



# Sitzungsaufzeichnung 2104

## Contents

<b>Neue Features</b>	<b>4</b>
<b>Behobene Probleme</b>	<b>4</b>
<b>Bekannte Probleme</b>	<b>4</b>
<b>Hinweise zu Drittanbietern</b>	<b>5</b>
<b>Systemanforderungen</b>	<b>6</b>
<b>Erste Schritte</b>	<b>8</b>
<b>Planen der Bereitstellung</b>	<b>10</b>
<b>Sicherheitsempfehlungen</b>	<b>13</b>
<b>Überlegungen zur Skalierbarkeit</b>	<b>19</b>
<b>Installieren, Aktualisieren und Deinstallieren</b>	<b>33</b>
<b>Dynamische Sitzungsaufzeichnung</b>	<b>60</b>
<b>Konfigurieren</b>	<b>65</b>
<b>Konfigurieren der Verbindung mit dem Sitzungsaufzeichnungsserver</b>	<b>66</b>
<b>Autorisieren von Benutzern</b>	<b>68</b>
<b>Richtlinien konfigurieren</b>	<b>69</b>
<b>Speicherort für Aufzeichnungen festlegen</b>	<b>103</b>
<b>Angeben der Dateigröße für Aufzeichnungen</b>	<b>109</b>
<b>Benachrichtigungsmeldungen anpassen</b>	<b>112</b>
<b>Aktivieren oder Deaktivieren der Aufzeichnung</b>	<b>112</b>
<b>Aktivieren oder Deaktivieren digitaler Signaturen</b>	<b>114</b>
<b>Administratorprotokollierung</b>	<b>115</b>
<b>Hohe Datenbankverfügbarkeit</b>	<b>118</b>
<b>Lastausgleich</b>	<b>119</b>

<b>Ändern des Kommunikationsprotokolls</b>	<b>123</b>
<b>Konfigurieren des Citrix-Programms zur Verbesserung der Benutzerfreundlichkeit (CEIP)</b>	<b>125</b>
<b>Protokollieren von Ereignissen</b>	<b>129</b>
<b>Anzeigen von Aufzeichnungen</b>	<b>144</b>
<b>Starten des Sitzungsaufzeichnungsplayers</b>	<b>144</b>
<b>Aktivieren und Deaktivieren von Livesitzungswiedergabe und Wiedergabeschutz</b>	<b>147</b>
<b>Öffnen und Wiedergeben von Aufzeichnungen</b>	<b>148</b>
<b>Hervorheben von Leerlaufperioden</b>	<b>156</b>
<b>Zwischenspeichern von Aufzeichnungen</b>	<b>156</b>
<b>Verwenden von Ereignissen und Textmarken</b>	<b>157</b>
<b>Suchen nach Aufzeichnungen</b>	<b>160</b>
<b>Webplayer für die Sitzungsaufzeichnung</b>	<b>162</b>
<b>Problembehandlung</b>	<b>184</b>
<b>Fehler bei der Installation von Serverkomponenten</b>	<b>185</b>
<b>Fehler beim Test der Datenbankverbindung während der Installation</b>	<b>185</b>
<b>Agent kann keine Verbindung mit dem Server herstellen</b>	<b>185</b>
<b>Verbindungsfehler zwischen dem Server und der Datenbank</b>	<b>187</b>
<b>Sitzungen werden nicht aufgezeichnet</b>	<b>189</b>
<b>Wiedergabe von Livesitzungen nicht möglich</b>	<b>190</b>
<b>Aufzeichnungen sind beschädigt oder unvollständig</b>	<b>190</b>
<b>Prüfen der Komponentenverbindungen</b>	<b>191</b>
<b>Fehler beim Suchen nach Aufzeichnungen im Player</b>	<b>194</b>
<b>Verwalten der Datensätze in der Datenbank</b>	<b>197</b>
<b>Bewährte Methoden</b>	<b>204</b>

<b>Konfigurieren des Lastausgleichs in einer vorhandenen Bereitstellung</b>	<b>204</b>
<b>Bereitstellen und Lastausgleich der Sitzungsaufzeichnung in Azure</b>	<b>252</b>



## Neue Features

November 5, 2021

### Neue Features in Release 2104

Dieses Release enthält die folgenden Erweiterungen und die Lösung für [ein Problem](#), um die Benutzererfahrung zu verbessern:

#### Verbesserung der Erstellung und Speicherung von Aufzeichnungsdateien

Zuvor wurden für alle Sitzungen bei deren Start Aufzeichnungsdateien erstellt und im Aufzeichnungsspeicherordner angezeigt. Die Dateien wurden dann gelöscht, wenn Richtlinien so festgelegt wurden, dass die Sitzungen nicht aufgezeichnet wurden. Ab diesem Release werden nur für Sitzungen Aufzeichnungsdateien erstellt, die tatsächlich aufgezeichnet werden.

## Behobene Probleme

February 2, 2022

Vergleich mit: Sitzungsaufzeichnung 2103

In Sitzungsaufzeichnung 2104 werden die folgenden Fixes hinzugefügt:

- Aufzeichnungsanzeigerichtlinien sind möglicherweise nicht sichtbar, wenn Sie die Datei `web.config` vor dem Upgrade der Version 7.15 der Sitzungsaufzeichnung manuell ändern. Die Datei `web.config` wird unter `\Citrix\SessionRecording\Server` gespeichert. [SRT-5740]

## Bekanntes Problem

April 3, 2024

Die folgenden Probleme wurden in diesem Release identifiziert:

- Wenn Sie [Citrix Web App Firewall \(WAF\)-Signaturen zur teilweisen Minderung des Sicherheitsrisikos CVE-2021-44228](#) verwenden, funktioniert die Sitzungsaufzeichnung möglicherweise nicht wie erwartet. Um das Problem zu beheben, schließen Sie die IP-Adressen Ihrer

Sitzungsaufzeichnungsserver von der Richtlinie **mitigate\_cve\_2021\_44228** auf der NetScaler-Seite aus. [CVADHELP-24365]

- Ein Domänenbenutzer mit lokalen Administratorrechten auf der Maschine mit der Richtlinienkonsole für die Sitzungsaufzeichnung kann sowohl lokale Benutzer als auch Domänenbenutzer hinzufügen, für die die Aktion einer Richtlinienregel gilt. Ein lokaler Benutzer mit lokalen Administratorrechten kann jedoch nur lokale Benutzer hinzufügen, aber keine Domänenbenutzer. [SRT-5769]
- Der Webplayer funktioniert nach einem Upgrade von Version 2009 oder früher möglicherweise nicht ordnungsgemäß. Löschen Sie den Cache Ihres Browsers, um das Problem zu umgehen. [SRT-5624]
- Regeln benutzerdefinierter Richtlinien für die Sitzungsaufzeichnung können nach dem Update der Sitzungsaufzeichnung von der in XenApp und XenDesktop 7.6 LTSR enthaltenen Version auf die neueste Version verloren gehen. Führen Sie als Workaround vor dem Update auf die neueste Version ein Update auf die Version aus, die im neuesten CU von XenApp und XenDesktop 7.15 LTSR enthalten ist. [SRT-4546]
- Wenn von Maschinenerstellungsdienste (MCS) oder Provisioning Services (PVS) mehrere VDAs mit dem konfigurierten Masterimage und installiertem Microsoft Message Queuing (MSMQ) erstellt werden, erhalten die VDAs unter bestimmten Bedingungen ggf. die gleiche **QMID**. Dies kann verschiedene Probleme verursachen, zum Beispiel:
  - Sitzungen werden nicht aufgezeichnet, selbst wenn eine Aufzeichnungsvereinbarung akzeptiert wurde.
  - Der Sitzungsaufzeichnungsserver empfängt möglicherweise keine Sitzungsabmeldungssignale, sodass Sitzungen dauerhaft den Zustand “live” behalten.

Informationen zu einem Workaround finden Sie unter [Installieren, Aktualisieren und Deinstallieren](#). [#528678]

## Hinweise zu Drittanbietern

January 15, 2024

[Sitzungsaufzeichnung Version 2104](#) (PDF-Download)

Dieses Release der Sitzungsaufzeichnung enthält u. U. Software von Drittanbietern, die gemäß den Bedingungen in diesem Dokument lizenziert wurden.

## Systemanforderungen

March 7, 2023

Die Komponenten der Sitzungsaufzeichnung umfassen Verwaltungskomponenten der Sitzungsaufzeichnung, den Sitzungsaufzeichnungsagent und den Sitzungsaufzeichnungsplayer. Sie können die Verwaltungskomponenten der Sitzungsaufzeichnung (Datenbank für die Sitzungsaufzeichnung, Sitzungsaufzeichnungsserver und Richtlinienkonsole) auf dem gleichen oder auf verschiedenen Servern installieren. Im folgenden Abschnitt werden die Anforderungen für die einzelnen Komponenten der Sitzungsaufzeichnung erläutert.

Weitere Informationen zur Verwendung dieser aktuellen Version (CR) in einer LTSR-Umgebung (Long Term Service Release) und zu anderen häufig gestellten Fragen finden Sie im [Knowledge Center-Artikel](#).

### Datenbank für die Sitzungsaufzeichnung

Unterstützte Betriebssysteme:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Unterstützte Microsoft SQL Server-Versionen:

- Microsoft SQL Server 2019 Enterprise, Express und Standard
- Microsoft SQL Server 2017 Enterprise, Express und Standard
- Microsoft SQL Server 2016 SP2 Enterprise, Express und Standard
- Microsoft SQL Server 2016 SP1 Enterprise, Express und Standard
- Microsoft SQL Server 2014 SP2 Enterprise, Express und Standard
- Microsoft SQL Server 2012 SP3 Enterprise, Express und Standard
- Microsoft SQL Server 2008 R2 SP3 Enterprise, Express und Standard

Unterstützte Azure SQL-Datenbankdienste:

- Verwaltete Azure SQL-Instanz
- SQL Server auf Azure-VMs  
(Verwenden Sie die zuvor aufgeführten unterstützten Versionen von Microsoft SQL Server.)

Unterstützte AWS RDS-Datenbankdienste:

- SQL Server

Voraussetzung: .NET Framework 4.7.2

## **Sitzungsaufzeichnungsserver**

Unterstützte Betriebssysteme:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Weitere Anforderungen:

- Internetinformationsdienste (IIS) Version 10, 8.5, 8.0 oder 7.5
- .NET Framework Version 4.7.2
- Wenn der Sitzungsaufzeichnungsserver HTTPS als Kommunikationsprotokoll verwendet, fügen Sie ein gültiges Zertifikat hinzu. Die Sitzungsaufzeichnung verwendet in der Standardeinstellung HTTPS; dies wird von Citrix empfohlen.
- Microsoft Message Queuing (MSMQ) mit deaktivierter Active Directory-Integration und aktivierter MSMQ-HTTP-Unterstützung
- Für die Administratorprotokollierung: neueste Version von Chrome, Firefox oder Internet Explorer 11

## **Richtlinienkonsole für die Sitzungsaufzeichnung**

Unterstützte Betriebssysteme:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Voraussetzung: .NET Framework 4.7.2

## **Sitzungsaufzeichnungsagent**

Installieren Sie den Sitzungsaufzeichnungsagent auf jedem Windows Virtual Delivery Agent (VDA), auf dem Sie Sitzungen aufzeichnen möchten.

Unterstützte Betriebssysteme:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10, Mindestversion 1607
- Windows 10 Enterprise für virtuelle Desktops

Anforderungen:

- Citrix Virtual Apps and Desktops 7 2103 mit Premium-Lizenz
- Citrix Virtual Apps and Desktops 7 1912 LTSR CU2 mit Platinum-Lizenz
- XenApp und XenDesktop 7.15 LTSR CU7 mit Platinum-Lizenz
- .NET Framework 4.7.2
- Microsoft Message Queuing (MSMQ) mit deaktivierter Active Directory-Integration und aktivierter MSMQ-HTTP-Unterstützung

## Sitzungsaufzeichnungsplayer

Unterstützte Betriebssysteme:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- 64-Bit-Windows 10, Mindestversion 1607

Voraussetzung: .NET Framework 4.7.2

**Hinweis:**

Unter 32-Bit-Windows 10 können Sie den Player nur über die Datei SessionRecordingPlayer.msi installieren. Die MSI-Datei ist im ISO-Image von Citrix Virtual Apps and Desktops unter **\layout\image-full\x86\Session Recording** gespeichert.

Für optimale Ergebnisse sollten Sie den Sitzungsaufzeichnungsplayer auf einer Arbeitsstation installieren, die folgende Anforderungen erfüllt:

- Eine Bildschirmauflösung von 1024 x 768
- Eine Farbtiefe von mindestens 32 Bit
- Mindestens 2 GB RAM, größere RAM- und CPU-/GPU-Ressourcen können die Leistung bei der Wiedergabe grafikintensiver Aufzeichnungen verbessern, insbesondere, wenn die Aufzeichnungen viele Animationen enthalten.

Die Reaktionszeit bei der Suche hängt von der Größe der Aufzeichnung und der Computerhardware ab.

## Erste Schritte

January 15, 2024

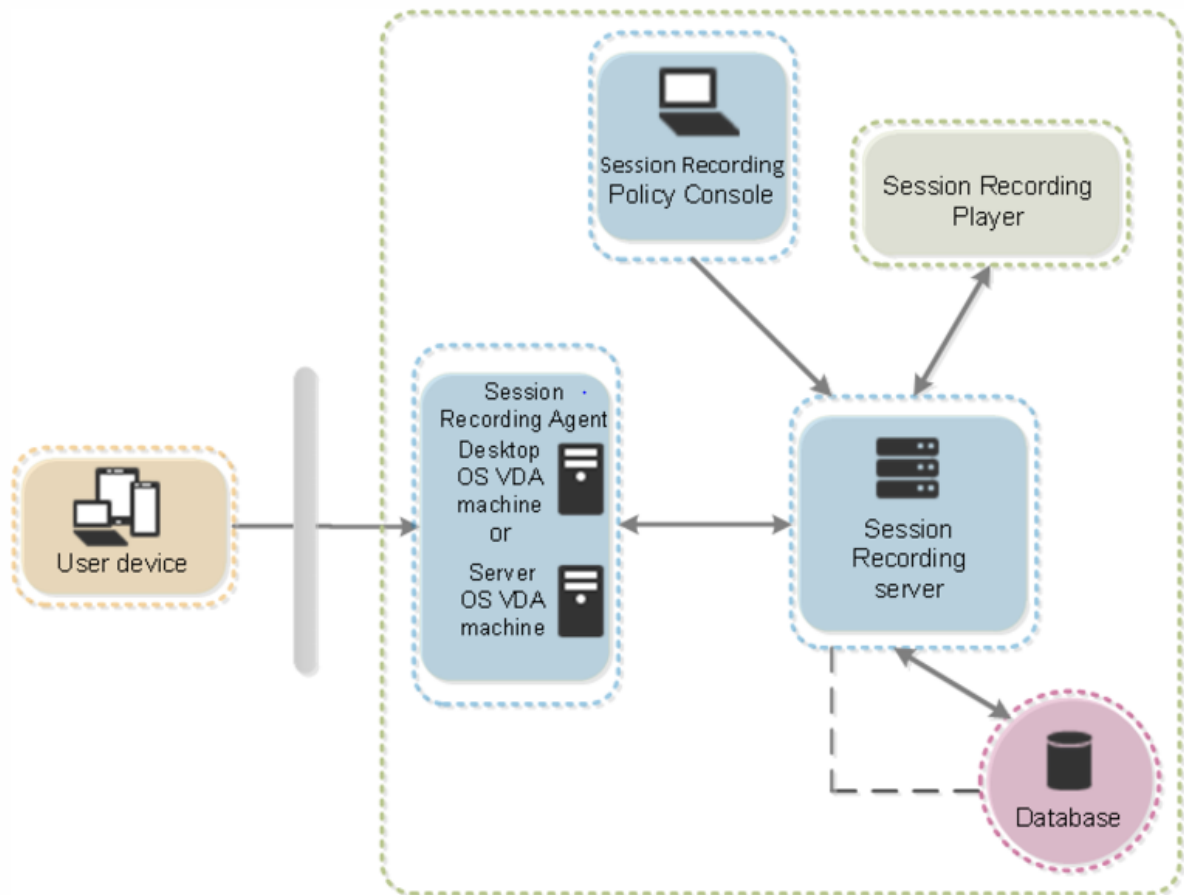
Die Sitzungsaufzeichnung besteht aus fünf Komponenten:

- **Sitzungsaufzeichnungsagent:** Komponente, die auf jedem VDA für Multisitzungs-OS oder Einzelsitzungs-OS installiert wird, um Aufzeichnungen zu ermöglichen. Mit dieser Komponente werden Sitzungsdaten aufgezeichnet.
- **Sitzungsaufzeichnungsserver:** Ein Server, auf dem die folgenden Programme ausgeführt werden:
  - Broker: Eine von IIS 6.0+ gehostete Webanwendung, die Such- und Dateidownloadanfragen vom Player und Richtlinienverwaltungsanforderungen von der Sitzungsaufzeichnungs-Richtlinienkonsole handhabt und Aufzeichnungsrichtlinien für jede Citrix Virtual Apps and Desktops-Sitzung auswertet.
  - Speichermanager: Ein Windows-Dienst, der Sitzungsaufzeichnungsdateien verwaltet, die von jedem für die Sitzungsaufzeichnung aktivierten Computer mit Citrix Virtual Apps and Desktops empfangen werden.
  - Administratorprotokollierung: Optionale Teilkomponente, die auf dem Sitzungsaufzeichnungsserver zum Protokollieren von Verwaltungsaktivitäten installiert wird. Alle Protokollierungsdaten werden in einer separaten SQL Server-Datenbank gespeichert, die standardmäßig **CitrixSessionRecordingLogging** heißt. Sie können den Datenbanknamen anpassen.
- **Sitzungsaufzeichnungsplayer:** Eine Benutzeroberfläche, auf die Benutzer von der Arbeitsstation aus zugreifen und mit der aufgezeichnete Sitzungsdateien wiedergegeben werden.
- **Datenbank für die Sitzungsaufzeichnung:** Eine Komponente, die die SQL Server-Datenbank zum Speichern von Sitzungsaufzeichnungsdaten verwaltet. Wenn diese Komponente installiert ist, erstellt sie standardmäßig eine Datenbank mit dem Namen **CitrixSessionRecording**. Sie können den Datenbanknamen anpassen.
- **Richtlinienkonsole für die Sitzungsaufzeichnung.** Konsole zum Erstellen von Richtlinien, um anzugeben, welche Sitzungen aufgezeichnet werden sollen.

In dieser Abbildung werden die Komponenten der Sitzungsaufzeichnung und deren Beziehung zueinander dargestellt:

Im dargestellten Beispiel einer Bereitstellung befinden sich der Sitzungsaufzeichnungsagent, der Sitzungsaufzeichnungsserver, die Datenbank für die Sitzungsaufzeichnung, die Richtlinienkonsole für die Sitzungsaufzeichnung und der Sitzungsaufzeichnungsplayer hinter einer Sicherheitsfirewall. Der Sitzungsaufzeichnungsagent ist auf einem VDA für Multisitzungs-OS oder Einzelsitzungs-OS installiert. Auf einem zweiten Server wird die Richtlinienkonsole für die Sitzungsaufzeichnung ausgeführt, ein dritter Server ist der Sitzungsaufzeichnungsserver und auf einem vierten Server wird die Datenbank für die Sitzungsaufzeichnung ausgeführt. Der Sitzungsaufzeichnungsplayer ist auf einer Arbeitsstation installiert. Ein Clientgerät außerhalb der Firewall kommuniziert mit dem VDA für Multisitzungs-OS, auf dem der Sitzungsaufzeichnungsagent installiert ist. Innerhalb der Firewall

kommunizieren der Sitzungsaufzeichnungsagent, die Richtlinienkonsole für die Sitzungsaufzeichnung, der Sitzungsaufzeichnungsplayer und die Datenbank für die Sitzungsaufzeichnung mit dem Sitzungsaufzeichnungsserver.



## Planen der Bereitstellung

January 15, 2024

### Einschränkungen und Hinweise

Die Sitzungsaufzeichnung unterstützt nicht den Anzeigemodus der Desktopgestaltungsumleitung (DCR). Wenn eine Sitzung gemäß Aufzeichnungsrichtlinie aufgezeichnet werden muss, deaktiviert die Sitzungsaufzeichnung standardmäßig DCR für diese Sitzung. Sie können dieses Verhalten in den Eigenschaften des Sitzungsaufzeichnungsagents konfigurieren.

Wenn einige URLs in der [Richtlinie zur Browserinhaltsumleitung](#) konfiguriert sind, die wurde in Version

7.16 des Windows VDA eingeführt, können Grafikaktivitäten beim Anzeigen dieser URLs im Internet Explorer-Browser nicht aufgezeichnet werden.

Die Sitzungsaufzeichnung unterstützt den Framehawk-Anzeigemodus nicht. Sitzungen im Framehawk-Anzeigemodus können nicht aufgezeichnet und einwandfrei wiedergegeben werden. Im Framehawk-Modus aufgezeichnete Sitzungen enthalten ggf. keine Sitzungsaktivitäten.

Die Sitzungsaufzeichnung kann keine Lync-Webcamvideos aufzeichnen, wenn das HDX RealTime Optimization Pack verwendet wird.

Abhängig von der Umgebung können Sie die Sitzungsaufzeichnungskomponenten in verschiedenen Szenarios bereitstellen.

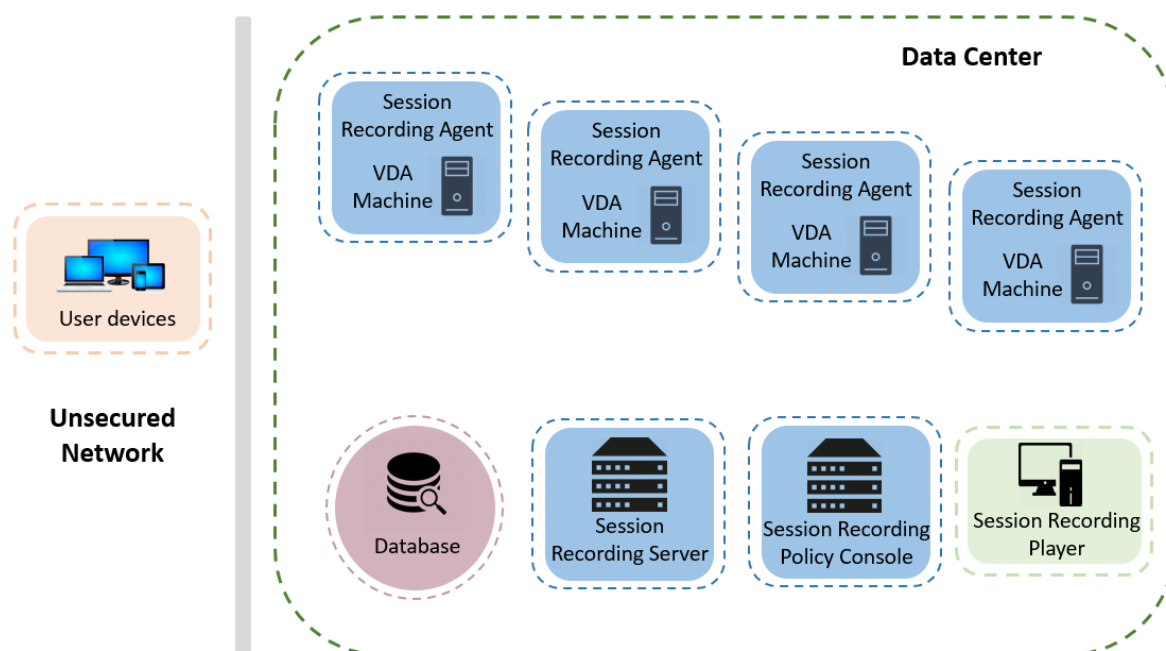
Eine Sitzungsaufzeichnungsbereitstellung muss nicht auf eine Site begrenzt sein. Mit Ausnahme des Sitzungsaufzeichnungsagents sind alle Komponenten von der Serversite unabhängig. Sie können beispielsweise mehrere Sites für einen Sitzungsaufzeichnungsserver konfigurieren.

Wenn Sie jedoch eine große Site mit vielen Instanzen der Agentsoftware haben und viele grafikintensive Anwendungen (z. B. AutoCAD-Anwendungen) oder viele Sitzungen aufzeichnen möchten, kann dies zu einem hohen Leistungsbedarf auf einem Sitzungsaufzeichnungsserver führen. Sie können zur Vermeidung von Leistungsproblemen mehrere Sitzungsaufzeichnungsserver installieren und das Lastausgleichsfeature aktivieren, damit die Sitzungsaufzeichnungsserver als Lastenausgleichspool fungieren und sich die Arbeitslast von verschiedenen VDAs teilen.

### **Empfohlene Serversitebereitstellung**

Verwenden Sie diesen Typ der Bereitstellung für die Aufzeichnung von Sitzungen für eine oder mehrere Sites. Der Sitzungsaufzeichnungsagent wird auf jedem VDA in einer Site installiert. Die Site befindet sich in einem Datacenter hinter einer Sicherheitsfirewall. Die Komponenten der Sitzungsaufzeichnungsverwaltung (Datenbank für die Sitzungsaufzeichnung, Sitzungsaufzeichnungsserver und Richtlinienkonsole für die Sitzungsaufzeichnung) sind außerhalb des Datacenters hinter der Firewall auf anderen Servern und der Sitzungsaufzeichnungsplayer ist auf einer Arbeitsstation installiert.





### Wichtige Bereitstellungshinweise

- Die Komponenten der Sitzungsaufzeichnung können nur miteinander kommunizieren, wenn sie in derselben Domäne oder in vertrauenswürdigen Domänen mit einer gegenseitigen Vertrauensbeziehung installiert sind. Das System kann nicht in einer Arbeitsgruppe oder in Domänen mit einer externen Vertrauensbeziehung installiert werden.
- Aufgrund des hohen Grafikanteils und der Speichernutzung bei der Wiedergabe von großen Aufzeichnungen, empfiehlt Citrix, dass der Sitzungsaufzeichnungsplayer nicht als veröffentlichte Anwendung installiert wird.
- Die Installation der Sitzungsaufzeichnung ist für die TLS/HTTPS-Kommunikation konfiguriert. Stellen Sie sicher, dass Sie ein Zertifikat auf dem Sitzungsaufzeichnungsserver installieren, und dass die Komponenten der Sitzungsaufzeichnung der Stammzertifizierungsstelle vertrauen.
- Wenn Sie die Sitzungsaufzeichnungsdatenbank auf einem eigenständigen Server installieren, auf dem Express Edition von SQL Server 2019, SQL Server 2017, SQL Server 2016, SQL Server 2014, SQL Server 2012 oder SQL Server 2008 R2 ausgeführt wird, muss auf dem Server das TCP/IP-Protokoll aktiviert sein und der SQL Server-Browserdienst ausgeführt werden. Diese Einstellungen sind standardmäßig deaktiviert, müssen jedoch für die Kommunikation zwischen dem Sitzungsaufzeichnungsserver und der Datenbank aktiviert werden. Informationen zur Aktivierung dieser Einstellungen finden Sie in den Microsoft-Artikeln [Enable TCP/IP Network Protocol for SQL Server](#) und [SQL Server Browser Service](#).
- Berücksichtigen Sie bei der Planung der Sitzungsaufzeichnungsbereitstellung die Auswirkungen der Sitzungsfreigabe. Die Sitzungsfreigabe für veröffentlichte Anwendungen kann

Konflikte mit Richtlinienregeln für Sitzungsaufzeichnungen für veröffentlichte Anwendungen verursachen. Die Sitzungsaufzeichnung ordnet die aktive Richtlinie der ersten veröffentlichten Anwendung zu, die ein Benutzer öffnet. Wenn der Benutzer die erste Anwendung geöffnet hat, halten weitere Anwendungen, die in derselben Sitzung geöffnet werden, die Richtlinie ein, die für die erste Anwendung gilt. Beispiel: Wenn eine Richtlinie festlegt, dass nur Outlook aufgezeichnet wird, beginnt die Aufzeichnung, wenn der Benutzer Outlook öffnet. Wenn der Benutzer Microsoft Word als zweite veröffentlichte Anwendung öffnet (während Outlook ausgeführt wird), wird Word auch aufgezeichnet. Sollte die aktive Richtlinie jedoch nicht festlegen, dass Word aufgezeichnet wird, und der Benutzer startet Word vor Outlook, wird Outlook nicht aufgezeichnet.

- Das Installieren des Sitzungsaufzeichnungsservers auf einem Delivery Controller kann zu Leistungsbeeinträchtigungen führen und Citrix empfiehlt es daher nicht; es ist jedoch grundsätzlich möglich.
- Sie können die Richtlinienkonsole für die Sitzungsaufzeichnung auf einem Delivery Controller installieren.
- Sie können den Sitzungsaufzeichnungsserver und die Richtlinienkonsole für die Sitzungsaufzeichnung auf demselben System installieren.
- Stellen Sie sicher, dass der NetBIOS-Name des Sitzungsaufzeichnungsservers nicht länger als 15 Zeichen ist. Microsoft begrenzt die Länge des Hostnamens auf max. 15 Zeichen.
- PowerShell 5.1 oder höher ist für die benutzerdefinierte Ereignisprotokollierung erforderlich. Aktualisieren Sie PowerShell, wenn Sie den Sitzungsaufzeichnungsagent unter Windows Server 2012 R2 installieren, für das PowerShell 4.0 installiert ist. Die Nichteinhaltung kann zu fehlgeschlagenen API-Aufrufen führen.

## Sicherheitsempfehlungen

January 15, 2024

Die Sitzungsaufzeichnung wird in einem sicheren Netzwerk mit Zugriff durch Administratoren bereitgestellt und ist daher sicher. Die Standardbereitstellung ist einfach, und Sicherheitsfunktionen, z. B. digitale Signatur und Verschlüsselung, können optional konfiguriert werden.

Die Komponenten der Sitzungsaufzeichnung kommunizieren über die Internetinformationsdienste (IIS) und Microsoft Message Queuing (MSMQ). Internetinformationsdienste stellen die Webdienstkommunikationsverbindung zwischen den Komponenten der Sitzungsaufzeichnung bereit. MSMQ bietet eine zuverlässige Datentransportmethode zum Senden von Sitzungsaufzeichnungsdaten vom Sitzungsaufzeichnungsagent zum Sitzungsaufzeichnungsserver.

**Warnung:**

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Berücksichtigen Sie diese Sicherheitsempfehlungen bei der Planung der Bereitstellung:

- Die verschiedenen Administratorrollen im Unternehmensnetzwerk, in der Sitzungsaufzeichnung und auf einzelnen Maschinen müssen ordnungsgemäß isoliert werden. Andernfalls besteht Gefahr durch Sicherheitsbedrohungen. Gefahr für den Systembetrieb und das System kann zweckentfremdet verwendet werden. Wir empfehlen, dass Sie unterschiedliche Administratorrollen verschiedenen Personen oder Konten zuweisen. Erteilen Sie normalen Sitzungsbenutzern keine Administratorprivilegien für das VDA-System.
  - Administratoren von Citrix Virtual Apps and Desktops erteilen keinem Benutzer von veröffentlichten Anwendungen oder Desktops die lokale Administratorrolle für den VDA. Wird die lokale Administratorrolle benötigt, schützen Sie die Komponenten des Sitzungsaufzeichnungsagents über Windows-Methoden oder die Lösung eines anderen Herstellers.
  - Weisen Sie die Administratorrollen für die Datenbank und die Richtlinie der Sitzungsaufzeichnung separat zu.
  - Wir empfehlen, dass Sie VDA-Administratorrechte nicht allgemeinen Sitzungsbenutzern zuweisen, besonders, wenn Remote-PC-Zugriff verwendet wird.
  - Das lokale Administratorkonto des Sitzungsaufzeichnungsservers muss streng geschützt werden.
  - Steuern Sie den Zugriff auf Maschinen, auf denen der Sitzungsaufzeichnungsplayer installiert ist. Hat ein Benutzer keine Playerrollenberechtigung, weisen Sie ihm für keinerlei Player-Maschinen eine lokale Administratorrolle zu. Deaktivieren Sie den anonymen Zugriff.
  - Wir empfehlen, eine physische Maschine als Speicherserver für die Sitzungsaufzeichnung zu verwenden.
- Die Sitzungsaufzeichnung zeichnet Grafikaktivitäten ohne Berücksichtigung des Datenschutzes auf. Unter bestimmten Umständen können sensible Daten (z. B. Benutzeranmeldeinformationen, persönliche Daten oder Bildschirme von Drittanbietern) unbeabsichtigt aufgezeichnet werden. Ergreifen Sie folgende Maßnahmen, um ein Risiko zu vermeiden:
  - Deaktivieren Sie das Kernspeicherabbild für VDAs, es sei denn, es wird zur Problembehandlung benötigt.

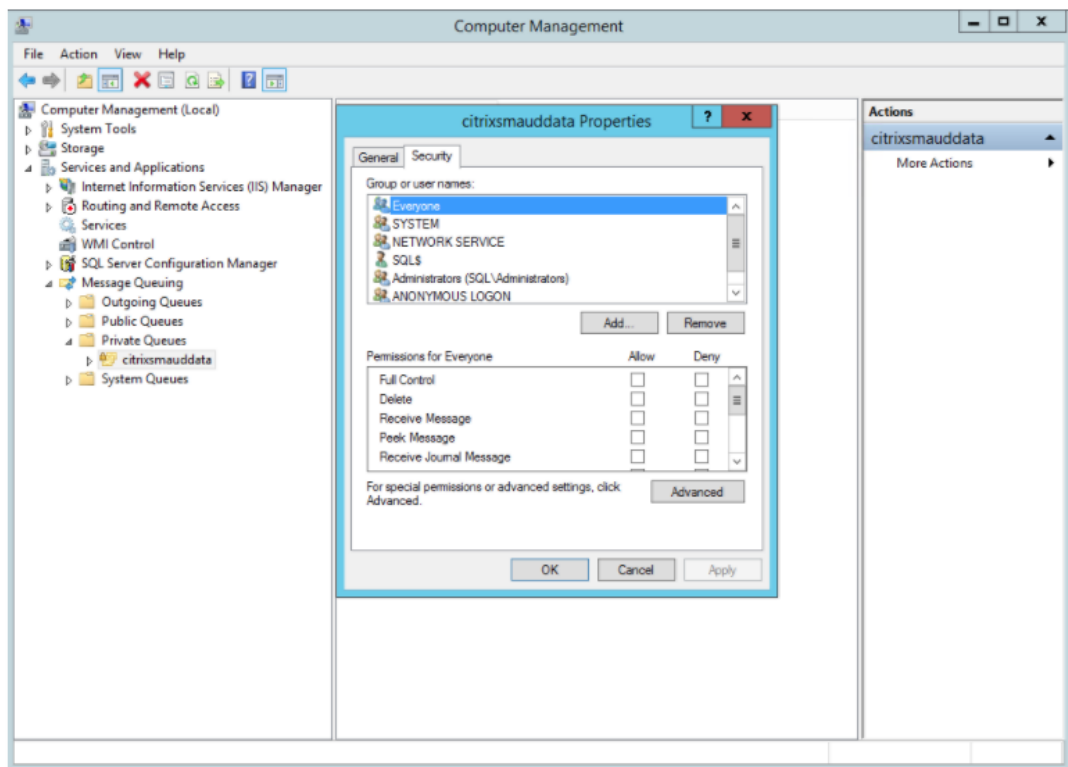
Zum Deaktivieren des Kernspeicherabbilds gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Erweitert** und dann unter **Starten und Wiederherstellen** auf **Einstellungen**.
3. Wählen Sie für **Debuginformationen speichern** die Option **Keine**.

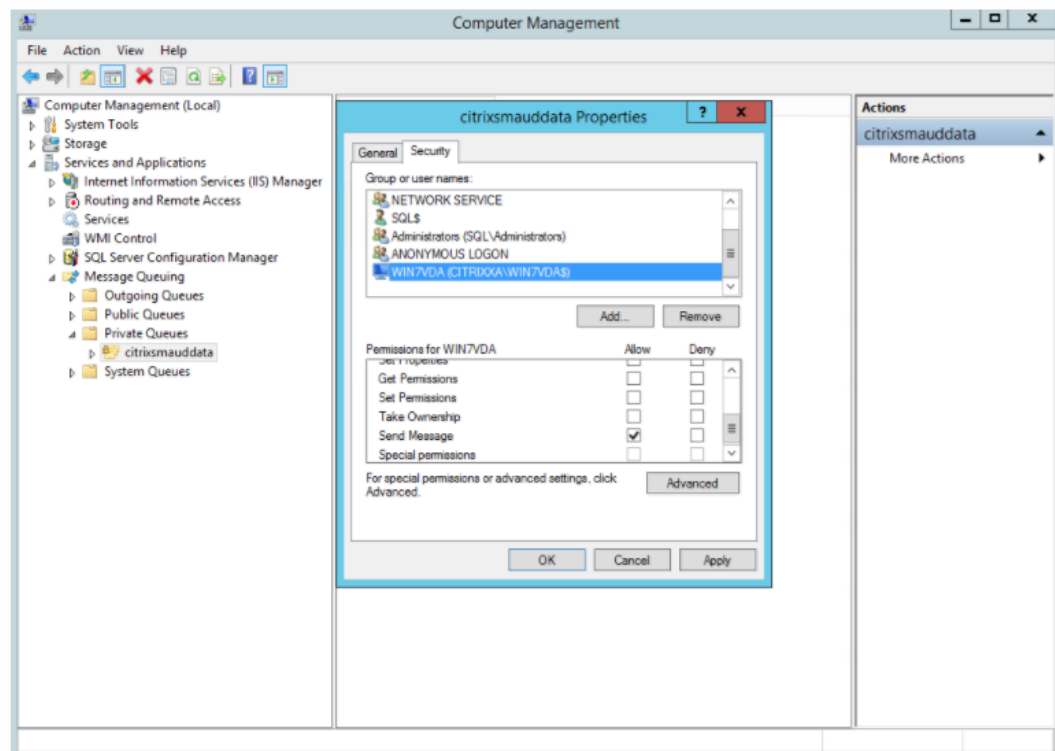
Weitere Informationen finden Sie im Microsoft-Artikel unter <https://support.microsoft.com/en-us/kb/307973>.

- Sitzungseigentümer machen die Teilnehmer darauf aufmerksam, dass Software von Online-Meetings und Remoteunterstützung im Rahmen einer Desktopsitzungsaufzeichnung aufgezeichnet werden kann.
  - Stellen Sie sicher, dass keine Anmelde- und Sicherheitsinformationen in veröffentlichten lokalen Anwendungen oder Webanwendungen oder unternehmensintern verwendeten Anwendungen angezeigt werden. Andernfalls werden die Informationen durch die Sitzungsaufzeichnung aufgezeichnet.
  - Schließen Sie vor Beginn einer ICA-Sitzung jede Anwendung, in der u. U. vertrauliche Informationen angezeigt werden.
  - Für den Zugriff auf veröffentlichte Desktops oder SaaS-Anwendungen wird ausschließlich der Einsatz automatischer Authentifizierungsmethoden (z. B. Single Sign-On oder Smartcard) empfohlen.
- Zur ordnungsgemäßen Funktion und zur Erfüllung von Sicherheitsanforderungen bei der Sitzungsaufzeichnung ist eine spezifische Hardware/-infrastruktur (z. B. Unternehmensnetzwerkgeräte, Betriebssystem) erforderlich. Sorgen Sie auf Infrastrukturebene dafür, dass diese Elemente weder beschädigt noch missbraucht werden können und dass die Sitzungsaufzeichnung sicher und zuverlässig ausgeführt wird.
    - Schützen und Sie die für die Sitzungsaufzeichnung verwendete Netzwerkinfrastruktur und sorgen Sie für deren zuverlässige Verfügbarkeit.
    - Wir empfehlen, eine Sicherheitslösung eines Drittanbieters oder Windows-Mechanismen zum Schutz der Sitzungsaufzeichnungskomponenten zu verwenden. Die Sitzungsaufzeichnung umfasst folgende Komponenten:
      - \* Auf dem Sitzungsaufzeichnungsserver
        - Prozesse: SsRecStorageManager.exe und SsRecAnalyticsService.exe
        - Dienste: CitrixSsRecStorageManager und CitrixSsRecAnalyticsService
        - Alle Dateien im Installationsordner des Sitzungsaufzeichnungsservers
        - Registrierungswerte unter HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server
      - \* Auf dem Sitzungsaufzeichnungsagent
        - Prozess: SsRecAgent.exe
        - Dienst: CitrixSmAudAgent
        - Alle Dateien im Installationsordner des Sitzungsaufzeichnungsagents

- Registrierungswerte unter HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent
- Schränken Sie über die Zugriffssteuerungsliste (ACL) für Message Queuing (MSMQ) auf dem Sitzungsaufzeichnungsserver VDA- und VDI-Maschinen ein, die MSMQ-Daten an den Sitzungsaufzeichnungsserver senden können, und blockieren Sie das Senden von Daten an den Sitzungsaufzeichnungsserver durch unbefugte Maschinen.
  1. Installieren Sie das Serverfeature Directory Service Integration auf jeder Sitzungsaufzeichnungsserver- und VDA- oder VDI-Maschine, auf der die Sitzungsaufzeichnung aktiviert ist. Starten Sie dann den Message Queuing-Dienst neu.
  2. Öffnen Sie auf jedem Sitzungsaufzeichnungsserver über das **Startmenü** von Windows **Verwaltungstools > Computerverwaltung**.
  3. Öffnen Sie **Dienste und Anwendungen > Message Queuing > Private Warteschlangen**.
  4. Klicken Sie auf die private Warteschlange **citrixsmduddata**, um die Seite **Eigenschaften** zu öffnen, und wählen Sie die Registerkarte **Sicherheit**.



5. Fügen Sie die Computer bzw. Sicherheitsgruppen der VDAs, die MSMQ-Daten an diesen Server senden, hinzu und erteilen Sie diesen die Berechtigung zum **Senden von Nachrichten**.



- Schützen Sie das Ereignisprotokoll des Sitzungsaufzeichnungsservers und des Sitzungsaufzeichnungsagents. Citrix empfiehlt die Verwendung einer Remoteprotokollierungslösung eines Drittanbieters oder eines entsprechenden Windows-Features zum Schutz des Ereignisprotokolls oder dessen Umleitung auf einen Remoteserver.
- Stellen Sie sicher, dass die Server mit den Sitzungsaufzeichnungskomponenten physisch geschützt werden. Schließen Sie diese Computer falls möglich in einem sicheren Raum ein, zu dem nur autorisierte Person direkten Zugang haben.
- Isolieren Sie die Server mit den Sitzungsaufzeichnungskomponenten in einem separaten Subnetz oder einer separaten Domäne.
- Installieren Sie eine Firewall zwischen dem Sitzungsaufzeichnungsserver und den anderen Servern, um die aufgezeichneten Sitzungsdaten vor Benutzern zu schützen, die auf andere Server zugreifen.
- Halten Sie den Verwaltungsserver und die SQL-Datenbank für die Sitzungsaufzeichnung durch Installation der aktuellen Sicherheitsupdates von Microsoft auf dem neuesten Stand.
- Verhindern Sie, dass Personen ohne Administratorberechtigung sich beim Verwaltungscomputer anmelden.
- Schränken Sie genau ein, welche Benutzer die Aufzeichnungsrichtlinien ändern und Sitzungsaufzeichnungen anzeigen können.

- Installieren Sie digitale Zertifikate, verwenden Sie die Funktion zur Dateisignatur der Sitzungsaufzeichnung und richten Sie die TLS-Kommunikation in IIS ein.
- Richten Sie MSMQ ein und legen Sie als Transportprotokoll HTTPS fest. Legen Sie zu diesem Zweck das MSMQ-Transportprotokoll in **Sitzungsaufzeichnungsagent - Eigenschaften** auf HTTPS fest. Weitere Informationen finden Sie unter [Problembehandlung bei MSMQ](#).
- Verwenden Sie TLS 1.1 oder TLS 1.2 (empfohlen) und deaktivieren Sie die Verschlüsselungsverfahren SSLv2, SSLv3 und TLS 1.0 auf dem Sitzungsaufzeichnungsserver und in der Datenbank für die Sitzungsaufzeichnung.
- Deaktivieren Sie die RC4-Verschlüsselungssammlungen für TLS auf dem Sitzungsaufzeichnungsserver und in der Datenbank für die Sitzungsaufzeichnung:
  1. Navigieren Sie mit dem Microsoft Gruppenrichtlinien-Editor zu **Computerkonfiguration > Administrative Vorlagen > Netzwerk > SSL-Konfigurationseinstellungen**.
  2. Legen Sie die Richtlinie **Reihenfolge der SSL-Verschlüsselungssammlungen** auf **Aktiviert** fest. Standardmäßig ist diese Richtlinie auf **Nicht konfiguriert** festgelegt.
  3. Entfernen Sie alle RC4-Verschlüsselungssammlungen.
- Verwenden Sie den Wiedergabeschutz. Der Wiedergabeschutz ist eine Funktion der Sitzungsaufzeichnung, mit der aufgezeichnete Dateien vor dem Download zum Sitzungsaufzeichnungsplayer verschlüsselt werden. Diese Option ist in der Standardeinstellung aktiviert und befindet sich in den **Sitzungsaufzeichnungsserver - Eigenschaften**.
- Folgen Sie den Anleitungen von NSIT für die Länge der Kryptografieschlüssel und den Kryptografiealgorithmen.
- Konfigurieren Sie TLS 1.2-Unterstützung für die Sitzungsaufzeichnung.

Wir empfehlen, TLS 1.2 als Kommunikationsprotokoll zu verwenden, um eine lückenlose Sicherheit für die Sitzungsaufzeichnungskomponenten sicherzustellen.

#### **Konfigurieren der TLS 1.2-Unterstützung für die Sitzungsaufzeichnung:**

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an. Installieren Sie die erforderlichen SQL Server-Clientkomponenten und -Treiber und legen Sie für .NET Framework (Version 4 oder höher) starke Kryptografie fest.
  - a) Installieren Sie Microsoft ODBC Driver 11 (oder eine neuere Version) for SQL Server.
  - b) Wenden Sie das aktuelle Hotfix-Rollup für .NET Framework an.
  - c) Installieren Sie **ADO.NET – SqlClient** gemäß Ihrer Version von .NET Framework. Weitere Informationen finden Sie unter <https://support.microsoft.com/en-us/kb/3135244>.
  - d) Fügen Sie DWORD-Wert SchUseStrongCrypto = 1 hinzu unter HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\Install\Source\MSI\MSIEXEC\Parameters und HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NetFramework\v4.0.30319.

- e) Starten Sie die Maschine neu.
2. Melden Sie sich bei der Maschine mit der Richtlinienkonsole für die Sitzungsaufzeichnung an. Wenden Sie das aktuelle Hotfix-Rollup für .NET Framework an und legen Sie für .NET Framework (Version 4 oder höher) starke Kryptografie fest. Die Methode zum Festlegen von starker Kryptografie ist identisch mit den Schritten 1-4 und 1-5. Sie können diese Schritte auslassen, wenn Sie die Richtlinienkonsole für die Sitzungsaufzeichnung auf demselben Computer wie den Sitzungsaufzeichnungsserver installieren.

Informationen zum Konfigurieren der TLS 1.2-Unterstützung für SQL Server-Versionen vor 2016 finden Sie unter <https://support.microsoft.com/en-us/kb/3135244>. Zur Verwendung von TLS 1.2 konfigurieren Sie HTTPS als Kommunikationsprotokoll für die Komponenten der Sitzungsaufzeichnung.

## Überlegungen zur Skalierbarkeit

January 15, 2024

Die Sitzungsaufzeichnung ist ein hochskalierbares System, das zehntausende Sitzungen verarbeiten kann. Zum Installieren und Ausführen der Sitzungsaufzeichnung sind nur wenige Ressourcen erforderlich, die nicht schon für Citrix Virtual Apps and Desktops gebraucht werden. Wenn Sie jedoch viele Sitzungen mit der Sitzungsaufzeichnung aufzeichnen möchten oder die Sitzungen, die Sie aufzeichnen möchten, möglicherweise große Sitzungsdateien erstellen (z. B. Anwendungen mit hohem Grafikanteil), sollten Sie die Leistung des Systems berücksichtigen, wenn Sie die Bereitstellung der Sitzungsaufzeichnung planen.

In diesem Artikel werden die Grundlagen der hohen Skalierbarkeit der Sitzungsaufzeichnung behandelt und es wird erläutert, wie Sie das System mit möglichst geringem Kostenaufwand optimal nutzen können.

### Faktoren für die gute Skalierbarkeit der Sitzungsaufzeichnung

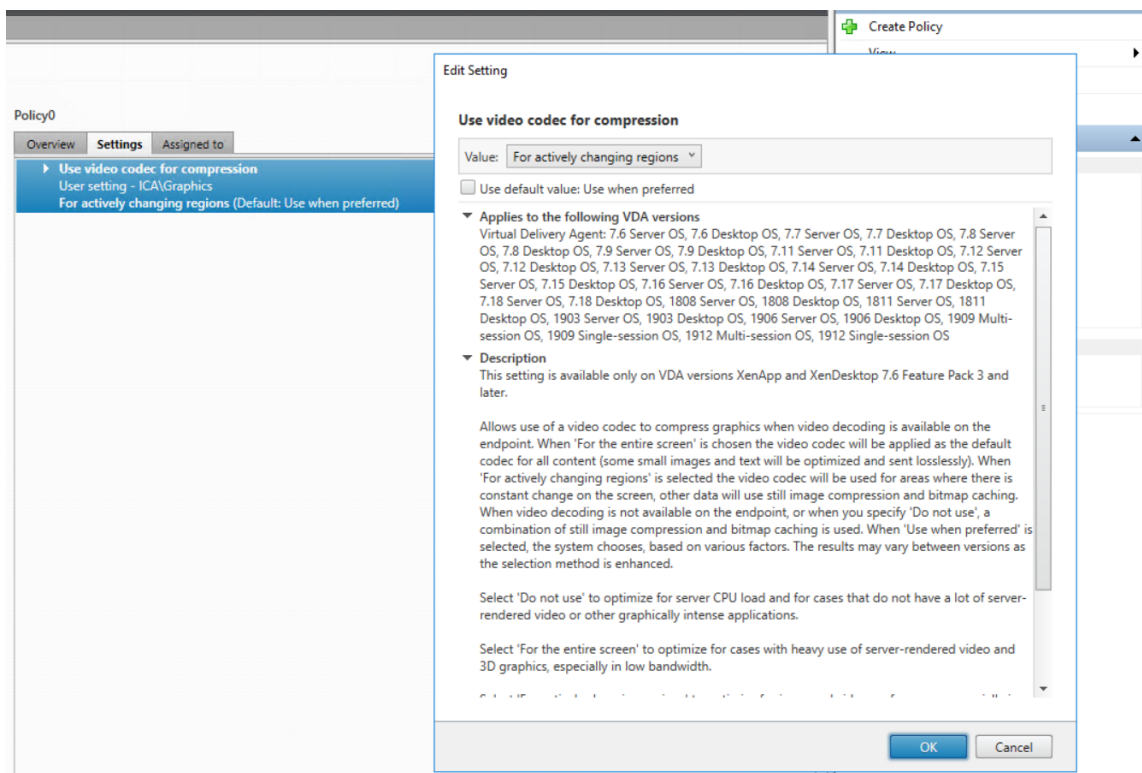
Es gibt zwei Hauptgründe für die im Vergleich zu Produkten von Mitbewerbern gute Skalierbarkeit der Sitzungsaufzeichnung:

- Kleine Dateigröße

Mit der Sitzungsaufzeichnung erstellte Aufzeichnungsdateien sind extrem kompakt. Sie sind um ein Vielfaches kleiner als äquivalente Videoaufnahmen, die von auf Screen Scraping basierenden Lösungen erstellt werden. Für die Übermittlung und Speicherung von Sitzungsaufzeichnungsdateien ist der Bedarf an Netzwerkbandbreite, Festplattenspeicher und Datenträger-IOPS in der Regel mindestens zehnmal geringer als bei äquivalenten Videodateien.



Die geringe Größe von Sitzungsaufzeichnungsdateien sorgt für eine schnellere und nahtlosere Wiedergabe von Videobildern. Die Aufzeichnung ist zudem verlustfrei und weist im Gegensatz zu den meisten kompakten Videoformaten keinerlei Pixelierung auf. Text in Aufzeichnungen ist bei der Wiedergabe genauso leicht zu lesen wie in der ursprünglichen Sitzung. Zur Minimierung der Dateigrößen werden bei der Sitzungsaufzeichnung keine Keyframes innerhalb von Dateien aufgezeichnet. Beim Aufzeichnen von Sitzungen mit Videowiedergabe können H.264-Pakete verworfen werden, um die Dateigröße der Aufzeichnung zu reduzieren. Zum Verwenden dieser Funktionalität legen Sie im Sitzungsaufzeichnungsagenten `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\DropH264Enabled` auf 1 fest und wählen für **Videocodex zur Komprimierung verwenden** die Einstellung **Für aktive Änderungsbereiche**.



- Geringer Verarbeitungsaufwand zum Generieren von Dateien

Eine Sitzungsaufzeichnungsdatei enthält die ICA-Protokolldaten für eine Sitzung, die virtuell im nativen Format extrahiert werden. Die Datei erfasst den ICA-Protokolldatenstrom, der für die Kommunikation mit der Citrix Workspace-App verwendet wird. Es müssen keine teuren Transcodierer oder Encoder zur Formatumwandlung in Echtzeit ausgeführt werden. Der geringe Verarbeitungsaufwand ist auch für die VDA-Skalierbarkeit wichtig und gewährleistet eine gute Benutzererfahrung, wenn ein VDA viele Sitzungen aufzeichnet.

Darüber hinaus werden nur die virtuellen ICA-Kanäle aufgezeichnet, die wiedergegeben werden können –eine weitere Optimierung. Beispielsweise werden der Drucker- und Clientlaufw-

erkzuordnungskanal nicht aufgezeichnet, da sie hohe Datenmengen erzeugen und ohne Vorteil für die Videowiedergabe sind.

## **Schätzung der Dateneingabe- und Verarbeitungsraten**

Der Sitzungsaufzeichnungsserver ist der zentrale Sammelpunkt für Sitzungsaufzeichnungsdateien. Jede Maschine mit Multisitzungs-OS und aktivierter Sitzungsaufzeichnung sendet Sitzungsaufzeichnungsdaten an den Sitzungsaufzeichnungsserver. Die Sitzungsaufzeichnung kann große Datenmengen verarbeiten und ist burst- und fehlertolerant. Es gibt jedoch physische Limits für die Datenmenge, die einzelne Server verarbeiten können.

Berücksichtigen Sie, wie viele Daten an jeden Sitzungsaufzeichnungsserver gesendet werden und wie schnell die Server diese Daten verarbeiten und speichern können. Die Rate, mit der das System die eingehenden Daten speichern kann, muss größer als die Dateneingaberate sein.

Sie können die Dateneingaberate schätzen, wenn Sie die Anzahl der aufgezeichneten Sitzungen mit der durchschnittlichen Größe jeder Sitzungsaufzeichnung multiplizieren und durch die Länge der Sitzungsaufzeichnungen dividieren. Beispiel: An einem 8-stündigen Arbeitstag zeichnen Sie 5000 Microsoft Outlook-Sitzungen auf, deren Größe 20 MB ist. Die Dateneingaberate beträgt dann ungefähr 3,5 MBit/s (5000 Sitzungen multipliziert mit 20 MB und dividiert durch 8 Stunden, dividiert durch 3600 Sekunden pro Stunde.) Ein an ein 100-MBit/s-LAN angeschlossener Sitzungsaufzeichnungsserver mit ausreichend Festplattenspeicher für die aufgezeichneten Daten kann basierend auf den physischen Limits durch Datenträger- und Netzwerk-IOPS in der Regel rund 5,0 MBit Daten pro Sekunde verarbeiten. Diese Rate ist die Verarbeitungsrate. In diesem Beispiel ist die Verarbeitungsrate (5,0 MBit/s) höher als die Eingaberate (3,5 MBit/s) und die Aufzeichnung der 5.000 Outlook-Sitzungen ist somit möglich.

Die pro Sitzung entstehenden Datenmengen können je nach aufgezeichneten Inhalten sowie Bildschirmauflösung, Farbtiefe und Grafikmodus stark variieren. Eine Sitzung, in der eine CAD-Anwendung mit konstant hoher Grafikaktivität ausgeführt wird, generiert wesentlich mehr Aufzeichnungsdaten als eine Sitzung, in der E-Mail in Microsoft Outlook gesendet und empfangen wird. Daher kann die Aufzeichnung einer identischen Anzahl CAD-Sitzungen eine hohe Eingaberate aufweisen und die Verwendung zusätzlicher Sitzungsaufzeichnungsserver erfordern.

## **Bursts und Fehler**

Das obige Beispiel basiert auf einem einfachen und konstanten Datendurchsatz und berücksichtigt keine Bursts –kurze Zeiträume mit höherer Aktivität. Ein Burst kann beispielsweise morgens auftreten, wenn sich alle Benutzer zur gleichen Zeit anmelden, oder wenn alle Benutzer die gleiche E-Mail im Outlook-Posteingang erhalten. Die Verarbeitungsrate des Sitzungsaufzeichnungsservers von 5,0 MBit/s ist zur Bewältigung eines solchen Bursts äußerst unzureichend.

Der auf jedem VDA ausgeführte Sitzungsaufzeichnungsagent sendet aufgezeichnete Daten unter Einsatz von Microsoft Message Queuing (MSMQ) an den Speichermanager, der auf dem zentralen Sitzungsaufzeichnungsserver ausgeführt wird. Die Daten werden im Teilstreckenverfahren (store and forward) gesendet, ähnlich wie E-Mail, die vom Absender über einen Mailserver an den Empfänger gesendet wird. Wenn der Sitzungsaufzeichnungsserver oder das Netzwerk die hohe Datenrate eines Bursts nicht verarbeiten kann, werden die aufgezeichneten Sitzungsdaten vorübergehend gespeichert, bis die aufgelaufenen Datennachrichten verarbeitet sind. Datennachrichten werden, wenn das Netzwerk überlastet ist, in der Ausgangswarteschlange auf dem VDA zwischengespeichert oder aber in der Eingangswarteschlange des Sitzungsaufzeichnungsservers, wenn sie bereits das Netzwerk durchlaufen haben und der Speichermanager noch andere Nachrichten verarbeitet.

MSMQ dient auch als Fehlertoleranzmechanismus. Fällt der Sitzungsaufzeichnungsserver aus oder wird die Verbindung unterbrochen, dann werden aufgezeichnete Daten in der Ausgangswarteschlange auf den VDAs gespeichert. Nach Beseitigung des Fehlers werden alle Daten in den Warteschlangen zusammen gesendet. Die Verwendung von MSMQ ermöglicht außerdem das Offlineschalten eines Sitzungsaufzeichnungsservers für Upgrades oder Wartungszwecke, ohne dass die Aufzeichnung bestehender Sitzungen unterbrochen wird und Daten verloren gehen.

Die Haupteinschränkung von MSMQ besteht darin, dass der Speicherplatz für die temporäre Speicherung von Datennachrichten begrenzt ist. Diese Einschränkung bestimmt, wie lange ein Burst-, Fehler- oder Wartungsereignis dauern kann, bis Daten verloren gehen. Das Gesamtsystem kann nach Datenverlust weiter ausgeführt werden, doch fehlen in diesem Fall Datenblöcke in einzelnen Aufzeichnungen. Eine Datei mit fehlenden Daten kann zwar wiedergegeben werden, doch nur bis zu dem Punkt des ersten Datenverlusts. Beachten Sie Folgendes:

- Die Ausstattung aller Server und insbesondere des Sitzungsaufzeichnungsservers mit mehr Speicherplatz und dessen Bereitstellung für MSMQ kann die Burst- und Fehlertoleranz erhöhen.
- Es ist wichtig, die Einstellung "Nachrichtenlebensdauer" (auf der Registerkarte **Verbindungen** in den Agenteigenschaften) für jeden Sitzungsaufzeichnungsagent auf einen geeigneten Wert festzulegen. Der Standardwert von 7.200 Sekunden (zwei Stunden) bedeutet, dass aufgezeichnete Datennachrichten zwei Stunden haben, um den Speichermanager zu erreichen. Nach Ablauf dieses Zeitraums werden sie verworfen und die Aufzeichnungsdateien werden beschädigt. Wenn mehr Speicherplatz verfügbar ist (oder weniger Sitzungen aufgezeichnet werden), können Sie diesen Wert erhöhen. Der maximale Wert beträgt 365 Tage.

Die andere Einschränkung bei MSMQ besteht darin, dass es bei einem Auflaufen von Daten in der Warteschlange zu zusätzlichen IOPS für das Lesen und Schreiben von Datennachrichten kommt. Unter normalen Bedingungen empfängt und verarbeitet der Speichermanager Daten direkt aus dem Netzwerk, ohne dass Datennachrichten auf den Datenträger geschrieben werden. Das Speichern der Daten erfordert einen Schreibvorgang auf dem Datenträger, der die Sitzungsaufzeichnungsdatei anfügt. Bei einem Auflaufen von Daten verdreifachen sich die Datenträger-IOPS: Jede Nachricht muss auf den Datenträger geschrieben, von diesem gelesen und in eine Datei geschrieben werden.

Da der Speichermanager sehr IOPS-gebunden ist, sinkt die Verarbeitungsrate des Sitzungsaufzeichnungsservers, bis die aufgelaufenen Nachrichten verarbeitet sind. Zur Minderung der Auswirkungen dieser zusätzlichen IOPS wird Folgendes empfohlen:

- Stellen Sie sicher, dass MSMQ Nachrichten auf einem anderen Datenträger speichert als dem, auf dem die Aufzeichnungsdateien gespeichert werden. Obwohl sich der IOPS-Wert verdreifacht, sinkt die reale Verarbeitungsrate nicht im gleichen Maß.
- Sorgen Sie dafür, dass geplante Ausfälle nur zu Nebenzeiten stattfinden. Folgen Sie unter Berücksichtigung von Budgetlimits anerkannten Ansätzen zum Erstellen hoch verfügbarer Server. Dazu gehören der Einsatz von UPS, duale Netzwerkkarten, redundante Switches und per Hot-Swap austauschbare Arbeitsspeicher und Datenträger.

### **Planung mit Kapazitätsreserve**

Die Datenrate der Sitzungsaufzeichnung ist in der Regel uneinheitlich, es sind Bursts und Fehler möglich und die Verarbeitung aufgelaufener Nachrichten erzeugt einen hohen IOPS-Wert. Die Sitzungsaufzeichnungsserver sollten daher über reichlich Kapazitätsreserven verfügen. Das Hinzufügen weiterer Server oder die Aufrüstung vorhandener Server (Erläuterungen hierzu weiter unten) kann die Kapazität erhöhen. Als allgemeine Faustregel sollte ein Sitzungsaufzeichnungsserver bei maximal 50 % Gesamtkapazität ausgeführt werden. Im vorangehenden Beispiel kann ein Server 5,0 MBit/s verarbeiten, setzen Sie als Ziel, das System mit nur 2,5 MBit/s auszuführen. Statt der Aufzeichnung von 5.000 Outlook-Sitzungen, die 3,5 Mbit/s auf einem Sitzungsaufzeichnungsserver generieren, lassen Sie 3.500 Sitzungen aufzeichnen, die nur etwa 2,5 MBit/s generieren.

### **Datenrückstau und Livewiedergabe**

Bei der Livewiedergabe wird eine Sitzungsaufzeichnung noch während der laufenden Sitzung zur Wiedergabe geöffnet. Bei der Livewiedergabe wechselt der für die Sitzung zuständige Sitzungsaufzeichnungsagent in den Streamingmodus und die Aufzeichnungsdaten werden direkt und ohne interne Pufferung an den Speichermanager gesendet. Da die Aufnahme-datei ständig aktualisiert wird, erhält der Player weiterhin die neuesten Daten aus der Livesitzung. Die Daten werden vom Agent allerdings über MSMQ an den Speichermanager gesendet, weshalb die o. g. Warteschlangenregeln gelten. In diesem Szenario kann ein Problem auftreten. Bei einem Datenrückstau in MSMQ werden die neuen Aufzeichnungsdaten für die Livewiedergabe wie alle anderen Datennachrichten in die Warteschlange gestellt. Die Datei kann zwar weiterhin wiedergegeben werden, doch die Anzeige der neuesten Liveaufzeichnungen verzögert sich. Ist die Livewiedergabe ein wichtiges Feature, sorgen Sie durch Kapazitätsreserven und Fehlertoleranz dafür, dass die Wahrscheinlichkeit eines Datenrückstaus gering ist.

## Skalierbarkeit für Citrix Virtual Apps and Desktops

Die Sitzungsaufzeichnung verringert nie die Sitzungsleistung und hält bei einem Datenrückstau nie eine Sitzung an. Der Fokus des Sitzungsaufzeichnungssystems richtet sich auf die Aufrechterhaltung der Benutzererfahrung und der Einzelserver-Skalierbarkeit. Bei einer irreversiblen Überlastung werden aufgezeichnete Sitzungsdaten verworfen. Umfangreiche Skalierbarkeitstests von Citrix haben ergeben, dass die Aufzeichnung von ICA-Sitzungen nur geringe Auswirkungen auf die Leistung und Skalierbarkeit von Citrix Virtual Apps and Desktops-Servern hat. Der Grad der Auswirkungen hängt von der Plattform, dem verfügbaren Arbeitsspeicher und der Art der aufgezeichneten Sitzungen ab. Bei der nachfolgend aufgeführten Konfiguration ist mit einer Verringerung der Einzelserver-Leistung zwischen 1 % und 5 % rechnen. Anders gesagt: Wenn ein Server ohne Sitzungsaufzeichnung 100 Benutzer hosten kann, kann er bei installierter Sitzungsaufzeichnung 95 bis 99 Benutzer hosten.

- 64-Bit-Server mit 8 GB RAM und einem VDA mit Multisitzungs-OS
- In allen Sitzungen werden Office-Anwendungen wie Outlook oder Excel ausgeführt.
- Die Anwendungen werden aktiv und dauerhaft genutzt.
- Alle Sitzungen werden gemäß den Richtlinien für die Sitzungsaufzeichnung aufgezeichnet.

Werden weniger Sitzungen aufgezeichnet oder ist die Sitzungsaktivität eher sporadisch, sind die Auswirkungen geringer. In vielen Fällen sind die Skalierbarkeitsauswirkungen vernachlässigbar und die Benutzerdichte pro Server bleibt gleich. Wie bereits erwähnt, sind die geringen Auswirkungen auf die einfachen Verarbeitungsanforderungen der auf den VDAs installierten Sitzungsaufzeichnungskomponenten zurückzuführen. Aufzeichnungsdaten werden aus dem ICA-Sitzungsstack extrahiert und unverändert über MSMQ an den Sitzungsaufzeichnungsserver gesendet. Es ist keine teure Datencodierung erforderlich.

Selbst wenn keine Sitzungen aufgezeichnet werden, besteht ein geringfügiger Mehraufwand für die Sitzungsaufzeichnung. Die Auswirkungen sind zwar gering, doch wenn Sie sicher sind, dass von einem Server keine Sitzungen aufgezeichnet werden, können Sie die Aufzeichnung dort deaktivieren. Eine Möglichkeit ist, die Sitzungsaufzeichnung zu entfernen. Weniger invasiv ist das Deaktivieren des Kontrollkästchens **Sitzungsaufzeichnung für diese VDA-Maschine aktivieren** auf der Registerkarte **Sitzungsaufzeichnung** unter Sitzungsaufzeichnungsagent - Eigenschaften. Wird die Sitzungsaufzeichnung in Zukunft benötigt, aktivieren Sie das Kontrollkästchen.

## Durchsatzmessung

Es gibt verschiedene Möglichkeiten, den Durchsatz der Sitzungsaufzeichnungsdaten vom VDA zum Sitzungsaufzeichnungsserver zu messen. Einer der einfachsten und effektivsten Methoden besteht in der Messung der Größe der Sitzungsaufzeichnungsdateien sowie der Geschwindigkeit, mit der Speicherplatz auf dem Sitzungsaufzeichnungsserver belegt wird. Die Menge der auf den Datenträger

geschriebenen Daten entspricht der Menge des generierten Netzwerkdatenverkehrs. Die Windows-Leistungsüberwachung (perfmon.exe) bietet eine Reihe von Standardsystemindikatoren, die zusätzlich den Leistungsindikatoren der Sitzungsaufzeichnung geprüft werden können. Die Indikatoren gestatten die Durchsatzmessung und die Identifizierung von Engpässen und Systemproblemen. In der folgenden Tabelle werden die nützlichsten Leistungsindikatoren beschrieben.

---

Leistungsobjekt	Indikatorname	Beschreibung
Citrix Sitzungsaufzeichnungsagent	Anzahl aktiver Aufzeichnungen	Gibt die Anzahl der Sitzungen an, die aktuell auf einem VDA aufgezeichnet werden.
Citrix Sitzungsaufzeichnungsagent	Vom Sitzungsaufzeichnungstreiber gelesene Bytes	Die Anzahl der von den für das Erfassen von Sitzungsdaten verantwortlichen Kernel-Komponenten gelesenen Bytes. Nützlich zur Ermittlung der Datenmenge, die ein VDA für alle auf dem betreffenden Server aufgezeichneten Sitzungen generiert.
Speichermanager der Citrix Sitzungsaufzeichnung	Anzahl aktiver Aufzeichnungen	Wie beim Leistungsindikator des Citrix Sitzungsaufzeichnungsagents doch im Hinblick auf den Sitzungsaufzeichnungsserver. Gibt die Gesamtzahl der Sitzungen an, die derzeit für alle Server aufgezeichnet werden.

Leistungsobjekt	Indikatorname	Beschreibung
Speichermanager der Citrix Sitzungsaufzeichnung	Message bytes/sec	Durchsatz aller aufgezeichneten Sitzungen. Kann verwendet werden, um die Datenverarbeitungsrate des Speichermanagers zu bestimmen. Bei einem MSMQ-Nachrichtenrückstand wird der Speichermanager mit voller Geschwindigkeit ausgeführt. Anhand dieses Werts kann die maximale Verarbeitungsrate des Speichermanagers angegeben werden.
LogicalDisk	Disk Write Bytes/sec	Kann zur Messung der Datenträger-Schreibleistung verwendet werden. Dies ist wichtig zur Erzielung einer hohen Skalierbarkeit für den Sitzungsaufzeichnungsserver. Auch die Leistung einzelner Laufwerke kann gemessen werden.
MSMQ-Warteschlange	Bytes in Queue	Anhand dieses Leistungsindikators kann die Menge der in der CitrixSmAudData-Warteschlange aufgelaufenen Daten ermittelt werden. Steigt dieser Wert im Laufe der Zeit an, so ist die Rate der vom Netzwerk empfangenen Aufzeichnungsdaten größer als die Datenverarbeitungsrate des Speichermanagers. Dieser Zähler ist nützlich, um die Auswirkungen von Bursts und Fehlern zu beobachten.

Leistungsobjekt	Indikatorname	Beschreibung
MSMQ-Warteschlange	Message in Queue	Ähnlich wie “Bytes in Queue”, jedoch wird die Anzahl der Nachrichten wiedergegeben.
Netzwerkschnittstelle	Bytes Total/sec	Kann an beiden Seiten der Verbindung gemessen werden, um zu ermitteln, wie viele Daten beim Aufzeichnen von Sitzungen generiert werden. Auf dem Sitzungsaufzeichnungsserver gibt dieser Indikator die Rate des Empfangs eingehender Daten an. Dies ist im Unterschied zu dem Leistungsindikator “Message bytes/sec” des Speichermanagers der Citrix Sitzungsaufzeichnung, der die Verarbeitungsrate der Daten wiedergibt. Wenn die Netzwerkrate größer als dieser Wert ist, laufen Nachrichten in der Warteschlange auf.
Prozessor	% Processor Time	Eine Überwachung dieses Indikators lohnt sich, obwohl die CPU als wahrscheinlicher Engpass eher nicht in Frage kommt.

### Hardware des Sitzungsaufzeichnungsservers

Sie können die Kapazität Ihrer Bereitstellung durch sorgfältige Auswahl der Hardware für den Sitzungsaufzeichnungsserver erhöhen. Sie können vertikal skalieren (durch Erhöhung der Kapazität der einzelnen Server) oder horizontal (durch Hinzufügen weiterer Server). In beiden Fällen geht es darum, die Kosten möglichst gering zu halten.



## **Vertikales Skalieren**

Für einzelne Sitzungsaufzeichnungsserver folgen Sie den folgenden bewährten Methoden, um die optimale Leistung zum verfügbaren Budget sicherzustellen. Das System hängt von IOPS ab. Dies gewährleistet einen hohen Durchsatz von Aufzeichnungsdaten aus dem Netzwerk auf den Datenträger. Daher ist es wichtig, in geeignete Netzwerk- und Datenträgerhardware zu investieren. Für einen leistungsstarken Sitzungsaufzeichnungsserver wird ein Dual- oder Dual-Core-Prozessor empfohlen. Eine höhere Spezifikation bringt keinen nennenswerten Vorteil. Es wird ein 64-Bit-Prozessor empfohlen, doch auch ein x86-Prozessor ist geeignet. 4 GB RAM werden empfohlen, mehr bringt auch hier wenig Nutzen.

## **Horizontales Skalieren**

Selbst bei einer optimalen vertikalen Skalierung gibt es Leistungs- und Skalierbarkeitsgrenzen, die ein einzelner Sitzungsaufzeichnungsserver erreichen kann, wenn eine große Anzahl von Sitzungen aufgezeichnet wird. Unter Umständen sind zusätzliche Server zur Bewältigung der Last erforderlich. Sie können weitere Sitzungsaufzeichnungsserver auf anderen Maschinen installieren, damit die Sitzungsaufzeichnungsserver als Lastausgleichspool fungieren. Bei dieser Art der Bereitstellung teilen sich die Sitzungsaufzeichnungsserver den Speicher und die Datenbank. Um die Last aufzuteilen, verweisen Sie die Sitzungsaufzeichnungsagents auf den Load Balancer, der für die Verteilung der Arbeitslast verantwortlich ist.

## **Netzwerkcapazität**

Ein Netzwerk mit 100 MBit/s ist für die Verbindung eines Sitzungsaufzeichnungsservers geeignet. Eine Gigabit-Ethernet-Verbindung kann die Leistung verbessern, führt jedoch nicht zu einer 10 Mal besseren Leistung als eine Verbindung mit 100 MBit/s. In der Praxis ist der Durchsatzgewinn deutlich geringer.

Stellen Sie sicher, dass Netzwerkschwitches, die von der Sitzungsaufzeichnung verwendet werden, nicht mit Anwendungen von Drittherstellern gemeinsam verwendet werden, die ggf. um die verfügbare Netzwerkbandbreite konkurrieren. Netzwerkschwitches sollten nur vom Sitzungsaufzeichnungsserver verwendet werden. Wenn sich das Netzwerk als Engpass erweist, bietet ein Netzwerkupgrade eine relativ kostengünstige Möglichkeit zur Erhöhung der Systemleistung.

