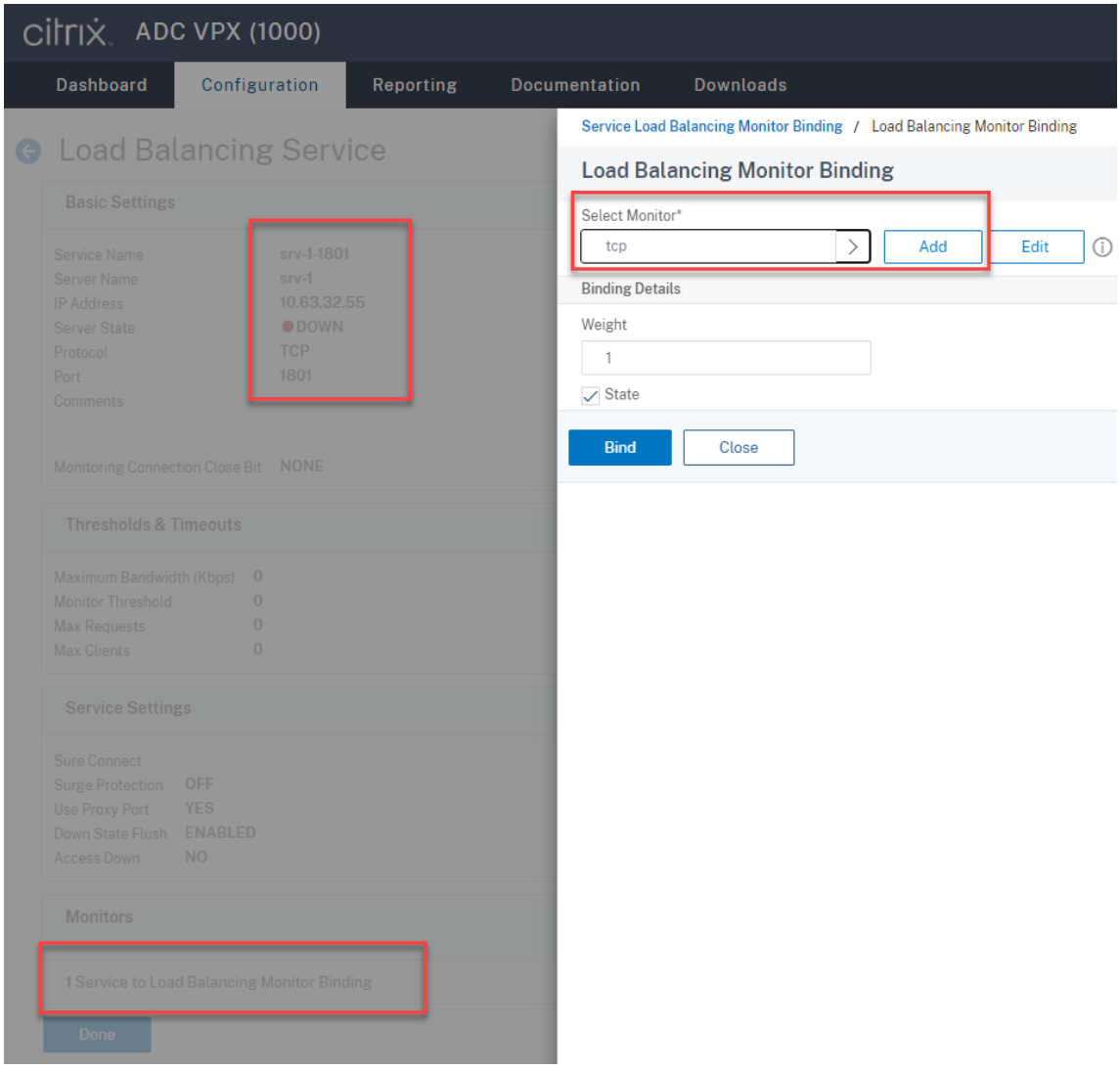
HTTPS モニターを、追加した **SSL** 負荷分散サービスにバインドします。



各 **Session Recording** サーバーにポート **1801** の **TCP** 負荷分散サービスを追加します。負荷分散サービスの名前を入力して［**Existing Server**］を選択し、Session Recording サーバーの IP アドレスを選択します。次に、サーバープロトコルとして［**TCP**］を選択し、ポート番号「1801」を入力して［**OK**］をクリックします。

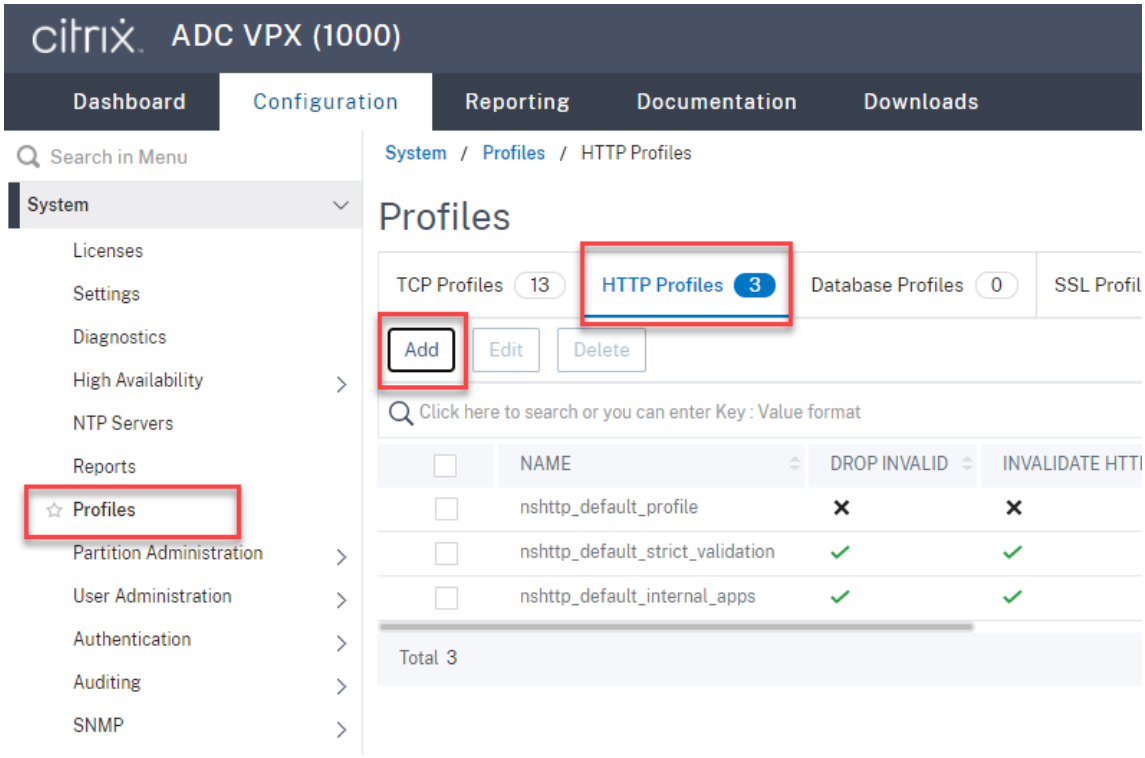


TCP モニターを、追加した **TCP** 負荷分散サービスにバインドします。

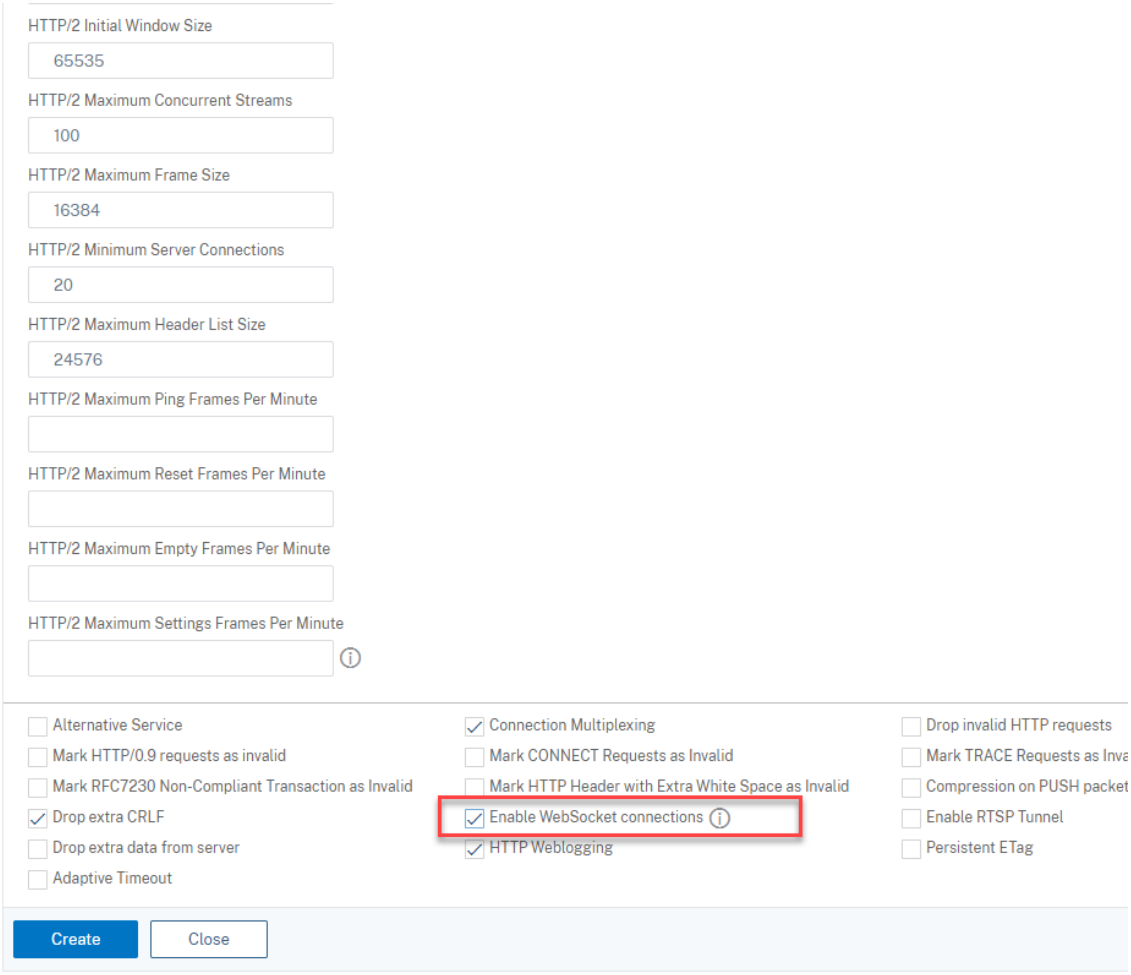


6. (WebSocket サーバーバージョン 1.0 を使用している場合にのみ必要) ポート 22334 の **SSL** 負荷分散サービスごとに HTTP プロファイルを追加します。

   [**System**] > [**Profiles**] > [**HTTP Profiles**] の順に選択し、[**Add**] をクリックします。

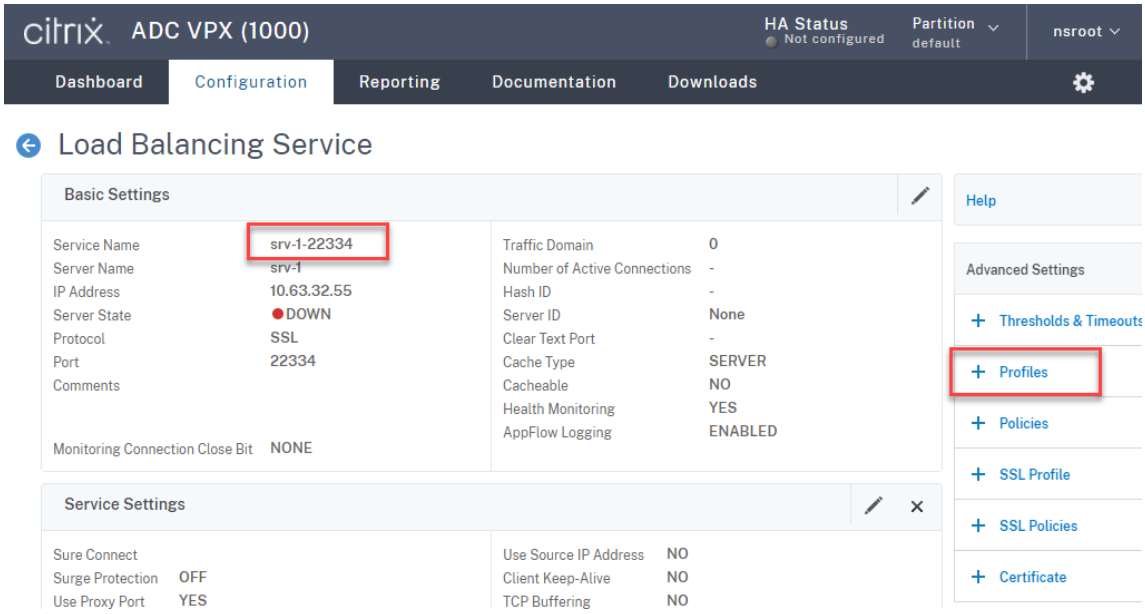


[**Enable WebSocket connections**] チェックボックスをオンにし、他の設定についてはデフォルトのままにします。

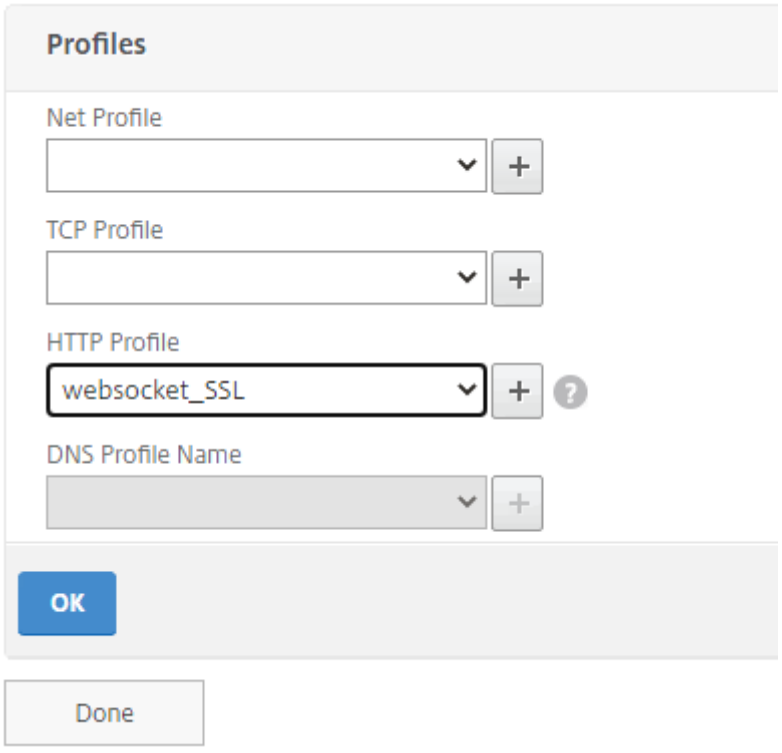


HTTP プロファイルの名前を入力します（例：`websocket_SSL`）。

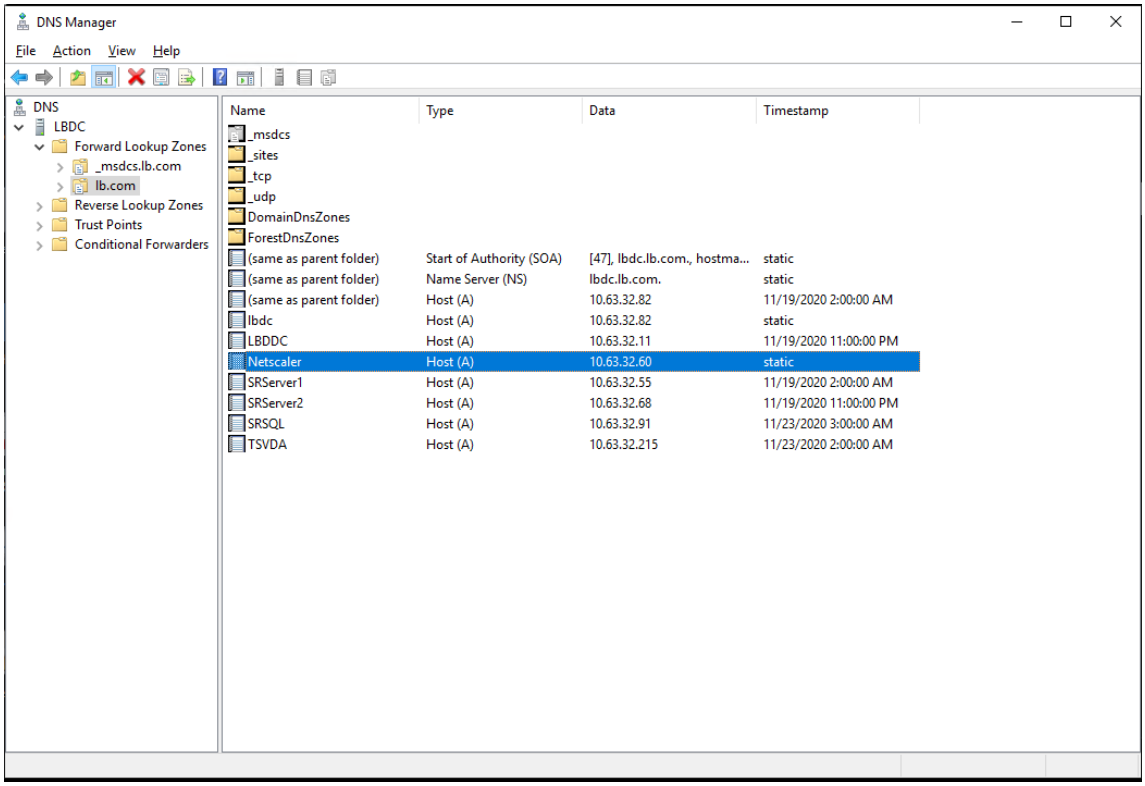
ポート 22334 の各 **SSL** 負荷分散サービスに戻ります（例：`srv-1-22334` ）。[**+ Profiles**] をクリックします。



HTTP プロファイル（例：websocket_SSL）を選択し、[**OK**]、[**Done**] の順にクリックします。



7. （WebSocket サーバーバージョン 2.0 を使用している場合にのみ必要）ポート 443 の **SSL** 負荷分散サービスごとに HTTP プロファイルを追加します。
8. ドメインコントローラーで Citrix ADC VIP アドレスのホストレコードを作成します。

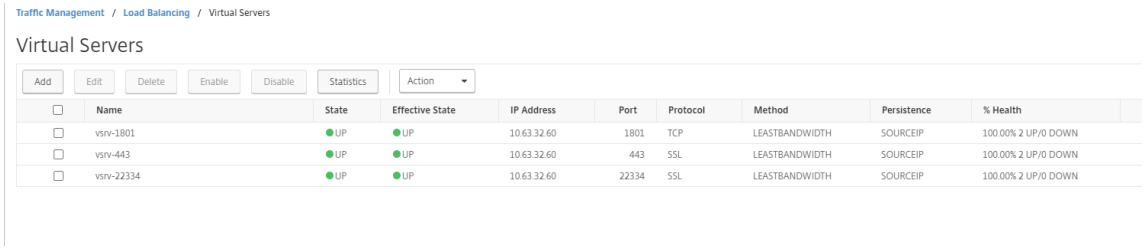


9. 負荷分散仮想サーバーを追加します。

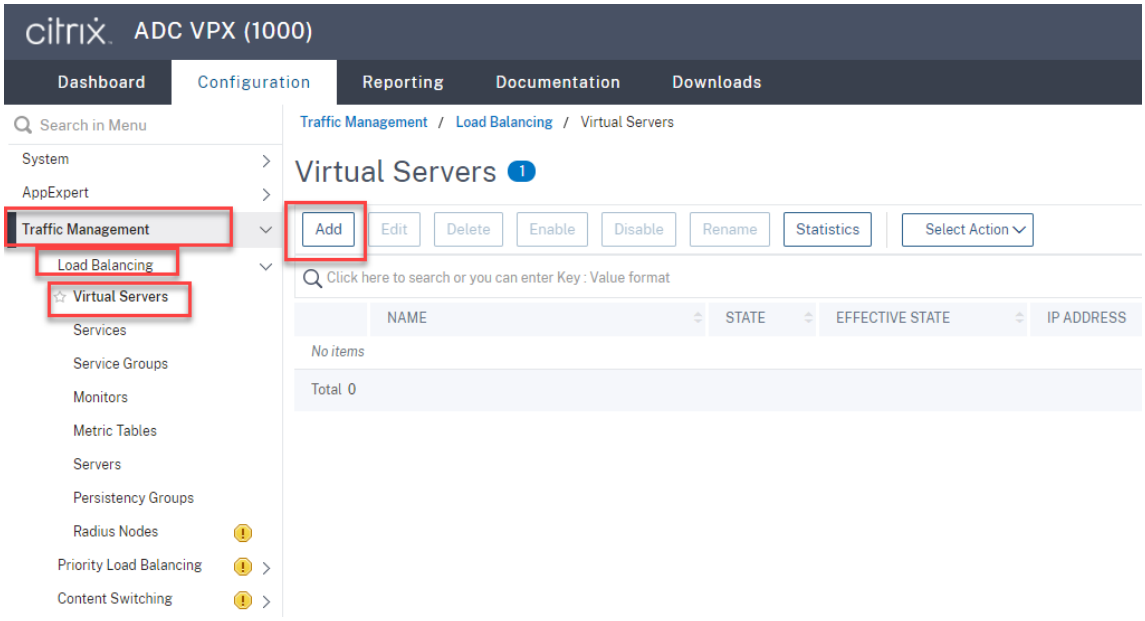
   Citrix ADC VIP アドレスで、次の負荷分散仮想サーバーを追加します。

   - （WebSocket サーバーバージョン 1.0 を使用している場合にのみ必要）SSL に基づくポート 22334 の負荷分散仮想サーバー
   - SSL に基づくポート 443 の負荷分散仮想サーバー
   - TCP に基づくポート 1801 の負荷分散仮想サーバー

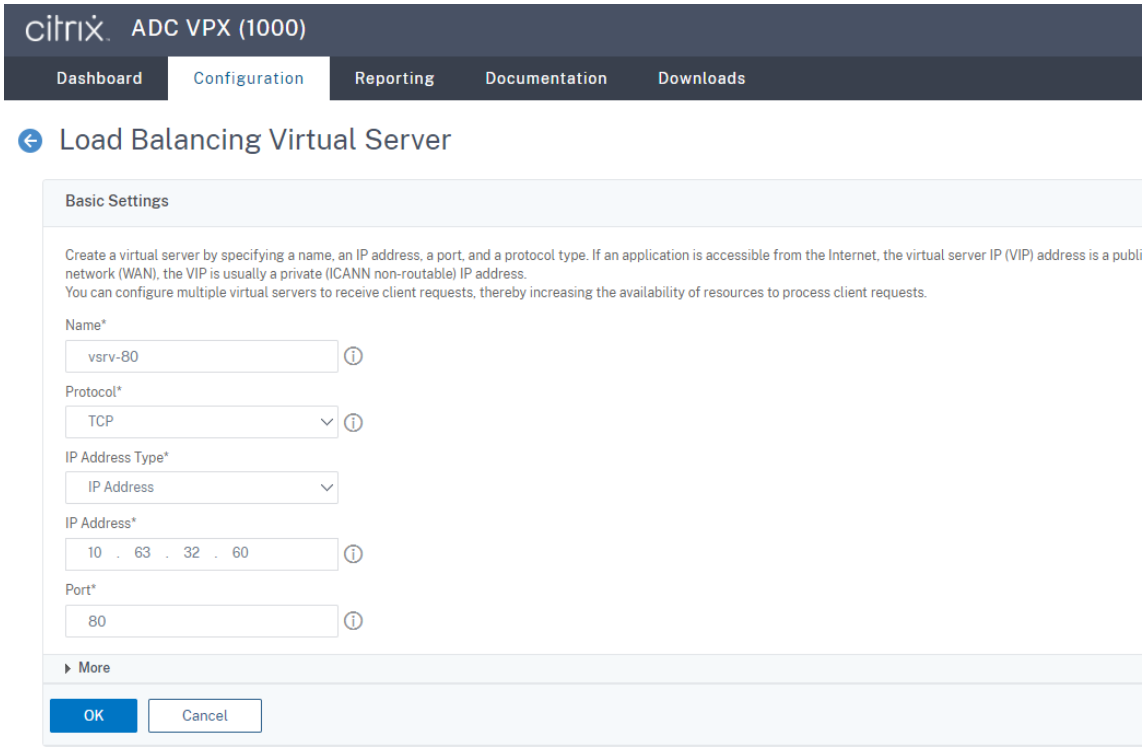
   たとえば、以下のスクリーンショットを参照してください。



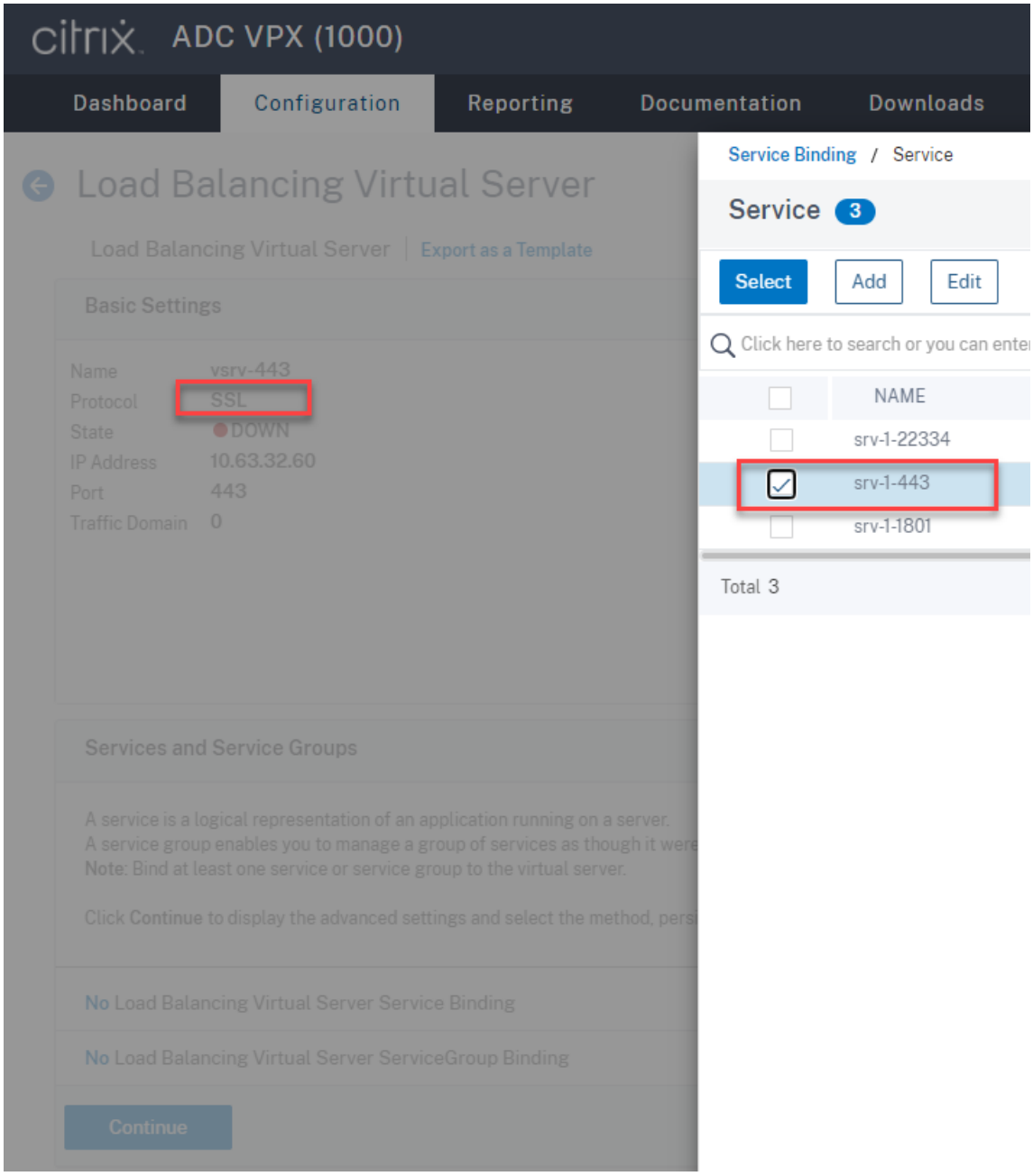
   [**Traffic Management**] > [**Load Balancing**] > [**Virtual Server**] の順に選択し、[**Add**] をクリックします。



Citrix ADC VIP アドレスで、各仮想サーバーを追加します。サーバー名を入力し、**TCP** または **SSL** を選択して、前の部分で説明したように関連するポート番号を選択します。