## **Speicher**

Investitionen in Datenträger- und Speicherhardware sind der wichtigste Faktor für die Serverskalierbarkeit. Je schneller Daten auf den Datenträger geschrieben werden, desto höher ist die Leistung

des Gesamtsystems. Berücksichtigen Sie bei der Auswahl einer Speicherlösung die Schreibleistung stärker als die Leseleistung.

Speichern Sie Daten auf lokalen Festplatten, die entweder von einem lokalen Festplattencontroller als RAID oder als SAN gesteuert werden.

**Hinweis:**

Das Speichern von Daten in einem NAS mit dateibasiertem Protokoll wie SMB und NFS kann Auswirkungen auf Leistung und Sicherheit haben. Verwenden Sie die neueste Version des Protokolls, um Auswirkungen auf die Sicherheit zu vermeiden, und führen Sie Skalierungstests durch, um eine zufriedenstellende Leistung sicherzustellen.

Bei der Installation auf einem lokalen Datenträger verwenden Sie möglichst einen Datenträgercontroller mit integriertem Cachespeicher. Caching ermöglicht dem Controller die Verwendung des Aufzug-Algorithmus beim Zurückschreiben, was die Bewegung des Festplattenkopfs minimiert und sicherstellt, dass Schreibvorgänge ohne Warten auf den Abschluss des physischen Festplattenvorgangs ausgeführt werden. Dies kann die Schreibleistung bei minimalen Mehrkosten erheblich verbessern. Beim Caching besteht jedoch das Problem eines möglichen Datenverlusts nach Stromausfall. Zur Gewährleistung der Integrität von Daten und Dateisystem sollten Sie eine batteriegetriebene Backuplösung für den Festplattencontroller mit Cache in Betracht ziehen, die den Cache bei einem Stromausfall aufrecht erhält und dafür sorgt, dass die Daten bei Wiederherstellung der Stromversorgung auf die Festplatte geschrieben werden können.

Erwägen Sie die Verwendung einer geeigneten RAID-Speicherlösung. Je nach Leistungs- und Redundanzanforderungen stehen viele RAID-Level zur Verfügung. In der folgenden Tabelle werden die einzelnen RAID-Level und ihre Eignung für die Sitzungsaufzeichnung angegeben.

---

RAID-Level	Typ	Mindestanzahl Datenträger	Beschreibung
RAID 0	Mit Striping, ohne Parität	2	Bietet eine hohe Leistung, aber keine Redundanz. Der Verlust eines Datenträgers zerstört das Array. Es ist eine kostengünstige Lösung für die Speicherung von Sitzungsaufzeichnungsdateien, wenn ein Datenverlust nur geringe Auswirkungen hat. Die Leistung kann durch Hinzufügen weiterer Datenträger mühelos erhöht werden.
RAID 1	Gespiegelt, ohne Parität	2	Keine größere Leistung als mit einem Datenträger und daher eine relativ kostspielige Lösung. Verwenden Sie diese Lösung nur, wenn eine hohe Redundanz erforderlich ist.

RAID-Level	Typ	Mindestanzahl Datenträger	Beschreibung
RAID 3	Mit Striping und dedizierter Parität	3	Bietet hohe Schreibleistung mit ähnlichen Redun- danzeigenschaften wie RAID 5. RAID 3 wird für die Videoproduktion und Livestreaming empfohlen. Da es sich bei der Sitzungsaufzeichnung um eine Anwendung dieser Art handelt, wird RAID 3 am ehesten empfohlen, es ist jedoch nicht üblich.
RAID 5	Mit Striping und verteilter Parität	3	Bietet eine hohe Leseleistung mit Redundanz, jedoch auf Kosten einer geringeren Schreibleistung. RAID 5 ist die am häufigsten die allgemeine Verwendung eingesetzte Lösung. Aufgrund der langsamen Schreibleistung wird RAID 5 jedoch nicht für die Sitzungsaufzeichnung empfohlen. Bei RAID 3 sind die Kosten ähnlich, die Schreibleistung ist aber deutlich besser.

RAID-Level	Typ	Mindestanzahl Datenträger	Beschreibung
RAID 10	Gespiegelt, mit Striping	4	Bietet Leistungsmerkmale wie RAID 0 mit Redundanz wie RAID 1. Eine teure Lösung, die für die Sitzungsaufzeichnung nicht empfohlen wird.

RAID 0 und RAID 3 sind die empfohlenen RAID-Level. RAID 1 und RAID 5 sind gängige Standards, werden aber für die Sitzungsaufzeichnung nicht empfohlen. RAID 10 bietet einige Leistungsvorteile, doch die Kosten stehen in keinem Vergleich dazu.

Wählen Sie den Typ und die Spezifikation der Laufwerke. IDE/ATA-Laufwerke und externe USB- oder Firewire-Laufwerke sind nicht für die Verwendung für die Sitzungsaufzeichnung geeignet. Die beiden Hauptalternativen sind SATA und SCSI. SATA-Laufwerke bieten im Vergleich zu SCSI-Laufwerken relativ hohe Übertragungsraten zu geringeren Kosten pro MB. SCSI-Laufwerke bieten jedoch eine bessere Leistung und sind bei Serverbereitstellungen gängiger. Server-RAID-Lösungen unterstützen meist SCSI-Laufwerke, es gibt jetzt aber auch einige SATA-RAID-Produkte. Berücksichtigen Sie bei der Auswahl von Datenträgern die Drehgeschwindigkeit und andere Leistungsmerkmale.

Da die Aufzeichnung von Tausenden von Sitzungen pro Tag erhebliche Mengen an Speicherplatz belegen kann, müssen Sie zwischen Gesamtkapazität und Leistung wählen. Die Aufzeichnung von 5.000 Outlook-Sitzungen des o. g. Beispiels belegt an einem 8-Stunden-Arbeitstag etwa 100 GB Speicherplatz. Zur Speicherung der Aufzeichnungen von 10 Tagen (d. h. 50.000 Sitzungsaufzeichnungsdateien) benötigen Sie 1.000 GB (1 TB). Durch einen kürzeren Aufbewahrungszeitraum vor der Archivierung oder dem Löschen von Aufzeichnungen kann Speicherplatz eingespart werden. Steht 1 TB Speicherplatz zur Verfügung, ist eine siebentägige Aufbewahrungsfrist sinnvoll, die sicherstellt, dass rund 700 GB Speicherplatz belegt werden und 300 GB als Puffer für einen hohen Betrieb zur Verfügung stehen. In der Sitzungsaufzeichnung wird das Archivieren und Löschen von Dateien mit dem ICLDB-Hilfsprogramm unterstützt. Die Mindestaufbewahrungsdauer beträgt zwei Tage. Sie können einen Hintergrundtask planen, der täglich einmal außerhalb der Spitzenzeiten ausgeführt wird. Weitere Informationen zu ICLDB-Befehlen und zur Archivierung finden Sie unter [Verwalten der Datensätze in der Datenbank](#).

Die Alternative zu lokalen Laufwerken und Controllern ist die Verwendung einer SAN-Speicherlösung mit Datenträgerzugriff auf Blockebene. Auf dem Sitzungsaufzeichnungsserver wird das Datenträgerarray als lokales Laufwerk angezeigt. SANs sind teurer, doch da das Datenträgerarray gemeinsam genutzt wird, ist ihre Verwaltung einfacher und zentral. Es gibt zwei SAN-Haupttypen: Fibre Channel

und iSCSI. iSCSI –im Wesentlichen SCSI über TCP/IP– gewinnt seit der Einführung von Gigabit-Ethernet an Beliebtheit gegenüber Fibre Channel.

## **Datenbankskalierbarkeit**

Die Datenbank für die Sitzungsaufzeichnung erfordert Microsoft SQL Server 2019, Microsoft SQL Server 2017, Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012 oder Microsoft SQL Server 2008 R2. Die an die Datenbank gesendete Datenmenge ist gering, da dort nur die Metadaten über die aufgezeichneten Sitzungen gespeichert werden. Die Sitzungsaufzeichnungsdateien werden auf einem separaten Datenträger gespeichert. Normalerweise benötigt jede aufgezeichnete Sitzung nur 1 KB in der Datenbank, es sei denn, Sie fügen durchsuchbare Ereignisse mit der Sitzungsaufzeichnungs-Ereignis-API in die Sitzung ein.

Bei den Express-Editionen von Microsoft SQL Server 2019, Microsoft SQL Server 2017, Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012 und Microsoft SQL Server 2008 R2 ist die Größe der Datenbank auf 10 GB beschränkt. Bei 1 KB pro aufgezeichneter Sitzung kann die Datenbank ungefähr 4.000.000 Sitzungen katalogisieren. Andere Editionen von Microsoft SQL Server haben keine Beschränkungen hinsichtlich Datenbankgröße und werden nur durch den verfügbaren Speicherplatz auf dem Datenträger beschränkt. Wenn die Zahl der Sitzungen in der Datenbank ansteigt, wird die Leistung der Datenbank und die Geschwindigkeit der Suchen nur geringfügig beeinträchtigt.

Wenn Sie keine Anpassungen über die [Sitzungsaufzeichnungs-Ereignis-API](#) machen, generiert jede aufgezeichnete Sitzung vier Datenbanktransaktionen: zwei beim Start der Aufzeichnung, eine bei der Benutzeranmeldung bei der aufgezeichneten Sitzung und eine am Ende der Aufzeichnung. Beim Anpassen der Sitzungen mit der Sitzungsaufzeichnungs-Ereignis-API erstellt jedes durchsuchbare Ereignis, das aufgezeichnet wurde, eine Transaktion. Da selbst bei der einfachsten Datenbankbereitstellung mehrere Hundert Transaktionen pro Sekunde gehandhabt werden können, wird die Verarbeitungslast für die Datenbank nie überstrapaziert. Die Auswirkung ist so gering, dass die Datenbank für die Sitzungsaufzeichnung normalerweise auf demselben SQL-Server wie andere Datenbanken ausgeführt werden kann, u. a. der Citrix Virtual Apps and Desktops-Datenbank des Datenspeichers.

Wenn Sie in der Bereitstellung der Sitzungsaufzeichnung viele Millionen aufgezeichneter Sitzungen in der Datenbank katalogisieren müssen, halten Sie die Microsoft-Richtlinien zur Skalierbarkeit von SQL Server ein.

## **Installieren, Aktualisieren und Deinstallieren**

January 15, 2024

Dieser Artikel enthält folgende Abschnitte:

- [Installationscheckliste](#)
- [Verwenden von Citrix-Skripts für die Installation der erforderlichen Windows-Rollen und -Features](#)
- [Installieren der Verwaltungskomponenten der Sitzungsaufzeichnung](#)
  - [Installieren der Datenbank für die Sitzungsaufzeichnung](#)
  - [Installieren des Sitzungsaufzeichnungsservers](#)
- [Installieren des Sitzungsaufzeichnungsagent](#)
- [Installieren des Sitzungsaufzeichnungsplayers und des Webplayers](#)
- [Automatisieren der Installationen](#)
- [Upgrade der Sitzungsaufzeichnung](#)
- [Deinstallieren der Sitzungsaufzeichnung](#)

## Installationscheckliste

Zum Installieren der Komponenten der Sitzungsaufzeichnung verwenden Sie die folgenden Dateien:

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

Stellen Sie vor der Installation sicher, dass Sie die in dieser Liste aufgeführten Schritte abgeschlossen haben:

---

<input checked="" type="checkbox"/>	Schritt
	Installieren Sie die Voraussetzungen, bevor Sie mit der Installation beginnen. Informationen hierzu finden Sie unter <a href="#">Systemanforderungen</a> und <a href="#">Installieren der erforderlichen Windows-Rollen und -Features mit Citrix Skripts</a> .



---

## Schritt

---

Wählen Sie die Maschinen aus, auf denen Sie die Sitzungsaufzeichnungskomponenten installieren möchten. Stellen Sie sicher, dass jede Maschine die Hardware- und Softwareanforderungen für die zu installierenden Komponenten erfüllt.

Rufen Sie unter Angabe Ihrer Citrix-Anmeldeinformationen die Citrix Virtual Apps and Desktops-Downloadseite auf und laden Sie die Produktdatei herunter. Entpacken Sie die Datei.

Installieren Sie die relevanten Zertifikate in der Umgebung zur Kommunikation zwischen den Komponenten der Sitzungsaufzeichnung per TLS.

Installieren Sie die für die Komponenten der Sitzungsaufzeichnung benötigten Hotfixes. Die Hotfixes sind unter [Citrix Support](#) verfügbar.

Konfigurieren Sie Director zum Erstellen und Aktivieren von Sitzungsaufzeichnungsrichtlinien.

Weitere Informationen finden Sie unter [Konfigurieren von Director zur Verwendung des Sitzungsaufzeichnungsservers](#).

---

### Hinweis:

- Wir empfehlen, dass Sie die veröffentlichten Anwendungen basierend auf den Aufzeichnungsrichtlinien in eigene Bereitstellungsgruppen unterteilen. Die Sitzungsfreigabe für veröffentlichte Anwendungen kann Konflikte mit aktiven Richtlinien auslösen, wenn die Anwendungen in derselben Bereitstellungsgruppe sind. Die Sitzungsaufzeichnung ordnet die aktive Richtlinie der ersten veröffentlichten Anwendung zu, die ein Benutzer öffnet. Ab Version 7.18 können Sie die dynamischen Sitzungsaufzeichnung verwenden, um jederzeit während der Sitzungen das Aufzeichnen der Sitzung zu starten oder zu beenden. Dieses Feature hilft, Konflikte mit der aktiven Richtlinie zu mildern. Weitere Informationen finden Sie unter [Dynamische Sitzungsaufzeichnung](#).
- Wenn Sie beabsichtigen, Maschinenerstellungsdienste (MCS) oder Provisioning Services zu verwenden, bereiten Sie eine eindeutige QMID vor. Wenn Sie dies nicht tun, kann dies zum



Verlust von Aufzeichnungsdaten führen.

- Für SQL Server muss TCP/IP aktiviert sein, der SQL Server-Browserdienst muss ausgeführt und die Windows-Authentifizierung muss verwendet werden.
- Zur Verwendung von HTTPS konfigurieren Sie Serverzertifikate für TLS/HTTPS.
- Stellen Sie sicher, dass Benutzer unter `Local Users and Groups > Groups > Users` Schreibrechte für den Ordner `C:\windows\Temp` haben.

## Verwenden von Citrix-Skripts für die Installation der erforderlichen Windows-Rollen und -Features

Damit die Sitzungsaufzeichnung ordnungsgemäß funktioniert, installieren Sie vor ihrer Installation die erforderlichen

Windows-Rollen und -Features mit folgenden Citrix-Skripts:

- `InstallPrereqsforSessionRecordingAdministration.ps1`

```
1 <#
2 .Synopsis
3     Installs Prereqs for Session Recording Administration
4 .Description
5     Supports Windows Server 2012 R2, Windows Server 2016, Windows
6     Server 2019.
7     Install below windows feature on this machine:
8     -Application Development
9     -Security - Windows Authentication
10    -Management Tools - IIS 6 Management Compatibility
11        IIS 6 Metabase Compatibility
12        IIS 6 WMI Compatibility
13        IIS 6 Scripting Tools
14        IIS 6 Management Console
15    -Microsoft Message Queuing (MSMQ), with Active Directory
16        integration disabled, and MSMQ HTTP support enabled.
17 #>
18 function AddFeatures($featurename)
19 {
20     {
21         try
22         {
23             $feature=Get-WindowsFeature | ? {
24                 $_.DisplayName -eq $featurename -or $_.Name -eq $featurename }
25             Add-WindowsFeature $feature
26         }
27         catch
28         {
29             }
30     }
```

```
31     Write-Host "Addition of Windows feature $featurename
32         failed"
33     }
34
35     Write-Host "Addition of Windows feature $featurename
36         succeeded"
37 }
38
39 $system= gwmi win32_operatingSystem | select name
40
41 if (-not (($system -Like '*Microsoft Windows Server 2012 R2*')
42 -or ($system -Like '*Microsoft Windows Server 2016*') -or (
43 $system -Like '*Microsoft Windows Server 2019*'))
44 {
45     Write-Host("This is not a supported server platform.
46         Installation aborted.")
47     Exit
48 }
49
50 # Start to install Windows feature
51 Import-Module ServerManager
52
53 AddFeatures('Web-Asp-Net45') #ASP.NET 4.5
54 AddFeatures('Web-Mgmt-Console') #IIS Management Console
55 AddFeatures('Web-Windows-Auth') # Windows Authentication
56 AddFeatures('Web-Metabase') #IIS 6 Metabase Compatibility
57 AddFeatures('Web-WMI') #IIS 6 WMI Compatibility
58 AddFeatures('Web-Lgcy-Scripting')#IIS 6 Scripting Tools
59 AddFeatures('Web-Lgcy-Mgmt-Console') #IIS 6 Management Console
60 AddFeatures('MSMQ-HTTP-Support') #MSMQ HTTP Support
61 AddFeatures('web-websockets') #IIS Web Sockets
62 AddFeatures('NET-WCF-HTTP-Activation45') #http activate
63 <!--NeedCopy-->
```

- InstallPrereqsforSessionRecordingAgent.ps1

```
1 <#
2 .Synopsis
3     Installs Prereqs for Session Recording Agent
4 .Description
5     Supports Windows Server 2012 R2, Windows Server 2016,
6     Windows Server 2019, Windows 7, Windows 8, Windows 8.1 and
7     Windows 10.
8     Install below windows feature on this machine:
9     -Microsoft Message Queuing (MSMQ), with Active Directory
10    integration disabled, and MSMQ HTTP support enabled.
11
12 #>
13 function AddFeatures($featurename)
14 {
```

```
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
25             failed"
26         Exit 1
27     }
28
29     Write-Host "Addition of Windows feature $featurename
30         succeeded"
31 }
32 # Start to install Windows feature
33 $system= gwmi win32_operatingSystem | select name
34
35 if (-not (($system -Like '*Microsoft Windows Server 2012 R2*')
36 -or ($system -Like '*Microsoft Windows Server 2016*') -or (
37 $system -Like '*Microsoft Windows Server 2019*')-or ($system
38 -Like '*Microsoft Windows 7*')-or ($system -Like '*
39 Microsoft Windows 8*')-or ($system -Like '*Microsoft Windows
40 10*'))))
41 {
42
43     Write-Host("This is not a supported platform. Installation
44         aborted.")
45     Exit
46 }
47
48 if ($system -Like '*Microsoft Windows Server*')
49 {
50
51     Import-Module ServerManager
52     AddFeatures('MSMQ') #Message Queuing
53     AddFeatures('MSMQ-HTTP-Support')#MSMQ HTTP Support
54 }
55
56 else
57 {
58
59     try
60     {
```

```
56
57     if($system -Like '*Microsoft Windows 7*')
58     {
59
60         dism /online /enable-feature /featurename:IIS-
            WebServerRole /featurename:IIS-WebServer /
            featurename:IIS-IIS6ManagementCompatibility /
            featurename:IIS-Metabase /featurename:IIS-
            ManagementConsole /featurename:IIS-
            ApplicationDevelopment /featurename:IIS-
            NetFxExtensibility /featurename:IIS-
            ISAPIExtensions /featurename:IIS-
            CommonHttpFeatures /featurename:IIS-
            DefaultDocument /featurename:IIS-DirectoryBrowsing
            /featurename:IIS-HttpErrors /featurename:IIS-
            HttpRedirect /featurename:IIS-StaticContent /
            featurename:IIS-HealthAndDiagnostics /featurename:
            IIS-RequestMonitor /featurename:IIS-Performance /
            featurename:IIS-HttpCompressionStatic /featurename
            :IIS-Security /featurename:IIS-RequestFiltering /
            featurename:IIS-LoggingLibraries /featurename:IIS-
            HttpTracing
61         dism /online /enable-feature /featurename:MSMQ-
            Container
62         dism /online /enable-feature /featurename:MSMQ-Server
63         dism /online /enable-feature /featurename:MSMQ-HTTP
64     }
65
66     else
67     {
68
69         dism /online /enable-feature /featurename:MSMQ-HTTP /
            all
70     }
71
72     }
73
74     catch
75     {
76
77         Write-Host "Addition of Windows feature MSMQ HTTP Support
            failed"
78         Exit 1
79     }
80
81     write-Host "Addition of Windows feature MSMQ HTTP Support
            succeeded"
82 }
83
84 <!--NeedCopy-->
```

Um die erforderlichen Windows-Rollen und -Features zu installieren, führen Sie die folgenden Schritte aus:

1. Führen Sie auf der Maschine, auf der Sie die Verwaltungskomponenten der Sitzungsaufzeichnung installieren möchten, die folgenden Schritte aus:

- a) Stellen Sie sicher, dass die Ausführungsrichtlinie in PowerShell auf **RemoteSigned** oder **Unrestricted** festgelegt ist.

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

- b) Starten Sie eine Eingabeaufforderung als Administrator und führen Sie den Befehl `powershell.exe -file InstallPrereqsforSessionRecordingAdministration.ps1` aus.

Das Skript zeigt die erfolgreich hinzugefügten Features an und wird dann angehalten.

- c) Stellen Sie nach der Skriptausführung sicher, dass die Ausführungsrichtlinie auf den für Ihre Unternehmensrichtlinie erforderlichen Wert festgelegt ist.
2. Führen Sie auf der Maschine, auf der Sie den Agent der Sitzungsaufzeichnung installieren möchten, die folgenden Schritte aus:

- a) Stellen Sie sicher, dass die Ausführungsrichtlinie in PowerShell auf **RemoteSigned** oder **Unrestricted** festgelegt ist.

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

- b) Starten Sie eine Eingabeaufforderung als Administrator und führen Sie den Befehl `powershell.exe -file InstallPrereqsforSessionRecordingAgent.ps1` aus.

Das Skript zeigt die erfolgreich hinzugefügten Features an und wird dann angehalten.

- c) Stellen Sie nach der Skriptausführung sicher, dass die Ausführungsrichtlinie auf den für die Unternehmensrichtlinie erforderlichen Wert festgelegt ist.

## Installieren der Verwaltungskomponenten der Sitzungsaufzeichnung

Wir empfehlen die Installation der Komponenten Sitzungsaufzeichnungsverwaltung, Sitzungsaufzeichnungsagent und Sitzungsaufzeichnungsplayer auf separaten Servern.

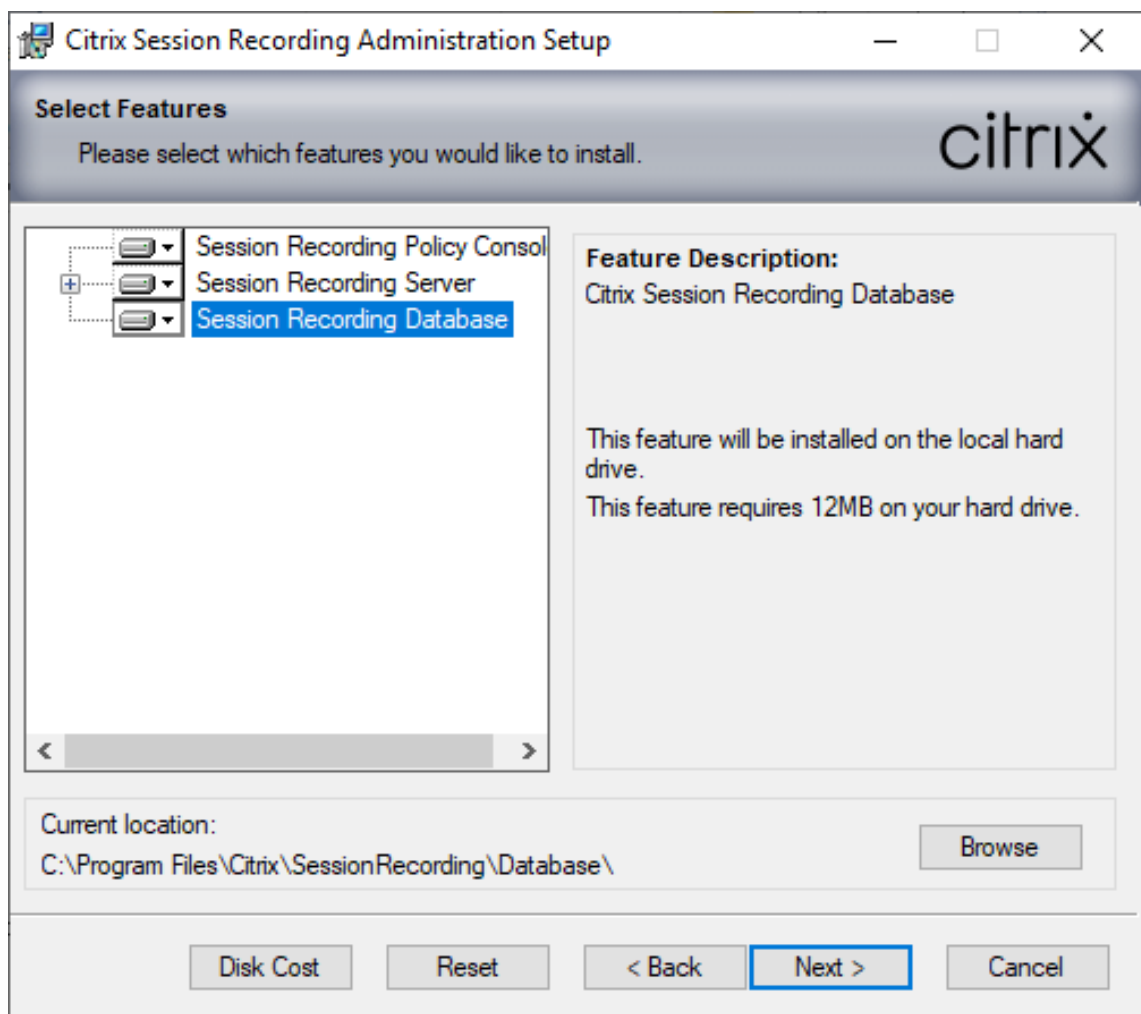
Die Verwaltungskomponenten der Sitzungsaufzeichnung umfassen die Datenbank für die Sitzungsaufzeichnung, den Sitzungsaufzeichnungsserver und die Richtlinienkonsole für die Sitzungsaufzeichnung. Sie können festlegen, welche dieser Komponenten auf einem Server installiert werden.

1. Installieren Sie **Broker\_PowerShellSnapIn\_x64.msi**.

**Wichtig:**

Um die Richtlinienkonsole für die Sitzungsaufzeichnung zu verwenden, muss das Broker PowerShell Snap-in (`Broker_PowerShellSnapIn_x64.msi`) installiert sein. Navigieren Sie zu dem Snap-In auf dem ISO-Image für Citrix Virtual Apps and Desktops (`\\layout\image-full\x64\Citrix Desktop Delivery Controller`) und folgen Sie den Anweisungen, um es manuell zu installieren. Anderenfalls kann es zu Fehlern kommen.

2. Rufen Sie eine Windows-Eingabeaufforderung als Administrator auf und führen Sie den Befehl `msiexec /i SessionRecordingAdministrationx64.msi` aus oder doppelklicken Sie auf die MSI-Datei.
3. Klicken Sie im Installationsprogramm auf **Weiter** und akzeptieren Sie die Lizenzvereinbarung.
4. Wählen Sie im **Setupbildschirm der Sitzungsaufzeichnungsverwaltung** die Verwaltungskomponenten aus, die Sie installieren möchten.



**Hinweis:**

Die Installation aller Komponenten der Sitzungsaufzeichnungsverwaltung auf einem einzelnen Server auf einem einzelnen Server ist für eine Machbarkeitsstudie geeignet. Für große Produktionsumgebungen empfehlen wir die Installation der Richtlinienkonsole für die Sitzungsaufzeichnung auf einem Server und die Installation von Sitzungsaufzeichnungsserver, Administratorprotokollierung der Sitzungsaufzeichnung und Datenbank für die Sitzungsaufzeichnung auf einem zweiten Server. Die Administratorprotokollierung ist ein optionales Teilfeature des Sitzungsaufzeichnungsservers. Sie müssen den Sitzungsaufzeichnungsserver auswählen, bevor Sie die Administratorprotokollierung auswählen können.

### Installieren der Datenbank für die Sitzungsaufzeichnung

**Hinweis:**

- Die Datenbank für die Sitzungsaufzeichnung ist eigentlich keine Datenbank. Sie ist für das Erstellen und Konfigurieren der erforderlichen Datenbanken in der Microsoft SQL Server-Instanz während der Installation zuständig. Die Sitzungsaufzeichnung unterstützt drei Lösungen für die hohe Verfügbarkeit der Datenbank basierend auf Microsoft SQL Server. Weitere Informationen finden Sie unter [Hohe Datenbankverfügbarkeit](#).
- Sie können die Datenbank für die Sitzungsaufzeichnung in einer verwalteten Azure SQL-Instanz, in SQL Server auf Azure-VMs und in AWS RDS bereitstellen. Weitere Informationen finden Sie unter [Bereitstellen der Datenbank für die Sitzungsaufzeichnung in einer verwalteten Azure SQL-Instanz oder in AWS RDS](#) und [Bereitstellen der Datenbank für die Sitzungsaufzeichnung in SQL Server auf Azure-VMs](#).

Es gibt drei typische Bereitstellungen der Datenbank für die Sitzungsaufzeichnung und von Microsoft SQL Server:

- Bereitstellung 1: Installation des Sitzungsaufzeichnungsservers und der Datenbank für die Sitzungsaufzeichnung auf derselben Maschine und Installation von Microsoft SQL Server auf einer Remotemaschine (**empfohlen**)
  - Bereitstellung 2: Installation des Sitzungsaufzeichnungsservers, der Datenbank für die Sitzungsaufzeichnung und von Microsoft SQL Server auf derselben Maschine
  - Bereitstellung 3: Installation des Sitzungsaufzeichnungsservers auf einer Maschine und Installation der Datenbank für die Sitzungsaufzeichnung sowie von Microsoft SQL Server auf einer anderen Maschine (**nicht empfohlen**)
1. Geben Sie auf der Seite **Datenbank- und Server** den Instanznamen und Datenbanknamen der Datenbank für die Sitzungsaufzeichnung und das Computerkonto des Sitzungsaufzeichnungsservers an. Klicken Sie auf **Weiter**.

- **Instanzname:** Wenn die Datenbankinstanz keine benannte Instanz ist, die Sie beim Setup der Instanz konfiguriert haben, können Sie nur den Computernamen des SQL Server-Computers verwenden. Wenn Sie die Instanz benannt haben, verwenden Sie Computername\Instanzname als Datenbankinstanznamen. Um den verwendeten Servernamen zu ermitteln, führen Sie **select @@servername** auf dem SQL Server aus. Der zurückgegebene Name ist der Datenbankinstanzname. Wenn Ihr SQL Server so konfiguriert ist, dass er auf einem benutzerdefinierten Port (außer dem Standardport 1433) abhört, legen Sie den benutzerdefinierten Listenerport fest, indem Sie ein Komma an den Instanznamen anhängen. Beispiel: Geben Sie **DXSBC-SRD-1,2433** in das Textfeld **Instanzname** ein, wobei 2433 nach dem Komma den benutzerdefinierten Listenerport angibt.
- **Datenbankname:** Geben Sie einen benutzerdefinierten Datenbanknamen in das Textfeld **Datenbankname** ein oder übernehmen Sie den Standardnamen. Klicken Sie auf **Verbindung testen** zum Testen der Verbindung mit der SQL Server-Instanz und der Gültigkeit des Datenbanknamens.

**Wichtig:**

Ein benutzerdefinierter Datenbankname darf nur Buchstaben (A–Z, a–z), Ziffern (0–9) und Unterstreichungsstriche enthalten und nicht länger als 123 Zeichen sein.

- Sie müssen die Serverrollenberechtigungen **securityadmin** und **dbcreator** für die Datenbank haben. Wenn Sie diese Berechtigungen nicht haben, gibt es folgende Möglichkeiten:
  - \* Bitten Sie den Datenbankadministrator darum, Berechtigungen für die Installation zuzuweisen. Nach Abschluss der Installation werden die Serverrollenberechtigungen **securityadmin** und **dbcreator** nicht mehr benötigt und können entfernt werden.
  - \* Während der MSI-Installation wird ein Dialogfeld angezeigt, in dem die Anmeldeinformationen eines Datenbankadministrators mit den Serverrollenberechtigungen **securityadmin** und **dbcreator** eingegeben werden müssen. Geben Sie die richtigen Anmeldeinformationen ein und klicken Sie auf **OK**, um mit der Installation fortzufahren.

Bei der Installation wird die Datenbank für die Sitzungsaufzeichnung erstellt und das Maschinenkonto des Sitzungsaufzeichnungsservers als **db\_owner** hinzugefügt.

- **Computerkonto des Sitzungsaufzeichnungsservers:**
  - **Bereitstellung 1 und 2:** Geben Sie im Textfeld **Computerkonto des Sitzungsaufzeichnungsservers** die Zeichenfolge **localhost** ein.
  - **Bereitstellung 3:** Geben Sie den Namen der Maschine mit dem Sitzungsaufze-



ichnungsserver im Format “Domäne\Computername” ein. Das Computerkonto des Sitzungsaufzeichnungsservers wird als Benutzerkonto für den Zugriff auf die Datenbank für die Sitzungsaufzeichnung verwendet.

**Hinweis:**

Die Installation der Komponenten der Sitzungsaufzeichnungsverwaltung kann mit dem Fehlercode 1603 fehlschlagen, wenn für **Computerkonto des Sitzungsaufzeichnungsservers** ein Domänenname festgelegt ist. Geben Sie als Workaround im Textfeld **Computerkonto des Sitzungsaufzeichnungsservers** die Option **localhost** oder einen Namen im Format “NetBIOS-Domänennamen\Maschinename” ein. Um den NetBIOS-Domänennamen zu erhalten, führen Sie auf dem Computer, auf dem der Sitzungsaufzeichnungsserver installiert ist, in PowerShell `$env:userdomain` aus oder `echo %UserDomain%` an der Eingabeaufforderung.

2. Folgen Sie den Anweisungen zum Abschließen der Installation.

## Installieren des Sitzungsaufzeichnungsservers

1. Wählen Sie die Optionen **Sitzungsaufzeichnungsserver** und **Administratorprotokollierung der Sitzungsaufzeichnung**.

**Hinweis:**

- Die Administratorprotokollierung ist ein optionales Teilfeature des Sitzungsaufzeichnungsservers. Sie müssen den Sitzungsaufzeichnungsserver auswählen, bevor Sie die Administratorprotokollierung auswählen können.
- Wir empfehlen, dass Sie die Administratorprotokollierung zusammen mit dem Sitzungsaufzeichnungsserver installieren. Wenn Sie die Administratorprotokollierung nicht aktivieren möchten, können Sie sie auf einer nachfolgenden Seite deaktivieren.

2. Geben Sie auf der Seite **Datenbank und Server - Konfiguration** die Einstellungen vor.

- **Instanzname:** Geben Sie den Namen des SQL Servers im Textfeld **Instanzname** ein. Wenn Sie eine benannte Instanz verwenden, machen Sie die Angabe im Format “Computername\Instanzname”, andernfalls geben Sie nur einen Computernamen ein. Wenn Ihr SQL Server so konfiguriert ist, dass er auf einem benutzerdefinierten Port (außer dem Standardport 1433) abhört, legen Sie den benutzerdefinierten Listenerport fest, indem Sie ein Komma an den Instanznamen anhängen. Beispiel: Geben Sie **DXSBC-SRD-1,2433** in das Textfeld **Instanzname** ein, wobei 2433 nach dem Komma den benutzerdefinierten Listenerport angibt.

- **Datenbankname:** Geben Sie einen benutzerdefinierten Datenbanknamen in das Textfeld **Datenbankname** ein oder übernehmen Sie den Standardnamen **CitrixSessionRecording**.  
Sie müssen die Serverrollenberechtigungen **securityadmin** und **dbcreator** für die Datenbank haben. Wenn Sie diese Berechtigungen nicht haben, gibt es folgende Möglichkeiten:
    - Bitten Sie den Datenbankadministrator darum, Berechtigungen für die Installation zuzuweisen. Nach Abschluss der Installation werden die Serverrollenberechtigungen **securityadmin** und **dbcreator** nicht mehr benötigt und können entfernt werden.
    - Während der MSI-Installation wird ein Dialogfeld angezeigt, in dem die Anmeldeinformationen eines Datenbankadministrators mit den Serverrollenberechtigungen **securityadmin** und **dbcreator** eingegeben werden müssen. Geben Sie die richtigen Anmeldeinformationen ein und klicken Sie auf **OK**, um mit der Installation fortzufahren.
  - Klicken Sie nach Eingabe der korrekten Namen für Instanz und Datenbank auf **Verbindung testen**, um die Verbindung zur Datenbank für die Sitzungsaufzeichnung zu testen.
  - Geben Sie das Computerkonto für die Sitzungsaufzeichnung ein und klicken Sie auf **Weiter**.
3. Geben Sie auf der Seite **Konfiguration der Administratorprotokollierung** die Konfigurationen für die Administratorprotokollierung an.
- **Datenbank für Administratorprotokollierung installieren auf SQL Server-Instanz:** Dieses Feld kann nicht bearbeitet werden. Der Name der SQL Server-Instanz der Datenbank für die Administratorprotokollierung wird automatisch aus dem Instanznamen abgerufen, den Sie auf der Seite **Datenbank und Server** eingegeben haben.
  - **Datenbankname für die Administratorprotokollierung:** Zum Installieren der Administratorprotokollierung für die Sitzungsaufzeichnung geben Sie auf der nächsten Seite einen benutzerdefinierten Namen für die Datenbank der Administratorprotokollierung im Textfeld ein oder übernehmen Sie den angegebenen Standarddatenbanknamen **CitrixSessionRecordingLogging**.
- Hinweis:**
- Der Name der Datenbank für die Administratorprotokollierung muss sich vom Namen der Datenbank für die Sitzungsaufzeichnung, der im Textfeld **Datenbankname** auf der vorherigen Seite **Datenbank und Server - Konfiguration** festgelegt wurde, unterscheiden.
- **Standarddatenbanknamen verwenden:** Bei Auswahl dieser Option wird der Standardname der Protokollierungsdatenbank verwendet.
  - **Protokollierung aktivieren:** Die Administratorprotokollierung ist standardmäßig aktiviert. Sie können sie deaktivieren, indem Sie das Kontrollkästchen deaktivieren.

- **Obligatorische Blockierung aktivieren:** Die obligatorische Blockierung ist standardmäßig aktiviert. Die normalen Funktionen werden möglicherweise blockiert, wenn die Protokollierung fehlschlägt. Sie können sie deaktivieren, indem Sie das Kontrollkästchen deaktivieren.

4. Klicken Sie auf **Weiter** und fahren Sie fort, um die Installation abzuschließen.

**Hinweis:**

Standardmäßig verwendet der Sitzungsaufzeichnungsserver HTTPS/TLS für die sichere Kommunikation. Wenn TLS nicht in der IIS-Standardsite des Sitzungsaufzeichnungsservers konfiguriert ist, verwenden Sie HTTP. Hierfür löschen Sie die SSL-Auswahl in der IIS-Verwaltungskonsole, indem Sie die Site des Sitzungsaufzeichnungsbrowsers aufrufen, die SSL-Einstellungen öffnen und das Kontrollkästchen **SSL erforderlich** deaktivieren.

## Installieren des Sitzungsaufzeichnungsagent

Installieren Sie den Sitzungsaufzeichnungsagent auf der Serverbetriebssystem-VDA bzw. -VDI-Maschine, auf der Sie Sitzungen aufzeichnen möchten.

1. Seite **Sitzungsaufzeichnungsagent - Konfiguration:** Wenn Sie den Sitzungsaufzeichnungsserver zuvor installiert haben, geben Sie den Computernamen der Maschine ein, auf der Sie den Server installiert haben, sowie das Protokoll und die Portinformationen für die Verbindung zum Sitzungsaufzeichnungsserver. Wenn Sie die Sitzungsaufzeichnung noch nicht installiert haben, können Sie diese Informationen später unter **Sitzungsaufzeichnungsagent - Eigenschaften** ändern.
2. Folgen Sie den Anweisungen zum Abschließen der Installation.

**Hinweis:**

Wenn von Maschinenerstellungsdienste (MCS) oder Provisioning Services (PVS) mehrere VDAs mit dem konfigurierten Masterimage und Microsoft Message Queuing (MSMQ) erstellt werden, erhalten die VDAs unter bestimmten Bedingungen ggf. die gleiche QMID. Dies kann verschiedene Probleme verursachen, zum Beispiel:

- Sitzungen werden nicht aufgezeichnet, selbst wenn eine Aufzeichnungsvereinbarung akzeptiert wurde.
- Der Sitzungsaufzeichnungsserver empfängt möglicherweise keine Sitzungsabmeldungssignale, sodass Sitzungen permanent den Status "Live" beibehalten.

Erstellen Sie als Workaround eine eindeutige QMID für jeden VDA (abhängig von der Bereitstellungsmethode).

Keine zusätzliche Aktion ist erforderlich, wenn VDAs für Einzelsitzungs-OS, auf denen ein Sitzungsaufzeichnungsagent installiert ist, mit PVS 7.7 oder höher oder MCS 7.9 oder höher im statischen Desktopmodus erstellt werden und beispielsweise festgelegt wurde, dass alle Änderungen mit einer separaten persönlichen vDisk oder einem lokalen Datenträger des VDAs persistent gemacht werden.

Bei VDAs für Multisitzungs-OS, die mit MCS oder PVS erstellt wurden, und bei VDAs für Einzelsitzungs-OS, auf denen Änderungen bei Abmeldung des Benutzers verworfen werden, verwenden Sie das Skript GenRandomQMID.ps1, um die QMID beim Systemstart zu ändern. Ändern Sie die Energieverwaltungsstrategie, um sicherzustellen, dass vor Anmeldeversuchen der Benutzer genug VDAs ausgeführt werden.

Um das Skript GenRandomQMID.ps1 zu verwenden:

1. Stellen Sie sicher, dass die Ausführungsrichtlinie in PowerShell auf **RemoteSigned** oder **Unrestricted** festgelegt ist.

```
1 Set-ExecutionPolicy RemoteSigned
```

2. Erstellen Sie einen geplanten Task und legen Sie als Auslöser "Bei Systemstart fest" und für die Ausführung auf dem Computer mit dem PVS- oder MCS-Masterimage das Konto SYSTEM.

3. Fügen Sie den Befehl als Starttask hinzu.

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

#### Zusammenfassung des GenRandomQMID.ps1-Skripts:

1. Entfernen Sie die aktuelle QMID aus der Registrierung.
2. Fügen Sie `SysPrep = 1` unter `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters` hinzu.
3. Anhalten zugehöriger Dienste, einschließlich CitrixSmAudAgent und MSMQ
4. Zum Generieren einer zufälligen QMID starten Sie die zuvor angehaltenen Dienste.

#### Beispiel: GENRANDOMQMID.PS1:

```
1 # Remove old QMID from registry and set SysPrep flag for MSMQ
2
3 Remove-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\
  MachineCache -Name QMID -Force
4
5 Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -Name "
  SysPrep" -Type DWord -Value 1
6
7 # Get dependent services
8
9 $depServices = Get-Service -name MSMQ -dependentservices | Select -
  Property Name
```

```
10
11 # Restart MSMQ to get a new QMID
12
13 Restart-Service -force MSMQ
14
15 # Start dependent services
16
17 if ($depServices -ne $null) {
18
19     foreach ($depService in $depServices) {
20
21         $startMode = Get-WmiObject win32_service -filter "NAME = '$(
22             $depService.Name)'" | Select -Property StartMode
23
24         if ($startMode.StartMode -eq "Auto") {
25
26             Start-Service $depService.Name
27         }
28     }
29 }
30
31 }
32
33
34 }
35
36 <!--NeedCopy-->
```

## Installieren des Sitzungsaufzeichnungsplayers und des Webplayers

Installieren Sie den Sitzungsaufzeichnungsplayer auf dem Sitzungsaufzeichnungsserver oder auf Arbeitsstationen in der Domäne. Installieren Sie den Webplayer nur auf dem Sitzungsaufzeichnungsserver.

Doppelklicken Sie auf `SessionRecordingPlayer.msi` und `SessionRecordingWebPlayer.msi` und folgen Sie den Anweisungen, um die Installation abzuschließen.

## Automatisieren der Installation

Die Sitzungsaufzeichnung unterstützt die automatische Installation mit Optionen. Schreiben Sie ein Skript, das die automatische Installation verwendet, und führen Sie die entsprechenden Befehle aus.

## Automatische Installation der Komponenten der Sitzungsaufzeichnungsverwaltung

**Installieren aller Verwaltungskomponenten für die Sitzungsaufzeichnung mit einem einzigen Befehl** Mit einem der folgenden Befehle installieren Sie alle Komponenten der Sitzungsaufzeichnungsverwaltung und erstellen eine Protokolldatei, in der die Installationsinstallationen erfasst werden.

```
1 msiexec /i "c:\SessionRecordingAdministrationx64.msi" ADDLOCAL="
    SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
    DATABASEINSTANCE="WNBIO-SRD-1" DATABASENAME="CitrixSessionRecording"
    LOGGINGDATABASENAME="CitrixSessionRecordingLogging" DATABASEUSER="
    localhost" /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" /q /l*vx "c:\WithLogging.log"
2 <!--NeedCopy-->
```

### Hinweis:

Die Datei `SessionRecordingAdministrationx64.msi` ist im ISO-Image von Citrix Virtual Apps and Desktops unter `\layout\image-full\x64\Session Recording`.

Wobei:

- **ADDLOCAL** stellt die Funktionen zur Auswahl bereit. Sie können mehrere Optionen auswählen. `SsRecServer` ist der Sitzungsaufzeichnungsserver. `PolicyConsole` ist die Richtlinienkonsole für die Sitzungsaufzeichnung. `SsRecLogging` ist das Feature zur Administratorprotokollierung. `StorageDatabase` ist die Datenbank für die Sitzungsaufzeichnung. Die Administratorprotokollierung ist ein optionales Teilfeature des Sitzungsaufzeichnungsservers. Sie müssen den Sitzungsaufzeichnungsserver auswählen, bevor Sie die Administratorprotokollierung auswählen können.
- **DATABASEINSTANCE** ist der Instanzname der Datenbank für die Sitzungsaufzeichnung. Beispielsweise `.\SQLEXPRESS,computer-name\SQLEXPRESS,computer-name` oder `tcp:srt-sql-support.public.ca7b16b60789.database.windows.net,3342`, wenn Sie eine verwaltete Azure SQL-Instanz verwenden.
- **DATABASENAME** ist der Name der Datenbank für die Sitzungsaufzeichnung.
- **LOGGINGDATABASENAME** ist der Name der Datenbank für die Administratorprotokollierung.
- **AZURESQLSERVICESUPPORT** legt fest, ob Cloud-SQL unterstützt wird. Um Cloud-SQL zu verwenden, wählen Sie die Einstellung 1.
- **DATABASEUSER** ist das Computerkonto des Sitzungsaufzeichnungsservers.

- **AZUREUSERNAME** ist der Name des Cloud-SQL-Administrators.
- **AZUREPASSWORD** ist das Kennwort des Cloud-SQL-Administrators.
- **/q** gibt den stillen Modus an.
- **/l\*v** gibt eine ausführliche Protokollierung an.
- **yourinstallationlog** ist der Speicherort der Installationsprotokolldatei.

### Erstellen eines Masterimages für die Bereitstellung des Sitzungsaufzeichnungsservers

Möglicherweise haben Sie bereits eine Datenbank für die Sitzungsaufzeichnung und eine Datenbank für die Administrationsprotokollierung aus einer vorhandenen Bereitstellung. In solchen Szenarios können Sie nun auf Datenbankprüfungen verzichten, wenn Sie die Komponenten der Sitzungsaufzeichnungsverwaltung mit `SessionRecordingAdministrationx64.msi` installieren. Sie können ein Masterimage für die einfache Bereitstellung des Sitzungsaufzeichnungsservers auf vielen anderen Maschinen erstellen. Nachdem Sie den Server auf Zielmaschinen mit dem Masterimage bereitgestellt haben, führen Sie auf jeder Maschine einen Befehl aus, um eine Verbindung mit der vorhandenen Datenbank für die Sitzungsaufzeichnung und der Administrationsprotokollierung herzustellen. Diese Unterstützung für Masterimages erleichtert die Bereitstellung und minimiert die potenziellen Auswirkungen menschlicher Fehler. Sie gilt nur für Neuinstallationen und besteht aus den folgenden Schritten:

1. Starten Sie eine Eingabeaufforderung, und führen Sie einen Befehl ähnlich dem Folgenden aus:

```
1 msixexec /i "SessionRecordingAdministrationx64.msi" ADDLOCAL="
  SsRecServer,PolicyConsole,SsRecLogging,StorageDatabase"
  DATABASEINSTANCE="sqlnotexists" DATABASENAME="
  CitrixSessionRecording2" LOGGINGDATABASENAME="
  CitrixSessionRecordingLogging2" DATABASEUSER="localhost" /q /l*
  vx "c:\WithLogging.log" IGNOREDBCHECK="True"
2 <!--NeedCopy-->
```

Mit diesem Befehl werden die Verwaltungskomponenten der Sitzungsaufzeichnung installiert, ohne die Verbindung zur Datenbank der Sitzungsaufzeichnung und zur Datenbank der Administrationsprotokollierung zu konfigurieren und zu testen.

Setzen Sie den Parameter **IGNOREDBCHECK** auf **True** und verwenden Sie Zufallswerte für **DATABASEINSTANCE**, **DATABASENAME** und **LOGGINGDATABASENAME**.

2. Erstellen Sie ein Masterimage auf der Maschine, die Sie verwenden.
3. Stellen Sie das Masterimage für die Bereitstellung des Sitzungsaufzeichnungsservers auf anderen Maschinen bereit.
4. Führen Sie auf jeder der Maschinen Befehle aus, die den Folgenden ähneln:

```
1 .\SsRecUtils.exe -modifydbconnectionpara DATABASEINSTANCE
  DATABASENAME LOGGINGDATABASENAME
2
```

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

Mit den Befehlen wird der zuvor installierte Sitzungsaufzeichnungsserver mit einer vorhandenen Datenbank für die Sitzungsaufzeichnung und die Administrationsprotokollierung verbunden.

Die `SsRecUtils.exe` Datei ist in `\Citrix\SessionRecording\Server\bin\`. Legen Sie die Parameter **DATABASEINSTANCE**, **DATABASENAME** und **LOGGINGDATABASENAME** nach Bedarf fest.

**Sie können die Datenbanken auch bei der Deinstallation der Verwaltungskomponenten für die Sitzungsaufzeichnung beibehalten** Wenn **KEEPDB** auf **True** festgelegt ist, wird mit dem folgenden Befehl die Datenbank der Sitzungsaufzeichnung und die Datenbank der Administrationsprotokollierung beibehalten, wenn die Komponenten der Sitzungsaufzeichnungsverwaltung deinstalliert werden:

```
1 msixexec /x "SessionRecordingAdministrationx64.msi" KEEPDB="True"
2 <!--NeedCopy-->
```

### Automatische Installation von Sitzungsaufzeichnungsplayer und Webplayer

Mit den folgenden Befehlen installieren Sie den Sitzungsaufzeichnungsplayer bzw. den Webplayer.

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

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

#### Hinweis:

Die Datei `SessionRecordingPlayer.msi` ist im ISO-Image von Citrix Virtual Apps and Desktops unter `\layout\image-full\x86\Session Recording`.

Die Datei `SessionRecordingWebPlayer.msi` ist im ISO-Image von Citrix Virtual Apps and Desktops unter `\layout\image-full\x64\Session Recording`.

Wobei:

- **/q** gibt den stillen Modus an.
- **/l\*v** gibt eine ausführliche Protokollierung an.
- **yourinstallationlog** ist der Speicherort der Installationsprotokolldatei.



**Automatische Installation des Sitzungsaufzeichnungsagent** Mit dem folgenden Befehl installieren Sie den Sitzungsaufzeichnungsagent und erstellen eine Protokolldatei, in der die Installationsinformationen erfasst werden.

**64-Bit-Systeme:**

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

**Hinweis:**

Die Datei `SessionRecordingAgentx64.msi` ist im ISO-Image von Citrix Virtual Apps and Desktops unter `\layout\image-full\x64\Session Recording`.

**32-Bit-Systeme:**

```
1 msiexec /i SessionRecordingAgent.msi /q /l*v yourinstallationlog  
    SESSIONRECORDINGSERVERNAME=yourservername  
2 SESSIONRECORDINGBROKERPROTOCOL=yourbrokerprotocol  
    SESSIONRECORDINGBROKERPORT=yourbrokerport  
3 <!--NeedCopy-->
```

**Hinweis:**

Die Datei `SessionRecordingAgent.msi` ist im ISO-Image von Citrix Virtual Apps and Desktops unter `\layout\image-full\x86\Session Recording`.

Wobei:

- **yourservername** ist der NetBIOS-Name oder FQDN der Maschine, auf der der Sitzungsaufzeichnungsserver ausgeführt wird. Wenn Sie keinen Namen eingeben, wird der Standardwert **localhost** verwendet.
- **yourbrokerprotocol** entspricht HTTP oder HTTPS und gibt an, wie der Sitzungsaufzeichnungsagent mit dem Sitzungsaufzeichnungsbroker kommuniziert. Erfolgt keine Angabe, wird standardmäßig HTTPS verwendet.
- **yourbrokerport** entspricht der Nummer des Ports, über den der Sitzungsaufzeichnungsagent mit dem Sitzungsaufzeichnungsbroker kommuniziert. Wenn Sie keine Eingabe machen, wird als Standardwert Null verwendet, d. h. der Sitzungsaufzeichnungsagent verwendet den Standardport für das ausgewählte Protokoll: 80 für HTTP oder 443 für HTTPS.
- **/q** gibt den stillen Modus an.
- **/l\*v** gibt eine ausführliche Protokollierung an.
- **yourinstallationlog** ist der Speicherort der Installationsprotokolldatei.

## Upgrade der Sitzungsaufzeichnung

Sie können bestimmte Bereitstellungen aktualisieren, ohne zunächst neue Maschinen oder Sites erstellen zu müssen. Sie können ein Upgrade von dem neuesten CU der Sitzungsaufzeichnung 7.15 LTSR und von jeder späteren Version auf das aktuelle Release durchführen.

### Hinweis:

Wenn Sie ein Upgrade der Sitzungsaufzeichnungsverwaltung von Version 7.6 auf 7.13 oder höher durchführen und unter "Sitzungsaufzeichnungsverwaltung" zum Hinzufügen der Administratorprotokollierung **Ändern** wählen, wird der SQL Server-Instanzname auf der Seite **Konfiguration der Administratorprotokollierung** nicht angezeigt. Die folgende Fehlermeldung wird angezeigt, wenn Sie auf **Weiter** klicken: **Fehler beim Datenbankverbindungstest. Geben Sie den richtigen Datenbankinstanznamen ein.** Fügen Sie als Workaround dem folgenden Ordner der SmartAuditor Server-Registrierung die Leseberechtigung für localhost-Benutzer hinzu: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server`.

Sie können kein Upgrade von einer Technical Preview-Version ausführen.

## Anforderungen, Vorbereitung und Einschränkungen

- Sie müssen über die grafische Oberfläche oder die Befehlszeile des Installationsprogramms für die Sitzungsaufzeichnung ein Upgrade von deren Komponenten auf der Maschine ausführen, auf der die Komponenten installiert sind.
- Vor Beginn des Upgrades sichern Sie die Datenbank "CitrixSessionRecording" auf der SQL Server-Instanz. Sollten Sie nach dem Datenbankupgrade Probleme entdecken, können Sie die Datenbank wiederherstellen.
- Auf den Maschinen, auf denen Sie die Komponenten der Sitzungsaufzeichnung aktualisieren, müssen Sie sowohl Domänenbenutzer als auch lokaler Administrator sein.
- Sind Server und Datenbank der Sitzungsaufzeichnung nicht auf dem gleichen Server installiert, benötigen Sie die Datenbankrollenberechtigung für das Upgrade der Datenbank für die Sitzungsaufzeichnung. Anderenfalls:
  - Bitten Sie den Datenbankadministrator die Rollenberechtigungen **securityadmin** und **dbcreator** für das Upgrade zuzuweisen. Nach Abschluss des Upgrades werden die Serverrollenberechtigungen **securityadmin** und **dbcreator** nicht mehr benötigt und können entfernt werden.
  - Oder verwenden Sie die Datei `SessionRecordingAdministrationx64.msi` für ein Upgrade. Während des Upgrades mit dem MSI-Paket wird ein Dialogfeld angezeigt, in dem die Anmeldeinformationen eines Datenbankadministrators mit den Serverrollenberechtigungen **securityadmin** und **dbcreator** eingegeben werden müssen. Geben Sie

die richtigen Anmeldeinformationen ein und klicken Sie auf **OK**, um mit dem Upgrade fortzufahren.

- Wenn Sie nicht alle Sitzungsaufzeichnungsagents zur gleichen Zeit aktualisieren möchten, können Sie Version 7.6.0 (und höher) für das aktuelle Release des Sitzungsaufzeichnungsservers verwenden. Allerdings stehen dann einige neue Features und Fehlerbehebungen ggf. nicht zur Verfügung.
- Sitzungen, die während des Upgrades des Sitzungsaufzeichnungsservers gestartet werden, werden nicht aufgezeichnet.
- Die Option **Grafikanpassung** unter “Sitzungsaufzeichnungsagent - Eigenschaften” ist nach einer Neuinstallation oder einem Upgrade standardmäßig aktiviert, um Kompatibilität mit der Desktopgestaltungsumleitung zu gewährleisten. Sie können diese Option nach einer Neuinstallation oder einem Upgrade manuell deaktivieren.
- Die Administratorprotokollierung wird nicht installiert, wenn Sie die Sitzungsaufzeichnung aktualisieren und das Feature in der Vorgängerversion nicht verfügbar war. Ändern Sie die Installation nach dem Upgrade, um das Feature hinzuzufügen.
- Laufen zu Beginn des Upgrades Sitzungen, kann deren Aufzeichnung sehr wahrscheinlich nicht ausgeführt werden.
- Lesen Sie den folgenden Abschnitt zur Upgradereihenfolge, damit Sie mögliche Ausfälle einplanen und das Risiko senken können.

### **Aktualisierungsreihenfolge**

1. Sind Server und Datenbank für die Sitzungsaufzeichnung auf verschiedenen Servern installiert, beenden Sie den Speichermanager der Sitzungsaufzeichnung auf dem Sitzungsaufzeichnungsserver manuell. Führen Sie dann zunächst das Upgrade der Datenbank durch.
2. Stellen Sie mithilfe des Internetinformationsdienste-Managers (IIS-Manager) sicher, dass der Sitzungsaufzeichnungsbroker ausgeführt wird. Führen Sie das Upgrade des Sitzungsaufzeichnungsservers durch. Sind Datenbank und Server der Sitzungsaufzeichnung auf dem gleichen Server installiert, erfolgt auch ein Upgrade der Datenbank.
3. Der Sitzungsaufzeichnungsdienst geht automatisch wieder online, sobald das Upgrade des Sitzungsaufzeichnungsservers abgeschlossen ist.
4. Führen Sie das Upgrade des Sitzungsaufzeichnungsagents (auf dem Masterimage) durch.
5. Führen Sie das Upgrade der Richtlinienkonsole für die Sitzungsaufzeichnung zusammen mit oder nach dem des Sitzungsaufzeichnungsservers durch.
6. Führen Sie das Upgrade des Sitzungsaufzeichnungsspieler durch.

## Bereitstellen der Datenbank für die Sitzungsaufzeichnung in Cloud-SQL-Datenbankdiensten

In diesem Abschnitt wird beschrieben, wie Sie die Datenbank für die Sitzungsaufzeichnung in einer verwalteten Azure SQL-Instanz, in AWS RDS und in SQL Server auf Azure-VMs bereitstellen.

### Bereitstellen der Datenbank für die Sitzungsaufzeichnung in einer verwalteten Azure SQL-Instanz oder in AWS RDS

#### Tipp:

Sie können auch einen einzelnen Befehl ähnlich dem folgenden ausführen, um die Datenbank für die Sitzungsaufzeichnung in einer verwalteten Azure SQL-Instanz oder in AWS RDS bereitzustellen. Weitere Informationen finden Sie im vorherigen Abschnitt [Automatische Installation](#) dieses Artikels.

```
1 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. Erstellen Sie eine verwaltete Azure SQL-Instanz oder erstellen Sie eine SQL Server-Instanz über die Amazon RDS-Konsole.
2. (Nur für Azure SQL) Notieren Sie die **Server**-Zeichenfolgen, die im Bereich “Eigenschaften” angezeigt werden. Diese Zeichenfolgen sind der Instanzname der Datenbank für die Sitzungsaufzeichnung. Ein Beispiel sehen Sie im folgenden Screenshot.

[ADO.NET](#) [JDBC](#) [ODBC](#) [PHP](#)

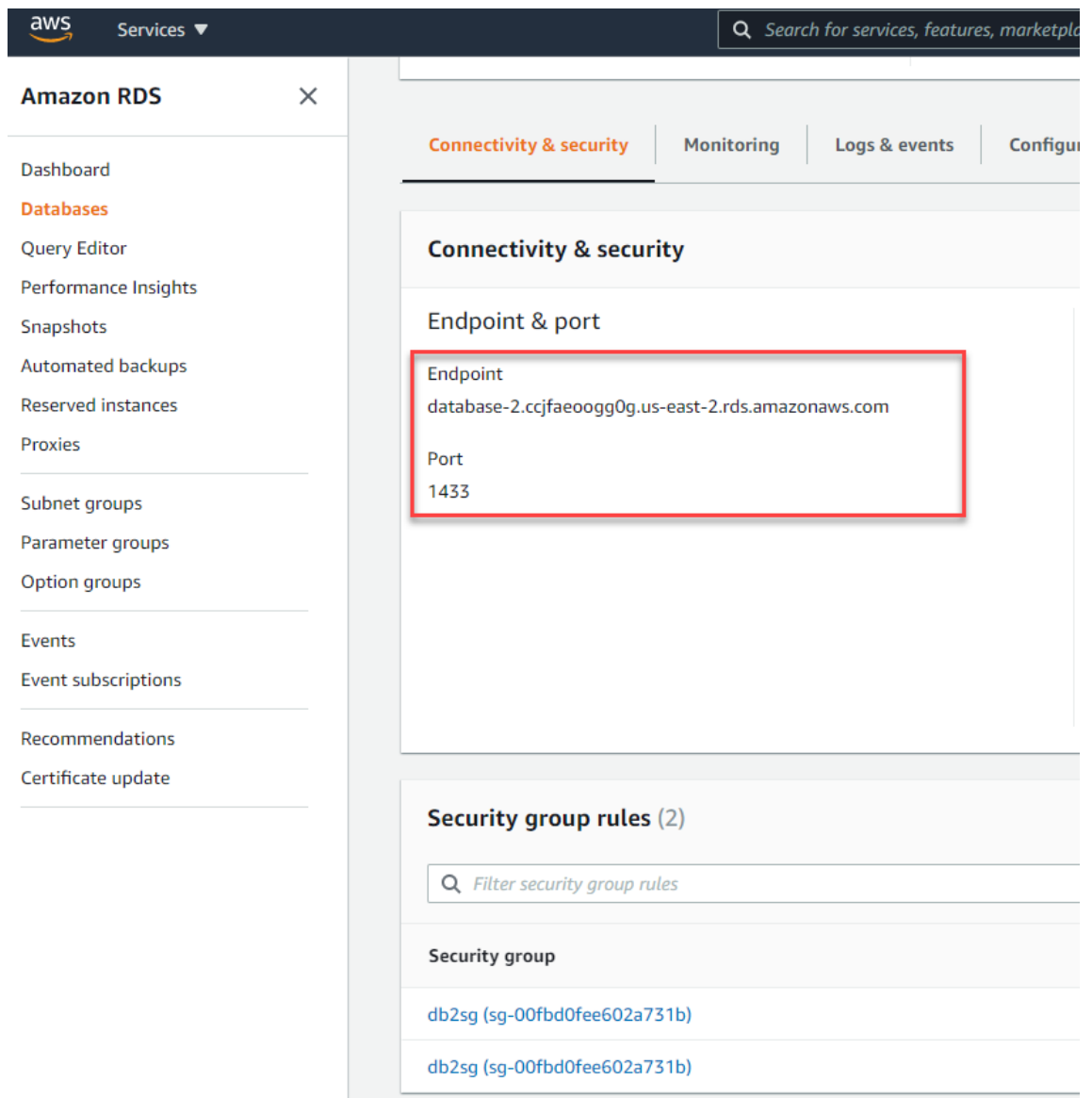
ADO.NET (SQL authentication) - private endpoint

```
Server=tcp:sr-sqlinstance.3141e49e4d94.database.windows.net,1433;Persist Security Info=False;User ID={your_username};Password={your_password};MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;
```

ADO.NET (SQL authentication) - public endpoint

```
Server=tcp:sr-sqlinstance.public.3141e49e4d94.database.windows.net,3342;Persist Security Info=False;User ID={your_username};Password={your_password};MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;
```

3. (Nur für AWS RDS) Notieren Sie sich den **Endpunkt** und **Port**. Wir verwenden diese Angaben als Instanznamen Ihrer Datenbank im Format **<Endpunkt, Port>**.



4. Führen Sie SessionRecordingAdministrationx64.msi aus, um die Datenbank für die Sitzungsaufzeichnung zu installieren.

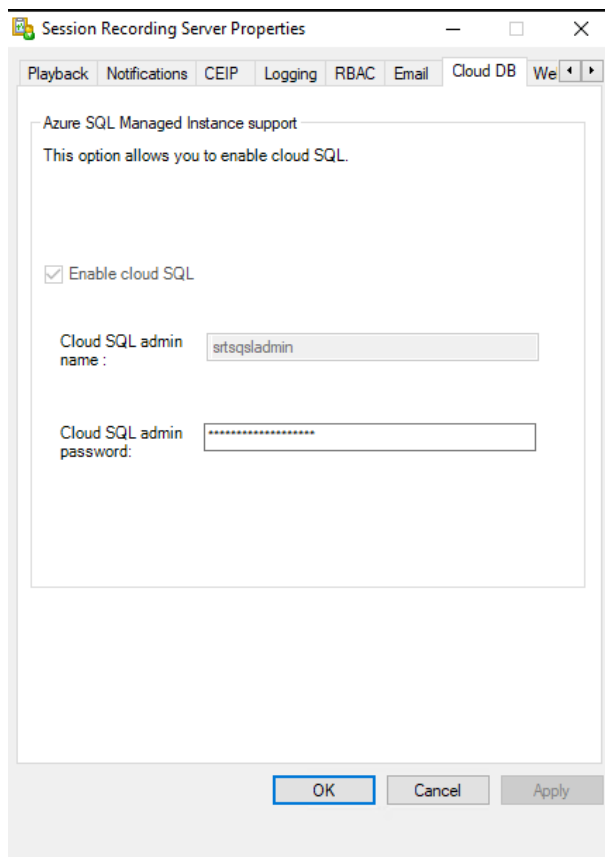
Aktivieren Sie das Kontrollkästchen **Cloud-SQL aktivieren** und geben Sie Namen und Kennwort des Azure SQL-Administrators an. Nehmen Sie andere erforderliche Konfigurationen vor.

The screenshot shows a Windows-style dialog box titled "Citrix Session Recording Administration Setup". The main heading is "Database and Server Configuration" with the Citrix logo on the right. Below the heading, there is a text instruction: "Specify the instance name and database name of the Session Recording Database and the computer account of the Session Recording Server." The form contains several input fields and checkboxes:

- Instance name:** A text input field with an example below it: ".\SQLEXPRESS, computer-name\SQLEXPRESS, computer-name, tcp:xxxx.database.windows.net, 3342".
- Enable cloud SQL:** A checked checkbox.
- Database name:** A text input field with an unchecked checkbox labeled "Use default database name" below it.
- Cloud SQL admin name:** A text input field.
- Cloud SQL admin password:** A text input field.
- Session Recording Server computer account:** A text input field with an example below it: "localhost, domain\computer-name".

At the bottom of the dialog, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

**Hinweis:** Wenn Sie das Kennwort des Cloud-SQL-Administrators ändern, müssen Sie es auch unter **Sitzungsaufzeichnungsserver - Eigenschaften** aktualisieren. Wenn Sie **Sitzungsaufzeichnungsserver - Eigenschaften** öffnen, wird eine Fehlermeldung angezeigt. Klicken Sie zum Fortfahren auf **OK**, wählen Sie die Registerkarte **Cloud-DB** und geben Sie das neue Kennwort des Cloud-SQL-Administrators ein. Starten Sie den Analysedienst der Citrix Sitzungsaufzeichnung, den Speichermanagerdienst der Citrix Sitzungsaufzeichnung und den IIS-Dienst neu.



### Migration einer On-Premises-Datenbank in eine verwaltete Cloud-SQL-Instanz

1. Migrieren Sie Ihre On-Premises-Datenbank gemäß <https://docs.microsoft.com/en-us/data-migration/> oder <https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-an-on-premises-microsoft-sql-server-database-to-amazon-rds-for-sql-server.html>.
2. Führen Sie auf dem Sitzungsaufzeichnungsserver die Datei `SsRecUtils.exe` aus, um sicherzustellen, dass die Sitzungsaufzeichnung nach der Migration ordnungsgemäß funktioniert.

```
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. Starten Sie auf dem Sitzungsaufzeichnungsserver den Analysedienst der Citrix Sitzungsaufzeichnung, den Speichermanagerdienst der Citrix Sitzungsaufzeichnung und den IIS-Dienst neu.

## **Migration einer Produktionsdatenbank von einer verwalteten Azure SQL-Instanz zu einer On-Premises-Datenbank**

1. Migrieren Sie die Datenbank gemäß <https://docs.microsoft.com/en-us/data-migration/>.
2. Führen Sie auf dem Sitzungsaufzeichnungsserver die Datei `SsRecUtils.exe` aus, um sicherzustellen, dass die Sitzungsaufzeichnung nach der Migration ordnungsgemäß funktioniert.

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

3. Starten Sie auf dem Sitzungsaufzeichnungsserver den Analysedienst der Citrix Sitzungsaufzeichnung, den Speichermanagerdienst der Citrix Sitzungsaufzeichnung und den IIS-Dienst neu.

## **Bereitstellen der Datenbank für die Sitzungsaufzeichnung in SQL Server auf Azure-VMs**

In SQL Server auf Azure-VMs können Sie die Datenbank für die Sitzungsaufzeichnung bereitstellen.

1. Checken Sie eine Azure SQL-VM aus.
2. Konfigurieren Sie die VM und fügen Sie sie der Domäne hinzu, in der Sie die Komponenten der Sitzungsaufzeichnung installieren.
3. Verwenden Sie den FQDN der VM als Instanznamen, wenn Sie die Datenbank für die Sitzungsaufzeichnung installieren.

**Hinweis:** Wenn Sie `SessionRecordingAdministrationx64.msi` für die Installation verwenden, deaktivieren Sie das Kontrollkästchen **Cloud-SQL aktivieren**.

4. Folgen Sie den Anweisungen zum Abschließen der Installation.

## **Deinstallieren der Sitzungsaufzeichnung**

**Verwenden Sie zum Entfernen von Komponenten der Sitzungsaufzeichnung von einem Server oder einer Arbeitsstation die Option zum Deinstallieren von Programmen in der Windows-Systemsteuerung.** Zum Entfernen der Datenbank für die Sitzungsaufzeichnung benötigen Sie die gleichen SQL Server-Rollenberechtigungen wie bei der Installation (**securityadmin** und **dbcreator**).

Aus Sicherheitsgründen wird die Datenbank der Administratorprotokollierung nach der Deinstallation der Komponenten nicht entfernt.



## Dynamische Sitzungsaufzeichnung

January 15, 2024

Zuvor begann die Sitzungsaufzeichnung genau zu Beginn von Sitzungen, die die Aufzeichnungsrichtlinien erfüllten, und endete genau dann, wenn diese Sitzungen beendet wurden.

Ab Version 7.18 hat Citrix ein Feature zur dynamischen Sitzungsaufzeichnung eingeführt. Mit dem Feature können Sie die Aufzeichnung einer oder mehrerer Sitzungen, die ein bestimmter Benutzer startet, jederzeit während der Sitzung starten und anhalten.

### Hinweis:

Aktualisieren Sie die Sitzungsaufzeichnung, den VDA und den Delivery Controller auf Version 7.18 oder höher, damit das Feature wie erwartet funktioniert.

## Aktivieren oder Deaktivieren der Sitzungsaufzeichnung

Auf dem Sitzungsaufzeichnungsagent wird ein Registrierungswert zum Aktivieren oder Deaktivieren des Features hinzugefügt. Der Registrierungswert ist standardmäßig auf **1** gesetzt; das Feature ist also standardmäßig aktiviert.

Mit den folgenden Schritten aktivieren oder deaktivieren Sie das Feature:

1. Melden Sie sich nach der Installation der Sitzungsaufzeichnung als Administrator an der Maschine an, auf der Sie den Sitzungsaufzeichnungsagent installiert haben.
2. Öffnen Sie den Registrierungs-Editor.
3. Gehen Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor`.
4. Legen Sie für **DynamicControlAllowed** den Wert **0** fest oder verwenden Sie den Standardwert **1**.
  - 1**: dynamische Aufzeichnung aktiviert
  - 0**: dynamische Aufzeichnung deaktiviert
5. Starten Sie den Sitzungsaufzeichnungsagent neu, damit die Einstellung wirksam wird. Wenn Sie MCS oder PVS für die Bereitstellung verwenden, ändern Sie die Einstellung in Ihrem Masterimage und führen Sie ein Update durch, damit Ihre Änderungen wirksam werden.

### Warnung:

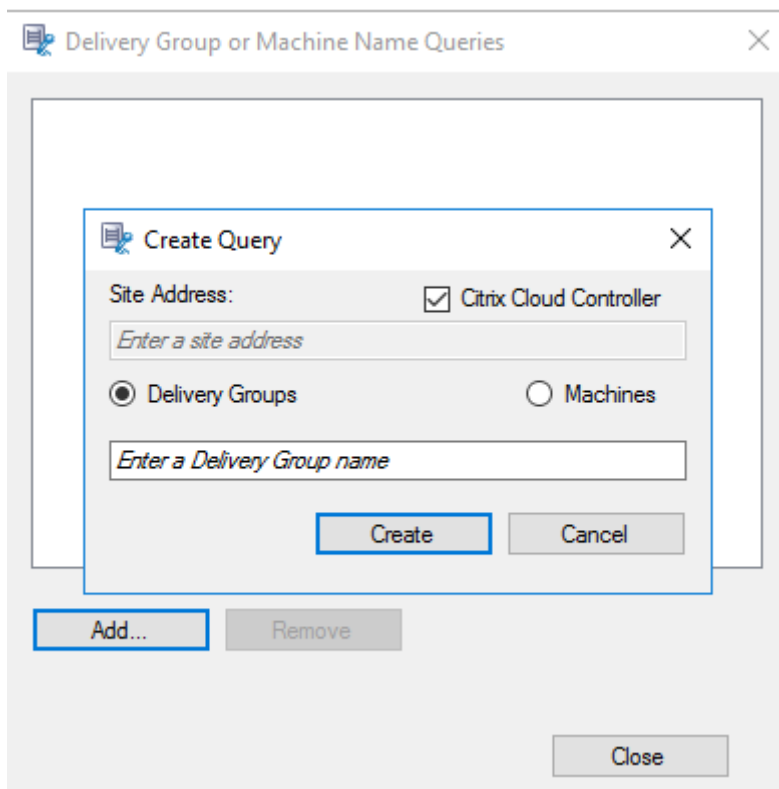
Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und ein erneutes Installieren des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des

Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

## Dynamisches Starten und Anhalten der Aufzeichnung mit PowerShell-Befehlen in den Citrix SDKs

Mit dem PowerShell SDK von Citrix Virtual Apps and Desktops bzw. dem Remote PowerShell SDK von Citrix Virtual Apps and Desktops können Sie die dynamische Sitzungsaufzeichnung in On-Premises- und Citrix Cloud-Umgebungen verwenden.

Welches SDK installiert und verwendet werden muss, hängt vom Delivery Controller ab, den Sie beim Erstellen Ihrer Aufzeichnungsrichtlinie festgelegt haben. Wenn Sie das Kontrollkästchen **Citrix Cloud Controller** aktiviert haben, um Sitzungen in einer Citrix Cloud-Umgebung aufzuzeichnen, ist eine Überprüfung Ihrer Citrix Cloud-Anmeldeinformationen erforderlich. Weitere Informationen finden Sie unter [Erstellen einer benutzerdefinierten Aufzeichnungsrichtlinie](#).



### Hinweis:

Installieren Sie das Remote PowerShell SDK nicht auf einer Citrix Cloud Connector-Maschine. Sie können das Remote PowerShell SDK auf jeder in der Domäne eingebundenen Maschine am gleichen Ressourcenstandort installieren. Wir empfehlen, die Cmdlets dieses SDKs nicht auf Cloud Connectors auszuführen. Am SDK-Betrieb sind die Cloud Connectors nicht beteiligt.

Die Tabelle unten enthält drei PowerShell-Befehle, die beide Citrix SDKs für die dynamische Sitzungsaufzeichnung bereitstellen.

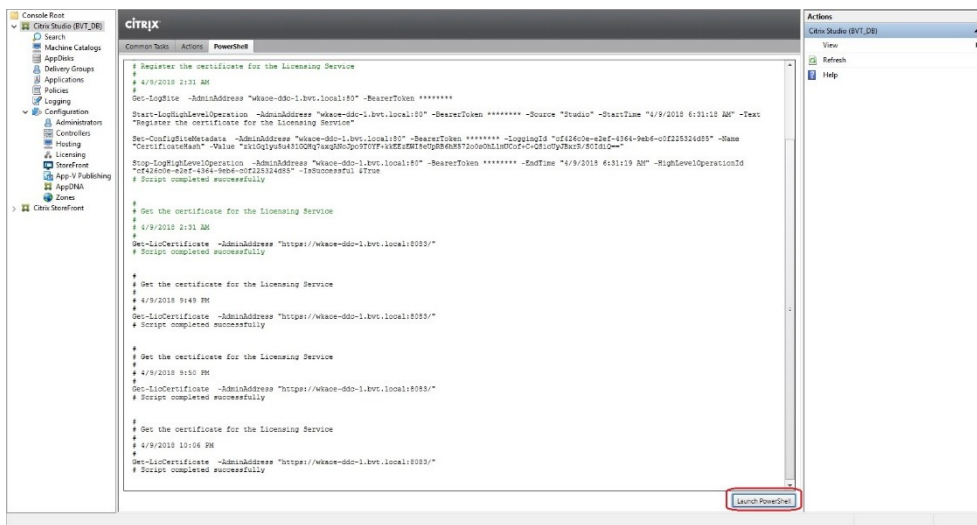
---

Befehl	Beschreibung
Start-BrokerSessionRecording	Ermöglicht das Aufzeichnen einer bestimmten aktiven Sitzung, einer Liste aktiver Sitzungen oder Sitzungen, die von einem bestimmten Benutzer gestartet wurden. Zum Aufrufen weiterer Informationen führen Sie <a href="#">Get-Help Start-BrokerSessionRecording</a> aus, um die Onlinehilfe zu dem Befehl anzuzeigen.
Stop-BrokerSessionRecording	Hiermit können Sie das Aufzeichnen anhalten für eine bestimmte aktive Sitzung, für eine Liste aktiver Sitzungen oder für Sitzungen, die von einem bestimmten Benutzer gestartet wurden. Zum Aufrufen weiterer Informationen führen Sie <a href="#">Get-Help Stop-BrokerSessionRecording</a> aus, um die Onlinehilfe zu dem Befehl anzuzeigen.
Get-BrokerSessionRecordingStatus	Hiermit können Sie den Aufzeichnungsstatus einer aktiven Sitzung abrufen. Zum Aufrufen weiterer Informationen führen Sie <a href="#">Get-Help Get-BrokerSessionRecordingStatus</a> aus, um die Onlinehilfe zu dem Befehl anzuzeigen.

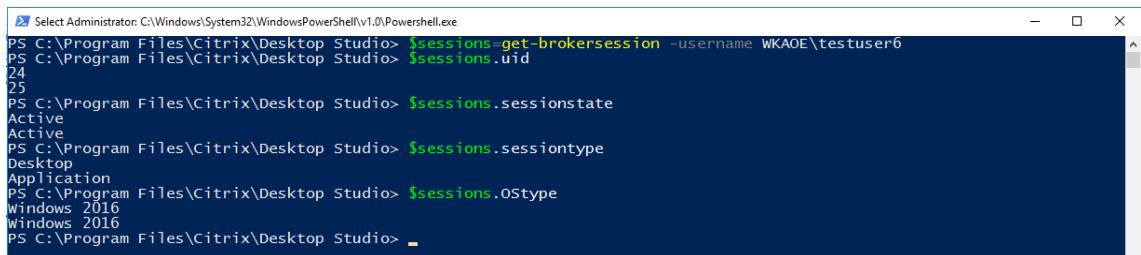
---

Wenn ein Benutzer beispielsweise ein Problem meldet und zeitnahe Hilfe benötigt, können Sie zur Problembehandlung mit dem Feature die aktiven Sitzungen des Benutzers dynamisch aufzeichnen und wiedergeben. Sie können die folgenden Aktionen ausführen:

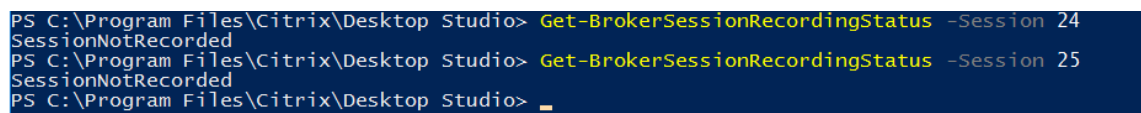
1. (Nur für Citrix Virtual Apps and Desktops PowerShell SDK) Starten Sie PowerShell über die Citrix Studio-Konsole.



2. Verwenden Sie den Befehl `Get-BrokerSession`, um alle aktiven Sitzungen des Zielbenutzers abzurufen.



3. Verwenden Sie den Befehl `Get-BrokerSessionRecordingStatus`, um den Aufzeichnungsstatus der angegebenen Sitzung abzurufen.



**Hinweis:**

Für den Parameter `-Session` können Sie nur eine Sitzungs-UID angeben.

4. Verwenden Sie den Befehl `Start-BrokerSessionRecording`, um die Aufnahme zu starten. Standardmäßig werden Benutzer per Benachrichtigung über die Aufnahme informiert.

Die folgende Tabelle zeigt gängige Verwendungen für den Befehl `Start-BrokerSessionRecording`.

Befehl	Beschreibung
Start-BrokerSessionRecording -User DomainA \ UserA	Startet die Aufzeichnung aller Sitzungen von Benutzer UserA in Domäne DomainA und benachrichtigt UserA.
Start-BrokerSessionRecording -User DomainA \ UserA -NotifyUser \$false	Startet die Aufzeichnung aller Sitzungen des Benutzers UserA in der Domäne DomainA und benachrichtigt UserA nicht.
Start-BrokerSessionRecording -Sessions \$ SessionObject	Startet die Aufzeichnung aller Sitzungen im Objekt \$SessionObject und benachrichtigt den Benutzer. Um das Objekt \$sessionObject zu erhalten, führen Sie <code>\$SessionObject=Get-BrokerSession -username UserA</code> aus. Dem Namen von Objekten wird ein Dollarzeichen (\$) vorangestellt. Weitere Informationen finden Sie unter Schritt 2 und in der Onlinehilfe zu dem Befehl.
Start-BrokerSessionRecording -Sessions uid1,uid2,...,uidn	Startet die Aufzeichnung der Sitzungen uid1, uid2, ... und uidn und benachrichtigt die Benutzer.

- Verwenden Sie den Befehl `Get-BrokerSessionRecordingStatus`, um den Aufzeichnungsstatus aller Zielsitzungen abzurufen. Der Status müsste **SessionBeingRecorded** sein.
- Spielen Sie die Aufnahmen **live** oder nach **Abschluss der Aufnahme** im Sitzungsaufzeichnungsplayer ab und nehmen Sie die Problembehandlung vor.

**Hinweis:**

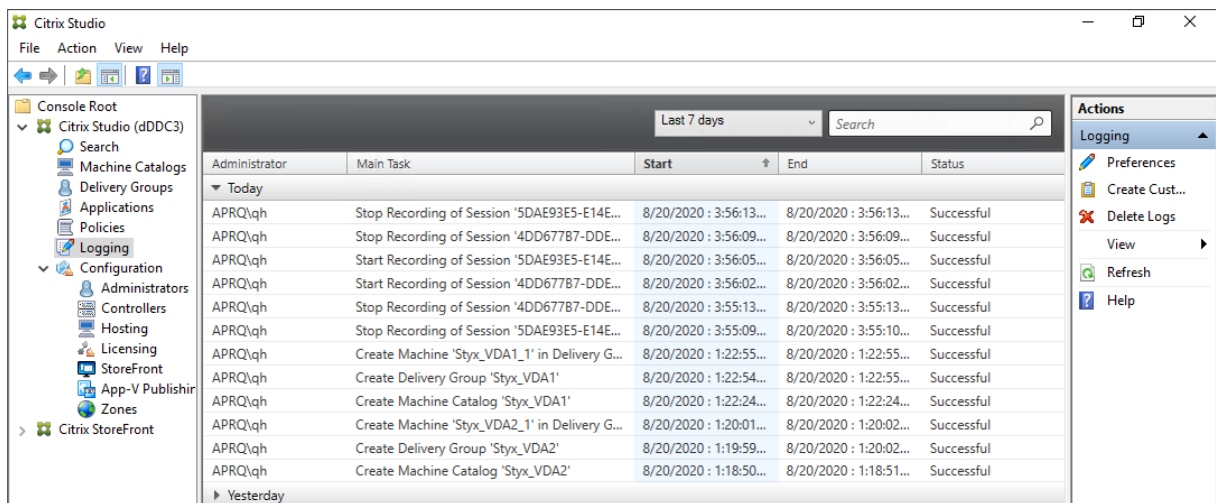
Der letzte Abschnitt der Zeitachse des Players wird möglicherweise grau angezeigt, wenn Sie eine abgeschlossene Sitzung wiedergeben, die mit dem Befehl `Stop-BrokerSessionRecording` beendet wurde und deren letzter Abschnitt inaktiv ist. Es ist nicht ersichtlich, wann eine aufgezeichnete Sitzung konstante Aktivitäten aufweist.

- Verwenden Sie den Befehl `Stop-BrokerSessionRecording`, um die Aufzeichnung anzuhalten, sobald das gemeldete Problem geklärt oder behoben wurde.

Die folgende Tabelle zeigt gängige Methoden zur Verwendung dieses Befehls:

Befehl	Beschreibung
Stop-BrokerSessionRecording -User DomainA \ UserA	Stoppt die Aufzeichnung aller Sitzungen von Benutzer UserA in Domäne DomainA.
Stop-BrokerSessionRecording -Sessions \$SessionObject	Stoppt die Aufzeichnung aller Sitzungen im Objekt \$SessionObject.
Stop-BrokerSessionRecording -Sessions uid1,uid2,...,uidn	Stoppt die Aufzeichnung der Sitzungen uid1, uid2, ... und uidn.

Auf dem Bildschirm **Protokollierung** von Citrix Studio können Sie die durch die Befehle **Start-BrokerSessionRecording** und **Stop-BrokerSessionRecording** erstellten Protokolle anzeigen.



## Konfigurieren

July 20, 2021

Nach der Installation der Sitzungsaufzeichnungskomponenten konfigurieren Sie die Sitzungsaufzeichnung mit den folgenden Schritten für die Aufzeichnung von Citrix Virtual Apps and Desktops-Sitzungen und das benutzerseitige Anzeigen der Sitzungen:

- [Konfigurieren der Verbindung mit dem Sitzungsaufzeichnungsserver](#)
- [Autorisieren von Benutzern](#)
- [Erstellen und Aktivieren von Aufzeichnungsrichtlinien](#)
- [Angaben des Speicherorts für Aufzeichnungen](#)
- [Angaben der Dateigröße für Aufzeichnungen](#)

- [Anpassen von Benachrichtigungen](#)
- [Aktivieren oder Deaktivieren der Aufzeichnung](#)
- [Aktivieren oder Deaktivieren digitaler Signaturen](#)
- [Administratorprotokollierung](#)
- [Hohe Datenbankverfügbarkeit](#)
- [Lastausgleich](#)
- [Ändern des Kommunikationsprotokolls](#)
- [Konfigurieren von CEIP](#)

## Konfigurieren der Verbindung mit dem Sitzungsaufzeichnungsserver

June 21, 2021

### Konfigurieren der Verbindung zwischen dem Sitzungsaufzeichnungsplayer und dem Sitzungsaufzeichnungsserver

Damit der Sitzungsaufzeichnungsplayer Sitzungen wiedergeben kann, konfigurieren Sie die Verbindung mit dem Sitzungsaufzeichnungsserver, auf dem die Sitzungsaufzeichnungen gespeichert sind. Jeder Player kann eine Verbindung mit mehreren Sitzungsaufzeichnungsservern herstellen, jedoch kann nur jeweils eine Verbindung aktiv sein. Wenn ein Sitzungsaufzeichnungsplayer eine Verbindung mit mehreren Sitzungsaufzeichnungsservern herstellen kann, können Benutzer den gewünschten Sitzungsaufzeichnungsserver durch Auswahl eines Kontrollkästchens auf der Registerkarte **Verbindungen** unter **Extras > Optionen** festlegen.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Starten Sie den Sitzungsaufzeichnungsplayer.
3. Klicken Sie auf der Menüleiste des Sitzungsaufzeichnungsplayers auf **Extras > Optionen**.
4. Klicken Sie auf der Registerkarte **Verbindungen** auf **Hinzufügen**.
5. Geben Sie im Feld **Hostname** den Namen oder die IP-Adresse der Maschine mit dem Sitzungsaufzeichnungsserver ein und wählen Sie das Protokoll aus. Standardmäßig verwendet die Sitzungsaufzeichnung HTTPS/SSL für die sichere Kommunikation. Wenn SSL nicht konfiguriert ist, wählen Sie HTTP.
6. Um den Sitzungsaufzeichnungsplayer so zu konfigurieren dass er eine Verbindung mit mehreren Sitzungsaufzeichnungsservern herstellen kann, wiederholen Sie Schritt 4 und 5 für jeden Server.
7. Aktivieren Sie das Kontrollkästchen für den Sitzungsaufzeichnungsserver, mit dem Sie eine Verbindung herstellen möchten.

## Konfigurieren der Verbindung zwischen dem Sitzungsaufzeichnungsagent und dem Sitzungsaufzeichnungsserver

Die Verbindung zwischen Sitzungsaufzeichnungsagent und dem Sitzungsaufzeichnungsserver wird normalerweise bei der Installation des Agents konfiguriert. Die Verbindung kann nach der Installation des Sitzungsaufzeichnungsagents in dessen Eigenschaften konfiguriert werden.

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Verbindungen**.
4. Geben Sie im Feld **Sitzungsaufzeichnungsserver** den FQDN des Sitzungsaufzeichnungsservers ein.

### Hinweis:

Um Message Queuing über HTTPS zu verwenden (Standardeinstellung ist TCP), geben Sie einen FQDN in das Feld **Sitzungsaufzeichnungsserver** ein. Andernfalls schlägt die Sitzungsaufzeichnung fehl.

5. Wählen Sie im Bereich **Nachrichtewarteschlange des Speichermanagers der Sitzungsaufzeichnung** das Protokoll aus, das der Speichermanager der Sitzungsaufzeichnung für die Kommunikation verwendet. Sie können auch die Standardportnummer ändern.

### Hinweis:

Um Message Queuing über HTTP und HTTPS zu verwenden, installieren Sie alle von IIS empfohlenen Features.

6. Akzeptieren Sie im Feld **Lebensdauer** den Standardwert 7200 Sekunden (zwei Stunden) oder geben Sie einen neuen Wert für die Anzahl der Sekunden ein, für die jede Nachricht in der Warteschlange gespeichert wird, wenn ein Kommunikationsfehler auftritt. Nach dem Ablauf dieses Zeitraums wird die Nachricht gelöscht und die Datei kann nur bis an die Stelle wiedergegeben werden, an der die Daten verloren wurden.
7. Wählen Sie im Bereich **Sitzungsaufzeichnungsbroker** das Protokoll aus, das der Sitzungsaufzeichnungsbroker für die Kommunikation verwendet. Sie können auch die Standardportnummer ändern.
8. Starten Sie auf Aufforderung den **Sitzungsaufzeichnungsagent-Dienst** neu, um die Änderung zu übernehmen.



## Autorisieren von Benutzern

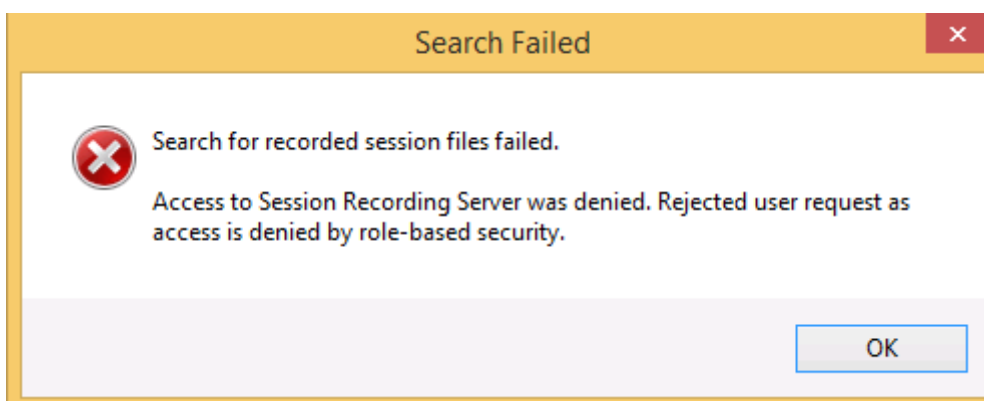
January 15, 2024

Zum Zuweisen von Berechtigungen weisen Sie Benutzern in der Sitzungsaufzeichnungsautorisierungskonsole auf dem Sitzungsaufzeichnungsserver Rollen zu. Fünf Rollen stehen zur Verfügung:

### Wichtig:

Aus Sicherheitsgründen sollten Sie den Benutzern nur die Rechte geben, die sie zum Ausführen bestimmter Funktionen benötigen, z. B. Anzeigen aufgezeichneter Sitzungen.

- **PolicyAdministrator.** Mitglieder dieser Rolle können Aufzeichnungsrichtlinien anzeigen, erstellen, bearbeiten, löschen und aktivieren. In der Standardeinstellung sind Administratoren der Maschine mit dem Sitzungsaufzeichnungsserver Mitglieder dieser Rolle.
- **PolicyQuery.** Die Server mit dem Sitzungsaufzeichnungsagent können Auswertungen der Aufzeichnungsrichtlinie anfordern. In der Standardeinstellung sind authentifizierte Benutzer Mitglieder dieser Rolle.
- **LoggingWriter.** Hat Berechtigung zum Schreiben von Administratorprotokollen. Standardmäßig sind lokale Administratoren und die Gruppe "Netzwerkdienst" Mitglied dieser Rolle. Eine Änderung der Standardmitglieder der Rolle **LoggingWriter** kann dazu führen, dass das Schreiben des Protokolls fehlschlägt.
- **LoggingReader.** Hat Berechtigung zum Abfragen von Administratorprotokollen. Für diese Rolle besteht keine Standardeinstellung.
- **Player.** Kann aufgezeichnete Citrix Virtual Apps and Desktops-Sitzungen anzeigen. Für diese Rolle besteht keine Standardeinstellung. Nach der Installation der Sitzungsaufzeichnung ist zunächst kein Benutzer berechtigt, Sitzungsaufzeichnungen wiederzugeben. Sie müssen jedem Benutzer, auch dem Administrator, diese Berechtigung zuweisen. Ein Benutzer ohne Berechtigung zur Wiedergabe von Sitzungsaufzeichnungen erhält die folgende Fehlermeldung bei dem Versuch, eine Sitzungsaufzeichnung wiederzugeben:



Führen Sie folgende Schritte aus, um Benutzer einer Rolle zuzuweisen:

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver als Administrator an.
2. Starten Sie die Sitzungsaufzeichnungsautorisierungskonsole.
3. Wählen Sie die Rolle, der Sie Benutzer zuweisen möchten.
4. Wählen Sie auf der Menüleiste **Aktion > Benutzer und Gruppen zuweisen**.
5. Fügen Sie die Benutzer und Gruppen hinzu.

Die Sitzungsaufzeichnung unterstützt in Active Directory definierte Benutzer und Gruppen.

In der Konsole vorgenommene Änderungen werden beim Update (das jede Minute erfolgt) übernommen. Darüber hinaus können Sie ab der Version 1906 die Richtlinienkonsole für die Sitzungsaufzeichnung verwenden, um Aufzeichnungsanzeigerichtlinien zu erstellen. Weitere Informationen finden Sie unter [Aufzeichnungsanzeigerichtlinien](#).

## Richtlinien konfigurieren

April 3, 2024

Mit der Richtlinienkonsole für die Sitzungsaufzeichnung erstellen Sie Richtlinien zum Aufzeichnen, für Ereignisprotokollierung und zum Anzeigen von Aufzeichnungen. Beim Erstellen von Richtlinien können Sie Delivery Controller in der Citrix Cloud und in On-Premises-Umgebungen angeben.

### **Wichtig:**

Um die Richtlinienkonsole für die Sitzungsaufzeichnung zu verwenden, muss das Broker PowerShell Snap-in (Broker\_PowerShellSnapIn\_x64.msi) oder das Citrix Virtual Apps and Desktops Remote PowerShell SDK (CitrixPoshSdk.exe) installiert sein. Das Installationsprogramm installiert die Snap-Ins nicht automatisch. Suchen Sie das Broker PowerShell-Snap-In auf dem Citrix Virtual Apps and Desktops-ISO (`\\layout\image-full\x64\Citrix Desktop Delivery Controller`). Suchen Sie das Citrix Virtual Apps and Desktops Remote PowerShell (PS) SDK auf der [Citrix Website](#). Folgen Sie den Anweisungen die manuelle Installation des Snap-Ins und des SDK. Anderenfalls kann es zu Fehlern kommen.

### **Tipp:**

Sie können die Registrierung bearbeiten, um den Verlust von Aufzeichnungsdateien zu verhindern, falls Ihr Sitzungsaufzeichnungsserver unerwartet ausfällt. Melden Sie sich als Administrator bei der Maschine an, auf der der Sitzungsaufzeichnungsagent installiert ist, öffnen Sie den Registrierungs-Editor und fügen Sie unter `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix`

```
\SmartAuditor\Agent einen DWORD-Wert hinzu: DefaultRecordActionOnError=1
```

## Aufzeichnungsrichtlinien

Sie können systemdefinierte Aufzeichnungsrichtlinien aktivieren oder eigene Aufzeichnungsrichtlinien erstellen und aktivieren. Systemdefinierte Aufzeichnungsrichtlinien wenden eine Regel auf alle Benutzer, veröffentlichten Anwendungen und Server an. In benutzerdefinierten Aufzeichnungsrichtlinien geben Sie an, welche Benutzer, veröffentlichten Anwendungen und Server aufgezeichnet werden.

Die aktive Aufzeichnungsrichtlinie legt fest, welche Sitzungen aufgezeichnet werden. Nur jeweils eine Aufzeichnungsrichtlinie ist aktiv.

### Systemdefinierte Aufzeichnungsrichtlinien

Die Sitzungsaufzeichnung bietet die folgenden systemdefinierten Aufzeichnungsrichtlinien:

- **Nicht aufzeichnen.** Die Standardrichtlinie. Wenn Sie keine andere Richtlinie festlegen, wird keine Sitzung aufgezeichnet.
- **Alle mit Benachrichtigung aufzeichnen.** Bei Auswahl dieser Richtlinie werden alle Sitzungen aufgezeichnet. Ein Popupfenster wird angezeigt, um auf die Aufzeichnung hinzuweisen.
- **Alle ohne Benachrichtigung aufzeichnen.** Bei Auswahl dieser Richtlinie werden alle Sitzungen aufgezeichnet. Kein Popupfenster wird angezeigt, um auf die Aufzeichnung hinzuweisen.

Sie können die systemdefinierten Aufzeichnungsrichtlinien nicht ändern oder löschen.

### Erstellen einer benutzerdefinierten Aufzeichnungsrichtlinie

Beim Erstellen einer eigenen Aufzeichnungsrichtlinie definieren Sie anhand von Regeln die Benutzer oder Gruppen, veröffentlichten Anwendungen oder Desktops, Bereitstellungsgruppen oder VDA-Maschinen sowie Client-IP-Adressen der Citrix Workspace-App, deren Sitzungen aufgezeichnet werden. Ein Assistent in der Richtlinienkonsole für die Sitzungsaufzeichnung unterstützt Sie beim Erstellen der Regeln. Zum Abrufen der Liste der veröffentlichten Anwendungen oder Desktops und der Liste der Bereitstellungsgruppen oder VDA-Maschinen ist eine Leseberechtigung als Siteadministrator erforderlich. Konfigurieren Sie die Administrator-Leseberechtigung auf dem Delivery Controller der Site.

Für jede erstellte Regel geben Sie eine Aufzeichnungsaktion und Regelkriterien an. Die Aufzeichnungsaktion gilt für Sitzungen, die das Regelkriterium erfüllen.

Wählen Sie für jede Regel eine Aufzeichnungsaktion aus:

- **Nicht aufzeichnen.** (Wählen Sie **Sitzungsaufzeichnung deaktivieren** im Assistenten für **Regeln**.) Diese Aufzeichnungsaktion gibt an, dass Sitzungen, die das Regelkriterium erfüllen, nicht aufgezeichnet werden.
- **Mit Benachrichtigung aufzeichnen.** (Wählen Sie **Sitzungsaufzeichnung mit Benachrichtigung aktivieren** im Assistenten für **Regeln**.) Diese Aufzeichnungsaktion gibt an, dass Sitzungen, die das Regelkriterium erfüllen, aufgezeichnet werden. Ein Popupfenster wird angezeigt, um auf die Aufzeichnung hinzuweisen.
- **Ohne Benachrichtigung aufzeichnen.** (Wählen Sie **Sitzungsaufzeichnung ohne Benachrichtigung aktivieren** im Assistenten für **Regeln**.) Diese Aufzeichnungsaktion gibt an, dass Sitzungen, die das Regelkriterium erfüllen, aufgezeichnet werden. Benutzer werden nicht über die Aufzeichnung informiert.

Wählen Sie für jede Regel mindestens eines der folgenden Elemente, um ein Regelkriterium zu erstellen:

- **Benutzer oder Gruppen.** Erstellt eine Liste der Benutzer oder Gruppen, für die die Aktion der Regel gilt. Sie können in der Sitzungsaufzeichnung [Active Directory-Gruppen](#) und [Positivlisten für Benutzer](#) verwenden.
- **Veröffentlichte Anwendungen oder Desktops.** Erstellt eine Liste der veröffentlichten Anwendungen oder Desktops, für die die Aktion der Regel gilt. Wählen Sie im Assistenten für **Regeln** die Citrix Virtual Apps and Desktops-Sites aus, auf denen die Anwendungen bzw. Desktops verfügbar sind.
- **Bereitstellungsgruppen oder Maschinen.** Erstellt eine Liste der Bereitstellungsgruppen oder Maschinen, für die die Aktion der Regel gilt. Wählen Sie im Assistenten für **Regeln** den Speicherort der Bereitstellungsgruppen oder Maschinen.
- **IP-Adresse oder IP-Bereich.** Erstellt eine Liste von IP-Adressen oder IP-Adressbereichen, für die die Aktion der Regel gilt. Fügen Sie auf dem Bildschirm **IP-Adresse und IP-Bereich auswählen** eine gültige IP-Adresse oder einen IP-Adressbereich hinzu, für die bzw. den die Aufzeichnung aktiviert oder deaktiviert werden soll. Bei den hier genannten IP-Adressen handelt es sich um die IP-Adressen der Citrix Workspace-Apps.

#### Hinweis:

Die Richtlinienkonsole für die Sitzungsaufzeichnung unterstützt das Konfigurieren mehrerer Kriterien innerhalb einer Regel. Ist eine Regel anwendbar, werden zum Berechnen der endgültigen Aktion die logischen Operatoren "AND" und "OR" verwendet. Dabei wird der Operator "OR" meist zwischen Elementen innerhalb eines Kriteriums verwendet, während der Operator "AND" zwischen separaten Kriterien zum Einsatz kommt. Wenn das Ergebnis "true" ist, führt die Engine für die Sitzungsaufzeichnungsrichtlinie die Regelaktion aus. Ansonsten wird die nächste Regel aufgerufen und der Prozess wird wiederholt.

Wenn Sie mehrere Regeln in einer Aufzeichnungsrichtlinie erstellen, können einige Sitzungen die Kri-

terien für mehrere Regeln erfüllen. In diesen Situationen wird die Regel mit der höchsten Priorität auf die Sitzungen angewendet.

Die Aufzeichnungsaktion einer Regel legt die Priorität fest:

- Regeln mit der Aktion **Sitzungsaufzeichnung deaktivieren** haben die höchste Priorität.
- Regeln mit der Aktion **Sitzungsaufzeichnung mit Benachrichtigung aktivieren** haben die nächsthöhere Priorität.
- Regeln mit der Aktion **Sitzungsaufzeichnung ohne Benachrichtigung aktivieren** haben die niedrigste Priorität.

Einige Sitzungen erfüllen ggf. kein Regelkriterium in einer Aufzeichnungsrichtlinie. Für diese Sitzungen gilt die Aktion der Fallbackregel der Richtlinie. Die Aktion der Fallbackregel ist immer **Nicht aufzeichnen**. Sie können die Fallbackregel nicht ändern oder löschen.

Erstellen einer benutzerdefinierten Aufzeichnungsrichtlinie:

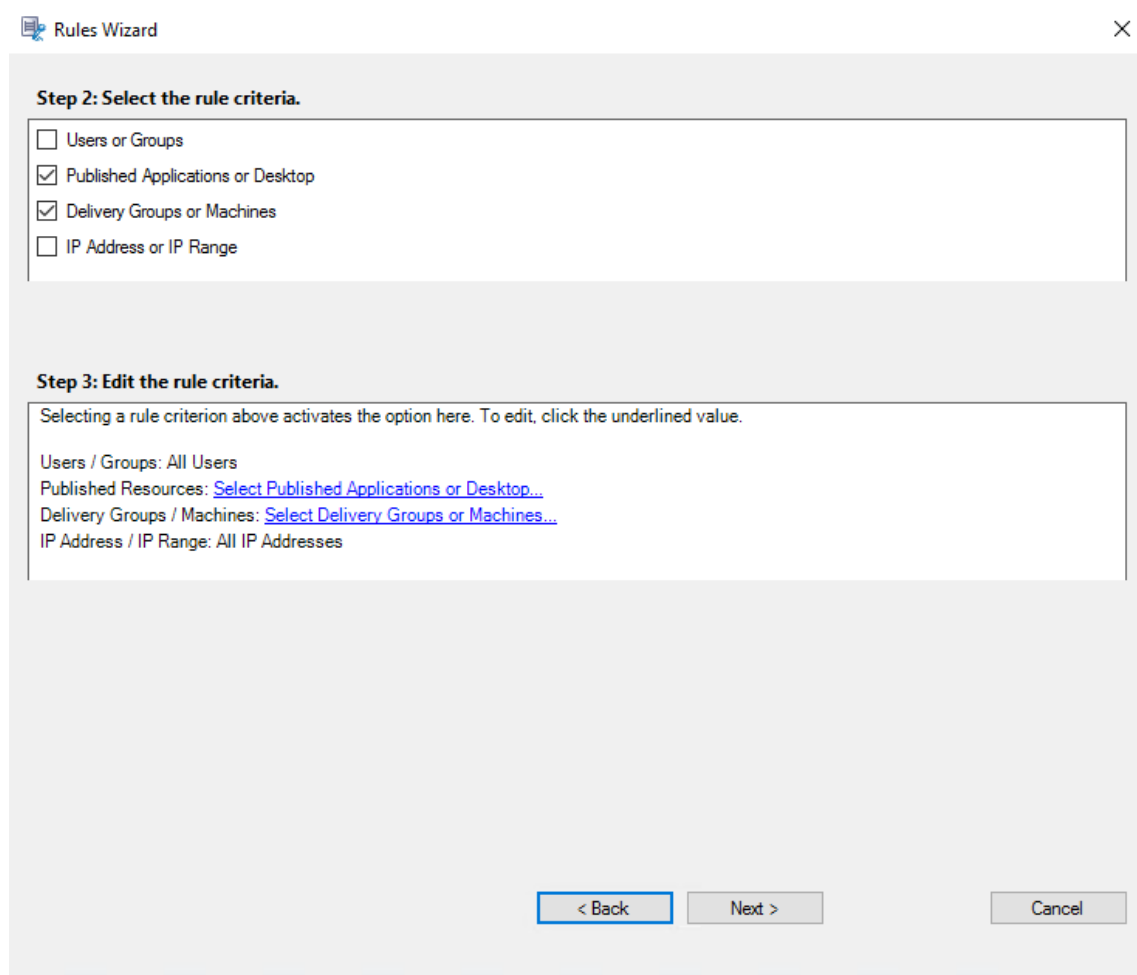
1. Melden Sie sich bei dem Server, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist, als autorisierter Richtlinienadministrator an.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung und wählen Sie links **Aufzeichnungsrichtlinien**. Wählen Sie in der Menüleiste **Neue Richtlinie hinzufügen**.
3. Klicken Sie mit der rechten Maustaste auf **Neue Richtlinie** und wählen Sie **Neue Regel hinzufügen**.
4. Aufzeichnungsoption - Wählen Sie im Assistenten für **Regeln** die Option **Sitzungsaufzeichnung deaktivieren**, **Sitzungsaufzeichnung mit Benachrichtigung aktivieren** oder **Sitzungsaufzeichnung ohne Benachrichtigung aktivieren** und klicken Sie auf **Weiter**.
5. Regelkriterien - Sie können ein oder mehrere Regelkriterien wählen:  
**Benutzer oder Gruppen**  
**Veröffentlichte Anwendungen oder Desktops**  
**Bereitstellungsgruppen oder Maschinen**  
**IP-Adresse oder IP-Bereich**
6. Regelkriterium bearbeiten: Klicken Sie zum Bearbeiten auf die unterstrichenen Werte. Welche Werte unterstrichen sind, hängt von den Kriterien ab, die Sie im vorherigen Schritt ausgewählt haben.

**Hinweis:**

Bei Auswahl der Option **Veröffentlichte Anwendungen oder Desktops** ist die **Siteadresse** die IP-Adresse, eine URL oder ein Maschinename, wenn der Controller in einem lokalen Netzwerk ist. Die Liste **Name der Anwendung** enthält den Anzeigenamen.

Wenn Sie **Veröffentlichte Anwendungen oder Desktops** oder **Bereitstellungsgruppen oder Maschinen** wählen, geben Sie den Delivery Controller an mit dem die Richtlinienkonsole für die Sitzungsaufzeichnung kommunizieren soll.

Die Richtlinienkonsole für die Sitzungsaufzeichnung ist die einzige Methode für die Kommunikation mit Delivery Controllern in der Citrix Cloud und On-Premises-Umgebungen.



The screenshot shows a 'Rules Wizard' dialog box with a close button (X) in the top right corner. It is divided into two sections:

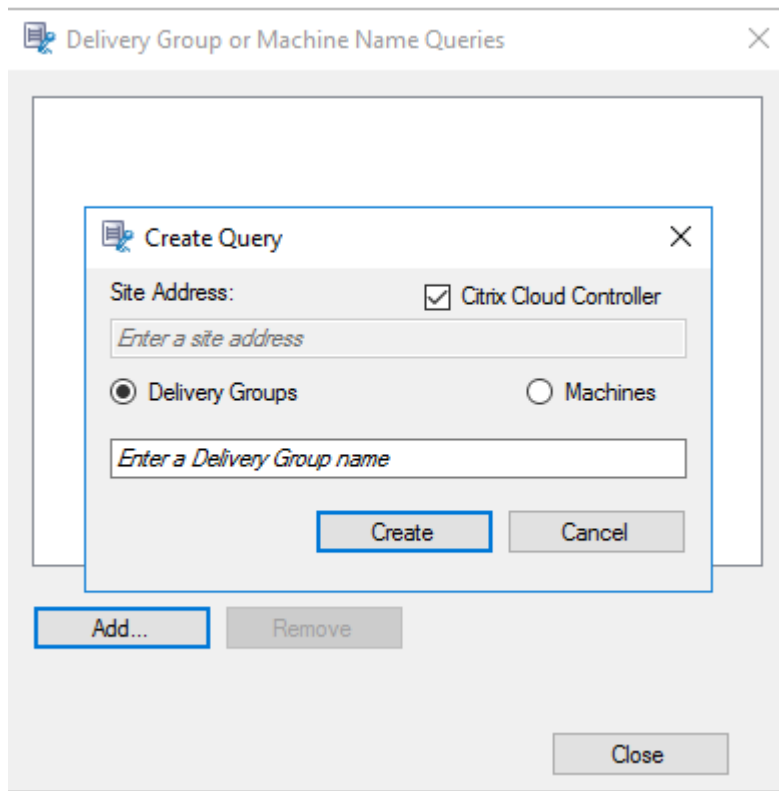
- Step 2: Select the rule criteria.** This section contains a list of four options with checkboxes:
  - Users or Groups
  - Published Applications or Desktop
  - Delivery Groups or Machines
  - IP Address or IP Range
- Step 3: Edit the rule criteria.** This section contains a text box with the following text:

Selecting a rule criterion above activates the option here. To edit, click the underlined value.

Users / Groups: All Users  
Published Resources: [Select Published Applications or Desktop...](#)  
Delivery Groups / Machines: [Select Delivery Groups or Machines...](#)  
IP Address / IP Range: All IP Addresses

At the bottom of the dialog, there are three buttons: '< Back' (highlighted with a blue border), 'Next >', and 'Cancel'.

Beispiel: Klicken Sie für **Bereitstellungsgruppen oder Maschinen** in Schritt 3 auf den entsprechenden Hyperlink wie im Screenshot oben, und klicken Sie auf **Hinzufügen**, um dem Controller Abfragen hinzuzufügen.



Eine Beschreibung der Anwendungsfälle für On-Premises und Citrix Cloud Delivery Controller finden Sie in der folgenden Tabelle:

Anwendungsfall	Aktion erforderlich
On-Premises Delivery Controller	a) Installieren Sie Broker_PowerShellSnapIn_x64.msi. 2. Deaktivieren Sie das Kontrollkästchen <b>Citrix Cloud Controller</b> .
Citrix Cloud Delivery Controller	a) Installieren Sie das Citrix Virtual Apps and Desktops Remote PowerShell SDK. 2. Überprüfen Sie die Anmeldeinformationen des Citrix Cloud-Kontos. 3. Aktivieren Sie das Kontrollkästchen <b>Citrix Cloud Controller</b> .

Anwendungsfall	Aktion erforderlich
Wechseln von einem On-Premises-Delivery Controller zu einem Citrix Cloud Delivery Controller	a) Deinstallieren Sie Broker_PowerShellSnapIn_x64.msi und starten Sie die Maschine neu. 2. Installieren Sie das Citrix Virtual Apps and Desktops Remote PowerShell SDK. 3. Überprüfen Sie die Anmeldeinformationen des Citrix Cloud-Kontos. 4. Aktivieren Sie das Kontrollkästchen <b>Citrix Cloud Controller</b> .
Wechseln von einem Citrix Cloud -Delivery Controller zu einem On-Premises-Delivery Controller	a) Deinstallieren Sie das Citrix Virtual Apps and Desktops Remote PowerShell SDK und starten Sie die Maschine neu. 2. Installieren Sie Broker_PowerShellSnapIn_x64.msi. 3. Deaktivieren Sie das Kontrollkästchen <b>Citrix Cloud Controller</b> .

---

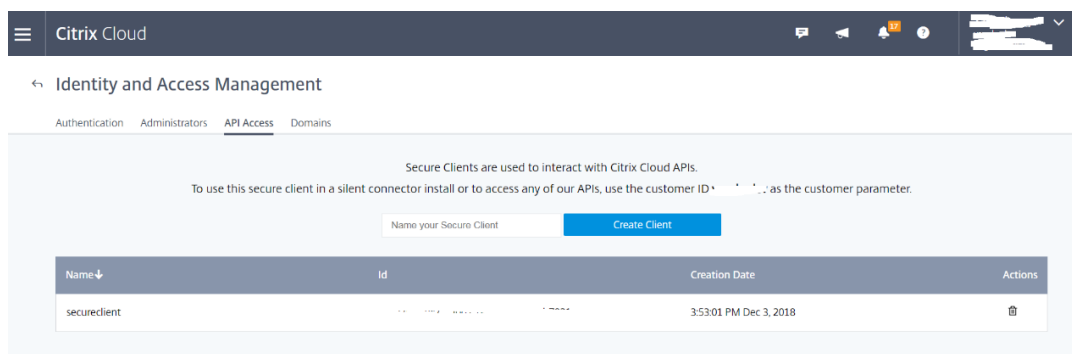
Überprüfen der Anmeldeinformationen des Citrix Cloud-Kontos

Für Abfragen an Delivery Controller, die in Citrix Cloud gehostet werden, validieren Sie Ihre Citrix Cloud-Anmeldeinformationen auf der Maschine, auf der die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist. Sonst kann zu einem Fehler kommen und die Richtlinienkonsole für die Sitzungsaufzeichnung funktioniert möglicherweise nicht wie erwartet.

Ausführen einer manuellen Überprüfung:

- a) Melden Sie sich an der Citrix Cloud-Konsole an und navigieren Sie zu **Identitäts- und Zugriffsverwaltung > API-Zugriff**. Erstellen Sie einen API-Zugriff Secure Client, um ein Authentifizierungsprofil zu erhalten, das die Citrix Cloud-Authentifizierungsaufforderungen umgehen kann. Laden Sie Ihren Secure Client herunter, benennen Sie ihn um und speichern Sie ihn an einem sicheren Ort. Der Dateiname wird standardmäßig auf `secureclient.csv` gesetzt.





- b) Öffnen Sie eine PowerShell-Sitzung und führen Sie den folgenden Befehl aus, damit das im vorherigen Schritt erhaltene Authentifizierungsprofil wirksam wird.

```
1 asnp citrix.*
2 Set-XDCredentials -CustomerId "citrixdemo" -SecureClientFile "
  c:\temp\secureclient.csv" -ProfileType CloudAPI -StoreAs "
  default"
3
4 <!--NeedCopy-->
```

Legen Sie **CustomerID** und **SecureClientFile** nach Bedarf fest. Mit dem voranstehenden Befehl wird ein Standardauthentifizierungsprofil für den Kunden `citrixdemo` erstellt, um Authentifizierungsaufforderungen in den aktuellen und allen nachfolgenden PowerShell-Sitzungen zu umgehen.

7. Folgen Sie dem Assistenten, um die Konfiguration abzuschließen.

**Hinweis:** Einschränkung für vorab gestartete Anwendungssitzungen:

- Wenn die aktive Richtlinie versucht, einen Anwendungsnamen zuzuordnen, werden die in der vorab gestarteten Sitzung gestartete Anwendungen nicht zugeordnet, sodass die Sitzung nicht aufgezeichnet wird.
- Wenn die aktive Richtlinie jede Anwendung aufzeichnet und der Benutzer sich bei Citrix Workspace-App für Windows anmeldet (zur gleichen Zeit, zu der die vorab gestartete Sitzung eingerichtet wird), erscheint eine Aufzeichnungsbenachrichtigung und die leere Sitzung sowie alle darin ab diesem Zeitpunkt gestarteten Anwendungen werden aufgezeichnet.

Veröffentlichen Sie als Workaround Anwendungen gemäß ihrer Aufzeichnungsrichtlinien in separaten Bereitstellungsgruppen. Verwenden Sie keine Anwendungsnamen als Aufzeichnungsbedingung. Dadurch wird sichergestellt, dass vorab gestartete Sitzungen aufgezeichnet werden können. Benachrichtigungen werden jedoch weiterhin angezeigt.

**Verwenden von Active Directory-Gruppen** Beim Erstellen von Richtlinien können Sie in der Sitzungsaufzeichnung Active Directory-Gruppen verwenden. Active Directory-Gruppen statt einzel-

ner Benutzer vereinfachen die Erstellung und Verwaltung von Regeln und Richtlinien. Beispiel: Wenn Benutzer in der Buchhaltungsabteilung des Unternehmens zur Active Directory-Gruppe "Finanz" gehören, können Sie eine Regel erstellen, die für alle Mitglieder dieser Gruppe gilt, indem Sie die Gruppe "Finanz" beim Erstellen der Regel im Assistenten für **Regeln** auswählen.

**Positivliste der Benutzer** Sie können Richtlinien für die Sitzungsaufzeichnung erstellen, die sicherstellen, dass die Sitzungen bestimmter Benutzer im Unternehmen nie aufgezeichnet werden. Dies wird

*Positivliste* der Benutzer genannt. Positivlisten sind nützlich für Benutzer, die mit datenschutzrelevanten Informationen umgehen oder wenn Ihre Organisation die Sitzungen einer bestimmten Mitarbeiterklasse nicht aufzeichnen möchte.

Wenn beispielsweise alle Mitglieder der Geschäftsleitung im Unternehmen zu einer Active Directory-Gruppe Geschäftsführung gehören, können Sie sicherstellen, dass die Sitzungen dieser Benutzer nie aufgezeichnet werden, indem Sie eine Regel erstellen, mit der die Sitzungsaufzeichnung für die Gruppe Geschäftsführung deaktiviert wird. Während die Richtlinie, die diese Regel enthält, aktiv ist, werden keine Sitzungen der Mitglieder der Gruppe "Geschäftsführung" aufgezeichnet. Die Sitzungen anderer Mitarbeiter im Unternehmen werden basierend auf den anderen Regeln in der aktiven Richtlinie aufgezeichnet.

## **Konfigurieren von Director zur Verwendung des Sitzungsaufzeichnungsservers**

Sie können mit der Director-Konsole die Aufzeichnungsrichtlinien erstellen und aktivieren.

1. Zur Verwendung einer HTTPS-Verbindung installieren Sie das Zertifikat zum Vertrauen des Sitzungsaufzeichnungsservers im Ordner mit den vertrauenswürdigen Stammzertifikaten des Director-Servers.
2. Zum Konfigurieren des Director-Servers für die Verwendung des Sitzungsaufzeichnungsservers führen Sie den Befehl **C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording** aus.
3. Geben Sie die IP-Adresse bzw. den FQDN des Sitzungsaufzeichnungsservers, die Portnummer und den Verbindungstyp (HTTP/HTTPS) für die Verbindung zwischen Sitzungsaufzeichnungssagent und Sitzungsaufzeichnungsbroker auf dem Director-Server ein.

## **Ereignisprotokollierungsrichtlinien**

Die Sitzungsaufzeichnung unterstützt die zentralisierte Konfiguration von Ereignisprotokollierungsrichtlinien. Sie können Richtlinien in der Richtlinienkonsole für die Sitzungsaufzeichnung erstellen, um verschiedene Ereignisse zu protokollieren.

**Hinweis:**

Verwenden Sie Sitzungsaufzeichnung Version 1811 oder höher, um das Anschließen von USB-Massenspeichergeräten sowie Anwendungsstarts und das Beenden von Anwendungen zu protokollieren.

Verwenden Sie zum Protokollieren von Dateivorgängen und Webbrowsingaktivitäten die Sitzungsaufzeichnung Version 1903 oder höher.

Verwenden Sie zum Protokollieren von Zwischenablageaktivitäten die Sitzungsaufzeichnung Version 2012 oder höher.

### **Systemdefinierte Ereignisprotokollierungsrichtlinie**

Die systemdefinierte Ereignisprotokollierungsrichtlinie ist **Nicht protokollieren**. Sie ist standardmäßig inaktiv. Wenn sie aktiv ist, werden keine Ereignisse protokolliert.

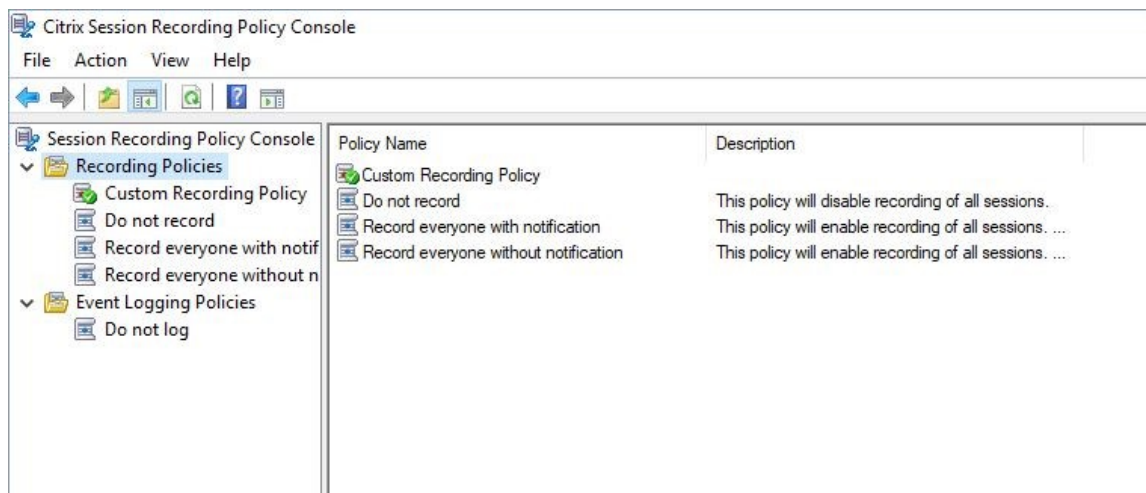
Sie können die systemdefinierte Ereignisprotokollierungsrichtlinie nicht ändern oder löschen.

### **Erstellen einer benutzerdefinierten Ereignisprotokollierungsrichtlinie**

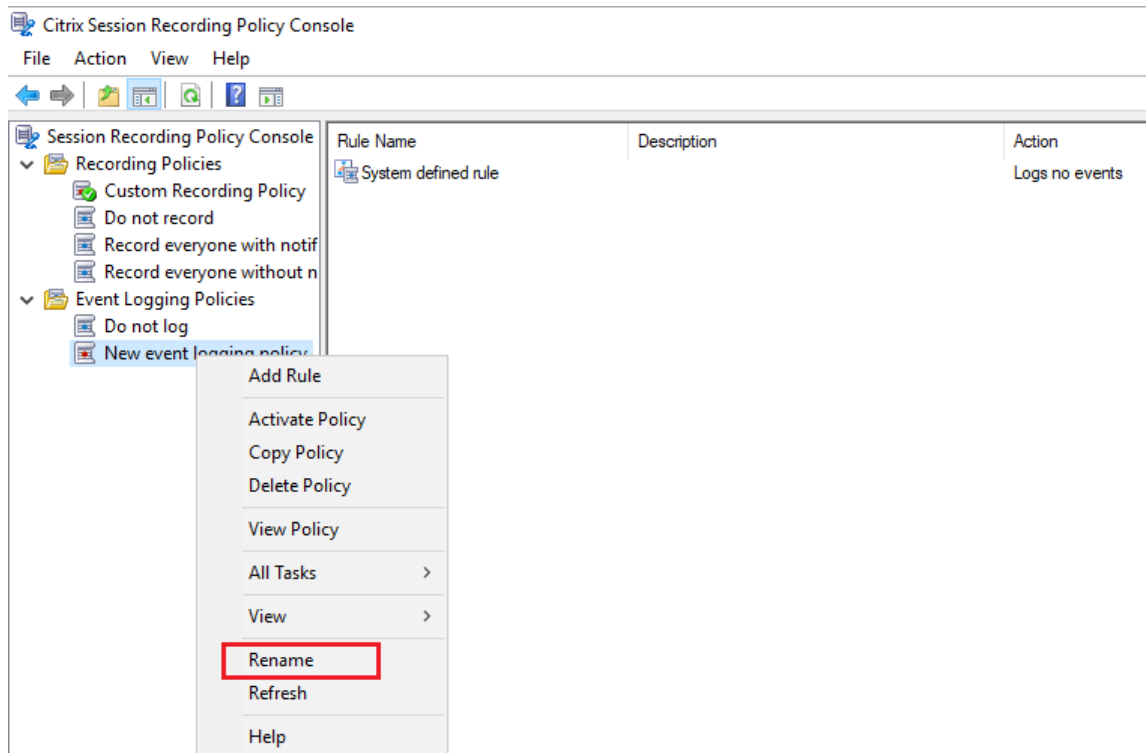
Beim Erstellen einer eigenen Ereignisprotokollierungsrichtlinie definieren Sie anhand von Regeln die Benutzer oder Gruppen, veröffentlichten Anwendungen oder Desktops, Bereitstellungsgruppen oder VDA-Maschinen sowie Client-IP-Adressen der Citrix Workspace-App, für die spezielle Ereignisse während der Sitzungsaufzeichnung protokolliert werden sollen. Ein Assistent in der Richtlinienkonsole für die Sitzungsaufzeichnung unterstützt Sie beim Erstellen der Regeln. Zum Abrufen der Liste der veröffentlichten Anwendungen oder Desktops und der Liste der Bereitstellungsgruppen oder VDA-Maschinen ist eine Leseberechtigung als Siteadministrator erforderlich. Konfigurieren Sie die Administrator-Leseberechtigung auf dem Delivery Controller der Site.

Erstellen einer benutzerdefinierten Ereignisprotokollierungsrichtlinie:

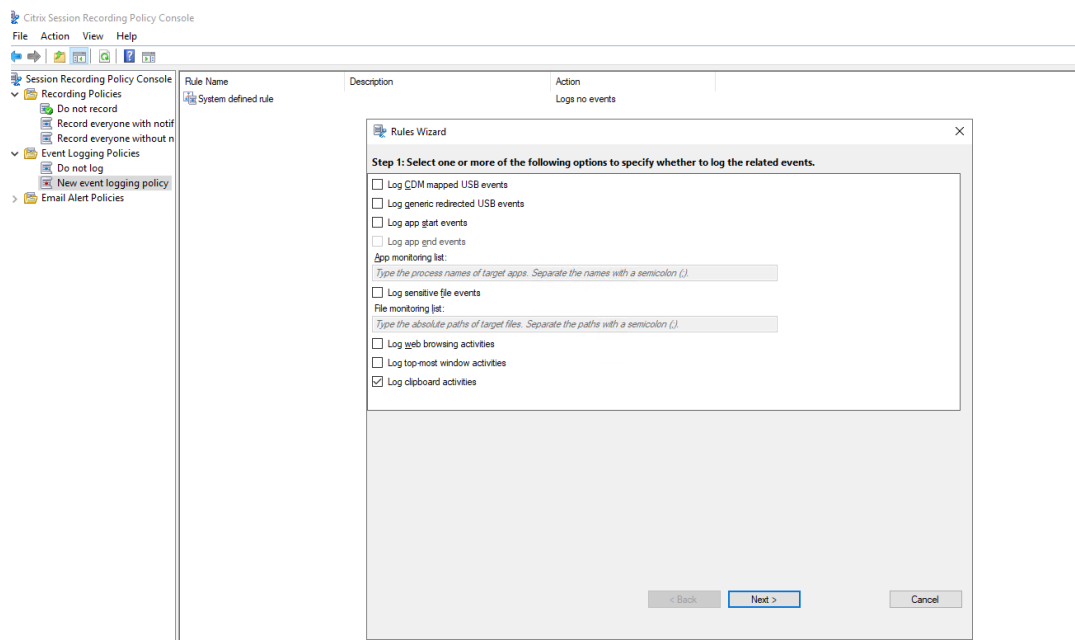
1. Melden Sie sich bei dem Server, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist, als autorisierter Richtlinienadministrator an.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung. Standardmäßig ist keine Ereignisprotokollierungsrichtlinie aktiv.



3. Wählen Sie im linken Bereich die Option **Ereignisprotokollierungsrichtlinien**. Wählen Sie in der Menüleiste **Neue Richtlinie hinzufügen**, um eine Ereignisprotokollierungsrichtlinie zu erstellen.
4. (Optional) Klicken Sie mit der rechten Maustaste auf die neue Ereignisprotokollierungsrichtlinie, um sie umzubenennen.



5. Klicken Sie mit der rechten Maustaste auf die neue Ereignisprotokollierungsrichtlinie und wählen Sie **Neue Regel hinzufügen**.
  - a) Aktivieren Sie das Kontrollkästchen neben jedem zu überwachenden Zielereignis.



- **CDM zugeordnete USB-Ereignisse protokollieren:** Protokolliert das Anschließen eines per Clientlaufwerkzuordnung (CDM) zugeordneten Massenspeichergeräts an ein Clientgerät und markiert das Ereignis in der Aufzeichnung, wenn die Citrix Workspace-App für Windows oder für Mac auf dem Clientgerät installiert ist.
- **Generische umgeleitete USB-Ereignisse protokollieren:** Protokolliert das Anschließen eines generischen umgeleiteten Massenspeichergeräts an einen Client und markiert das Ereignis in der Aufzeichnung, wenn die Citrix Workspace-App für Windows oder für Mac auf dem Clientgerät installiert ist.
- **App-Startereignisse protokollieren:** Protokolliert das Starten von Ziellanwendungen und markiert das Ereignis in der Aufzeichnung.
- **App-Endereignisse protokollieren:** Protokolliert das Beenden von Ziellanwendungen und markiert das Ereignis in der Aufzeichnung.

#### Hinweis:

Die Sitzungsaufzeichnung kann das Beenden einer Anwendung nur protokollieren, wenn auch der Start erfasst wurde. Daher ist im Assistenten für Regeln das Kontrollkästchen **App-Endereignisse protokollieren** abgeblendet, bis Sie **App-Startereignisse protokollieren** auswählen.

- **App-Überwachungsliste:** Wenn Sie **App-Startereignisse protokollieren** und **App-Endereignisse protokollieren** auswählen, können Sie mit der **App-Überwachungsliste** die zu überwachenden Ziellanwendungen angeben, um eine übermäßige Anzahl an Ereignissen in den Aufzeichnungen zu vermeiden.

**Hinweis:**

- Um das Starten oder Beenden einer Anwendung zu erfassen, fügen Sie den Prozessnamen der Anwendung der **App-Überwachungsliste** hinzu. Um beispielsweise den Start der Remotedesktopverbindung zu erfassen, fügen Sie der **App-Überwachungsliste** den Prozessnamen `mstsc.exe` hinzu. Wenn Sie in der **App-Überwachungsliste** einen Prozess hinzufügen, werden Anwendungen überwacht, die vom hinzugefügten Prozess und seinen untergeordneten Prozessen gesteuert werden. Die Sitzungsaufzeichnung fügt standardmäßig die Prozessnamen `cmd.exe`, `powershell.exe` und `wsl.exe` zur **App-Überwachungsliste** hinzu. Wenn Sie **App-Startereignisse protokollieren** und **App-Endereignisse protokollieren** für eine Ereignisprotokollierungsrichtlinie auswählen, werden Starts und Beenden der Apps Eingabeaufforderung, PowerShell und Windows-Subsystem für Linux (WSL) unabhängig davon protokolliert, ob Sie die zugehörigen Prozessnamen manuell zur **App-Überwachungsliste** hinzugefügt haben. Die Standardprozessnamen sind in der **App-Überwachungsliste** nicht sichtbar.
- Trennen Sie Prozessnamen durch ein Semikolon (;).
- Nur exakte Übereinstimmungen werden unterstützt. Platzhalter werden nicht unterstützt.
- Bei Prozessnamen muss die Groß-/Kleinschreibung nicht beachtet werden.
- Um zu vermeiden, dass zu viele Ereignisse die Aufzeichnungen überfluten, fügen Sie keine Systemprozessnamen (z. B. `explorer.exe`) und Webbrowser in den Registrierungseintrag ein.

- **Vertrauliche Dateiereignisse protokollieren:** Vorgänge für Zieldateien in der Aufzeichnung protokollieren.
- **Dateiüberwachungsliste:** Wenn Sie **Vertrauliche Dateiereignisse protokollieren** wählen, geben Sie mit der **Dateiüberwachungsliste** die zu überwachenden Zieldateien an. Sie können Ordner angeben, um alle darin enthaltenen Dateien zu erfassen. Standardmäßig ist keine Datei angegeben, d. h. es wird keine Datei standardmäßig erfasst.

**Hinweis:**

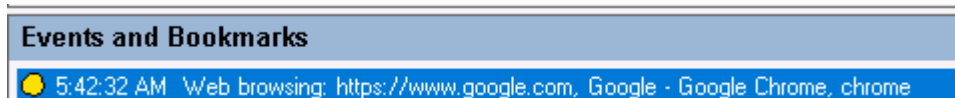
- Um Vorgänge zum Umbenennen, Erstellen, Löschen oder Verschieben einer Datei zu erfassen, fügen Sie die Pfadzeichenfolge des Dateiordners (nicht den Dateinamen oder den Stammpfad des Dateiordners) in **Dateiüberwachungsliste** ein. Um beispielsweise das Umbenennen, Erstellen, Löschen oder Verschieben der Datei `“sharing.ppt”` in `“C:\`

User\File” zu erfassen, fügen Sie die Pfadzeichenfolge C:\User\File in **Dateiüberwachungsliste** ein.

- Es werden Pfade für lokale Dateien und freigegebene Remoteordner unterstützt. Um beispielsweise Vorgänge in der Datei RemoteDocument.txt im Ordner \\remote.address\Documents zu erfassen, fügen Sie **Dateiüberwachungsliste** die Pfadzeichenfolge \\remote.address\Documents hinzu.
- Trennen Sie die Angaben überwachter Pfade mit Semikolons (;) voneinander ab.
- Es werden nur exakte Übereinstimmungen unterstützt. Platzhalter werden nicht unterstützt.
- Pfadzeichenfolgen berücksichtigen die Groß-/Kleinschreibung nicht.

**Einschränkungen:**

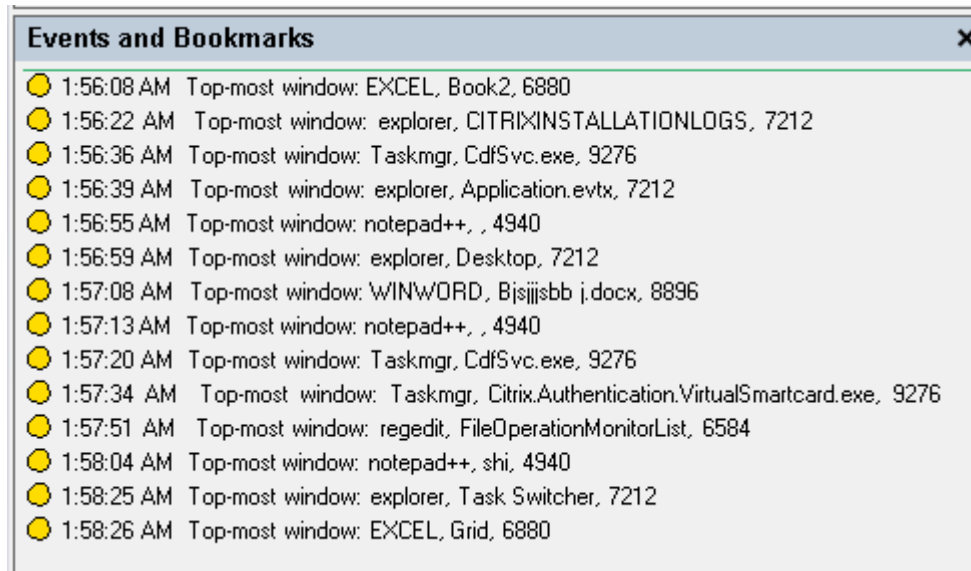
- Das Kopieren von Dateien oder Ordnern von einem überwachten lokalen Ordner in einen nicht überwachten lokalen Ordner kann nicht erfasst werden.
  - Wenn die Länge eines Datei- oder Ordnerpfads einschließlich Datei- oder Ordnernamen die maximale Länge von 260 Zeichen überschreitet, können Datei- oder Ordnervorgänge nicht erfasst werden.
  - Achten Sie auf die Datenbankgröße. Um zu verhindern, dass eine große Anzahl von Ereignissen erfasst wird, machen Sie regelmäßig ein Backup oder löschen die Ereignistabelle.
  - Wenn viele Ereignisse im Zeitintervall erfasst werden, wird der Player angezeigt und die Datenbank speichert nur ein Ereigniselement pro Ereignistyp, um eine Speichererweiterung zu vermeiden.
- **Webbrowsingaktivitäten protokollieren:** Protokolliert Benutzeraktivitäten in unterstützten Browsern und markiert den Browsernamen, die URL und den Seitentitel in der Aufzeichnung.



**Liste der unterstützten Browser:**

Browser	Version
Chrome	69 und höher
Internet Explorer	11
Firefox	61 und höher

- **Aktivitäten im obersten Fenster protokollieren:** Protokolliert die Aktivitäten im obersten Fenster und markiert den Prozessnamen, den Titel und die Prozessnummer in der Aufzeichnung.



- **Zwischenablageaktivitäten protokollieren:** Protokolliert das Kopieren von Text, Bildern und Dateien unter Verwendung der Zwischenablage. Beim Kopieren einer Datei werden Prozessname und Dateipfad protokolliert. Beim Kopieren eines Texts werden Prozessname und Titel protokolliert. Beim Kopieren eines Bilds wird der Prozessname protokolliert.

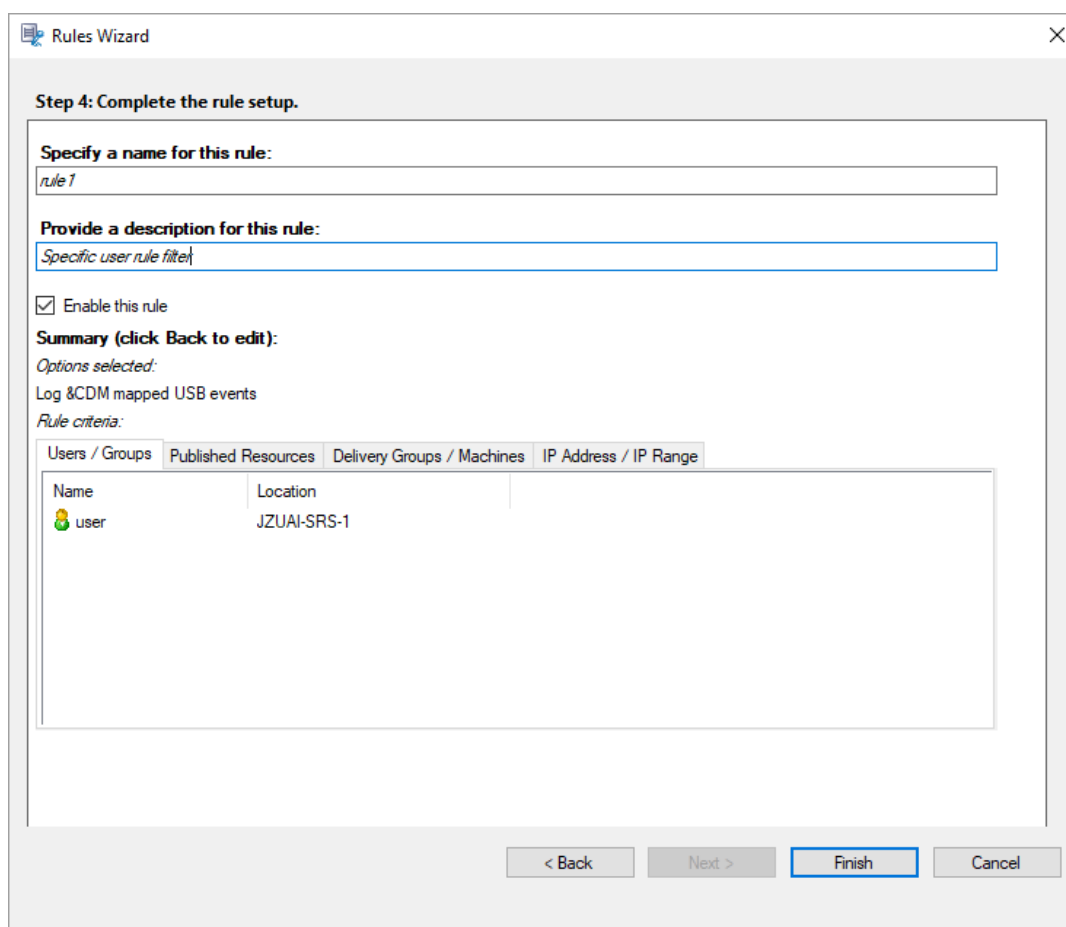
b) Wählen Sie die Regelkriterien aus, und bearbeiten Sie sie.

Wie beim Erstellen einer benutzerdefinierten Aufzeichnungsrichtlinie können Sie eine oder mehrere Regelkriterien wählen: **Benutzer oder Gruppen, Veröffentlichte Anwendungen oder Desktops, Bereitstellungsgruppen** oder **Maschinen sowie IP-Adresse oder IP-Bereich**. Weitere Informationen finden Sie unter **Erstellen benutzerdefinierter Aufzeichnungsrichtlinien**.

**Hinweis** Einige Sitzungen erfüllen ggf. kein Regelkriterium in einer Ereignisprotokollierungsrichtlinie. Für diese Sitzungen gilt die Ereignisprotokollierungsaktion der Fallbackregel, die immer **Nicht protokollieren** ist. Sie können die Fallbackregel nicht ändern oder löschen.

c) Folgen Sie den Anweisungen im Assistenten, um die Konfiguration abzuschließen.





## Kompatibilität mit Registrierungskonfigurationen

Wenn die Sitzungsaufzeichnung neu installiert oder aktualisiert wurde, ist standardmäßig keine aktive Ereignisprotokollierungsrichtlinie verfügbar. Jeder Sitzungsaufzeichnungsagent legt anhand der Registrierungswerte unter `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SessionEvents` fest, ob bestimmte Ereignisse protokolliert werden. Die folgende Tabelle enthält eine Beschreibung der einzelnen Registrierungswerte:

Registrierungswert	Beschreibung
EnableSessionEvents	<b>1:</b> Ereignisprotokollierung ist global aktiviert; <b>0:</b> Ereignisprotokollierung ist global deaktiviert (Standardwert)

Registrierungswert	Beschreibung
EnableCDMUSBDriveEvents	<b>1:</b> Das Anschließen von per CDM zugeordneten USB-Massenspeichergeräten wird protokolliert; <b>0:</b> Das Anschließen von per CDM zugeordneten USB-Massenspeichergeräten wird nicht protokolliert (Standardwert)
EnableGenericUSBDriveEvents	<b>1:</b> Das Anschließen von generischen umgeleiteten USB-Massenspeichergeräten wird protokolliert; <b>0:</b> Das Anschließen von generischen umgeleiteten USB-Massenspeichergeräten wird nicht protokolliert (Standardwert)
EnableAppLaunchEvents	<b>1:</b> Nur Anwendungsstarts werden protokolliert; <b>2:</b> Start und Ende von Anwendungen werden protokolliert; <b>0:</b> Start und Ende von Anwendungen werden nicht protokolliert (Standardwert)
AppMonitorList	Legt Zielanwendungen für die Überwachung fest. Standardmäßig ist keine Anwendung angegeben, d. h. es wird keine Anwendung standardmäßig erfasst.
EnableFileOperationMonitorEvents	<b>1:</b> Dateivorgänge werden protokolliert; <b>0:</b> Dateivorgänge werden nicht protokolliert (Standardwert).
FileOperationMonitorList	Gibt die Zielordner an, die überwacht werden sollen. Standardmäßig ist kein Ordner angegeben, d. h. es wird kein Dateivorgang standardmäßig erfasst.
EnableWebBrowsingActivities	<b>1:</b> Webbrowseraktivitäten werden protokolliert; <b>0:</b> Webbrowseraktivitäten werden nicht protokolliert (Standardwert).

---

Dies sind einige kompatible Szenarien:

- Die Sitzungsaufzeichnung 1912 wird neu installiert oder von einer früheren Version (vor 1811) ohne Unterstützung der Ereignisprotokollierung aktualisiert. Auf jedem Sitzungsaufzeichnungsagent gelten die Standardeinstellungen der zugehörigen Registrierungswerte. Da

standardmäßig keine Ereignisprotokollierungsrichtlinie aktiv ist, werden keine Ereignisse protokolliert.

- Wenn die Sitzungsaufzeichnung 1912 von einer früheren Version (vor 1811) aktualisiert wurde, bei der die Ereignisprotokollierung zwar unterstützt, aber vor dem Upgrade deaktiviert wurde, gelten auf jedem Sitzungsaufzeichnungsagent weiterhin die Standardeinstellungen der zugehörigen Registrierungswerte. Da standardmäßig keine Ereignisprotokollierungsrichtlinie aktiv ist, werden keine Ereignisse protokolliert.
- Wenn die Sitzungsaufzeichnung 1912 von einer früheren Version (vor 1811) aktualisiert wurde, bei der die Ereignisprotokollierung unterstützt und vor dem Upgrade teilweise oder vollständig aktiviert wurde, gelten auf jedem Sitzungsaufzeichnungsagent weiterhin dieselben Einstellungen der zugehörigen Registrierungswerte. Da standardmäßig keine Ereignisprotokollierungsrichtlinie aktiv ist, ändert sich das Protokollierungsverhalten nicht.
- Wenn für die Sitzungsaufzeichnung 1912 ein Upgrade von 1811 durchgeführt wird, bleiben die in der Richtlinienkonsole konfigurierten Ereignisprotokollierungsrichtlinien weiterhin aktiv.

#### **Achtung:**

Wenn Sie die systemdefinierte oder eine benutzerdefinierte Ereignisprotokollierungsrichtlinie in der Richtlinienkonsole für die Sitzungsaufzeichnung aktivieren, werden die entsprechenden Registrierungseinstellungen auf jedem Sitzungsaufzeichnungsagent ignoriert und können nicht länger für die Ereignisprotokollierung verwendet werden.