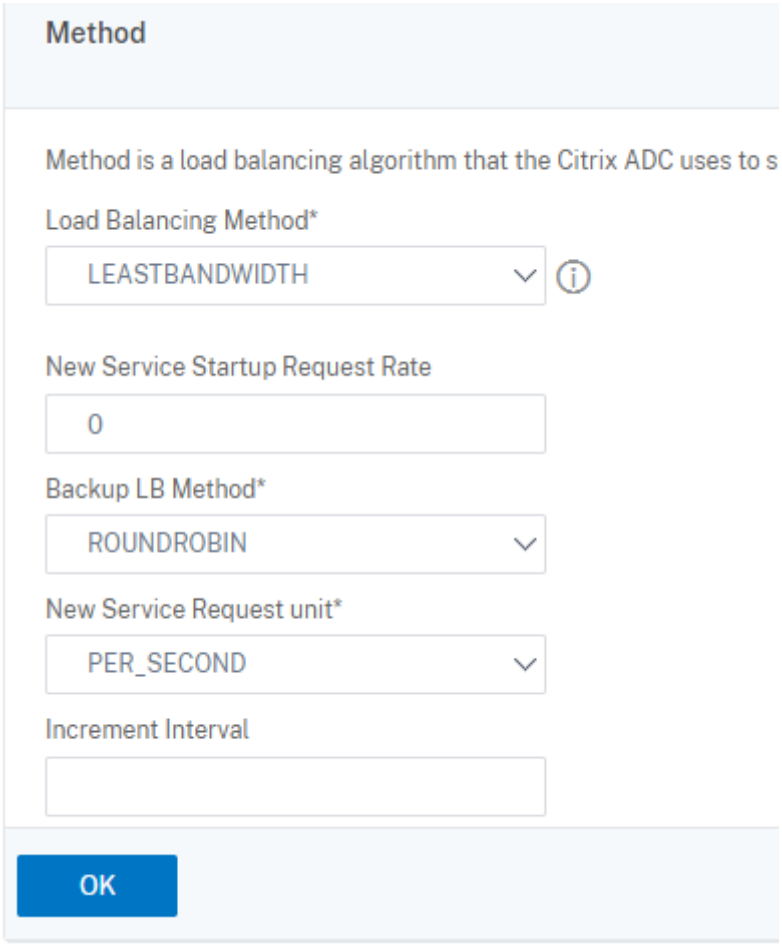


各仮想サーバーを同じポートの負荷分散サービスにバインドします。例:

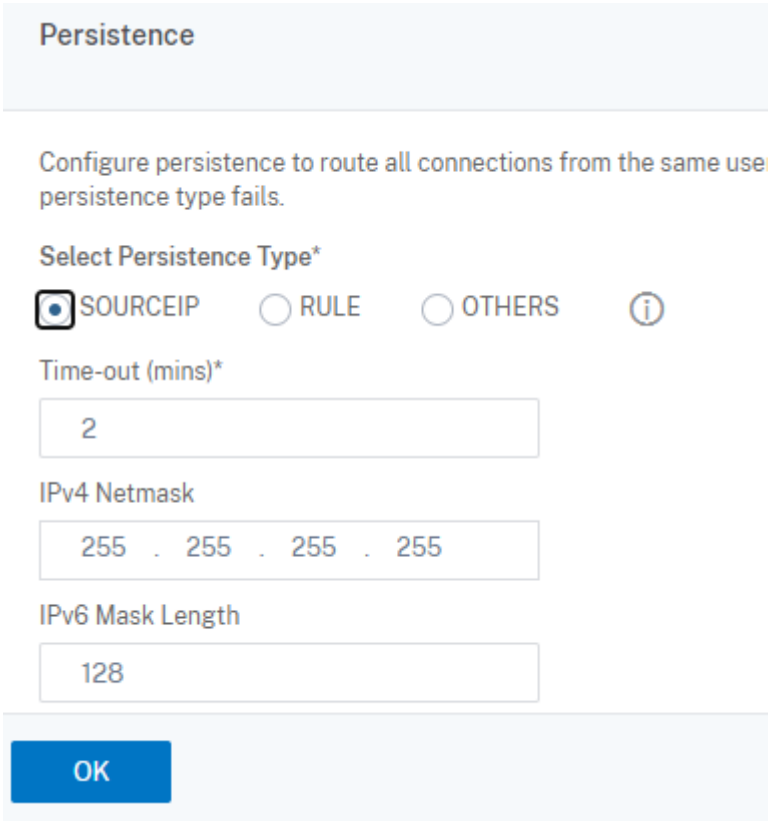


> ヒント：
>
> ポート 22334 の負荷分散サービスは、WebSocket サーバーバージョン 1.0 を使用する場合にのみ必要です。

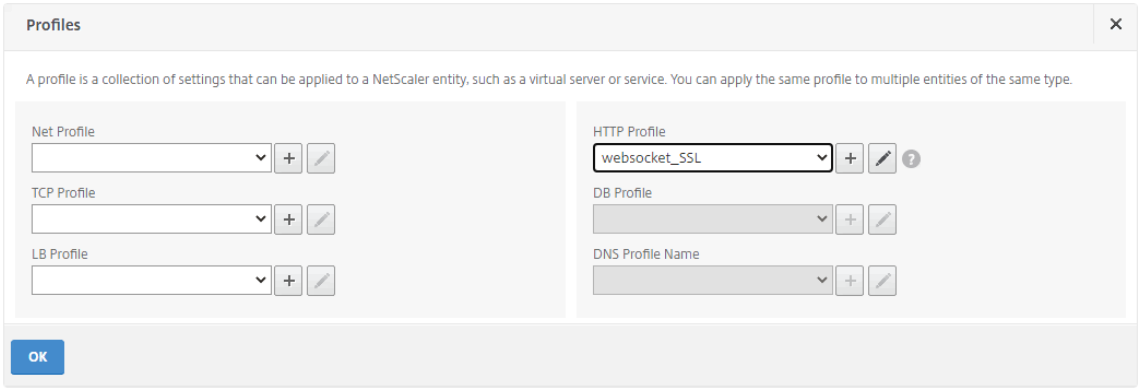
負荷分散の方法を選択します。



各仮想サーバーでパーシステンスを構成します。パーシステンスタイプとして **SOURCEIP** を選択することをお勧めします。詳しくは、「パーシステンスの設定」を参照してください。



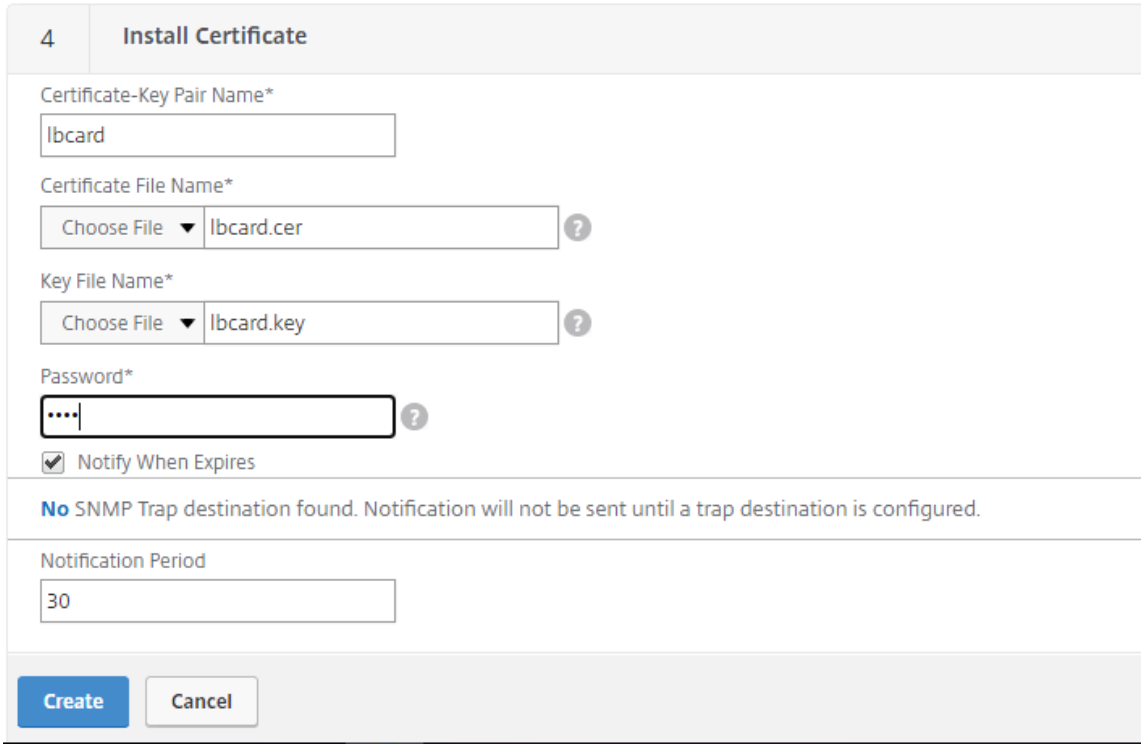
（WebSocket サーバーバージョン 1.0 を使用している場合にのみ必要）ポート 22334 の負荷分散仮想サーバーの HTTP プロファイルを追加します。



10. Citrix ADC にサブジェクトの別名（SAN）証明書をインストールします。

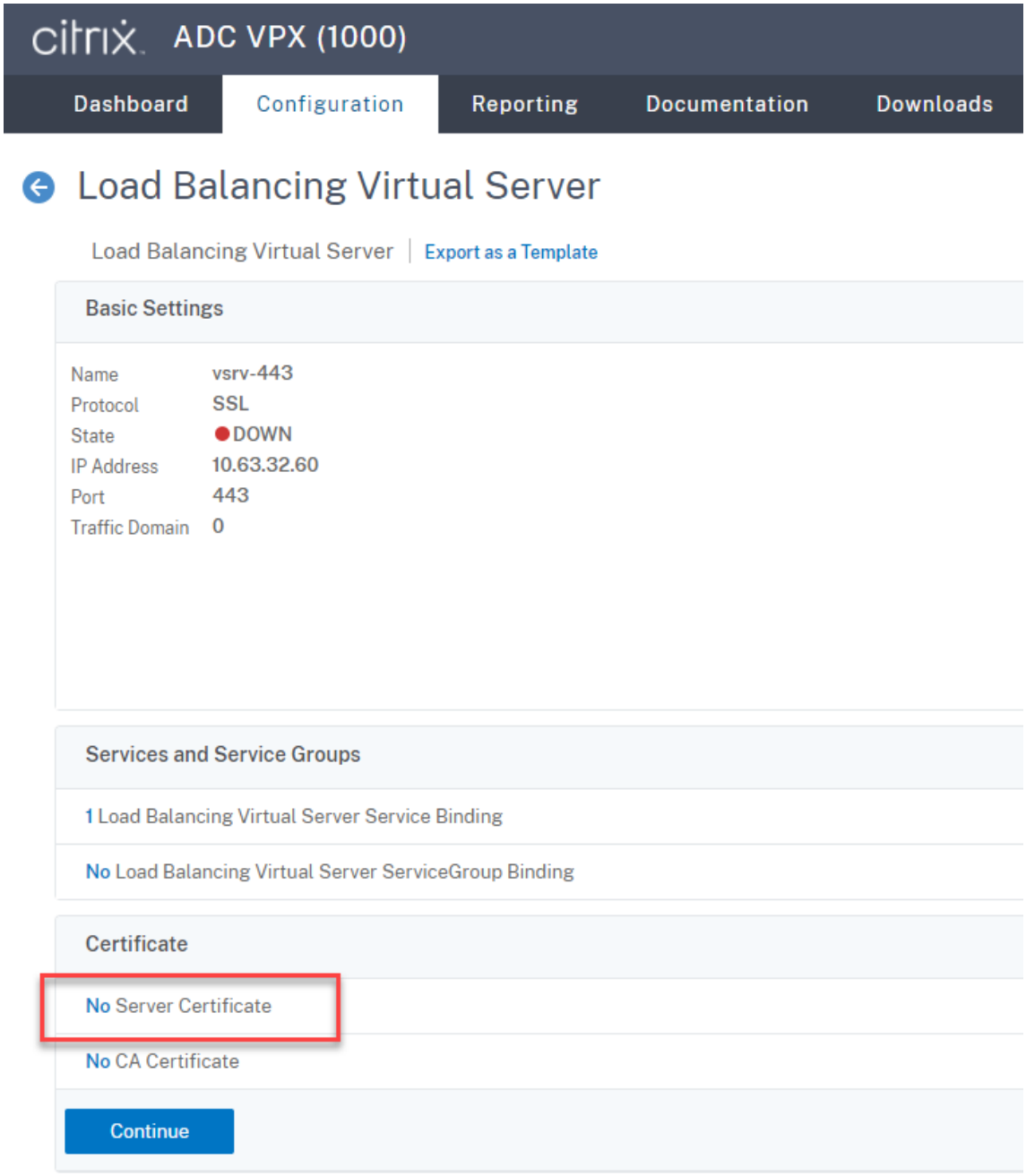
    信頼できる証明機関（CA）から PEM 形式の SAN 証明書を取得します。［**Traffic Management**］**>** ［**SSL**］**>** ［**Server Certificate Wizard**］の順に選択して、Citrix ADC の証明書および秘密キーのファイルを抽出してアップロードします。

    詳しくは、「SSL 証明書」を参照してください。



11. SAN 証明書を各 SSL 負荷分散仮想サーバーにバインドします。

    [**Traffic Management**] > [**Load Balancing**] > [**Virtual Servers**] の順に選択します。次に、SSL 負荷分散仮想サーバーを選択し、[**Server Certificate**] をクリックします。

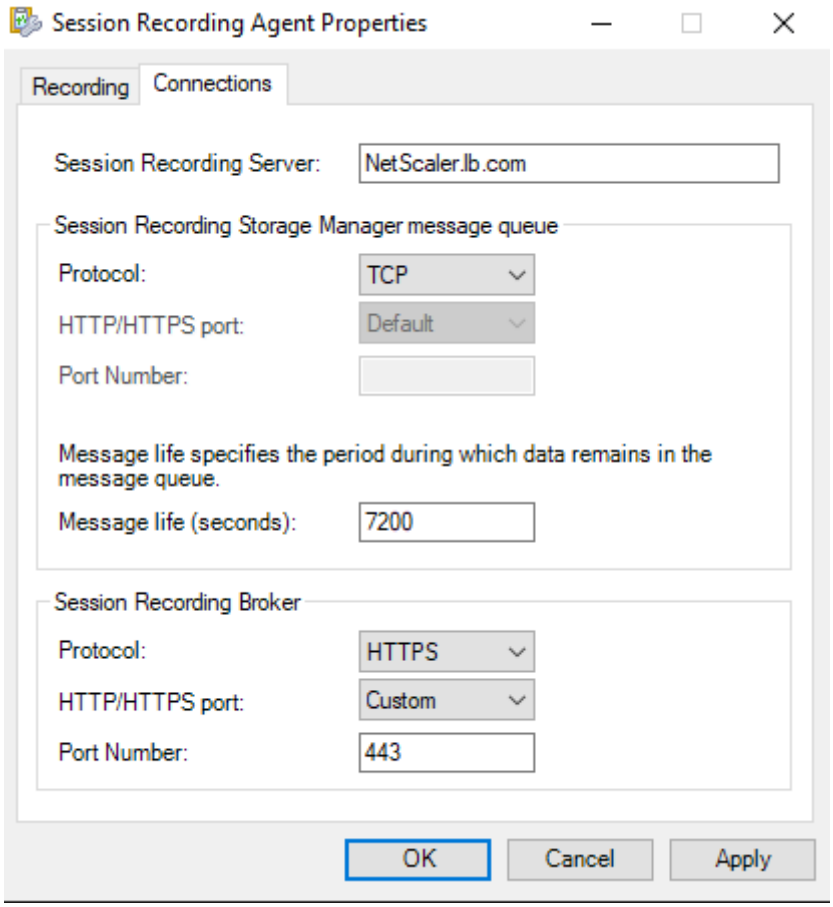


前述の SAN 証明書を追加し、[**Bind**] をクリックします。

手順 **4**: 負荷分散をサポートするように既存の **Session Recording Agent** を構成する

1. ドメイン管理者アカウントを使用して、Session Recording Agent にログオンします。
2. **Session Recording Agent** のプロパティを開きます。
3. TCP 経由で Microsoft Message Queuing（MSMQ）を使用する場合は、この手順を実行してください。

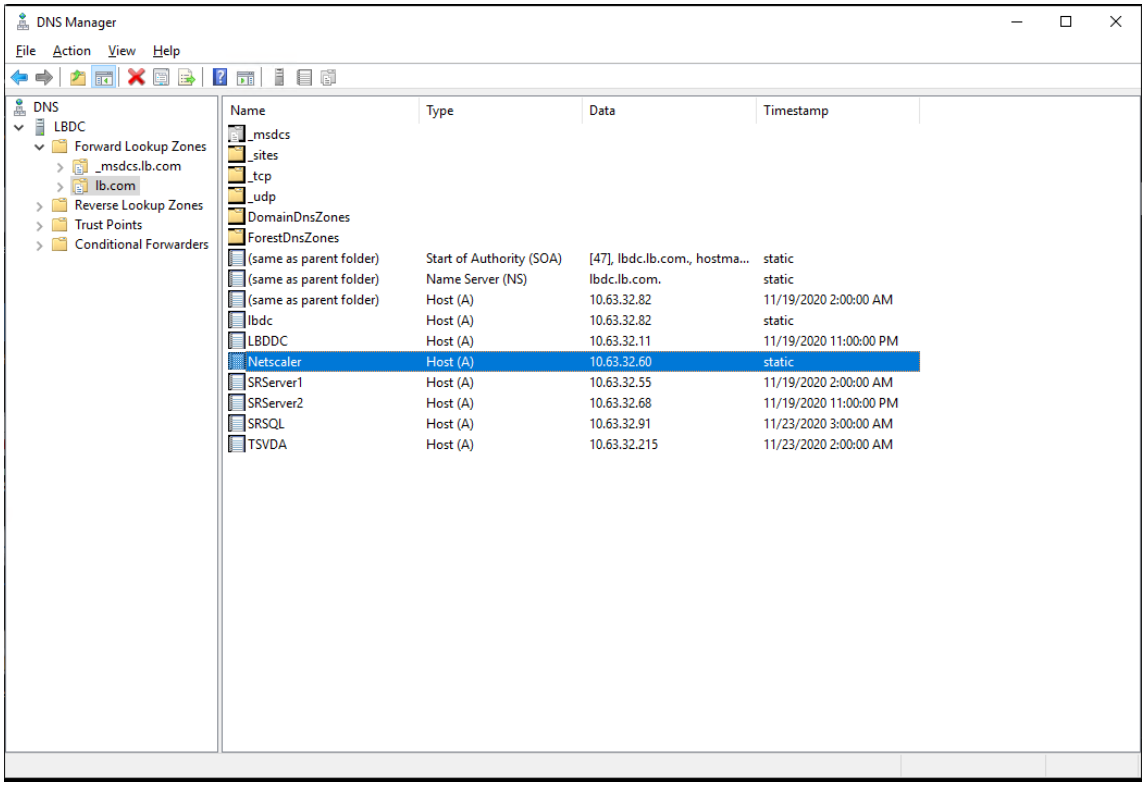
［**Session Recording Server**］ボックスに Citrix ADC VIP アドレスの完全修飾ドメイン名を入力します。



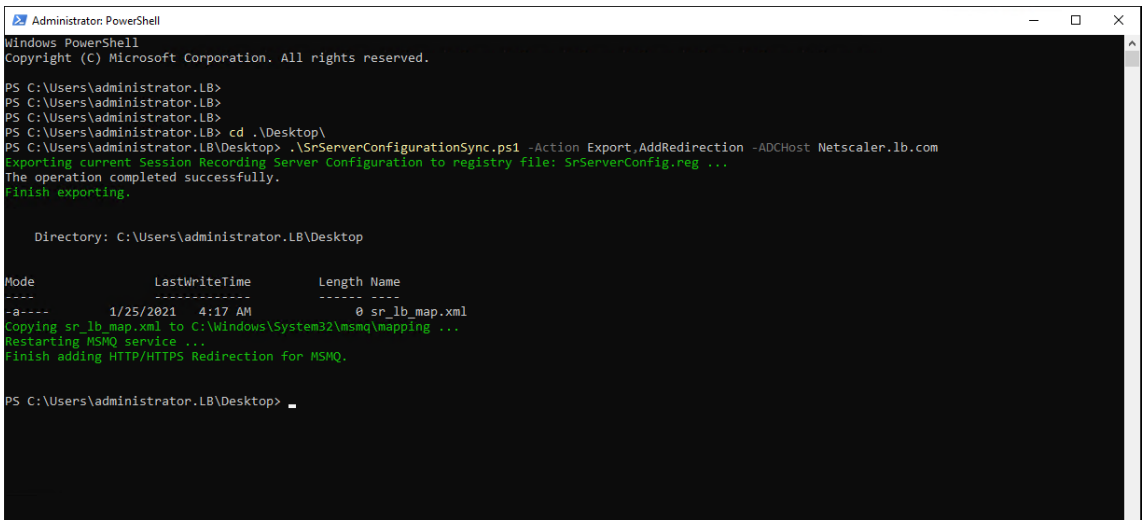
各 Session Recording サーバー上で、`HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\MSMQ\Parameters`にある`IgnoreOSNameValidation`の DWORD 値に「1」を追加して設定します。詳しくは、Knowledge Center の記事CTX248554を参照してください。

4. MSMQ over HTTP または MSMQ over HTTPS を使用する場合は、この手順を実行してください。

   （この手順が完了している場合はスキップ）ドメインコントローラーで Citrix ADC VIP アドレスのホストレコードを作成します。



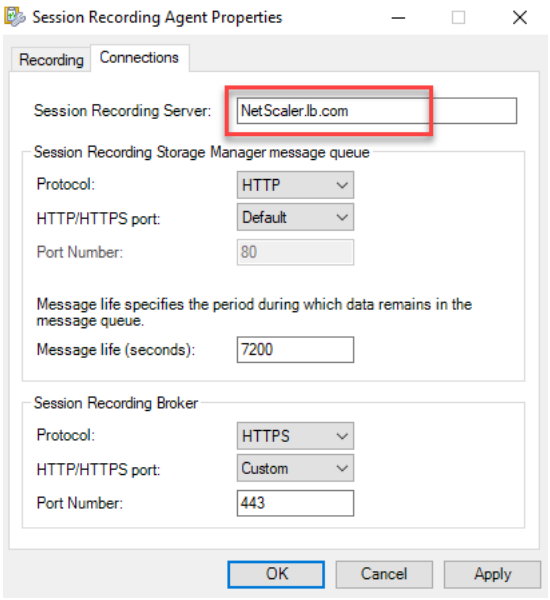
各 Session Recording サーバーで、`powershell.exe -file SrServerConfigurationSync.ps1 -Action AddRedirection - ADCHost <ADCHost>`コマンドを実行して、Citrix ADC からローカルホストにリダイレクトを追加します。<ADCHost>は Citrix ADC VIP アドレスの完全修飾ドメイン名です。リダイレクトファイル（例：`sr_lb_map.xml`）が`C:\Windows\System32\msmq\Mapping`に生成されます。



注：PowerShell.exe を実行するとき、`SrServerConfigurationSync.ps1`が存在するフォルダーに移動します。

[**Session Recording Server**］ボックスに Citrix ADC VIP アドレスの完全修飾ドメイン名を入力します。

例：



手順 **5**：負荷分散をサポートするように既存の **Session Recording Player** を構成する

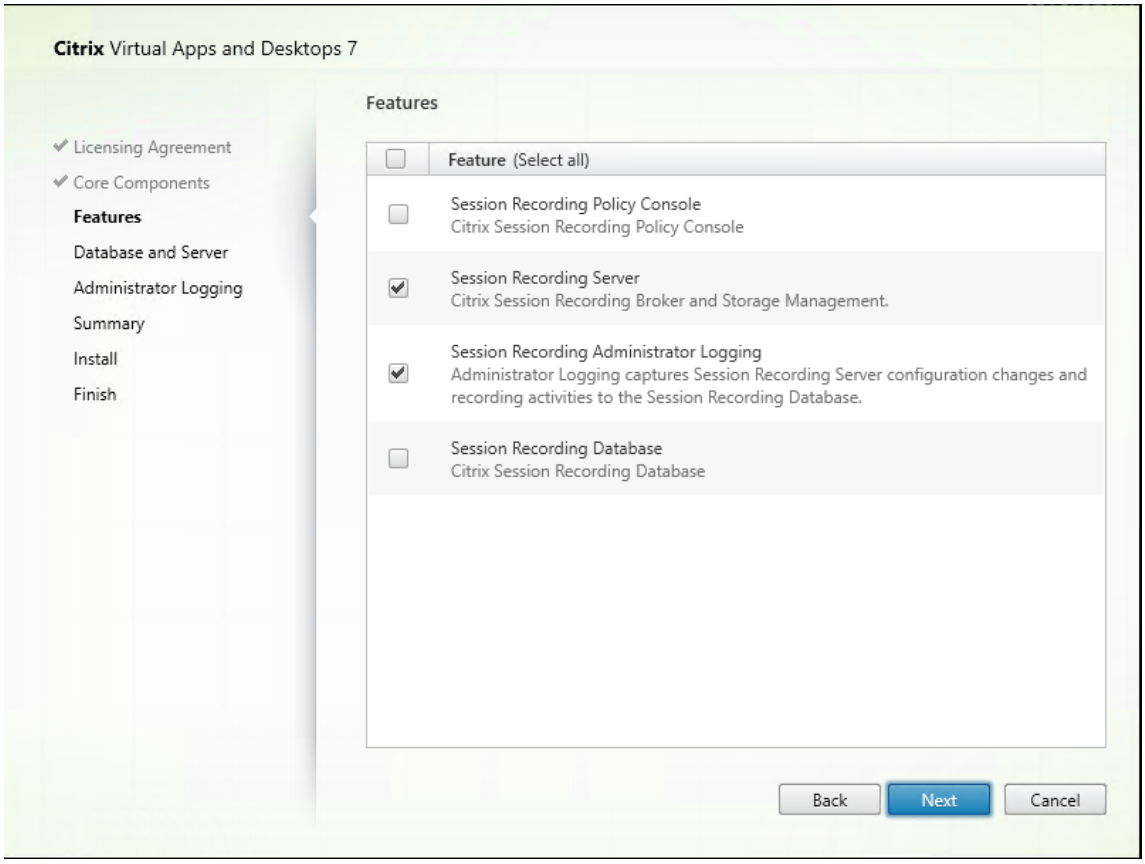
Session Recording Player コンポーネントをインストールした各マシンで、接続された Session Recording サーバーとして Citrix ADC VIP アドレスまたは Citrix ADC VIP の完全修飾ドメイン名を追加します。

手順 **6**：構成済みの既存の **Session Recording** サーバーで負荷分散が機能するかどうかを確認する

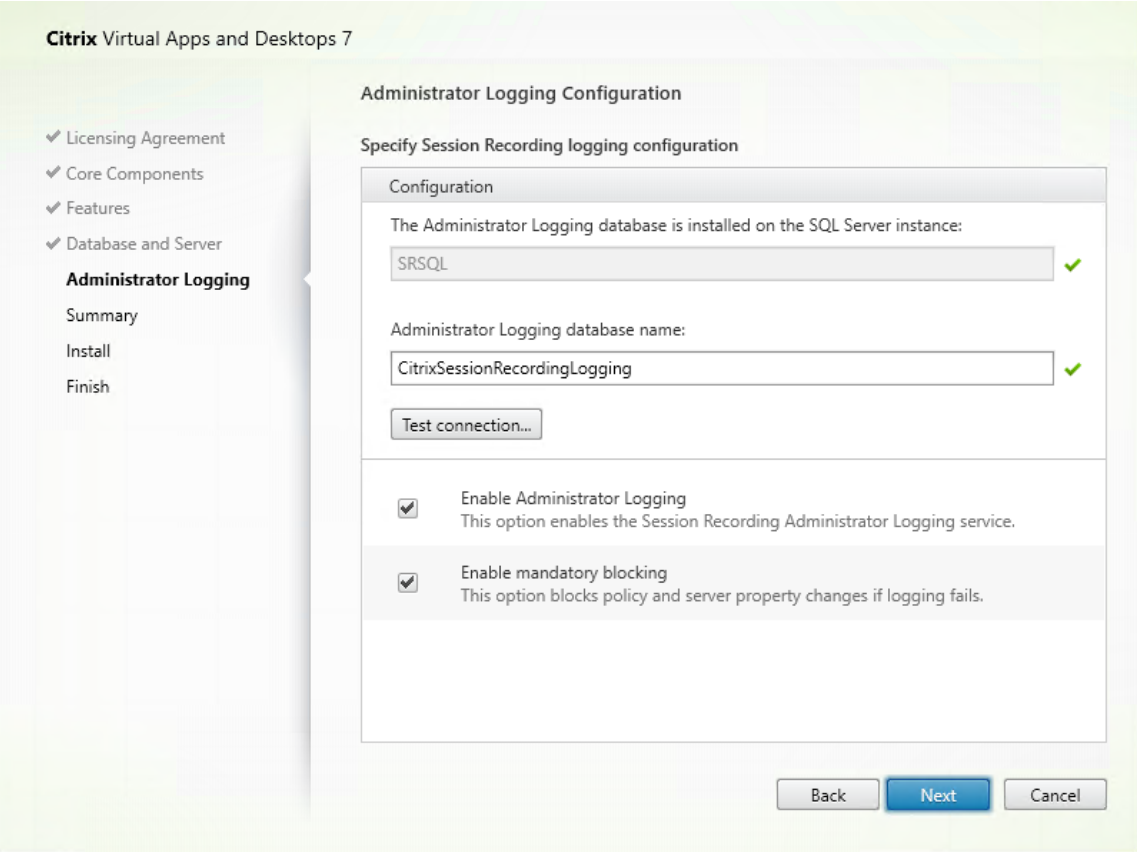
1. Citrix 仮想セッションを起動します。
2. セッションを録画できるかどうかを確認します。
3. Web Player と Session Recording Player が録画ファイルを再生できるかどうかを確認します。