## **Aufzeichnungsanzeigerichtlinien**

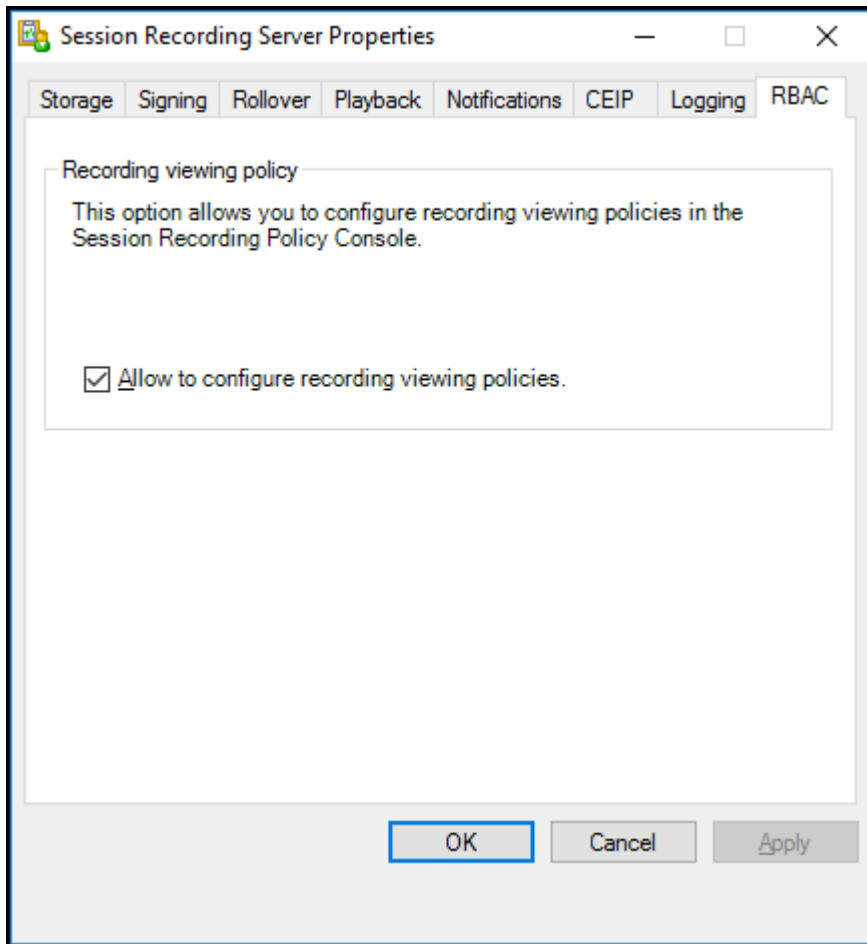
Der Sitzungsaufzeichnungsplayer unterstützt rollenbasierte Zugriffskontrolle. Sie können Aufzeichnungsanzeigerichtlinien in der Richtlinienkonsole für die Sitzungsaufzeichnung erstellen und jeder Richtlinie mehrere Regeln hinzufügen. Jede Regel legt fest, welcher Benutzer oder welche Benutzergruppe die Aufzeichnungen anzeigen kann, die von anderen von Ihnen angegebenen Benutzern, Benutzergruppen, veröffentlichten Anwendungen und Desktops und VDAs stammen.

### **Erstellen einer benutzerdefinierten Aufzeichnungsanzeigerichtlinie**

Bevor Sie Aufzeichnungsanzeigerichtlinien erstellen können, aktivieren Sie das Feature wie folgt:

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **RBAC**.

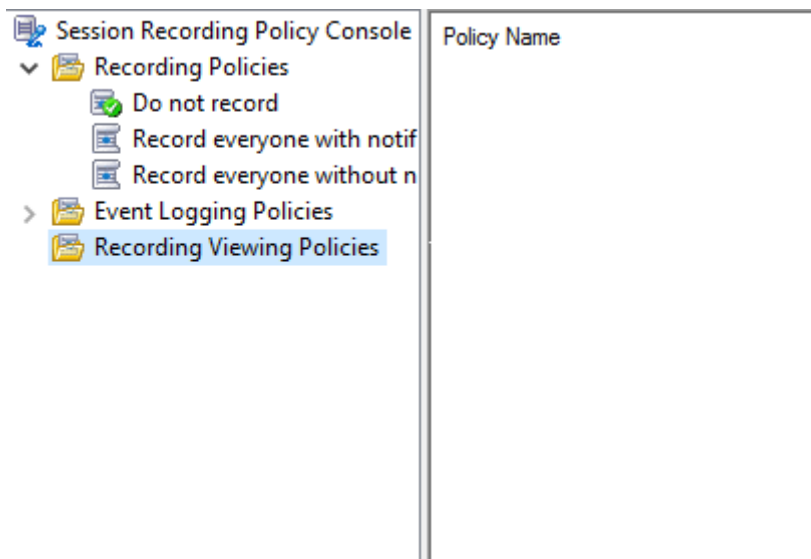
4. Aktivieren Sie das Kontrollkästchen **Konfiguration von Aufzeichnungsanzeigerichtlinien zulassen**.



Sie erstellen Sie eine benutzerdefinierte Aufzeichnungsanzeigerichtlinie:

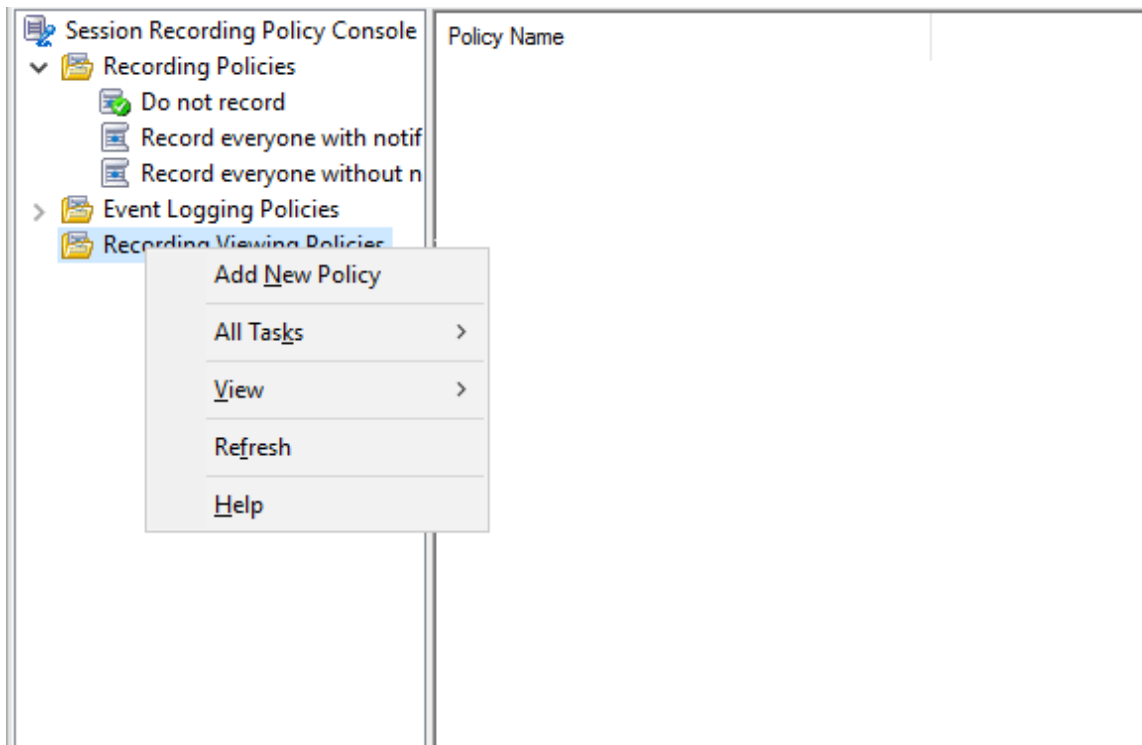
**Hinweis:** Abweichend von Aufzeichnungs- und Ereignisprotokollierungsrichtlinien ist eine Aufzeichnungsanzeigerichtlinie (einschließlich aller darin hinzugefügten Regeln) sofort beim Erstellen aktiv. Sie müssen sie nicht aktivieren.

1. Melden Sie sich bei dem Server, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist, als autorisierter Richtlinienadministrator an.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung. Standardmäßig gibt es keine Aufzeichnungsanzeigerichtlinie.

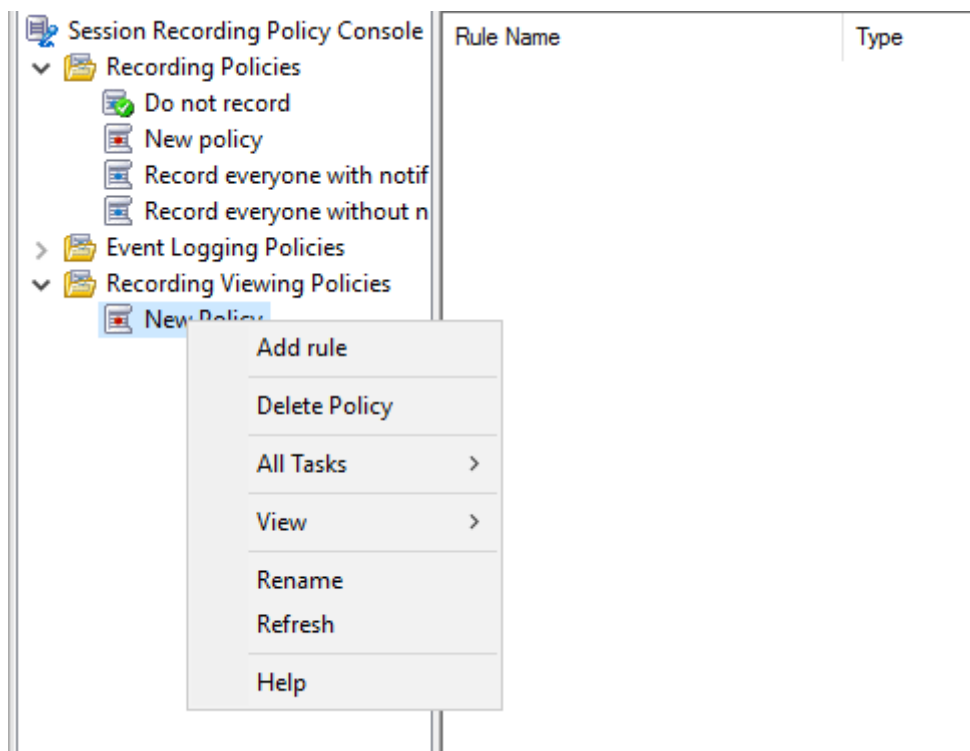


**Hinweis:** Das Menü **Aufzeichnungsanzeigerichtlinien** ist nur verfügbar, wenn Sie das Feature in den **Eigenschaften des Sitzungsaufzeichnungsservers** aktiviert haben.

3. Wählen Sie im linken Bereich die Option **Aufzeichnungsanzeigerichtlinien**. Wählen Sie in der Menüleiste die Option **Neue Richtlinie hinzufügen**, um eine Aufzeichnungsanzeigerichtlinie zu erstellen.



4. (Optional) Klicken Sie mit der rechten Maustaste auf die neue Richtlinie, um sie umzubenennen.



5. Klicken Sie mit der rechten Maustaste auf die neue Richtlinie und wählen Sie **Regel hinzufügen**.
  - a) Geben Sie an, welcher Benutzer oder welche Benutzergruppe die Aufzeichnungen anzeigen kann, die von anderen von Ihnen angegebenen Benutzern und Benutzergruppen erstellt werden.

The screenshot shows a 'Rules Wizard' dialog box. It has a title bar with a close button (X). The main area is divided into two sections. The first section is titled 'Selected user or user group who can view recordings' and contains a text input field and an 'Add...' button. The second section is titled 'Selected users and user groups whose recordings can be viewed' and contains a large empty list box. To the right of this list box are three buttons: 'Add...', 'Remove', and 'Remove All'. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

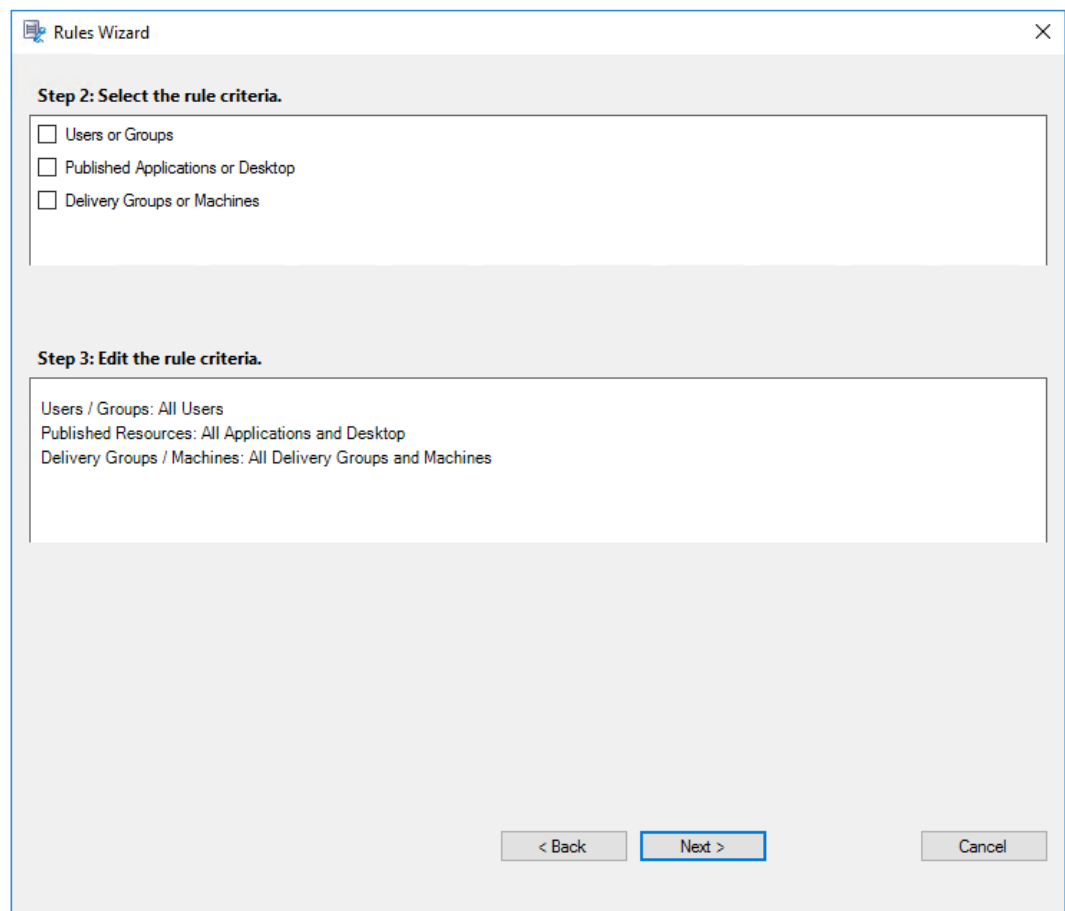
**Hinweis:**

In jeder Regel können Sie nur einen Benutzer oder eine Benutzergruppe als Leseberechtigten für Aufzeichnungen wählen. Wenn Sie mehrere Benutzer oder Benutzergruppen auswählen, wird nur Ihre letzte Auswahl wirksam und wird im Textfeld angezeigt.

Wenn Sie einen Leseberechtigten für Aufzeichnungen angeben, stellen Sie sicher, dass Sie dem Leseberechtigten die Rolle "Player" zugewiesen haben. Ein Benutzer ohne Berechtigung zur Wiedergabe von Sitzungsaufzeichnungen erhält eine Fehlermeldung bei dem Versuch, eine Sitzungsaufzeichnung wiederzugeben. Weitere Informationen finden Sie unter [Autorisieren von Benutzern](#).

b) Bearbeiten Sie die Regelkriterien, um anzugeben, wessen Aufzeichnungen der zuvor angegebene Leseberechtigte sehen kann:

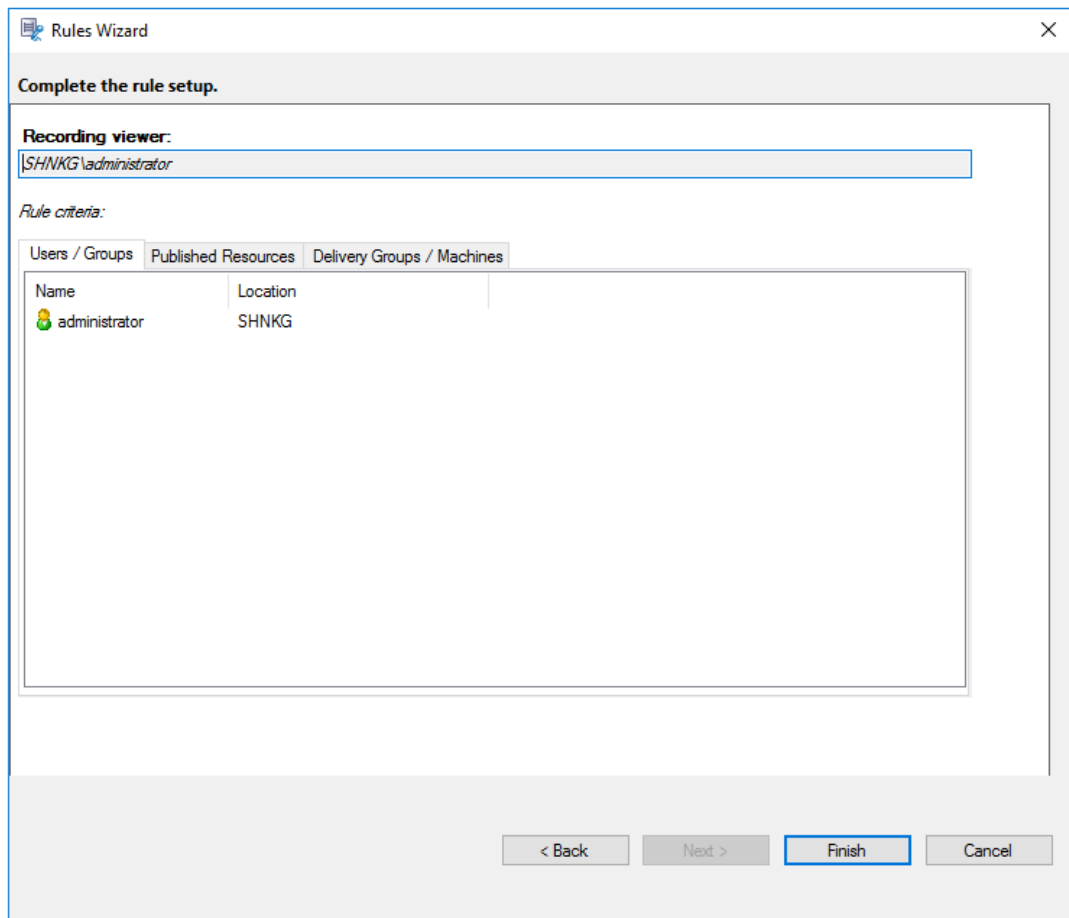
- **Benutzer oder Gruppen**
- **Veröffentlichte Anwendungen oder Desktops**
- **Bereitstellungsgruppen oder Maschinen**



**Hinweis:** Wenn Sie die Regelkriterien nicht angeben, sind für den Leseberechtigten keine Aufzeichnungen verfügbar.

- c) Folgen Sie den Anweisungen im Assistenten, um die Konfiguration abzuschließen.

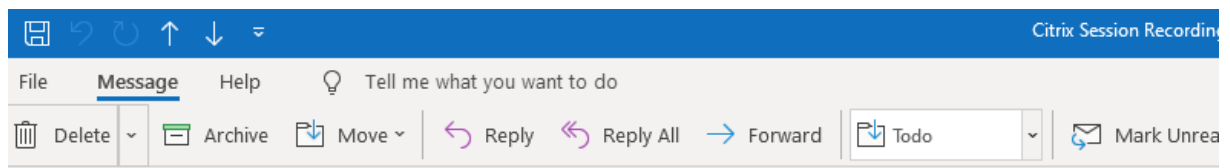





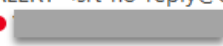
## E-Mail-Benachrichtigungsrichtlinien

Mit dieser Richtlinieneinstellung können Sie E-Mail-Benachrichtigungen an bestimmte Empfänger senden, sobald ein Sitzungsstart oder ein protokolliertes Ereignis erkannt werden. E-Mail-Benachrichtigungen sind für aufgezeichnete Sitzungen und protokollierte Ereignisse gemäß den aktiven Aufzeichnungs- und Ereignisprotokollierungsrichtlinien vorgesehen.

Das Beispiel einer E-Mail-Benachrichtigung sehen Sie im folgenden Screenshot:



Citrix Session Recording Alert: A TopMost was detected. VDAMachine: AWTSVDA-0002;

 SR-ALERT <srt-no-reply@outlook.com>  
To: 

[CAUTION - EXTERNAL EMAIL] DO NOT REPLY

Hi, @citrix.com

This email comes from Citrix Session Recording to notify you that a **TopMost** was detected:

#### Session Details

User Name	administrator
Domain Name	X0X7E
Start Time	11/9/2020 3:15:06 AM
Delivery Group	RdsDesktopAndAppGroup
Application	###Desktop,
VDA Machine	
Playback URL	<a data-bbox="901 974 1053 1008" href="https://&lt;img alt=" redacted="" url"=""></a> /webplayer/#/player/">https://  /webplayer/#/player/
Event Text	TopApp: regedit
Event Time	11/9/2020 3:17:51 AM

You can find the session recording video and more information [here](#).

*This is an automated email from Citrix Session Recording. Do not reply.*

#### Tipp:

Wenn Sie auf die Wiedergabe-URL klicken, wird die Wiedergabeseite der aufgezeichneten Sitzung im Webplayer geöffnet. Wenn Sie **hier** klicken, wird die Seite **Alle Aufzeichnungen** im Webplayer geöffnet.

Sie können die systemdefinierte E-Mail-Benachrichtigungsrichtlinie aktivieren oder eigene Richtlinien erstellen und aktivieren. Wenn Sie eine benutzerdefinierte Richtlinie erstellen, können Sie ihr mehrere Regeln hinzufügen. Jede Regel legt fest, welche Benutzer oder Gruppen, veröffentlichte Anwendungen oder Desktops, Bereitstellungsgruppen oder VDA-Maschinen und Citrix Workspace-App-Client-IP-Adressen eine E-Mail-Benachrichtigung auslösen können, wenn Sitzungsstarts erkannt werden.

Es kann jeweils nur eine E-Mail-Benachrichtigungsrichtlinie aktiv sein.

### Systemdefinierte E-Mail-Benachrichtigungsrichtlinie

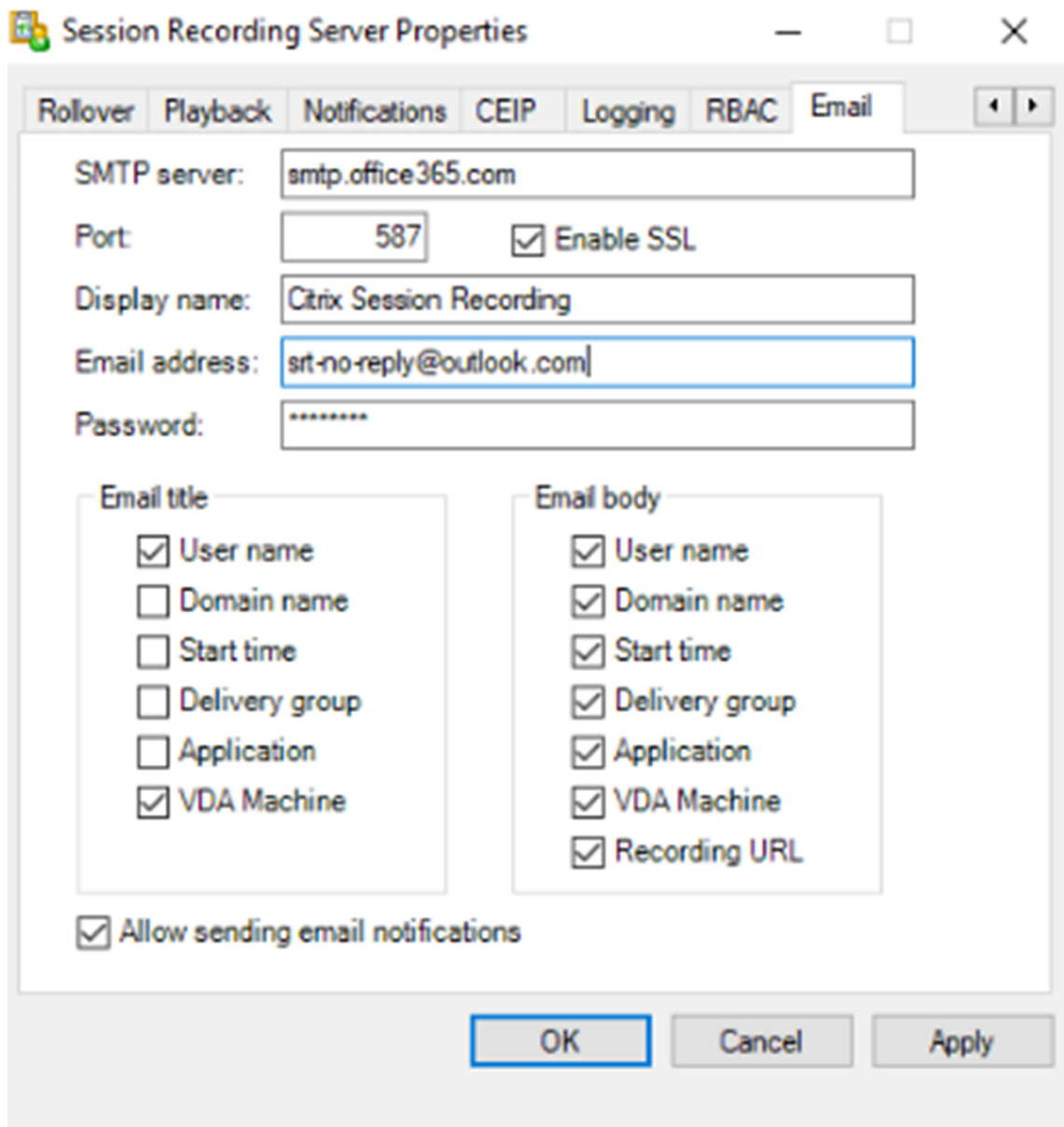
Die Sitzungsaufzeichnung bietet eine systemdefinierte E-Mail-Benachrichtigungsrichtlinie:

- **Keine Benachrichtigungen.** Die Standardrichtlinie. Wenn Sie keine andere Richtlinie angeben, werden keine E-Mail-Benachrichtigungen gesendet.

### Erstellen einer benutzerdefinierten E-Mail-Benachrichtigungsrichtlinie

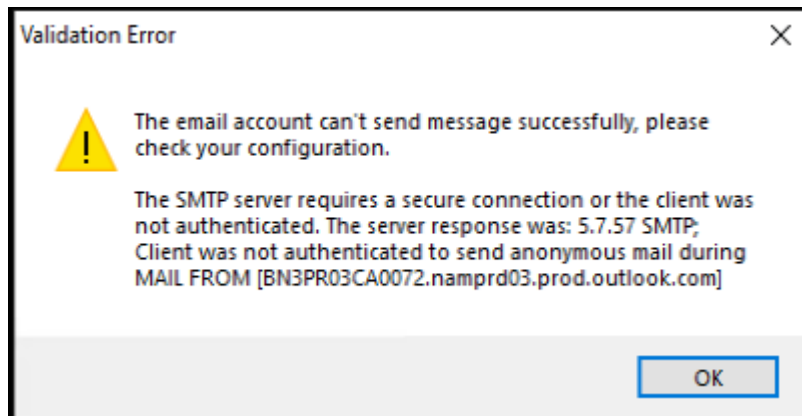
Gehen Sie folgendermaßen vor, um eine benutzerdefinierte E-Mail-Benachrichtigungsrichtlinie zu erstellen:

1. Konfigurieren Sie unter Sitzungsaufzeichnungsserver - Eigenschaften die Einstellungen für ausgehende E-Mails.



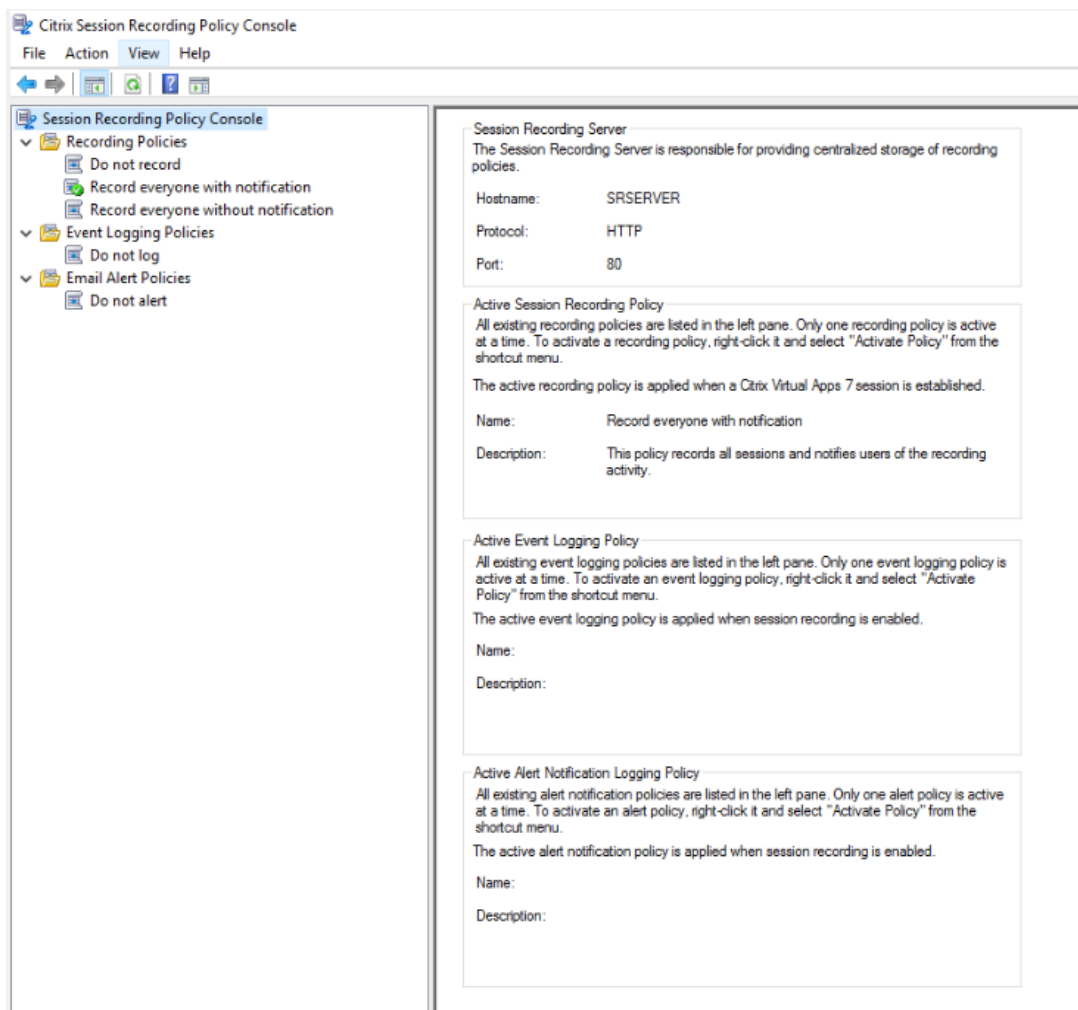
**Hinweis:**

Wenn Sie mehr als zwei Optionen unter **E-Mail-Titel** auswählen, wird die Warnung angezeigt, dass der E-Mail-Betreff möglicherweise zu lang ist. Nachdem Sie **Senden von E-Mail-Benachrichtigungen zulassen** ausgewählt und auf **Anwenden** geklickt haben, sendet die Sitzungsaufzeichnung eine E-Mail, um Ihre E-Mail-Einstellungen zu überprüfen. Ist eine Einstellung (z. B. Kennwort oder Port) falsch, gibt die Sitzungsaufzeichnung eine Fehlermeldung mit den Fehlerdetails zurück.



Die E-Mail-Einstellungen benötigen etwa fünf Minuten, um wirksam zu werden. Um die E-Mail-Einstellungen sofort in Kraft zu setzen oder das Problem E-Mail-Versands gemäß Einstellungen zu beheben, starten Sie den Speichermanagerdienst (CitrixSsRecStorageManager) neu. Starten Sie den Speichermanagerdienst auch dann neu, wenn Sie ein Upgrade von Version 2006 und früher auf das aktuelle Release ausführen.

2. Erstellen Sie eine benutzerdefinierte E-Mail-Benachrichtigungsrichtlinie in der Richtlinienkonsole für die Sitzungsaufzeichnung.
  - a) Melden Sie sich bei dem Server, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist, als autorisierter Richtlinienadministrator an.
  - b) Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung. Standardmäßig gibt es keine aktive E-Mail-Benachrichtigungsrichtlinie.

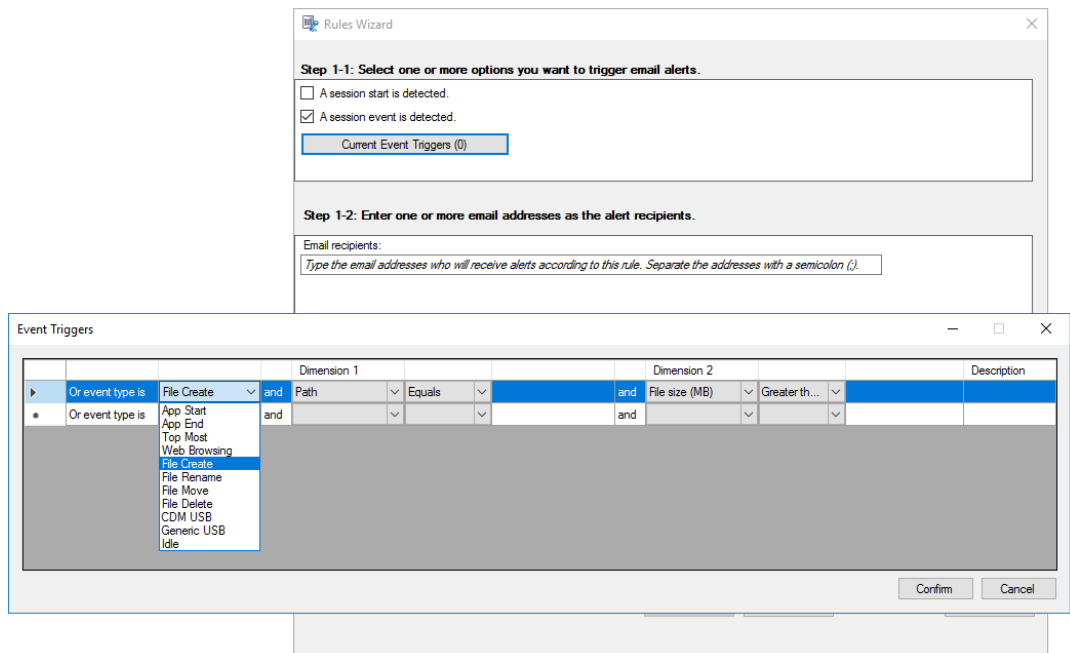


- c) Wählen Sie im linken Bereich die Option **Benachrichtigungsrichtlinien**. Wählen Sie in der Menüleiste **Neue Richtlinie hinzufügen**, um eine Benachrichtigungsrichtlinie zu erstellen.
- d) (Optional) Klicken Sie mit der rechten Maustaste auf die neue E-Mail-Benachrichtigungsrichtlinie, um sie umbenennen.
- e) Klicken Sie mit der rechten Maustaste auf die neue E-Mail-Benachrichtigungsrichtlinie und wählen Sie **Regel hinzufügen**.
  - 5a. Wählen Sie **Ein Sitzungsstart wurde erkannt** oder **Ein Sitzungsereignis wurde erkannt**. Fügen Sie die E-Mail-Adressen der Benachrichtigungsempfänger hinzu.

The screenshot shows a 'Rules Wizard' dialog box with two steps. Step 1-1 is titled 'Step 1-1: Select one or more options you want to trigger email alerts.' and contains two checkboxes: 'A session start is detected.' (unchecked) and 'A session event is detected.' (checked). Below the checkboxes is a button labeled 'Current Event Triggers (0)'. Step 1-2 is titled 'Step 1-2: Enter one or more email addresses as the alert recipients.' and contains a text input field with the placeholder text 'Type the email addresses who will receive alerts according to this rule. Separate the addresses with a semicolon (;)'. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

Bei Auswahl von **Ein Sitzungsereignis wurde erkannt** klicken Sie auf **Aktuelle Ereignisauslöser**, um festzulegen, welche protokollierten Ereignisse eine E-Mail-Benachrichtigung auslösen. Wählen Sie Ereignistypen aus der Dropdownliste und legen Sie Ereignisregeln über die beiden Felder fest, die mit dem logischen Operatoren AND kombiniert werden. Sie können bis zu sieben Ereignisregeln einrichten. Wenn Sie einen Ereignistyp auswählen, ohne die Felder zu definieren, werden E-Mail-Benachrichtigungen gesendet, wenn Ereignisse dieses Typs auftreten. Sie können die Ereignisauslöser auch in der Spalte **Beschreibung** definieren oder die Spalte leer lassen. Die von Ihnen definierte Beschreibung eines Ereignisauslösers wird in der E-Mail-Benachrichtigung angegeben, wenn Ereignisse dieses Typs protokolliert werden. Klicken Sie zum Abschluss auf **Bestätigen**.

**Hinweis:** Sie müssen die Ereignistypen auswählen, die die aktive Ereignisprotokollierungsrichtlinie protokolliert.



Eine vollständige Liste der unterstützten Ereignistypen finden Sie in der folgenden Tabelle.

Ereignistyp	Feld	Option
App-Start		App-Name
		Vollständige Befehlszeile
App-Ende		App-Name
Oberstes Fenster		App-Name
		Fenstertitel
Webbrowsing		URL
		Registerkartentitel
		Browsername
Erstellen von Datei		Pfad
		Dateigröße (MB)

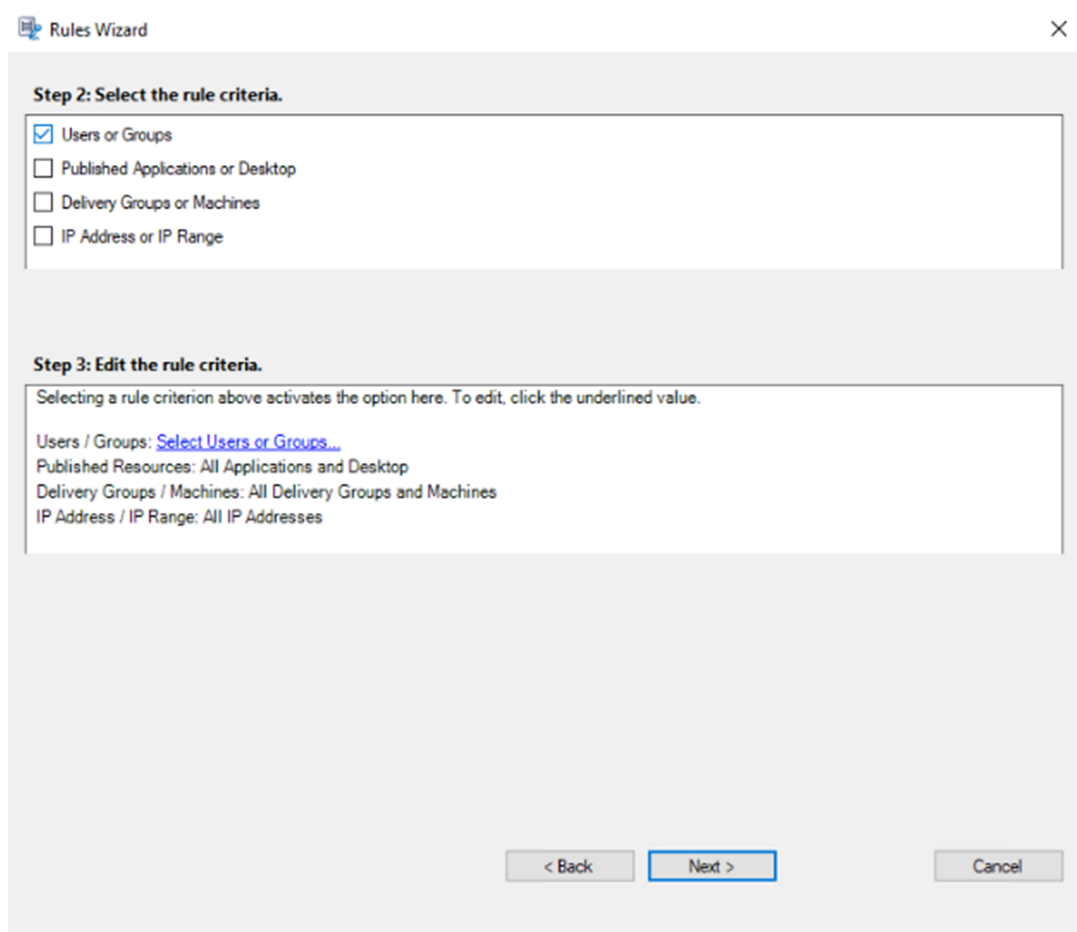
Ereignistyp	Feld	Option
Umbenennen von Datei		Pfad
		Name
Verschieben von Datei		Quellpfad
		Zielpfad
		Dateigröße (MB)
Löschen von Datei		Pfad
		Dateigröße (MB)
CDM USB		Laufwerksbuchstabe
		Gerätename
Leerlauf		Leerlaufzeit (Std.)

5b. Fügen Sie die E-Mail-Adressen der Benachrichtigungsempfänger hinzu.

5c. Klicken Sie auf **Weiter**, um die Regelkriterien auszuwählen und zu bearbeiten.

Wie beim Erstellen einer benutzerdefinierten Aufzeichnungsrichtlinie können Sie eine oder mehrere Regelkriterien wählen: **Benutzer oder Gruppen, Veröffentlichte Anwendungen oder Desktops, Bereitstellungsgruppen** oder **Maschinen sowie IP-Adresse oder IP-Bereich**. Weitere Informationen finden Sie unter [Erstellen benutzerdefinierter Aufzeichnungsrichtlinien](#).



**Hinweis:**

Wenn eine Sitzung oder ein Ereignis mehr als eine Regel in einer E-Mail-Benachrichtigungsrichtlinie erfüllt, wird die älteste Regel wirksam.

5d. Folgen Sie den Anweisungen im Assistenten, um die Konfiguration abzuschließen.

f) Aktivieren Sie die neue E-Mail-Benachrichtigungsrichtlinie.

3. Bearbeiten Sie die Registrierung für den Zugriff Webplayerzugriff.

Damit die Wiedergabe-URLs in den E-Mail-Benachrichtigungen funktionieren, navigieren Sie zum Registrierungsschlüssel unter `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server` und führen Sie die folgenden Schritte aus:

- Legen Sie den Wert von **LinkHost** auf die URL der Domäne fest, die Sie für den Webplayerzugriff verwenden. Für einen Webplayer in `https://example.com/webplayer/#/player/` legen Sie beispielsweise den LinkHost-Wert auf `https://example.com` fest.
- Fügen Sie einen neuen **EmailThreshold** hinzu und legen Sie den Wert auf eine

Zahl zwischen 1 und 100 fest. Der Wert bestimmt die maximale Anzahl von E-Mail-Benachrichtigungen, die ein Konto in einer Sekunde sendet. Diese Einstellung hilft, den E-Mail-Versand zu drosseln und die CPU-Auslastung zu reduzieren. Wird kein Wert spezifiziert oder ein ungültiger Wert gewählt, wird der Wert auf 25 gesetzt.

#### Hinweis:

- Der E-Mail-Server kann ein Konto für den E-Mail-Versand u. U. als Spam-Bot interpretieren und den E-Mail-Versand unterbinden. Damit ein Konto E-Mail senden kann, fordern E-Mail-Clients wie Outlook evtl. eine Bestätigung an, dass das Konto von einem menschlichen Benutzer verwendet wird.
- Es gibt eine Begrenzung für das Senden von E-Mails innerhalb eines bestimmten Zeitraums. Wenn beispielsweise das Tageslimit erreicht ist, ist kein E-Mail-Versand bis zum Beginn des nächsten Tages möglich. Stellen Sie in diesem Fall sicher, dass das Limit größer ist als die Anzahl der Sitzungen, die innerhalb des Zeitraums aufgezeichnet werden.

### Aktivieren einer Richtlinie

1. Melden Sie sich als Administrator bei der Maschine an, auf der Sie die Richtlinienkonsole für die Sitzungsaufzeichnung installiert haben.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld **Mit Sitzungsaufzeichnungsserver verbinden** angezeigt wird, stellen Sie sicher, dass der Name des Sitzungsaufzeichnungsservers, das Protokoll und der Port richtig sind. Klicken Sie auf **OK**.
4. Erweitern Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung je nach Bedarf **Aufzeichnungsrichtlinien** oder **Ereignisprotokollierungsrichtlinien**.
5. Wählen Sie die zu aktivierende Richtlinie.
6. Wählen Sie im Menü **Richtlinie aktivieren**.

### Ändern von Richtlinien

1. Melden Sie sich als Administrator bei der Maschine an, auf der Sie die Richtlinienkonsole für die Sitzungsaufzeichnung installiert haben.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld **Mit Sitzungsaufzeichnungsserver verbinden** angezeigt wird, stellen Sie sicher, dass der Name des Sitzungsaufzeichnungsservers, das Protokoll und der Port richtig sind. Klicken Sie auf **OK**.
4. Erweitern Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung je nach Bedarf **Aufzeichnungsrichtlinien** oder **Ereignisprotokollierungsrichtlinien**.

5. Wählen Sie die Richtlinie aus, die Sie ändern möchten. Die Regeln für die Richtlinie werden im rechten Bereich angezeigt.
6. Hinzufügen, Ändern und Löschen von Regeln:
  - Wählen Sie in der Menüleiste **Neue Regel hinzufügen**. Wenn die Richtlinie aktiv ist, werden Sie in einem Popupfenster zum Bestätigen der Aktion aufgefordert. Erstellen Sie mit dem Assistenten für **Regeln** eine Regel.
  - Markieren Sie die Regel, die Sie ändern möchten, klicken Sie mit der rechten Maustaste und wählen Sie **Eigenschaften**. Ändern Sie die Regel mit dem Assistenten für **Regeln**.
  - Markieren Sie die Regel, die Sie löschen möchten, klicken Sie mit der rechten Maustaste und wählen Sie **Regel löschen**.

## Löschen von Richtlinien

### Hinweis:

Eine systemdefinierte oder aktive Richtlinie kann nicht gelöscht werden.

1. Melden Sie sich als Administrator bei der Maschine an, auf der Sie die Richtlinienkonsole für die Sitzungsaufzeichnung installiert haben.
2. Starten Sie die Richtlinienkonsole für die Sitzungsaufzeichnung.
3. Wenn das Dialogfeld **Mit Sitzungsaufzeichnungsserver verbinden** angezeigt wird, stellen Sie sicher, dass der Name des Sitzungsaufzeichnungsservers, das Protokoll und der Port richtig sind. Klicken Sie auf **OK**.
4. Erweitern Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung je nach Bedarf **Aufzeichnungsrichtlinien** oder **Ereignisprotokollierungsrichtlinien**.
5. Wählen Sie im linken Bereich die Richtlinie aus, die Sie löschen möchten. Wenn die Richtlinie aktiv ist, müssen Sie eine andere aktivieren.
6. Wählen Sie in Menüleiste **Richtlinie löschen**.
7. Klicken Sie auf **Ja**, um die Aktion zu bestätigen.

## Grundlegendes zu Rollover

Wenn Sie eine Richtlinie aktivieren, bleibt die zuvor aktive Richtlinie so lange in Kraft, bis die aufgezeichnete Sitzung endet oder ein Rollover der Sitzungsaufzeichnungsdatei erfolgt. Ein Dateirolover tritt auf, wenn die maximale Größe erreicht wird. Weitere Informationen zur maximalen Dateigröße für Aufzeichnungen finden Sie unter [Angaben der Dateigröße für Aufzeichnungen](#).

In der folgenden Tabelle werden die Vorgänge beschrieben, die beim Anwenden einer neuen Aufzeichnungsrichtlinie auftreten, während eine Sitzung aufgezeichnet wird und ein Rollover erfolgt:

Vorherige Aufzeichnungsrichtlinie	Neue Aufzeichnungsrichtlinie	Aufzeichnungsrichtlinie nach Rollover
Nicht aufzeichnen	Jede andere Richtlinie	Keine Änderung. Die neue Richtlinie wird nur gültig, wenn sich der Benutzer an einer neuen Sitzung anmeldet. Aufzeichnung wird gestoppt.
Ohne Benachrichtigung aufzeichnen	Nicht aufzeichnen	Aufzeichnung wird gestoppt.
Ohne Benachrichtigung aufzeichnen	Mit Benachrichtigung aufzeichnen	Aufzeichnung wird fortgesetzt, und eine Benachrichtigung wird angezeigt.
Mit Benachrichtigung aufzeichnen	Nicht aufzeichnen	Aufzeichnung wird gestoppt.
Mit Benachrichtigung aufzeichnen	Ohne Benachrichtigung aufzeichnen	Aufzeichnung wird fortgesetzt. Bei der nächsten Anmeldung des Benutzers wird keine Meldung angezeigt.

## Speicherort für Aufzeichnungen festlegen

January 15, 2024

Geben Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** das Verzeichnis zum Speichern von Aufzeichnungen und Wiederherstellen archivierter Aufzeichnungen für die Wiedergabe an.

Sie können Aufzeichnungen auf einem lokalen Datenträger, einem SAN-Volume und an einem durch UNC-Netzwerkpfad angegebenen Speicherort speichern. Ab Version 2103 können Sie Aufzeichnungen in Azure-Dateifreigaben speichern. Weitere Informationen finden Sie unter [Konfigurieren einer Azure-Dateifreigabe zum Speichern von Aufzeichnungen](#) weiter unten in diesem Artikel.

### Hinweis:

- Das Speichern von Daten in einem NAS mit dateibasiertem Protokoll wie SMB und NFS kann Auswirkungen auf Leistung und Sicherheit haben. Verwenden Sie die neueste Version des Protokolls, um Auswirkungen auf die Sicherheit zu vermeiden, und führen Sie Skalierungstests durch, um eine zufriedenstellende Leistung sicherzustellen.
- Verwenden Sie den Befehl `ICLDB`, um Dateien zu archivieren oder gelöschte Dateien wiederherzustellen.

## **Festlegen eines oder mehrerer Ordner zum Speichern von Aufzeichnungen und eines Ordners zum Wiederherstellen archivierter Aufzeichnungen**

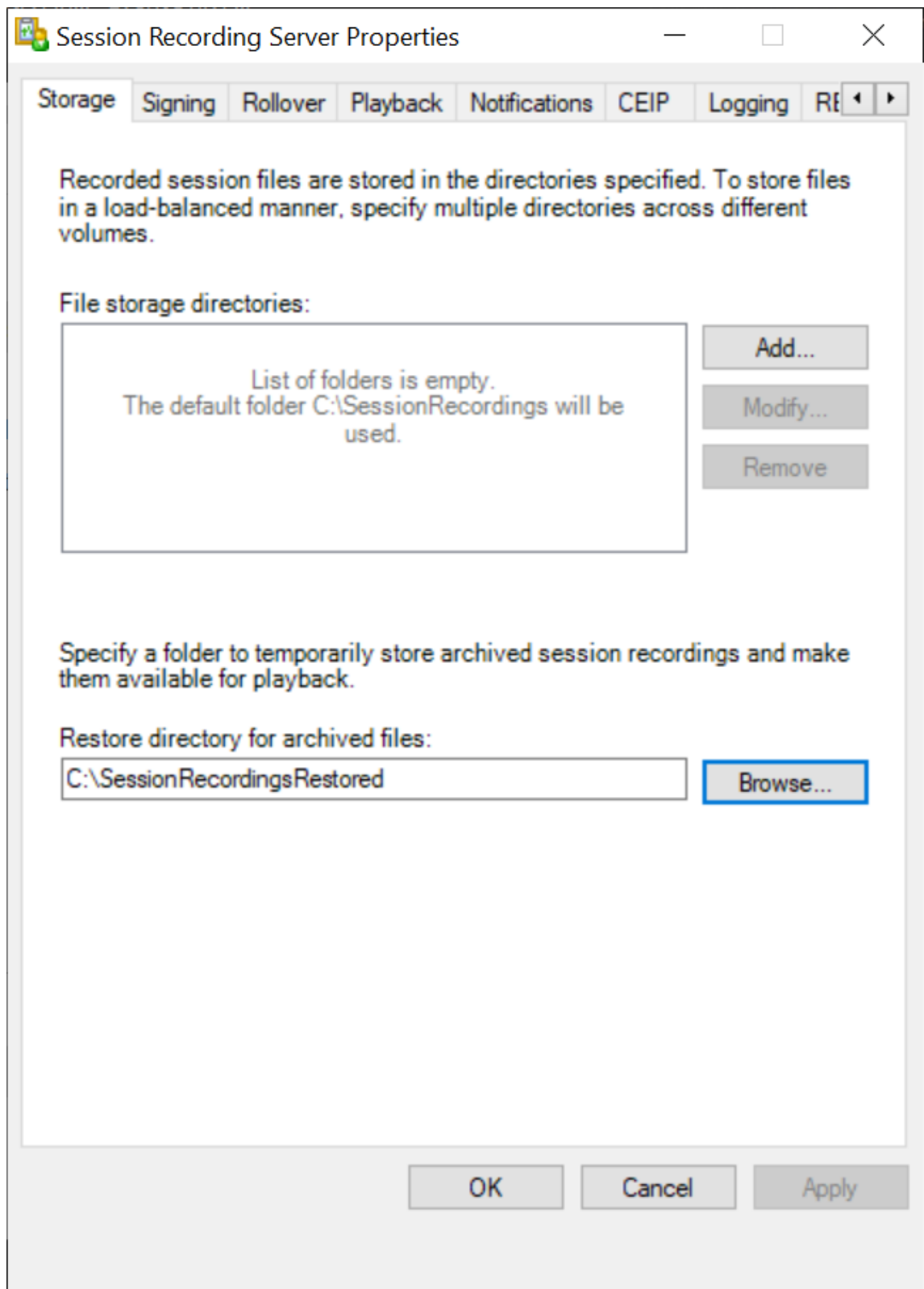
1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Speicher**.
4. Verwenden Sie die Liste **Verzeichnisse für Dateispeicherung**, um die Ordner zu verwalten, in denen die Aufzeichnungen gespeichert werden.

Nach der Auswahl der Ordner erhalten die Dienste der Sitzungsaufzeichnung Vollzugriff auf diese Ordner.

In der Standardeinstellung werden Aufzeichnungen im Ordner **<Laufwerk>:SessionRecordings** der Maschine mit dem Sitzungsaufzeichnungsserver gespeichert. Sie können den Ordner ändern, in dem Sie Aufzeichnungen speichern, zum Lastausgleich auf mehreren Volumes weitere Ordner hinzufügen oder freien Speicherplatz zu nutzen. Mehrere Ordner in der Liste geben an, dass Aufzeichnungen per Lastausgleich auf mehrere Ordner verteilt werden. Der Lastausgleich durchläuft alle Ordner.

5. Geben Sie im Feld **Wiederherstellungsverzeichnis für archivierte Dateien** den Ordner zum Wiederherstellen archivierter Aufzeichnungen an.

In der Standardeinstellung werden Aufzeichnungen im Ordner **<Laufwerk>:SessionRecordingsRestore** der Maschine mit dem Sitzungsaufzeichnungsserver gespeichert. Sie können den Ordner ändern.



## Konfigurieren einer Azure-Dateifreigabe zum Speichern von Aufzeichnungen

Führen Sie folgende Schritte aus, um eine Azure-Dateifreigabe zum Speichern von Aufzeichnungen zu erstellen:

1. Erstellen Sie im [Azure-Portal](#) zuerst ein Speicherkonto und dann eine Azure-Dateifreigabe.

Eine Kurzanleitung finden Sie unter [Erstellen und Verwalten von Azure-Dateifreigaben mit dem Azure-Portal](#). Die folgende Tabelle enthält empfohlene Konfigurationen.

Größe der Aufzeichnungsdatei (MB/Stunde)	Anzahl der Sitzungen	Typ der Dateifreigabe	Kontingent der Dateifreigabe (TB)	Sitzungsaufzeichnung –Serveranzahl	Sitzungsaufzeichnung –Servergröße
< 6,37	< 1000	HDD Standard (StorageV2)	2	1	Standard D4as_v4
< 6,37	1000–2000	SSD Premium	3	1	Standard D4as_v4
< 6,37	2000–3000	SSD Premium	5	1	Standard D4as_v4
< 6,37	3000–4000	SSD Premium	6	1	Standard D4as_v4
ca. 10	< 1000	HDD Standard (StorageV2)	3	1	Standard D4as_v4
ca. 10	1000–2500	SSD Premium	6	1	Standard D4as_v4
ca. 10	2500–4000	SSD Premium	10	2	Standard D4as_v4

Das Kontingent für Dateifreigaben wird basierend auf acht Stunden pro Tag, 23 Arbeitstagen pro Monat und einer einmonatigen Aufbewahrungsdauer für jede Aufzeichnungsdatei berechnet.

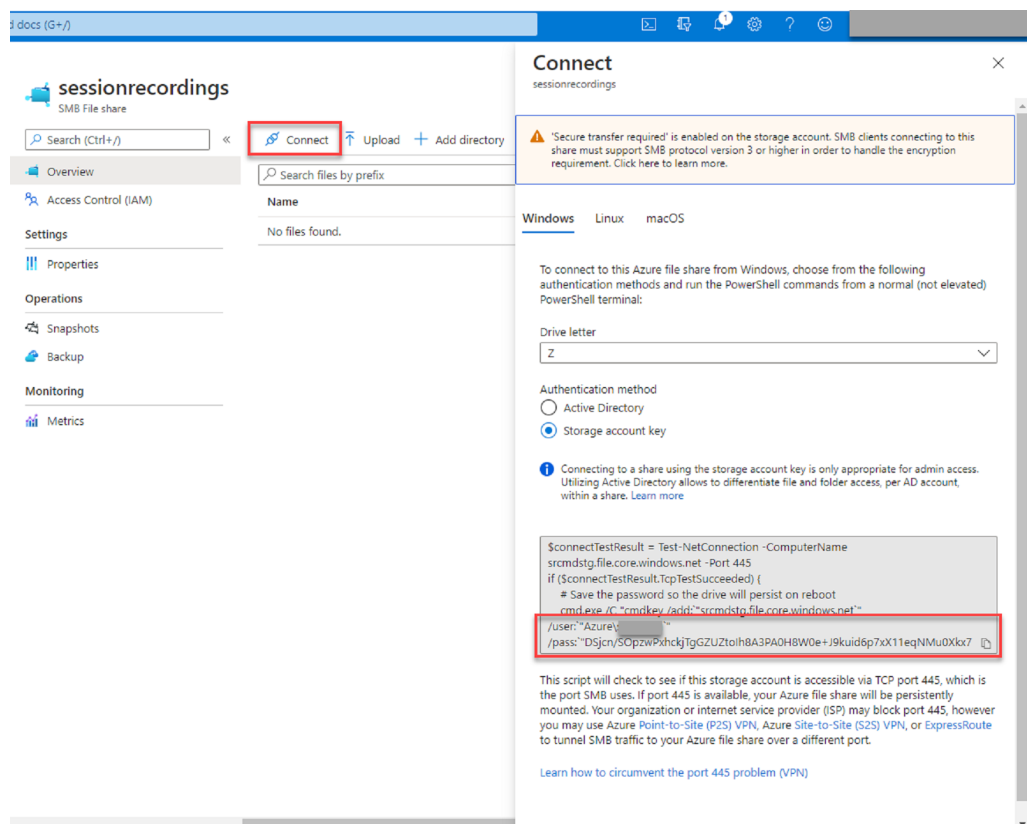
2. Fügen Sie dem Host, auf dem Sie den Sitzungsaufzeichnungsserver installiert haben, die Anmeldeinformationen der Azure-Dateifreigabe hinzu.
  - a) Starten Sie eine Eingabeaufforderung als Administrator und ändern Sie das Laufwerk in den Ordner **<Installationspfad des Sitzungsaufzeichnungsservers>\Bin**.  
Standardmäßig wird der Sitzungsaufzeichnungsserver in `C:\Program Files\Citrix\SessionRecording\Server` installiert.
  - b) Führen Sie den Befehl **SsRecUtils.exe -AddAzureFiles <storageAccountName> <fileShareName> <accesskey>** aus.

Hierbei gilt:

- **<storageaccountname>** ist der Name Ihres Speicherkontos in Azure.
- **<filesharename>** ist der Name der Dateifreigabe, die in Ihrem Speicherkonto enthalten ist.
- **<accesskey>** ist Ihr Speicherkontoschlüssel, der für den Zugriff auf die Dateifreigabe verwendet werden kann.

Sie haben zwei Möglichkeiten, Ihren Speicherkontoschlüssel abzufragen:

- Sie finden den Speicherkontoschlüssel in der angezeigten Verbindungszeichenfolge, wenn Sie auf der Dateifreigabeseite auf die Schaltfläche **Verbinden** klicken.



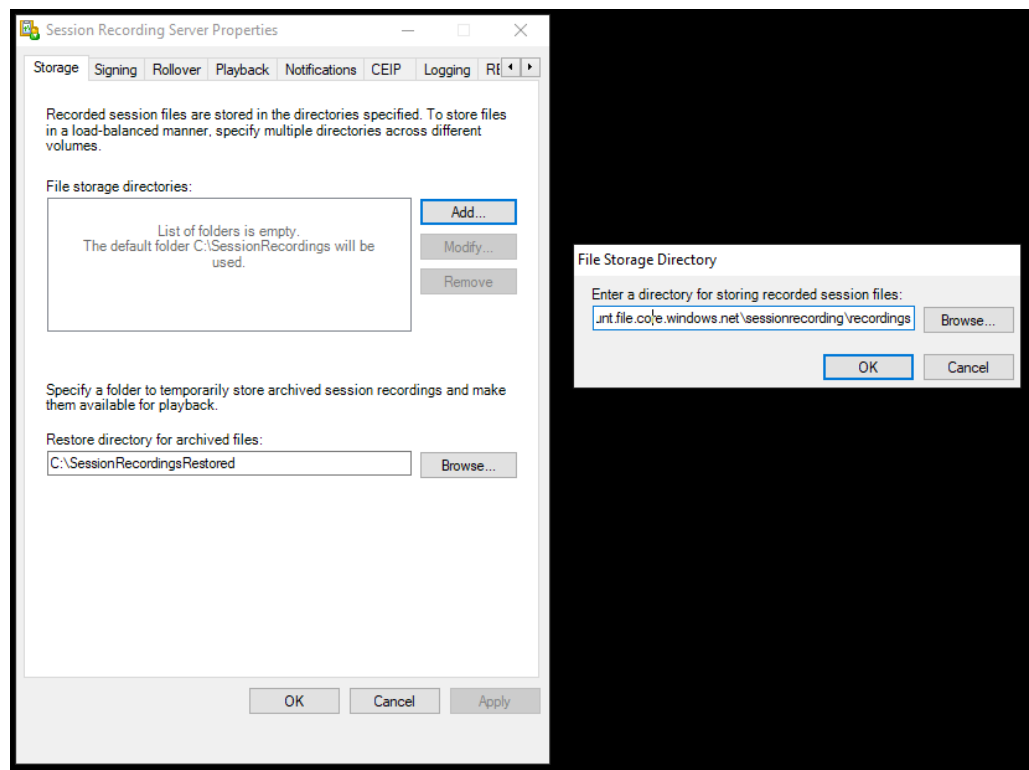
- Sie können den Speicherkontoschlüssel auch abrufen, indem Sie links in der Speicherkontoseite auf **Zugriffsschlüssel** klicken.



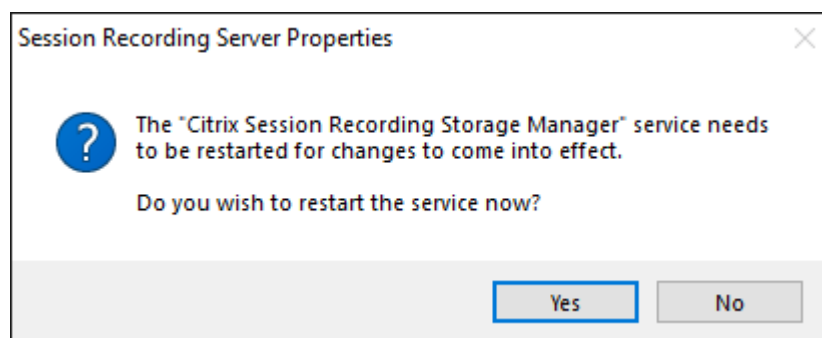
The screenshot shows the Microsoft Azure portal interface. At the top, there is a blue header with the Microsoft Azure logo and a search bar. Below the header, the breadcrumb navigation shows 'Home > srcmd > [Storage account]'. The main heading is 'Access keys'. On the left, there is a navigation pane with various options, and 'Access keys' is highlighted with a red box. The main content area contains instructions on using access keys and details for two keys, 'key1' and 'key2', including their keys and connection strings.

- c) Stellen Sie die Azure-Dateifreigabe auf dem Host bereit, auf dem Sie den Sitzungsaufzeichnungsserver installiert haben.
- Öffnen Sie **Sitzungsaufzeichnungsserver - Eigenschaften**.
  - Klicken Sie auf der Registerkarte **Speicher** auf **Hinzufügen**.
  - Geben Sie den UNC-Pfad im Format `\\<storageaccountname>.file.core.windows.net\\<filesshare>` ein.

Legen Sie unter der Dateifreigabe einen Unterordner fest, in dem Ihre Aufzeichnungsdateien gespeichert werden sollen. Der Sitzungsaufzeichnungsserver erstellt dann automatisch den Unterordner für Sie.



- iv. Klicken Sie im Dialogfeld **Verzeichnis für Dateispeicherung** auf **OK**.
- v. Klicken Sie im Fenster **Sitzungsaufzeichnungsserver - Eigenschaften** auf **Übernehmen**.
- vi. Klicken Sie auf **OK**, nachdem **Übernehmen** abgeblendet ist.
- vii. Klicken Sie auf **Ja**, wenn Sie aufgefordert werden, den Speichermanager der Sitzungsaufzeichnung neu zu starten.



## Angeben der Dateigröße für Aufzeichnungen

January 15, 2024

Wenn die Größe der Aufzeichnungsdateien zunimmt, kann ihr Download länger dauern, und die Reaktionszeit kann sich verlangsamen, wenn Sie mit dem Schieberegler durch die Wiedergabe navigieren. Sie können die Dateigröße durch Festlegen eines Schwellenwerts für eine Datei steuern. Wenn die Aufzeichnung dieses Limit erreicht, schließt die Sitzungsaufzeichnung die Datei und erstellt eine weitere Datei, um die Aufzeichnung fortzusetzen. Dies wird Rollover genannt.

Sie können zwei Schwellenwerte für ein Rollover angeben:

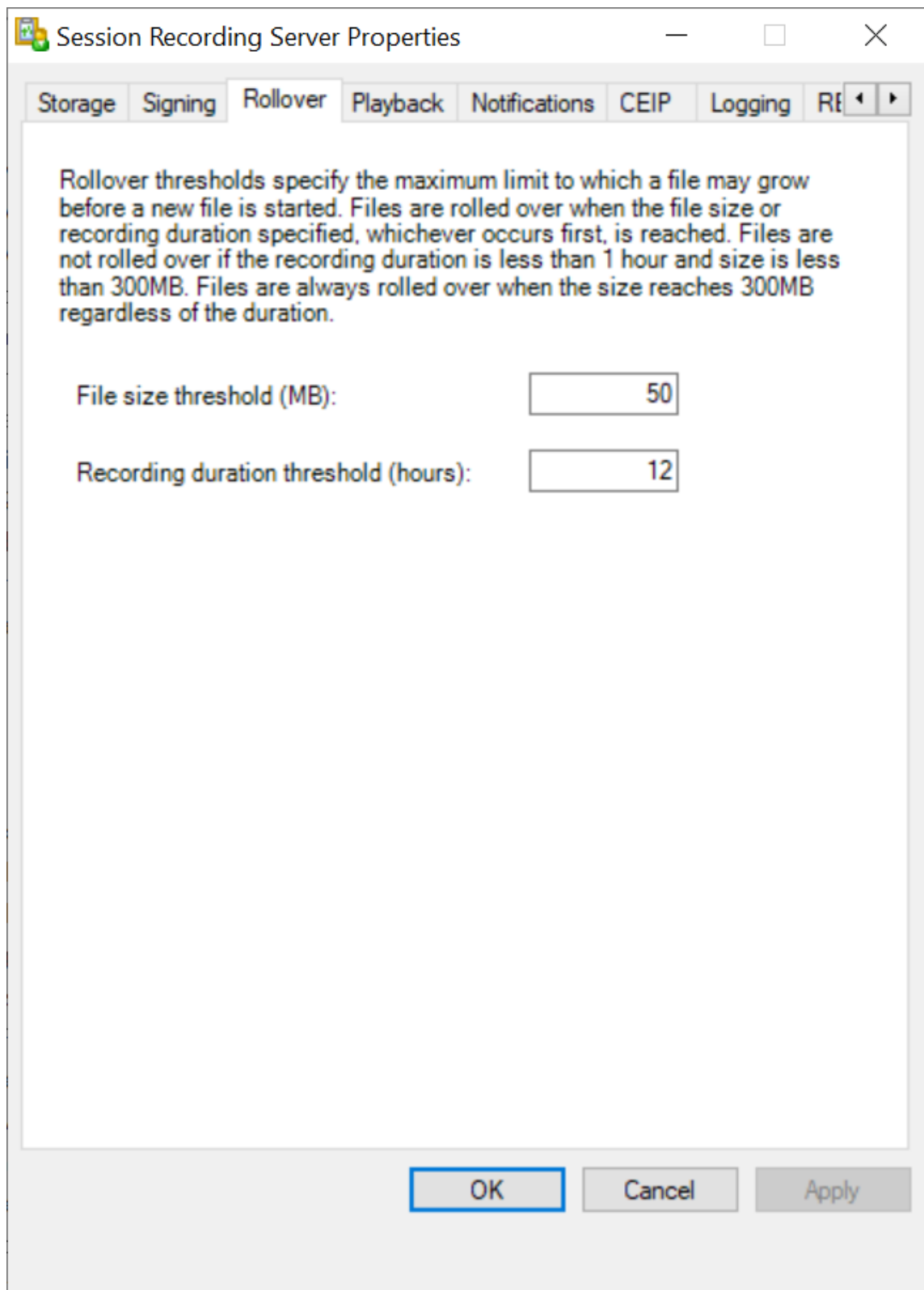
- **Dateigröße:** Wenn die Größe der Datei die angegebene Zahl MB erreicht, schließt die Sitzungsaufzeichnung die Datei und öffnet eine neue. Standardmäßig wird ein Dateirollover durchgeführt, wenn die Dateigröße 50 MB erreicht. Sie können ein Limit von 10 MB bis 300 MB angeben.
- **Dauer:** Wenn die Sitzung für die angegebene Anzahl der Stunden aufgezeichnet wurde, wird die Datei geschlossen und eine neue Datei wird geöffnet. Standardmäßig wird nach 12 Stunden Aufzeichnung ein Dateirollover durchgeführt. Sie können ein Limit von einer bis zu 24 Stunden festlegen.

Die Sitzungsaufzeichnung prüft beide Felder und ermittelt, welches Ereignis zuerst auftritt, und legt dann den Rollover fest. Beispiel: Wenn Sie 17 MB für die Dateigröße und sechs Stunden für die Dauer eingeben, und die Aufzeichnung erreicht 17 MB nach drei Stunden, reagiert die Sitzungsaufzeichnung auf die Dateigröße von 17 MB, schließt die Datei und öffnet eine neue.

Unabhängig vom eingegebenen Wert für die Dateigröße führt die Sitzungsaufzeichnung ein Rollover frühestens nach einer Stunde durch (dies ist der Mindestwert, den Sie eingeben können), um das Erstellen von zu vielen kleinen Dateien zu vermeiden. Diese Regel gilt nicht, wenn die Dateigröße 300 MB übersteigt.

### **Angeben der maximalen Dateigröße für Aufzeichnungen**

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Rollover**.



4. Geben Sie eine Ganzzahl zwischen 10 und 300 ein, um die maximale Dateigröße in MB festzulegen.

5. Geben Sie ein Ganzzahl zwischen 1 und 24 ein, mit der Sie die maximale Aufzeichnungslänge in Stunden angeben.

## Benachrichtigungsmeldungen anpassen

April 3, 2024

Wenn in der aktiven Aufzeichnungsrichtlinie festgelegt ist, dass Benutzer über das Aufzeichnen der Sitzung benachrichtigt werden, wird eine Benachrichtigung angezeigt, nachdem die Benutzer die Anmeldeinformationen eingegeben haben. Die Standardbenachrichtigung ist: **Ihre Aktivität in den von Ihnen vor kurzem gestarteten Programmen oder dem Desktop wird aufgezeichnet. Schließen Sie den Desktop bzw. die Programme, wenn Sie dies ablehnen.** Die Benutzer können auf **OK** klicken, um das Fenster zu schließen und die Sitzung fortzusetzen.

Die Standardbenachrichtigung wird in der Sprache des Betriebssystems auf dem VDA angezeigt.

Sie können benutzerdefinierte Benachrichtigungen in ausgewählten Sprachen erstellen. Sie können jedoch nur eine Benachrichtigung pro Sprache erstellen. Den Benutzern wird die Benachrichtigung in der Sprache der lokalen Einstellungen angezeigt.

### Erstellen einer Benachrichtigung

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Benachrichtigungen**.
4. Klicken Sie auf **Hinzufügen**.
5. Wählen Sie die Sprache für die Nachricht und geben Sie die neue Nachricht ein. Sie können nur eine Nachricht pro Sprache erstellen.

Nach der Annahme und Aktivierung wird die neue Benachrichtigung im Feld Sprachspezifische Benachrichtigungen angezeigt.

## Aktivieren oder Deaktivieren der Aufzeichnung

June 21, 2021

Der Sitzungsaufzeichnungsagent wird auf VDAs für Multisitzungs-OS installiert, auf denen Sie Sitzungen aufzeichnen möchten. Jeder Agent bietet eine Einstellung, mit der die Aufzeichnungsfunktion auf

dem VDA aktiviert wird. Nach dem Aktivieren der Aufzeichnungsfunktion wertet die Sitzungsaufzeichnung die aktive Aufzeichnungsrichtlinie aus, mit der festgelegt wird, welche Sitzungen aufgezeichnet werden.

Bei Installation des Sitzungsaufzeichnungsagents ist die Aufzeichnungsfunktion aktiviert. Wir empfehlen, dass Sie die Sitzungsaufzeichnung auf VDAs deaktivieren, für die kein Aufzeichnen vorgesehen ist, da die Anwendung die Serverleistung geringfügig beeinträchtigt, selbst wenn keine Aufzeichnung erfolgt.