手順 **7**：**Session Recording** サーバーを追加する

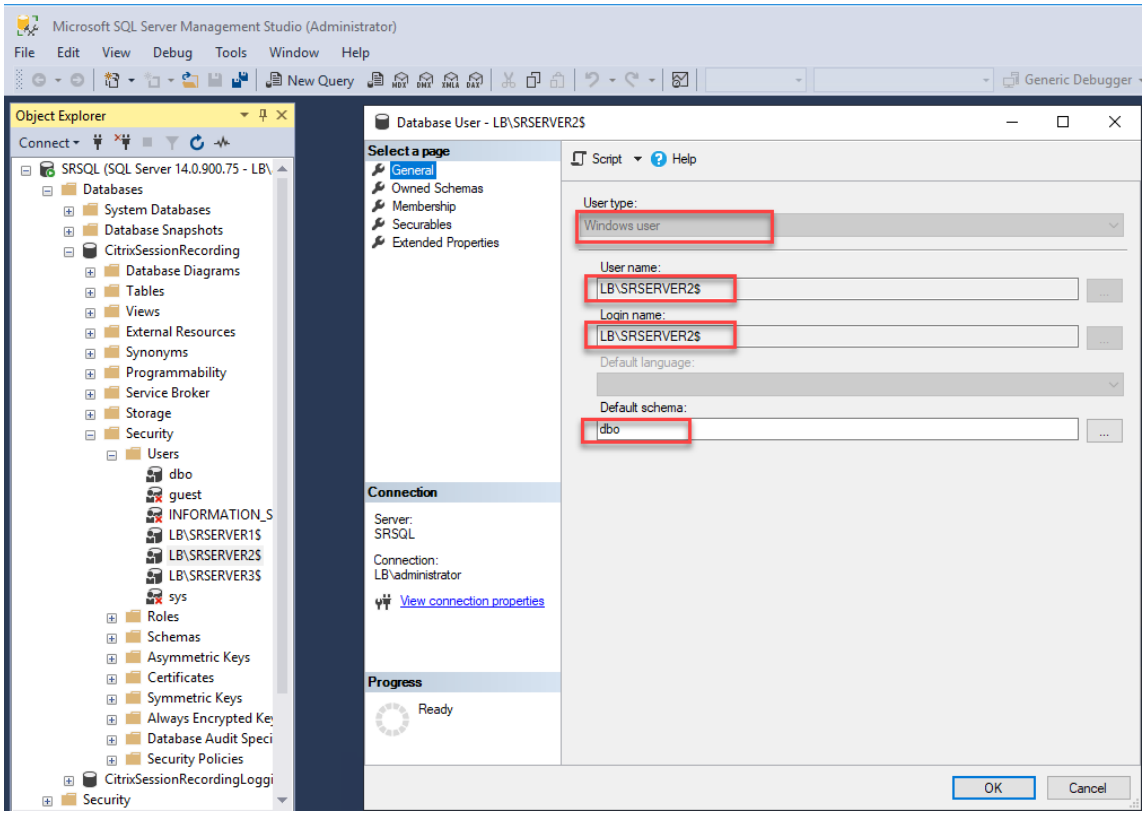
1. 同じドメインにマシンを準備し、Session Recording サーバーモジュールと Session Recording 管理者ログモジュールのみをマシンにインストールします。

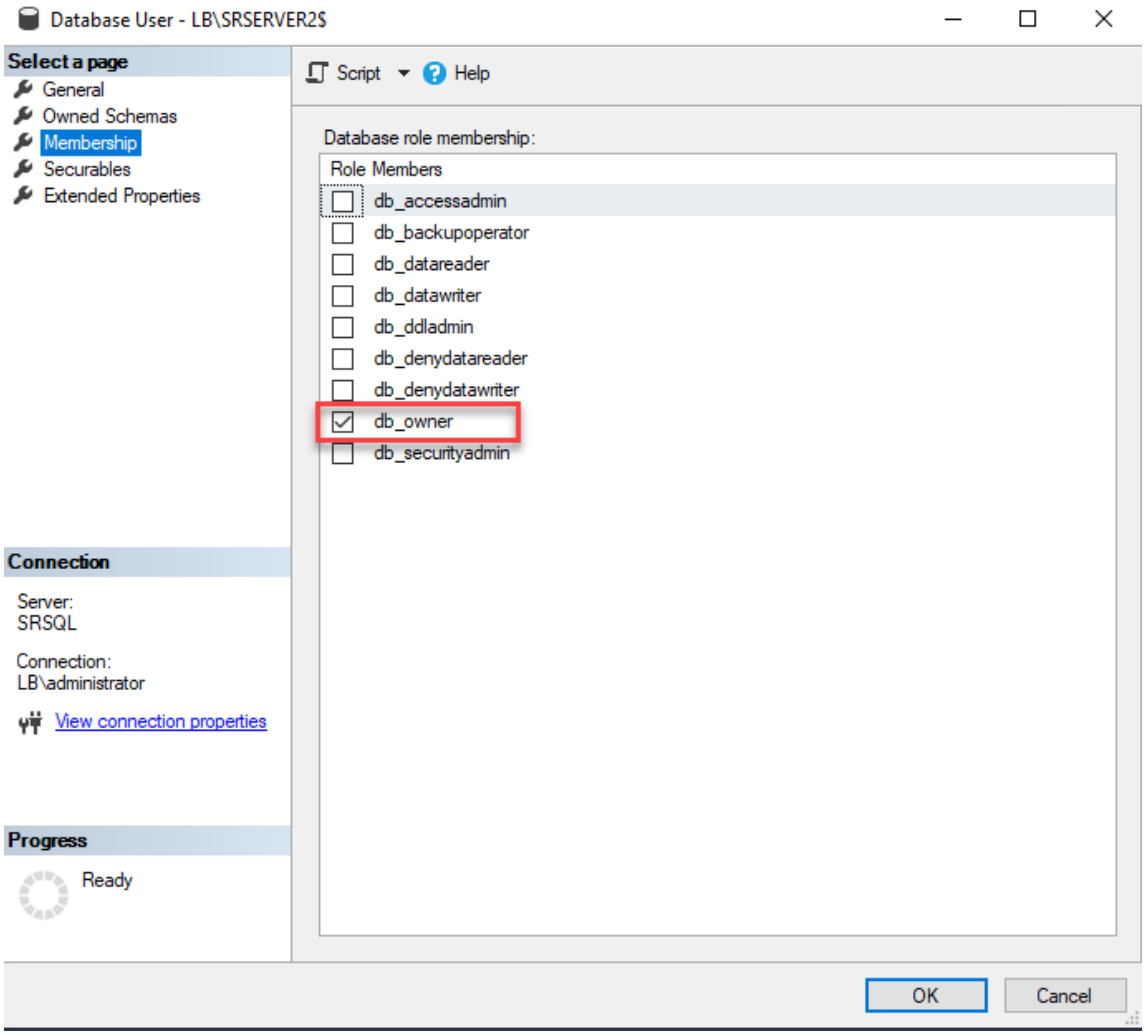


2. 既存の Session Recording サーバーと同じデータベース名を使用します。例:



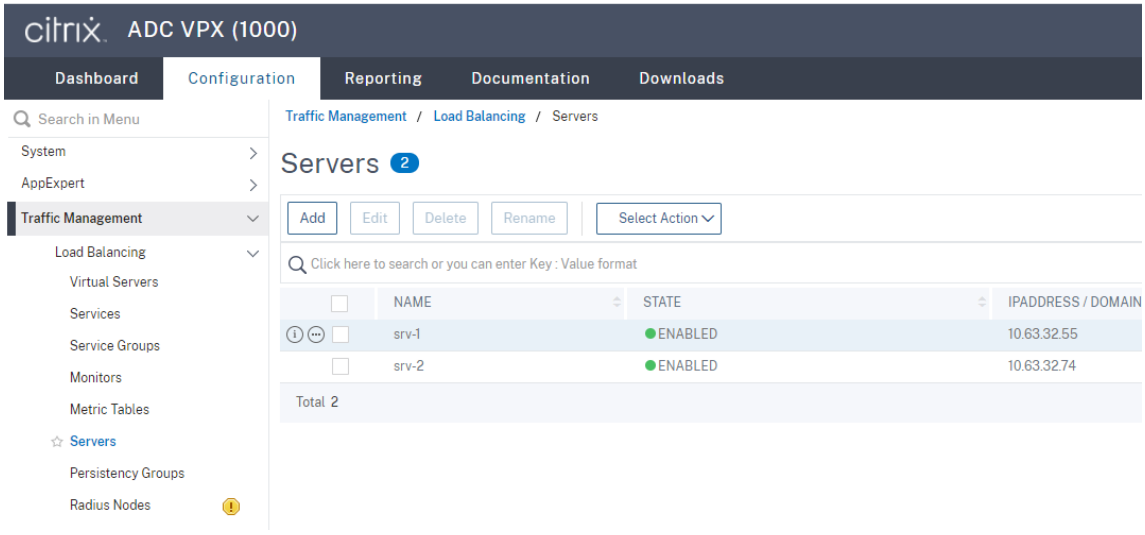
3. マシンのネットワークファイアウォールを無効にします。
4. Session Recording データベースをインストールした SQL Server で、すべての Session Recording サーバーマシンアカウントを共有 Session Recording データベースに追加し、db_owner権限を割り当てます。例:

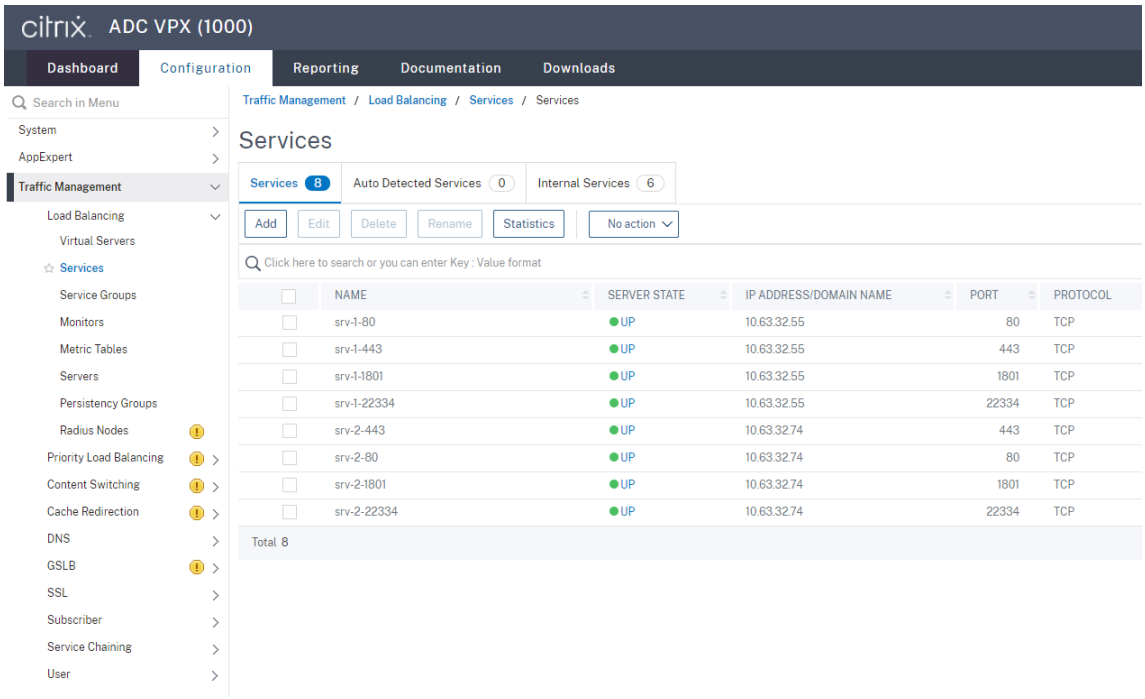


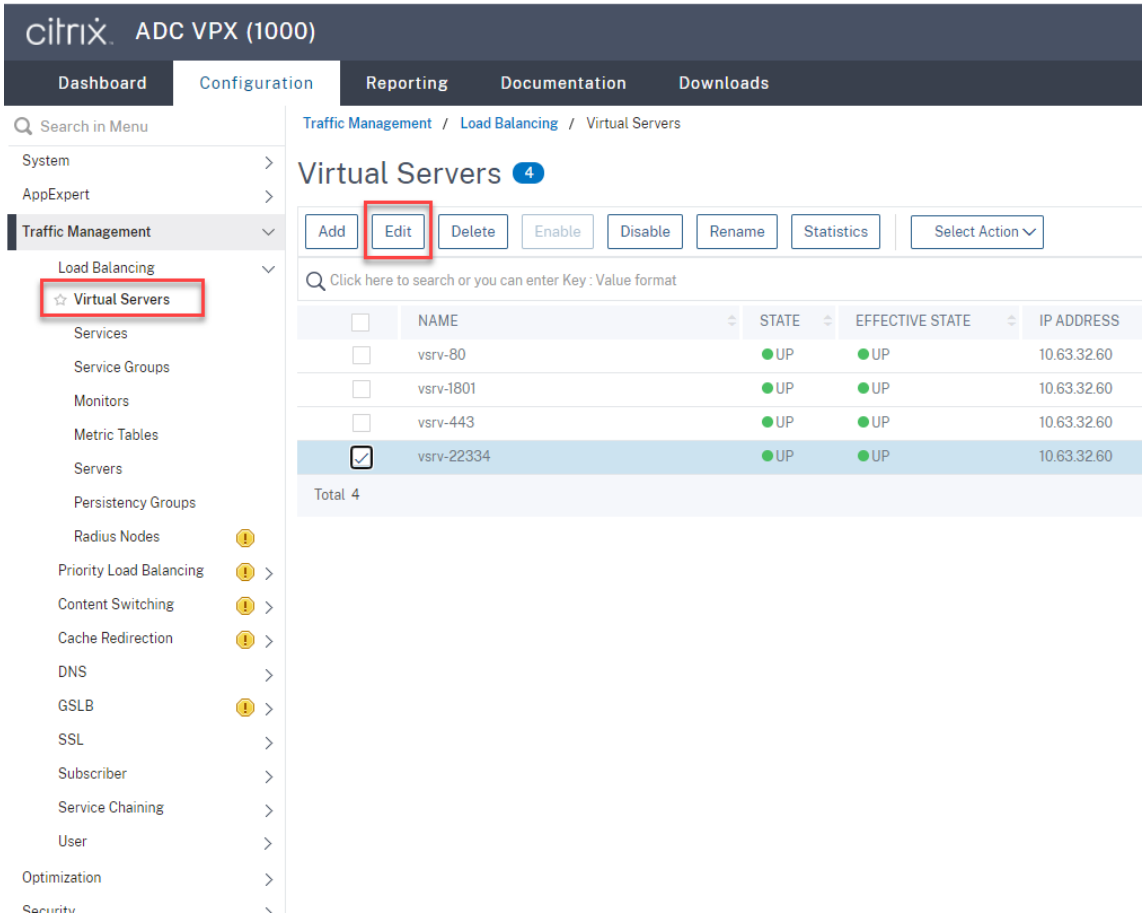


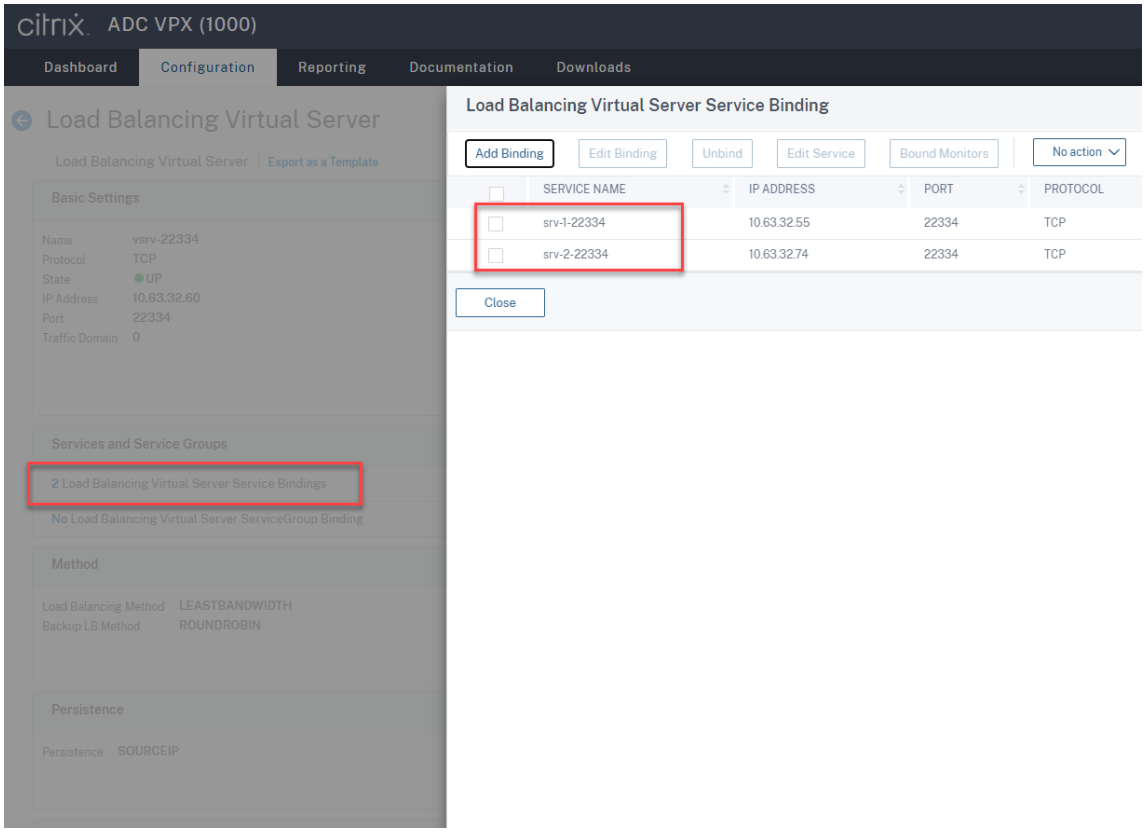
5. 新しい Session Recording サーバーのマシンアカウント（例：`LB\SRServer2$`）と、録画の格納場所および復元フォルダー（例：`SessionRecording`および`SessionRecordingsRestored`）の読み取り/書き込み権限を共有します。ドル記号`$`は必要です。

6. 手順 3を繰り返して、新しい Session Recording サーバー用の負荷分散サービスを追加し、既存の仮想サーバーを編集して、負荷分散サービスにバインドを追加します。仮想サーバーを追加する必要はありません。例:









7. Session Recording 承認コンソールの構成ファイル`SessionRecordingAzManStore.xml`を既存の Session Recording サーバーから新しい Session Recording サーバーにコピーします。ファイルは`<Session Recording Server installation path>\App_Data`にあります。

8. 新しい Session Recording サーバーに MSMQ over HTTP または MSMQ over HTTPS を使用するには、次の手順を実行して、現在機能している Session Recording サーバーのレジストリ設定をインポートします。

   既存の Session Recording サーバー（例: `SRServer1`）で、`powershell.exe -file SrServerConfigurationSync.ps1 -Action Export - ADCHost <ADCHost >`コマンドを実行します。ここで`<ADCHost>`は、Citrix ADC VIP アドレスの完全修飾ドメイン名です。エクスポートされたレジストリファイル `SrServerConfig.reg`が生成されます。

   `SrServerConfig.reg`ファイルを新しい Session Recording サーバーにコピーし、`powershell.exe -file SrServerConfigurationSync.ps1 -Action Import,AddRedirection - ADCHost <ADCHost>`コマンドを実行します。**EnableLB** 値は、`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`で新しい Session Recording サーバーのレジストリキーに追加され、`sr_lb_map.xml`ファイルは`C:\Windows\System32\msmq\Mapping`の下に追加されます。

9. 手順を繰り返して、別の Session Recording サーバーを追加します。

トラブルシューティング

- Session Recording サーバーに CNAME レコードまたは ALIAS レコードを使用する場合、セッションは録画されません。詳しくは、Knowledge Center の記事CTX248554を参照してください。
- 録画ファイルはローカルに格納できますが、UNC パスに格納することはできません。この問題に対処するには、Citrix Session Recording ストレージマネージャーサービスの開始モードを自動（遅延開始）に変更します。

Azure で Session Recording を展開して負荷分散する

February 20, 2024

前提条件

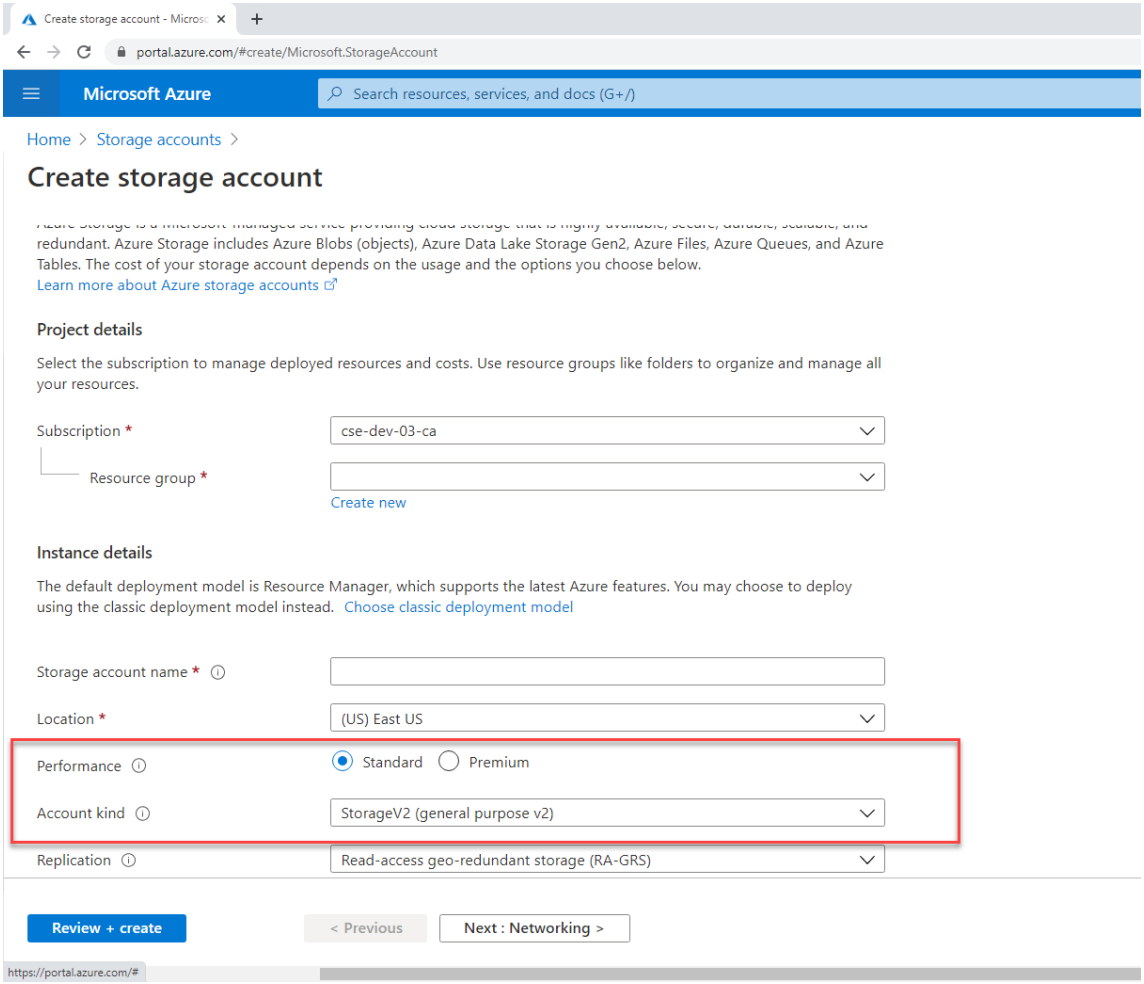
- Azure に Citrix Virtual Apps and Desktops または Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）をインストールしてある。
- Azure アカウントを持っている。

手順 1：Citrix Virtual Apps and Desktops インストーラーを Azure にアップロードする

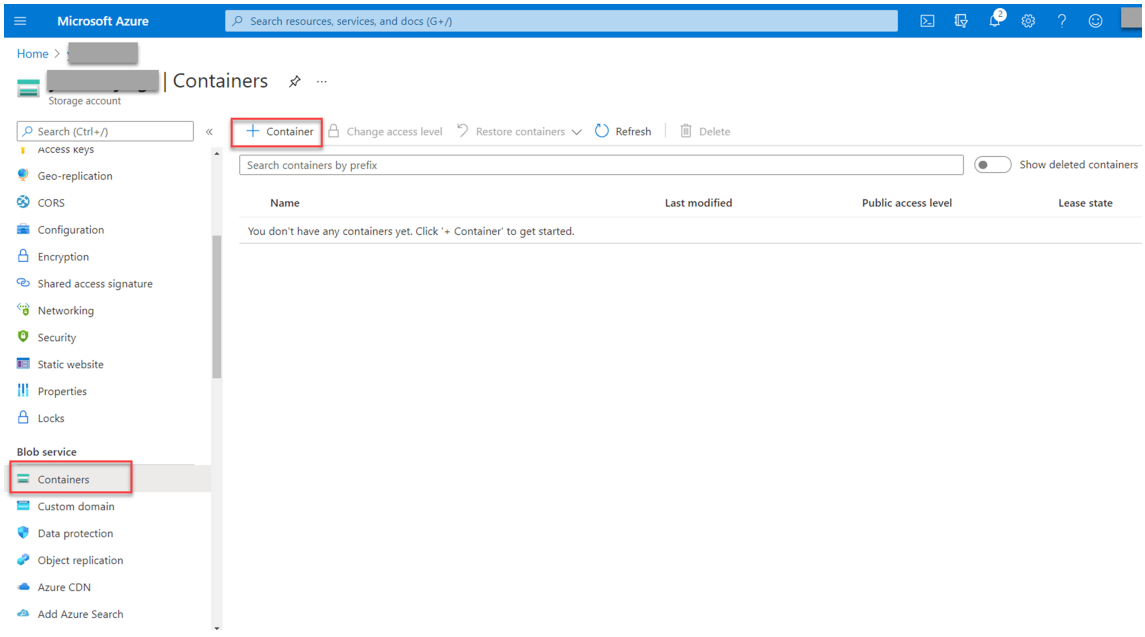
> 注：
>
> Citrix アカウント資格情報を使用して、Citrix Virtual Apps and Desktops のダウンロードページにアクセスして、製品の ISO ファイルを Azure の VM にダウンロードする場合は、手順 1 をスキップしてください。

1. Azure Portalで ［**general-purpose v2**］ストレージアカウントを作成し、デフォルトのパフォーマンスの階層である ［**Standard**］のままにします。

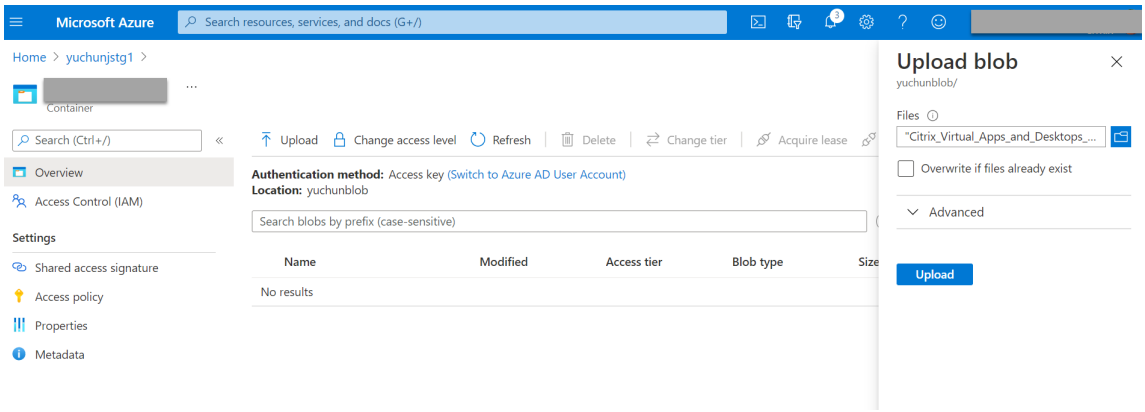
   Azure Storage へのすべてのアクセスは、ストレージアカウントを経由します。