### **Aktivieren oder Deaktivieren der Aufzeichnung auf einem VDA**

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
3. Legen Sie unter **Sitzungsaufzeichnung** mit dem Kontrollkästchen **Sitzungsaufzeichnung für diese VDA-Maschine aktivieren** fest, ob Sitzungen für den VDA aufgezeichnet werden sollen.
4. Starten Sie auf Aufforderung den Sitzungsaufzeichnungsagent-Dienst neu, um die Änderung zu übernehmen.

#### **Hinweis:**

Bei der Installation der Sitzungsaufzeichnung wird als aktive Richtlinie **Nicht aufzeichnen** (auf keinem Server werden Sitzungen aufgezeichnet) verwendet. Aktivieren Sie in der Richtlinienkonsole für die Sitzungsaufzeichnung eine andere Richtlinie, um die Aufzeichnungsfunktion zu aktivieren.

### **Aktivieren der Aufzeichnung benutzerdefinierter Ereignisse**

In der Sitzungsaufzeichnung können Sie mit Anwendungen von Drittanbietern benutzerdefinierte Daten, so genannte Ereignisse, in die Sitzungsaufzeichnungen einfügen. Diese Ereignisse werden angezeigt, wenn die Sitzung mit dem Sitzungsaufzeichnungsplayer wiedergegeben wird. Die Ereignisse sind Teil der Sitzungsaufzeichnungsdatei und können nach dem Aufzeichnen der Sitzung nicht geändert werden.

Ein Ereignis kann beispielsweise den folgenden Text enthalten: "Benutzer öffnete einen Browser". Jedes Mal, wenn ein Benutzer einen Browser in einer Sitzung öffnet, die aufgezeichnet wird, wird der Text zu diesem Zeitpunkt in die Aufzeichnung eingefügt. Wenn die Sitzung mit dem Sitzungsaufzeichnungsplayer wiedergegeben wird, kann der Benutzer die Anzahl der Marker in der Liste Ereignisse und Textmarken im Player notieren, und damit schnell die Stellen suchen und zählen, an denen der Benutzer einen Browser geöffnet hat.

Einfügen benutzerdefinierter Ereignisse in Aufzeichnungen auf einem Server

- Aktivieren Sie über die **Eigenschaften des Sitzungsaufzeichnungsagents** eine Einstellung auf jedem Server, auf dem Sie benutzerdefinierte Ereignisse einfügen möchten. Aktivieren Sie jeden Server separat. Das globale Aktivieren aller Server in einer Site ist nicht möglich.
- Entwickeln Sie Anwendungen, die auf der Event-API basieren, die in der Citrix Virtual Apps and Desktops-Sitzung jedes Benutzers ausgeführt werden (zum Einfügen der Daten in die Aufzeichnung).

Bei der Installation der Sitzungsaufzeichnung wird auch eine Ereignisaufzeichnungs-COM-Anwendung (API) installiert, mit der Sie Text von Anwendungen von Drittherstellern in die Aufzeichnung einfügen können. Sie können die API von vielen Programmiersprachen verwenden, u. a. Visual Basic, C++ oder C#. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX226844](#). Die DLL-Datei der Sitzungsaufzeichnungs-Event-API ist Teil der Installation der Sitzungsaufzeichnung. Die Datei ist unter C:\Programme\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll gespeichert.

Zum Aktivieren der Aufzeichnung von benutzerdefinierten Ereignissen auf einem Server führen Sie folgende Schritte aus:

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsagent - Eigenschaften** auf die Registerkarte **Aufzeichnung**.
4. Aktivieren Sie unter **Benutzerdefinierte Ereignisaufzeichnung** das Kontrollkästchen **Anwendungen von Drittherstellern können benutzerdefinierte Daten auf diesem Server aufzeichnen**.

## Aktivieren oder Deaktivieren digitaler Signaturen

June 21, 2021

Wenn Sie Zertifikate auf Maschinen installieren, auf denen der Sitzungsaufzeichnungsserver und der Sitzungsaufzeichnungsplayer installiert sind, können Sie die Sicherheit der Bereitstellung erhöhen, indem Sie den Sitzungsaufzeichnungen digitale Signaturen zuweisen.

In der Standardeinstellung sind digitale Signaturen deaktiviert. Nachdem Sie das Zertifikat zum Signieren der Aufzeichnungen ausgewählt haben, gewährt die Sitzungsaufzeichnung Leseberechtigung für den Storage Manager-Dienst der Sitzungsaufzeichnung.

### Aktivieren digitaler Signaturen

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an.

2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Signieren**.
4. Navigieren Sie zu dem Zertifikat, das die sichere Kommunikation zwischen den Maschinen ermöglicht, auf denen die Sitzungsaufzeichnungskomponenten installiert sind.

## Deaktivieren digitaler Signaturen

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Signieren**.
4. Klicken Sie auf **Entfernen**.

## Administratorprotokollierung

January 15, 2024

Die Administratorprotokollierung der Sitzungsaufzeichnung erfasst die folgenden Aktivitäten:

- Änderungen an Aufzeichnungsrichtlinien und Ereignisprotokollierungsrichtlinien, die in der Richtlinienkonsole für die Sitzungsaufzeichnung oder in Citrix Director vorgenommen werden
- Änderungen an Eigenschaften des Sitzungsaufzeichnungsservers
- Downloads von Aufzeichnungen im Sitzungsaufzeichnungsplayer
- Aufzeichnung einer Sitzung durch die Sitzungsaufzeichnung nach einer Richtlinienabfrage
- Nicht autorisierte Zugriffsversuche auf die Administratorprotokollierung

### Warnung:

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.



## Deaktivieren oder Aktivieren der Administratorprotokollierung

Nach der Installation können Sie die Administratorprotokollierung der Sitzungsaufzeichnung in den **Eigenschaften des Sitzungsaufzeichnungsservers** deaktivieren oder aktivieren.

1. Melden Sie sich als Administrator bei der Maschine an, auf der die Administratorprotokollierung für die Sitzungsaufzeichnung installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Protokollierung**.

Wenn Sie die Administratorprotokollierung deaktivieren, werden keine neuen Aktivitäten protokolliert. Sie können die vorhandenen Protokolle über die webbasierte Oberfläche abfragen.

Wenn die **obligatorische Sperrung** aktiviert ist, werden die folgenden Aktivitäten blockiert, wenn die Protokollierung fehlschlägt. Außerdem wird ein Systemereignis mit der Ereignis-ID 6001 protokolliert:

- Änderungen an Aufzeichnungsrichtlinien, die in der Richtlinienkonsole für die Sitzungsaufzeichnung oder in Citrix Director vorgenommen werden
- Änderungen an Eigenschaften des Sitzungsaufzeichnungsservers

Die obligatorische Sperrereinstellung hat keine Auswirkungen auf das Aufzeichnen von Sitzungen.

## Konfigurieren eines Dienstkontos für die Administratorprotokollierung

In der Standardeinstellung wird die Administratorprotokollierung als Webanwendung mit der Identität "Netzwerkdienst" in IIS ausgeführt. Zur Erhöhung der Sicherheit können Sie die Identität der Webanwendung in ein Dienstkonto oder ein bestimmtes Domänenkonto ändern.

1. Melden Sie sich als Administrator bei der Maschine mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im IIS-Manager auf **Anwendungspools**.
3. Klicken Sie unter **Anwendungspools** mit der rechten Maustaste auf **SessionRecordingLoggingAppPool** und wählen Sie **Erweiterte Einstellungen**.
4. Ändern Sie das Attribut **Identität** unter Auswahl des gewünschten Kontos.
5. Erteilen Sie dem Konto die Berechtigung **db\_owner** für die Datenbank **CitrixSessionRecordingLogging** in Microsoft SQL Server.
6. Erteilen Sie dem Konto Leseberechtigung für den Registrierungsschlüssel **HKEY\_LOCAL\_MACHINE\SOFTWARE**

## Deaktivieren oder Aktivieren der Protokollierung von Aufzeichnungsaktivitäten

Standardmäßig erfasst die Administratorprotokollierung nach Abschluss der Richtlinienabfrage alle Aufzeichnungsaktionen. Dabei können große Datenmengen entstehen. Zum Verbessern der

Leistung und Einsparen von Speicherplatz deaktivieren Sie diese Art von Protokollierung in der Registrierung.

1. Melden Sie sich als Administrator bei der Maschine mit dem Sitzungsaufzeichnungsserver an.
2. Öffnen Sie den Registrierungs-Editor.
3. Gehen Sie zu **HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server**.
4. Legen Sie für **EnableRecordingActionLogging** folgenden Wert fest:
  - 0** zum Deaktivieren der Protokollierung von Aufzeichnungsaktivitäten
  - 1** zum Aktivieren der Protokollierung von Aufzeichnungsaktivitäten

## Abfragen des Administratorprotokolls

Die Sitzungsaufzeichnung bietet eine webbasierte Oberfläche zum Abfragen des Administratorprotokolls.

Führen Sie auf dem Computer mit dem Sitzungsaufzeichnungsserver folgende Schritte aus:

1. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnung - Administratorprotokollierung**.
2. Geben Sie die Anmeldeinformationen eines **LoggingReader**-Benutzers ein.

Die im Webplayer integrierte Webseite der Administratorprotokollierung wird angezeigt.

ID	Logging Time	Task Category	Component Affected	Task Details	Task Executed By	Authorized
18	2/22/2021 10:07 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...		true
17	2/22/2021 10:06 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...		true
16	2/22/2021 9:41 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...		true
15	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...		true
14	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...		true
13	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...		true
12	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...		true
11	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...		true
10	2/22/2021 9:31 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...		true
9	2/22/2021 9:31 PM	Recording File Play Back	Session Recording Player	+ Action = Session File Path and Size Query ...		true

Auf anderen Maschinen:

1. Öffnen Sie einen Webbrowser und rufen Sie die Webseite der Administratorprotokollierung auf.
  - **HTTPS:** <https://servername/WebPlayer/#/logging/config> und <https://servername/WebPlayer/#/logging/record>, wobei **servername** der Name der Maschine ist, auf der der Sitzungsaufzeichnungsserver ausgeführt wird.

- **HTTP:** <http://servername/WebPlayer/#/logging/config> and <http://servername/WebPlayer/#/logging/record>, wobei `servername` der Name der Maschine ist, auf der der Sitzungsaufzeichnungsserver ausgeführt wird.

2. Geben Sie die Anmeldeinformationen eines **LoggingReader**-Benutzers ein.

## Hohe Datenbankverfügbarkeit

September 22, 2022

Die Sitzungsaufzeichnung unterstützt die folgenden Lösungen für hohe Datenbankverfügbarkeit basierend auf Microsoft SQL Server. Fällt die Hardware oder Software eines wichtigen oder primären SQL Server-Computers aus, kann durch einen automatischen Failover der Datenbanken sichergestellt werden, dass die Sitzungsaufzeichnung weiterhin ordnungsgemäß funktioniert.

- Always-On-Verfügbarkeitsgruppen

Always-On-Verfügbarkeitsgruppen sind eine Lösung für hohe Verfügbarkeit und Wiederherstellung im Notfall, die eine für Unternehmen geeignete Alternative zur Datenbankspiegelung darstellt. Always-On-Verfügbarkeitsgruppen wurden mit SQL Server 2012 eingeführt und maximieren die Verfügbarkeit diverser Benutzerdatenbanken für Unternehmen. Sie erfordern, dass die SQL Server-Instanzen auf den Windows Server Failover Clustering-Knoten (WSFC) residieren. Weitere Informationen finden Sie unter [Always-On-Verfügbarkeitsgruppen: Lösung für hohe Verfügbarkeit und Notfallwiederherstellung](#).

- SQL Server-Clustering

Bei dieser Technologie von Microsoft kann ein Server automatisch die Aufgaben und Verantwortlichkeiten eines anderen, fehlgeschlagenen Servers übernehmen. Es ist jedoch komplizierter, diese Lösung einzurichten. Zudem ist das automatische Failover in der Regel langsamer als bei anderen Lösungen (etwa der Spiegelung der SQL Server-Datenbank). Weitere Informationen finden Sie unter [Always-On-Failoverclusterinstanzen \(SQL Server\)](#).

- SQL Server-Datenbankspiegelung

Die Datenbankspiegelung gewährleistet, dass bei einem Ausfall des aktiven Datenbankservers innerhalb von Sekunden ein automatischer Failover erfolgt. Diese Lösung ist teurer als die anderen beiden Lösungen, da auf jedem Datenbankserver eine vollständige SQL Server-Lizenz vorliegen muss. Die SQL Server Express Edition kann in einer gespiegelten Umgebung nicht verwendet werden. Weitere Informationen finden Sie unter [Datenbankspiegelung \(SQL Server\)](#).

## Methoden zum Konfigurieren der Sitzungsaufzeichnung mit hoher Datenbankverfügbarkeit

Konfigurieren Sie die Sitzungsaufzeichnung mit hoher Datenbankverfügbarkeit mit einer der folgenden Methoden:

- Installieren Sie zuerst die Komponenten des Sitzungsaufzeichnungsservers und konfigurieren Sie anschließend die hohe Datenbankverfügbarkeit für die erstellten Datenbanken. Sie können die Komponenten der Sitzungsaufzeichnungsverwaltung mit Datenbanken installieren, die zur Installation auf der vorbereiteten SQL Server-Instanz konfiguriert sind. Konfigurieren Sie anschließend die hohe Verfügbarkeit für die erstellten Datenbanken.
  - Für Always-On-Verfügbarkeitsgruppen und Clustering müssen Sie in HKEY\_LOCAL\_MACHINE\SOFTWARE den Namen der SQL Server-Instanz manuell in den Namen des Verfügbarkeitsgruppen-Listeners oder des SQL Server-Netzwerks ändern.
  - Für die Datenbankspiegelung müssen Sie die Failoverpartner für die Datenbanken in HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\DatabaseFailoverPartner und HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\LoggingDatabaseFailoverPartner manuell hinzufügen.
- Konfigurieren Sie zunächst die hohe Verfügbarkeit für leere Datenbanken und installieren Sie dann die Komponenten der Sitzungsaufzeichnungsverwaltung. Sie können zwei leere Datenbanken als Datenbank für die Sitzungsaufzeichnung und als Datenbank für die Konfigurationsprotokollierung auf der künftigen primären SQL Server-Instanz erstellen und hohe Verfügbarkeit konfigurieren. Geben Sie dann den Namen der SQL Server-Instanz bei der Installation der Komponenten des Sitzungsaufzeichnungsservers an:
  - Zur Verwendung von Always-On-Verfügbarkeitsgruppen geben Sie den Namen des Verfügbarkeitsgruppen-Listeners an.
  - Zur Verwendung der Datenbankspiegelung geben Sie den Namen des primären SQL Server-Computers ein.
  - Zur Verwendung der Clusterlösung geben Sie den Netzwerknamen des SQL Server-Computers ein.

## Lastausgleich

November 5, 2021

Die Sitzungsaufzeichnung unterstützt den Lastausgleich zwischen Sitzungsaufzeichnungsservern. In diesem Artikel wird die Konfiguration des Lastausgleichs am Beispiel des Citrix ADC zusammengefasst.

Weitere Informationen finden Sie unter [Konfigurieren des Lastausgleichs in einer vorhandenen Bereitstellung](#) und [Bereitstellen und Lastausgleich der Sitzungsaufzeichnung in Azure](#).

Sie können die Lastausgleichskonfigurationen aller Sitzungsaufzeichnungsserver miteinander synchronisieren.

**Hinweis:**

Das Lastausgleichsfeature erfordert mindestens Version 7.16 des Sitzungsaufzeichnungsservers und des Sitzungsaufzeichnungsagents.

**Änderungen an der Sitzungsaufzeichnung mit Lastausgleich:**

- Alle Server der Sitzungsaufzeichnung verwenden denselben Ordner für die Speicherung von Aufzeichnungsdateien.
- Alle Server der Sitzungsaufzeichnung verwenden dieselbe Datenbank für die Sitzungsaufzeichnung.
- (Empfohlen) Installation einer Richtlinienkonsole für die Sitzungsaufzeichnung und Verwendung dieser Konsole durch alle Sitzungsaufzeichnungsserver.

**Konfigurieren des Lastausgleichs**

Zur Verwendung dieses Features führen Sie folgende Schritte in Citrix ADC und den verschiedenen Sitzungsaufzeichnungskomponenten aus:

**Konfigurieren des Lastausgleichs (Citrix ADC-Teil)**

**Konfigurieren der Lastausgleichsserver** Fügen Sie die Sitzungsaufzeichnungsserver den Lastausgleichsservern in Citrix ADC hinzu.

**Konfigurieren der Lastausgleichsdienste**

1. Fügen Sie einen Lastausgleichsdienst für jedes erforderliche Protokoll auf jedem Sitzungsaufzeichnungsserver hinzu.
2. (Empfohlen) Wählen Sie die entsprechende Protokollüberwachung zum Binden jeder Dienstüberwachung.

**Konfigurieren der virtuellen Server für den Lastausgleich**

1. Erstellen Sie virtuelle Server mit derselben Citrix ADC-VIP-Adresse auf Grundlage der erforderlichen Protokolle und binden Sie die virtuellen Server an den jeweiligen Lastausgleichsdienst.
2. Konfigurieren Sie Persistenz auf jedem virtuellen Server.

3. (Empfohlen) Wählen Sie LEASTBANDWIDTH oder LEASTPACKETS als Lastausgleichsmethode anstelle der Standardmethode LEASTCONNECTION.
4. Erstellen Sie ein Zertifikat, um den virtuellen HTTPS-Server zu aktualisieren.

### Konfigurieren des Lastausgleichs (Sitzungsaufzeichnung)

#### Führen Sie auf jedem Server, auf dem der Sitzungsaufzeichnungsserver installiert wurde, folgende Schritte aus

1. (Empfohlen) Geben Sie während der Installation des Sitzungsaufzeichnungsservers denselben Namen für die Sitzungsaufzeichnungsdatenbank ein.
2. Wenn Sie die Administratorprotokollierung wählen, empfiehlt Citrix, dass Sie bei der Installation der einzelnen Sitzungsaufzeichnungsserver jeweils denselben Datenbanknamen für die Administratorprotokollierung eingeben.
3. Wenn Sie allen Maschinenkonten der Sitzungsaufzeichnungsserver Lese-/Schreibberechtigung für den Ordner zur Dateispeicherung erteilt haben, ändern Sie die Einstellung für Sitzungsaufzeichnungsserver - Eigenschaften so, dass der Ordner als gemeinsamer Ordner verwendet wird. Weitere Informationen finden Sie unter [Angaben des Speicherortes für wiederhergestellte Dateien](#).
4. Fügen Sie im Registrierungsschlüssel des Sitzungsaufzeichnungsservers unter HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Recording\Server einen Wert hinzu.  
Wertname: **EnableLB**  
Wert: **1** (DWORD, was "Aktivieren" bedeutet)
5. Wenn Sie für die Nachrichtenwarteschlange des Speichermanagers der Sitzungsaufzeichnung HTTP oder HTTPS auswählen, erstellen Sie einen Hosteintrag für die Citrix ADC-VIP-Adresse, fügen Sie Umleitungen in C:\Windows\System32\msmq\Mapping\sample\_map hinzu und starten Sie den Message Queuing-Dienst neu.

Die Umleitung sieht in etwa folgendermaßen aus:

```
1 <redirections xmlns="msmq-queue-redirections.xml">
2   <redirection>
3     <from>http://<ADCHost>*/msmq/private$/
4       CitrixSmAudData</from>
5     <to>http://<LocalFqdn>/msmq/private$/
6       CitrixSmAudData</to>
7   </redirection>
8   <redirection>
9     <from>https://<ADCHost>*/msmq/private$/
10    CitrixSmAudData</from>
11    <to>https://<LocalFqdn>/msmq/private$/
12    CitrixSmAudData</to>
13  </redirection>
```

```
10 </redirections>
11 <!--NeedCopy-->
```

Wobei **<ADCHost>** der erstellte FQDN der Citrix ADC-VIP-Adresse und **<LocalFqdn>** der FQDN des lokalen Hosts ist.

6. (Empfohlen) Nach dem Konfigurieren der Registrierung eines Sitzungsaufzeichnungsservers können Sie mit dem Skript **<Installationspfad des Sitzungsaufzeichnungsservers>\Scripts\SrServerCon** die Konfigurationen aus der Registrierung dieses Servers exportieren und in die Registrierungen der anderen Sitzungsaufzeichnungsserver importieren. Sie können auch das Skript **SrServerConfigurationSync.ps1** zum Hinzufügen einer Umleitungszuordnung für die Nachrichtenwarteschlange verwenden.
  - a) Starten Sie auf einem Sitzungsaufzeichnungsserver nach dem Konfigurieren des Registrierungswerts **EnableLB** eine Eingabeaufforderung als Administrator und führen Sie den Befehl **powershell.exe -file SrServerConfigurationSync.ps1 -Action Export,AddRedirection -ADCHost <ADCHost>** aus, wobei **<ADCHost>** der erstellte FQDN der Citrix ADC-VIP-Adresse ist.
  - b) Nachdem das Skript ausgeführt wurde, wird eine exportierte Registrierungsdatei mit dem Namen **SrServerConfig.reg** generiert und die Datei **sr\_lb\_map.xml** wird dem Pfad **C:\Windows\System32\msmq\Mapping** hinzugefügt.
  - c) Kopieren Sie für die anderen Sitzungsaufzeichnungsserver die in dem obigen Schritt erstellte Datei **SrServerConfig.reg**, starten Sie dann eine Eingabeaufforderung als Administrator und führen Sie den Befehl **powershell.exe -file SrServerConfigurationSync.ps1 -Action Import,AddRedirection -ADCHost <ADCHost>** aus, wobei **<ADCHost>** der erstellte FQDN der Citrix ADC-VIP-Adresse ist.
  - d) Nachdem das Skript ausgeführt wurde, wird der Wert **EnableLB** den übrigen Registrierungsschlüsseln des Sitzungsaufzeichnungsservers hinzugefügt und die Datei **sr\_lb\_map.xml** unter **C:\Windows\System32\msmq\Mapping** eingefügt.

#### **Führen Sie auf der Maschine mit installiertem Sitzungsaufzeichnungsagenten folgende Schritte in den Sitzungsaufzeichnungseigenschaften aus**

- Wenn Sie für die Nachrichtenwarteschlange des Speichermanagers der Sitzungsaufzeichnung HTTP oder HTTPS wählen, geben Sie den FQDN der Citrix ADC-VIP-Adresse im Textfeld **Sitzungsaufzeichnungsserver** ein.
- Wenn Sie für die Nachrichtenwarteschlange des Speichermanagers der Sitzungsaufzeichnung das Standardprotokoll TCP wählen, geben Sie die Citrix ADC-VIP-Adresse im Textfeld **Sitzungsaufzeichnungsserver** ein.

**Führen Sie auf der Maschine mit installiertem Sitzungsaufzeichnungsplayer folgende Schritte aus** Fügen Sie die Citrix ADC-VIP-Adresse oder den zugehörigen FQDN als verbundenen Sitzungsaufzeichnungsserver hinzu.

**Führen Sie auf dem SQL-Server mit installierter Datenbank für die Sitzungsaufzeichnung folgende Schritte aus** Fügen Sie alle Maschinenkonten der Sitzungsaufzeichnung der Datenbank für die Sitzungsaufzeichnung hinzu und weisen Sie ihnen die Berechtigung **db\_owner** zu.

## Ändern des Kommunikationsprotokolls

June 21, 2021

Aus Sicherheitsgründen empfiehlt Citrix, HTTP nicht als Kommunikationsprotokoll zu verwenden. Die Sitzungsaufzeichnung ist für die Verwendung von HTTPS konfiguriert. Zur Verwendung von HTTP anstelle von HTTPS müssen Sie mehrere Einstellungen ändern.

### Verwenden von HTTP als Kommunikationsprotokoll

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an und deaktivieren Sie sichere Verbindungen für den Sitzungsaufzeichnungsbroker in IIS.
2. Ändern Sie auf jedem Server, auf dem der Sitzungsaufzeichnungsagent installiert ist, das eingestellte Protokoll von HTTPS in HTTP im Dialogfeld **Sitzungsaufzeichnungsagent - Eigenschaften**:
  - a) Melden Sie sich bei jedem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
  - b) Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
  - c) Klicken unter **Sitzungsaufzeichnungsagent - Eigenschaften** auf die Registerkarte **Verbindungen**.
  - d) Klicken Sie im Bereich **Sitzungsaufzeichnungsbroker** in der Dropdownliste **Protokoll** auf **HTTP** und bestätigen Sie die Änderung mit **OK**. Bestätigen Sie den Neustart des Dienstes mit **Ja**.
3. Ändern Sie die Protokolleinstellung von HTTPS zu HTTP in den Einstellungen des Sitzungsaufzeichnungsplayers:
  - a) Melden Sie sich an jeder Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
  - b) Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.



- c) Klicken Sie im Menü von **Sitzungsaufzeichnungsplayer** auf **Extras > Optionen > Verbindungen**, wählen Sie den Server aus und klicken Sie auf **Ändern**.
  - d) Wählen Sie **HTTP** aus der Dropdownliste **Protokoll** und klicken Sie zwei Mal auf **OK**, um die Änderung zu akzeptieren und das Dialogfeld zu schließen.
4. Ändern Sie die Protokolleinstellung von HTTPS zu HTTP in der Richtlinienkonsole für die Sitzungsaufzeichnung:
- a) Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
  - b) Klicken Sie im Menü **Start** auf **Richtlinienkonsole für die Sitzungsaufzeichnung**.
  - c) Wählen Sie **HTTP** in der Dropdownliste **Protokoll** und klicken Sie auf **OK**, um die Verbindung herzustellen. Wenn die Verbindung erfolgreich hergestellt wird, wird diese Einstellung gespeichert und beim nächsten Starten der Richtlinienkonsole für die Sitzungsaufzeichnung verwendet.

### Zurücksetzen des Kommunikationsprotokolls auf HTTPS

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an und aktivieren Sie sichere Verbindungen für den Sitzungsaufzeichnungsbroker in IIS.
2. Ändern Sie auf jedem Server, auf dem der Sitzungsaufzeichnungsagent installiert ist, das eingestellte Protokoll von HTTP in HTTPS im Dialogfeld **Sitzungsaufzeichnungsagent - Eigenschaften**:
  - a) Melden Sie sich bei jedem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
  - b) Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
  - c) Klicken unter **Sitzungsaufzeichnungsagent - Eigenschaften** auf die Registerkarte **Verbindungen**.
  - d) Klicken Sie im Bereich **Sitzungsaufzeichnungsbroker** in der Dropdownliste **Protokoll** auf **HTTPS** und bestätigen Sie die Änderung mit **OK**. Bestätigen Sie den Neustart des Dienstes mit **Ja**.
3. Ändern Sie die Protokolleinstellung von HTTP zu HTTPS in den Einstellungen des Sitzungsaufzeichnungsplayers:
  - a) Melden Sie sich an jeder Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
  - b) Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
  - c) Klicken Sie im Menü von **Sitzungsaufzeichnungsplayer** auf **Extras > Optionen > Verbindungen**, wählen Sie den Server aus und klicken Sie auf **Ändern**.

- d) Wählen Sie **HTTPS** aus der Dropdownliste **Protokoll** und klicken Sie zwei Mal auf **OK**, um die Änderung zu akzeptieren und das Dialogfeld zu schließen.
4. Ändern Sie die Protokolleinstellung von HTTP zu HTTPS in der Sitzungsregistrierungsrichtlinienkonsole:
    - a) Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
    - b) Klicken Sie im Menü **Start** auf **Richtlinienkonsole für die Sitzungsaufzeichnung**.
    - c) Wählen Sie **HTTPS** in der Dropdownliste **Protokoll** und klicken Sie auf **OK**, um die Verbindung herzustellen. Wenn die Verbindung erfolgreich hergestellt wird, wird diese Einstellung gespeichert und beim nächsten Starten der Richtlinienkonsole für die Sitzungsaufzeichnung verwendet.

## Konfigurieren des Citrix-Programms zur Verbesserung der Benutzerfreundlichkeit (CEIP)

April 3, 2024

Wenn Sie am Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) teilnehmen, werden anonyme Konfigurations- und Nutzungsdaten erfasst und an Citrix gesendet, damit die Qualität und Leistung von Produkten verbessert werden kann. Außerdem wird eine Kopie der anonymen Daten zur schnellen und effizienten Analyse an Google Analytics (GA) gesendet.

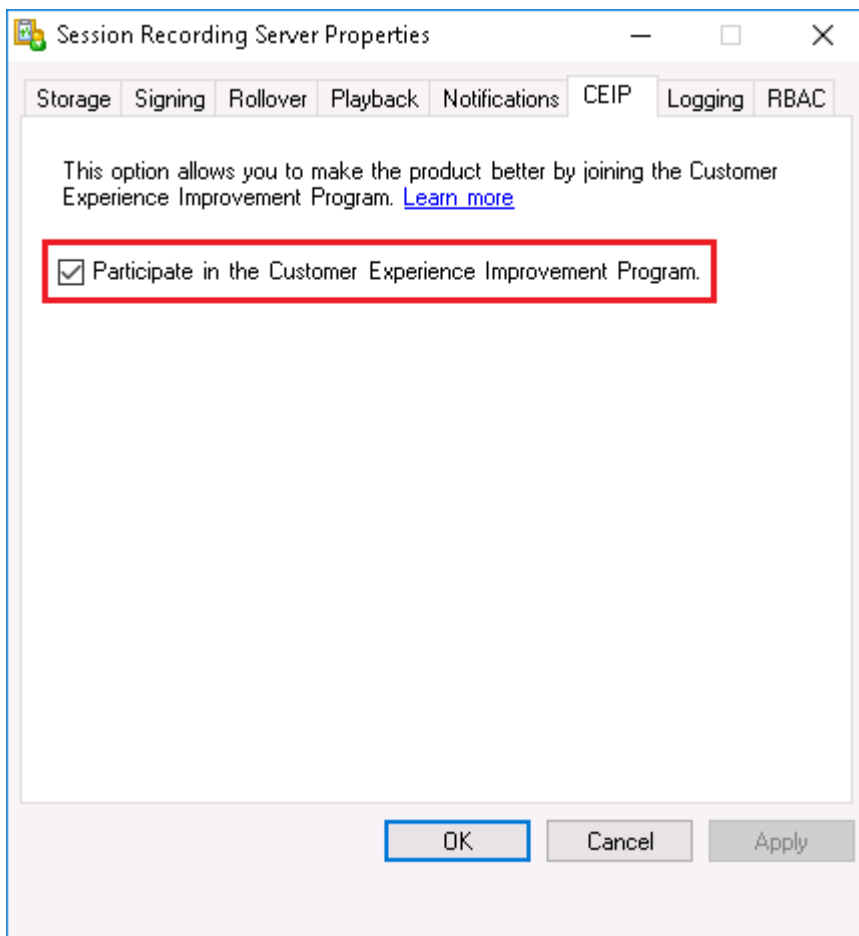
### Einstellungen

#### CEIP-Einstellung

Standardmäßig nehmen Sie bei der Installation der Sitzungsaufzeichnung automatisch am CEIP teil. Der erste Datenupload erfolgt ca. sieben Tage nach Installation der Sitzungsaufzeichnung. Um sich vom CEIP abzumelden, gehen Sie folgendermaßen vor:

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **CEIP**.
4. Deaktivieren Sie das Kontrollkästchen **Am Programm zur Verbesserung der Benutzerfreundlichkeit** teilnehmen.

5. Starten Sie den **Analysedienst der Citrix Sitzungsaufzeichnung** neu, damit die Einstellung wirksam wird.



### GA-Einstellung

Wenn GA aktiviert ist, werden die Heartbeat-Daten zwischen GA und dem Sitzungsaufzeichnungsserver alle 5 Stunden erfasst.

Die Registrierungseinstellung, mit der das GA aktiviert oder deaktiviert wird (Standardwert = 0):

Speicherort: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\

Name: CeipHeartBeatDisable

Wert: 1 = deaktiviert , 0 = aktiviert

Wenn nicht angegeben, ist GA aktiviert.

So deaktivieren Sie GA:

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an.

2. Öffnen Sie den **Registrierungs-Editor**.
3. Navigieren Sie zu **\*\*HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\\*\***.
4. Fügen Sie einen Registrierungswert hinzu und nennen Sie ihn **CeipHeartBeatDisable**.
5. Setzen Sie den Wert von **CeipHeartBeatDisable** auf 1.
6. Starten Sie den Analysedienst der Citrix Sitzungsaufzeichnung neu, damit die Einstellung wirksam wird.

### Vom Sitzungsaufzeichnungsserver erfasste Daten

In der folgende Tabelle sehen Sie Beispiele für die Art der anonymen Informationen, die gesammelt werden. Die Daten enthalten keine Informationen, die Sie als Kunden identifizieren.

Datenpunkt	Schlüsselname	Beschreibung
Maschinen-GUID	machine_guid	Identifiziert die Maschine, von der die Daten stammen. Wenn GA aktiviert ist, werden die Heartbeat-Daten, unabhängig davon, ob CEIP aktiviert ist, an GA gesendet.
Betriebssystemversion	OS_version	Textzeichenfolge, die das Betriebssystem der Maschine angibt. Wenn GA aktiviert ist, werden die Heartbeat-Daten, unabhängig davon, ob CEIP aktiviert ist, an GA gesendet.
Version des Sitzungsaufzeichnungsservers	SRS_version	Textzeichenfolge, die die installierte Version des Sitzungsaufzeichnungsservers angibt. Wenn GA aktiviert ist, werden die Heartbeat-Daten, unabhängig davon, ob CEIP aktiviert ist, an GA gesendet.
Anzahl der Anwendungsaufzeichnungen	application-recording-number	Ganzzahl, die die Anzahl der Anwendungsaufzeichnungsdateien angibt. Die Daten werden gesendet, wenn sowohl GA als auch CEIP aktiviert ist.

Datenpunkt	Schlüsselname	Beschreibung
Anzahl der Aufzeichnungen	recording-number	Ganzzahl, die die Anzahl der Anwendungs- und der Desktop-Aufzeichnungsdateien angibt. Die Daten werden gesendet, wenn sowohl GA als auch CEIP aktiviert ist.
Anzahl dynamischer Aufzeichnungen	dynamic-recording-number	Ganzzahl, die die Anzahl der Dateien dynamischer Aufzeichnungen angibt. Die Daten werden gesendet, wenn sowohl GA als auch CEIP aktiviert ist.
Anzahl der Agents, die aufgezeichnete Sitzungen hosten	recorded-agent-number	Ganzzahl, die die Anzahl der VDAs angibt, die aufgezeichnete Sitzungen hosten. Die Daten werden gesendet, wenn sowohl GA als auch CEIP aktiviert ist.
Anzahl der Agents, die aufgezeichnete Sitzungen mit protokollierten Ereignissen hosten	event-logging-enabled-agent-number	Ganzzahl, die die Anzahl der VDAs angibt, die aufgezeichnete Sitzungen mit protokollierten Ereignissen hosten. Die Daten werden gesendet, wenn sowohl GA als auch CEIP aktiviert ist.
Anzahl der aufgezeichneten Sitzungen mit protokollierten Ereignissen	event-logging-recording-number	Ganzzahl, die die Anzahl der Dateien aufgezeichneter Sitzungen mit protokollierten Ereignissen angibt. Die Daten werden gesendet, wenn sowohl GA als auch CEIP aktiviert ist.
Aktivierung der Administratorprotokollierung	admin-logging-status	Ziffer, die angibt, ob die Administratorprotokollierung aktiviert ist. 1 bedeutet aktiviert, 0 bedeutet deaktiviert. Die Daten werden gesendet, wenn sowohl GA als auch CEIP aktiviert ist.

Datenpunkt	Schlüsselname	Beschreibung
Anzahl protokollierter Ereignisse	collected-events-number	Ganzzahl, die die Anzahl der protokollierten Ereignisse angibt. Die Daten werden gesendet, wenn sowohl GA als auch CEIP aktiviert ist.
Anzahl der benutzerdefinierten Richtlinien	customized-policies-number	Ganzzahl, die die Anzahl der benutzerdefinierten Sitzungsaufzeichnungs- und Ereignisprotokollierungsrichtlinien angibt. Die Daten werden gesendet, wenn sowohl GA als auch CEIP aktiviert ist.
Aktivierung des Lastausgleichs	load-balancing-status	Ziffer, die angibt, ob der Lastausgleich aktiviert ist. 1 bedeutet aktiviert, 0 bedeutet deaktiviert. Die Daten werden gesendet, wenn sowohl GA als auch CEIP aktiviert ist.
Aktivierung der Aufzeichnungsanzeigerichtlinie	rbac-status	Ziffer, die angibt, ob die Aufzeichnungsanzeigerichtlinie aktiviert ist. 1 bedeutet aktiviert, 0 bedeutet deaktiviert. Die Daten werden gesendet, wenn sowohl GA als auch CEIP aktiviert ist.

## Protokollieren von Ereignissen

January 15, 2024

Die Sitzungsaufzeichnung kann Ereignisse protokollieren und Ereignisse in Aufzeichnungen für die spätere Suche und Wiedergabe markieren. So können Sie nach interessanten Ereignissen aus einer großen Anzahl von Aufzeichnungen suchen und die Ereignisse während der Wiedergabe im Sitzungsaufzeichnungsplayer finden.

## Systemdefinierte Ereignisse

Folgende systemdefinierte Ereignisse können in der Sitzungsaufzeichnung protokolliert werden:

- Anschluss von USB-Massenspeichergeräten
- Starten und Beenden von Anwendungen
- Umbenennen, Erstellen, Löschen und Verschieben von Dateien
- Webbrowsingaktivitäten
- Aktivitäten im obersten Fenster
- Zwischenablageaktivitäten

### Anschluss von USB-Massenspeichergeräten

Die Sitzungsaufzeichnung kann das Anschließen eines per Clientlaufwerkzuordnung (CDM) zugeordneten oder generisch umgeleiteten USB-Massenspeichergeräts an einen Client protokollieren, wenn die Citrix Workspace-App für Windows oder für Mac auf dem Clientgerät installiert ist. Die Sitzungsaufzeichnung kennzeichnet diese Ereignisse in der Aufzeichnung.

#### Hinweis:

Derzeit kann nur das Anschließen von USB-Massenspeichergeräten (USB-Klasse 08) protokolliert werden. Aktualisieren Sie die Verwaltungskomponenten der Sitzungsaufzeichnung und den Sitzungsaufzeichnungsagent auf Version 1811 oder höher, damit das Feature wie erwartet funktioniert. Weitere Informationen finden Sie unter [Ereignisprotokollierungsrichtlinien](#).

### Starten und Beenden von Anwendungen

#### Hinweis:

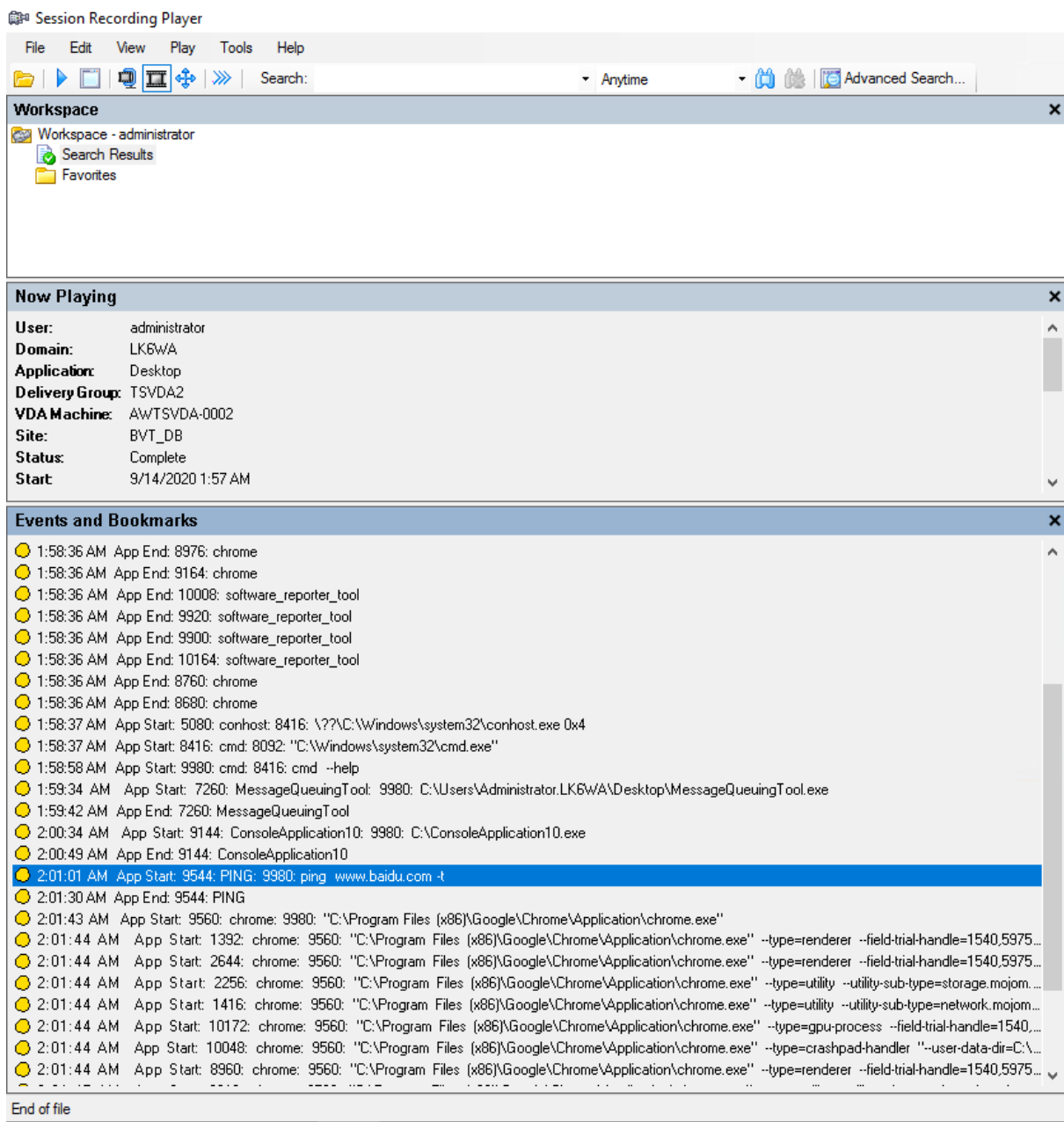
Dieses Feature erfordert Sitzungsaufzeichnung Version 1811 oder höher. Weitere Informationen finden Sie unter [Ereignisprotokollierungsrichtlinien](#).

Die Sitzungsaufzeichnung unterstützt das Protokollieren von Starten und Beenden der Anwendung. Wenn Sie einen Prozess in der **App-Überwachungsliste** hinzufügen, werden Apps überwacht, die vom hinzugefügten Prozess und seinen untergeordneten Prozessen gesteuert werden. Untergeordnete Prozesse eines Prozesses, der vor dem Ausführen der Sitzungsaufzeichnung gestartet wurde, können ebenfalls erfasst werden.

Die Sitzungsaufzeichnung fügt standardmäßig die Prozessnamen `cmd.exe`, `powershell.exe` und `ws1.exe` zur **App-Überwachungsliste** hinzu. Wenn Sie **App-Startereignisse protokollieren** und **App-Endereignisse protokollieren** für eine Ereignisprotokollierungsrichtlinie auswählen,

werden Starts und Beenden der Apps Eingabeaufforderung, PowerShell und Windows-Subsystem für Linux (WSL) unabhängig davon protokolliert, ob Sie die zugehörigen Prozessnamen manuell zur **App-Überwachungsliste** hinzugefügt haben. Die Standardprozessnamen sind in der **App-Überwachungsliste** nicht sichtbar.

Darüber hinaus bietet die Sitzungsaufzeichnung eine Befehlszeile für jedes protokollierte App-Startereignis.





## Umbenennen, Erstellen, Löschen und Verschieben von Dateien

Die Sitzungsaufzeichnung kann Vorgänge zum Umbenennen, Erstellen, Löschen und Verschieben von Dateien oder Unterordnern in Zielordnern protokollieren und die Ereignisse in der Aufzeichnung markieren. Weitere Informationen finden Sie unter [Ereignisprotokollierungsrichtlinien](#).

### Hinweis:

Dieses Feature erfordert Sitzungsaufzeichnung Version 1903 oder höher.

## Webbrowsingaktivitäten

Sie können Benutzeraktivitäten in unterstützten Browsern protokollieren und die Ereignisse in der Aufzeichnung markieren. Der Browsername, die URL und der Seitentitel werden protokolliert. Ein Beispiel sehen Sie im folgenden Screenshot.



Wenn Sie den Cursor von einer Webseite wegbewegen, die den Fokus hat, wird Ihr Browsing auf dieser Webseite markiert, ohne den Browsernamen anzuzeigen. Dieses Feature kann verwendet werden, um zu schätzen, wie lange ein Benutzer auf einer Webseite verbleibt. Ein Beispiel sehen Sie im folgenden Screenshot.



Liste der unterstützten Browser:

---

Browser	Version
Chrome	69 und höher
Internet Explorer	11
Firefox	61 und höher

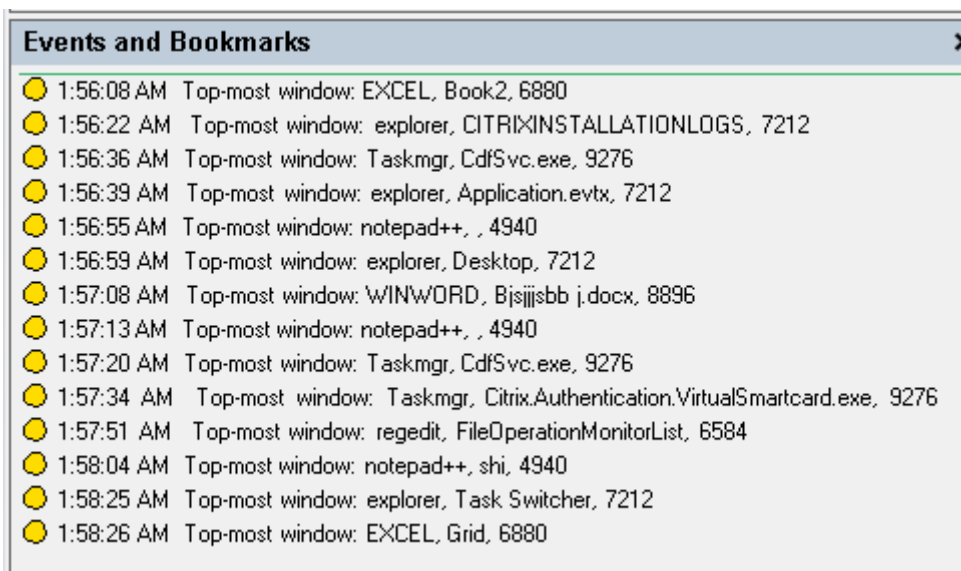
---

### Hinweis:

Dieses Feature erfordert Sitzungsaufzeichnung Version 1906 oder höher. Weitere Informationen finden Sie unter [Ereignisprotokollierungsrichtlinien](#).

## Aktivitäten im obersten Fenster

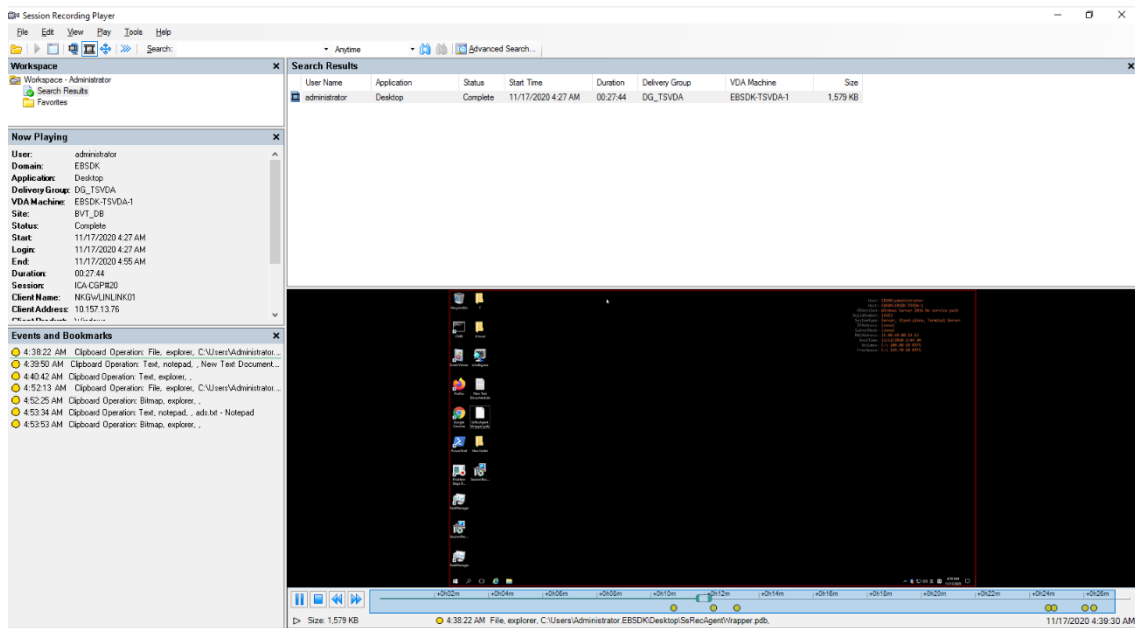
Die Sitzungsaufzeichnung kann die Aktivitäten im obersten Fenster protokollieren und die Ereignisse in der Aufzeichnung kennzeichnen. Der Prozessname, der Titel und die Prozessnummer werden protokolliert.



## Zwischenablageaktivitäten

Die Sitzungsaufzeichnung kann protokollieren, wenn Text, Bilder und Dateien mithilfe der Zwischenablage kopiert werden. Beim Kopieren einer Datei werden Prozessname und Dateipfad protokolliert. Beim Kopieren eines Texts werden Prozessname und Titel protokolliert. Beim Kopieren eines Bilds wird der Prozessname protokolliert.

**Hinweis:** Der Inhalt kopierter Texte wird standardmäßig nicht protokolliert. Um Textinhalte zu protokollieren, rufen Sie den Sitzungsaufzeichnungsagenten auf und legen `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Agent\CaptureClipboardContent` auf 1 fest (der Standardwert ist 0).

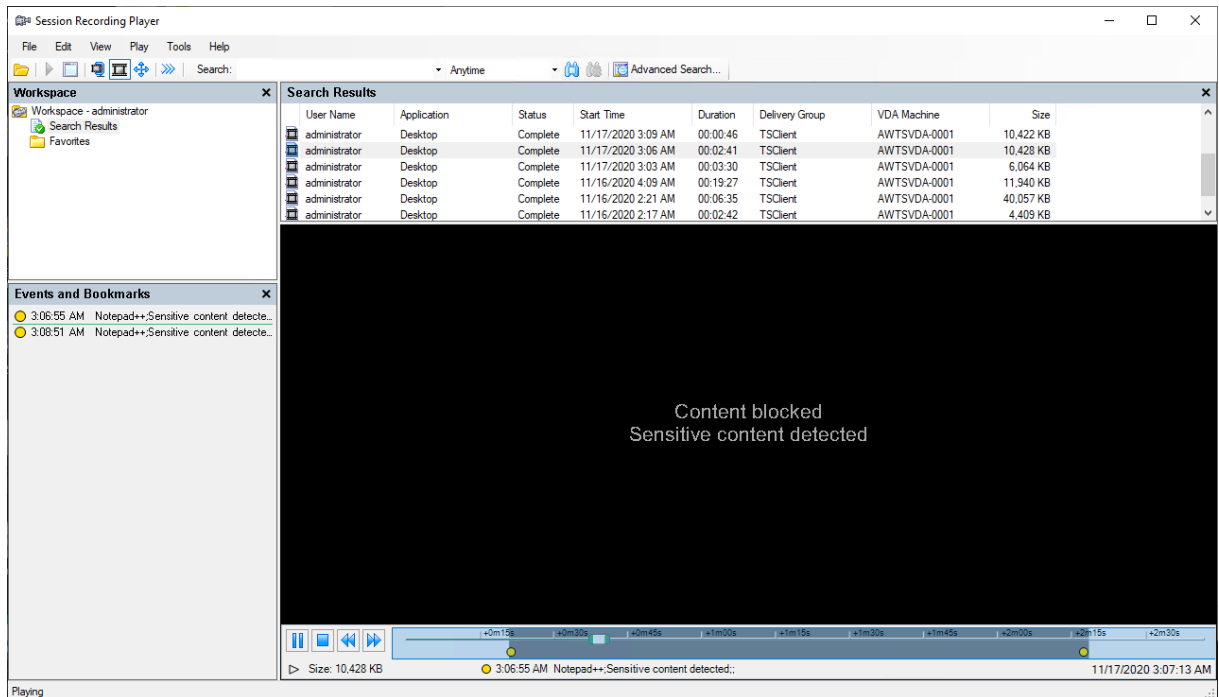


## Benutzerdefinierte Ereignisse

Mit der IUserApi-COM-Schnittstelle im Sitzungsaufzeichnungsagenten können Anwendungen von Drittanbietern anwendungsspezifische Ereignisdaten zu aufgezeichneten Sitzungen hinzufügen. Je nach Ereignisanpassung können vertrauliche Informationen dann in der Sitzungsaufzeichnung blockiert und Ereignisse zur Sitzungspause und Sitzungsfortsetzung entsprechend protokolliert werden.

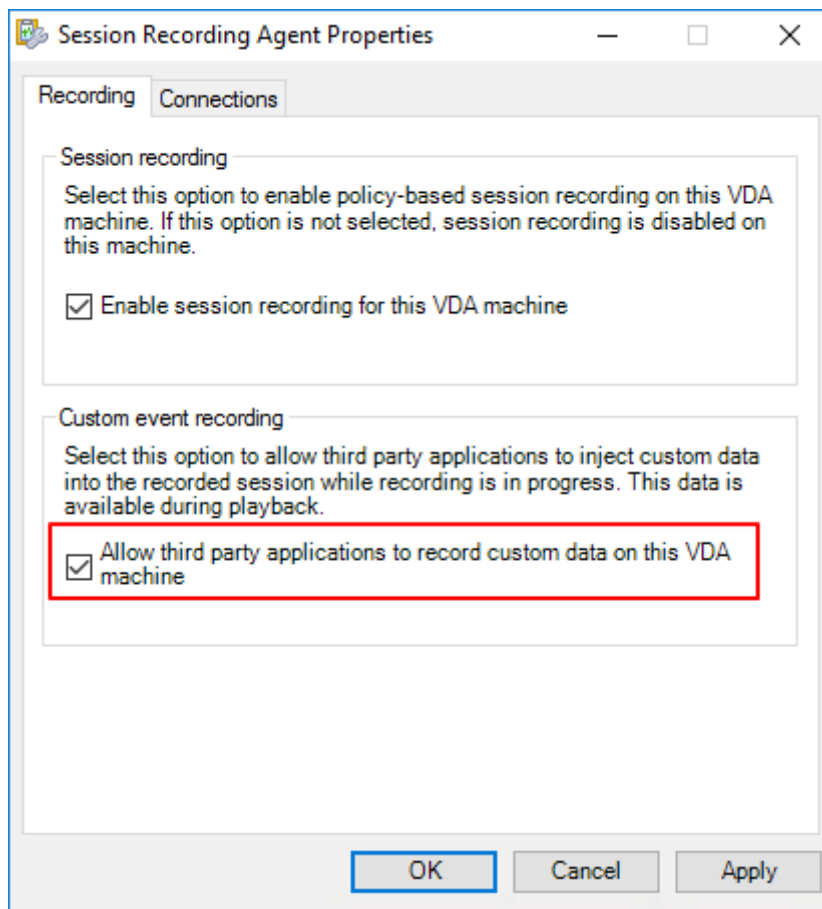
## Blockieren vertraulicher Informationen

Bei der Bildschirmaufzeichnung können Sie bestimmte Zeitabschnitte überspringen und vertrauliche Informationen, die in dieser Zeit angezeigt werden, bei der anschließenden Sitzungswiedergabe blockieren. Für diese Funktion benötigen Sie die Sitzungsaufzeichnung 2012 und höher.



Führen Sie die folgenden Schritte aus, um die Funktion zu nutzen:

1. Aktivieren Sie unter **Sitzungsaufzeichnungsagent - Eigenschaften** das Kontrollkästchen **Anwendungen von Dritten können benutzerdefinierte Daten auf dieser VDA-Maschine aufzeichnen** und klicken Sie auf **Übernehmen**.

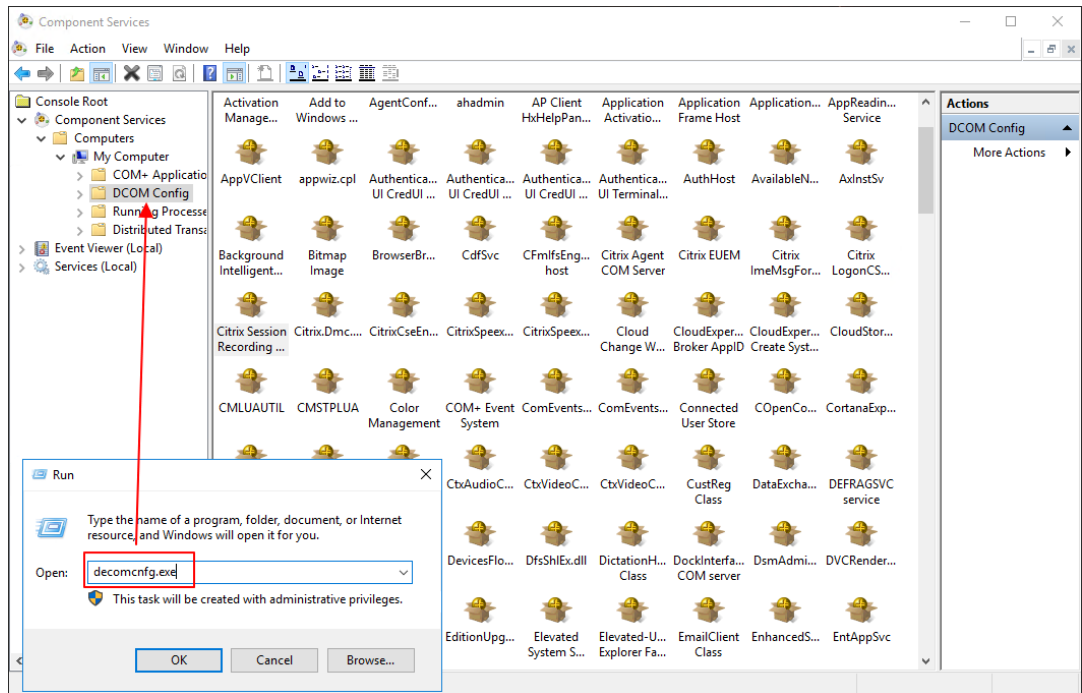


2. Gewähren Sie Benutzern die Berechtigung zum Aufrufen der Sitzungsaufzeichnungs-Ereignis-API (IUserApi-COM-Schnittstelle).

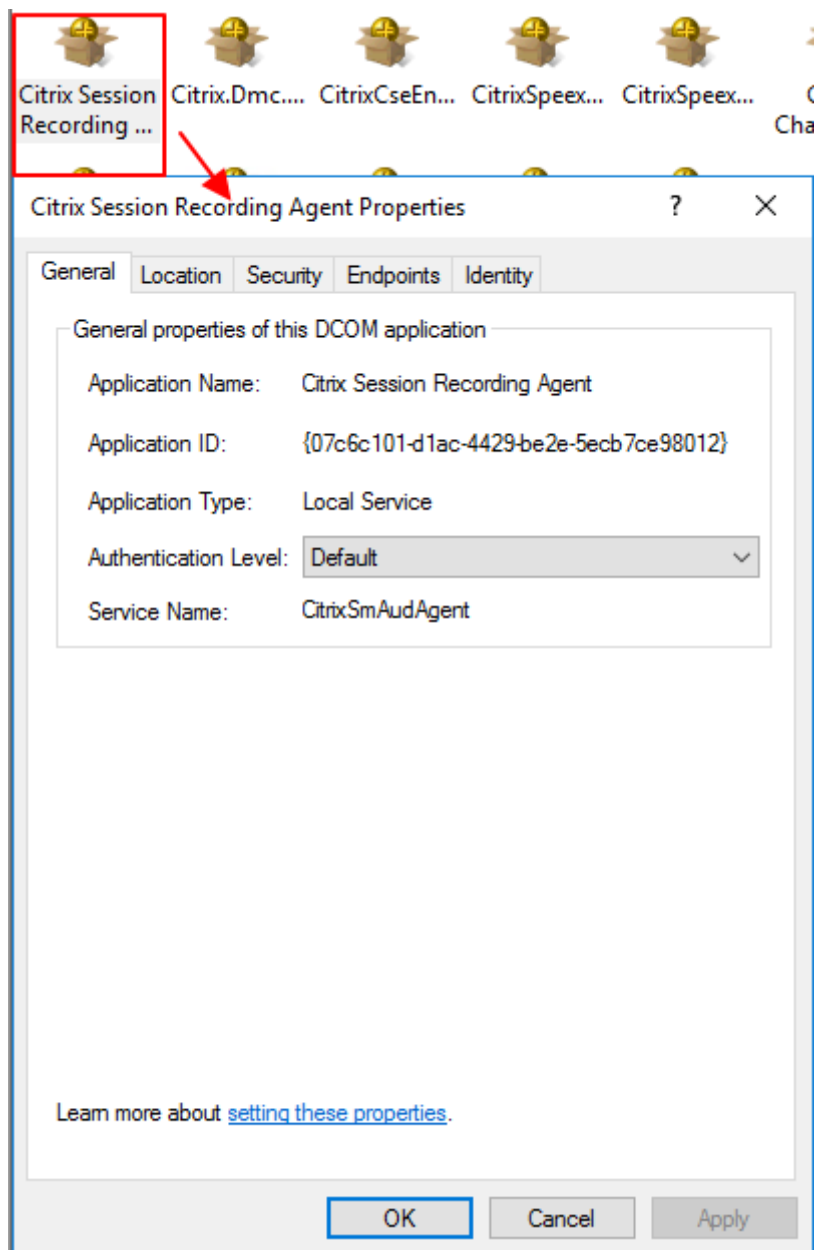
Die Zugriffssteuerung der Ereignis-API-COM-Schnittstelle wurde der Sitzungsaufzeichnung in Version 7.15 hinzugefügt. Nur autorisierte Benutzer können mit dieser Funktionalität Ereignismetadaten in eine Aufzeichnung einfügen.

Lokalen Administratoren wird diese Berechtigung standardmäßig erteilt. Um anderen Benutzern diese Berechtigung zu erteilen, verwenden Sie das Windows DCOM-Konfigurationstool:

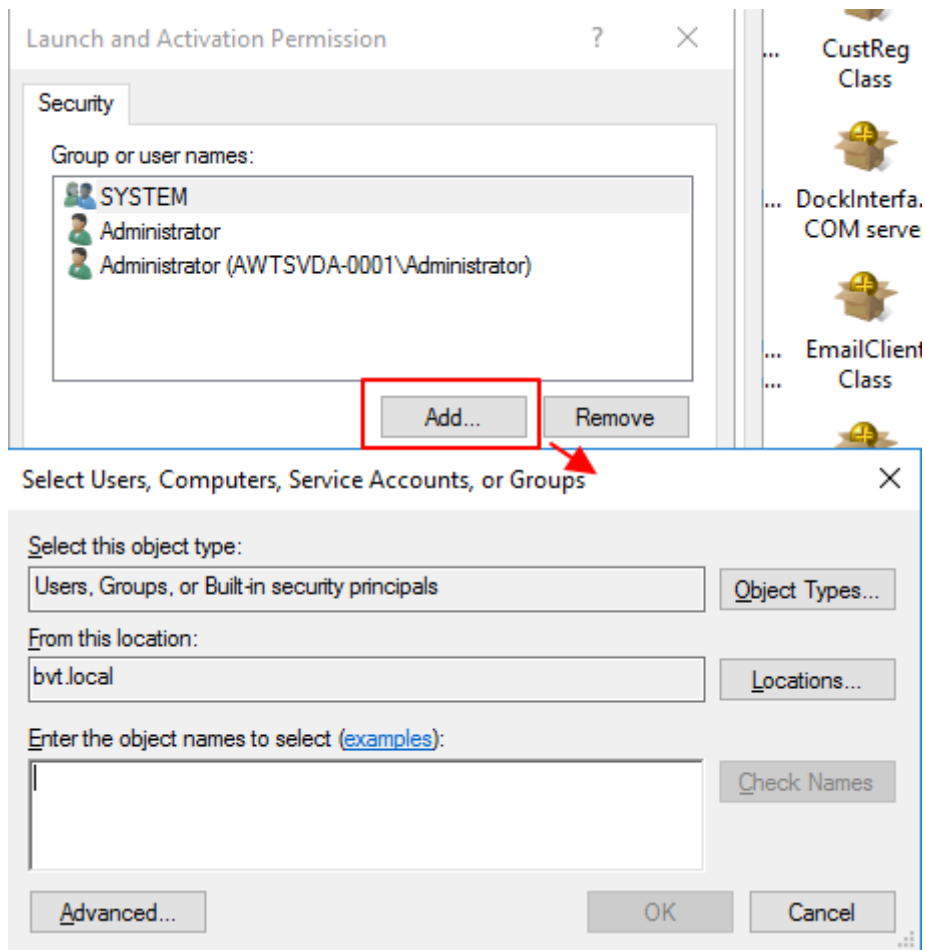
- a) Öffnen Sie das Windows DCOM-Konfigurationstool im Sitzungsaufzeichnungsagenten durch Ausführen von `dcomcnfg.exe`.



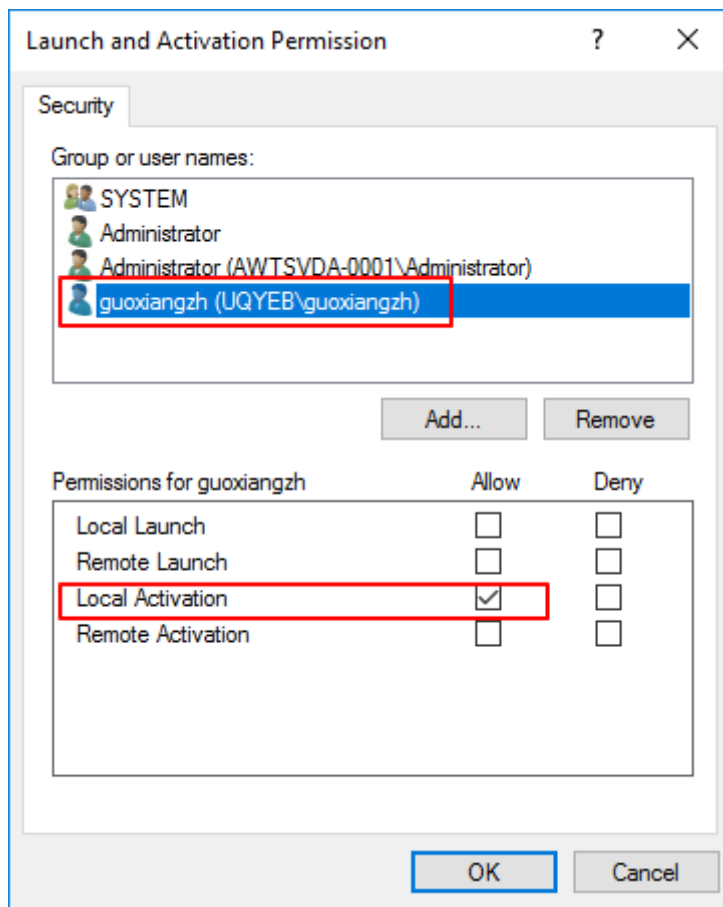
- b) Klicken Sie mit der rechten Maustaste auf **Citrix Sitzungsaufzeichnungsagent** und wählen Sie **Eigenschaften**.



- c) Wählen Sie die Registerkarte **Sicherheit** und klicken Sie auf **Bearbeiten**, um Benutzer mit der Berechtigung **Lokale Aktivierung** im Abschnitt **Start- und Aktivierungsberechtigungen** hinzuzufügen.







**Hinweis:**

Die DCOM-Konfiguration wird sofort wirksam. Es ist nicht notwendig, Dienste oder die Maschine neu zu starten.

3. Starten Sie eine virtuelle Citrix-Sitzung.
4. Starten Sie PowerShell und ändern Sie das aktuelle Laufwerk in den Ordner **<Sitzungsaufzeichnungsagent-Installationspfad>\Bin**, um das Modul SRUserEventHelperSnapin.dll zu importieren.
5. Führen Sie die Cmdlets `Session-Pause` und `Session-Resume` aus, um Parameter festzulegen, mit denen vertrauliche Informationen blockiert werden.

Parameter	Beschreibung	Erforderlich oder optional
-APP	Der App-Name, der das Cmdlet aufruft.	Erforderlich

Parameter	Beschreibung	Erforderlich oder optional
-Reason	Der Grund, warum der Inhalt blockiert wird. Wenn Sie diesen Parameter nicht festlegen, wird die Standardeinstellung angezeigt: <b>Inhalt blockiert und Vorhandener sensibler Inhalt wird blockiert</b> . Wenn Sie diesen Parameter festlegen, wird der von Ihnen angegebene Grund angezeigt, wenn Sie bei der Sitzungswiedergabe zum blockierten Zeitabschnitt navigieren.	Optional

Sie können beispielsweise `Session-Pause` ausführen, wie im folgenden Beispiel:

```

Select Administrator: PowerShell
PS C:\Program Files\Citrix\SessionRecording\Agent\Bin> man Session-Pause

NAME
    Session-Pause

SYNOPSIS
    Session-Pause [-App] <string> [[-Reason] <string>] [<CommonParameters>]

SYNTAX
    Session-Pause [-App] <string> [[-Reason] <string>] [<CommonParameters>]

DESCRIPTION
    User can use it to pause current session.

RELATED LINKS

REMARKS
    To see the examples, type: "get-help Session-Pause -examples".
    For more information, type: "get-help Session-Pause -detailed".
    For technical information, type: "get-help Session-Pause -full".

PS C:\Program Files\Citrix\SessionRecording\Agent\Bin> Session-Pause -App Notepad++ -Reason 'Sensitive content detected'
Getting type from local machine...
Creating instance...
Querying IUserApi interface...
*** Connected ***

Formatting data for send...
Calling IUserApi.LogDataWithExtData...
*** Call Success ***
PS C:\Program Files\Citrix\SessionRecording\Agent\Bin>
    
```

## Suchen nach und Wiedergeben von Aufzeichnungen mit markierten Ereignissen

### Suchen nach Aufzeichnungen mit markierten Ereignissen

Im Sitzungsaufzeichnungsplayer können Sie erweiterte Suchen nach Aufzeichnungen mit markierten Ereignissen durchführen.

1. Klicken Sie im Sitzungsaufzeichnungsplayer auf der Symbolleiste auf **Erweiterte Suche** oder wählen Sie auf der Symbolleiste **Extras > Erweiterte Suche**.
2. Legen Sie die Suchkriterien im Dialogfeld **Erweiterte Suche** fest.

Auf der Registerkarte **Ereignisse** können Sie markierte Ereignisse in Sitzungen nach **Ereignistext** und nach **Ereignistyp** oder beiden suchen. Sie können die Filter **Ereignisse**, **Allgemein**, **Datum/Uhrzeit** und **Andere** in Kombination verwenden, um nach Aufzeichnungen zu suchen, die Ihren Kriterien entsprechen.

Advanced Search

Saved Searches... Save As... Reset Values

Search Criteria

Common Date/Time Events Other

Citrix-defined events and events inserted by third-party applications can be tagged while a session is being recorded. To search for recordings with target events tagged, set the search criteria below.

Event text:

Event type:

- Citrix.EventMonitor.AppEnd
- Citrix.EventMonitor.AppStart
- Citrix.EventMonitor.CDMUSBDriveAttach
- Citrix.EventMonitor.Clipboard
- Citrix.EventMonitor.FileCreate
- Citrix.EventMonitor.FileDelete
- Citrix.EventMonitor.FileMove
- Citrix.EventMonitor.FileRename
- Citrix.EventMonitor.GenericUSBDriveAttach
- Citrix.EventMonitor.TopMost
- Citrix.EventMonitor.WebBrowsing
- Citrix.UserApi.SessionPause
- Citrix.UserApi.SessionResume
- Any Citrix-defined event

Query Builder

Find the 200 most relevant re...

Search Stop Close

#### Hinweis:

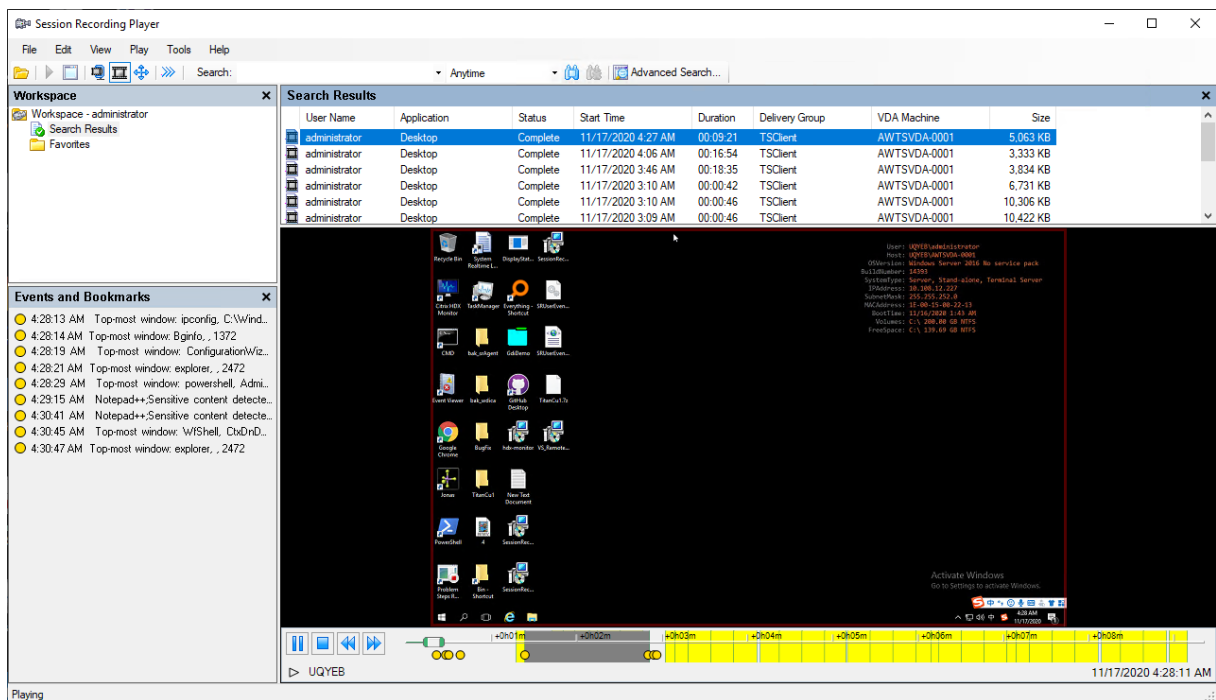
- Die Liste **Ereignistyp** zeigt alle Ereignistypen an, die von der Citrix Sitzungsaufzeichnung

protokolliert wurden. Sie können für die Suche einen beliebigen Ereignistyp auswählen. Wenn Sie **Jedes von Citrix definierte Ereignis** auswählen, wird nach allen Aufzeichnungen mit Ereignissen gesucht, die von der Citrix Sitzungsaufzeichnung protokolliert wurden.

- Der Filter **Ereignistext** unterstützt teilweise Übereinstimmungen. Platzhalter werden nicht unterstützt.
- Bei dem Filter **Ereignistext** spielt die Groß-/Kleinschreibung keine Rolle.
- Für den Ereignistyp werden die Wörter **App Start**, **App End**, **Client drive mapping** und **File Rename** nicht berücksichtigt, wenn Sie nach **Ereignistext** suchen. Daher wird keine Entsprechung gefunden, wenn Sie **App Start**, **App End**, **Client drive mapping** oder **File Rename** in das Feld **Ereignistext** eingeben.

### Wiedergeben von Aufzeichnungen mit markierten Ereignissen

Wenn Sie eine Aufzeichnung mit Ereignissen wiedergeben sind die Ereignisse im Bereich **Ereignisse und Textmarken** sichtbar und werden im unteren Teil des Sitzungsaufzeichnungsplayers als gelbe Punkte angezeigt:



Sie können mit Ereignissen durch eine aufgezeichnete Sitzung navigieren oder zu den Punkten springen, an denen die Ereignisse markiert sind.

## Anzeigen von Aufzeichnungen

June 21, 2021

Mit dem Sitzungsaufzeichnungsplayer zeigen Sie aufgezeichnete Citrix Virtual Apps and Desktops-Sitzungen an, suchen die Sitzungsaufzeichnungsdateien und fügen Textmarken hinzu.

Wenn Sitzungen mit aktiviertem Liveplayback aufgezeichnet werden, können Sie aktuell ausgeführte Sitzungen mit einer Verzögerung von ein bis zwei Sekunden anzeigen.

Sitzungen, die länger als die vom Sitzungsaufzeichnungsadministrator festgelegten Höchstwerte sind oder deren Dateigröße das Limit übersteigt, werden in mehreren Sitzungsdateien aufgezeichnet.

### Hinweis:

Ein Sitzungsaufzeichnungsadministrator muss Benutzern Berechtigung für den Zugriff auf aufgezeichnete VDA-Sitzungen erteilen. Wenden Sie sich an den Sitzungsaufzeichnungsadministrator, wenn Sie nicht auf Sitzungsaufzeichnungen zugreifen können.

Bei der Installation des Sitzungsaufzeichnungsplayers richtet der Administrator normalerweise die Verbindung zwischen dem Player und einem Sitzungsaufzeichnungsserver ein. Wenn die Verbindung nicht eingerichtet ist, müssen Sie die Verbindung beim ersten Suchen nach Dateien angeben. Weitere Informationen zum Einrichten der Verbindung erhalten Sie vom Sitzungsaufzeichnungsadministrator.

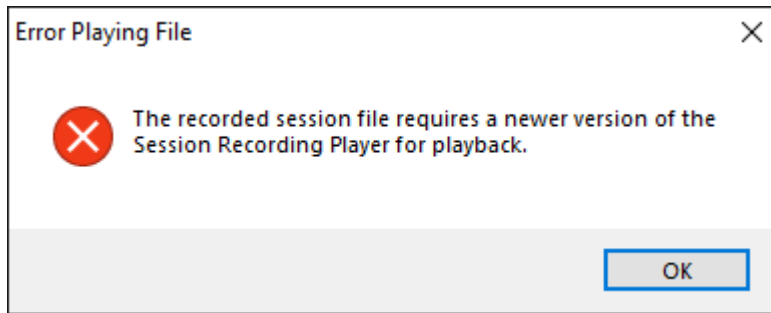
## Starten des Sitzungsaufzeichnungsplayers

January 15, 2024

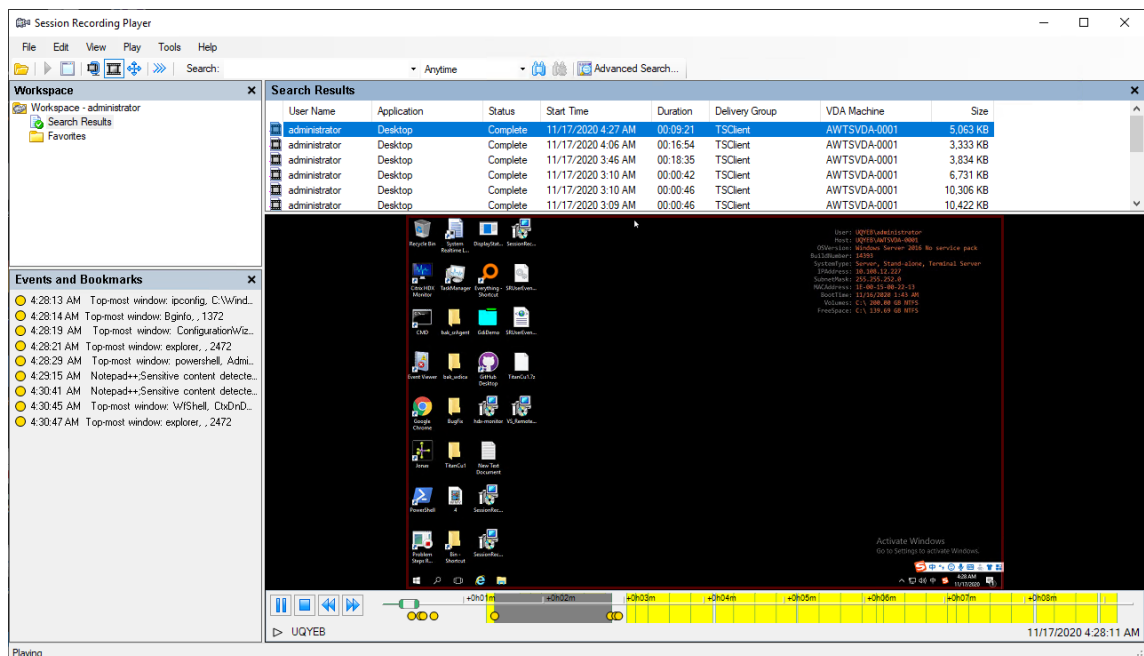
### Starten des Sitzungsaufzeichnungsplayers

#### Hinweis:

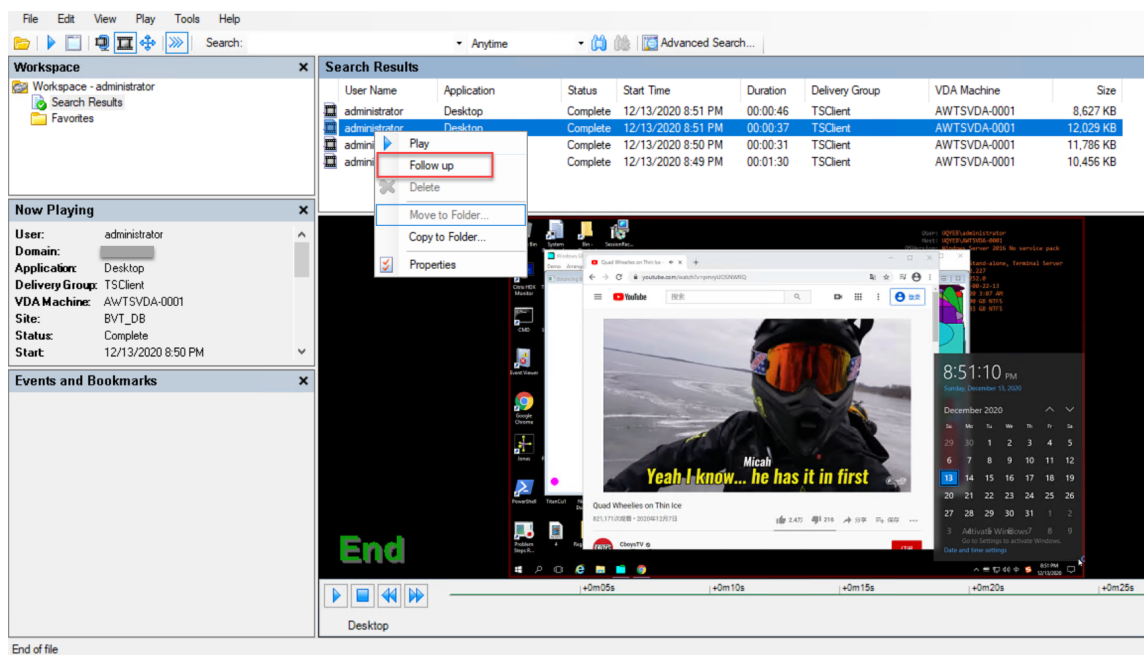
- Wenn eine Aufzeichnung blockierte Inhalte enthält, werden diese bei Wiedergabe der Sitzungsaufzeichnung übersprungen. Wenn Sie jedoch zum blockierten Zeitabschnitt navigieren, wird ein schwarzer Bildschirm mit einer Meldung, dass der Inhalt blockiert ist, angezeigt. Für diese Funktion benötigen Sie die Sitzungsaufzeichnung 2012 und höher.
- Wenn Sie zur Aufzeichnungswiedergabe den Sitzungsaufzeichnungsplayer 2009 und früher verwenden, wird folgende Fehlermeldung angezeigt. Der Webplayer ist nicht betroffen.



1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**. Der Sitzungsaufzeichnungsplayer wird angezeigt.



Um alle Aufzeichnungsdateien einer aufgezeichneten Sitzung anzuzeigen, klicken Sie mit der rechten Maustaste auf eine Aufzeichnung in der Liste und wählen Sie **Nachverfolgen**.



## Ausblenden oder Einblenden der Fensterelemente

Der Sitzungsaufzeichnungsplayer hat Fensterelemente, die Sie ein- und ausblenden können.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der **Sitzungsaufzeichnungsplayer**-Menüleiste auf **Ansicht**.
4. Wählen Sie die Elemente aus, die Sie anzeigen möchten. Bei der Auswahl eines Elements wird es sofort angezeigt. Ein Häkchen gibt die Auswahl des Elements an.

## Verbinden mit dem gewünschten Sitzungsaufzeichnungsserver

Wenn der Administrator eine Verbindung mit mehreren Sitzungsaufzeichnungsservern im Sitzungsaufzeichnungsplayer ermöglicht hat, können Sie den Server wählen, mit dem der Player eine Verbindung herstellen soll. Der Sitzungsaufzeichnungsplayer kann nur jeweils eine Verbindung mit einem Sitzungsaufzeichnungsserver herstellen.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Extras > Optionen > Verbindungen**.

4. Wählen Sie den Sitzungsaufzeichnungsserver aus, mit dem Sie eine Verbindung herstellen möchten.

## Aktivieren und Deaktivieren von Livesitzungswiedergabe und Wiedergabeschutz

June 21, 2021

### Aktivieren oder Deaktivieren der Wiedergabe von Livesitzungen

Wenn Sitzungen mit aktivierter Livewiedergabefunktion aufgezeichnet werden, können Sie eine Sitzung nach oder während der Aufzeichnung anzeigen. Das Anzeigen einer Sitzung, die gerade aufgezeichnet wird, ähnelt dem Anzeigen von Live-Aktionen. Es gibt jedoch eine Verzögerung von 1-2 Sekunden, wenn die Daten vom VDA übertragen werden.

Einige Funktionen stehen nicht zur Verfügung, wenn Sie Sitzungen anzeigen, deren Aufzeichnung noch nicht abgeschlossen ist:

- Eine digitale Signatur kann erst nach dem Abschluss der Aufzeichnung zugewiesen werden. Wenn die digitale Signatur aktiviert ist, können Sie Live-Wiedergabesitzungen anzeigen. Sie sind jedoch nicht digital signiert und Sie können die Zertifikate erst anzeigen, wenn die Sitzung abgeschlossen ist.
- Der Wiedergabeschutz kann erst nach dem Abschluss der Aufzeichnung angewendet werden. Wenn der Wiedergabeschutz aktiviert ist, können Sie Live-Wiedergabesitzungen anzeigen. Sie werden jedoch erst verschlüsselt, wenn die Sitzung abgeschlossen ist.
- Eine Datei kann erst nach dem Abschluss der Aufzeichnung zwischengespeichert werden.

In der Standardeinstellung ist die Wiedergabe von Livesitzungen aktiviert.

1. Melden Sie sich bei dem Computer mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Wiedergabe**.
4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Wiedergabe von Livesitzungen zulassen**.



## Aktivieren oder Deaktivieren des Wiedergabeschutzes

Als Sicherheitsmaßnahme werden Aufzeichnungsdateien, die zum Anzeigen im Sitzungsaufzeichnungsplayer heruntergeladen werden, automatisch von der Sitzungsaufzeichnung verschlüsselt. Dieser Wiedergabeschutz stellt sicher, dass die Dateien nur von dem Benutzer, der die Datei heruntergeladen hat, und nicht von anderen Benutzern kopiert oder angezeigt werden können. Die Wiedergabe der Dateien kann nicht auf einer anderen Arbeitsstation oder von einem anderen Benutzer durchgeführt werden. Verschlüsselte Dateien haben die Erweiterung `.icle`. Unverschlüsselte Dateien haben die Erweiterung `.icl`. Die Dateien bleiben verschlüsselt, wenn sie unter `%localAppData%\Citrix\SessionRecording\Player\Cache` des Sitzungsaufzeichnungsplayers sind, bis ein autorisierter Benutzer sie öffnet.

Wir empfehlen, HTTPS für den Schutz der übermittelten Daten zu verwenden.

In der Standardeinstellung ist der Wiedergabeschutz aktiviert.

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsserver - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Wiedergabe**.
4. Aktivieren Sie das Kontrollkästchen **Für die Wiedergabe heruntergeladene Sitzungsaufzeichnungsdateien verschlüsseln** oder heben Sie die Markierung auf.

## Öffnen und Wiedergeben von Aufzeichnungen

January 15, 2024

### Öffnen von Aufzeichnungen

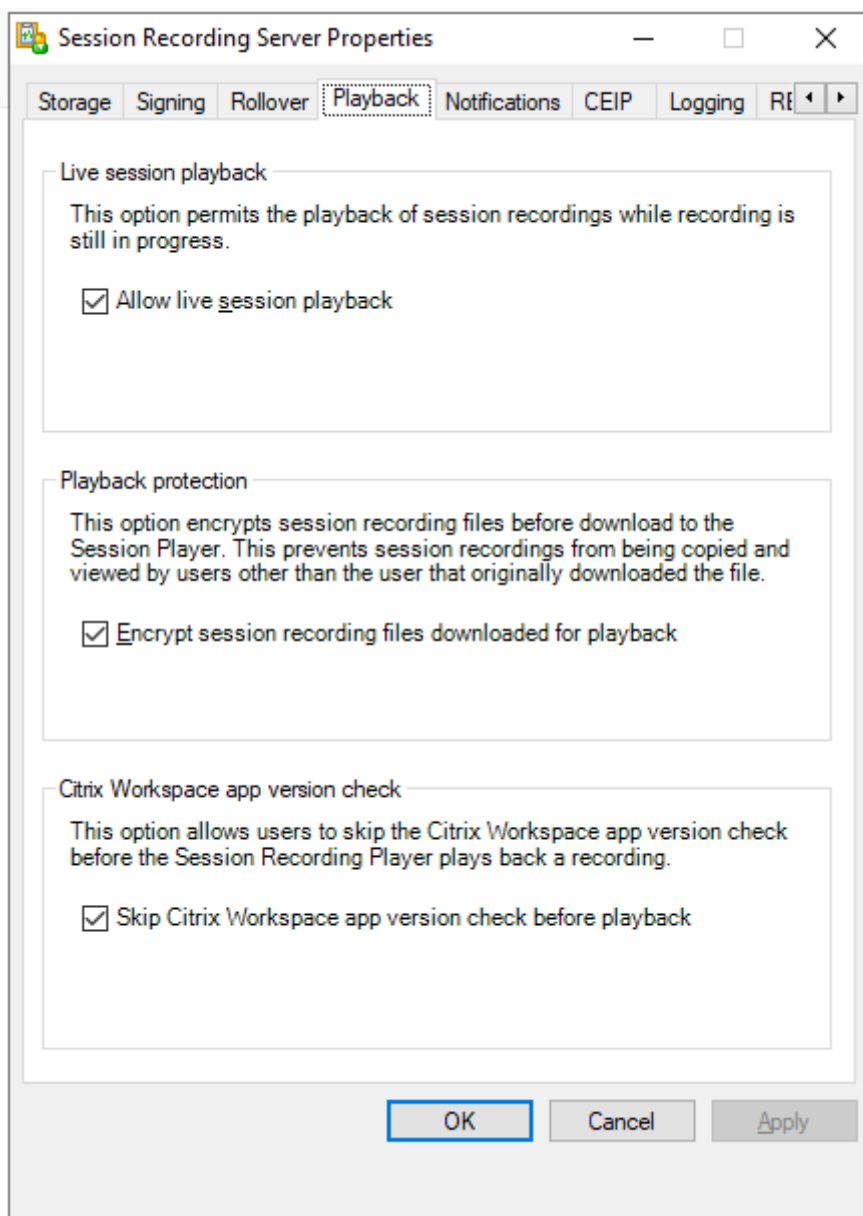
Sie öffnen Sitzungsaufzeichnungen im Sitzungsaufzeichnungsplayer auf dreierlei Weise:

- Führen Sie eine Suche mit dem Sitzungsaufzeichnungsplayer durch. Sitzungsaufzeichnungen, die die Suchkriterien erfüllen, werden im Bereich der Suchergebnisse angezeigt.
- Greifen Sie auf Sitzungsaufzeichnungsdateien direkt von der lokalen Festplatte oder einem freigegebenen Laufwerk zu.
- Greifen Sie auf Sitzungsaufzeichnungsdateien vom Ordner "Favoriten" zu

Beim Öffnen einer Datei, die ohne digitale Signatur aufgezeichnet wurde, werden Sie in einer Warnmeldung darauf hingewiesen, dass Ursprung und Integrität der Datei nicht geprüft werden konnten.

Bestätigen Sie die Warnmeldung mit **Ja** und öffnen Sie die Datei, wenn Sie hinsichtlich der Integrität der Datei keine Bedenken haben.

Vor der Aufzeichnungswiedergabe wird vom Sitzungsaufzeichnungsplayer die Version der Citrix Workspace-App überprüft. Wenn die Datei mit einer Version der Citrix Workspace-App aufgezeichnet wurde, die vom Player nicht unterstützt wird, wird ein Fehler zurückgegeben. Um den Fehler zu umgehen, wählen Sie vor der Wiedergabe in **Sitzungsaufzeichnungsserver - Eigenschaften** die Option **Versionsprüfung der Citrix Workspace-App**.

**Hinweis:**

Die Administratorprotokollierung der Sitzungsaufzeichnung ermöglicht die Protokollierung der

Downloads von Sitzungsaufzeichnungen im Sitzungsaufzeichnungsplayer. Weitere Informationen finden Sie unter [Administratorprotokollierung](#).

### Öffnen einer Aufzeichnung im Bereich der Suchergebnisse

1. Melden Sie sich bei der Maschine an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Führen Sie eine Schnellsuche durch.
4. Wenn der Bereich mit den Suchergebnissen nicht sichtbar ist, wählen Sie **Suchergebnisse** im Arbeitsbereich.
5. Wählen Sie im Suchergebnisbereich die Sitzung aus, die Sie wiedergeben möchten.
6. Führen Sie einen der folgenden Schritte aus:
  - Doppelklicken Sie auf die Sitzung.
  - Klicken Sie mit der rechten Maustaste und wählen Sie **Wiedergeben**.
  - Klicken Sie auf der **Sitzungsaufzeichnungsplayer**-Menüleiste auf **Wiedergabe > Wiedergabe**.

### Öffnen einer Aufzeichnung durch Zugriff auf die Datei

Der Name von Sitzungsaufzeichnungsdateien beginnt mit **i\_** gefolgt von einer eindeutigen alphanumerischen Datei-ID und der Dateierweiterung **.icl** oder **.icle**. Die Erweiterung **.icl** kennzeichnet Aufnahmen ohne Wiedergabeschutz. Die Erweiterung **.icle** kennzeichnet Aufnahmen mit Wiedergabeschutz. Sitzungsaufzeichnungsdateien werden in einem Ordner gespeichert, der das Datum der Sitzungsaufzeichnung enthält. Beispiel: Die Datei für eine Sitzung, die am 22. Dezember 2014 aufgezeichnet wurde, wird im Ordnerpfad 2014\12\22 gespeichert.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Führen Sie einen der folgenden Schritte aus:
  - Wählen Sie auf der **Sitzungsaufzeichnungsplayer**-Menüleiste **Datei > Öffnen** und navigieren Sie zu der Datei.
  - Navigieren Sie mit dem Windows-Explorer auf die Datei und ziehen Sie sie in das **Player**-Fenster.
  - Navigieren Sie mit dem Windows-Explorer auf die Datei und doppelklicken Sie.
  - Wenn Sie Favoriten im Arbeitsbereich erstellt haben, wählen Sie **Favoriten** und öffnen Sie die Datei im Favoritenbereich auf die gleiche Weise wie Dateien im Suchergebnisbereich.

## Verwenden von Favoriten

Das Erstellen von **Favoriten**-Ordnern ermöglicht den schnellen Zugriff auf oft angezeigte Sitzungsaufzeichnungen. Diese Favoritenordner verweisen auf Sitzungsaufzeichnungsdateien, die auf der Arbeitsstation oder auf einem Netzwerklaufwerk gespeichert sind. Sie können diese Dateien von anderen Arbeitsstationen importieren, zu anderen exportieren und die Ordner für andere Sitzungsaufzeichnungsplayer-Benutzer freigeben.

### Hinweis:

Nur Benutzer mit Zugriffsrechten für den Sitzungsaufzeichnungsplayer können die Sitzungsaufzeichnungsdateien herunterladen, die dem Favoritenordner zugeordnet sind. Wenden Sie sich bezüglich Zugriffsrechten an den Sitzungsaufzeichnungsadministrator.

### Erstellen eines Favoriten-Unterordners

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Wählen Sie im **Sitzungsaufzeichnungsplayer** den Ordner **Favoriten** im Bereich "Arbeitsbereich".
4. Klicken Sie auf der Menüleiste auf **Datei > Ordner > Neuer Ordner**. Ein neuer Ordner wird unter dem Ordner **Favoriten** angezeigt.
5. Geben Sie den Ordnernamen ein und drücken Sie die **Eingabetaste** oder klicken Sie auf eine beliebige Stelle, um den neuen Namen zu übernehmen.

Mit den anderen Optionen im Menü **Datei > Ordner** können Sie die Ordner löschen, umbenennen, verschieben, kopieren, importieren und exportieren.

## Wiedergeben von Aufzeichnungen

Nach dem Öffnen einer aufgezeichneten Sitzung im Sitzungsaufzeichnungsplayer können Sie in der Aufzeichnung folgendermaßen navigieren:

- Mit den Player-Bedienelementen können Sie die Aufzeichnung wiedergeben, anhalten oder stoppen und die Wiedergabegeschwindigkeit erhöhen oder verringern.
- Mit dem Schieberegler für das Positionieren gehen Sie vorwärts oder rückwärts.






Wenn Sie Marker in die Aufzeichnung eingefügt haben, oder die aufgezeichnete Sitzung benutzerdefinierte Ereignisse enthält, können Sie mit diesen Markern oder Ereignissen durch die Sitzungsaufzeichnung navigieren.

**Hinweis:**

- Bei der Wiedergabe einer aufgezeichneten Sitzung wird möglicherweise ein zweiter Mauszeiger angezeigt. Der zweite Mauszeiger wird an der Stelle in der Aufzeichnung angezeigt, an der der Benutzer in Internet Explorer navigiert und auf ein Bild geklickt hat, das im Original größer als der Bildschirm war, das jedoch von Internet Explorer automatisch skaliert wurde. While only one pointer appears during the session, two might appear during playback.
- Diese Version der Sitzungsaufzeichnung unterstützt weder die SpeedScreen-Multimediabeschleunigung noch die Richtlinieneinstellung zum Optimieren der Flash-Inhalte. Wenn diese Option aktiviert ist, wird bei der Wiedergabe ein schwarzes Rechteck angezeigt.
- Beim Aufzeichnen einer Sitzung mit einer Auflösung über 4096 x 4096 ist die Aufzeichnungsanzeige u. U. fragmentiert.

**Verwenden der Player-Bedienelemente**

Sie können auf die Player-Bedienelemente unten im Player-Fenster klicken oder im **Sitzungsaufzeichnungsplayer**-Menü auf **Wiedergabe** klicken.

Player-Bedienelement	Funktion
	Wiedergeben der ausgewählten Sitzungsdatei.
	Anhalten der Wiedergabe.
	Stoppen der Wiedergabe. Wenn Sie auf <b>Stopp</b> und dann auf <b>Wiedergabe</b> klicken, springt die Wiedergabe wieder an den Anfang der Datei.
	Halbieren der momentanen Wiedergabegeschwindigkeit um die Hälfte auf mindestens ein Viertel der Normalgeschwindigkeit.
	Verdoppeln der momentanen Wiedergabegeschwindigkeit auf maximal das 32-fache der Normalgeschwindigkeit.

## Verwenden des Schiebereglers für das Positionieren

Mit dem Schieberegler für das Positionieren unten im Player-Fenster springen Sie auf eine andere Stelle in der aufgezeichneten Sitzung. Sie können den Schieberegler für das Positionieren auf eine Stelle in der Aufzeichnung ziehen, die Sie anzeigen möchten, oder auf eine Stelle auf dem Schieberegler klicken, um auf diese Stelle zu gehen.

Sie können den Schieberegler für das Positionieren auch mit den folgenden Tasten auf der Tastatur steuern:

---

Tastaturtaste	Funktion
Pos1	An den Anfang positionieren.
Ende	An das Ende positionieren.
Nach-Rechts-Taste	Fünf Sekunden vorwärts positionieren.
Nach-Links-Taste	Fünf Sekunden rückwärts positionieren.
Mausrad eine Kerbe nach unten bewegen	15 Sekunden vorwärts positionieren.
Mausrad eine Kerbe nach oben bewegen	15 Sekunden rückwärts positionieren.
Strg + Nach-Rechts-Taste	30 Sekunden vorwärts positionieren.
Strg + Nach-Links-Taste	30 Sekunden rückwärts positionieren.
Bild ab	Eine Minute vorwärts positionieren.
Bild auf	Eine Minute rückwärts positionieren.
Strg + Mausrad eine Kerbe nach unten bewegen	90 Sekunden vorwärts positionieren.
Strg + Mausrad eine Kerbe nach oben bewegen	90 Sekunden rückwärts positionieren.
Strg + Bild-Ab	Sechs Minuten vorwärts positionieren.
Strg + Bild-Auf	Sechs Minuten rückwärts positionieren.

---

Klicken Sie im Menü des **Sitzungsaufzeichnungsplayers** auf **Extras > Optionen > Player** und verschieben Sie den Schieberegler, um die Reaktionszeit des Schiebereglers zu verlängern oder zu verkürzen. Für eine schnellere Reaktionszeit wird mehr Speicher benötigt. Die Reaktion kann, abhängig von der Größe der Aufzeichnungen und der Computerhardware, langsam sein.

## Ändern der Wiedergabegeschwindigkeit

Sie können die Wiedergabe aufgezeichneter Sitzungen im Sitzungsaufzeichnungsplayer in exponentiellen Erhöhungen von einem Viertel der normalen Wiedergabegeschwindigkeit bis zum 32-fachen der normalen Wiedergabegeschwindigkeit einstellen.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der **Sitzungsaufzeichnungsplayer**-Menüleiste auf **Wiedergabe** > **Wiedergabegeschwindigkeit**.
4. Wählen Sie eine Geschwindigkeitsoption.

Die Geschwindigkeit wird sofort geändert. Text, der die exponentielle Rate angibt, wird unten im Player-Fenster kurz in Grün angezeigt.

### **Hervorheben von Leerlaufperioden in aufgezeichneten Sitzungen**

Leerlaufperioden sind die Teile einer aufgezeichneten Sitzung, in denen keine Aktion stattfindet. Der Sitzungsaufzeichnungsplayer kann Leerlaufperioden in aufgezeichneten Sitzungen bei der Wiedergabe hervorheben. Die Standardeinstellung ist **Ein**. Weitere Informationen finden Sie unter Hervorheben von [Leerlaufperioden](#).

### **Überspringen von Stellen ohne Aktionen**

Im Schnellprüfmodus überspringt der Sitzungsaufzeichnungsplayer die Teile von aufgezeichneten Sitzungen, in denen keine Aktion stattfindet. Mit dieser Einstellung sparen Sie Zeit bei der Wiedergabe. Animierte Folgen werden jedoch nicht übersprungen, z. B. ein animierter Mauszeiger, blinkende Cursor oder angezeigte Uhren, bei denen sich die zweite Hand bewegt.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie im Menü des **Sitzungsaufzeichnungsplayers** auf **Wiedergabe** > **Schnellprüfmodus**.

Sie können die Option aktivieren oder deaktivieren. Bei jeder Auswahl wird der Status kurz in grün im Player -Fenster angezeigt.

### **Ändern der Wiedergabeanzeige**

Mit Optionen können Sie ändern, wie die aufgezeichneten Sitzungen im Player-Fenster angezeigt werden. Sie können das Bild mit Panning und Skalieren ändern, die Wiedergabe im Vollbild anzeigen, das Player-Fenster in einem eigenen Fenster und einen Rahmen um die Sitzungsaufzeichnung anzeigen, um sie vom Hintergrund des Player-Fensters zu unterscheiden.

### **Anzeigen des Player-Fensters im Vollbild**

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie im Menü des **Sitzungsaufzeichnungsplayers** auf **Ansicht > Player-Vollbild**.
4. Drücken Sie **ESC** oder **F11**, um die Originalgröße des Fensters wieder herzustellen.

### **Anzeigen des Player-Fensters in einem eigenen Fenster**

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie im Menü des **Sitzungsaufzeichnungsplayers** auf **Ansicht > Player in neuem Fenster**. Ein neues Fenster wird mit dem Player-Fenster angezeigt. Sie können das Fenster ziehen und seine Größe ändern.
4. Wenn Sie das Player-Fenster im Hauptfenster einbetten möchten, wählen Sie **Ansicht > Player in neuem Fenster** oder drücken Sie **F10**.

### **Skalieren der Sitzungswiedergabe auf die Größe des Player-Fensters**

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie im Menü des **Sitzungsaufzeichnungsplayers** auf **Wiedergabe > Panning und Skalieren > Passend skalieren**.
  - **Bei Passend skalieren (Schnellrendering)** wird das Bild verkleinert, die Bildqualität ist jedoch noch gut. Bilder werden schneller als mit der Option “Passend skalieren (hohe Qualität)” aufgebaut, die Bilder und der Text sind jedoch nicht scharf. Verwenden Sie diese Option, wenn Sie Leistungsprobleme mit der Option “Passend skalieren (hohe Qualität)” feststellen.
  - **Bei Passend skalieren (hohe Qualität)** wird das Bild verkleinert, die Qualität ist sehr gut. Bei dieser Option werden die Bilder möglicherweise langsamer als bei der Option “Passend skalieren (Schnellrendering)” aufgebaut.

### **Durchführen von Panning des Bilds**

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.



3. Klicken Sie im Menü des **Sitzungsaufzeichnungsplayers** auf **Wiedergabe > Panning und Skalieren > Panning**. Der Mauszeiger nimmt Handform an. Eine kleine Darstellung des Bildschirms wird oben rechts im Playerfenster angezeigt.
4. Ziehen Sie das Bild. Die kleine Bildschirmdarstellung zeigt an, wo Sie sich im Bild befinden.
5. Um das Verschieben zu stoppen, wählen Sie eine der Skalierungsoptionen.

### Anzeigen eines roten Rahmens um die Sitzungsaufzeichnung

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Extras > Optionen > Player**.
4. Aktivieren Sie das Kontrollkästchen **Rahmen um Sitzungsaufzeichnung anzeigen**.  
Ist **Rahmen um Sitzungsaufzeichnung anzeigen** nicht aktiviert, können Sie den roten Rahmen vorübergehend anzeigen, indem Sie die linke Maustaste gedrückt halten, wenn der Zeiger im Player-Fenster ist.

### Hervorheben von Leerlaufperioden

June 21, 2021

Leerlaufperioden sind die Teile einer aufgezeichneten Sitzung, in denen keine Aktion stattfindet. Der Sitzungsaufzeichnungsplayer kann Leerlaufperioden in aufgezeichneten Sitzungen bei der Wiedergabe hervorheben. Die Standardeinstellung ist **Ein**.

**Hinweis:** Bei der Wiedergabe aktiver Sitzungen werden Leerlaufperioden nicht hervorgehoben.

Mit diesen Schritten heben Sie Leerlaufperioden in aufgezeichneten Sitzungen hervor:

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie in der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Ansicht > Leerlauf** und aktivieren oder deaktivieren Sie das Kontrollkästchen.

### Zwischenspeichern von Aufzeichnungen

November 5, 2021

Bei jedem Öffnen einer Sitzungsaufzeichnungsdatei lädt der Sitzungsaufzeichnungsplayer die Datei vom Speicherort herunter, auf dem die Aufzeichnungen gespeichert sind. Wenn Sie dieselben Dateien oft herunterladen, sparen Sie Zeit, wenn Sie die Dateien auf der Arbeitsstation zwischenspeichern. Zwischengespeicherte Dateien werden auf der Arbeitsstation in diesem Ordner gespeichert:

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

Sie können die verwendete Cachegröße angeben. Wenn die Aufzeichnungen den angegebenen Speicherplatz auf der Festplatte vollständig belegen, löscht die Sitzungsaufzeichnung die ältesten und am wenigsten verwendeten Aufzeichnungen, um Platz für neue Aufzeichnungen zu machen. Sie können den Cache jederzeit leeren, um freien Speicherplatz auf der Festplatte zu erhalten.

### Aktivieren der Zwischenspeicherung

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Extras > Optionen > Cache**.
4. Aktivieren Sie das Kontrollkästchen **Heruntergeladene Dateien lokal zwischenspeichern**.
5. Zum Beschränken des für die Zwischenspeicherung verwendeten Speicherplatzes auf dem Datenträger aktivieren Sie das Kontrollkästchen **Verwendeten Speicherplatz auf Datenträger beschränken**, und geben Sie den Speicherplatz in MB an.
6. Klicken Sie auf **OK**.

### Leeren des Cache

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Extras > Optionen > Cache**.
4. Aktivieren Sie das Kontrollkästchen **Heruntergeladene Dateien lokal zwischenspeichern**.
5. Klicken Sie im Sitzungsaufzeichnungsplayer auf **Extras > Optionen > Cache**.
6. Klicken Sie auf **Cache löschen** und dann zur Bestätigung auf **OK**.

### Verwenden von Ereignissen und Textmarken

June 21, 2021

Ereignisse und Textmarken erleichtern das Navigieren in aufgezeichneten Sitzungen.

Citrix definierte Ereignisse werden bei der Sitzungsaufzeichnung in Sitzungen eingefügt. Sie können mit der Ereignis-API und einer Anwendung eines Drittanbieters auch benutzerdefinierte Ereignisse einfügen. Ereignisse werden als Teil der Sitzungsdatei gespeichert. Sie können mit dem Sitzungsaufzeichnungsplayer nicht gelöscht oder geändert werden.

Textmarken sind Marker, die Sie während der Sitzungswiedergabe mit dem Sitzungsaufzeichnungsplayer in Sitzungsaufzeichnungen einfügen. Textmarken werden der aufgezeichneten Sitzung zugeordnet, bis sie gelöscht werden. Sie werden jedoch nicht mit der Sitzungsdatei gespeichert, sondern als eigene `.icl`-Datei im Cacheordner **Bookmarks** auf dem Sitzungsaufzeichnungsplayer gespeichert (Beispiel: C:\Users\SpecificUser\AppData\Local\Citrix\SessionRecording\Player\Bookmarks). Der Name ist mit dem der `.icl`-Datei (Aufzeichnungsdatei) identisch. Um eine Aufzeichnungsdatei mit Textmarken auf einem anderen Player wiederzugeben, kopieren Sie die `.icl`-Dateien in den Cacheordner **Bookmarks** auf dem betreffenden Player. In der Standardeinstellung ist jede Textmarke mit "Textmarke" beschriftet. Sie können diese Beschriftung beliebig ändern und maximal 128 Zeichen eingeben.

Ereignisse werden als gelbe Punkte und Textmarken als blaue Quadrate unten im Playerfenster angezeigt. Wenn Sie mit der Maus auf die Punkte bzw. Quadrate zeigen, wird der zugehörige Text angezeigt. Sie können die Ereignisse und Textmarken auch in der Liste **Ereignisse und Textmarken** im Sitzungsaufzeichnungsplayer anzeigen. Sie werden in dieser Liste in chronologischer Reihenfolge mit den Textbeschriftungen und den Uhrzeiten angezeigt, zu denen sie in der aufgezeichneten Sitzung erscheinen.

Ereignisse und Textmarken erleichtern das Navigieren in aufgezeichneten Sitzungen. Wenn Sie auf ein Ereignis oder eine Textmarke gehen, springen Sie auf die Stelle in der aufgezeichneten Sitzung, an der das Ereignis oder die Textmarke eingefügt ist.

## Anzeigen von Ereignissen und Textmarken in der Liste

In der Liste **Ereignisse und Textmarken** werden die Ereignisse und Textmarken angezeigt, die in der momentan wiedergegebenen Sitzungsaufzeichnung eingefügt sind. Sie können in der Liste nur Ereignisse, nur Textmarken oder Ereignisse und Textmarken anzeigen.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Verschieben Sie den Mauszeiger auf die Liste **Ereignisse und Textmarken** und klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen.
4. Wählen Sie **Nur Ereignisse anzeigen**, **Nur Textmarken anzeigen** oder **Alle anzeigen**.

## Einfügen einer Textmarke

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Beginnen Sie mit der Wiedergabe der aufgezeichneten Sitzung, der Sie eine Textmarke hinzufügen möchten.
4. Schieben Sie den Schieberegler für das Positionieren auf die Stelle, an der Sie die Textmarke einfügen möchten.
5. Bewegen Sie den Mauszeiger in das Playerfenster und klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen.
6. Fügen Sie eine Textmarke mit der Standardbeschriftung **Textmarke** hinzu oder erstellen Sie eine Anmerkung:
  - Zum Hinzufügen einer Textmarke mit der Standardbeschriftung **Textmarke** wählen Sie **Textmarke hinzufügen**.
  - Um eine Textmarke mit einer von Ihnen erstellten Beschriftung hinzuzufügen, wählen Sie **Anmerkung hinzufügen**. Geben Sie die Anmerkung (max. 128 Zeichen) ein, die Sie der Textmarke zuordnen möchten. Klicken Sie auf **OK**.

## Hinzufügen oder Ändern einer Anmerkung

Nach dem Erstellen einer Textmarke können Sie eine Anmerkung hinzufügen oder eine bestehende Anmerkung ändern.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Beginnen Sie mit der Wiedergabe der aufgezeichneten Sitzung, die eine Textmarke hat.
4. Stellen Sie sicher, dass in der Liste **Ereignisse und Textmarken** Textmarken angezeigt werden.
5. Wählen Sie die Textmarke aus der Liste **Ereignisse und Textmarken** aus und klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen.
6. Wählen Sie **Anmerkung bearbeiten**.
7. Geben Sie im angezeigten Fenster die neue Anmerkung ein und klicken Sie auf **OK**.

## Löschen einer Textmarke

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.

3. Beginnen Sie mit der Wiedergabe der aufgezeichneten Sitzung, die eine Textmarke hat.
4. Stellen Sie sicher, dass in der Liste **Ereignisse und Textmarken** Textmarken angezeigt werden.
5. Wählen Sie die Textmarke aus der Liste **Ereignisse und Textmarken** aus und klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen.
6. Wählen Sie **Löschen**.

## Gehen auf ein Ereignis oder eine Textmarke

Wenn Sie auf ein Ereignis oder eine Textmarke gehen, springt der Sitzungsaufzeichnungsplayer an die Stelle in der Sitzungsaufzeichnung, an der das Ereignis oder die Textmarke eingefügt ist.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Beginnen Sie mit der Wiedergabe einer Sitzungsaufzeichnung mit Ereignissen oder Textmarken.
4. Gehen Sie auf ein Ereignis oder eine Textmarke.
  - Klicken Sie unten im Player-Fenster auf den Punkt oder das Quadrat, der das Ereignis oder die Textmarke darstellt, um zu dem Ereignis bzw. der Textmarke zu gehen.
  - Doppelklicken Sie in der Liste **Ereignisse und Textmarken** auf ein Ereignis oder eine Textmarke, um an die entsprechende Stelle zu gehen. Um zum nächsten Ereignis oder der nächsten Textmarke zu gelangen, klicken Sie mit der rechten Maustaste, um das Menü anzuzeigen, und wählen Sie **Auf Textmarke positionieren**.

## Suchen nach Aufzeichnungen

June 21, 2021

Im Sitzungsaufzeichnungsplayer können Sie Schnellsuchen und erweiterte Suchen durchführen und Optionen festlegen, die für alle Suchen gelten. Die Suchergebnisse werden im Bereich "Suchergebnisse" des Sitzungsaufzeichnungsplayers angezeigt.

### Hinweis:

Wenn Sie alle verfügbaren Sitzungsaufzeichnungen (bis zur Höchstanzahl der in einer Suche angezeigten Sitzungen) anzeigen möchten, führen Sie die Suche ohne Suchparameter durch.

## Ausführen einer Schnellsuche

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Definieren Sie die Suchkriterien:
  - Geben Sie ein Suchkriterium im Feld **Suchen** ein.
  - Zeigen Sie auf **Suchen**, um eine Liste der Parameter als Richtlinie zu anzeigen.
  - Klicken Sie auf den Pfeil rechts neben dem Feld **Suchen**, um den Text für die letzten 64 Suchen anzuzeigen.
  - Wählen Sie in der Dropdownliste rechts neben dem Feld **Suchen** den Zeitraum der Aufzeichnung der Sitzung aus.
4. Klicken Sie auf das Fernglas-Symbol rechts von der Dropdownliste, um die Suche zu starten.

## Durchführen einer erweiterten Suche

Die erweiterte Suche kann bis zu 20 Sekunden dauern, wenn das Ergebnis über 150.000 Einheiten umfasst. Citrix empfiehlt die Verwendung gezielterer Suchbedingungen, z. B. einen Datumsbereich oder Benutzer, um den Umfang des Ergebnisses zu limitieren.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie im **Sitzungsaufzeichnungsplayer**-Fenster auf der Symbolleiste auf **Erweiterte Suche** oder wählen Sie auf der Symbolleiste **Extras > Erweiterte Suche**.
4. Legen Sie die Suchkriterien auf den Registerkarten im Dialogfeld **Erweiterte Suche** fest:
  - **Allgemein** ermöglicht die Suche nach Domäne oder Kontoautorität, Site, Gruppe, VDA für Multisitzungs-OS, Anwendung oder Datei-ID.
  - **Datum/Uhrzeit** ermöglicht die Suche nach Datum, Wochentag und Tageszeit.
  - **Ereignisse** ermöglicht die Suche nach Citrix-definierten und benutzerdefinierten Ereignissen, die in die Sitzungen eingefügt werden.
  - **Sonstiges** ermöglicht die Suche nach Sitzungsname, Clientname, Clientadresse und Aufzeichnungsdauer. Sie können für diese Suche auch die Höchstzahl der angezeigten Suchergebnisse und den Einschluss von archivierten Dateien in der Suche festlegen. Wenn Sie Suchkriterien angeben, wird die erstellte Abfrage im unteren Bereich des Dialogfelds angezeigt.
5. Klicken Sie auf **Suchen**, um die Suche zu starten.

Sie können erweiterte Suchen speichern und abrufen. Klicken Sie im Dialogfeld **Erweiterte Suche** auf **Speichern**, um die aktuelle Abfrage zu speichern. Klicken Sie im Dialogfeld **Erweiterte Suche** auf **Öffnen**, um eine gespeicherte Abfrage abzurufen. Abfragen werden als Dateien mit der Erweiterung `.isq` gespeichert.

## Festlegen von Suchoptionen

Mit den Suchoptionen im Sitzungsaufzeichnungsplayer beschränken Sie die Höchstzahl der Sitzungsaufzeichnungen, die in den Suchergebnissen angezeigt werden, und legen den Ein- oder Ausschluss von archivierten Sitzungsaufzeichnungsdateien fest.

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsplayer**.
3. Klicken Sie auf der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Extras > Optionen > Suche**.
4. Geben Sie im Feld **Angezeigte Ergebnisse (max.)** die Anzahl der Suchergebnisse ein, die angezeigt werden. Sie können maximal 500 Ergebnisse anzeigen.
5. Abhängig davon, ob Sie archivierte Dateien in Suchen einschließen möchten, aktivieren oder deaktivieren Sie **Archivierte Dateien einschließen**.

## Webplayer für die Sitzungsaufzeichnung

January 15, 2024

### Übersicht

Mit dem Webplayer können Sie Aufnahmen mit einem Webbrowser anzeigen und wiedergeben. Mit dem Webplayer ist Folgendes möglich:

- Suchen von Aufzeichnungen mithilfe von Filtern (Hostname, Clientname, Benutzername, Anwendung, Client-IP-Adresse, Ereignistext, Ereignistyp und Uhrzeit).
- Anzeigen und Wiedergeben von Live- und abgeschlossenen Aufzeichnungen mit markierten Ereignissen im rechten Fensterbereich.
- Konfigurieren des Caches zum Speichern von Aufzeichnungen während der Wiedergabe.
- Aufzeichnen von Leerlaufereignissen und Hervorheben von Leerlaufzeiträumen

- Kommentare zu einer Aufzeichnung hinterlassen und einen Schweregrad für den Kommentar festlegen.
- URLs von Aufzeichnungen freigeben.

**Hinweis:**

Zu den unterstützten Browsern gehören Google Chrome, Microsoft Edge und Firefox.

## Aktivieren des Webplayers

Der Webplayer ist standardmäßig aktiviert.

- Um den Webplayer zu deaktivieren, starten Sie eine Windows-Eingabeaufforderung und führen Sie den Befehl `<Session Recording Server installation path>\Bin\SsRecUtils.exe -disablewebplayer` aus.
- Um den Webplayer zu aktivieren, starten Sie eine Windows-Eingabeaufforderung und führen Sie den Befehl `<Session Recording Server installation path>\Bin\SsRecUtils.exe -enablewebplayer` aus.

## Anmeldung und Kennwort

Die URL der Webplayersite ist `http(s)://<FQDN of Session Recording Server>/WebPlayer`. Um sicherzustellen, dass HTTPS verwendet wird, fügen Sie der Website in IIS eine SSL-Bindung hinzu und aktualisieren Sie die Konfigurationsdatei `SsRecWebSocketServer.config`. Weitere Informationen finden Sie im Abschnitt [HTTPS-Konfiguration](#) in diesem Artikel.

**Hinweis:**

Domänenbenutzer müssen bei der Anmeldung beim Webplayer im Gegensatz zu externen Benutzern keine Anmeldeinformationen eingeben.

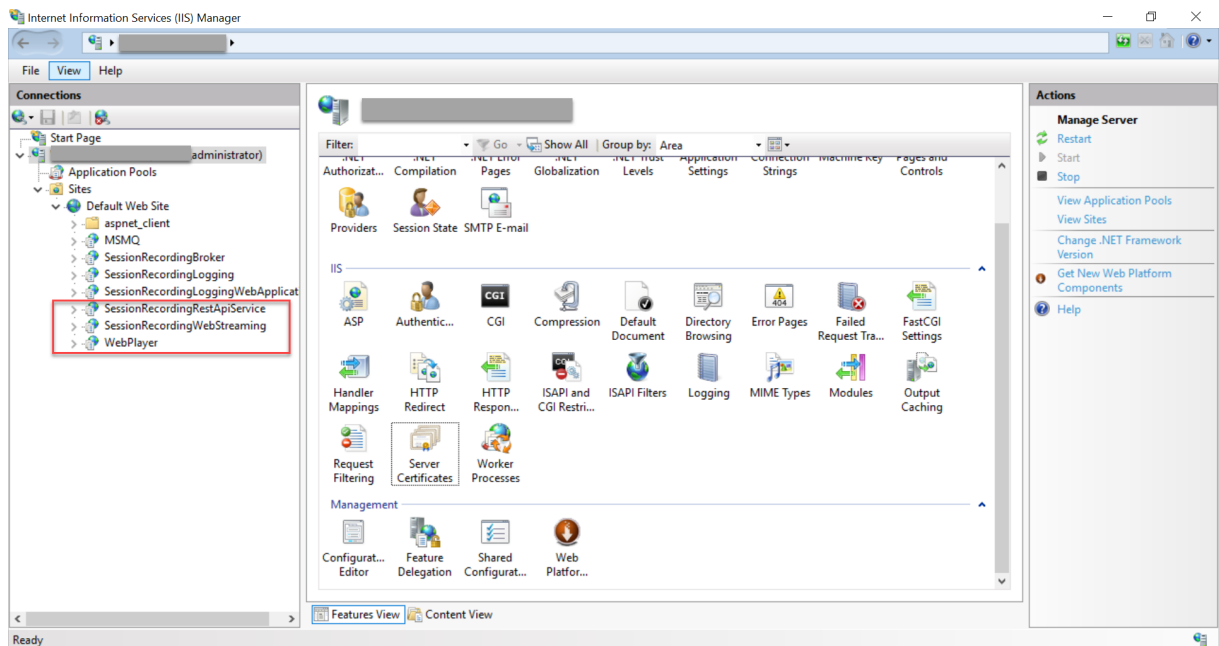
## Installation

Installieren Sie den Webplayer nur auf dem Sitzungsaufzeichnungsserver. Doppelklicken Sie auf `SessionRecordingWebPlayer.msi` und folgen Sie den Anweisungen, um die Installation abzuschließen. Weitere Informationen zum Installieren der Sitzungsaufzeichnung finden Sie unter [Installieren, Aktualisieren und Deinstallieren](#).

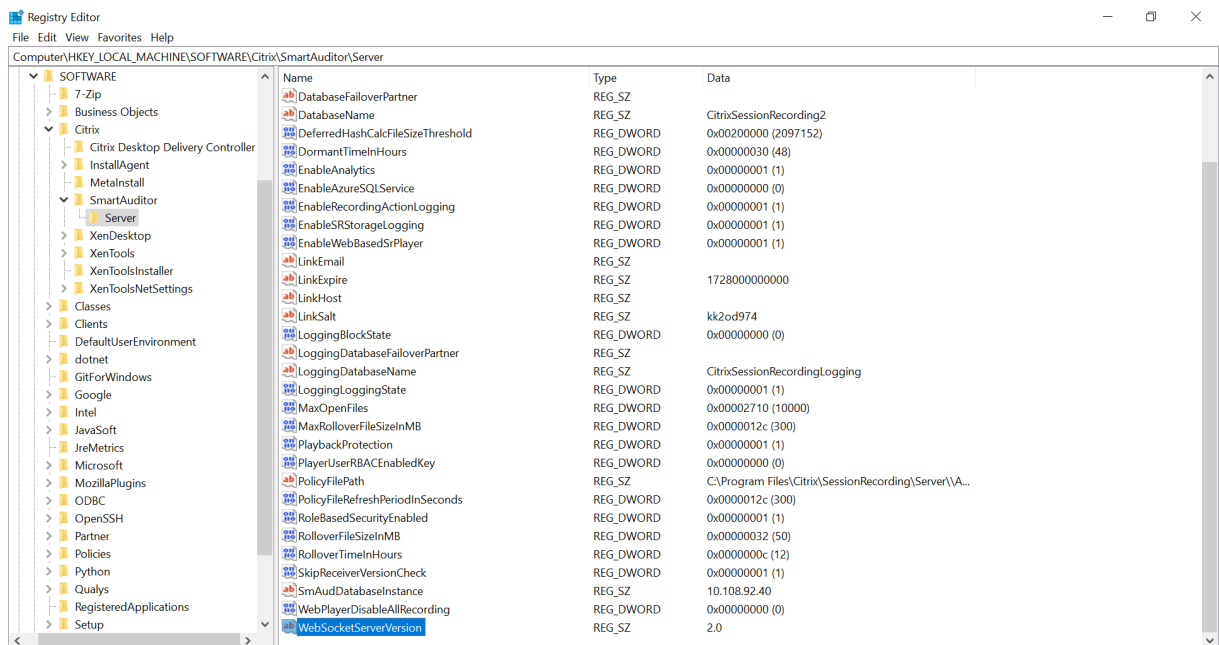
Ab Version 2103 migriert die Sitzungsaufzeichnung den WebSocket-Server auf IIS. Nach Installation des Webplayers werden die Anwendungen **SessionRecordingRestApiService**, **SessionRecording-WebStreaming** und **WebPlayer** in IIS angezeigt.



## Sitzungsaufzeichnung 2104



Bei einer Neuinstallation von Sitzungsaufzeichnung 2103 und höher wird Ihr Webbrowser mit dem in IIS gehosteten WebSocket-Server verbunden, wenn Sie auf die Website des Webplayers zugreifen. Der in IIS gehostete WebSocket-Server hat die Version 2.0, wie im Registrierungswert **WebSocketServerVersion** unter dem Registrierungsschlüssel HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server angegeben.



Bei einem Upgrade von einer früheren Version auf Sitzungsaufzeichnung 2103 und höher wird Ihr Webbrowser mit dem Python-basierten WebSocket-Server verbunden. Um eine Verbindung mit dem in IIS gehosteten WebSocket-Server herzustellen, führen Sie den Befehl **<Installation-**

**spfad des Sitzungsaufzeichnungsservers>\Bin\SsRecUtils.exe -enablestreamingservice** aus. Um eine erneute Verbindung mit dem Python-basierten WebSocket-Server herzustellen, führen Sie den Befehl **<Installationspfad des Sitzungsaufzeichnungsservers>\Bin\SsRecUtils.exe -disablestreamingservice** aus. Der Python-basierte WebSocket-Server hat die Version 1.0.

## HTTPS-Konfiguration

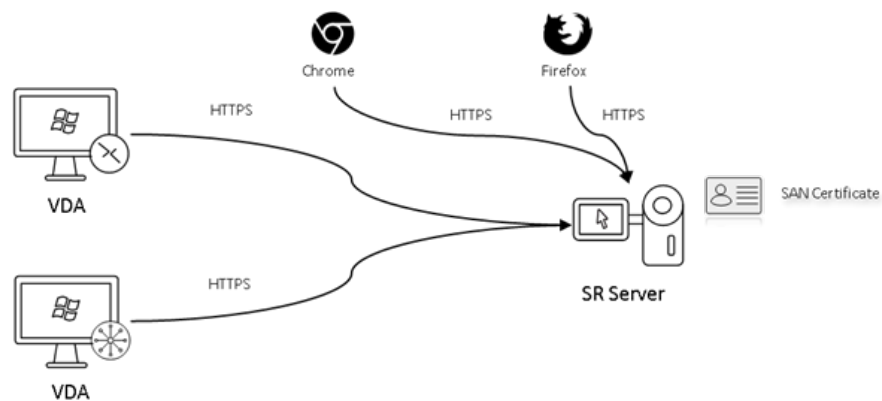
Verwenden von HTTPS für den Zugriff auf den Webplayer:

1. Fügen Sie eine SSL-Bindung in IIS hinzu.
  - a) Beziehen Sie von einer vertrauenswürdigen Zertifizierungsstelle ein SSL-Zertifikat im PEM-Format.

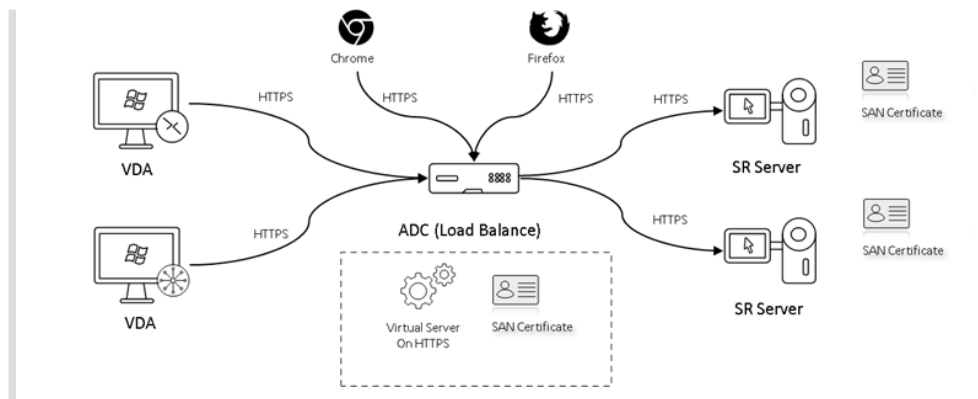
### Hinweis:

Die gängigsten Browser wie Google Chrome und Firefox unterstützen in einer Zertifikatsignieranforderung (CSR) keine allgemeinen Namen (CN) mehr. Sie erzwingen in allen öffentlich vertrauten Zertifikaten einen alternativen Antragstellernamen. Um den Webplayer über HTTPS zu verwenden, führen Sie die entsprechende Aktion aus:

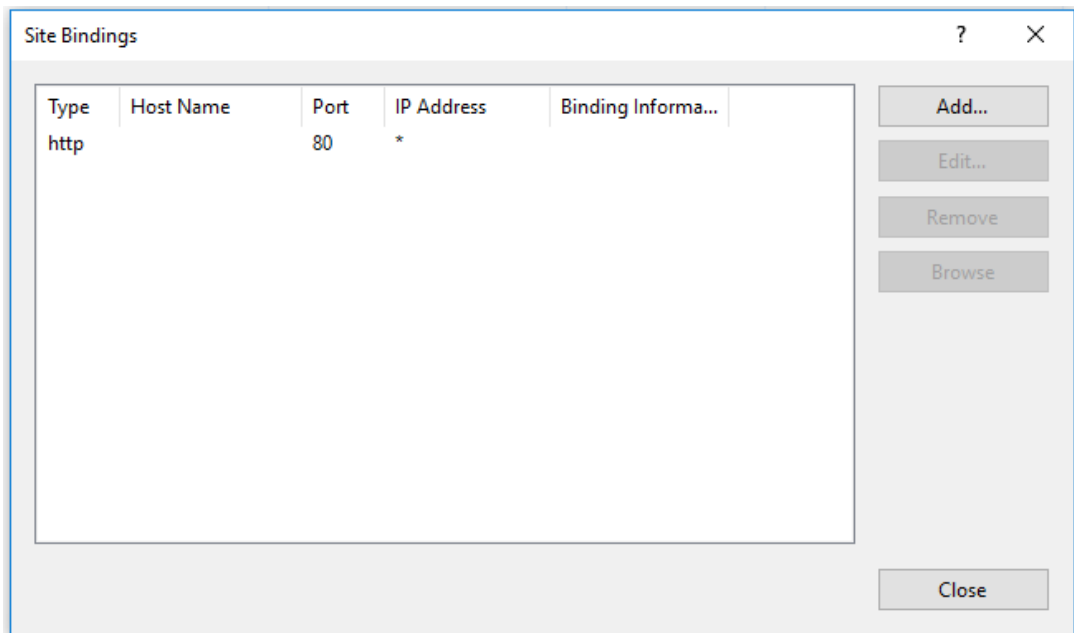
- Wenn ein einzelner Sitzungsaufzeichnungsserver verwendet wird, ändern Sie das Zertifikat dieses Sitzungsaufzeichnungsservers in ein SAN-Zertifikat.



- Bei Verwendung des Lastausgleichs muss ein SAN-Zertifikat auf Citrix ADC und auf jedem Sitzungsaufzeichnungsserver verfügbar sein.



- b) Klicken Sie in IIS mit der rechten Maustaste auf die Website und wählen Sie **Bindungen hinzufügen**. Das Dialogfeld **Websitebindungen** wird angezeigt.



- c) Klicken Sie oben rechts auf **Hinzufügen**. Das Dialogfeld **Websitebindung hinzufügen** wird angezeigt.
- d) Wählen Sie **https** aus der Liste **Typ** und dann Ihr SSL-Zertifikat aus.

The screenshot shows the 'Add Site Binding' dialog box. The 'Type' dropdown menu is open, displaying 'http' and 'https' options. The 'IP address' dropdown is set to 'All Unassigned', and the 'Port' text box contains '80'. Below these fields is a text box with the example 'Example: www.contoso.com or marketing.contoso.com'. At the bottom right, there are 'OK' and 'Cancel' buttons.

The screenshot shows the 'Add Site Binding' dialog box with 'https' selected as the type and port '443'. The 'Host name' field is empty. The 'Require Server Name Indication' checkbox is unchecked. The 'SSL certificate' dropdown is open, showing 'Not selected' and 'test' options. There are 'Select...' and 'View...' buttons next to the dropdown. 'OK' and 'Cancel' buttons are at the bottom right.

- e) Klicken Sie auf **OK**.
- 2. Aktualisieren Sie die Konfigurationsdatei `SsRecWebSocketServer.config`.
  - a) Suchen Sie die Konfigurationsdatei `SsRecWebSocketServer.config` und öffnen Sie sie.

Die Konfigurationsdatei `SsRecWebSocketServer.config` ist üblicherweise im Ordner `<Session Recording Server installation path>\Bin\`.
  - b) (Optional) Für die Sitzungsaufzeichnung 2103 und höher mit WebSocket-Server in IIS aktivieren Sie TLS, indem Sie `TLSEnable=1` bearbeiten und die Felder **ServerPort**, **SSLCert**

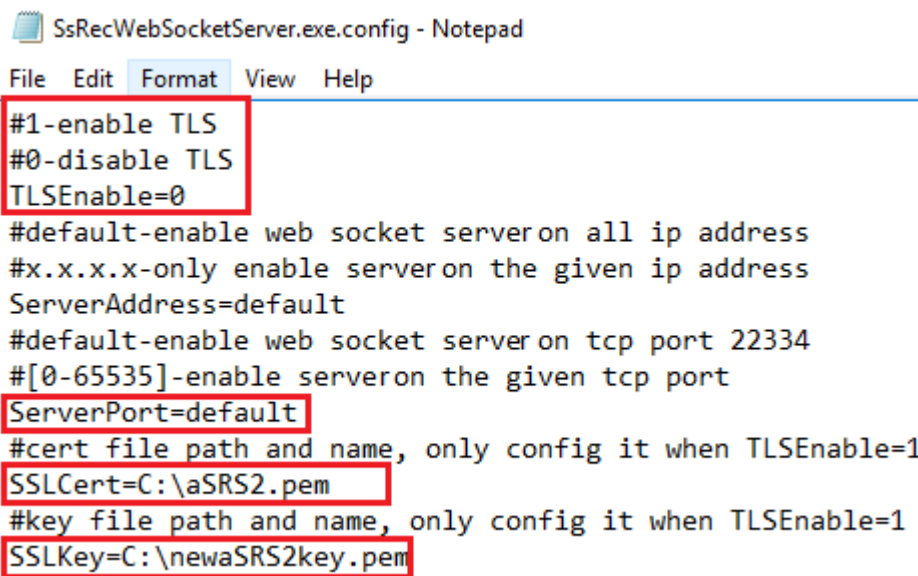
und **SSLKey** ignorieren.

- c) (Optional) Für die Sitzungsaufzeichnung 2012 und früher aktivieren Sie TLS, indem Sie `TLSEnable=1` bearbeiten und die Pfade zum SSL-Zertifikat bzw. dessen Schlüssel eingeben.

**Hinweis:**

SSL-Zertifikate und Schlüsseldateien werden nur im PEM-Format unterstützt.

Das Feld **ServerPort** enthält die Nummer des Ports, über den der Webplayer Aufzeichnungsdateien sammelt. In der folgenden Abbildung ist dies der Standardwert (22334).



```
SsRecWebSocketServer.exe.config - Notepad
File Edit Format View Help
#1-enable TLS
#0-disable TLS
TLSEnable=0
#default-enable web socket server on all ip address
#x.x.x.x-only enable server on the given ip address
ServerAddress=default
#default-enable web socket server on tcp port 22334
#[0-65535]-enable server on the given tcp port
ServerPort=default
#cert file path and name, only config it when TLSEnable=1
SSLCert=C:\aSRS2.pem
#key file path and name, only config it when TLSEnable=1
SSLKey=C:\newaSRS2key.pem
```

Extrahieren Sie wie folgt die separaten Zertifikat- und Schlüsseldateien, die in der WebSocket-Serverkonfiguration verwendet werden:

- i. Stellen Sie sicher, dass OpenSSL auf dem Sitzungsaufzeichnungsserver installiert ist, der das SSL-Zertifikat enthält.
- ii. Exportieren Sie das SSL-Zertifikat als PFX-Datei. Die PFX-Datei enthält das Zertifikat und den privaten Schlüssel.
- iii. Öffnen Sie eine Eingabeaufforderung und wechseln Sie zu dem Ordner, der die PFX-Datei enthält.
- iv. Starten Sie OpenSSL aus dem Ordner `OpenSSL\bin`.
- v. Führen Sie den folgenden Befehl aus, um das Zertifikat zu extrahieren:

```
1 openssl pkcs12 -in [yourfile.pfx] -clcerts -nokeys -out [
  aSRS2.pem]
```

```
2 <!--NeedCopy-->
```

Geben Sie das Importkennwort ein, das Sie beim Exportieren der PFX-Datei erstellt haben.

- vi. Führen Sie den folgenden Befehl aus, um den privaten Schlüssel zu extrahieren:

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

Geben Sie das Importkennwort ein, das Sie beim Exportieren der PFX-Datei erstellt haben. Geben Sie ein neues Kennwort zum Schutz der Schlüsseldatei ein, wenn Sie zur Eingabe der PEM-Passphrase aufgefordert werden.

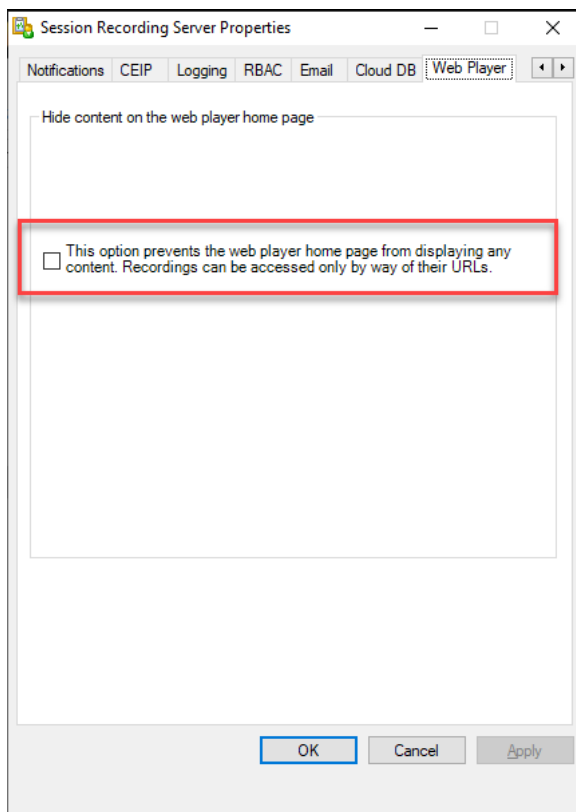
- vii. Führen Sie den folgenden Befehl aus, um den privaten Schlüssel zu entschlüsseln:

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

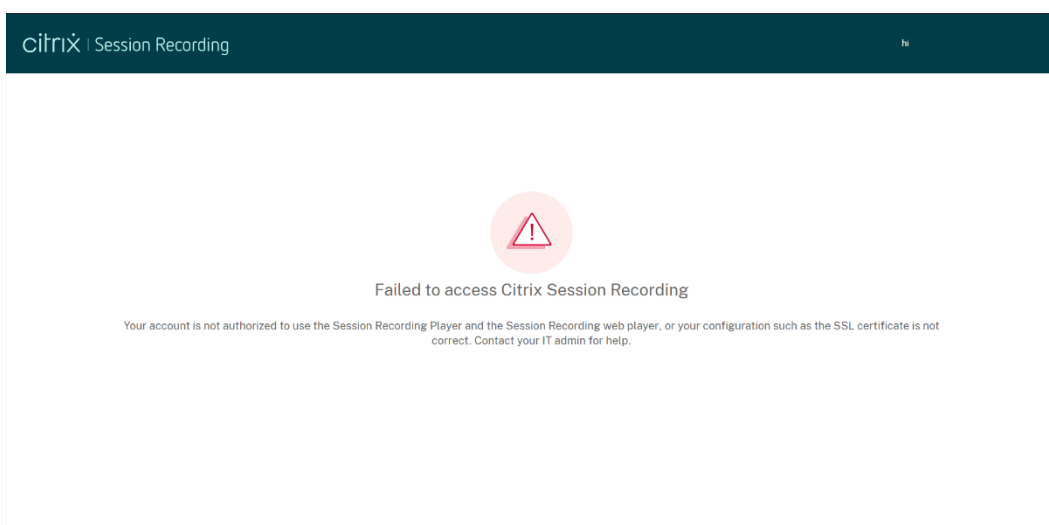
- d) Speichern Sie Ihre Änderungen.
- e) Überprüfen Sie Ihre Firewallinstellungen. Lassen Sie zu, dass SsRecWebSocket-Server.exe, den TCP-Port (standardmäßig 22334) verwendet und erlauben Sie den Zugriff auf die Webplayer-URL.
- f) Führen Sie den Befehl `SsRecUtils -stopwebsocketserver` aus.

## Anzeigen von Aufzeichnungen

Nach der Anmeldung kann die Webplayer-Startseite Inhalte ausblenden oder anzeigen, je nachdem, ob die folgende Option in **Sitzungsaufzeichnungsserver - Eigenschaften** ausgewählt ist.

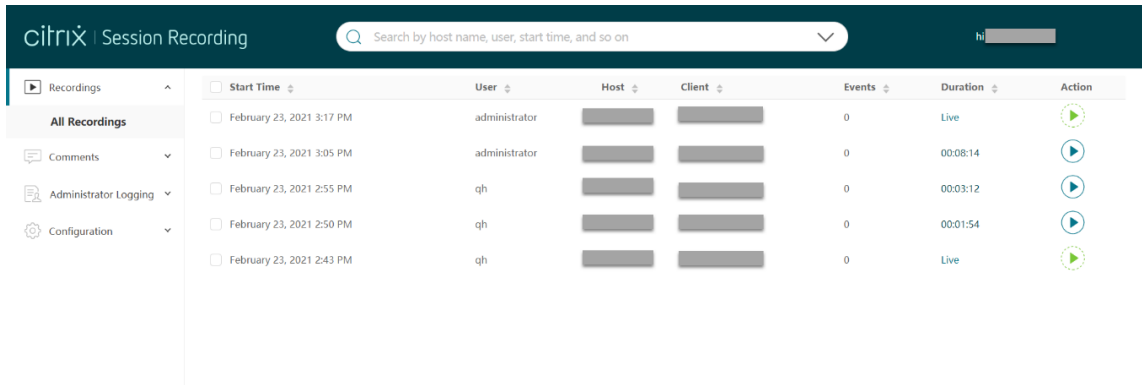


- Wenn die Option ausgewählt ist, blendet die Webplayer-Startseite alle Inhalte aus. Aufzeichnungen können dann nur über ihre URLs abgerufen werden. Aufzeichnungs-URLs werden in E-Mail-Benachrichtigungen bereitgestellt, die an festgelegte Empfänger gesendet werden. Informationen zu E-Mail-Benachrichtigungen finden Sie unter [E-Mail-Benachrichtigungsrichtlinien](#). Sie können Aufzeichnungs-URLs auch über **Aktuelle Wiedergabe freigeben** auf der Wiedergabe-seite von Aufzeichnungen freigeben. Siehe Beschreibungen weiter unten in diesem Artikel.

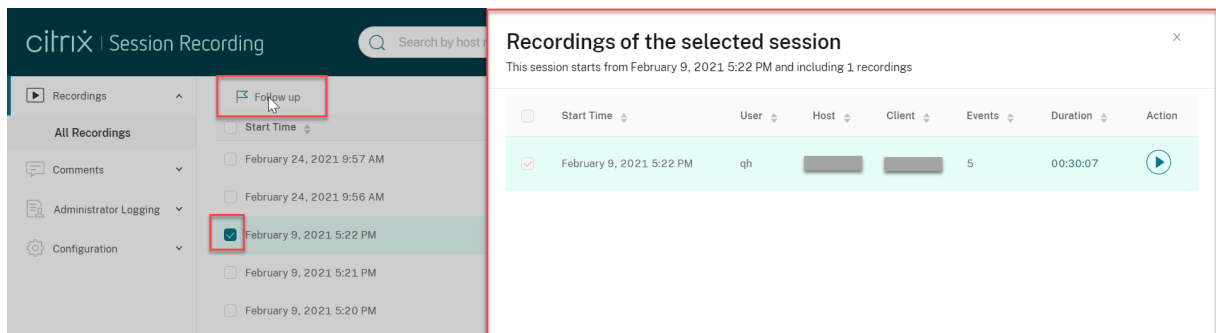


- Wenn die Option nicht ausgewählt ist, zeigt die Webplayer-Startseite Inhalte an, ähnlich dem fol-

genden Screenshot. Klicken Sie links auf **Alle Aufzeichnungen**, um die Seite zu aktualisieren und neue Aufzeichnungen, falls vorhanden, anzuzeigen. Scrollen Sie die Webseite nach unten, um Aufzeichnungen zum Anzeigen auszuwählen oder Filter zum Anpassen der Suchergebnisse zu verwenden. Bei Liveaufzeichnungen wird in der Spalte **Dauer** die Angabe **Live** und die Wiedergabeschaltfläche in Grün angezeigt.



Um alle Aufzeichnungsdateien einer aufgezeichneten Sitzung anzuzeigen, wählen Sie eine Aufzeichnung in der Liste aus und klicken auf das Symbol **Nachverfolgen**. Das Symbol **Nachverfolgen** ist nur dann verfügbar, wenn eine Aufzeichnung ausgewählt ist.



Die folgende Tabelle enthält eine Beschreibung der einzelnen Aufzeichnungselemente:

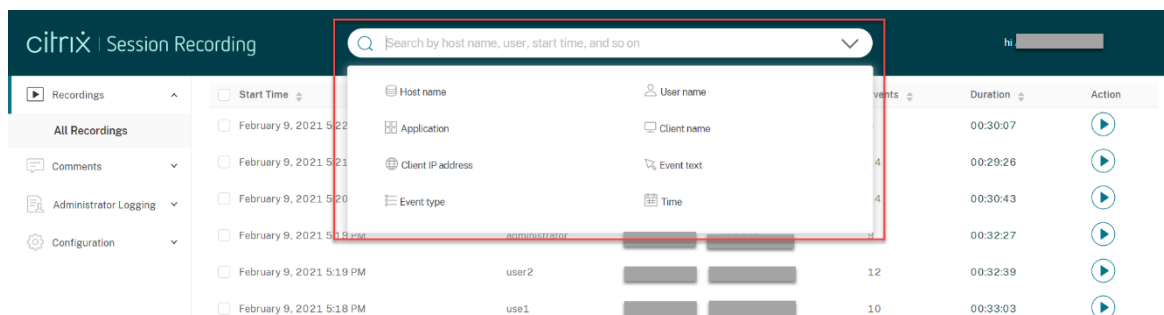
Element	Beschreibung
Startzeit	Startzeit der Aufnahme. Klicken Sie auf die Pfeile, um die Aufzeichnungen in chronologischer Reihenfolge aufzulisten.
Benutzer	Benutzer, dessen Sitzung aufgezeichnet wurde. Klicken Sie auf die Pfeile, um Aufnahmen eines Benutzers auf der Liste zusammenzufassen und die Benutzer in alphabetischer Reihenfolge zu sortieren.