2. 新しいストレージアカウントに移動し、［**Blob service**］セクションで ［**Containers**］を選択してコンテナを作成します。



3. Citrix Virtual Apps and Desktops インストーラーをコンテナにアップロードします。

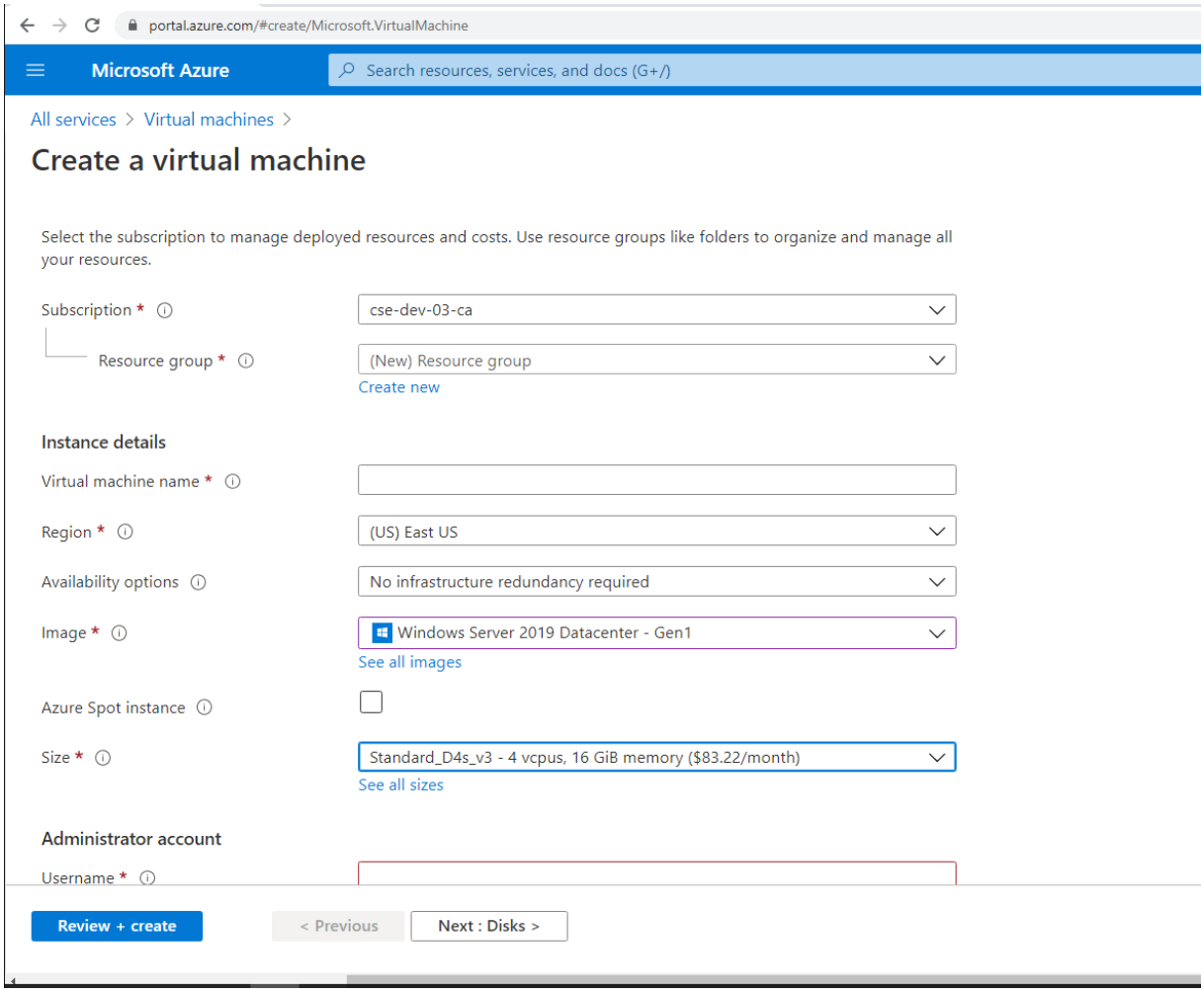


手順 **2**：**Azure** ポータルで **SQL Managed Instance** を作成する

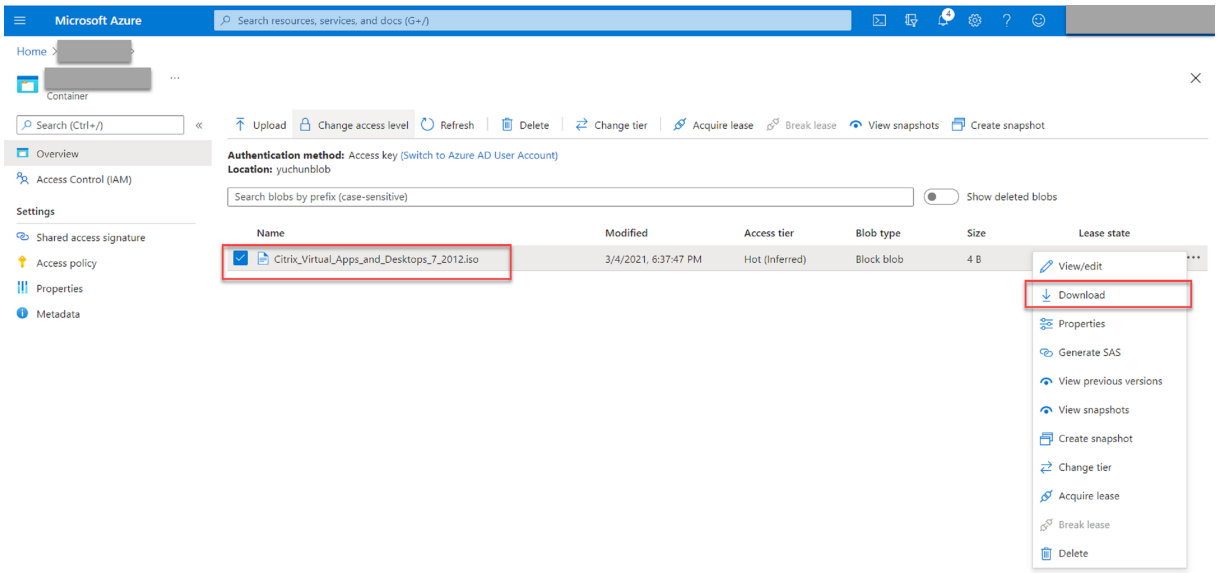
詳しくは、Azure SQL マネージドインスタンスの作成を参照してください。

手順 **3**：**Azure** 仮想マシン（**VM**）を作成する

[Image] で［**Windows Server 2019 Datacenter -Gen1**］を選択し、[Size] で［**Standard_D4as_v4 -4 vcpus, 16GiB memory**］を選択します。詳しくは、「Azure Portal で Windows 仮想マシンを作成する」参照してください。



手順 **4**：リモートデスクトップにし、**Citrix Virtual Apps and Desktops** インストーラーを **Azure** にアップロードする



手順 **5**：インストーラーを実行して、**Azure VM** に **Session Recording** コンポーネントをインストールする

詳しくは、「Session Recording Administration コンポーネントのインストール」を参照してください。

手順 **6**：録画を保存するための **Azure** ファイル共有を構成する

録画を保存するための Azure ファイル共有を作成するには、次の手順を実行します：

1. Azure Portalで、ストレージアカウントを作成してから、Azure ファイル共有を作成します。

   クイックスタートガイドについては、Azure Portal を使用したAzure ファイル共有の作成および管理を参照してください。次の表は、検討すべきお勧めの構成です。

録画ファイルサイズ（MB/時間）	1 日あたりの録画されたセッション数	ファイル共有タイプ	ファイル共有クォータ（TB）	Session Recording サーバーの数	Session Recording サーバーのサイズ
< 6.37	< 1,000	HDD Standard (StorageV2)	2	1	Standard D4as_v4
< 6.37	1,000～2,000	SSD Premium	3	1	Standard D4as_v4
< 6.37	2,000～3,000	SSD Premium	5	1	Standard D4as_v4

録画ファイルサイズ（MB/時間）	1 日あたりの録画されたセッション数	ファイル共有タイプ	ファイル共有クォータ（TB）	Session Recording サーバーの数	Session Recording サーバーのサイズ
< 6.37	3,000～4,000	SSD Premium	6	1	Standard D4as_v4
約 10	< 1,000	HDD Standard (StorageV2)	3	1	Standard D4as_v4
約 10	1,000～2,500	SSD Premium	6	1	Standard D4as_v4
約 10	2,500～4,000	SSD Premium	10	2	Standard D4as_v4

ファイル共有クォータは、1 日あたり 8 時間、1 か月あたり 23 営業日、各録画ファイルの 1 か月の保有期間に基づいて計算されます。

2. Session Recording サーバーをインストールしたホストに、Azure ファイル共有の資格情報を追加します。

   a) 管理者としてコマンドプロンプトを起動し、ドライブを **<Session Recording** サーバーのパス **>\Bin** フォルダーに変更します。

   デフォルトでは、Session Recording サーバーは`C:\Program Files\Citrix\SessionRecording\Server`にインストールされています。

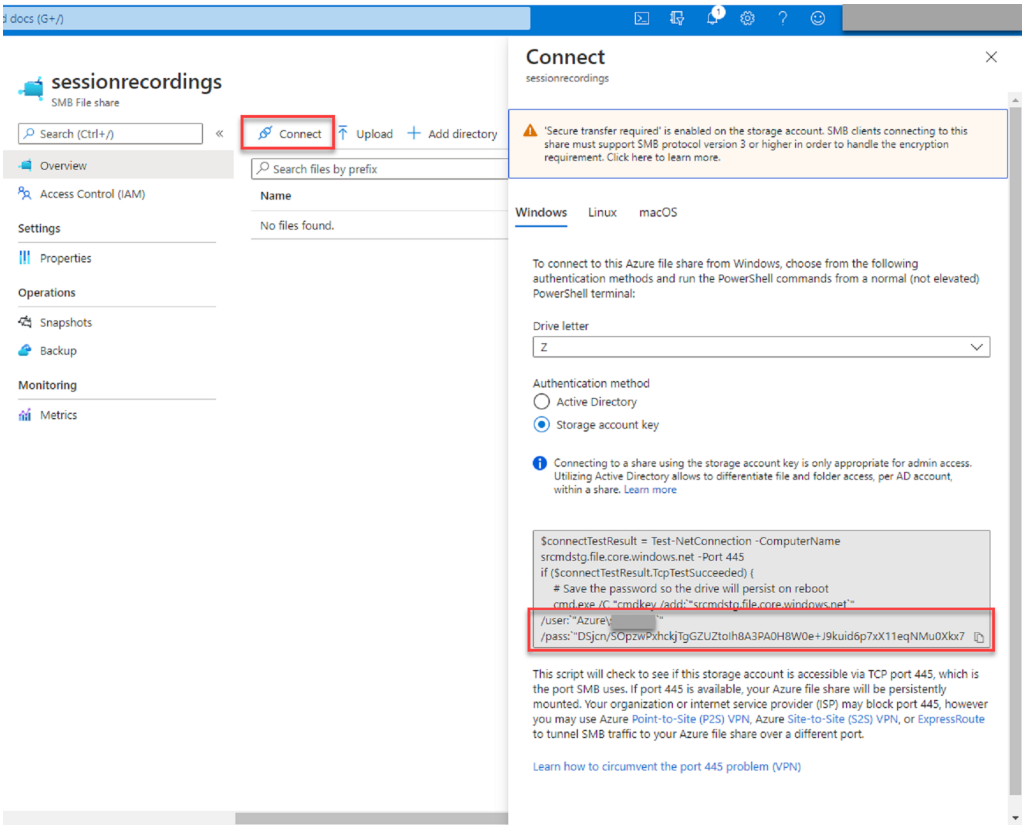
   b)「**SsRecUtils.exe -AddAzureFiles <storageAccountName> <fileShareName> <accesskey>**」コマンドを実行します。

   各項目の意味は次のとおりです。

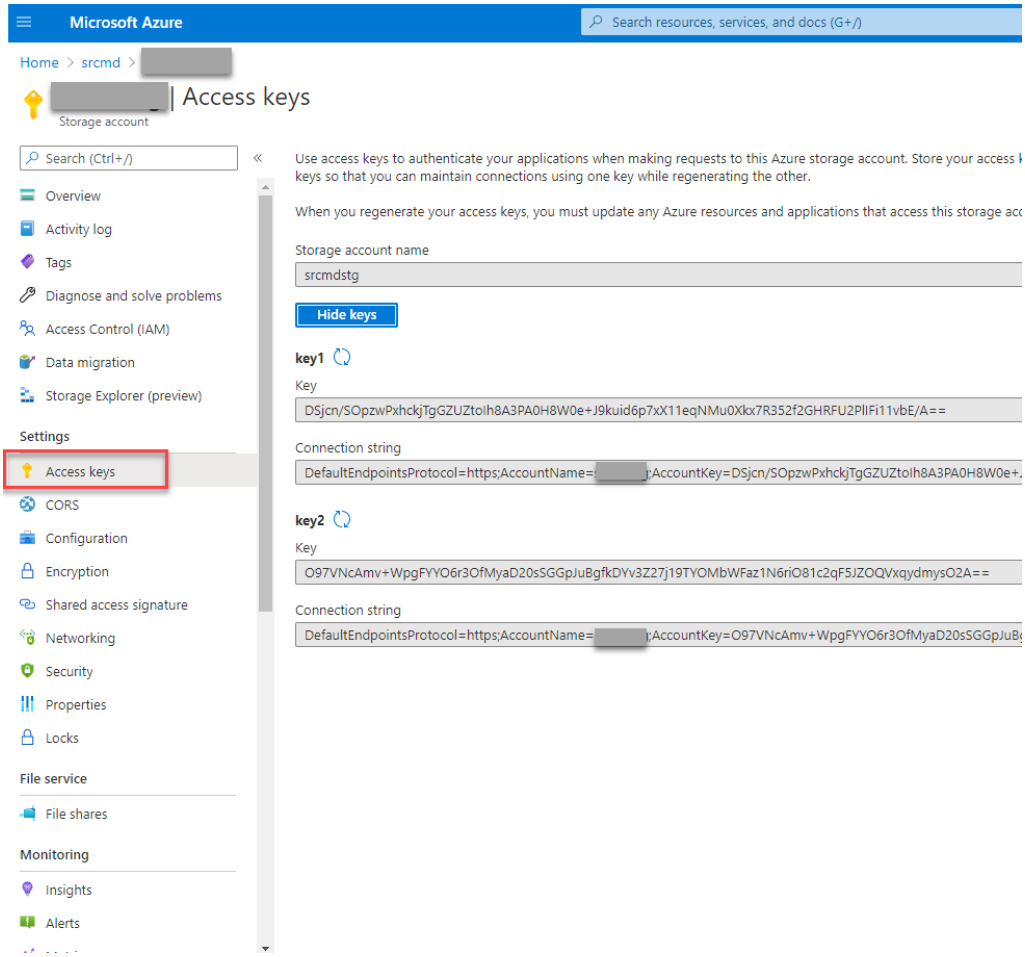
   - **<storageaccountname>** は、Azure のストレージアカウントの名前です。
   - **<filessharename>** は、ストレージアカウントに含まれるファイル共有の名前です。
   - **<accesskey>** は、ファイル共有へのアクセスに使用できるストレージアカウントキーです。

   ストレージアカウントキーを取得するには、次の 2 つの方法があります:

   - ストレージアカウントキーは、ファイル共有ページの［**Connect**］アイコンをクリックしたときに表示される接続文字列から取得できます。



- ストレージアカウントページの左側のナビゲーションにある［**Access keys**］をクリックして、ストレージアカウントキーを取得することもできます。



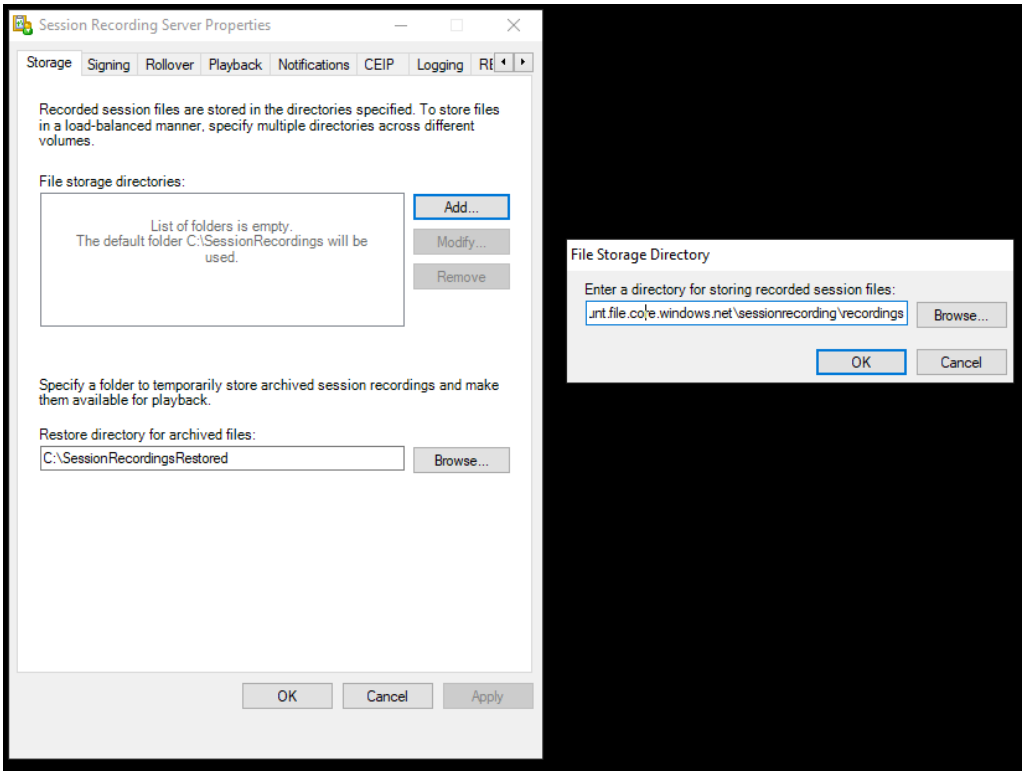
c) Session Recording サーバーをインストールしたホストに、Azure ファイル共有をマウントします。

i. [**Session Recording** サーバーのプロパティ] を開きます。

ii. [格納場所] タブで [追加] をクリックします。

iii. 次の形式で UNC パスを入力します: **\\<storageaccountname>.file.core.windows.net\<filessharena**

録画ファイルを保存する場所として、ファイル共有の下にあるサブフォルダーを指定します。そうすると、Session Recording サーバーが自動的にサブフォルダーを作成します。

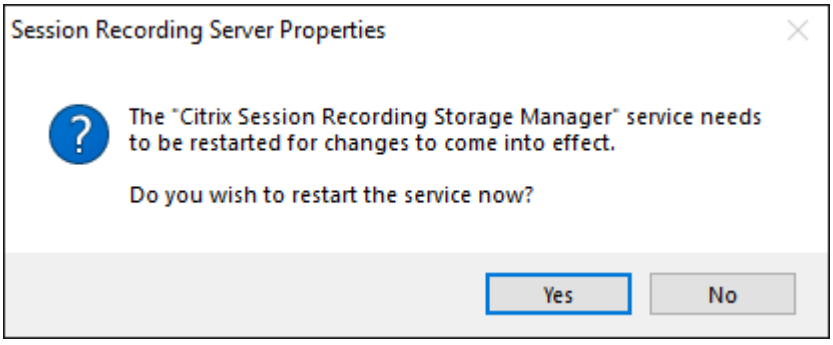


iv. ［ファイル格納フォルダー］ダイアログボックスで ［**OK**］をクリックします。

v. ［**Session Recording** サーバーのプロパティ］ウィンドウで ［適用］をクリックします。

vi. ［適用］がグレー表示になったら、［**OK**］をクリックします。

vii. Session Recording ストレージマネージャーサービスを再起動するよう求められたら、［はい］をクリックします。

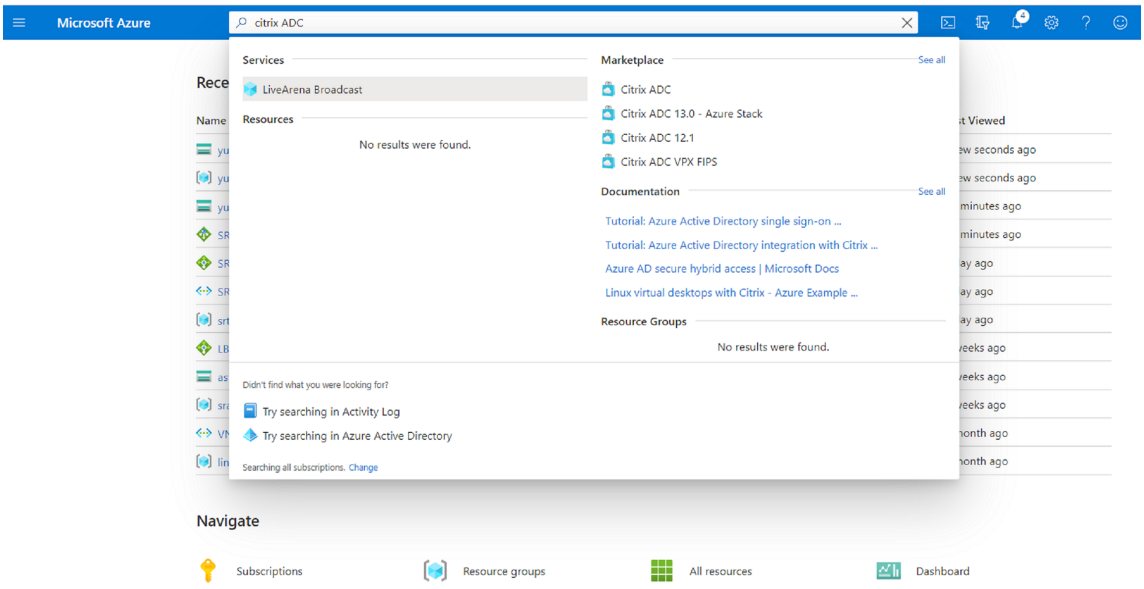


手順 **7**: ロードバランサーを追加する

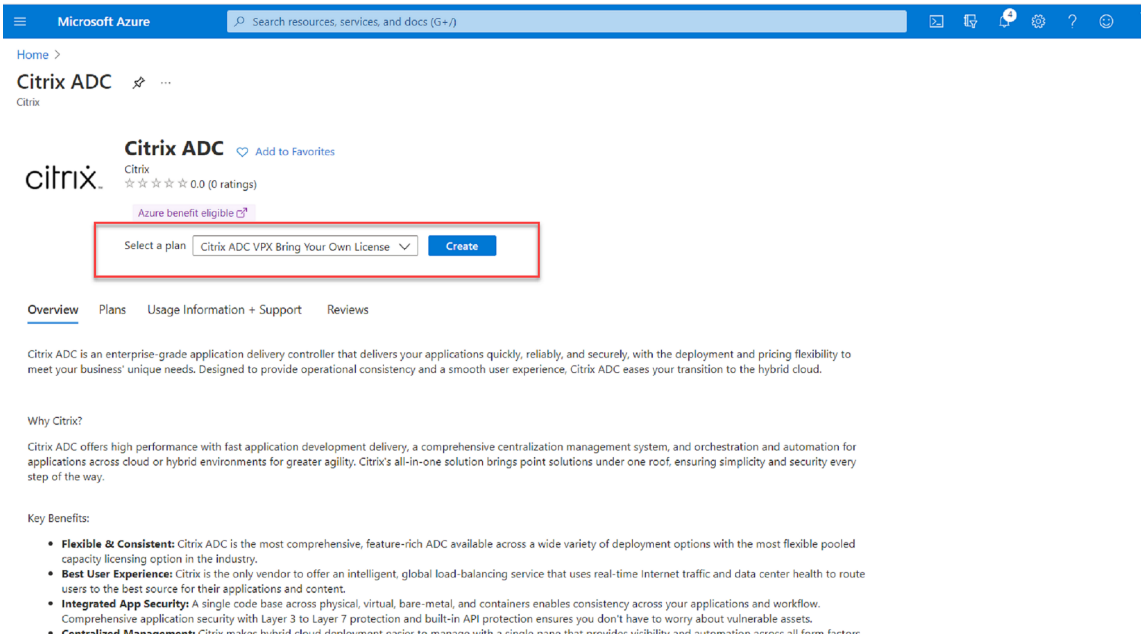
複数の Session Recording サーバーがある場合、それらの前にロードバランサーを追加することをお勧めします。Azure では、トラフィック要求の負荷分散をするためのオプションが多数用意されています。このセクションでは、Azure で Citrix ADC、Azure Load Balancer、Azure Application Gateway を作成するプロセスについて説明します。

オプション **1**: **Azure** で **Citrix ADC VPX** インスタンスを作成する

1. Azure Portalで、検索ボックスに「Citrix ADC」と入力します。

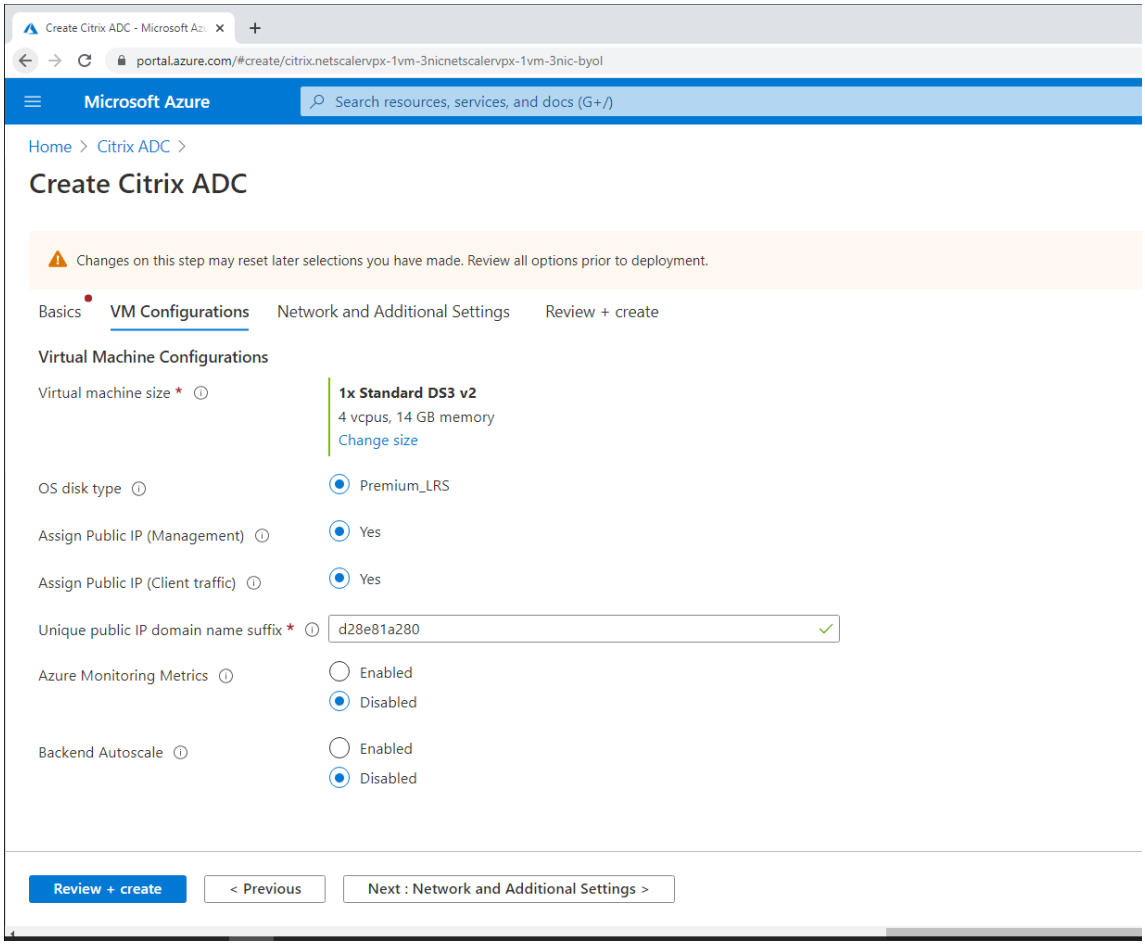


2. [**Citrix ADC VPX Bring Your Own License**] プランを選択し、[**Create**] をクリックします。



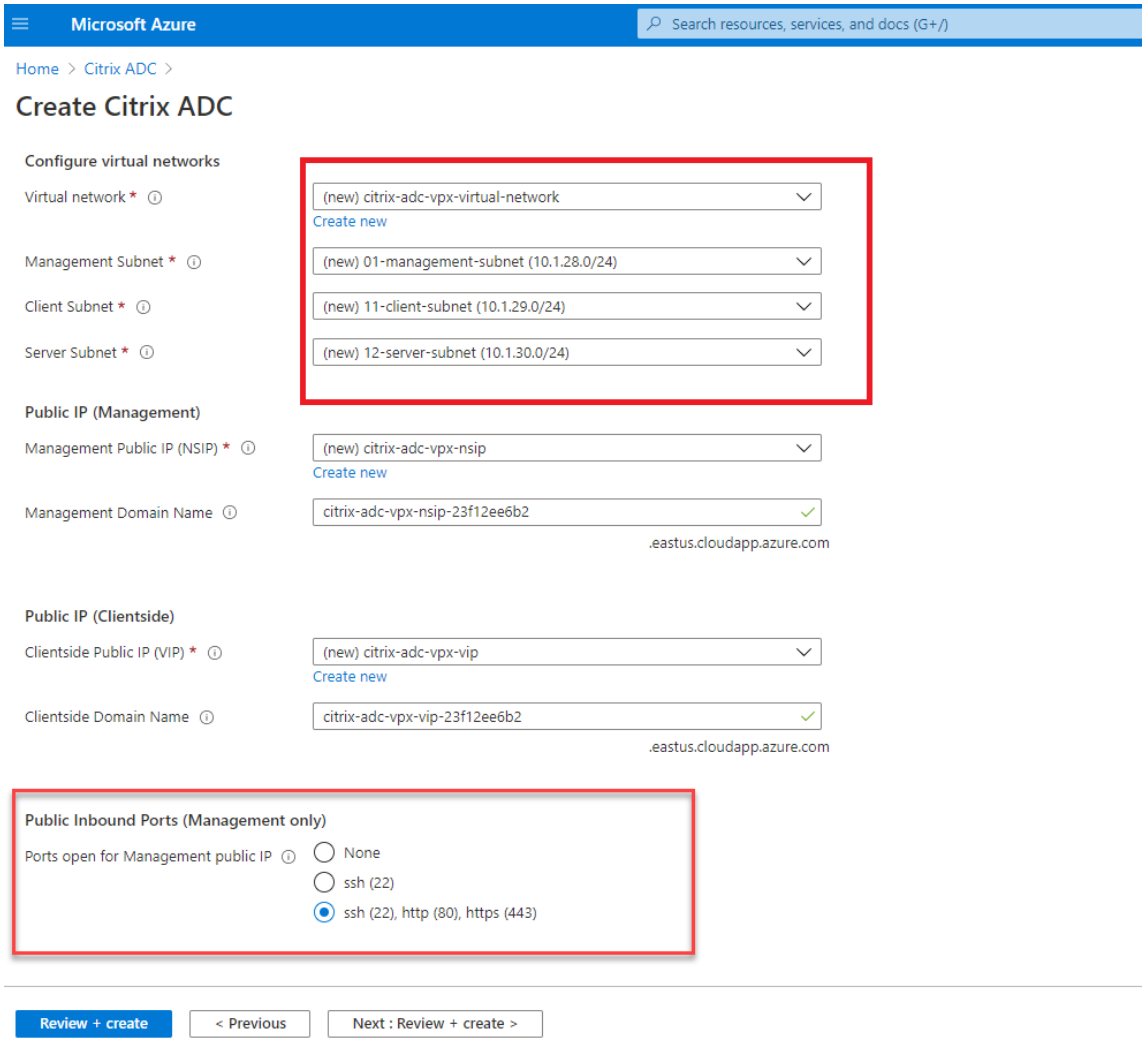
3. リソースグループを選択または作成し、[**Basics**] タブで他の設定を行います。