Element	Beschreibung
Host	Der Hostname des VDAs, auf dem die aufgezeichnete Sitzung gehostet wurde. Klicken Sie auf die Pfeile, um die VDA-Hostnamen in alphabetischer Reihenfolge zu sortieren.
Client	Der Name des Clientgeräts, auf dem die Sitzung ausgeführt wurde. Klicken Sie auf die Pfeile, um die Client-Hostnamen in alphabetischer Reihenfolge zu sortieren.
Ereignisse	Anzahl der Ereignisse in der Aufzeichnung. Klicken Sie auf die Pfeile, um Aufzeichnungen in der Liste nach Ereigniszahl zu sortieren.
Dauer	Zeitdauer der Aufnahme. Klicken Sie auf die Pfeile, um Aufzeichnungen in der Liste nach Dauer zu sortieren.

### Suchen von Aufzeichnungen mithilfe von Filtern

Sie können mithilfe von Filtern nach Aufzeichnungen suchen. Als Filter stehen Hostname, Clientname, Benutzername, Anwendung, Client-IP-Adresse, Ereignistext, Ereignistyp und Uhrzeit zur Verfügung.



Wenn Sie beispielsweise den Filter “Hostname” auswählen, wird das folgende Dialogfeld angezeigt. Geben Sie den Hostnamen (des VDAs, der aufgezeichnete Sitzungen hostet) ein und klicken Sie auf **Suchen**, um irrelevante Aufzeichnungen herauszufiltern.

Sie können zu einem anderen Filter wechseln, indem Sie auf die Auswahl **Hostname** klicken (siehe Abbildung). Alle Filter werden aufgeführt, wenn Sie auf **Hostname** klicken. Wählen Sie den gewünschten Filter aus.

FILTER

Search Clear All

Host name Enter one Host name + X

- Host name
- User name
- Application
- Client name
- Client IP address
- Event text
- Comments
- Event type
- Time

	User	Host	Client	Events	Duration	Action
<input type="checkbox"/>	qh			5	00:30:07	
<input type="checkbox"/>	dzl			14	00:29:26	
<input type="checkbox"/>	dlq			14	00:30:43	
<input type="checkbox"/>	administrator			9	00:32:27	
<input type="checkbox"/>	user2			12	00:32:39	

Sie können auch auf das Symbol + klicken, um Filter hinzuzufügen.

FILTER

Search Clear All

Host name Enter one Host name + X

Beispielsweise können Sie den Filter **Zeit** hinzufügen (siehe folgende Abbildung).

FILTER

Search Clear All

Host name Enter one Host name + X

Time

Start date Select date End date Select date

Start Time Select time End time Select time

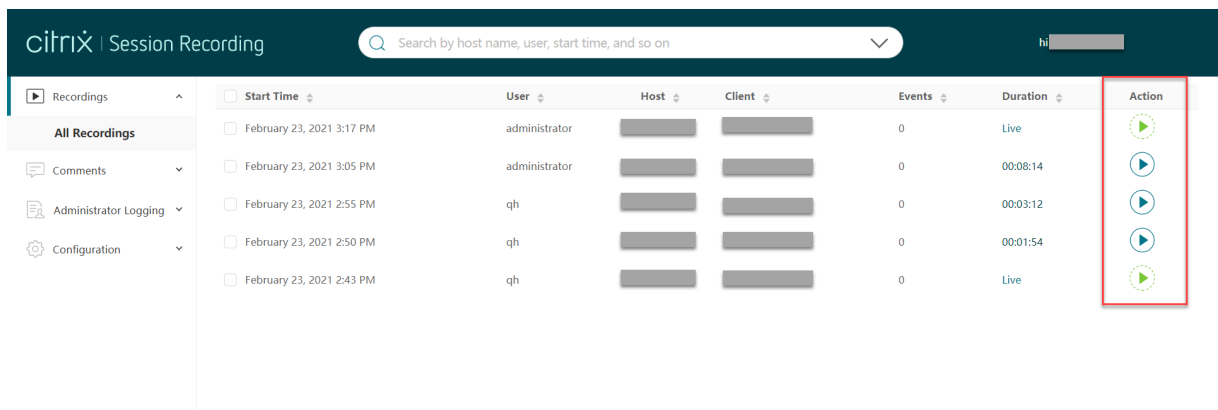
Duration At least [ ] Seconds [ ]

<input type="checkbox"/>	Start Time	User	Host	Client	Events	Duration	Action
<input type="checkbox"/>	February 9, 2021 5:22 PM	qh			5	00:30:07	

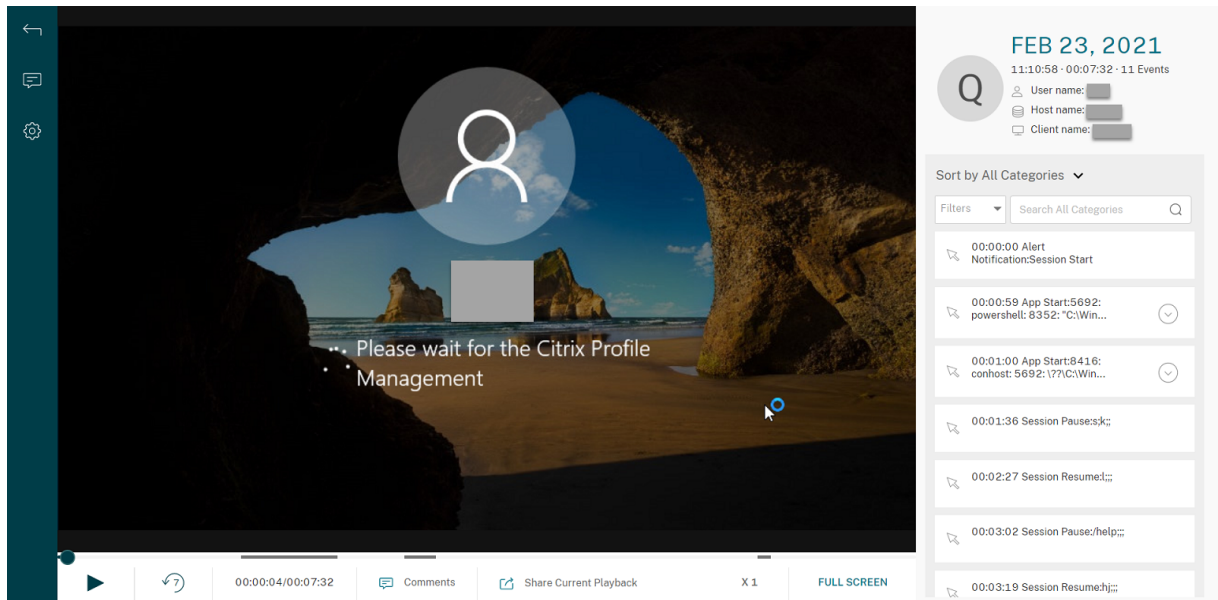
Der Filter **Zeit** basiert auf dem Datum und der Uhrzeit des Aufzeichnungsstarts und der Dauer einer der Aufzeichnung.

### Öffnen und Wiedergeben von Aufzeichnungen




Auf der Seite "Aufzeichnungen" wird rechts neben dem Element **Dauer** jeder Aufzeichnung eine Wiedergabe-Schaltfläche angezeigt.






Klicken Sie auf die Schaltfläche “Wiedergeben”. Die Seite “Wiedergeben” wird angezeigt. Die Wiedergabe beginnt nach dem Zwischenspeichern.



Die folgende Tabelle enthält eine Beschreibung der Bedienelemente für die Wiedergabe:

Player-Bedienelement	Beschreibung
	Gibt die ausgewählte Aufzeichnung wieder.
	Anhalten der Wiedergabe.
	Sie können den Fortschrittsbalken während der Wiedergabe ziehen. Leerlaufzeiten aufgezeichneter Sitzungen werden während der Wiedergabe hervorgehoben.

Player-Bedienelement	Beschreibung
	7 Sekunden rückwärts positionieren.
00:00:00/00:02:17	Gibt die aktuelle Position der Wiedergabe und die gesamte Aufzeichnungsdauer an. Das Zeitformat ist HH:MM:SS.
 Comments	Ermöglicht das Eingeben eines Kommentars zu der wiedergegebenen Aufzeichnung.
 Share Current Playback	Ermöglicht das Klicken und Kopieren der URL der aktuellen Aufzeichnung in die Zwischenablage.
X 1	Gibt die aktuelle Wiedergabegeschwindigkeit an. Klicken Sie auf das Symbol, um zwischen Optionen (X0.5, X1, X2 und X4) zu wechseln.
FULL SCREEN	Zeigt die Wiedergabe im Vollbildmodus an.
Exit full screen	Zeigt die Wiedergabe innerhalb der Webseite an.

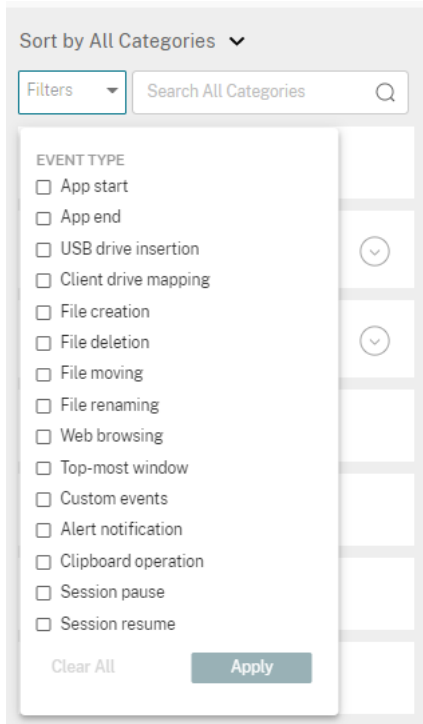
---

Im rechten Bereich der Wiedergabeseite stehen Aufzeichnungsdaten, Ereignisfilter und das Schnell-suchfeld zur Verfügung:

The screenshot displays a session recording interface. At the top, it shows the date **FEB 23, 2021** and the session duration **11:10:58 · 00:07:32 · 11 Events**. Below this, there is a circular profile icon with the letter 'Q' and three fields for user information: 'User name:', 'Host name:', and 'Client name:', each followed by a redacted grey box. A 'Sort by All Categories' dropdown menu is visible. Below the menu are two input fields: 'Filters' with a dropdown arrow and 'Search All Categories' with a search icon. The main area contains a list of seven events, each with a mouse cursor icon on the left and a dropdown arrow on the right. The events are: 00:00:00 Alert Notification:Session Start; 00:00:59 App Start:5692: powershell: 8352: "C:\Win...; 00:01:00 App Start:8416: conhost: 5692: \??\C:\Win...; 00:01:36 Session Pause:s;k;; 00:02:27 Session Resume:l;;; 00:03:02 Session Pause:/help;;; 00:03:19 Session Resume:hj;;;.

- Datum und Uhrzeit auf der Webplayer-Maschine. In diesem Beispiel **23. Februar 2021** und **11:10:58**.
- Die Dauer der wiedergegebenen Aufzeichnung. In diesem Beispiel **00:07:32**.
- Die Anzahl der Ereignisse in der Aufzeichnung. In diesem Beispiel **11 EREIGNISSE**.
- Der Name des Benutzers, dessen Sitzung aufgezeichnet wurde.
- Der Hostname des VDAs, auf dem die aufgezeichnete Sitzung gehostet wurde.
- Der Name des Clientgeräts, auf dem die Sitzung ausgeführt wurde.

- Optionen zum Sortieren von Suchergebnissen: **Sortieren nach allen Kategorien**, **Sortieren nach Ereignissen** und **Sortieren nach Kommentaren**.
- Ereignisfilter. Sie können mehrere Filter auswählen, um nach Ereignissen in der aktuellen Aufzeichnung zu suchen.



Klicken Sie auf das Symbol, um die Anzeige von Ereignissen zu erweitern.



- Ereignisliste. Wenn Sie auf ein Ereignis in der Liste klicken, gelangen Sie zur Position des Ereignisses in der Aufzeichnung.
- Schnellsuchfeld. Das Suchfeld für **Ereignisse suchen** ermöglicht das Einschränken der Liste von Ereignissen in der aktuellen Aufzeichnung.

### Konfigurieren des Caches zum Speichern von Aufzeichnungen während der Wiedergabe

Auf der Seite **Konfiguration** des Webplayers klicken Sie auf den Schieberegler, um den Cache für die Speicherung von Aufzeichnungen während der Wiedergabe einzurichten.

**Tipp:**

Sie können auf die Seite **Konfiguration** direkt über **http(s)://<FQDN des Sitzungsaufzeich-**

...ungsservers>/WebPlayer/#/configuration/cache zugreifen.

### Aufzeichnen von Leerlaufereignissen und Hervorheben von Leerlaufzeiträumen

Die Sitzungsaufzeichnung kann Leerlaufereignisse aufzeichnen und Leerlaufzeiten im Webplayer für die Sitzungsaufzeichnung hervorheben. Leerlaufereignisse sind im Sitzungsaufzeichnungsplayer nicht sichtbar, da sie zwar in der Sitzungsaufzeichnungsdatenbank, nicht aber in den Aufzeichnungsdateien (.icl-Dateien) gespeichert werden.

Legen Sie die folgenden Registrierungsschlüssel nach Bedarf fest, um das Leerlaufereignisfeature anzupassen. Die Registrierungsschlüssel sind unter HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SmartAuditor\Sess

Registrierungsschlüssel	Standardwert	Beschreibung
DisableIdleEvent	0	Um das Leerlaufereignisfeature zu deaktivieren, setzen Sie den Wert auf <b>1</b> . Um das Leerlaufereignisfeature zu aktivieren, setzen Sie den Wert auf <b>0</b> .

---

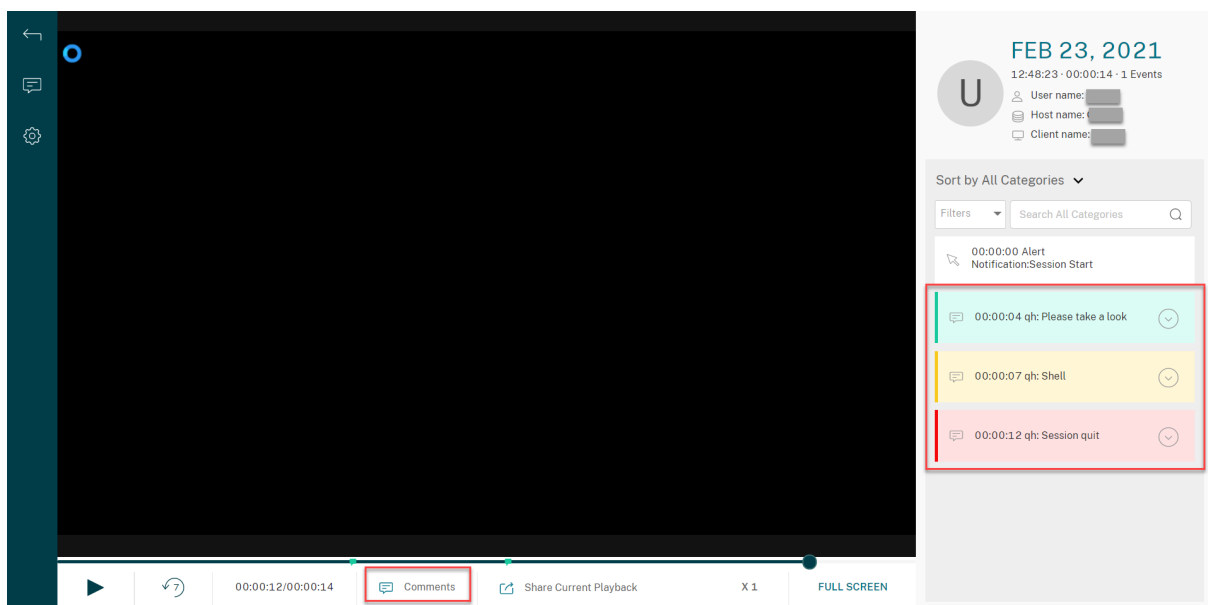
Registrierungsschlüssel	Standardwert	Beschreibung
IdleEventThrottle	120 Sekunden	Findet länger als durch den Registrierungsschlüssel festgelegt keine Benutzeraktivität statt (einschließlich Grafikänderungen und Tastatur-/Mauseingaben), wird ein Leerlaufereignis aufgezeichnet. Der Leerlaufzeitraum wird hervorgehoben, wenn die aufgezeichnete Sitzung auf dem Webplayer der Sitzungsaufzeichnung wiedergegeben wird.
IdleEventActiveThrottle	30 Sekunden	Nur eine bestimmte Anzahl Grafikänderungen innerhalb einer Zeitspanne gelten als Benutzeraktivitäten. Standardmäßig gelten mindestens drei Pakete innerhalb von 30 Sekunden als Benutzeraktivitäten.
IdleEventActivePktNumThrottle	3 Pakete	Nur eine bestimmte Anzahl Grafikänderungen innerhalb einer Zeitspanne gelten als Benutzeraktivitäten. Standardmäßig gelten mindestens drei Pakete innerhalb von 30 Sekunden als Benutzeraktivitäten.
IdleEventActivePktSizeThrottle	100 Byte	Grafikpakete, die kleiner sind als der Schlüsselwert, werden ignoriert und die entsprechende Zeitdauer gilt als Leerlauf.

---

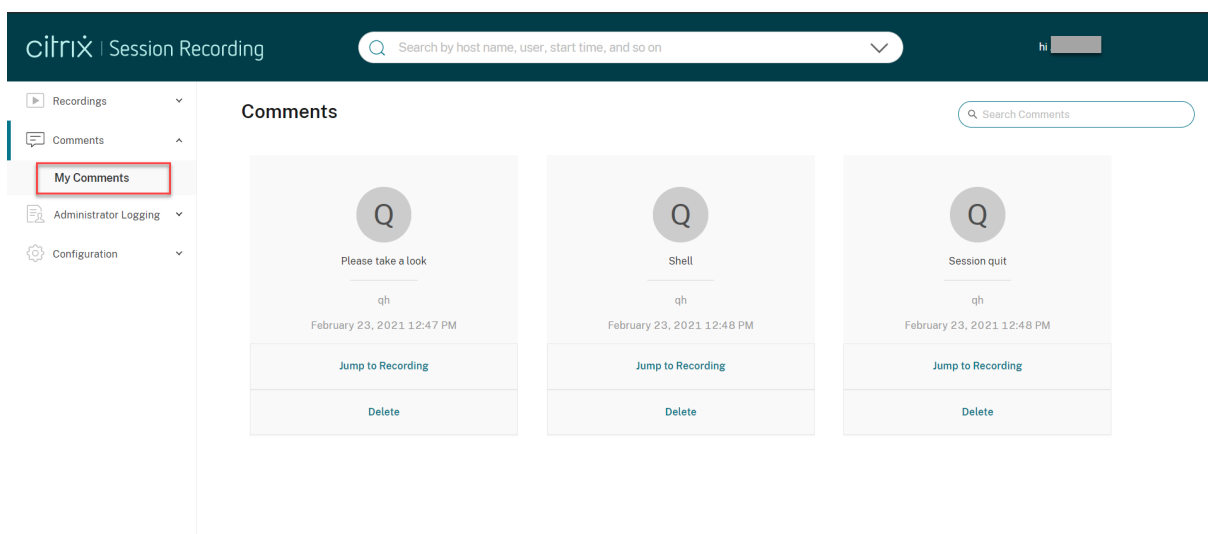


## Kommentar zu Aufzeichnungen

Wird eine aufgezeichnete Sitzung wiedergegeben, können Sie auf das Symbol **Kommentar** klicken, um Kommentare einzugeben und einen Kommentarschweregrad festzulegen. Kommentare unterschiedlicher Schweregrade werden in verschiedenen Farben im Ereignislistenbereich rechts angezeigt. Es gibt die Schweregrade Normal, Mittel und Hoch. Bei der Sitzungswiedergabe können Sie alle Kommentare zu einer Aufzeichnung anzeigen und Kommentare aus der Ereignisliste löschen. Sie müssen die Webseite aktualisieren, bevor Sie einen gerade eingegebenen Kommentar löschen können.


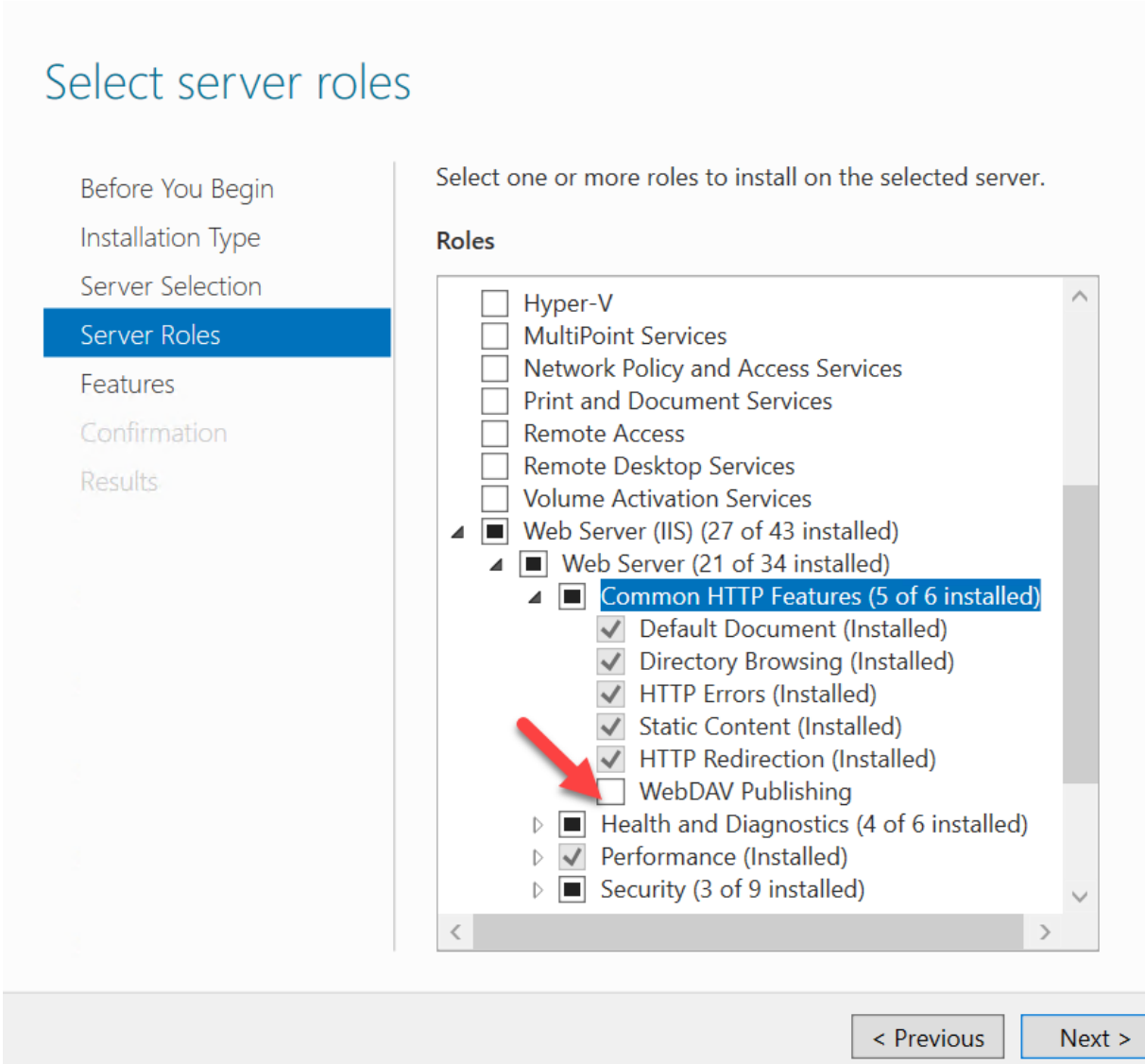


Durch Klicken auf einen Kommentar in der Ereignisliste können Sie zu dem Ort springen, an er abgegeben wurde. Mit einem Klick auf das Kommentarsymbol oben links gelangen Sie zur Seite **Meine Kommentare**, auf der Ihre gesamten Kommentare angezeigt werden.



**Hinweis:**

Damit das Kommentarfeature erwartungsgemäß funktioniert, deaktivieren Sie das Kontrollkästchen **WebDAV-Veröffentlichung** im **Assistenten zum Hinzufügen von Rollen und Features** des Server-Managers auf dem Sitzungsaufzeichnungsserver.

 Add Roles and Features Wizard

## Select server roles

Before You Begin

Installation Type

Server Selection

**Server Roles**

Features

Confirmation

Results

Select one or more roles to install on the selected server.

### Roles

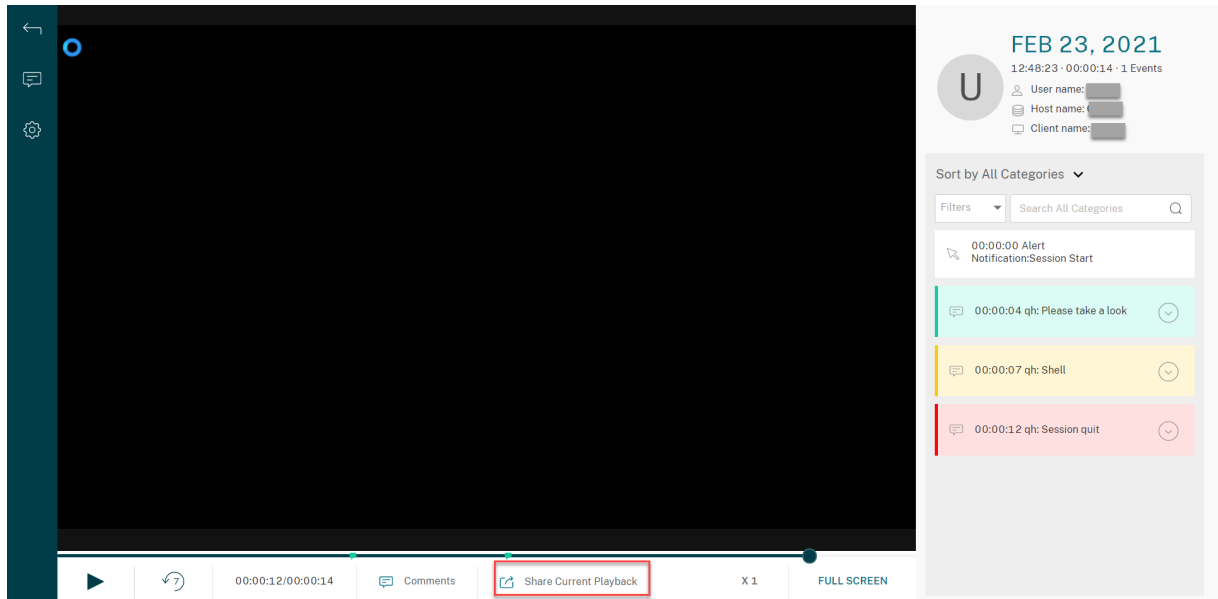
- Hyper-V
- MultiPoint Services
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS) (27 of 43 installed)
  - Web Server (21 of 34 installed)
    - Common HTTP Features (5 of 6 installed)
      - Default Document (Installed)
      - Directory Browsing (Installed)
      - HTTP Errors (Installed)
      - Static Content (Installed)
      - HTTP Redirection (Installed)
      - WebDAV Publishing
    - Health and Diagnostics (4 of 6 installed)
    - Performance (Installed)
    - Security (3 of 9 installed)

< Previous    Next >

**URLs von Aufzeichnungen freigeben**

Wenn Sie auf der Wiedergabeseite einer Aufzeichnung auf **Aktuelle Wiedergabe freigeben** klicken, wird die Aufzeichnungs-URL in die Zwischenablage kopiert. Sie können die URL mit anderen Benutzern teilen, damit sie direkt auf die Aufzeichnung zugreifen können, ohne in allen Aufzeichnungen

suchen zu müssen.



Nachdem Sie auf **Aktuelle Wiedergabe freigeben** geklickt haben, wird eine der folgenden Meldungen angezeigt, die auf einen erfolgreichen bzw. fehlgeschlagenen Vorgang hinweisen:

- **Die URL für die freigegebene Aufzeichnung wurde in die Zwischenablage kopiert**
- **Fehler beim Freigeben der URL für die Aufzeichnung**

Wenn Sie die freigegebene URL in die Adressleiste einfügen, können Sie zu dem Speicherort springen, an dem die URL kopiert wurde.

Legen Sie für eine sichere Freigabe die folgenden Registrierungswerte unter `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server` fest:

Registrierungswert	Beschreibung	Standardwert	Bemerkungen
LinkExpire	Zeitspanne, nach der eine freigegebene URL abläuft. Als Zeitgeberticks mit der Einheit 10 Mikrosekunden gezählt.	1.728.000.000.000 (Der Standardwert entspricht 2 Tagen.)	-

Registrierungswert	Beschreibung	Standardwert	Bemerkungen
LinkSalt	Eine Sicherheitsmethode zum Schutz der vorhergehenden URL-Ablaufzeit	Kk2od974	Ändern Sie den Standardwert in eine beliebige Zeichenfolge, die vorzugsweise mit Ziffern endet.

### Im Webplayer integrierte Administratorprotokollierung

Der Webplayer integriert die Webseite der Administratorprotokollierung. Ein Administrator mit den Rollen **LoggingReader** und **Player** kann die Administratoraktivitätsprotokolle im Webplayer anzeigen.

**Hinweis:**

Die für den Webplayer-Browser festgelegte Sprache muss mit der Sprache übereinstimmen, die Sie bei der Installation der Verwaltungskomponenten der Sitzungsaufzeichnung ausgewählt haben.

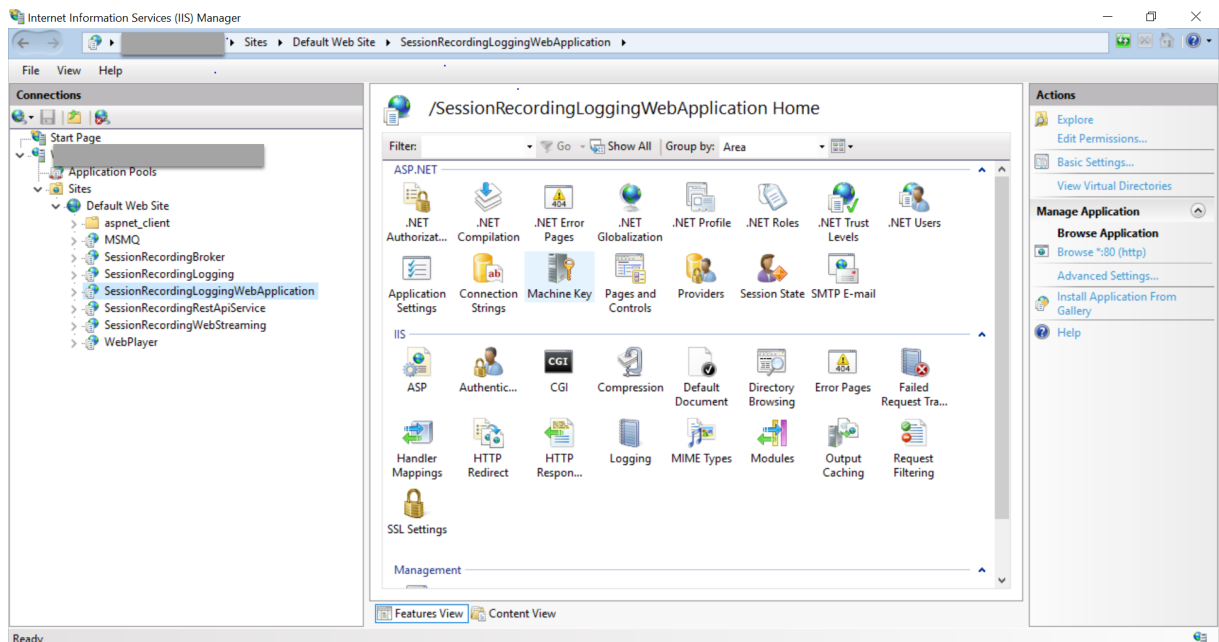
- Konfigurationsprotokollierung:

ID	Logging Time	Task Category	Component Affected	Task Details	Task Executed By	Authorized
18	2/22/2021 10:07 PM	Recording File Play Back	Session Recording Player	Action = Session File Path and Size Query ...	[Redacted]	true
17	2/22/2021 10:06 PM	Recording File Play Back	Session Recording Player	Action = Session File Path and Size Query ...	[Redacted]	true
16	2/22/2021 9:41 PM	Recording File Play Back	Session Recording Player	Action = Session File Path and Size Query ...	[Redacted]	true
15	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	Action = Session File Path and Size Query ...	[Redacted]	true
14	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	Action = Session File Path and Size Query ...	[Redacted]	true
13	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	Action = Session File Path and Size Query ...	[Redacted]	true
12	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	Action = Session File Path and Size Query ...	[Redacted]	true
11	2/22/2021 9:32 PM	Recording File Play Back	Session Recording Player	Action = Session File Path and Size Query ...	[Redacted]	true
10	2/22/2021 9:31 PM	Recording File Play Back	Session Recording Player	Action = Session File Path and Size Query ...	[Redacted]	true
9	2/22/2021 9:31 PM	Recording File Play Back	Session Recording Player	Action = Session File Path and Size Query ...	[Redacted]	true

- Protokollierung des Aufzeichnungsgrunds

ID	Logging Time	Task Category	Component Affected	Task Details	Task Executed By	Authorized
32	2/9/2021 1:26 AM	Event Logging Reason	Session Recording Agent	Applications = GDDC:Desktop###Desktop...		true
31	2/9/2021 1:26 AM	Email Alert Reason	Session Recording Agent	Applications = GDDC:Desktop###Desktop...		true
30	2/9/2021 1:26 AM	Record Reason	Session Recording Agent	Applications = GDDC:Desktop###Desktop...		true
29	2/9/2021 1:24 AM	Event Logging Reason	Session Recording Agent	Applications = GDDC:Desktop###Desktop...		true
28	2/9/2021 1:24 AM	Email Alert Reason	Session Recording Agent	Applications = GDDC:Desktop###Desktop...		true
27	2/9/2021 1:24 AM	Record Reason	Session Recording Agent	Applications = GDDC:Desktop###Desktop...		true
26	2/9/2021 1:21 AM	Event Logging Reason	Session Recording Agent	Applications = GDDC:Desktop###Desktop...		true
25	2/9/2021 1:21 AM	Email Alert Reason	Session Recording Agent	Applications = GDDC:Desktop###Desktop...		true
24	2/9/2021 1:21 AM	Record Reason	Session Recording Agent	Applications = GDDC:Desktop###Desktop...		true
23	2/9/2021 1:18 AM	Event Logging Reason	Session Recording Agent	Applications = GDDC:Desktop###Desktop...		true

Stellen Sie sicher, dass Ihre Site **SessionRecordingLoggingWebApplication** in IIS und im Webplayer dieselben SSL-Einstellungen haben. Andernfalls kommt es beim Zugriff auf die Administratoraktivitätsprotokolle zu 403-Fehlern.



## Problembehandlung

June 21, 2021

In diesen Informationen finden Sie Lösungen zu Problemen, auf die Sie möglicherweise während oder nach der Installation der Sitzungsaufzeichnungskomponenten stoßen.

**Warnung:**

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

## Fehler bei der Installation von Serverkomponenten

June 21, 2021

Die Installation der Sitzungsaufzeichnungsserverkomponenten schlägt mit den Fehlercodes 2503 und 2502 fehl.

Lösung: Überprüfen Sie die Zugriffssteuerungsliste (ACL) im Ordner C:\windows\temp, um sicherzustellen, dass lokale Benutzer und Gruppen Schreibberechtigung für diesen Ordner haben. Falls nicht, fügen Sie die Schreibberechtigung manuell hinzu.

## Fehler beim Test der Datenbankverbindung während der Installation

June 21, 2021

Bei der Installation der Datenbank für die Sitzungsaufzeichnung oder des Sitzungsaufzeichnungsservers schlägt der Test der Verbindung fehl und es wird die Fehlermeldung **Database connection test failed. Please correct Database instance name** angezeigt, selbst wenn der Datenbankinstanzname richtig ist.

Stellen Sie in diesem Fall sicher, dass der aktuelle Benutzer die öffentliche SQL Server-Rollenberechtigung hat, damit der Test nicht aufgrund einer fehlenden Berechtigung fehlschlägt.

## Agent kann keine Verbindung mit dem Server herstellen

January 15, 2024

Wenn der Sitzungsaufzeichnungsagent keine Verbindung mit dem Sitzungsaufzeichnungsserver herstellen kann, wird die Ereignismeldung **Exception caught while sending poll messages to Session**

**Recording Broker** gefolgt vom Ausnahmetext protokolliert. Der Ausnahmetext gibt die Gründe für den Verbindungsfehler an. Es sind folgende Ursachen möglich:

- **Die zugrundeliegende Verbindung wurde geschlossen. Eine vertrauenswürdige Beziehung konnte für den sicheren Kanal (SSL/TLS) nicht erstellt werden.** Diese Ausnahme bedeutet, dass der Sitzungsaufzeichnungsserver ein Zertifikat verwendet, das von einer Zertifizierungsstelle signiert ist, die der Server mit dem Sitzungsaufzeichnungsagent nicht als vertrauenswürdig einstuft oder, dass der Server der den Sitzungsaufzeichnungsagent hostet kein Zertifikat der Zertifizierungsstelle hat. Das Zertifikat kann auch abgelaufen oder widerrufen sein.

Lösung: Stellen Sie sicher, dass das richtige Zertifikat der Zertifizierungsstelle auf dem Server mit dem Sitzungsaufzeichnungsagent installiert ist oder ein vertrauenswürdiges Zertifikat verwendet wird.

- **Der Remoteserver gaben einen Fehler zurück: (403) verboten.** Dies ist ein HTTPS-Standardfehler, der angezeigt wird, wenn Sie eine Verbindung mit HTTP (nicht sicheres Protokoll) versuchen. Die Maschine mit dem Sitzungsaufzeichnungsserver lehnt die Verbindung ab, da sie nur sichere Verbindungen akzeptiert.

Lösung: Ändern Sie in den Eigenschaften des Sitzungsaufzeichnungsagents das Protokoll des Sitzungsaufzeichnungsbrokers in **HTTPS**.

- **Der Sitzungsaufzeichnungsbroker gab beim Auswerten einer Aufzeichnungsrichtlinienabfrage einen unbekanntes Fehler zurück. Fehlercode 5 (Zugriff verweigert). Weitere Informationen finden Sie im Ereignisprotokoll auf dem Sitzungsaufzeichnungsserver.** Dieser Fehler tritt auf, wenn Sitzungen gestartet werden und eine Anfrage für eine Auswertung der Aufzeichnungsrichtlinie gemacht wird. Der Fehler tritt auf, wenn die Gruppe der authentifizierten Benutzer (die Standardmitglieder) von der Rolle "PolicyQuery" in der Sitzungsaufzeichnungsautorisierungskonsole entfernt werden.

Lösung: Fügen Sie die Gruppe der authentifizierten Benutzer wieder der Rolle hinzu oder fügen Sie alle Server mit dem Sitzungsaufzeichnungsagent der Rolle "PolicyQuery" hinzu.

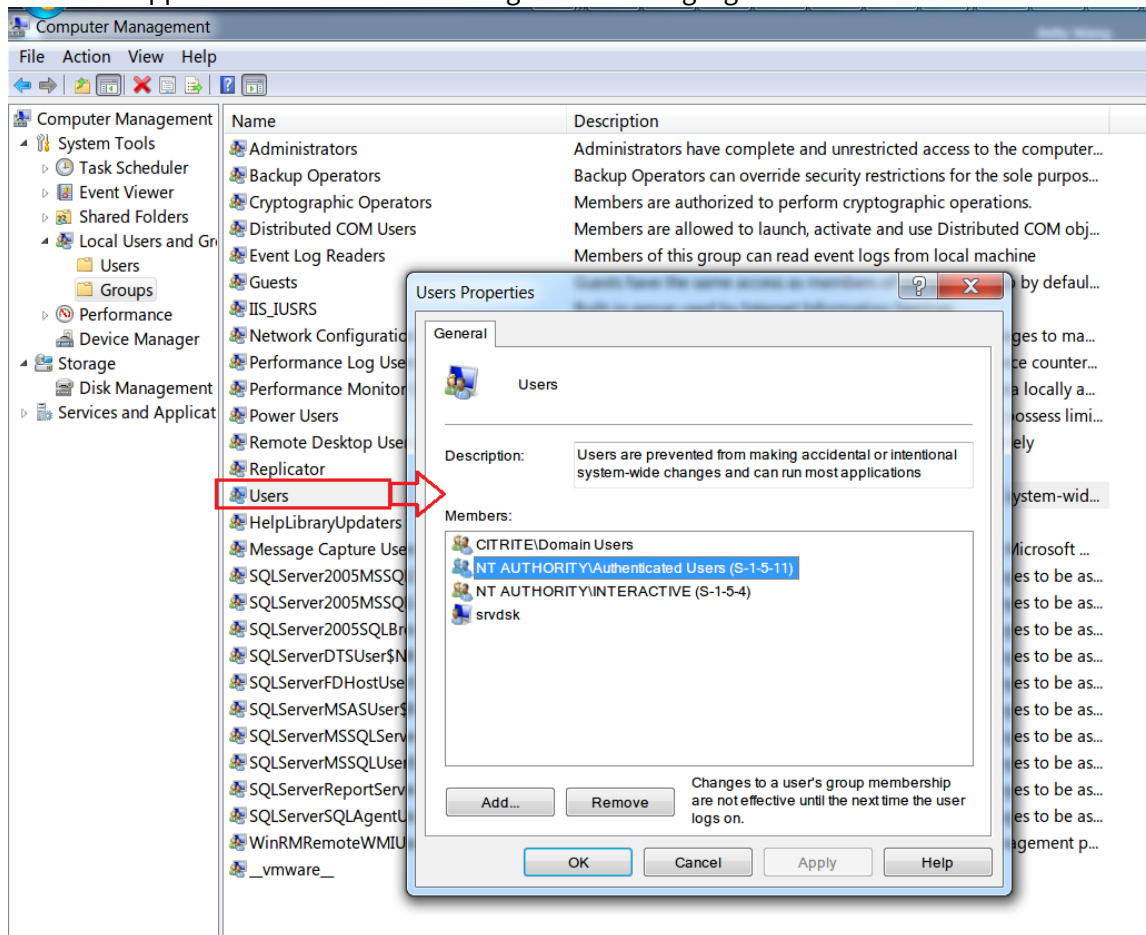
- **Die zugrundeliegende Verbindung wurde geschlossen. Eine Verbindung, die aktiv bleiben sollte, wurde vom Server geschlossen.** Dieser Fehler bedeutet, dass der Sitzungsaufzeichnungsserver nicht ausgeführt wird oder keine Anfragen annehmen kann. IIS können offline geschaltet sein oder werden neu gestartet oder der Server ist offline geschaltet.

Lösung: Stellen Sie sicher, dass der Sitzungsaufzeichnungsserver gestartet wurde, IIS auf dem Server ausgeführt wird und der Server eine Verbindung zum Netzwerk hat.

- **Der Remoteserver hat einen Fehler zurückgegeben: 401 (Nicht autorisiert).** Dieser Fehler manifestiert sich auf folgende Weise:

- Beim Start des Sitzungsaufzeichnungsagentdienst wird ein Fehler mit der Beschreibung des 401-Fehlers im Ereignisprotokoll aufgezeichnet.
- Richtlinienabfrage schlägt auf dem Sitzungsaufzeichnungsagent fehl.
- Sitzungsaufzeichnungen werden nicht auf dem Sitzungsaufzeichnungsagent erfasst.

Lösung: Stellen Sie sicher, dass die Gruppe **NT AUTHORITY\Authenticated Users** Mitglied der lokalen Gruppe **Benutzer** auf dem Sitzungsaufzeichnungsagent ist.



## Verbindungsfehler zwischen dem Server und der Datenbank

June 21, 2021

Wenn der Sitzungsaufzeichnungsserver keine Verbindung mit der Datenbank für die Sitzungsaufzeichnung herstellen kann, wird möglicherweise eine Fehlermeldung mit ungefähr dem folgenden Wortlaut angezeigt:

**Ereignisquelle:**



**A network-related or instance-specific error occurred while establishing a connection to SQL Server.** Dieser Fehler wird mit der ID 2047 im Anwendungsereignisprotokoll der Ereignisanzeige des Computers aufgezeichnet, auf dem der Sitzungsaufzeichnungsserver gehostet wird.

**Citrix Speichermanager der Sitzungsaufzeichnung - Beschreibung: Citrix: Ausnahme beim Herstellen der Datenbankverbindung.** Dieser Fehler wird im Anwendungsereignisprotokoll der Ereignisanzeige der Maschine aufgezeichnet, auf der der Sitzungsaufzeichnungsserver gehostet wird.

**Verbindung mit dem Sitzungsaufzeichnungsserver kann nicht hergestellt werden. Überprüfen Sie, ob der Sitzungsaufzeichnungsserver ausgeführt wird.** Diese Fehlermeldung wird angezeigt, wenn Sie die Richtlinienkonsole für die Sitzungsaufzeichnung starten.

Lösung:

- Die Express Edition von Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, Microsoft SQL Server 2014 oder Microsoft SQL Server 2016 ist auf einem eigenständigen Server installiert und Dienste oder Einstellungen sind nicht richtig für die Sitzungsaufzeichnung konfiguriert. Auf dem Server muss das TCP/IP-Protokoll aktiviert sein, und der SQL Server Browser-Dienst muss ausgeführt werden. Weitere Informationen zur Aktivierung dieser Einstellungen finden Sie in der Microsoft Dokumentation.
- Bei der Installation der Sitzungsaufzeichnung (Verwaltungskomponenten) wurden falsche Server- und Datenbankinformationen angegeben. Deinstallieren Sie die Datenbank für die Sitzungsaufzeichnung und installieren Sie sie mit den richtigen Informationen neu.
- Der Server mit der Datenbank für die Sitzungsaufzeichnung ist ausgefallen. Prüfen Sie die Serverkonnektivität.
- Die Maschine mit dem Sitzungsaufzeichnungsserver oder die Maschine mit dem Datenbankserver für die Sitzungsaufzeichnung kann den vollqualifizierten Domännennamen oder den NetBIOS-Namen des jeweils anderen nicht auflösen. Stellen Sie mit "Ping" sicher, dass die Namen aufgelöst werden können.
- Prüfen Sie, ob in der Firewallkonfiguration für die Datenbank für die Sitzungsaufzeichnung SQL Server-Verbindungen zugelassen sind. Weitere Informationen finden Sie im Microsoft-Artikel <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>.

**Logon failed for user 'NT\_AUTHORITY\ANONYMOUS LOGON'.** Diese Fehlermeldung gibt an, dass die Dienste falsch als .\administrator angemeldet sind.

Lösung: Starten Sie die Dienste als lokaler Systembenutzer und die SQL-Dienste neu.

## Sitzungen werden nicht aufgezeichnet

June 21, 2021

Wenn die Anwendungssitzungen nicht aufgezeichnet werden, prüfen Sie auf dem VDA für Multisitzungs-OS, auf dem der Sitzungsaufzeichnungsagent und der Sitzungsaufzeichnungsserver ausgeführt werden, das Anwendungsereignisprotokoll in der Ereignisanzeige. Auf diese Weise können Sie nützliche Diagnoseinformationen erhalten.

Wenn Sitzungen nicht aufgezeichnet werden, kann dies folgende Ursachen haben:

- **Komponentenverbindungen und Zertifikate.** Wenn die Sitzungsaufzeichnungskomponenten nicht miteinander kommunizieren können, können Sitzungsaufzeichnungen fehlschlagen. Bei Aufzeichnungsproblemen sollten Sie überprüfen, ob alle Komponenten richtig konfiguriert sind und auf die richtigen Maschinen verweisen, und ob Zertifikate gültig und richtig installiert sind.
- **Umgebungen ohne Active Directory-Domäne.** Die Sitzungsaufzeichnung ist für eine Ausführung in einer Microsoft Active Directory-Domänenumgebung konzipiert. Wenn Sie keine Active Directory-Umgebung ausführen, können Aufzeichnungsprobleme auftreten. Stellen Sie sicher, dass alle Komponenten der Sitzungsaufzeichnung auf Maschinen ausgeführt werden, die Mitglieder einer Active Directory-Domäne sind.
- **Die Sitzungsfreigabe verursacht einen Konflikt mit der aktiven Richtlinie:** Die Sitzungsaufzeichnung ordnet die aktive Richtlinie der ersten veröffentlichten Anwendung zu, die ein Benutzer öffnet. Anwendungen, die später in derselben Sitzung geöffnet werden, halten die Richtlinie ein, die für die erste Anwendung gilt. Veröffentlichen Sie die problematischen Anwendungen auf separaten VDAs für Multisitzungs-OS, um einen Konflikt zwischen der Sitzungsfreigabe und der aktiven Richtlinie zu vermeiden.
- **Die Aufzeichnung ist nicht aktiviert:** Wenn Sie den Sitzungsaufzeichnungsagent auf einem VDA für Multisitzungs-OS installieren, wird die Aufzeichnung für den VDA standardmäßig aktiviert. Die Aufzeichnung erfolgt erst, wenn eine aktive Aufzeichnungsrichtlinie konfiguriert ist, die Aufzeichnungen zulässt.
- **Die aktive Aufzeichnungsrichtlinie lässt die Aufzeichnung nicht zu.** Sitzungen können nur aufgezeichnet werden, wenn sie die Regeln der aktiven Aufzeichnungsrichtlinie erfüllen.
- **Die Dienste der Sitzungsaufzeichnung werden nicht ausgeführt.** Zum Aufzeichnen von Sitzungen muss der Sitzungsaufzeichnungsagent auf dem VDA für Multisitzungs-OS und der Speichermanager der Sitzungsaufzeichnung auf der Maschine mit dem Sitzungsaufzeichnungsserver ausgeführt werden.
- **MSMQ ist nicht konfiguriert:** Wenn MSMQ auf dem Computer mit dem Sitzungsaufzeichnungsagent und der Maschine mit dem Sitzungsaufzeichnungsserver falsch konfiguriert ist, können Aufzeichnungsprobleme auftreten.

## Wiedergabe von Livesitzungen nicht möglich

June 21, 2021

Wenn Sie Probleme beim Wiedergeben von Aufzeichnungen im Sitzungsaufzeichnungsplayer haben, werden möglicherweise die folgenden Fehlermeldungen angezeigt:

**Fehler beim Download der Sitzungsaufzeichnungsdatei. Wiedergabe einer Livesitzung ist nicht zulässig. Die Konfiguration des Servers lässt diese Funktion nicht zu.** Dieser Fehler gibt an, dass der Server die Aktion nicht zulässt.

Lösung: Klicken Sie unter **Sitzungsaufzeichnungsserver - Eigenschaften** auf die Registerkarte **Wiedergabe** und aktivieren Sie das Kontrollkästchen **Wiedergabe von Livesitzungen zulassen**.

## Aufzeichnungen sind beschädigt oder unvollständig

July 20, 2021

- Wenn Aufzeichnungen beim Anzeigen im Sitzungsaufzeichnungsplayer beschädigt oder unvollständig sind, werden u. U. auch Warnungen in den Ereignisprotokollen auf dem Sitzungsaufzeichnungsagent protokolliert.

**Ereignisquelle:** Citrix Speichermanager der Sitzungsaufzeichnung

**Beschreibung:** Datenverlust bei der Aufzeichnung von **<Name der ICL-Datei>**.

Das Problem tritt auf, wenn mit MCS oder PVS VDAs mit einem Masterimage und installiertem Microsoft Message Queuing (MSMQ) erstellt werden. In diesem Fall haben die VDAs die gleiche QMId für MSMQ.

Erstellen Sie als Workaround eine eindeutige QMId für jeden VDA. Weitere Informationen finden Sie unter [Installieren, Aktualisieren und Deinstallieren](#).

- Im Sitzungsaufzeichnungsplayer wird bei der Wiedergabe einer Aufzeichnungsdatei möglicherweise folgender interner Fehler gemeldet: **Die wiedergegebene Datei meldet, dass ein interner Systemfehler (Fehlercode: 9) bei der Originalaufzeichnung aufgetreten ist. Die Datei kann noch bis zu der Stelle wiedergegeben werden, an der der Aufzeichnungsfehler auftrat.**

Das Problem tritt aufgrund unzureichender Puffergröße auf dem Sitzungsaufzeichnungsagent auf, wenn grafikintensive Sitzungen aufgezeichnet werden.

Wählen Sie als Workaround im Sitzungsaufzeichnungsagent einen höheren Wert für `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SmAudBufferSizeMB` und starten Sie die Maschine neu.

## Prüfen der Komponentenverbindungen

November 5, 2021

Beim Setup der Sitzungsaufzeichnung stellen die Komponenten möglicherweise keine Verbindung mit den anderen Komponenten her. Alle Komponenten kommunizieren mit dem Sitzungsaufzeichnungsserver (Broker). In der Standardeinstellung ist der Broker (eine IIS-Komponente) mit dem Standardwebsitzertifikat von IIS gesichert. Wenn eine Komponente keine Verbindung mit dem Sitzungsaufzeichnungsserver herstellen kann, kann der Verbindungsversuch der anderen Komponenten auch fehlschlagen.

Der Sitzungsaufzeichnungsagent und der Sitzungsaufzeichnungsserver (Speichermanager und Broker) protokollieren Verbindungsfehler im Ereignisprotokoll der Anwendungen in der Ereignisanzeige auf der Maschine mit dem Sitzungsaufzeichnungsserver. Die Richtlinienkonsole für die Sitzungsaufzeichnung und der Sitzungsaufzeichnungsplayer zeigen Fehlermeldungen auf dem Bildschirm an, wenn keine Verbindung hergestellt werden kann.

### Prüfen, ob der Sitzungsaufzeichnungsagent verbunden ist

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Klicken Sie im Menü **Start** auf **Sitzungsaufzeichnungsagent - Eigenschaften**.
3. Klicken Sie unter **Sitzungsaufzeichnungsagent - Eigenschaften** auf **Verbindung**.
4. Stellen Sie sicher, dass der richtige FQDN im Feld **Sitzungsaufzeichnungsserver** eingegeben wird.
5. Stellen Sie sicher, dass der Multisitzungs-OS-VDA auf den Server zugreifen kann, der als Sitzungsaufzeichnungsserver angegeben wurde.

**Hinweis:** Überprüfen Sie das Anwendungsereignisprotokoll auf Fehler und Warnungen.

### Prüfen, ob der Sitzungsaufzeichnungsserver verbunden ist

#### **Achtung:**

Die Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt

keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr.

1. Melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an.
2. Öffnen Sie den Registrierungs-Editor.
3. Gehen Sie zu HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.
4. Stellen Sie sicher, dass der Wert für **SmAudDatabaseInstance** auf die Datenbank für die Sitzungsaufzeichnung verweist, die Sie in der SQL Server-Instanz installiert haben.

### Prüfen, ob die Datenbank für die Sitzungsaufzeichnung verbunden ist

1. Öffnen Sie mit einem SQL-Verwaltungswerkzeug die SQL-Instanz, die die installierte Sitzungsaufzeichnungsdatenbank enthält.
2. Öffnen Sie die Sicherheitsberechtigungen der Datenbank für die Sitzungsaufzeichnung.
3. Stellen Sie sicher, dass das Computerkonto der Sitzungsaufzeichnung Zugriffsrechte auf die Datenbank hat. Beispiel: Wenn die Maschine mit dem Sitzungsaufzeichnungsserver in der MIS-Domäne **SsRecSrv** genannt wird, muss das Computerkonto in der Datenbank als **MIS\SsRecSrv\$** konfiguriert werden. Dieser Wert wird während der Installation der Datenbank für die Sitzungsaufzeichnung konfiguriert.

### Testen der IIS-Konnektivität

Mit dem Testen der Verbindungen zwischen Sitzungsaufzeichnungsserver und IIS-Site unter Zugriff auf die Webseite des Sitzungsaufzeichnungsbrokers mit einem Webbrowser können Sie feststellen, ob Kommunikationsprobleme zwischen den Sitzungsaufzeichnungskomponenten auf eine falsche Protokollkonfiguration, Zertifizierungsprobleme oder Probleme beim Start des Sitzungsaufzeichnungsbrokers zurückzuführen sind.

Prüfen der IIS-Konnektivität für den Sitzungsaufzeichnungsagent

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent installiert ist.
2. Öffnen Sie einen Webbrowser und geben Sie die folgende Adresse ein:
  - HTTPS: <https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl>, wobei **servername** der Name der Maschine ist, auf der der Sitzungsaufzeichnungsserver ausgeführt wird.
  - HTTP: <http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl>, wobei **servername** der Name der Maschine ist, auf der der Sitzungsaufzeichnungsserver ausgeführt wird.

3. Wenn Sie zur NTLM-Authentifizierung aufgefordert werden, melden Sie sich mit dem Domänenadministratorkonto an.

Prüfen der IIS-Konnektivität für den Sitzungsaufzeichnungsplayer

1. Melden Sie sich bei der Arbeitsstation an, auf der der Sitzungsaufzeichnungsplayer installiert ist.
2. Öffnen Sie einen Webbrowser und geben Sie die folgende Adresse ein:
  - HTTPS: <https://servername/SessionRecordingBroker/Player.rem?wsdl>, wobei `servername` der Name der Maschine ist, auf der der Sitzungsaufzeichnungsserver ausgeführt wird.
  - HTTP: <http://servername/SessionRecordingBroker/Player.rem?wsdl>, wobei `servername` der Name der Maschine ist, auf der der Sitzungsaufzeichnungsserver ausgeführt wird.
3. Wenn Sie zur NTLM-Authentifizierung aufgefordert werden, melden Sie sich mit dem Domänenadministratorkonto an.

Prüfen der IIS-Konnektivität für die Richtlinienkonsole für die Sitzungsaufzeichnung

1. Melden Sie sich bei dem Server an, auf dem die Richtlinienkonsole für die Sitzungsaufzeichnung installiert ist.
2. Öffnen Sie einen Webbrowser und geben Sie die folgende Adresse ein:
  - HTTPS: <https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl>, wobei `servername` der Name der Maschine ist, auf der der Sitzungsaufzeichnungsserver ausgeführt wird.
  - HTTP: <http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl>, wobei `servername` der Name der Maschine ist, auf der der Sitzungsaufzeichnungsserver ausgeführt wird.
3. Wenn Sie zur NTLM-Authentifizierung aufgefordert werden, melden Sie sich mit dem Domänenadministratorkonto an.

Wenn ein XML-Dokument im Browser angezeigt wird, bestätigt dies, dass die Maschine, auf der die Richtlinienkonsole für die Sitzungsaufzeichnung ausgeführt wird, mit der Sitzungsaufzeichnungsserver-Maschine verbunden ist und das konfigurierte Protokoll verwendet.

## Problembehandlung bei Zertifikaten

Wenn Sie HTTPS als Kommunikationsprotokoll verwenden, muss die Maschine mit dem Sitzungsaufzeichnungsserver mit einem Serverzertifikat konfiguriert werden. Alle Komponentenverbindungen

mit dem Sitzungsaufzeichnungsserver müssen ein Zertifikat der Stammzertifizierungsstelle haben. Sonst schlagen die Verbindungen zwischen den Komponenten fehl.

Sie können die Zertifikate genauso wie beim Testen der IIS-Konnektivität durch Zugriff auf die Webseite des Sitzungsaufzeichnungsbrowsers testen. Wenn Sie auf die XML-Seite für jede Komponente zugreifen können, sind die Zertifikate richtig konfiguriert.

Im Anschluss finden Sie Gründe, warum Zertifikate zu Verbindungsproblemen führen:

- **Ungültige oder fehlende Zertifikate:** Wenn der Server mit dem Sitzungsaufzeichnungsagent kein Stammzertifikat für die Vertrauenswürdigkeit des Serverzertifikats hat, den Sitzungsaufzeichnungsserver nicht als vertrauenswürdig ansieht und keine Verbindung über HTTPS herstellen kann, schlägt die Verbindung fehl. Stellen Sie in diesem Fall sicher, dass alle Komponenten das Serverzertifikat auf dem Sitzungsaufzeichnungsserver als vertrauenswürdig einstufen.
- **Inkonsistente Benennung:** Wenn das Serverzertifikat, das der Maschine mit dem Sitzungsaufzeichnungsserver zugewiesen ist, mit einem FQDN erstellt wurde, müssen alle Komponenten, die eine Verbindung herstellen, für die Verbindung mit dem Sitzungsaufzeichnungsserver den FQDN verwenden. Wenn ein NetBIOS-Name verwendet wird, konfigurieren Sie die Komponenten mit einem NetBIOS-Namen für den Sitzungsaufzeichnungsserver.
- **Abgelaufene Zertifikate.** Wenn ein Serverzertifikat abgelaufen ist, schlägt eine Verbindung mit dem Sitzungsaufzeichnungsserver über HTTPS fehl. Stellen Sie sicher, dass das Zertifikat, das der Maschine mit dem Sitzungsaufzeichnungsserver zugewiesen ist, gültig und nicht abgelaufen ist. Wenn dasselbe Zertifikat für die digitale Signatur der Sitzungsaufzeichnungen verwendet wird, enthält das Ereignisprotokoll der Maschine mit dem Sitzungsaufzeichnungsserver Fehlermeldungen, dass das Zertifikat abgelaufen ist, oder Warnmeldungen, wenn das Zertifikat bald abläuft.

## Fehler beim Suchen nach Aufzeichnungen im Player

November 5, 2021

Wenn Sie Probleme beim Suchen nach Aufzeichnungen im Sitzungsaufzeichnungsplayer haben, werden möglicherweise die folgenden Fehlermeldungen angezeigt:

- **Fehler bei der Suche nach Sitzungsaufzeichnungsdateien. Der Name des Remoteservers konnte nicht aufgelöst werden: servername.** **Servername** ist der Name des Servers, mit dem der Sitzungsaufzeichnungsplayer versucht, eine Verbindung herzustellen. Der Sitzungsaufzeichnungsplayer kann den Sitzungsaufzeichnungsserver nicht kontaktieren. Zu den beiden möglichen Gründen gehören ein falsch eingegebener Servername, oder DNS kann den Servernamen nicht auflösen.

Lösung: Klicken Sie im Player-Menü auf **Extras > Optionen > Verbindungen** und prüfen Sie die Richtigkeit des Servernamens, der in der Liste **Sitzungsaufzeichnungsserver** aufgeführt ist. Wenn der Name richtig ist, stellen Sie mit dem Ping-Befehl sicher, dass der Name aufgelöst werden kann. Wenn der Sitzungsaufzeichnungsserver nicht betriebsbereit oder offline geschaltet ist, tritt ein Fehler beim Suchen nach Sitzungsaufzeichnungsdateien auf. Die Fehlermeldung ist **Fehler beim Verbinden mit dem Remoteserver**.

- **Fehler beim Verbinden mit dem Remoteserver.** Dieser Fehler tritt auf, wenn der Sitzungsaufzeichnungsserver nicht betriebsbereit oder offline geschaltet ist.

Resolution: Verify that the Session Recording Server is connected.

- **Zugriff verweigert.** Ein Fehler "Zugriff verweigert" kann auftreten, wenn der Benutzer nicht berechtigt ist, Sitzungsaufzeichnungsdateien zu suchen und herunterzuladen.

Lösung: Weisen Sie den Benutzer in der Sitzungsaufzeichnungs-Autorisierungskonsole der Rolle "Player" zu.

- **Zugriff bei zugewiesener Playerrolle verweigert.** Dieser Fehler tritt auf, wenn Sie den Sitzungsaufzeichnungsplayer auf derselben Maschine wie den Sitzungsaufzeichnungsserver installiert und die Benutzerkontensteuerung (UAC) aktiviert haben. Wenn Sie der Playerrolle die Gruppe der Domänenadministratoren oder Administratoren zuweisen, kann es vorkommen, dass ein in der Gruppe enthaltenes, nicht integriertes Administratorkonto bei der Suche von Aufzeichnungen mit dem Sitzungsaufzeichnungsplayer die rollenbasierte Prüfung nicht besteht.

Resolutions:

- Run the Session Recording Player as an administrator.
- Assign specific users as the Player role rather than the entire group.
- Install the Session Recording Player in a separate machine rather than Session Recording Server.

- **Fehler bei der Suche nach Sitzungsaufzeichnungsdateien. Die zugrundeliegende Verbindung wurde geschlossen. Eine vertrauenswürdige Beziehung konnte für den sicheren Kanal (SSL/TLS) nicht erstellt werden.** Dieser Fehler tritt auf, wenn der Sitzungsaufzeichnungsserver ein Zertifikat verwendet, das von einer Zertifizierungsstelle signiert ist, die das Clientgerät nicht vertrauenswürdig ansieht oder für die das Clientgerät kein Zertifikat der Zertifizierungsstelle hat.

Resolution: Install the correct or trusted CA certificate workstation where the Session Recording Player is installed.

- **Der Remoteserver gab einen Fehler zurück: (403) verboten.** Dies ist ein HTTPS-Standardfehler, der angezeigt wird, wenn Sie eine Verbindung mit HTTP (nicht sicheres



Protokoll) versuchen. Der Server lehnt die Verbindung ab, da er standardmäßig nur sichere Verbindungen annimmt.

Lösung: Klicken Sie auf der Menüleiste des **Sitzungsaufzeichnungsplayers** auf **Extras > Optionen > Verbindungen**. Wählen Sie den Server aus der Liste **Sitzungsaufzeichnungsserver** aus und klicken Sie auf **Ändern**. Ändern Sie das Protokoll von **HTTP** in **HTTPS**.

## Problembehandlung bei MSMQ

Wenn eine Benachrichtigung angezeigt wird, mit einer Suche im Sitzungsaufzeichnungsplayer jedoch keine Aufzeichnungen gefunden werden, kann ein Problem mit MSMQ bestehen. Prüfen Sie, ob die Warteschlange mit dem Sitzungsaufzeichnungsserver (Speichermanager) verbunden ist. Testen Sie mit einem Webbrowser, ob Verbindungsfehler bestehen (wenn Sie HTTP oder HTTPS als MSMQ-Kommunikationsprotokoll verwenden).

Sicherstellen der Verbindung der Warteschlange

1. Melden Sie sich bei dem Server an, auf dem der Sitzungsaufzeichnungsagent gehostet wird, und zeigen Sie die ausgehenden Warteschlangen an.
2. Stellen Sie sicher, dass die Warteschlange der Maschine mit dem Sitzungsaufzeichnungsserver verbunden ist.
  - Wenn der Zustand **Warten auf Verbindung** ist, Nachrichten in der Warteschlange sind und als Protokoll HTTP oder HTTPS verwendet wird (gemäß Auswahl auf der Registerkarte **Verbindungen** unter **Sitzungsaufzeichnungsagent - Eigenschaften**), führen Sie Schritt 3 aus.
  - Wenn der Zustand **Verbunden** ist und keine Nachrichten in der Warteschlange sind, besteht möglicherweise ein Problem mit dem Server, auf dem der Sitzungsaufzeichnungsserver ausgeführt wird. Überspringen Sie Schritt 3 und führen Sie Schritt 4 aus.
3. Wenn Nachrichten in der Warteschlange sind, öffnen Sie einen Webbrowser und geben Sie folgende Adresse ein:
  - HTTPS: [https://servername/msmq/private\\$/CitrixSmAudData](https://servername/msmq/private$/CitrixSmAudData), wobei [servername](#) der Name der Maschine ist, auf der der Sitzungsaufzeichnungsserver ausgeführt wird.
  - HTTP: [http://servername/msmq/private\\$/CitrixSmAudData](http://servername/msmq/private$/CitrixSmAudData), wobei [servername](#) der Name der Maschine ist, auf der der Sitzungsaufzeichnungsserver ausgeführt wird.

Wenn die Seite einen Fehler zurückgibt, z. B. **Der Server nimmt nur sichere Verbindungen an**, ändern Sie das für MSMQ unter **Sitzungsaufzeichnungsagent - Eigenschaften** aufgeführte

Protokoll in HTTPS. Wird ein Problem mit dem Websitesicherheitszertifikat gemeldet, besteht möglicherweise ein Problem mit der Vertrauensbeziehung für den sicheren Kanal (TLS). Installieren Sie dann das richtige Zertifikat der Zertifizierungsstelle oder verwenden Sie eine vertrauenswürdige Zertifizierungsstelle.

4. Wenn die Warteschlange keine Nachrichten enthält, melden Sie sich bei der Maschine mit dem Sitzungsaufzeichnungsserver an und zeigen Sie private Warteschlangen an. Wählen Sie **citrixsmalldata**. Wenn Nachrichten in der Warteschlange sind (Spalte "Nachrichtenzahl"), stellen Sie sicher, dass der Dienst des Speichermanagers der Sitzungsaufzeichnung gestartet ist. Starten Sie sonst den Dienst neu.

## Verwalten der Datensätze in der Datenbank

November 5, 2021

Das ICLDB-Hilfsprogramm (ICA Log database) ist ein Datenbankbefehlszeilenprogramm, mit dem Sie Sitzungsaufzeichnungsdatensätze in der Datenbank manipulieren. Dieses Hilfsprogramm wird mit der Sitzungsaufzeichnung in Laufwerk:\Program Files\Citrix\SessionRecording\Server\Bin auf dem Server mit der Serversoftware der Sitzungsaufzeichnung installiert.

### Übersichtstabelle

In der folgenden Tabelle finden Sie die Befehle und Optionen für das ICLDB-Hilfsprogramm. Geben Sie die Befehle im folgenden Format ein:

```
iclodb [version | locate | dormant | import | archive | remove |  
removeall] command-options [/l] [/f] [/s] [/?]
```

#### Hinweis:

Ausführlichere Anweisungen finden Sie in der Hilfe des Hilfsprogramms. Um auf die Hilfe zuzugreifen, geben Sie an der Eingabeaufforderung den Ordner Laufwerk:\Program Files\Citrix\SessionRecording\Server\Bin ein und dann `iclodb /?`. Um Hilfe für bestimmte Befehle zu erhalten, geben Sie Folgendes ein: `iclodb *command* /?`.

Befehl	Beschreibung
<code>archive</code>	Archiviert Sitzungsaufzeichnungsdateien, die älter als der angegebene Aufbewahrungszeitraum sind. Verwenden Sie diesen Befehl, um Aufzeichnungen und Ereignisse in den Aufzeichnungen zu archivieren. Die Ereignisse werden in der Datenbanktabelle <code>ArchivedEvent</code> archiviert.
<code>dormant</code>	Zählt oder zeigt die Sitzungsaufzeichnungsdateien an, die als inaktiv angesehen werden. Inaktive Dateien sind Sitzungsaufzeichnungen, die aufgrund von Datenverlust nicht abgeschlossen wurden. Verwenden Sie diesen Befehl, wenn Sie den Verdacht haben, dass Sie Daten verlieren. Sie können prüfen, ob die Sitzungsaufzeichnungsdateien für die ganze Datenbank oder nur Aufzeichnungen inaktiv werden, die in der angegebenen Anzahl von Tagen, Stunden oder Minuten aufgezeichnet wurden.
<code>import</code>	Importiert Sitzungsaufzeichnungsdateien in die Datenbank für die Sitzungsaufzeichnung. Mit diesem Befehl erstellen Sie die Datenbank neu, wenn Sie Datensätze der Datenbank verlieren. Mit diesem Befehl führen Sie auch Datenbanken zusammen (wenn Sie zwei Datenbanken haben, können Sie die Dateien von einer der Datenbanken importieren).
<code>locate</code>	Sucht und zeigt den vollständigen Pfad einer Sitzungsaufzeichnungsdatei an. Als Kriterium wird die Datei-ID verwendet. Mit diesem Befehl suchen Sie den Speicherort einer Sitzungsaufzeichnungsdatei. Außerdem können Sie mit einer bestimmten Datei prüfen, ob die Datenbank aktuell ist.

Befehl	Beschreibung
<code>remove</code>	Entfernt die Verweise auf Sitzungsaufzeichnungsdateien aus der Datenbank. Mit diesem Befehl bereinigen Sie die Datenbank (verwenden Sie diesen Befehl mit Vorsicht). Geben Sie den Aufbewahrungszeitraum als Kriterium an. Sie können auch die zugeordnete physische Datei löschen.
<code>removeall</code>	Entfernt alle Verweise auf Sitzungsaufzeichnungsdateien aus der Datenbank für die Sitzungsaufzeichnung und setzt diese auf den Originalzustand zurück. Die physische Datei wird nicht gelöscht. Sie können diese Dateien jedoch nicht im Sitzungsaufzeichnungsplayer suchen. Mit diesem Befehl bereinigen Sie die Datenbank (verwenden Sie diesen Befehl mit Vorsicht). Gelöschte Verweise können nur von einer Sicherungskopie wieder hergestellt werden.
<code>version</code>	Zeigt die Schemaversion der Datenbank für die Sitzungsaufzeichnung an.
<code>/l</code>	Protokolliert die Ergebnisse und Fehler im Windows-Ereignisprotokoll.
<code>/f</code>	Erzwingt die Ausführung des Befehls ohne Aufforderungen.
<code>/s</code>	Unterdrückt die Copyright-Nachricht.
<code>/?</code>	Zeigt die Hilfe für die Befehle an.

---

### Archivieren von Sitzungsaufzeichnungsdateien

Archivieren Sie Sitzungsaufzeichnungsdateien regelmäßig, damit an den Speicherorten für die Aufzeichnung immer ausreichend freier Platz zur Verfügung steht. Das Archivierungsintervall hängt von dem verfügbaren Speicherplatz und der Größe typischer Sitzungsaufzeichnungsdateien ab. Sitzungsaufzeichnungsdateien können ab zwei Tage nach dem Sitzungsstart archiviert werden. Diese Regel soll verhindern, dass Liveaufzeichnungen vor Abschluss archiviert werden.

Sitzungsaufzeichnungen können auf zweierlei Weise archiviert werden. Der Datenbankdatensatz

einer Sitzungsaufzeichnung kann auf den Status “Archiviert”aktualisiert werden, während die Sitzungsaufzeichnungsdatei an ihrem Speicherort verbleibt. Durch diese Methode werden die Suchergebnisse im Player verringert. Die zweite Methode besteht darin, den Datenbankdatensatz der Sitzungsaufzeichnung auf “Archiviert”zu aktualisieren und die Sitzungsaufzeichnungsdatei zur Sicherung auf ein alternatives Speichermedium zu verschieben. Bei Verwendung des ICLDB-Hilfsprogramms werden Sitzungsaufzeichnungsdateien in das angegebene Verzeichnis verschoben, in dem die ursprüngliche Ordnerstruktur “Jahr/Monat/Tag”nicht besteht.