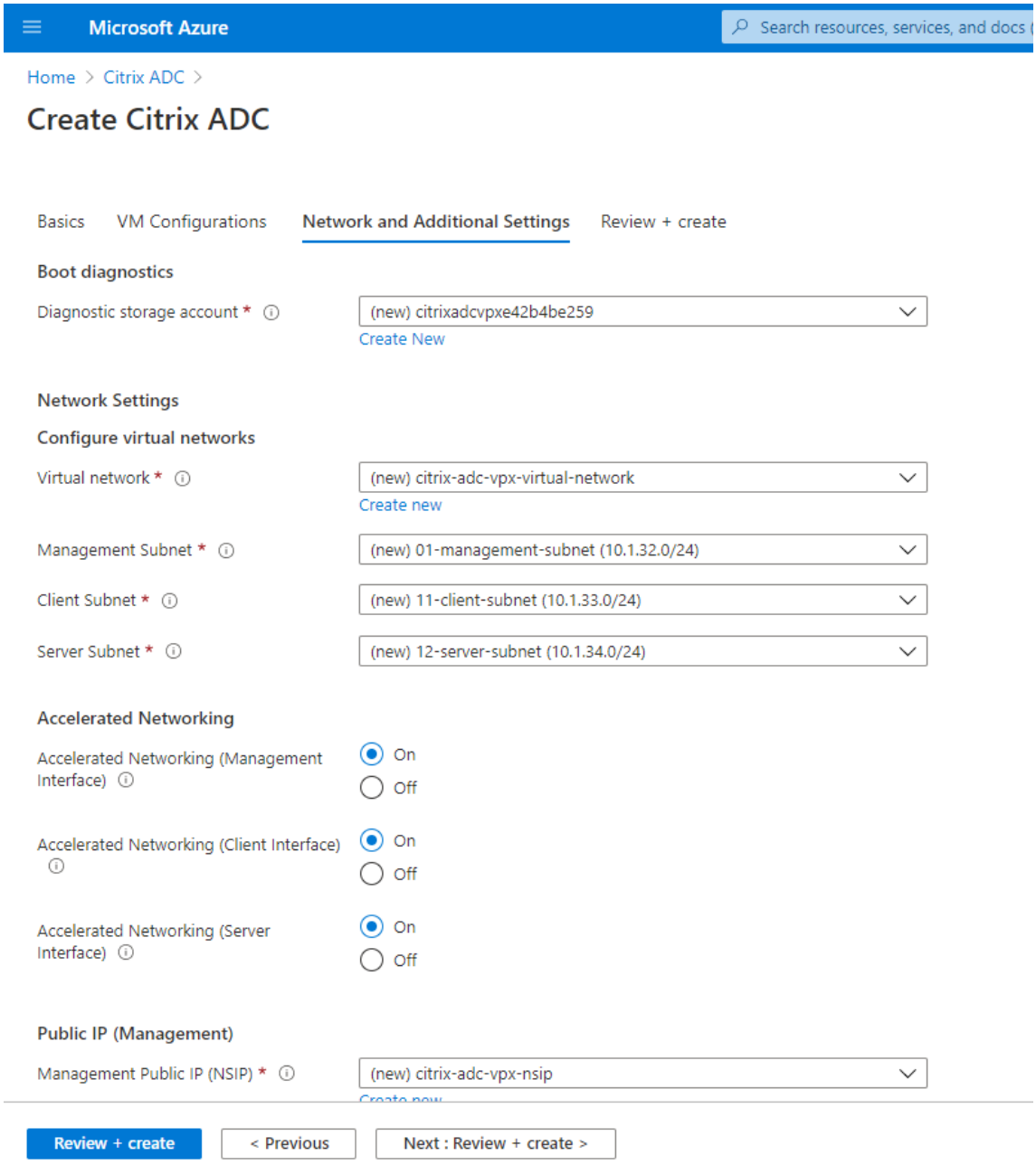
4. [VM Configurations] を設定します。



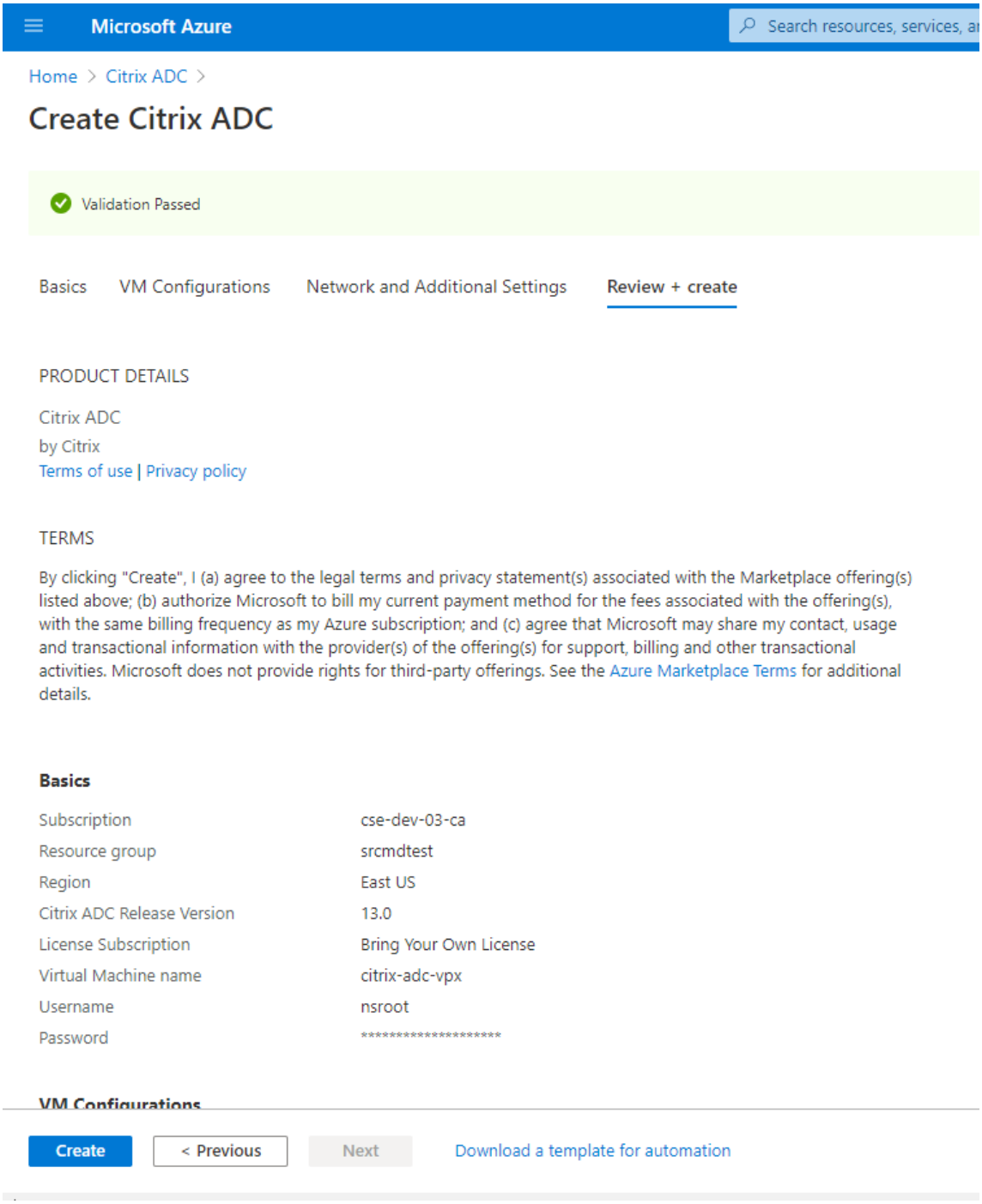
5. 必要に応じて、ネットワーク設定を確認および変更します。パブリック受信ポートには、[**ssh (22), http (80), https (443)**]を選択します。

   仮想ネットワークが自動的に作成されます。Session Recording 環境が既にインストールされている場合は、その仮想ネットワークとサーバーのサブネット設定を使用できます。





6. [**Next: Review + create**] をクリックして Citrix ADC VPX インスタンスを作成し、展開が完了するのを待ちます。

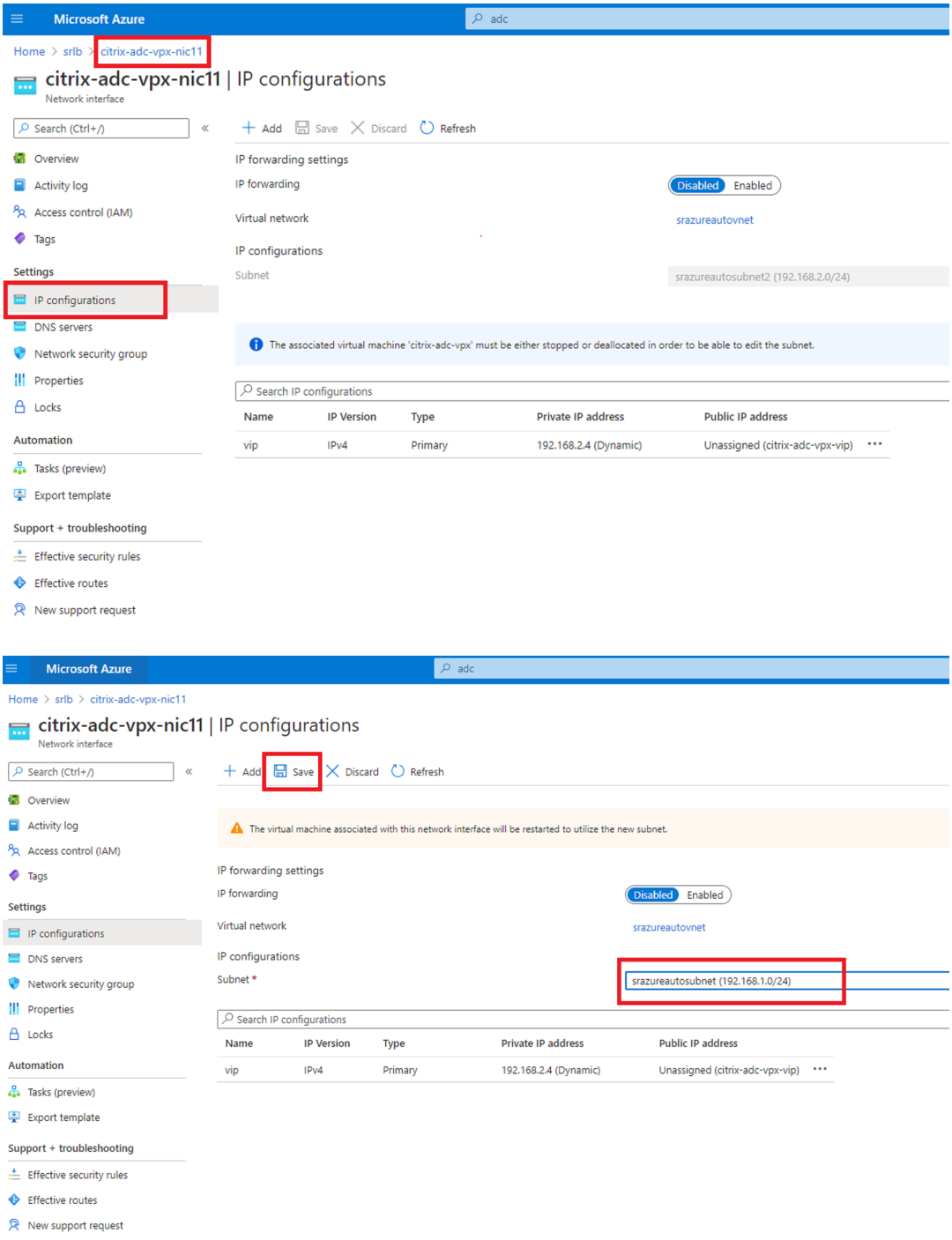


7. サブネット IP（SNIP）アドレスと Citrix ADC VIP アドレスを同じサブネット上に設定します。

   SNIP アドレスと VIP アドレスは同じサブネット上にある必要があります。この例では、VIP アドレスを SNIP アドレスのサブネット上に設定します。

   a) **citrix-adc-vpx** 仮想マシンを停止します。

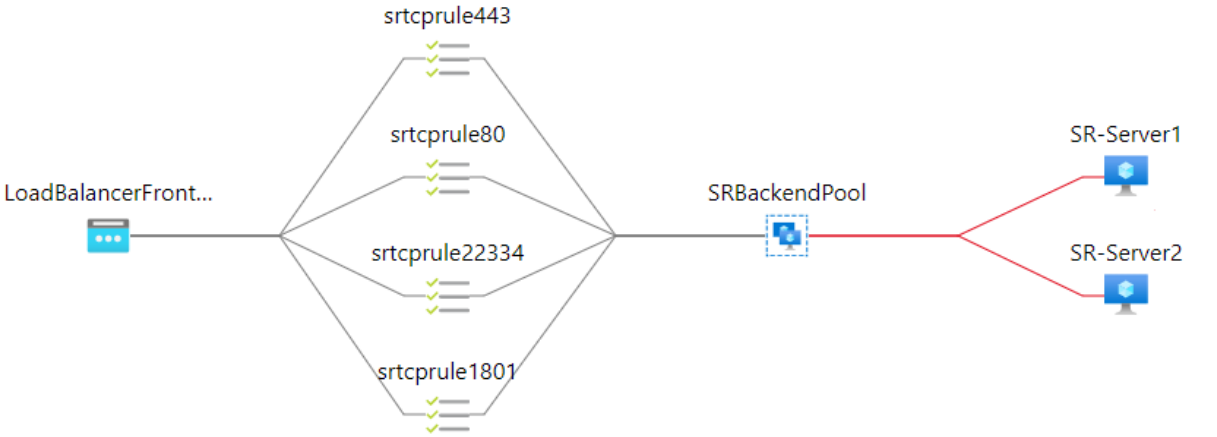
   b) VIP アドレスのサブネットを変更します。



c) **citrix-adc-vpx** 仮想マシンを起動します。

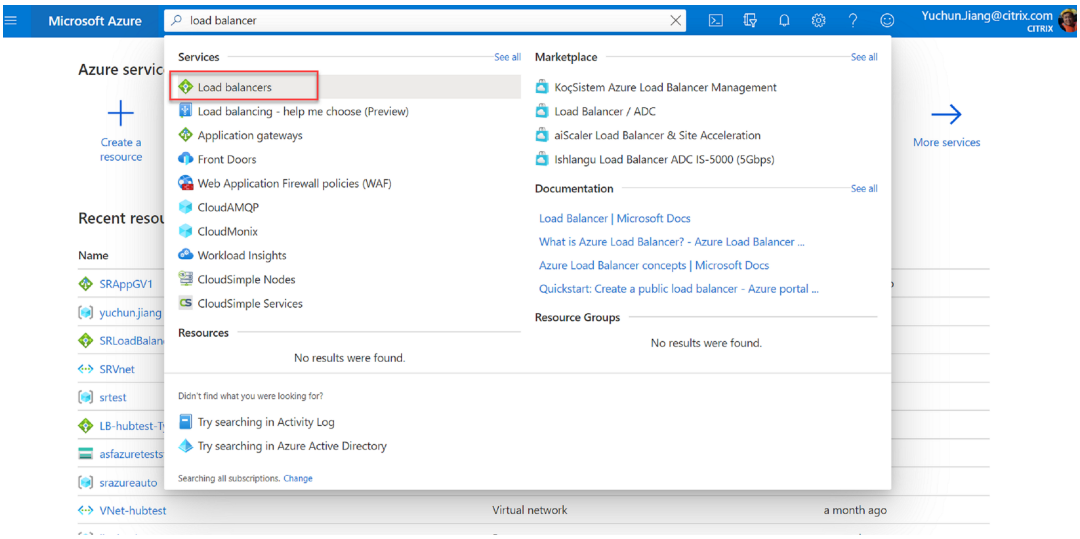
オプション **2**: **Azure Load Balancer** を作成する

Azure Load Balancer は、TCP パススルーサービスです。次の図は、TCP パススルーによる負荷分散を示しています。



1. Azure Load Balancer を作成します。

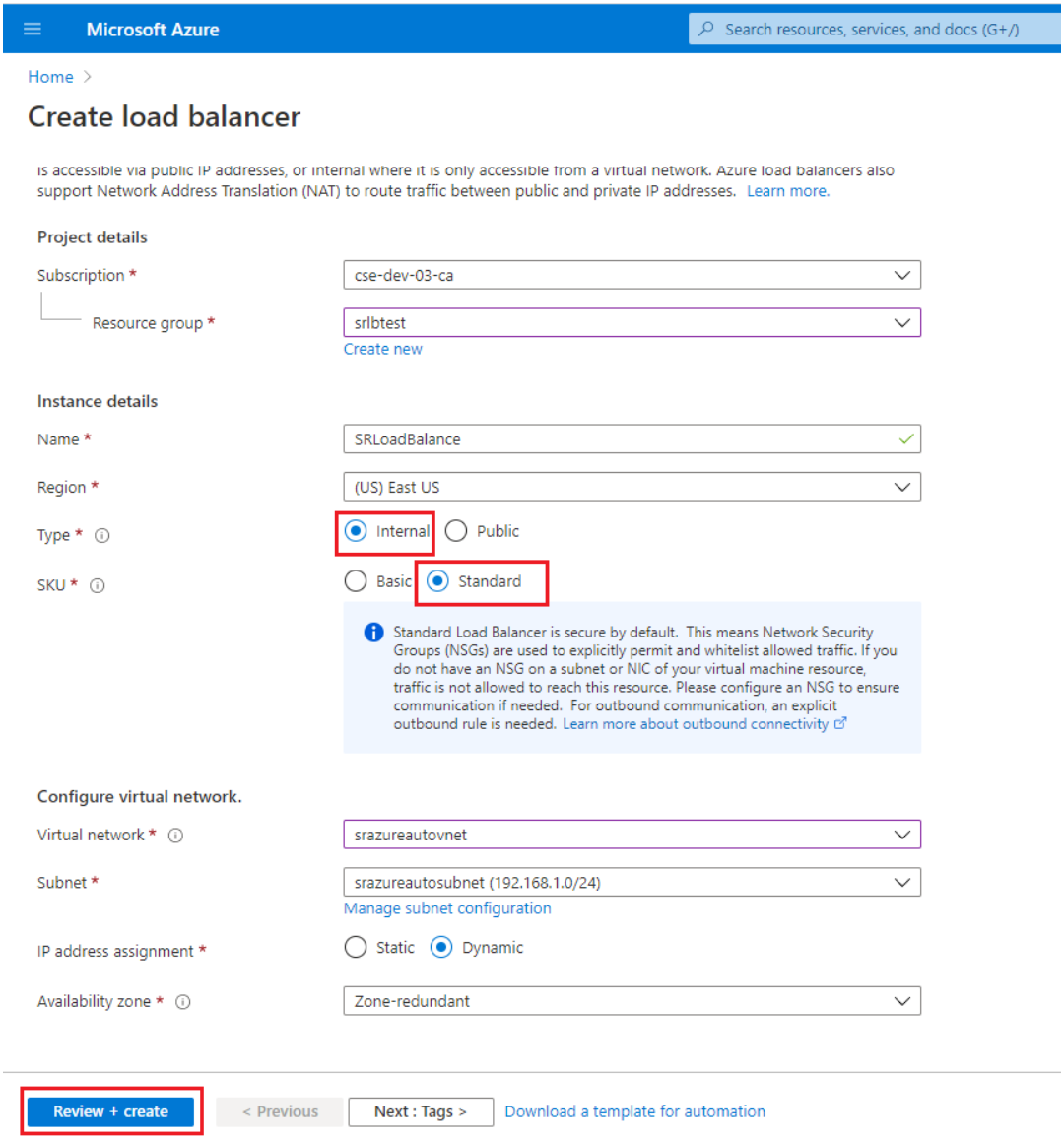
   a) Azure Portal で検索し、［**Marketplace**］で ［**Load Balancers**］を選択します。



［**Create load balancer**］ページの ［**Basics**］タブで、次の表のとおりに設定します:

設定	値
Subscription	サブスクリプションを選択します。
Resource group	たとえば、前に作成した ［**srlbtest**］を選択します。
名前	「**SRLoadBalance**」と入力します。
リージョン	［**(US) East US**］を選択します。
種類	［**Internal**］を選択します。
SKU	［**Standard**］を選択します。

設定	値
仮想ネットワーク	たとえば、前に作成した［**srazureautovnet**］を選択します。
Subnet	たとえば、前に作成した［**srazureautosubnet**］を選択します。
IP address assignment	［**Dynamic**］を選択します。
アベイラビリティゾーン	［**Zone-redundant**］を選択します。

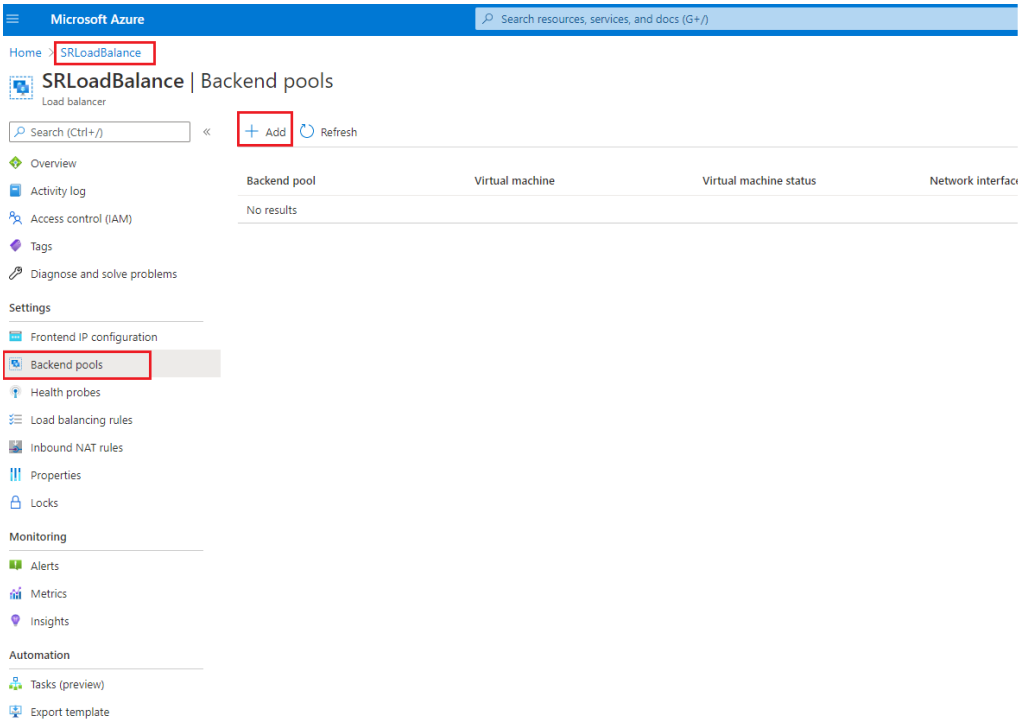


b) バックエンドプール、ヘルスプローブ、負荷分散の規則などのロードバランサーリソースを追加します。

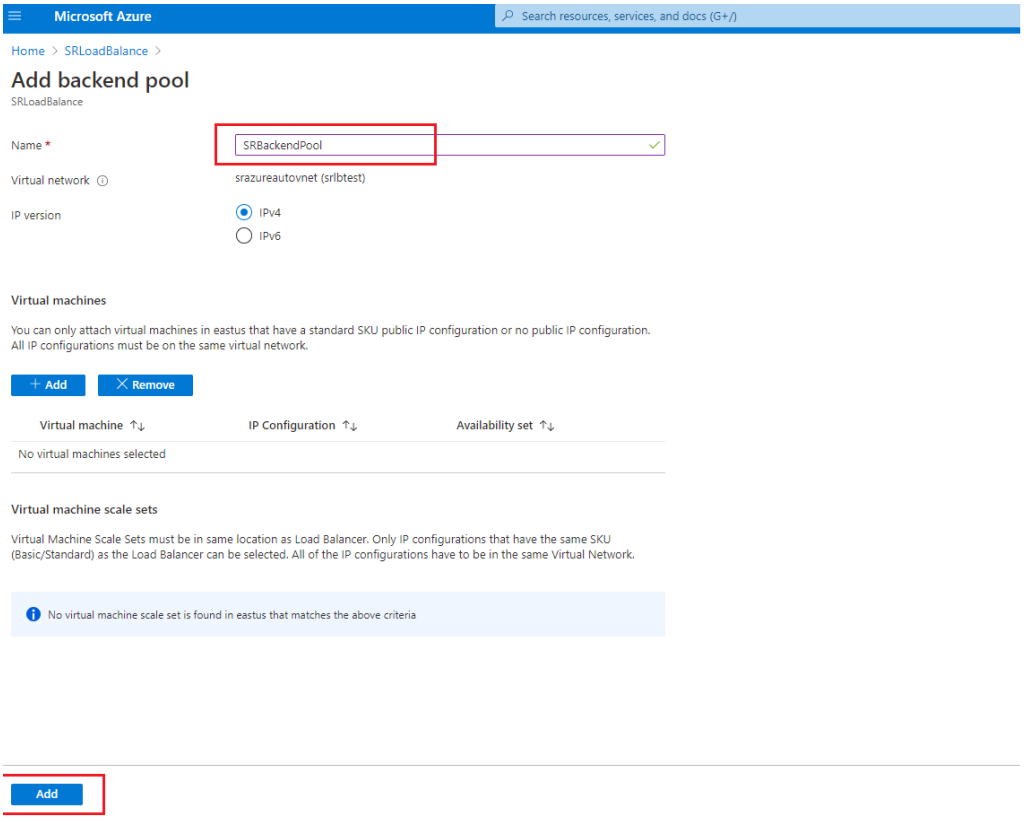
- バックエンドプールを追加します。

  リソースリストから、作成したロードバランサーを選択し、左側のナビゲーションで［**Backend**

pools］をクリックします。［**Add**］をクリックして、バックエンドプールを追加します。

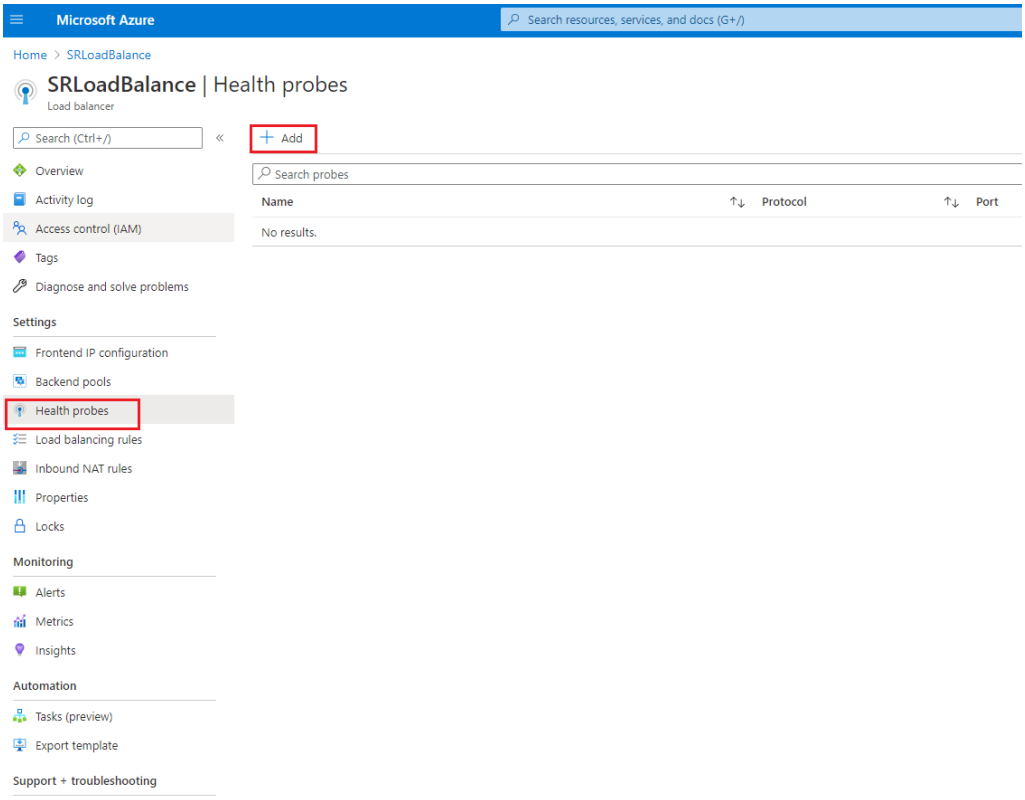


新しいバックエンドプールの名前を入力してから、［**Add**］をクリックします。

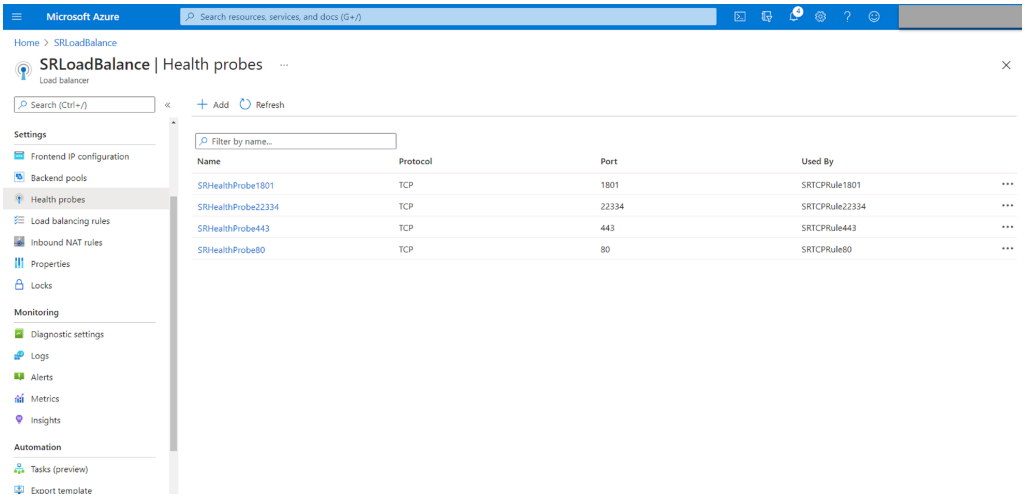


- ヘルスプローブを追加します。

リソースリストから、作成したロードバランサーを選択し、左側のナビゲーションで［**Health probes**］をクリックします。



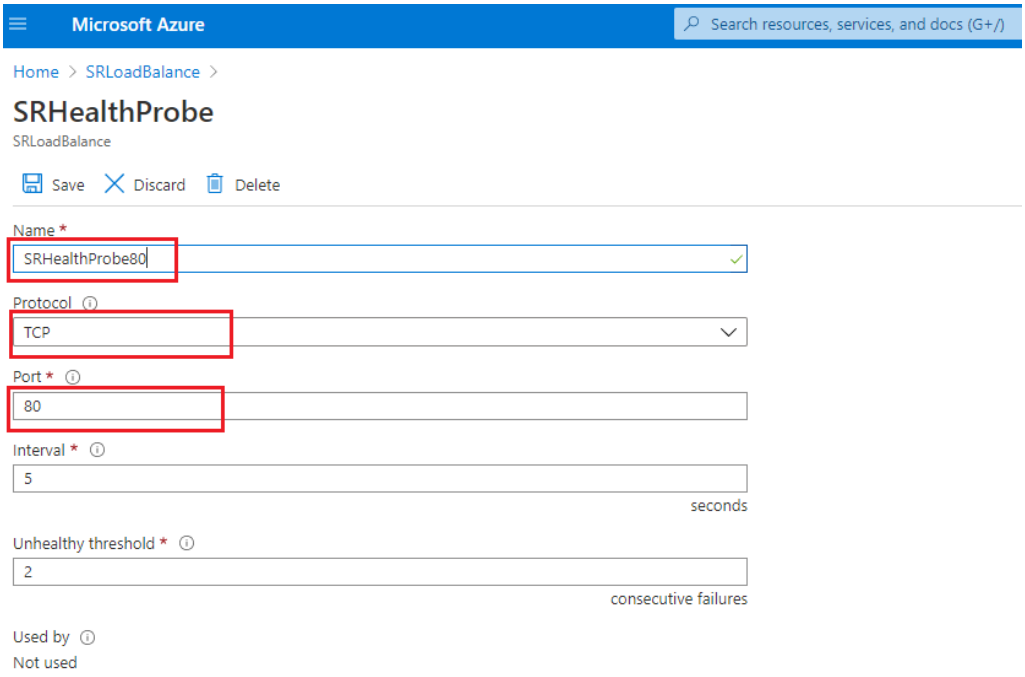
［**Add**］をクリックして、ポート 80、22334、1801、443 にヘルスプローブを追加します。



たとえば、次の設定を使用して、ポート 80 にヘルスプローブを作成します。

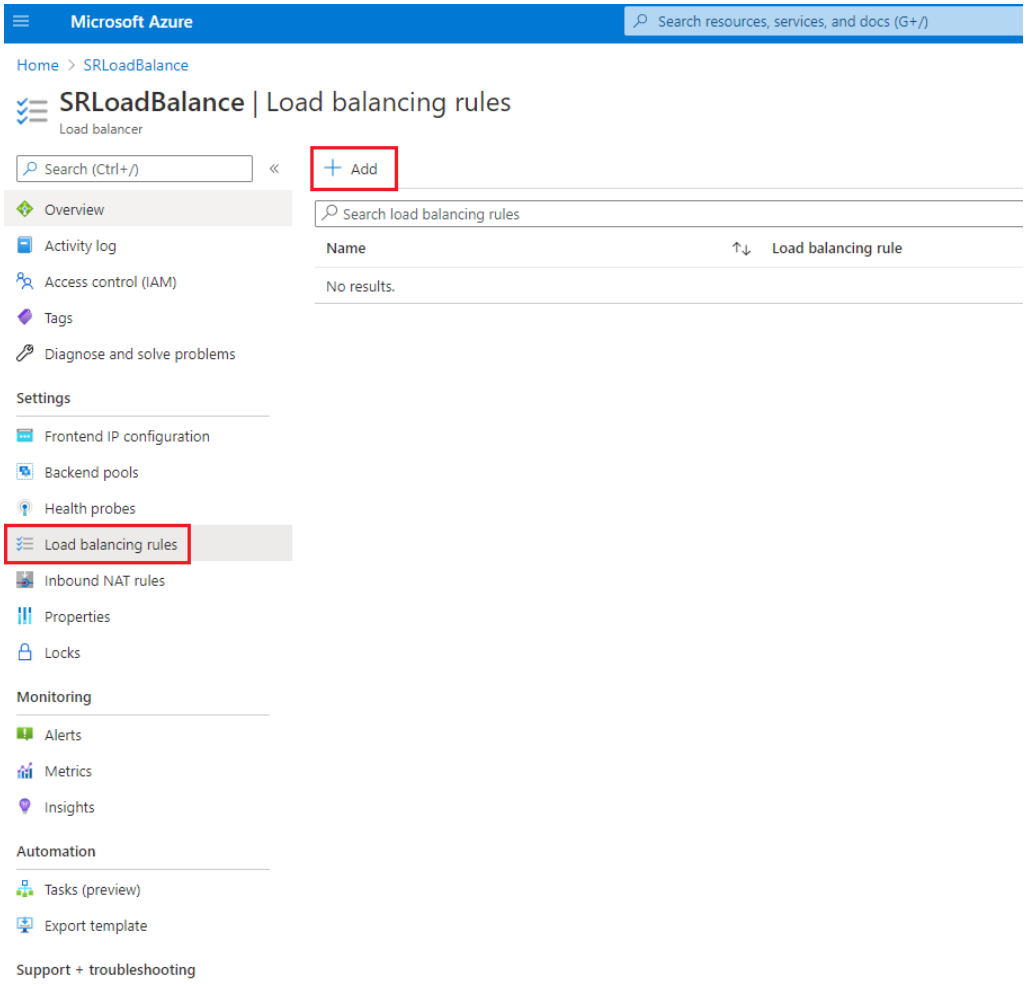
設定	値
名前	「**SRHealthProbe80**」と入力します。
Protocol	［**TCP**］を選択します。

設定	値
ポート	「**80**」と入力します。
Interval	5
Unhealthy threshold	VM が異常であると判断される前に必ず発生する、異常なしきい値、または連続するプローブエラーの数として、2 を選択します。

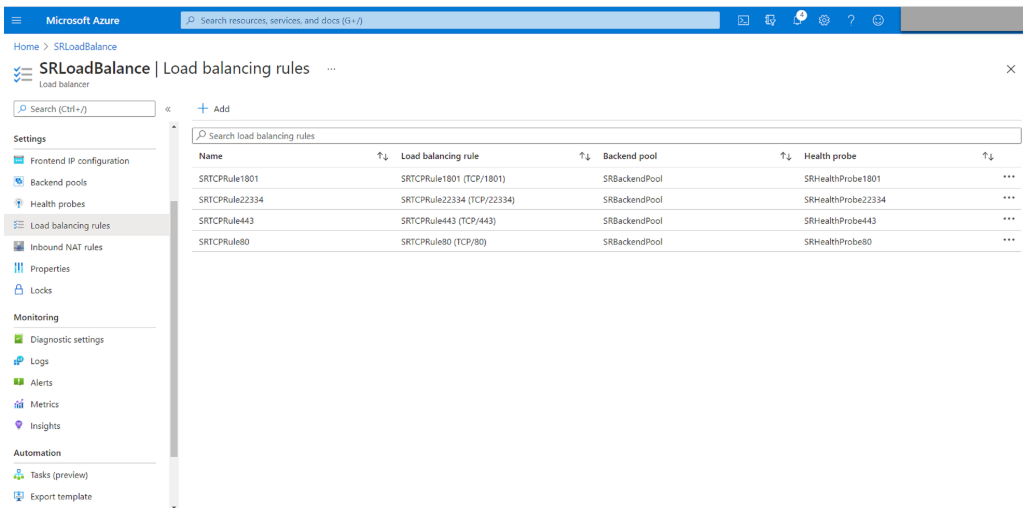


- 負荷分散の規則を追加します。

  リソースリストから、作成したロードバランサーを選択し、左側のナビゲーションで［**Load balancing rules**］をクリックします。［**Add**］をクリックして、負荷分散の規則を追加します。

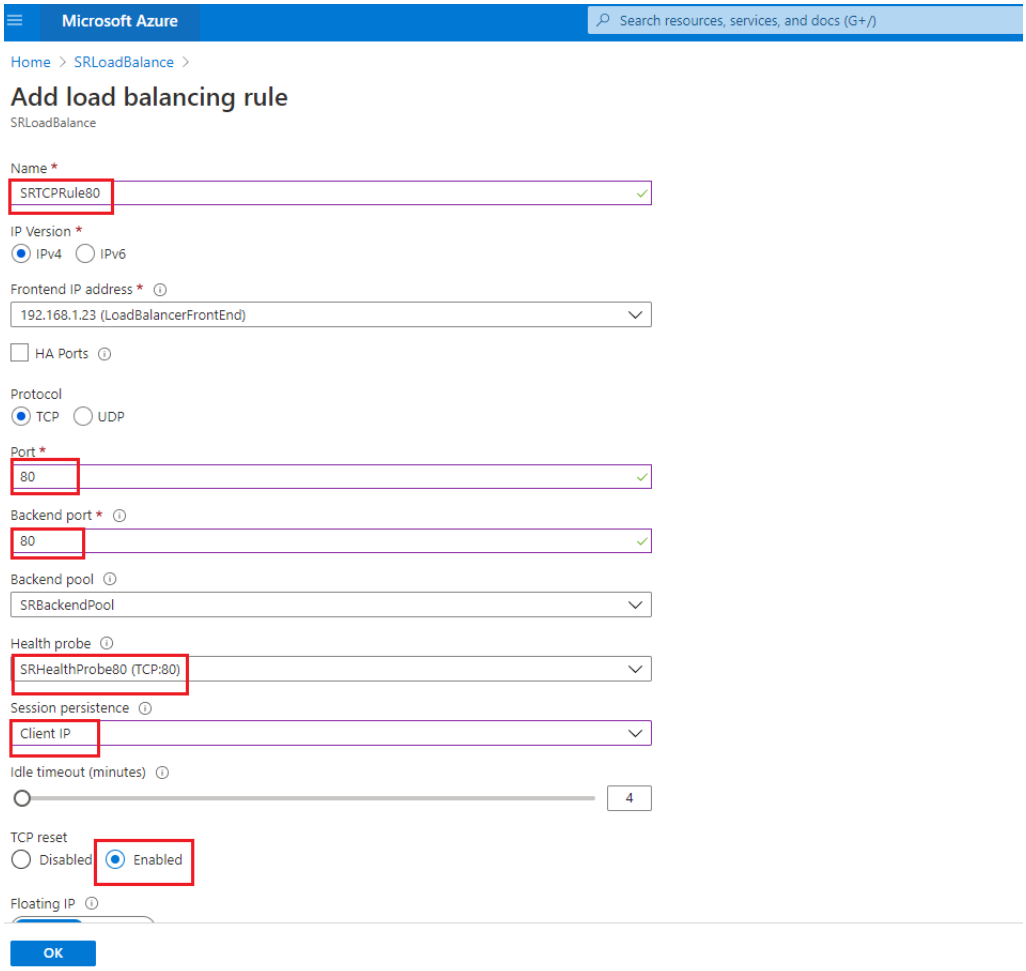


[**Add**] をクリックして、ポート 80、22334、1801、443 の負荷分散の規則を追加します。

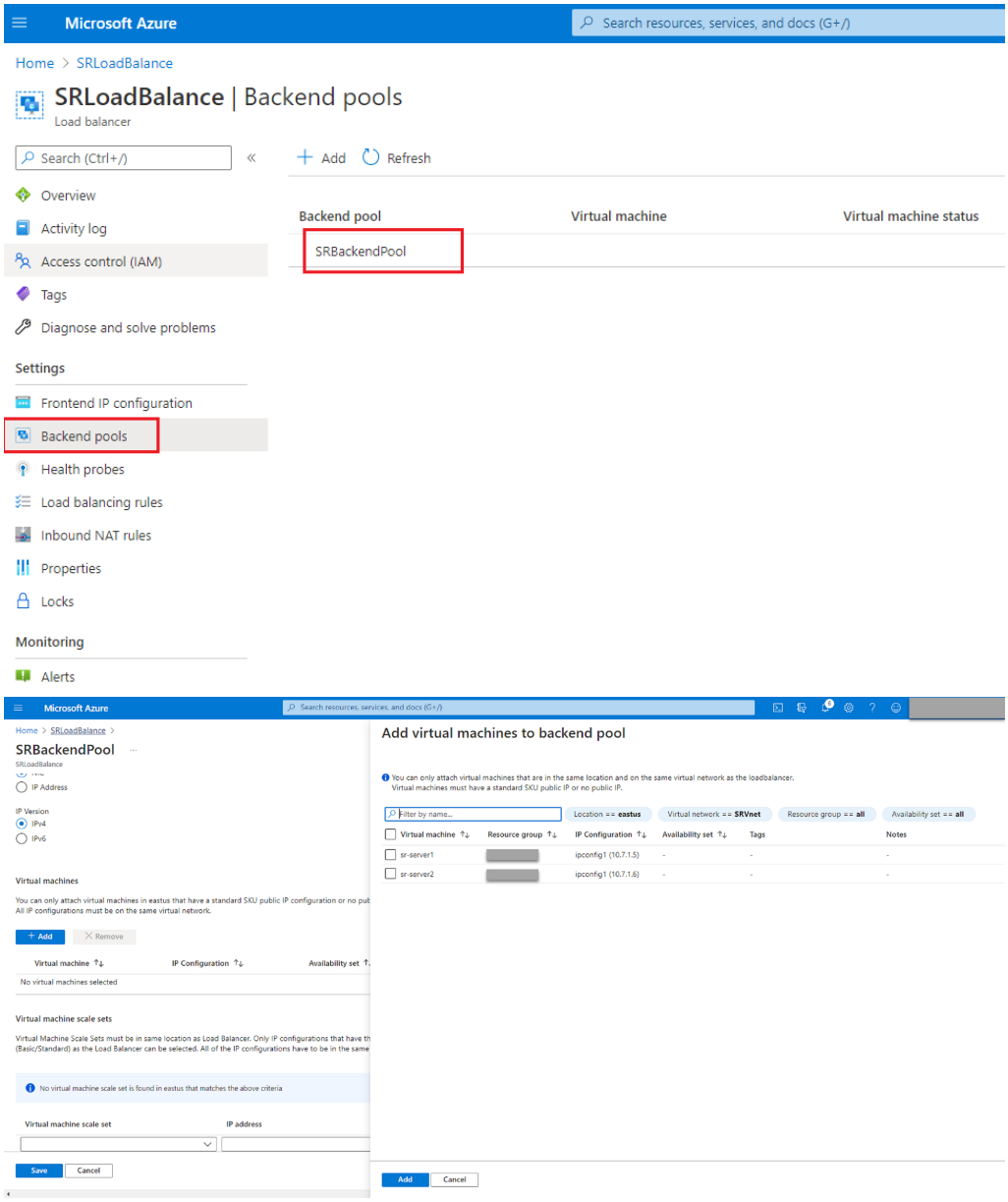


たとえば、次の設定を使用して、ポート 80 の負荷分散の規則を作成します。

設定	値
名前	「**SRTCPRule80**」などの名前を入力します。
IP Version	［**IPv4**］を選択します。
Frontend IP address	［**LoadBalancerFrontEnd**］を選択します。
Protocol	［**TCP**］を選択します。
ポート	「**80**」と入力します。
Backend port	「**80**」と入力します。
Backend pool	［**SRBackendPool**］を選択します。
Health probe	［**SRHealthProbe80**］を選択します。
Session persistence	［**Client IP**］を選択します。
Idle timeout (minutes)	デフォルト設定のままにします。
TCP reset	［有効］をクリックします。
送信元ネットワークアドレス変換（SNAT）	［**(Recommended) Use outbound rules to provide backend pool members access to the internet**］（（推奨）送信規則を使用してバックエンドプールのメンバーにインターネットへのアクセス権を付与する）を選択します。

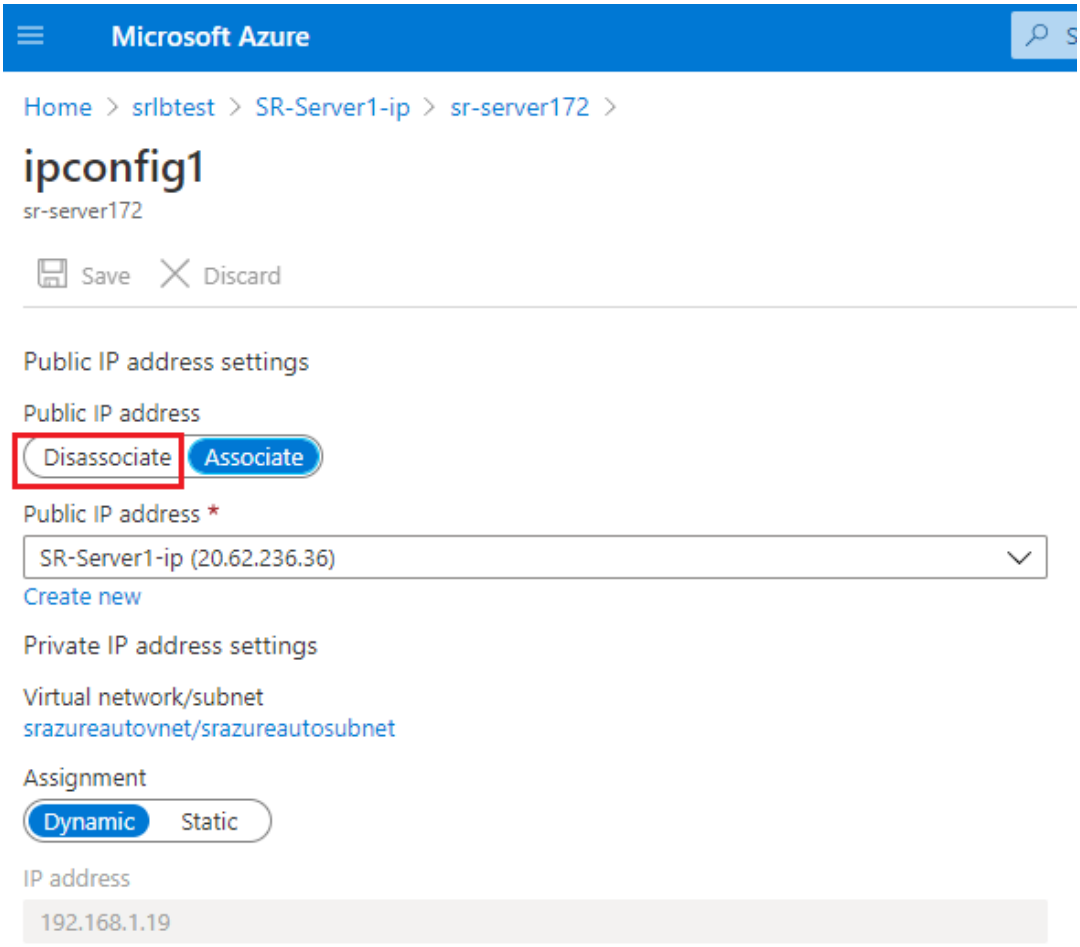


- Session Recording サーバーがインストールされている Azure VM をバックエンドプールに追加します。



c) Azure Load Balancer をテストします。

サーバーをバックエンドプールに追加できず、次のエラーメッセージに **NetworkInterfaceAndLoadBalancerAreInDifferentAvailabilitySets** と表示される場合は、サーバーネットワークインターフェイスのパブリック IP アドレスの関連付けを解除します。



オプション **3**: **Azure** アプリケーションゲートウェイを作成する

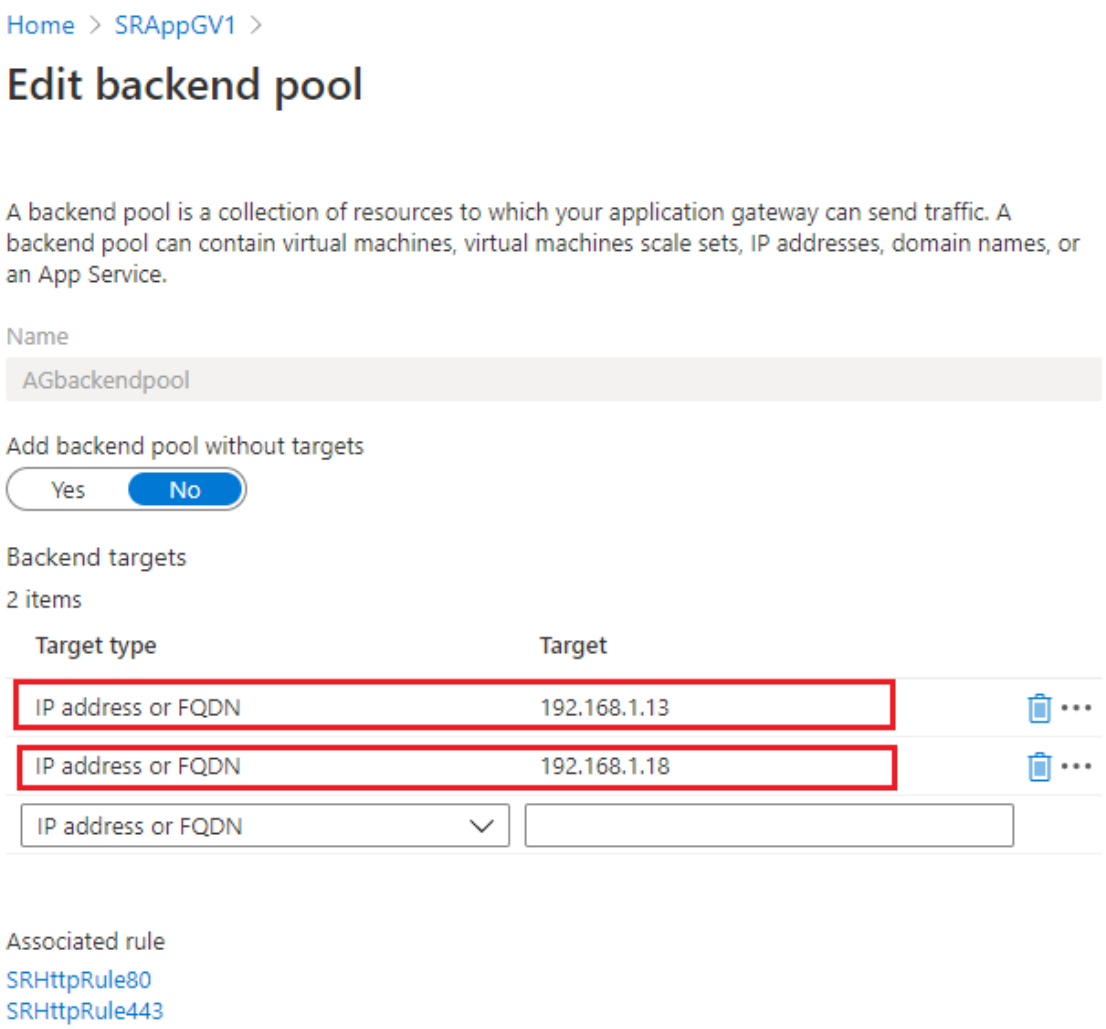
> ヒント:
>
> Application Gateway V2 は、NTLM 対応プロキシを介したルーティング要求をサポートしていません。

1. Azure アプリケーションゲートウェイを作成します。

   アプリケーションゲートウェイを作成するときに、次の設定を構成します。

   - [**Basics**] タブで、[**Tier**] を [**Standard**] に設定します。
   - [**Frontends**] タブで、[**Frontend IP address type**] を [**Private**] に設定します。新しいアプリケーションゲートウェイは、内部ロードバランサーとして使用されます。

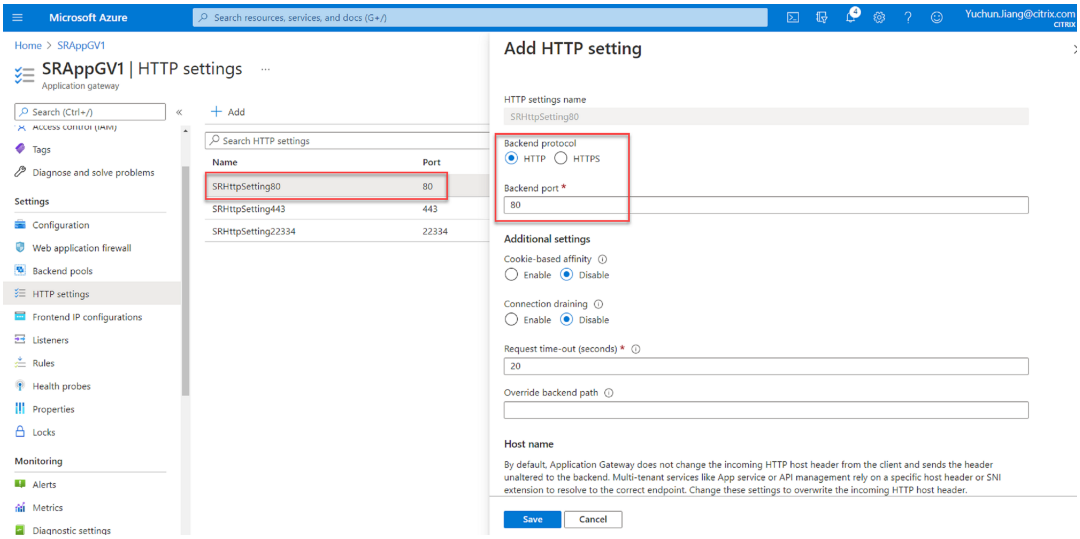
2. バックエンドプールを追加します。



3. HTTP 設定を作成します。

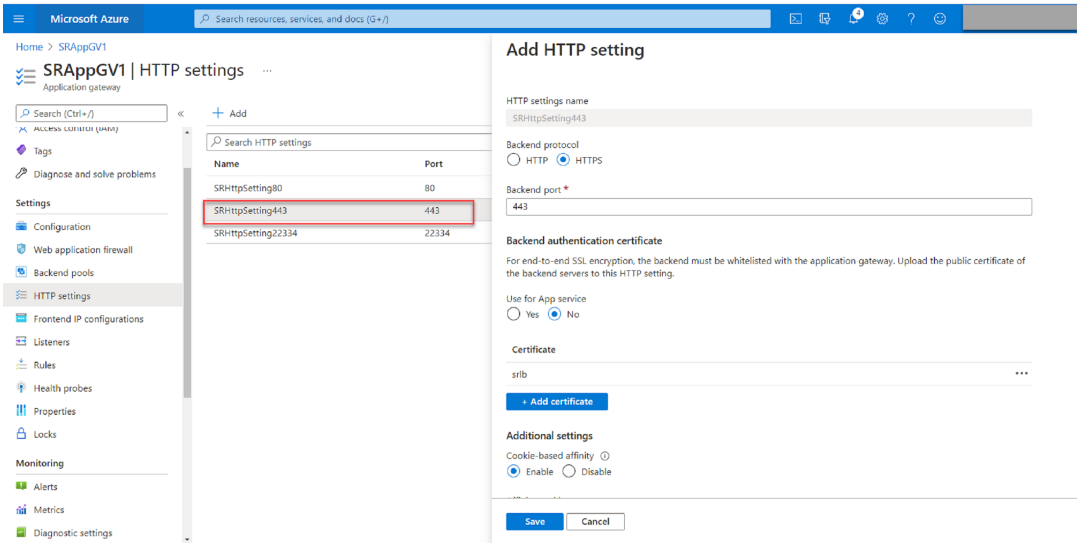
   Azure Application Gateway では、要求をバックエンドサーバーにルーティングするために HTTP と HTTPS の両方を使用できます。ポート 80、443、22334 の HTTP 設定を作成します。

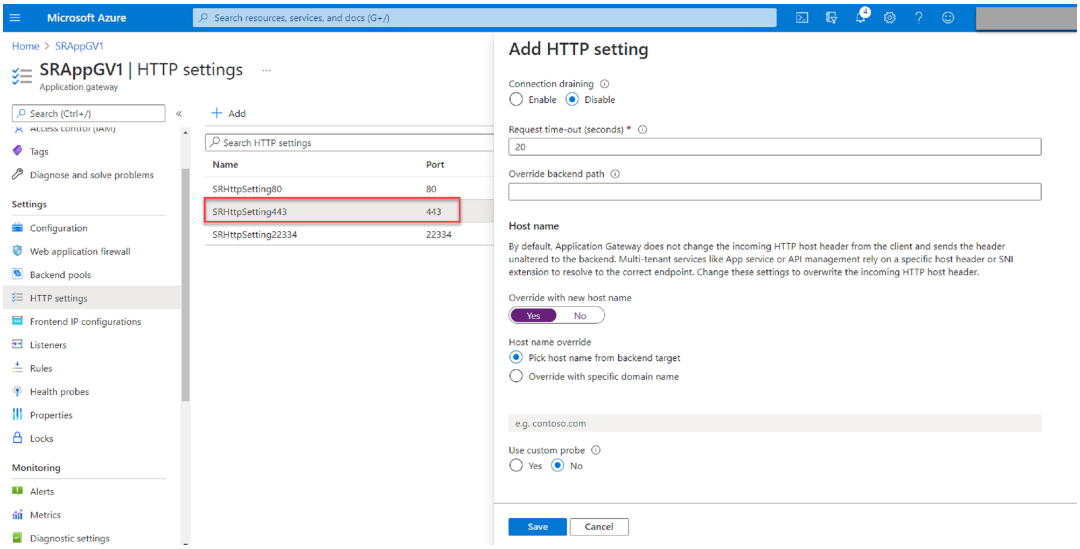
   - ポート 80 を介した HTTP



- ポート 443 を介した HTTP

  Application Gateway V1 でバックエンドサーバーを許可するには、認証証明書が必要です。認証証明書は、Base-64 でエンコードされた X.509（.CER）形式のバックエンドサーバー証明書の公開キーです。TLS/SSL 証明書から公開キーをエクスポートする方法については、「認証証明書のエクスポート（v1 SKU 用）」を参照してください。

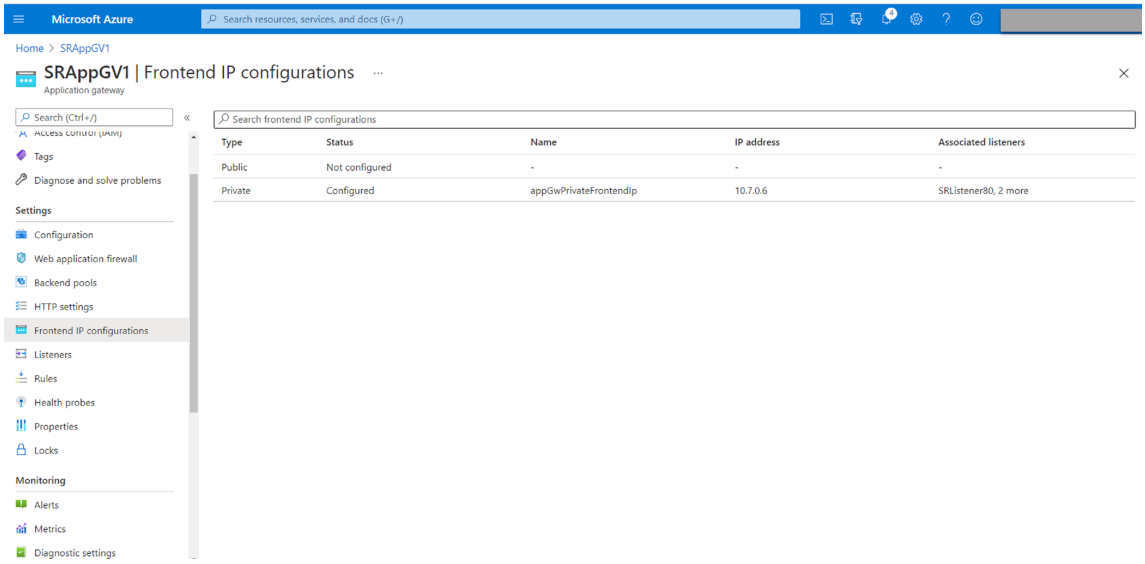




- ポート 22334 を介した HTTP または HTTPS

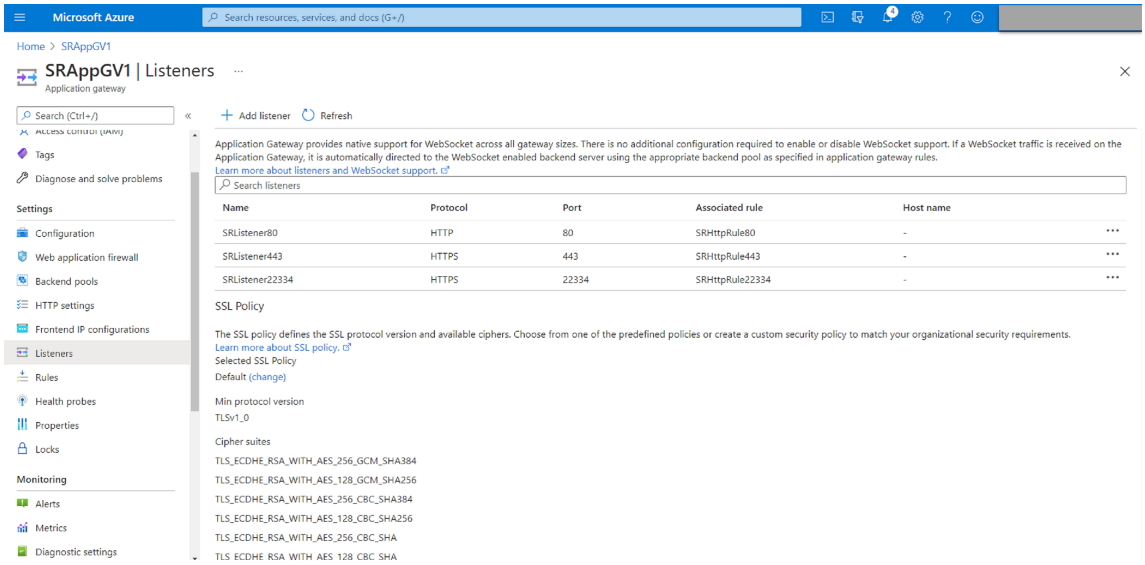
  WebSocket が HTTP を使用する場合は、ポート 80 と同じ設定を使用します。
  WebSocket が HTTPS を使用する場合は、ポート 443 と同じ設定を使用します。

4. フロントエンド IP アドレスを追加します。

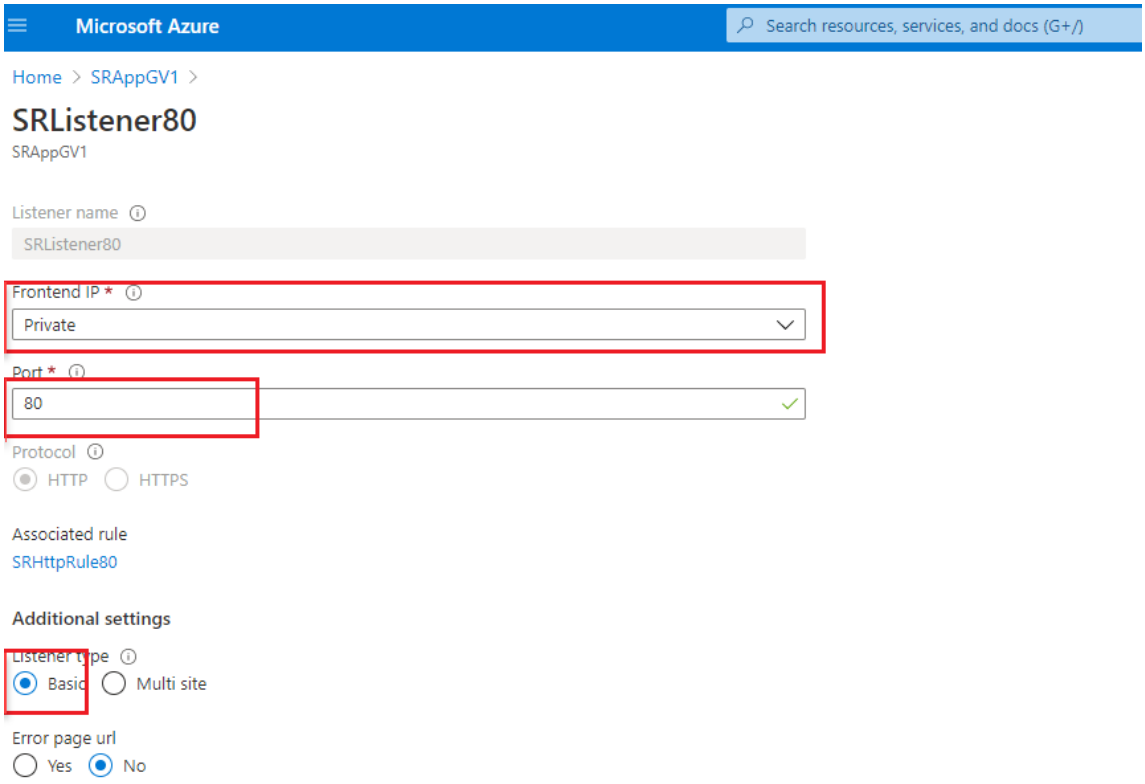


5. リスナーを追加します。

   次の例のように、ポート 80、443、22334 にリスナーを追加します:

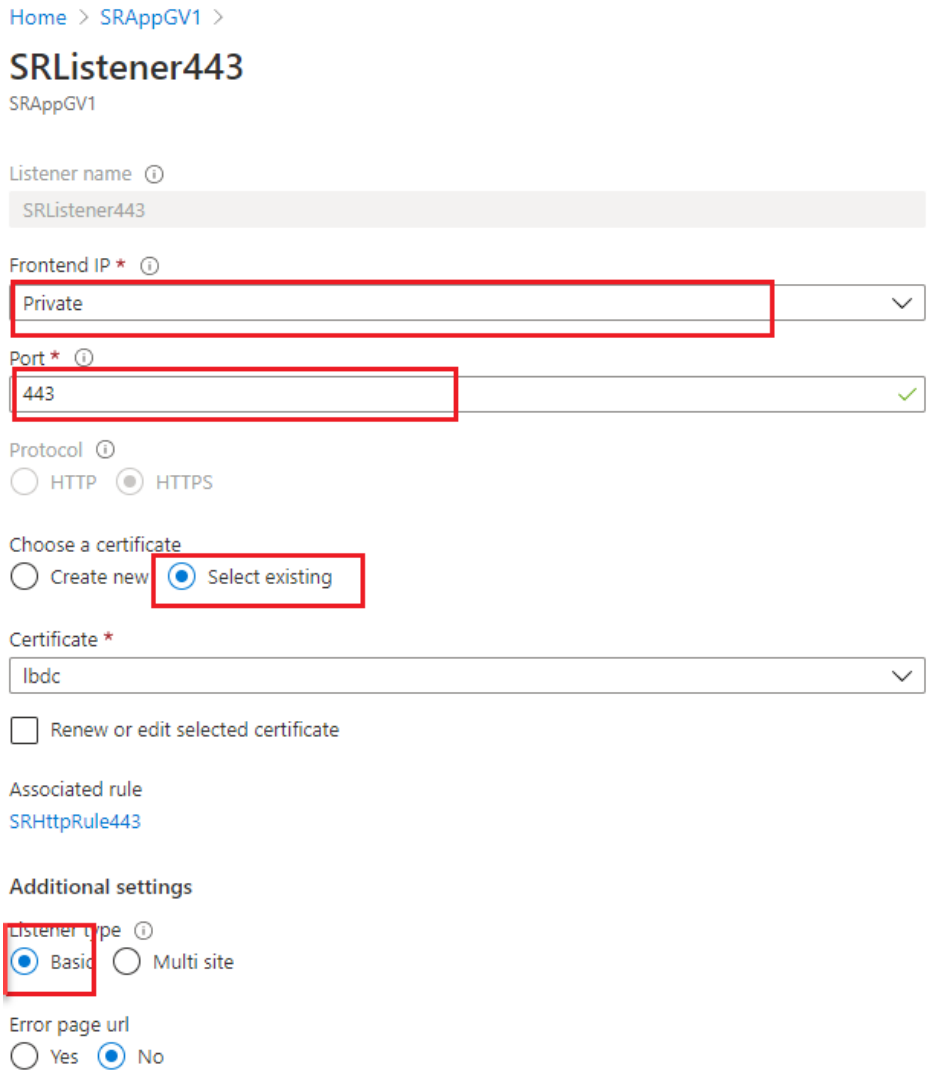


- ポート 80 のリスナー



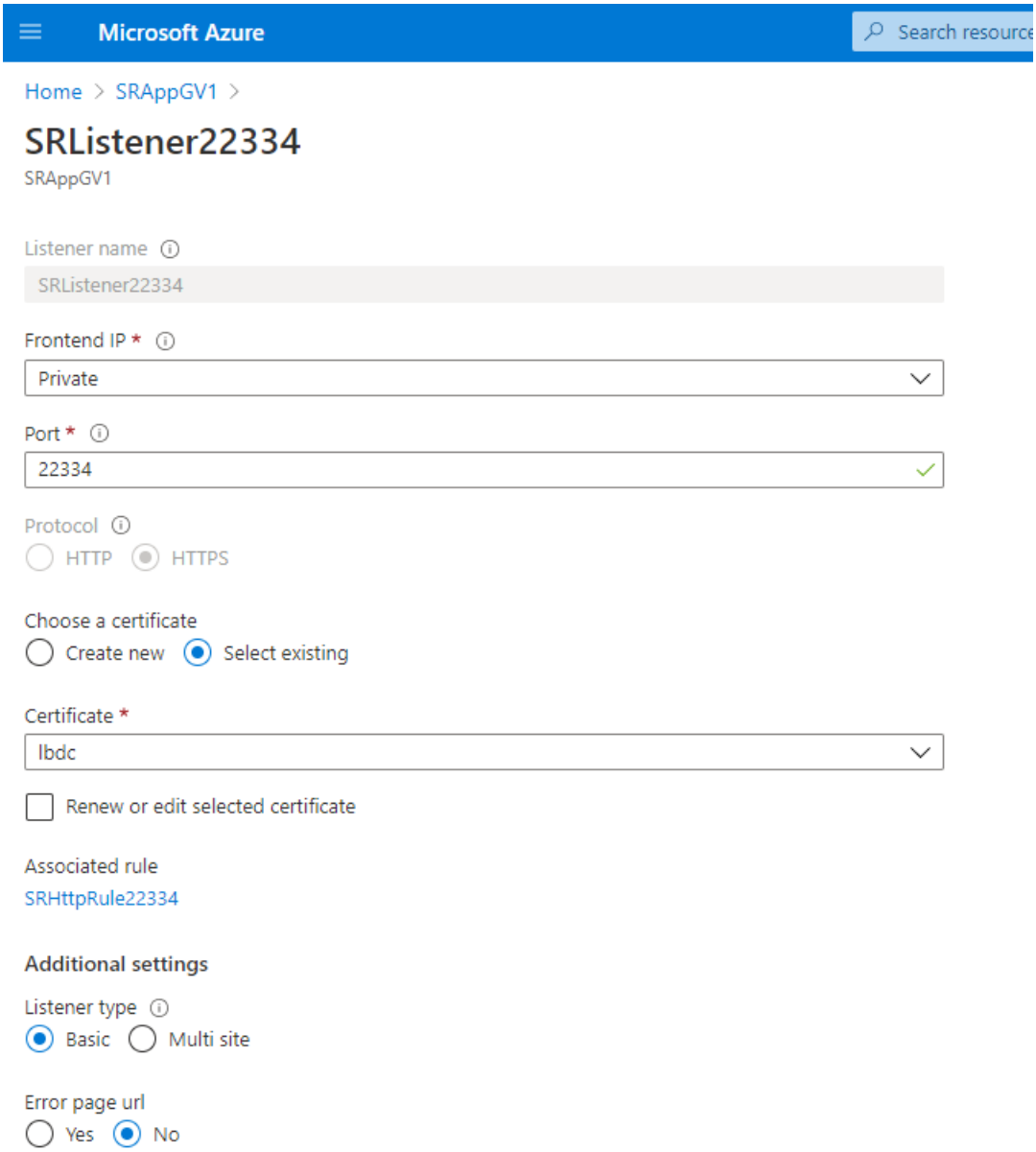
- ポート 443 のリスナー

  HTTPS リスナーを作成するとき、自己署名証明書を作成してAzure Portalにアップロードします。詳しくは、「TLS 終端でサポートされる証明書」および「自己署名証明書の作成」を参照してください。



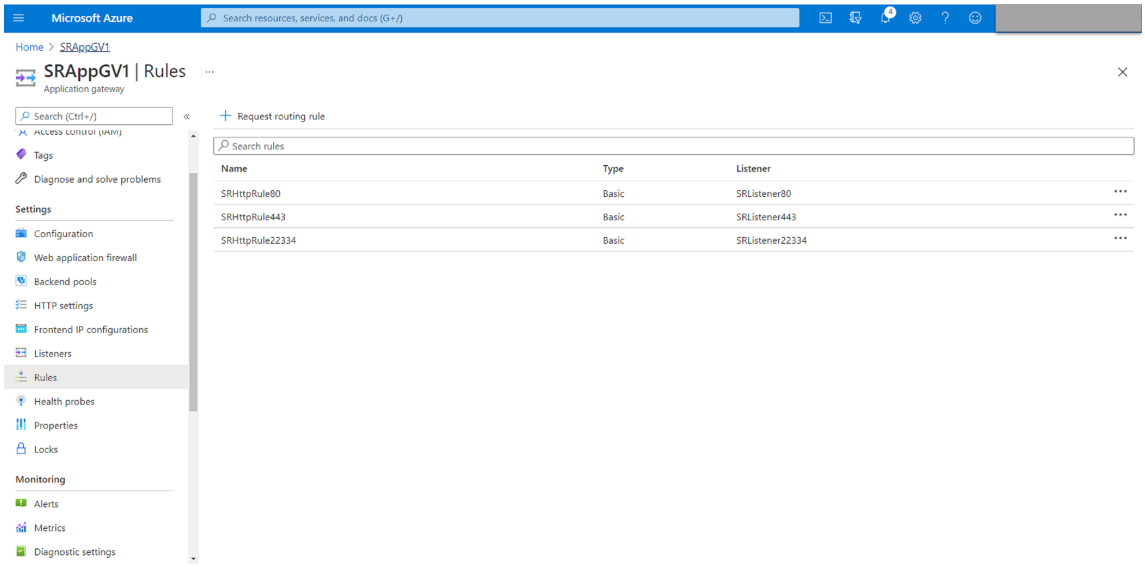
- ポート 22334 のリスナー

  WebSocket が HTTP を使用する場合は、ポート 80 と同じ設定を使用します。WebSocket が HTTPS を使用する場合は、ポート 443 と同じ設定を使用します。次の例は、ポート 22334 での HTTPS リスナーの設定を示しています。

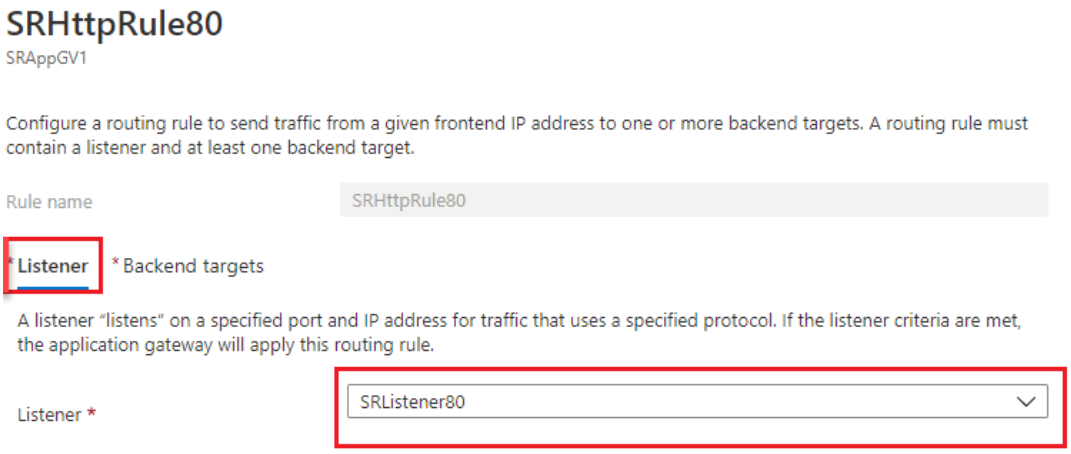


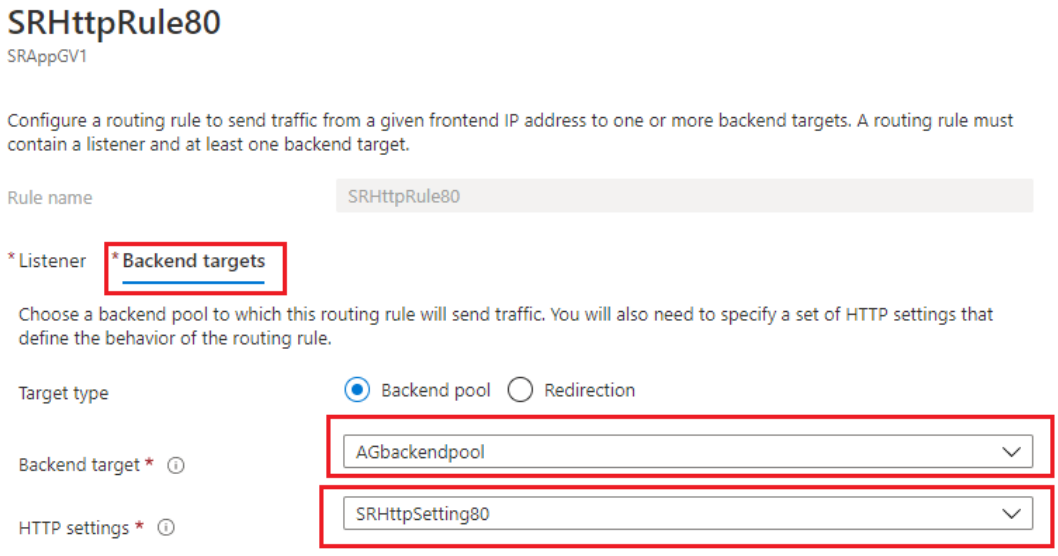
6. 要求ルーティングの規則を作成します。

   次の例のように、ポート 80、443、22334 の規則を作成します：

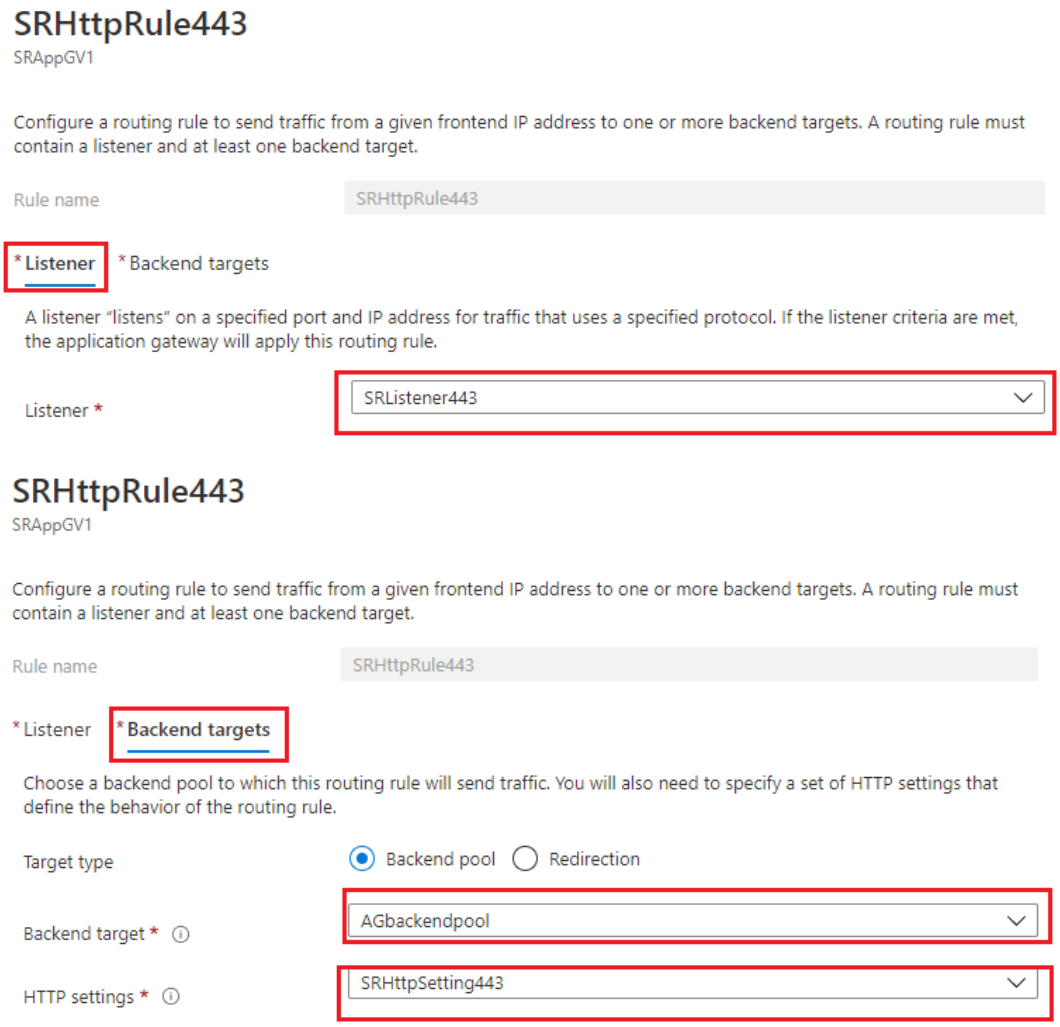


- ポート 80 のルーティングの規則

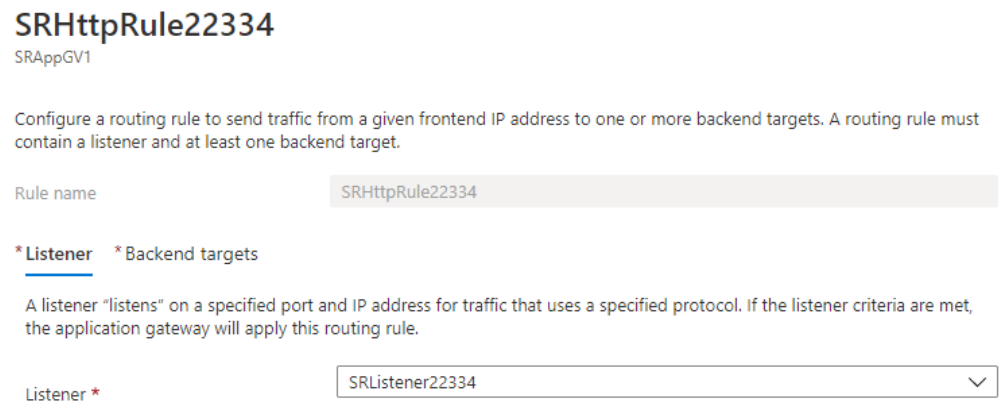


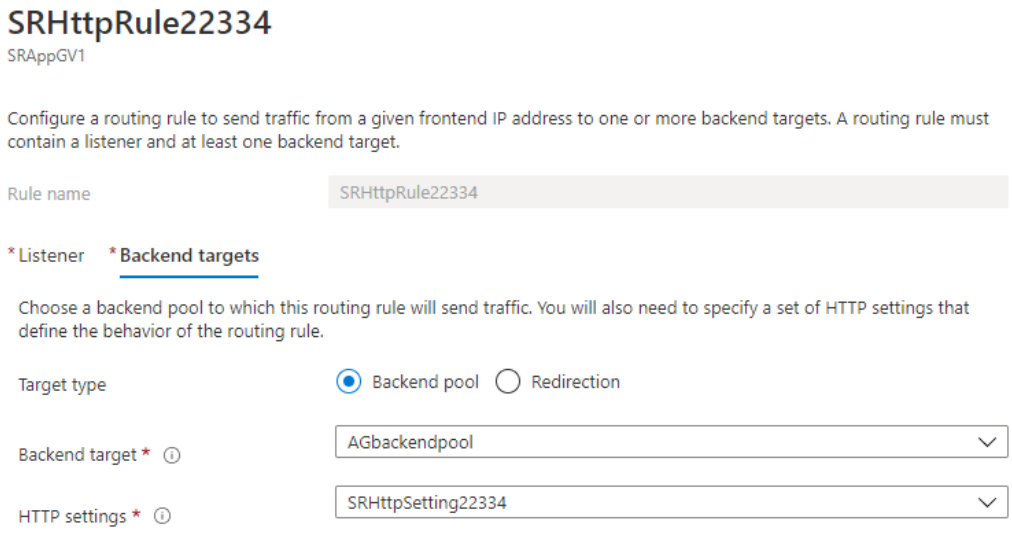


- ポート 443 のルーティングの規則



- ポート 22334 のルーティングの規則





7. Session Recording サーバーがインストールされている Azure VM をバックエンドプールに追加します。
8. Knowledge Center の記事CTX230015に従って、Session Recording サーバーを構成します。

トラブルシューティング

December 22, 2022

このトラブルシューティング情報には、Session Recording コンポーネントのインストール中またはインストール後に発生する可能性のある、次のような問題に対する解決策が含まれています。

> 警告:
>
> 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、オペレーティングシステム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、シトリックス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。

サーバーコンポーネントをインストールできない

December 22, 2022

Session Recording サーバーコンポーネントのインストールが、エラーコード 2503 および 2502 で失敗します。解決策: C:\Windows\Temp フォルダーのアクセス制御リスト（ACL）をチェックし、ローカルユーザーとローカルグループにこのフォルダーに対する書き込み権限が付与されていることを確認します。付与されていない場合は、書き込み権限を手動で付与します。

インストール中にデータベースへの接続のテストに失敗した

December 22, 2022

Session Recording データベースまたは Session Recording サーバーのインストール時に、データベースインスタンス名が正しくても、エラーメッセージ「データベース接続テストに失敗しました。正しいデータベース インスタンス名を入力してください。」が表示されて接続テストが失敗します。

そのような場合は、現在のユーザーに、権限制限エラーを修正するためのパブリック SQL Server の役割権限があることを確認してください。

エージェントがサーバーに接続できない

February 20, 2024

Session Recording Agent から Session Recording サーバーに接続できないとき、「**Session Recording Broker** にポールメッセージを送信しています **-** この処理の実行中に例外が見つかりました。」というイベントメッセージが、例外のテキストとともにログに記録されます。例外のテキストには接続に失敗した原因が記載されます。次のような原因があります:

- 接続が閉じられました。**SSL/TLS** の安全なチャネルを確立できませんでした。この例外は、Session Recording サーバーで使用している証明書を署名した CA が、Session Recording Agent が動作するサーバーに信頼されていないか、Session Recording Agent が動作するサーバーに CA 証明書がインストールされていないことを示します。または、証明書の有効期限が切れているか失効している可能性があります。

  解決策：Session Recording Agent をホストするサーバーに正しい CA 証明書をインストールします。信頼された CA を使用してください。

- リモートサーバーがエラーを返しました：**HTTP 403**（アクセス不可）。この標準の HTTPS エラーは、セキュリティで保護されていない HTTP を使用して接続しようとしたときに発生します。Session Recording サーバーをホストするマシンは、セキュリティで保護された接続のみを受け付けるため、この接続は拒否されます。

  解決策：［**Session Recording Agent** のプロパティ］を使用して Session Recording Broker のプロトコルを **HTTPS** に変更します。

- レコードポリシークエリの検証中に、**Session Recording Broker** が不明なエラーを返しました。エラーコード **5**（アクセスが拒否されました）。詳しくは、**Session Recording** サーバー上のイベントログを参照してください。このエラーは、セッションが開始され録画ポリシーの評価要求が送信されると発生します。このエラーは、Session Recording 承認コンソールの役割であるポリシークエリの役割から、デフォルトのメンバーである Authenticated Users グループが削除された結果発生します。

  解決策：Authenticated Users グループをこの役割に再追加するか、各 Session Recording Agent をホストする各サーバーをポリシークエリの役割に追加します。

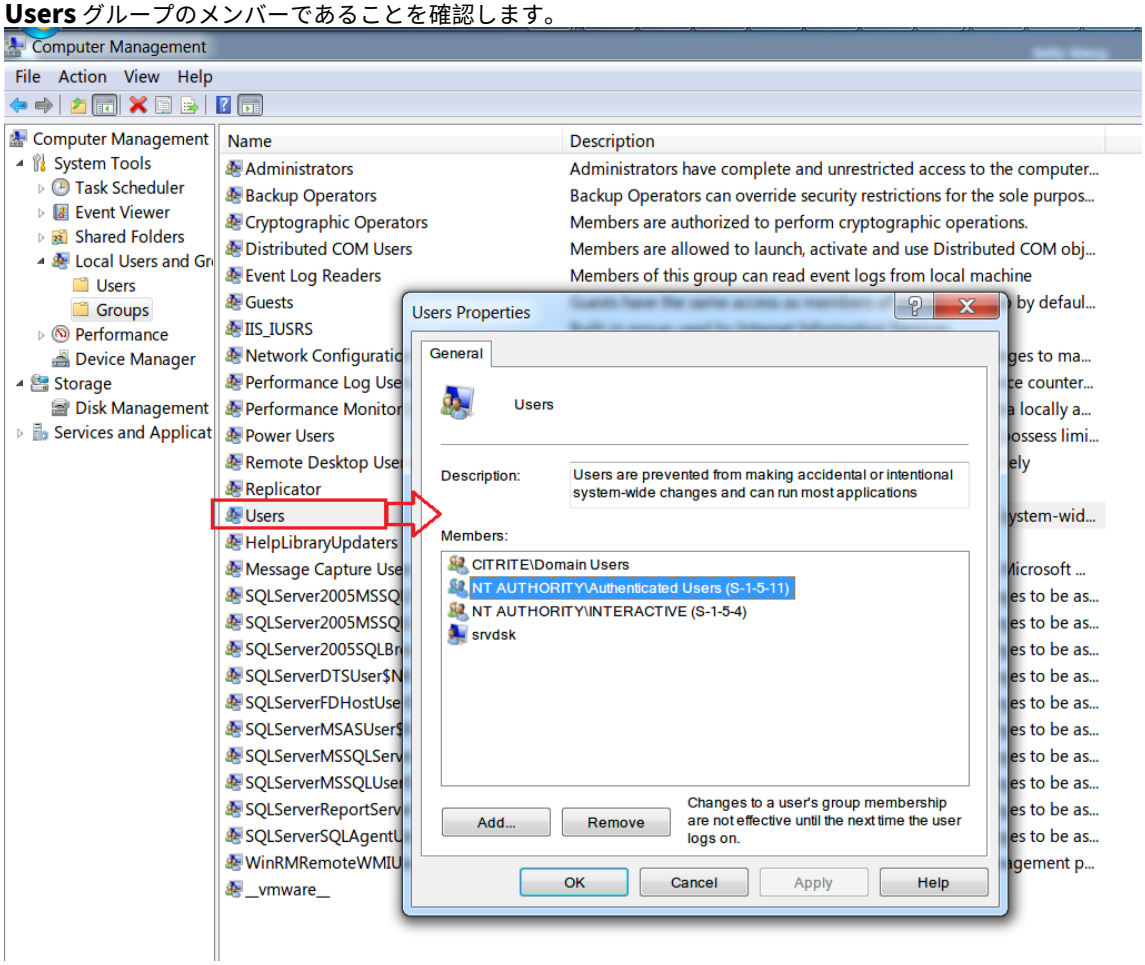
- 接続が閉じられました。維持される必要があった接続が、サーバーによって切断されました。このエラーは、Session Recording サーバーが停止しているか、要求を受け付けられないことを示します。IIS がオフラインまたは再起動されたか、サーバー全体がオフラインである可能性があります。

  解決策：Session Recording サーバーが開始されていてネットワークに接続していることを確認します。IIS がサーバーで実行されていることを確認してください。

- リモートサーバーがエラーを返しました。**401**（未承認アクセス）。このエラーにより、次のような現象が発生します：

  - Session Recording Agent サービスのスタートアップ時に、401 エラーがイベントログに記録されます。
  - Session Recording Agent でポリシーをクエリできません。
  - セッションの録画が Session Recording Agent でキャプチャされません。

  解決策：**NT AUTHORITY\Authenticated Users** グループが、Session Recording Agent のローカルの **Users** グループのメンバーであることを確認します。



サーバーがデータベースに接続できない

December 22, 2022

Session Recording サーバーから Session Recording データベースに接続できないとき、次のいずれかのメッセージが表示されることがあります:

イベントソース:

「**SQL** サーバーへの接続確立時にネットワーク関連またはインスタンス固有のエラーが発生しました。」このエラーは、ID 2047 のアプリケーションイベントログに表示されます。このイベントログは、Session Recording サーバーの［イベントビューアー］で確認できます。

「**Citrix Session Recording** ストレージマネージャーの説明**:** データベース接続を確立しています **-** この処理の実行中に例外が見つかりました。」このエラーは、Session Recording サーバーの［イベントビューアー］にあるアプリケーションイベントログに表示されます。

Session Recording サーバーに接続できません。**Session Recording** サーバーが実行中か確認してください。このエラーメッセージは、Session Recording ポリシーコンソールの起動時に表示されます。

解決方法:

- スタンドアロンサーバーに Microsoft SQL Server をインストールしましたが、Session Recording の正しいサービスまたは設定を構成できませんでした。サーバーで TCP/IP プロトコルを有効にして SQL Server Browser サービスを実行する必要があります。これらの設定を有効にする方法について詳しくは、Microsoft 社のドキュメントを参照してください。
- Session Recording 管理ツールのインストール中に、サーバーとデータベースについて誤った情報が指定されました。Session Recording データベースをアンインストールし、正しい情報を指定して再インストールします。
- Session Recording データベースサーバーが停止しています。サーバーに接続できることを確かめます。
- Session Recording サーバーまたは Session Recording データベースサーバーをホストするマシンで、もう一方の FQDN または NetBIOS 名を解決できません。ping コマンドを使用して、名前を解決できることを確認します。
- Session Recording データベースのファイアウォールの構成をチェックし、SQL Server の接続が許可されていることを確認します。詳しくは、Microsoft 社のhttps://docs.microsoft.com/en-us/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?redirectedfrom=MSDN&view=sql-server-ver15を参照してください。

「ユーザー‘**NT_AUTHORITY\ANONYMOUS LOGON**’ログオン失敗。」このエラーメッセージは、サービスのログオンアカウントが誤って.\administrator になっていることを意味します。

解決策:ローカルシステムユーザーとしてサービスを再起動し、SQL サービスを再起動します。

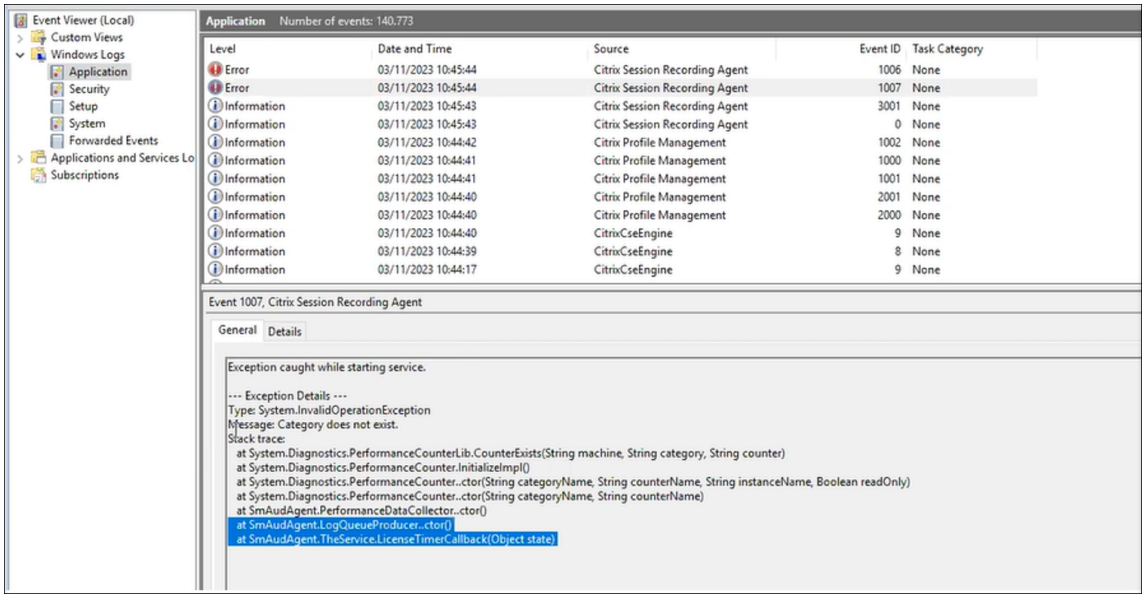
セッションが録画されない

February 20, 2024

セッションが正常に録画されない場合は、Session Recording Agent と Session Recording サーバーが動作するイベントビューアーで、アプリケーションイベントログを確認します。このログには有益な診断情報が含まれています。

セッションが録画されない場合、次の原因が考えられます。

- コンポーネント間の接続と証明書。Session Recording コンポーネントの間で通信ができない場合は、セッションの録画に失敗します。録画の問題のトラブルシューティングをするには、すべてのコンポーネントが適切に設定されていて正しいマシンを参照していることと、すべての証明書が有効で適切にインストールされていることを確かめます。
- 非 **Active Directory** ドメイン環境。Session Recording は Microsoft Active Directory ドメインの環境で動作するように設計されています。Active Directory 環境で運用していない場合は、録画で問題が発生する可能性があります。Session Recording のすべてのコンポーネントは、必ず Active Directory ドメインに参加しているマシンで実行します。
- セッション共有がアクティブなポリシーと競合している。Session Recording では、アクティブなポリシーとユーザーが最初に開いた公開アプリケーションを照合します。同じセッション上で次のアプリケーションを開くと、最初のアプリケーションに対して有効なポリシーが、次のアプリケーションにも適用されます。セッション共有がアクティブなポリシーと競合することを防ぐには、競合するアプリケーションを別のマルチセッション OS VDA で公開します。
- 録画が有効になっていない。マルチセッション OS 対応 VDA に Session Recording Agent をインストールすると、デフォルトで VDA の録画が有効になります。録画を許可するアクティブな録画ポリシーを設定するまでは、録画はされません。
- アクティブな録画ポリシーによって録画が許可されない。セッションは、アクティブな記録ポリシーの規則をセッションが満たしている場合にのみ録画できます。
- **Session Recording** サービスが実行されていない。セッションを録画するには、マルチセッション OS VDA で Session Recording Agent サービスが実行されており、Session Recording サーバーをホストするマシンで Session Recording ストレージマネージャーサービスが実行されている必要があります。
- **MSMQ** が設定されていない。Session Recording Agent が動作するサーバーと Session Recording サーバーをホストするマシンで MSMQ が適切に設定されていない場合は、録画の問題が起きる可能性があります。
- **Session Recording Agent** の **Windows** パフォーマンスカウンターが見つからないか、無効になっているか、破損している。Session Recording Agent のアプリケーションログに次のエラーが表示される場合があります:



この問題を解決するには、次の手順を実行してすべてのパフォーマンスカウンターを再構築します:

1. コマンドプロンプト（CMD）を管理者として開きます。
2. `cd c:\windows\system32\`と入力して、「windows\system32」に移動します。
3. `lodctr /R`と入力して、**Enter** キーを押します。`lodctr /R`コマンドはパフォーマンスカウンターを再構築します。
4. `lodctr /R`コマンドの実行後、再構築された一部のカウンターが無効になる可能性があります。カウンターの状態を確認するには、`lodctr /Q`コマンドを実行します。カウンターが無効になっている場合は、`lodctr /E: [counter name]`コマンドを実行して有効にできます。

ライブセッションを再生できない

December 22, 2022

Session Recording Player で録画を再生できないときは、次のエラーメッセージが表示されることがあります:

「セッションの録画ファイルをダウンロードできませんでした。ライブセッションの再生は許可されていません。サーバーがこの機能を許可しない設定になっています。」このエラーは、サーバーがこの操作を許可しないように設定されていることを示します。

解決策:［**Session Recording** サーバーのプロパティ］で ［再生］タブをクリックし、［ライブセッションの再生を許可する］チェックボックスをオンにします。

録画が破損しているまたは不完全

December 22, 2022

- Player で、破損した、または不完全な録画を表示すると、Session Recording Agent のイベントログで警告が表示されることがあります。

  イベントソース：Citrix Session Recording ストレージマネージャー

  説明：ファイル **** を録画中のデータ喪失

  この問題は、MCS または PVS で構成済みのマスターイメージとインストール済みの Microsoft Message Queuing（MSMQ）を使用して VDA を作成する場合に発生します。この状況では、VDA で MSMQ の`QMId`が同じになります。

  これを回避するには、各 VDA に対し、一意の`QMId`を作成します。詳しくは、「インストール、セットアップ、およびアンインストール」を参照してください。

- 特定の録画ファイルを再生しているときに、Session Recording Player がメッセージ「再生中のファイルにより、内部システムエラー（エラーコード**: 9**）が元の録画中に発生したことが報告されました。エラーが発生した箇所までは再生できます。」を表示して内部エラーをレポートすることがあります。

  この問題は、グラフィック指向セッションの録画中に Session Recording Agent のバッファーサイズが不十分なために発生します。

  これを回避するには、Session Recording Agent で`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SmAudBufferSizeMB`をより大きな値のデータに変更してから、マシンを再起動します。

コンポーネント間の接続の確認

December 22, 2022

Session Recording のセットアップ中にコンポーネント間の接続に成功しないことがあります。すべてのコンポーネントが Session Recording サーバー（Broker）と通信を行います。デフォルトでは、IIS のコンポーネントであるブローカーのセキュリティは、IIS の既定の Web サイトの証明書を使用して保護されます。あるコンポーネントから Session Recording サーバーに接続できないときは、ほかのコンポーネントから接続を試行しても失敗することがあります。

Session Recording Agent と Session Recording サーバー（ストレージマネージャーとブローカー）の接続エラーは、アプリケーションイベントログに記録されます。このログは、Session Recording サーバーをホストしているマシンの［イベントビューアー］で確認できます。Session Recording ポリシーコンソールと Session Recording Player では、接続に失敗したときに画面にエラーメッセージが表示されます。

Session Recording Agent が接続されていることの確認

1. Session Recording Agent がインストールされているサーバーにログオンします。
2. ［スタート］ボタンをクリックし、［**Session Recording Agent** のプロパティ］を選択します。
3. ［**Session Recording Agent** のプロパティ］で、［接続］をクリックします。
4. ［**Session Recording** サーバー］フィールドに正しい完全修飾ドメイン名が入力されていることを確認します。
5. ［Session Recording サーバー］の値として入力されているサーバーに、マルチセッション OS 対応 VDA からアクセスできることを確認します。

詳しくは、「エージェントがサーバーに接続できない」を参照してください。

> 注:
>
> アプリケーションイベントログで、エラーと警告を確認します。

Session Recording サーバーが接続されていることの確認

> 注意:
>
> レジストリエディターの使用によって、深刻な問題が発生する可能性があり、オペレーティングシステム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、シトリックス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。

1. Session Recording サーバーをホストするマシンにログオンします。
2. レジストリエディターを開きます。
3. 「`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`」を参照します。
4. **SmAudDatabaseInstance** の値で、SQL Server のインスタンスにインストールした Session Recording データベースが正しく参照されていることを確認します。

詳しくは、「サーバーがデータベースに接続できない」を参照してください。

Session Recording データベースが接続されていることの確認

1. SQL 管理ツールを使って、インストールした Session Recording データベースを含む SQL インスタンスを開きます。
2. Session Recording データベースの［セキュリティ］権限を開きます。
3. Session Recording コンピューターアカウントにデータベースへのアクセス許可が与えられていることを確かめます。たとえば、Session Recording サーバーをホストするマシンの名前が MIS ドメインの **SsRecSrv** である場合、データベースにコンピューターアカウントとして **MIS\SsRecSrv$** を指定する必要があります。この値は Session Recording データベースのインストール中に設定します。

IIS の接続のテスト

Web ブラウザーを使用して Session Recording Broker Web ページにアクセスすることにより、Session Recording サーバーの IIS サイトへの接続をテストできます。これは、Session Recording コンポーネント間で通信に問題が起きたとき、問題の原因がプロトコルの誤設定なのか、証明書の問題なのか、Session Recording Broker の起動の問題なのかを判断するのに役立ちます。

Session Recording Agent の IIS の接続を確認するには:

1. Session Recording Agent がインストールされているサーバーにログオンします。
2. Web ブラウザーを開いて次のアドレスを入力します:
    - HTTPS で接続する場合: `https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl`（ここで、`servername`は Session Recording サーバーをホストするマシンの名前です。）
    - HTTP で接続する場合: `http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl`（ここで、`servername`は Session Recording サーバーをホストするマシンの名前です。）
3. NTLM（NT LAN Manager）認証の資格情報の入力を求められた場合は、ドメイン管理者のアカウントでログオンします。

Session Recording Player の IIS の接続を確認するには:

1. Session Recording Player がインストールされているワークステーションにログオンします。
2. Web ブラウザーを開いて次のアドレスを入力します:
    - HTTPS で接続する場合: `https://servername/SessionRecordingBroker/Player.rem?wsdl`（ここで、`servername`は Session Recording サーバーをホストするマシンの名前です。）
    - HTTP で接続する場合: `http://servername/SessionRecordingBroker/Player.rem?wsdl`（ここで、`servername`は Session Recording サーバーをホストするマシンの名前です。）
3. NTLM（NT LAN Manager）認証の資格情報の入力を求められた場合は、ドメイン管理者のアカウントでログオンします。

Session Recording ポリシーコンソールの IIS の接続を確認するには:

1. Session Recording ポリシーコンソールがインストールされているサーバーにログオンします。
2. Web ブラウザーを開いて次のアドレスを入力します:
    - HTTPS で接続する場合: `https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`（ここで、`servername`は Session Recording サーバーをホストするマシンの名前です。）

- HTTP で接続する場合: `http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl`（ここで、`servername`は Session Recording サーバーをホストするマシンの名前です。）

3. NTLM（NT LAN Manager）認証の資格情報の入力を求められた場合は、ドメイン管理者のアカウントでログオンします。

ブラウザーに XML ドキュメントが表示された場合は、設定したプロトコルを使用して、Session Recording ポリシーコンソールが Session Recording サーバーと接続していることが確認されたことになります。

証明書の問題のトラブルシューティング

通信プロトコルに HTTPS を使用する場合は、Session Recording サーバーをホストするマシンにサーバー証明書を設定する必要があります。すべてのコンポーネントの Session Recording サーバーへの接続には、ルート CA（Certificate Authority：証明機関）が必要です。この証明書をインストールしないと、コンポーネント間の通信は失敗します。

IIS の接続をテストするときのように、Session Recording Broker の Web ページにアクセスすることによって、証明書をテストすることができます。各コンポーネントの XML ページにアクセスできる場合は、証明書は正しく設定されています。

ここでは、接続エラーの原因になる、証明書によくある問題について説明します：

- 無効な証明書または証明書の不足。Session Recording Agent が動作するサーバーにサーバー証明書を信頼するためのルート証明書がインストールされていない場合は、HTTPS を介して Session Recording サーバーを信頼できず、接続できません。Session Recording サーバー上のサーバー証明書がすべてのコンポーネントで信頼されていることを確かめてください。
- 名前の不一致。Session Recording サーバーをホストするマシンに割り当てられたサーバー証明書が、FQDN を使用して作成されている場合、Session Recording サーバーに接続するとき、接続するすべてのコンポーネントで FQDN を使用する必要があります。サーバー証明書が NetBIOS 名を使用して作成されている場合、Session Recording サーバーに接続するとき、接続するすべてのコンポーネントで NetBIOS 名を使用するように設定します。
- 期限切れまたは失効した証明書。サーバー証明書が失効している場合、HTTPS を介した Session Recording サーバーへの接続は失敗します。Session Recording サーバーをホストするマシンに割り当てられているサーバー証明書が有効で、失効していないことを確認してください。録画したセッションのデジタル署名に同じ証明書を使用している場合は、Session Recording サーバーのイベントログに、証明書が失効したことを示すエラーメッセージ、または失効日が近づいていることを示す警告メッセージが記録されます。

Player で録画を検索できない

December 22, 2022

Session Recording Player で録画を検索できないときは、次のエラーメッセージが表示されることがあります:

- セッションの録画ファイルを検索できませんでした。リモート名を解決できませんでした: **servername**。(ここで、**servername** は Session Recording Player で接続を試行しているサーバーの名前です。) Session Recording Player は Session Recording サーバーと通信することができません。誤ったサーバー名が入力されているか、DNS でサーバー名を解決できていないという、2 つの理由が考えられます。

  解決策: Session Recording Player のメニューバーで、[ツール] **>** [オプション] **>** [接続] の順に選択し、[**Session Recording** サーバー] の一覧のサーバー名が正しいことを確認します。サーバー名が正しい場合は、コマンドプロンプトで ping コマンドを実行し、名前を解決できるかどうかを確認します。Session Recording サーバーが停止しているかオフラインのときにセッションの録画ファイルを検索すると、「リモートサーバーに接続できません」というエラーメッセージが返されます。

- リモートサーバーに接続できません。このエラーは、Session Recording サーバーが停止しているかオフラインのときに発生します。

  解決策: Session Recording サーバーが接続していることを確かめます。

- アクセスが拒否されました。アクセス拒否のエラーは、ユーザーにセッションの録画ファイルを検索およびダウンロードする権限がない場合に発生します。

  解決策: Session Recording 承認コンソールで、ユーザーを Player の役割に割り当てます。

- **Player** の役割が割り当てられているときにアクセスが拒否されました。このエラーは、Session Recording Player と Session Recording サーバーを同じマシンにインストールし、UAC を有効にしているときに発生します。Domain Admins または Administrators ユーザーグループに Player の役割を割り当てたときに、そのグループの非組み込みの管理者ユーザーが役割ベースのチェックを渡せないことがあります。

  解決策:

  - Session Recording Player を管理者として実行します。
  - グループ全体ではなく特定のユーザーに Player の役割を割り当てます。
  - Session Recording サーバーではなく Session Recording Player を個別のマシンにインストールします。

- セッションの録画ファイルを検索できませんでした。接続が閉じられました。**SSL/TLS** の安全なチャネルを確立できませんでした。このエラーは、Session Recording サーバーで使用している証明書を署名した CA (Certificate Authority: 証明機関) がクライアントデバイスに信頼されていないか、クライアントデバイスに CA 証明書がインストールされていないために発生します。

  解決策: Session Recording Player がインストールされているワークステーションに、正しい、つまり信頼されている CA 証明書をインストールします。

- リモートサーバーがエラーを返しました: **HTTP 403** (アクセス不可)。このエラーは、HTTP (セキュリティで保護されていないプロトコル) を使用して接続しようとしたときに発生する、標準の HTTPS エラーです。

デフォルトでは、セキュリティで保護されている接続のみを受け入れるように設定されるため、サーバーにより接続が拒否されます。

解決策：**Session Recording Player** のメニューバーで、［ツール］> ［オプション］> ［接続］の順に選択します。［**Session Recording** サーバー］ボックスの一覧でサーバーを選択し、［変更］をクリックします。プロトコルを ［**HTTP**］から ［**HTTPS**］に変更します。

MSMQ のトラブルシューティング

セッションの録画を知らせる通知メッセージが表示されているのに、Session Recording Player で検索しても録画が見つからない場合は、MSMQ に問題があります。Session Recording サーバー（ストレージマネージャー）にキューが接続されていることを確認します。Web ブラウザーを使用して接続エラーが発生しないかテストします (MSMQ の接続プロトコルとして HTTP または HTTPS を使用している場合)。

キューが接続されていることを確認するには:

1. Session Recording Agent をホストするサーバーにログインして、発信キューを表示します。
2. Session Recording サーバーをホストするマシンへのキューが接続された状態であることを確認します。
    - 接続を待っている状態で、メッセージがキューにあり、プロトコルが HTTP または HTTPS の場合は（［**Session Recording Agent** のプロパティ］の ［接続］ タブで選択されているプロトコルに対応します)、手順 3 を実行します。
    - 接続済みの状態で、メッセージがキューにない場合は、Session Recording サーバーをホストするサーバーに問題がある可能性があります。手順 3 を省略し、手順 4 を実行します。
3. キューにメッセージがある場合は、Web ブラウザーを起動して次のアドレスを入力します:
    - HTTPS で接続する場合:`https://servername/msmq/private$/CitrixSmAudData`（ここで、`servername`は Session Recording サーバーをホストするマシンの名前です。）
    - HTTP で接続する場合: `http://servername/msmq/private$/CitrixSmAudData`（ここで、`servername`は Session Recording サーバーをホストするマシンの名前です。）

    「サーバーはセキュリティで保護された接続のみを受け付けます」というようなエラーが返される場合は、［**Session Recording Agent** のプロパティ］に一覧されている MSMQ プロトコルを HTTPS に変更します。Web サイトのセキュリティ証明書に問題があるというエラーが返される場合は、TLS のセキュアチャネルのための信頼関係に問題がある可能性があります。その場合は、正しい CA 証明書をインストールするか、信頼されている CA を使用します。
4. キューにメッセージがない場合は、Session Recording サーバーをホストするマシンにログオンし、専用キューを表示します。**citrixsmauddata** を選択します。キューにメッセージがある場合は（[メッセージ数] 列を確認します)、Session Recording StorageManager サービスが開始されていることを確認します。開始されていない場合は、サービスを再起動します。