Ein Datensatz in der Sitzungsaufzeichnungsdatenbank enthält zwei mit der Archivierung verbundene Felder: die Archivierungszeit (Datum und Uhrzeit der Archivierung) und die Archivierungsnotiz, d. h. ein optionaler Text, den der Administrator bei der Archivierung eingeben kann. Die beiden Felder weisen darauf hin, dass und wann eine Sitzungsaufzeichnung archiviert wurde.

Im Sitzungsaufzeichnungsplayer werden archivierte Sitzungsaufzeichnungen mit dem Status “Archiviert”und dem Datum und der Uhrzeit der Archivierung angezeigt. Archivierte Sitzungsaufzeichnungen können weiterhin abgespielt werden, sofern die Dateien nicht verschoben wurden. Wurde eine Sitzungsaufzeichnungsdatei bei der Archivierung verschoben, wird gemeldet, dass die Datei nicht gefunden wurde. Die Sitzungsaufzeichnungsdatei muss wiederhergestellt werden, damit sie abgespielt werden kann. Zum Wiederherzustellen einer Sitzungsaufzeichnung benötigt der Administrator die im Dialogfeld “Eigenschaften”des Sitzungsaufzeichnungsplayers zu der Sitzung angezeigte Datei-ID und Uhrzeit der Archivierung. Das Verfahren zur Wiederherstellung archivierter Dateien wird unter [Wiederherstellen von Sitzungsaufzeichnungsdateien](#) weiter unten erläutert.

Der Befehl **archive** des Hilfsprogramms ICLDB kann mit folgenden Parametern verwendet werden:

- **/RETENTION:<Tage>** - Dauer der Aufbewahrung von Sitzungsaufzeichnungen in Tagen. Aufnahmen, die älter als die angegebene Anzahl von Tagen sind, werden in der Sitzungsaufzeichnungsdatenbank als archiviert markiert. Der Aufbewahrungszeitraum muss mindestens 2 Tage betragen.
- **/LISTFILES:** vollständigen Pfad und Dateiname der Sitzungsaufzeichnungsdateien bei der Archivierung. Dieser Parameter ist optional.
- **/MOVETO:<Verzeichnis>** - Verzeichnis, in das archivierte Sitzungsaufzeichnungsdateien verschoben werden. Das Verzeichnis muss vorhanden sein. Dieser Parameter ist optional. Wird kein Verzeichnis angegeben, verbleiben die Dateien an ihrem ursprünglichen Speicherort.
- **/NOTE:<Notiz>** - Textnotiz, die dem Datenbankdatensatz für jede archivierte Sitzungsaufzeichnung hinzugefügt wird. Die Notiz muss in doppelte Anführungszeichen gesetzt werden. Dieser Parameter ist optional.
- **/L:** protokolliert Ergebnisse und Fehler in Verbindung mit den archivierten Sitzungsaufzeichnungsdateien im Windows-Ereignisprotokoll. Dieser Parameter ist optional.
- **/F:** erzwingt die Ausführung des Archivierungsbefehls ohne Aufforderungen. Dieser Parameter ist optional.

### **Archivieren von Sitzungsaufzeichnungen in der Sitzungsaufzeichnungsdatenbank unter physischem Verschieben der Sitzungsaufzeichnungsdateien**

1. Melden Sie sich als lokaler Administrator bei dem Server an, auf dem der Sitzungsaufzeichnungsserver installiert ist.
2. Rufen Sie eine Eingabeaufforderung auf.
3. Wechseln Sie vom aktuellen Arbeitsverzeichnis in das Bin-Verzeichnis des Sitzungsaufzeichnungsserver-Installationspfads (<Session Recording Server Installation Path>/Server /Bin).
4. Führen Sie den Befehl `ICLDB ARCHIVE /RETENTION:<days> /LISTFILES /MOVETO:<directory> /NOTE:<note> /L`. **days** ist der Aufbewahrungszeitraum für Sitzungsaufzeichnungsdateien, **directory** ist das Verzeichnis, in das archivierte Sitzungsaufzeichnungsdateien verschoben werden, und **note** ist eine Textnotiz, die dem Datenbankdatensatz jeder archivierten Sitzungsaufzeichnungsdatei hinzugefügt wird. Geben Sie **Y** ein, um die Archivierung zu bestätigen.

### **Ausschließliches Archivieren von Sitzungsaufzeichnungen in der Sitzungsaufzeichnungsdatenbank**

1. Melden Sie sich als lokaler Administrator bei dem Server an, auf dem der Sitzungsaufzeichnungsserver installiert ist.
2. Rufen Sie eine Eingabeaufforderung auf.
3. Wechseln Sie vom aktuellen Arbeitsverzeichnis in das Bin-Verzeichnis des Sitzungsaufzeichnungsserver-Installationspfads (<Installationspfad>/Server/Bin).
4. Führen Sie den Befehl `ICLDB ARCHIVE /RETENTION:<days> /LISTFILES /NOTE :<note> /L` aus. **days** entspricht dem Aufbewahrungszeitraum für Sitzungsaufzeichnungen und **note** ist eine Textnotiz, die dem Datenbankdatensatz jeder archivierten Sitzungsaufzeichnung hinzugefügt wird. Geben Sie **Y** ein, um die Archivierung zu bestätigen.

### **Wiederherstellen von Sitzungsaufzeichnungsdateien**

Sitzungsaufzeichnungsdateien müssen wiederhergestellt werden, wenn Sie eine Sitzungsaufzeichnung aufrufen möchten, die in der Sitzungsaufzeichnungsdatenbank unter Verschieben der Datei aus dem Speicherort der Aufzeichnung archiviert wurde. Archivierte Sitzungsaufzeichnungen, die nicht aus dem Speicherort der Aufzeichnung verschoben wurden, stehen im Sitzungsaufzeichnungsplayer weiterhin zur Verfügung.

Es gibt zwei Wiederherstellungsmethoden für Sitzungsaufzeichnungsdateien, die verschoben wurden. Kopieren der Sitzungsaufzeichnungsdatei in das Wiederherstellungsverzeichnis für archivierte Dateien, oder Reimportieren der Datei mithilfe von ICLDB in die Sitzungsaufzeichnungsdatenbank. Citrix empfiehlt das Kopieren. Entfernen Sie in das Wiederherstellungsverzeichnis kopierte archivierte Dateien, wenn Sie sie nicht mehr benötigen.

Der Sitzungsaufzeichnungsbroker verwendet das **Wiederherstellungsverzeichnis für archivierte Dateien**, wenn eine Sitzungsaufzeichnungsdatei nicht am ursprünglichen Speicherort gefunden wird. Dies passiert, wenn der Sitzungsaufzeichnungsplayer eine Sitzungsaufzeichnungsdatei zur Wiedergabe anfordert. Der Sitzungsaufzeichnungsbroker sucht die Datei zunächst am ursprünglichen Speicherort. Wird sie dort nicht gefunden, überprüft der Sitzungsaufzeichnungsbroker das **Wiederherstellungsverzeichnis**. Befindet sich die Datei im Wiederherstellungsverzeichnis, sendet der Sitzungsaufzeichnungsbroker sie zur Wiedergabe an den Sitzungsaufzeichnungsplayer. Andernfalls sendet er eine Fehlermeldung an den Sitzungsaufzeichnungsplayer, dass die Datei nicht gefunden wurde.

Beim Importieren einer archivierten Sitzungsaufzeichnungsdatei mit ICLDB wird die Sitzungsaufzeichnungsdatenbank durch die in der Datei enthaltenen Sitzungsaufzeichnungsinformationen einschließlich des neuen Speicherpfads aktualisiert. Beim Importieren mit ICLDB werden Sitzungsaufzeichnungsdateien nicht an den ursprünglichen Speicherort ihrer Aufzeichnung zurückverschoben.

**Hinweis:** Bei importierten Sitzungsaufzeichnungsdateien werden die Uhrzeit der Archivierung und die Archivierungsnotiz gelöscht. Wenn Sie das nächste Mal den ICLDB-Befehl `archive` ausführen, können solche importierten Dateien daher wieder archiviert werden.

Der ICLDB-Befehl `import` eignet sich zum Importieren großer Zahlen archivierter Sitzungsaufzeichnungsdateien, zum Reparieren bzw. Aktualisieren falscher oder fehlender Sitzungsaufzeichnungsdaten in der Sitzungsaufzeichnungsdatenbank und zum Verschieben von Sitzungsaufzeichnungsdateien an einen anderen Speicherort auf dem Sitzungsaufzeichnungsserver. Der ICLDB-Befehl `import` kann auch verwendet werden, um die Sitzungsaufzeichnungsdatenbank wieder aufzufüllen, nachdem der Befehl `removeall` ausgeführt wurde.

Der ICLDB-Befehl `import` kann mit folgenden Parametern verwendet werden:

- **/LISTFILES:** vollständigen Pfad und Dateiname der Sitzungsaufzeichnungsdateien beim Import. Dieser Parameter ist optional.
- **/RECURSIVE:** durchsucht alle Unterverzeichnisse nach Sitzungsaufzeichnungsdateien. Dieser Parameter ist optional.
- **/L:** protokolliert Ergebnisse und Fehler in Verbindung mit den importierten Sitzungsaufzeichnungsdateien im Windows-Ereignisprotokoll. Dieser Parameter ist optional.
- **/F:** erzwingt die Ausführung des Importbefehls ohne Aufforderungen. Dieser Parameter ist optional.

### **Wiederherstellen von Sitzungsaufzeichnungsdateien unter Verwendung des Wiederherstellungsverzeichnisses für archivierte Dateien**

1. Melden Sie sich als lokaler Administrator bei dem Server an, auf dem der Sitzungsaufzeichnungsserver installiert ist.
2. Sehen Sie im Sitzungsaufzeichnungsplayer unter "Eigenschaften" die Datei-ID und die Archivierungszeit der gewünschten Sitzungsaufzeichnungsdatei nach.
3. Suchen Sie die Sitzungsaufzeichnungsdatei anhand der Datei-ID in der Sicherung. Jede Sitzungsaufzeichnung hat einen Dateinamen im Format `i_<FileID>.icl`, wobei "FileID" die Datei-ID der Sitzungsaufzeichnungsdatei ist.
4. Kopieren Sie die Sitzungsaufzeichnungsdatei aus Ihrer Sicherung in das Wiederherstellungsverzeichnis für archivierte Dateien. Suchen des Wiederherstellungsverzeichnisses für archivierte Dateien
  - a) Klicken Sie im Menü **Start** auf **Start > Programme > Citrix > Sitzungsaufzeichnungsserver - Eigenschaften**.
  - b) Klicken Sie unter "Sitzungsaufzeichnungsserver - Eigenschaften" auf die Registerkarte **Speicher**. Das aktuelle Wiederherstellungsverzeichnis wird im Feld **Wählen Sie das Wiederherstellungsverzeichnis für archivierte Dateien aus** angezeigt.

### **Wiederherstellen von Sitzungsaufzeichnungsdateien mit dem ICLDB-Befehl "import"**

1. Melden Sie sich als lokaler Administrator bei dem Server an, auf dem der Sitzungsaufzeichnungsserver installiert ist.
2. Rufen Sie eine Eingabeaufforderung auf.
3. Wechseln Sie vom aktuellen Arbeitsverzeichnis in das Bin-Verzeichnis des Sitzungsaufzeichnungsserver-Installationspfads (`<Session Recording Server Installation Path>/Server /Bin`).
4. Führen Sie einen der folgenden Schritte aus:
  - Führen Sie den Befehl `ICLDB IMPORT /LISTFILES /RECURSIVE /L <directory>` aus. **directory** steht für ein oder mehrere Verzeichnisse mit Sitzungsaufzeichnungsdateien. Mehrere Verzeichnisse trennen Sie durch Leerzeichen. Geben Sie **Y** ein, um den Import zu bestätigen.
  - Führen Sie den Befehl `ICLDB IMPORT /LISTFILES /L <file>` aus. **file** ist der Name einer oder mehrerer Sitzungsaufzeichnungsdateien. Mehrere Dateien trennen Sie durch Leerzeichen. Platzhalterzeichen können beim Angeben Sitzungsaufzeichnungsdateien verwendet werden. Geben Sie **Y** ein, um den Import zu bestätigen.



## Bewährte Methoden

July 20, 2021

Die folgende Dokumentation enthält bewährte Methoden zum Bereitstellen der Sitzungsaufzeichnung und zum Konfigurieren des Lastausgleichs:

- [Konfigurieren des Lastausgleichs in einer vorhandenen Bereitstellung](#)
- [Bereitstellen und Lastausgleich der Sitzungsaufzeichnung in Azure](#)

## Konfigurieren des Lastausgleichs in einer vorhandenen Bereitstellung

January 15, 2024

Dieser Artikel beschreibt das Hinzufügen von Lastausgleichsknoten mit Citrix ADC in einer vorhandenen Sitzungsaufzeichnungsbereitstellung. Die folgenden Server werden beispielhaft in diesem Prozess verwendet. Sie können die Sitzungsaufzeichnung auch in Azure bereitstellen und einen Lastausgleich festlegen.

- Sitzungsaufzeichnung

---

Hostname	Serverrolle	OS	IP-Adresse
SRServer1	Sitzungsaufzeichnungsserver	Windows Server	10.63.32.55
LBDC	Domänencontroller	Windows Server	10.63.32.82
TSVDA	Sitzungsaufzeichnungsserver	Windows Server	10.63.32.215
SRSQL	Datenbank für die Sitzungsaufzeichnung und Dateiserver	Windows Server	10.63.32.91

---

Alle Sitzungsaufzeichnungskomponenten und der Domänencontroller teilen sich eine Domäne, zum Beispiel `lb.com`. Das Domänenadministratorkonto (zum Beispiel: `lb\administrator`) wird für die Serveranmeldung verwendet.

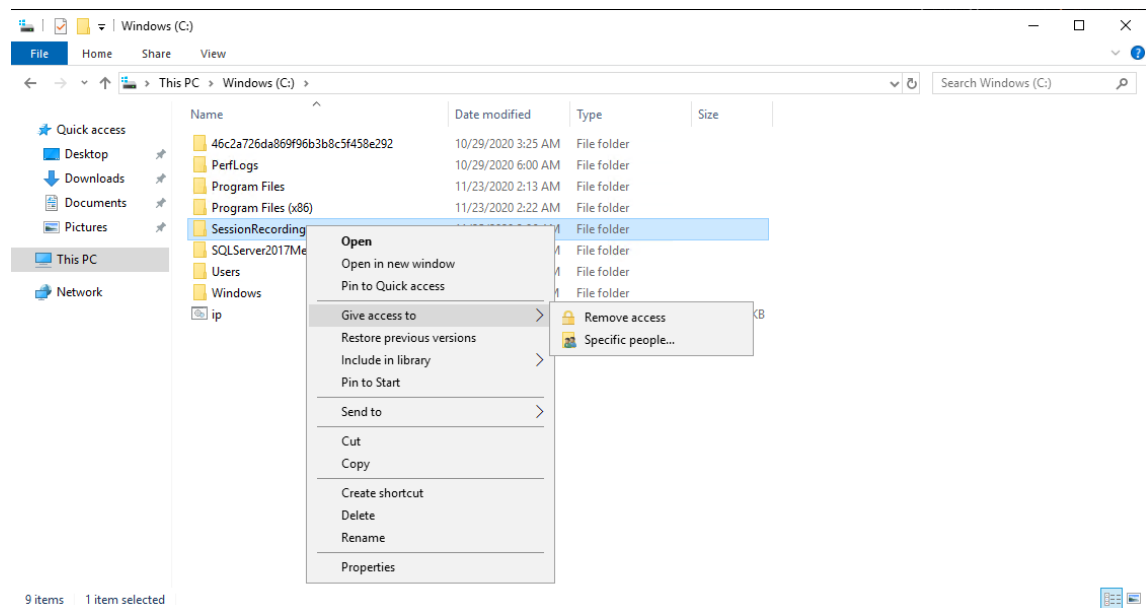
- Citrix ADC

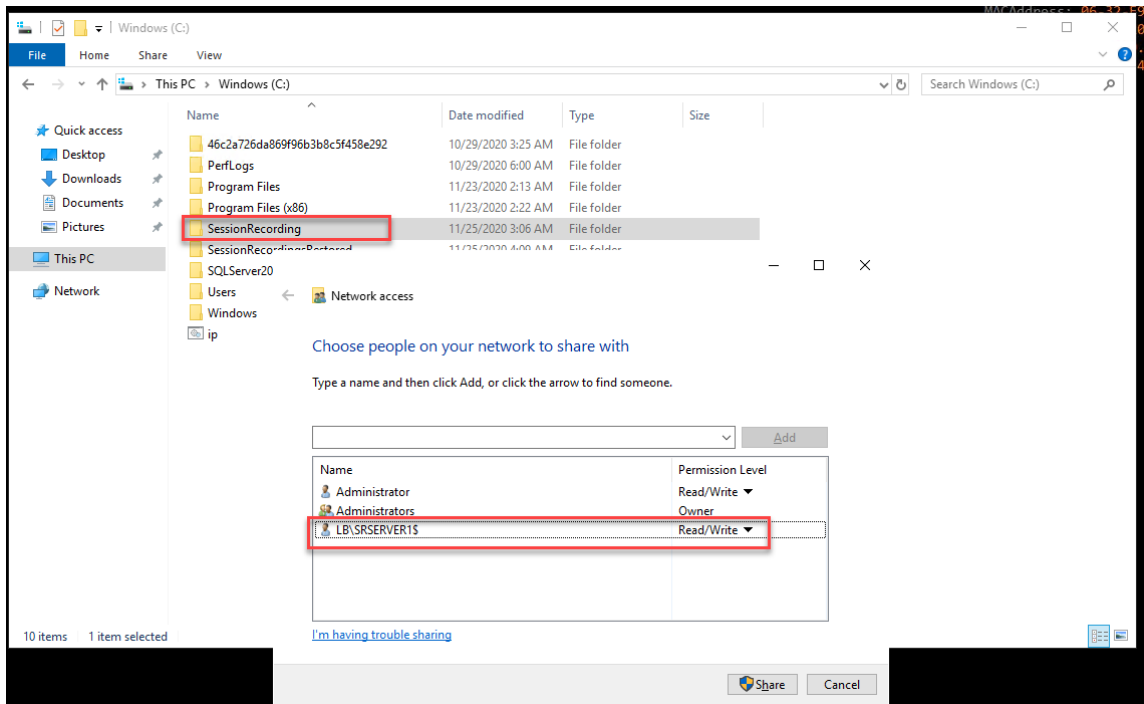
Hostname	Serverrolle	Management-IP-Adresse (NSIP)	Subnetz-IP-Adresse (SNIP)
NetScaler	Citrix ADC VPX-Instanz	10.63.32.40	10.63.32.109

Weitere Informationen finden Sie unter [Bereitstellen einer Citrix ADC VPX-Instanz](#).

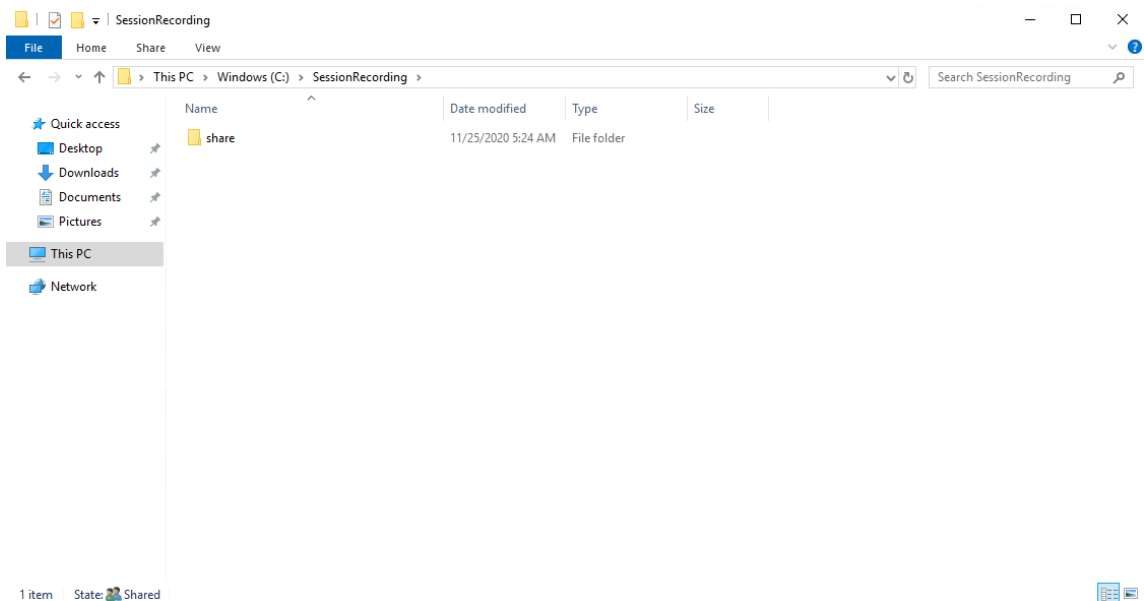
### Schritt 1: Erstellen von freigegebenen Ordnern auf dem Dateiserver

1. Melden Sie sich mit einem Domänenadministratorkonto (zum Beispiel: `lb\administrator`) am Dateiserver an.
2. Erstellen Sie den Ordner `SessionRecording` zum Speichern von Aufzeichnungen (zum Beispiel: `C:\SessionRecording`). Erteilen Sie einem Sitzungsaufzeichnungsserver Lese-/Schreibrechte für den Ordner. Bei Verwendung von `SRServer1` wie im Beispiel geben Sie `LB\SRSERVER1$` ein. Das Dollarzeichen `$` ist erforderlich.





- Erstellen Sie einen Unterordner im Ordner `SessionRecording`. Nennen Sie diesen Unterordner `share`, also zum Beispiel `C:\SessionRecording\share`.



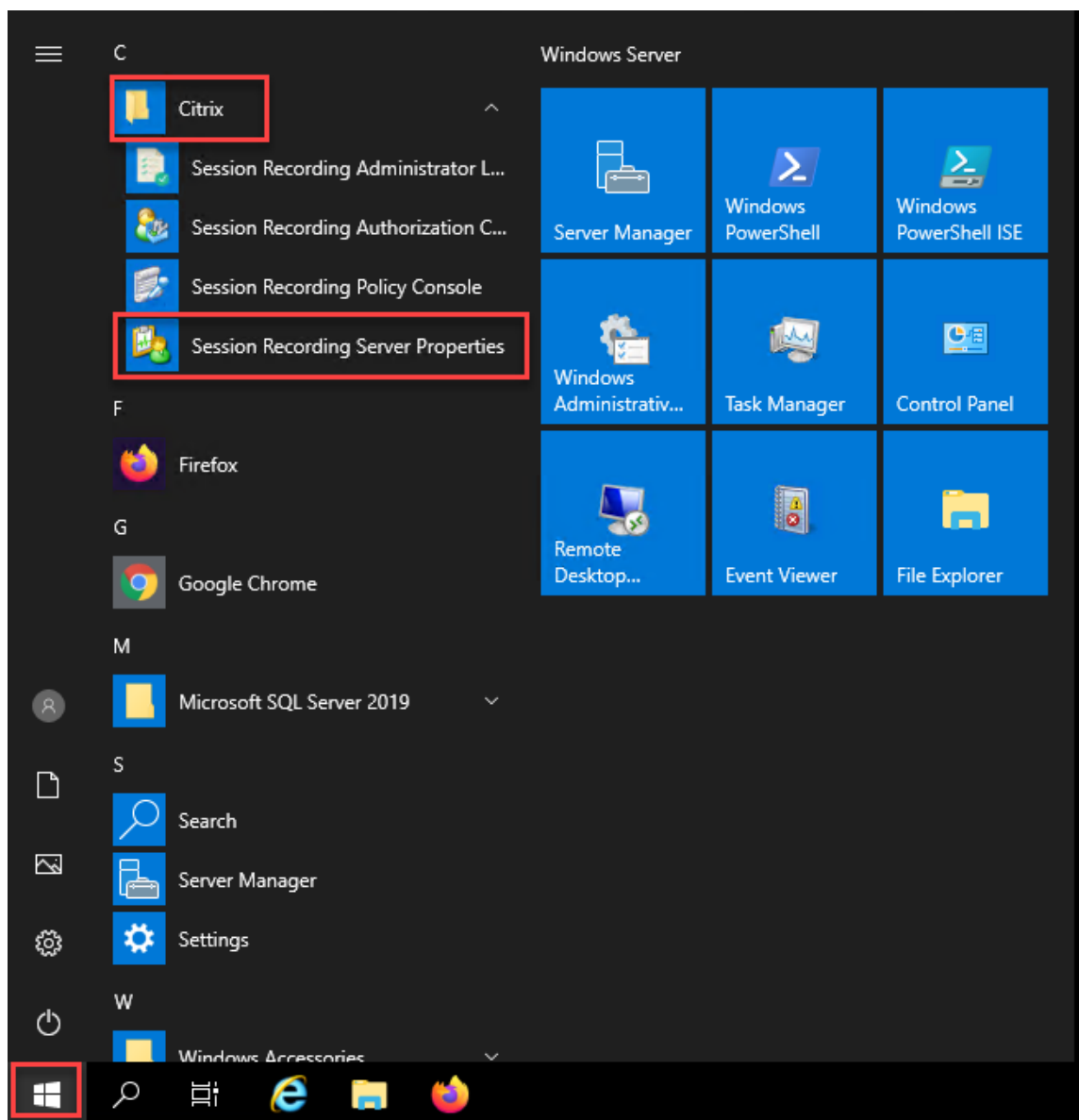
- Erstellen Sie einen weiteren Ordner zum Wiederherstellen archivierter Aufzeichnungen. Nennen Sie diesen Ordner `SessionRecordingsRestored`, also zum Beispiel `C:\SessionRecordingsRestored`. Erteilen Sie einem Sitzungsaufzeichnungsserver Lese-/Schreibrechte für den Ordner. Bei Verwendung von `SRServer1` wie im Beispiel geben Sie `LB\SRSERVER1$` ein. Das Dollarzeichen `$` ist erforderlich.
- Erstellen Sie einen Unterordner im Ordner `SessionRecordingsRestored`. Nennen Sie

diesen Unterordner `share`, also zum Beispiel `C:\SessionRecordingsRestored\share`.

## Schritt 2: Konfigurieren eines vorhandenen Sitzungsaufzeichnungsservers für den Lastausgleich

In diesem Schritt wird beschrieben, wie Sie einen vorhandenen Sitzungsaufzeichnungsserver für den Lastausgleich konfigurieren. [Schritt 7](#) gibt an, wie Sie Ihrer vorhandenen Bereitstellung weitere Sitzungsaufzeichnungsserver hinzufügen.

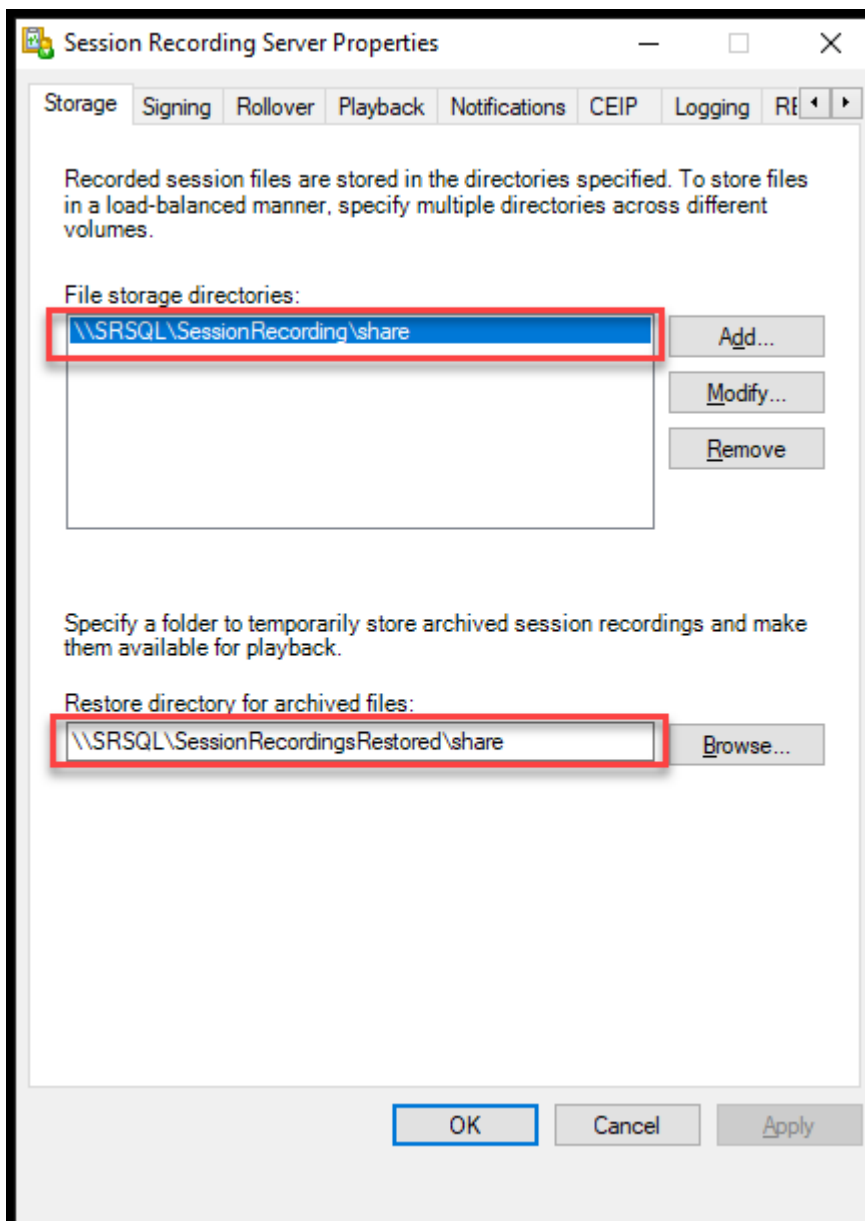
1. Melden Sie sich mit einem Domänenadministratorkonto bei einem Sitzungsaufzeichnungsserver an.
2. Öffnen Sie **Sitzungsaufzeichnungsserver - Eigenschaften**.



3. Fügen Sie die in [Schritt 1](#) erstellten UNC-Pfade hinzu, um Aufzeichnungsdateien zu speichern und wiederherzustellen (Pfade `\\SRSQL\SessionRecording\share` und `\\SRSQL\SessionRecordingRestored\share` im Beispiel). SRSQL ist der Hostname des Dateiservers.

**Hinweis:**

Dateien mit Laufwerksbuchstaben oder Dollarzeichen (\$) im Pfadnamen können vom Sitzungsaufzeichnungsplayer nur dann wiedergegeben werden, wenn Player und Sitzungsaufzeichnungsserver auf derselben Maschine installiert sind.

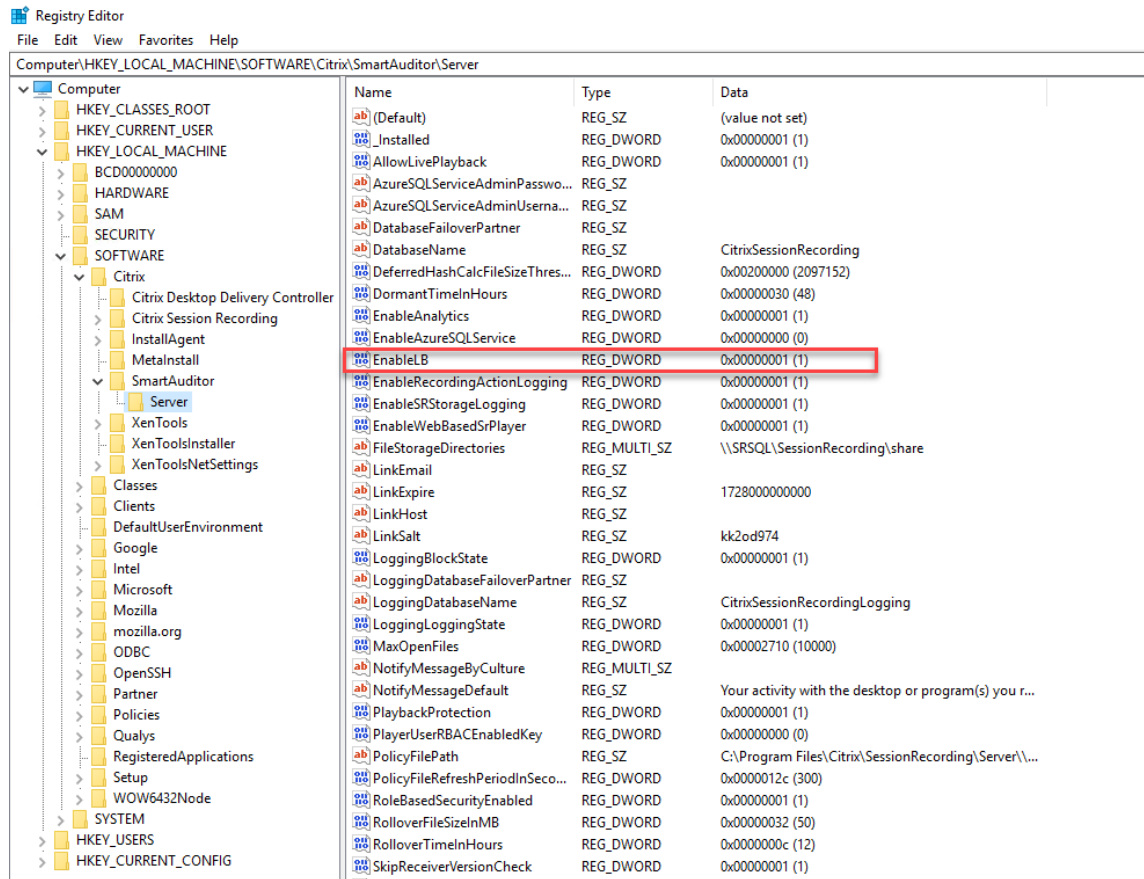


4. Fügen Sie dem Registrierungsschlüssel des Sitzungsaufzeichnungsservers unter `HKEY_LOCAL_MACHINE`

\SOFTWARE\Citrix\SmartAuditor\Server einen Wert hinzu.

Wertname: EnableLB

Wert: 1 (D\_WORD, was "Aktivieren" bedeutet)



5. Starten Sie den Citrix Speichermanager der Sitzungsaufzeichnung neu.

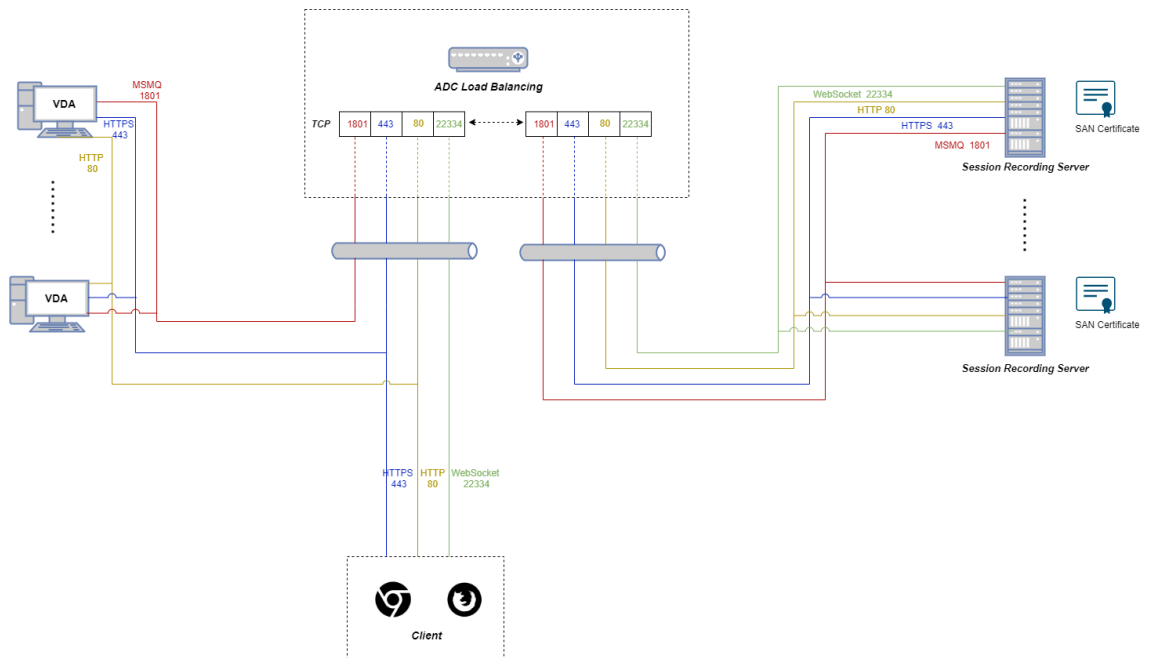
### Schritt 3: Konfigurieren des Lastausgleichs in Citrix ADC

Es gibt zwei Möglichkeiten, den Lastausgleich in Citrix ADC zu konfigurieren: TCP-Passthrough und SSL-Offloading.

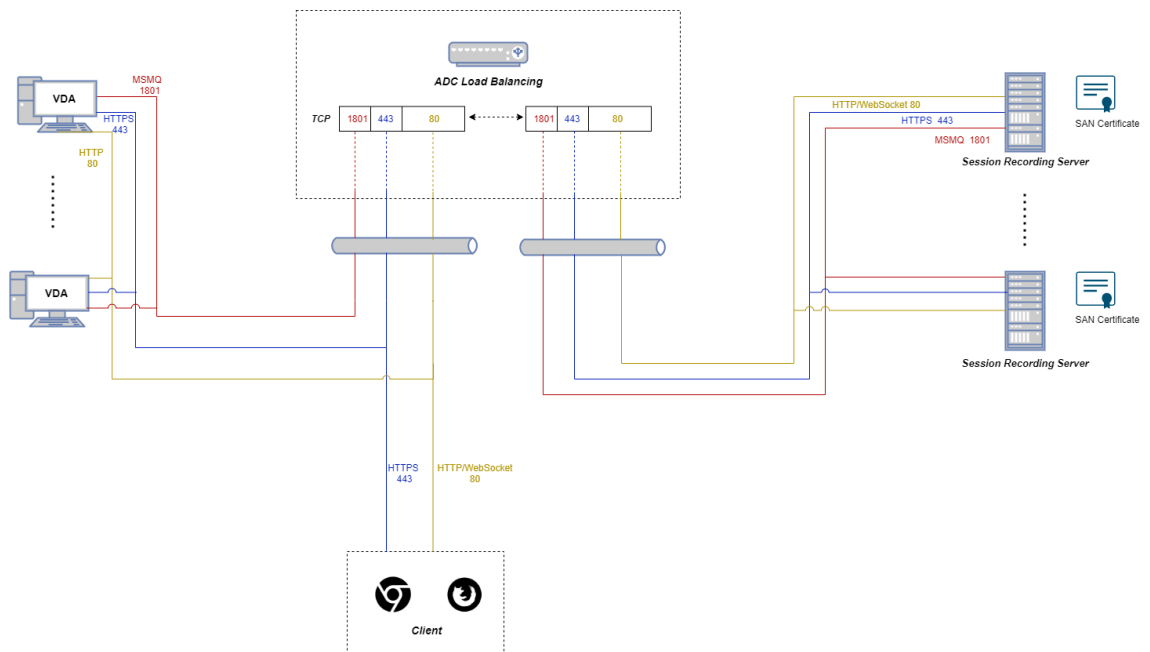
#### Konfigurieren des Lastausgleichs über TCP-Passthrough

Die folgenden Topologien zeigen, wie Sie den Lastausgleich über TCP-Passthrough konfigurieren.

- Bei Verwendung des Python-basierten WebSocket-Servers (Version 1.0):

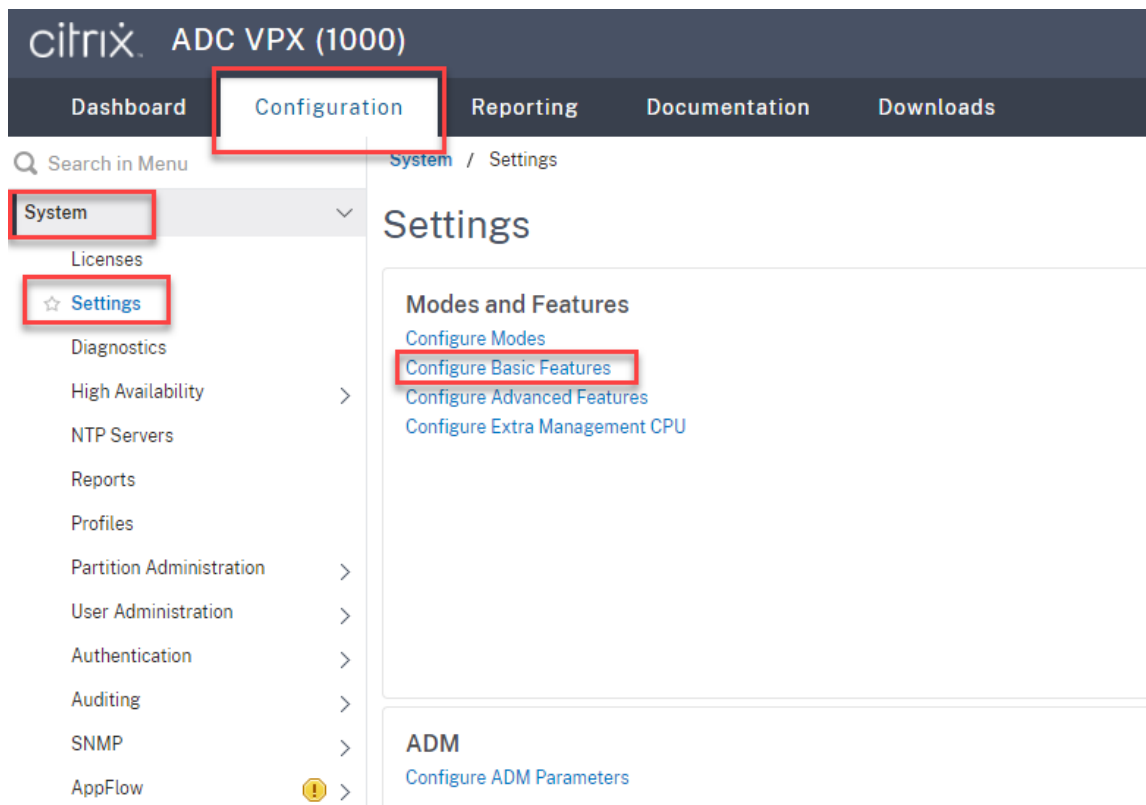


- Bei Verwendung des in IIS gehosteten WebSocket-Servers (Version 2.0):

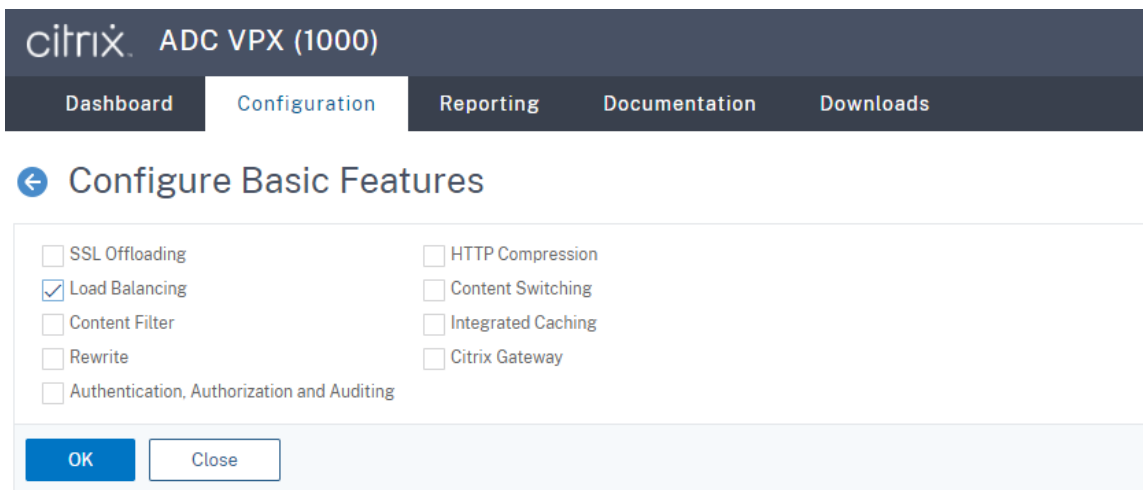


Um den Lastausgleich über TCP-Passthrough zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei Ihrer Citrix ADC VPX-Instanz an.
2. Navigieren Sie zu **Configuration > System > Settings > Configure Basic Features**.



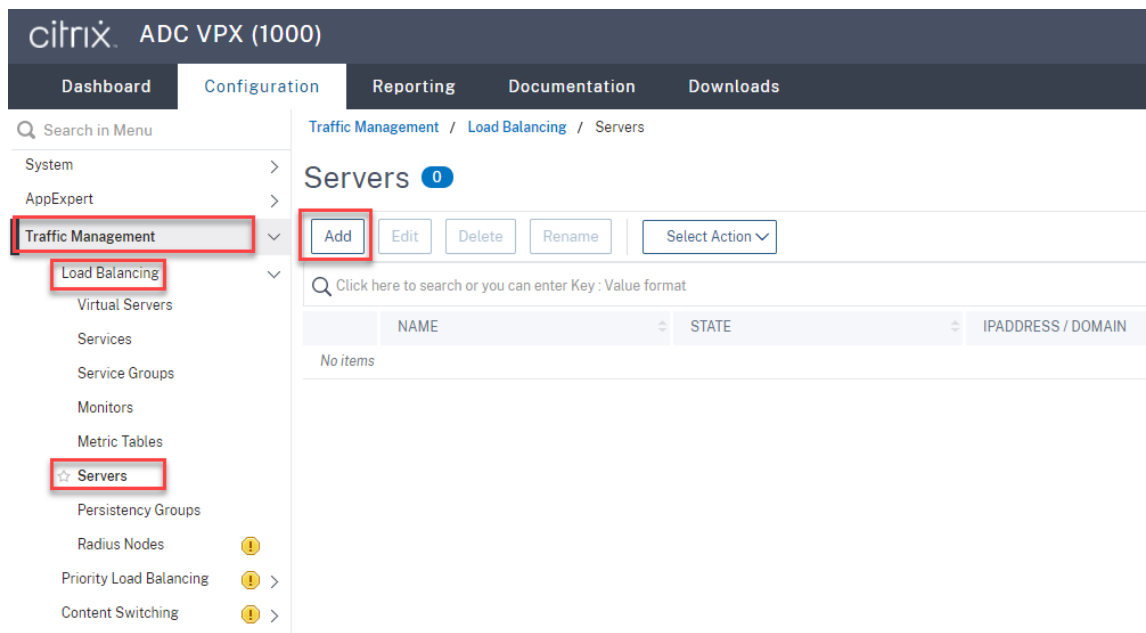
3. Wählen Sie **Load Balancing** und klicken Sie auf **OK**.



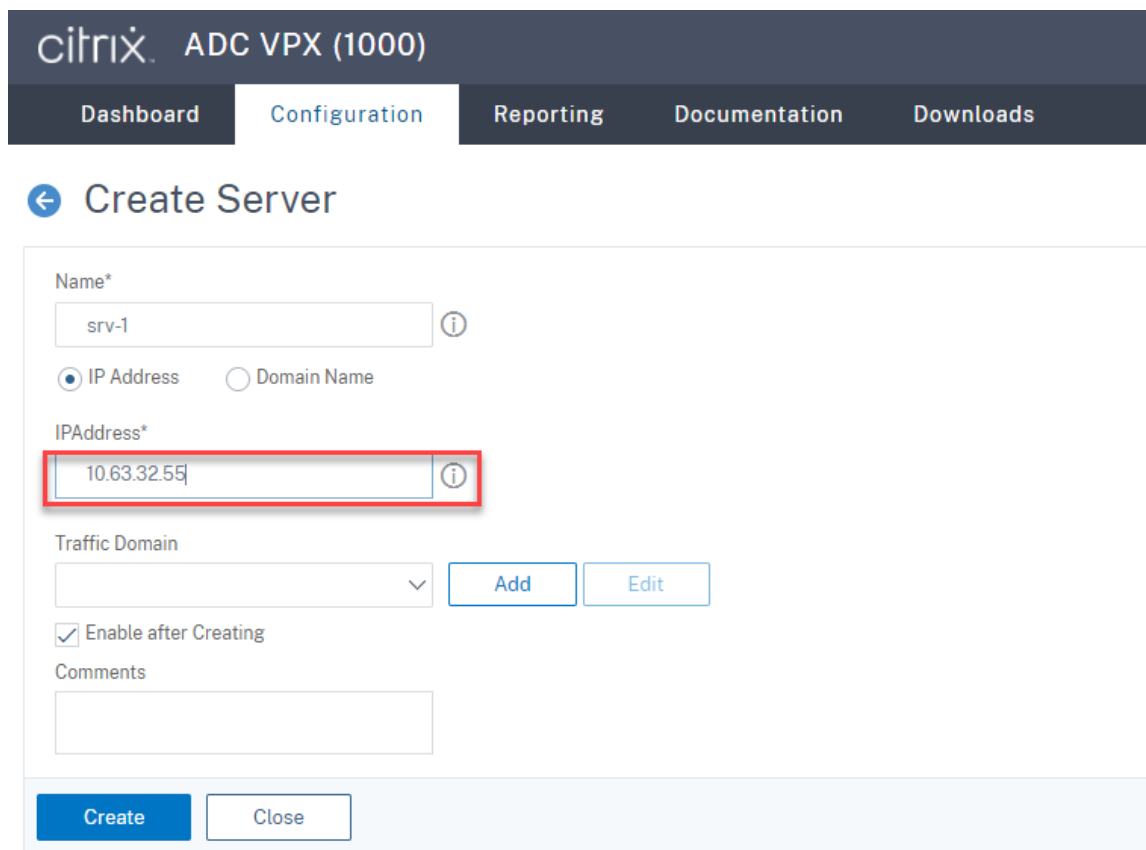
4. Fügen Sie Lastausgleichsserver hinzu.

Navigieren Sie zu **Traffic Management > Load Balancing > Servers** und klicken Sie auf **Add**.

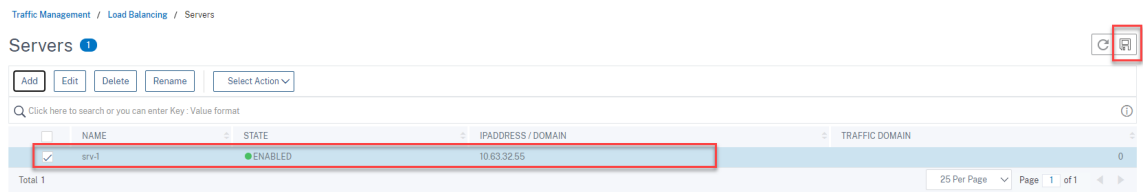




Geben Sie Namen und IP-Adresse eines Sitzungsaufzeichnungsservers ein und klicken Sie auf **Create**. Beispiel:

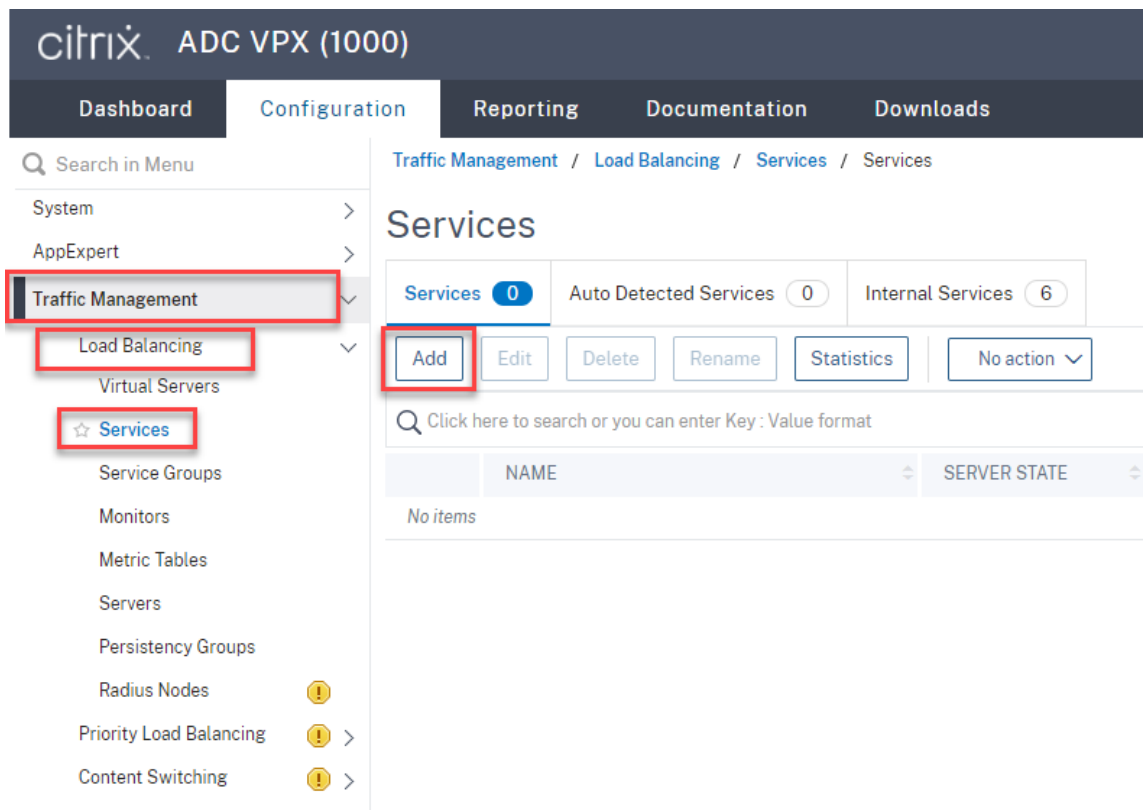


Klicken Sie rechts oben auf das Speichersymbol, um Ihre Änderungen zu speichern.



5. Fügen Sie für WebSocket-Server Version 1.0 für jeden Sitzungsaufzeichnungsserver Lastausgleichsdienste der Ports 80, 1801, 22334 und 443 hinzu. Fügen Sie für WebSocket-Server Version 2.0 für jeden Sitzungsaufzeichnungsserver Lastausgleichsdienste der Ports 80, 1801 und 443 hinzu.

Navigieren Sie zu **Traffic Management > Load Balancing > Services** und klicken Sie auf **Add**.



Geben Sie für jeden hinzugefügten Lastausgleichsdienst einen Namen ein. Wählen Sie **Existing Server**, wählen Sie die IP-Adresse Ihres Zielsitzungsaufzeichnungsservers aus, wählen Sie **TCP** als Serverprotokoll und geben Sie eine Portnummer ein. Klicken Sie auf **OK**.

**citrix** ADC VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

### ← Load Balancing Service

#### Basic Settings

Service Name\*  
 ⓘ

New Server  Existing Server

Server\*  
 ▾

Protocol\*  
 ▾ ⓘ

Port\*  
 ⓘ

▶ More

Binden Sie den TCP-Protokollmonitor an jeden Lastausgleichsdienst.

The screenshot shows the Citrix ADC VPX (1000) configuration interface. The main panel displays the configuration for a Load Balancing Service named 'srv-1-80'. The service is currently in a 'DOWN' state. The modal dialog 'Load Balancing Monitor Binding' is open, showing a 'Select Monitor\*' dropdown menu with 'tcp' selected. The 'Binding Details' section shows a weight of '1' and the 'State' checkbox is checked. A 'Bind' button is highlighted with a red box. In the background, the 'Monitors' section shows '1 Service to Load Balancing Monitor Binding' also highlighted with a red box.

Klicken Sie rechts oben auf das Speichersymbol, um Ihre Änderungen zu speichern.

Traffic Management / Load Balancing / Services / Services

Services

Services (4) Auto Detected Services (0) Internal Services (6)

Add Edit Delete Statistics Action Search

	Name	State	IP Address/Domain Name	Port	Protocol	Max Clients	Max Requests	Cache Type	Traffic Domain
<input type="checkbox"/>	srv-1-1801	UP	10.63.32.55	1801	TCP	0	0	SERVER	0
<input type="checkbox"/>	srv-1-22334	UP	10.63.32.55	22334	TCP	0	0	SERVER	0
<input type="checkbox"/>	srv-1-443	UP	10.63.32.55	443	TCP	0	0	SERVER	0
<input checked="" type="checkbox"/>	srv-1-80	UP	10.63.32.55	80	TCP	0	0	SERVER	0

**Tipp:**

Der Lastausgleichsdienst von Port 22334 ist nur für den WebSocket-Server Version 1.0 erforderlich.

6. Fügen Sie virtuelle Lastausgleichsserver hinzu.

Führen Sie für den WebSocket-Server Version 1.0 die folgenden Schritte aus, um virtuelle Lastausgleichsserver der Ports 80, 443, 1801 und 22334 hinzuzufügen. Fügen Sie für WebSocket-Server Version 2.0 virtuelle Lastausgleichsserver der Ports 80, 443 und 1801 hinzu. Beispiel:

Traffic Management / Load Balancing / Virtual Servers

Virtual Servers 🔄 🔍

Search

<input type="checkbox"/>	Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Health	Traffic Domain
<input type="checkbox"/>	vsvr-80	● UP	● UP	10.63.32.60	80	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 1 UP/0 DOWN	0
<input type="checkbox"/>	vsvr-1801	● UP	● UP	10.63.32.60	1801	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 1 UP/0 DOWN	0
<input type="checkbox"/>	vsvr-443	● UP	● UP	10.63.32.60	443	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 1 UP/0 DOWN	0
<input type="checkbox"/>	vsvr-22334	● UP	● UP	10.63.32.60	22334	TCP	LEASTBANDWIDTH	SOURCEIP	100.00% 1 UP/0 DOWN	0

Navigieren Sie zu **Traffic Management > Load Balancing > Virtual Servers** und klicken Sie auf **Add**.

**citrix ADC VPX (1000)**

Dashboard Configuration Reporting Documentation Downloads

Search in Menu

- System >
- AppExpert >
- Traffic Management** >
  - Load Balancing >
  - Virtual Servers**
  - Services
  - Service Groups
  - Monitors
  - Metric Tables
  - Servers
  - Persistence Groups
  - Radius Nodes !
  - Priority Load Balancing ! >
  - Content Switching ! >

Traffic Management / Load Balancing / Virtual Servers

Virtual Servers 1

Click here to search or you can enter Key : Value format

NAME	STATE	EFFECTIVE STATE	IP ADDRESS
No items			
Total 0			

Fügen Sie jeden virtuellen Server mit der Citrix ADC VIP-Adresse auf Basis des TCP-Protokolls hinzu.

**CITRIX ADC VPX (1000)**

Dashboard Configuration Reporting Documentation Downloads

### ← Load Balancing Virtual Server

**Basic Settings**

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public network (WAN), the VIP is usually a private (ICANN non-routable) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name\*  ⓘ

Protocol\*  ⓘ

IP Address Type\*  ⓘ

IP Address\*  ⓘ

Port\*  ⓘ

▶ More

Binden Sie jeden virtuellen Server an den Lastausgleichsdienst desselben Ports. Beispiel:

**CITRIX ADC VPX (1000)**

Dashboard Configuration Reporting Documentation Downloads

### ← Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

**Basic Settings**

Name	vsrv-80	Listen Priority	-
Protocol	TCP	Listen Policy Expression	NONE
State	● DOWN	Redirection Mode	IP
IP Address	10.63.32.60	Range	1
Port	80	IPset	-
Traffic Domain	0	RHI State	PASSIV
		AppFlow Logging	ENABLI
		Retain Connections on Cluster	NO
		TCP Probe Port	-

**Services and Service Groups**

A service is a logical representation of an application running on a server.  
 A service group enables you to manage a group of services as though it were a single service. After creating a service group, you can bind it to a virtual server, and you can add services.  
**Note:** Bind at least one service or service group to the virtual server.

Click Continue to display the advanced settings and select the method, persistence type, and any other configuration detail that you might need.

No Load Balancing Virtual Server Service Binding

No Load Balancing Virtual Server ServiceGroup Binding

The screenshot displays the Citrix ADC VPX (1000) configuration interface. The main navigation bar includes Dashboard, Configuration, Reporting, Documentation, and Downloads. The current page is titled "Load Balancing Virtual Server" under the Configuration tab. The interface is divided into two main sections: a left sidebar for configuration and a right panel for service binding.

**Left Panel: Load Balancing Virtual Server Configuration**

- Basic Settings:**
  - Name: vsrv-80
  - Protocol: TCP
  - State: DOWN
  - IP Address: 10.63.32.60
  - Port: 80
  - Traffic Domain: 0
- Services and Service Groups:**
  - No Load Balancing Virtual Server Service Binding
  - No Load Balancing Virtual Server ServiceGroup Binding
- Traffic Settings:**
  - Health Threshold: 0
  - Client Idle Time-out: 9000
  - Minimum Autoscale Members: 0
  - Maximum Autoscale Members: 0
  - ICMP Virtual Server Response: PASSIVE

A "Done" button is located at the bottom of the left panel.

**Right Panel: Service Binding / Service**

The right panel shows a "Service" section with a count of 4. It includes "Select", "Add", and "Edit" buttons. The "Add" button is highlighted with a red box. Below the buttons is a search bar with the text "Click here to search or you can enter Key : Value format". A table lists the services:

<input type="checkbox"/>	NAME
<input type="checkbox"/>	srv-1-80
<input type="checkbox"/>	srv-1-443
<input type="checkbox"/>	srv-1-1801
<input type="checkbox"/>	srv-1-22334

A "Total 4" summary is shown at the bottom of the right panel.

Wählen Sie eine Lastausgleichsmethode.

### Method

Method is a load balancing algorithm that the Citrix ADC uses to s

Load Balancing Method\*

LEASTBANDWIDTH  ⓘ

New Service Startup Request Rate

0

Backup LB Method\*

ROUNDROBIN

New Service Request unit\*

PER\_SECOND

Increment Interval

Konfigurieren Sie Persistenz auf jedem virtuellen Server. Wir empfehlen die Auswahl von **SOURCEIP** als Persistenztyp. Weitere Informationen finden Sie unter [Persistenzeinstellungen](#).



### Persistence

Configure persistence to route all connections from the same use persistence type fails.

Select Persistence Type\*

SOURCEIP     RULE     OTHERS    ⓘ

Time-out (mins)\*

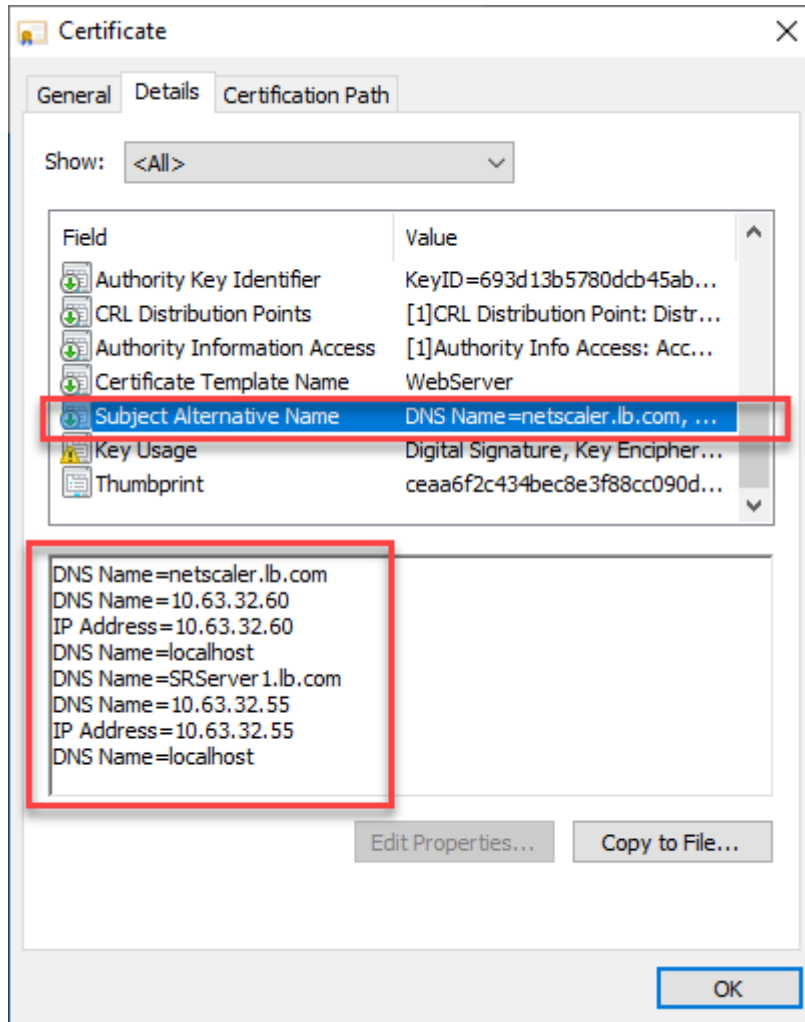
IPv4 Netmask

IPv6 Mask Length

7. Erstellen Sie einen Hostdatensatz für die Citrix ADC VIP-Adresse auf dem Domänencontroller.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[47], lbdc.lb.com., hostma...	static
(same as parent folder)	Name Server (NS)	lbdc.lb.com.	static
(same as parent folder)	Host (A)	10.63.32.82	11/19/2020 2:00:00 AM
lbdc	Host (A)	10.63.32.82	static
LBDDC	Host (A)	10.63.32.11	11/19/2020 11:00:00 PM
Netscaler	Host (A)	10.63.32.60	static
SRServer1	Host (A)	10.63.32.55	11/19/2020 2:00:00 AM
SRServer2	Host (A)	10.63.32.68	11/19/2020 11:00:00 PM
SRSQL	Host (A)	10.63.32.91	11/23/2020 3:00:00 AM
TSVDA	Host (A)	10.63.32.215	11/23/2020 2:00:00 AM

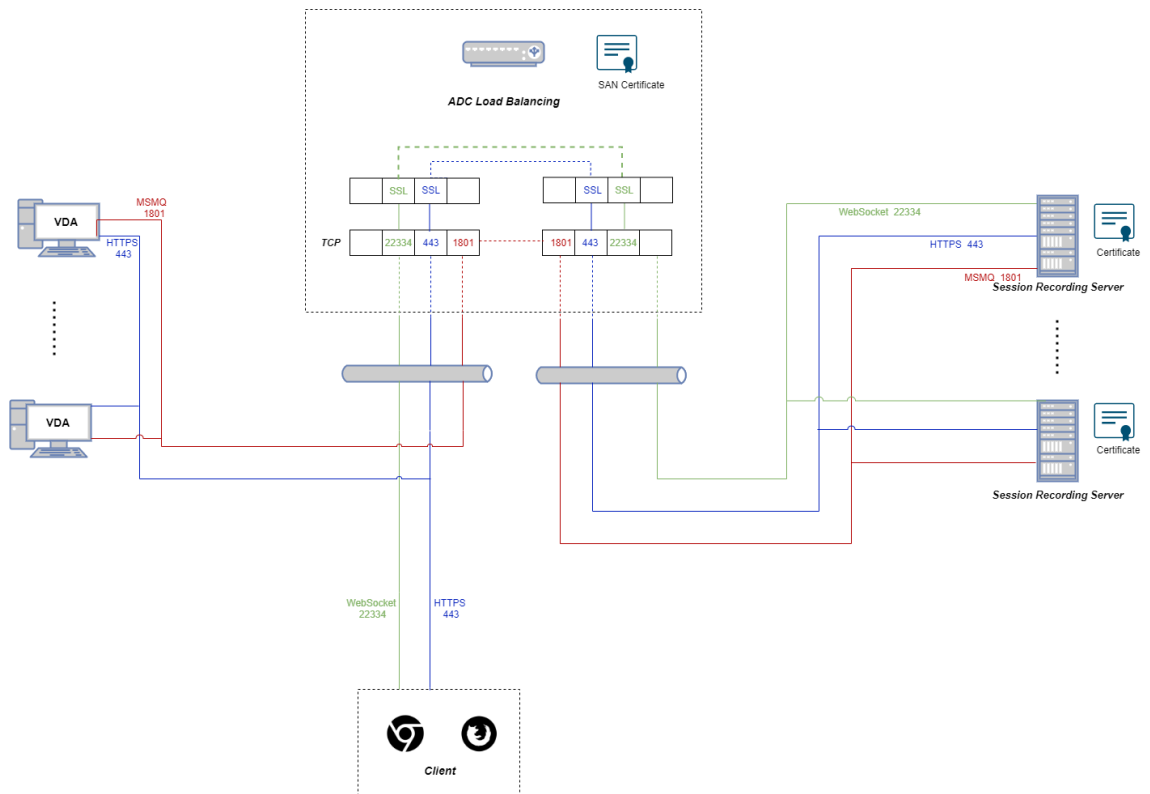
8. Für einen Zugriff auf den Webplayer über HTTPS muss ein SAN-Zertifikat auf Citrix ADC und auf jedem Sitzungsaufzeichnungsserver verfügbar sein. Ein SAN-Zertifikat enthält die FQDNs des Citrix ADC und von jedem Sitzungsaufzeichnungsserver.



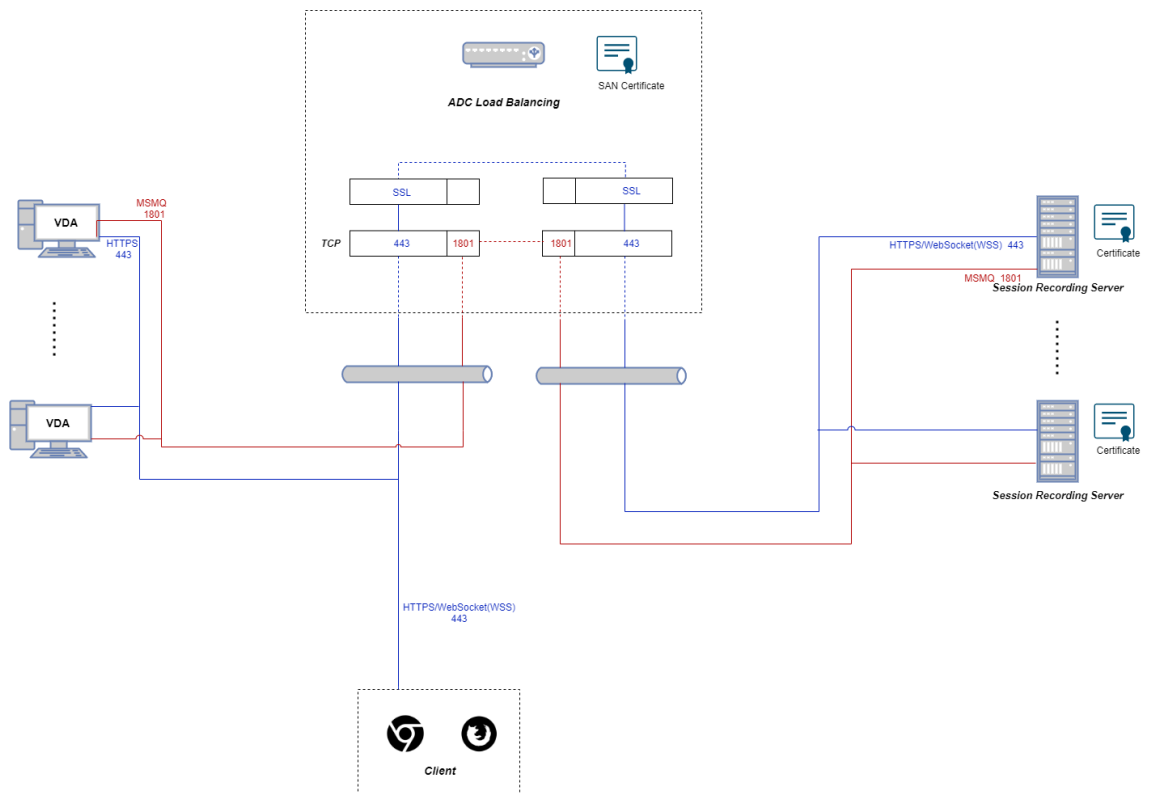
### Konfigurieren des Lastausgleichs über SSL-Offloading

Die folgenden Topologien zeigen, wie Sie den Lastausgleich über SSL-Offloading konfigurieren.

- Bei Verwendung des Python-basierten WebSocket-Servers (Version 1.0):

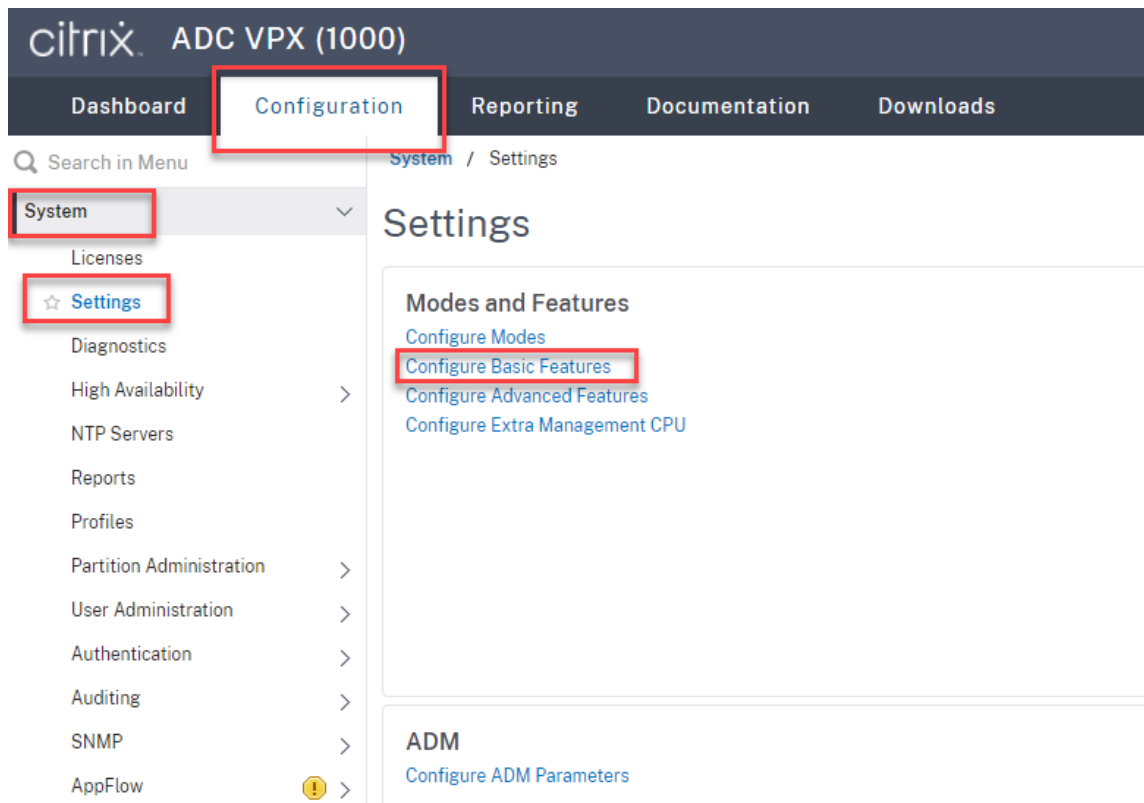


- Bei Verwendung des in IIS gehosteten WebSocket-Servers (Version 2.0):

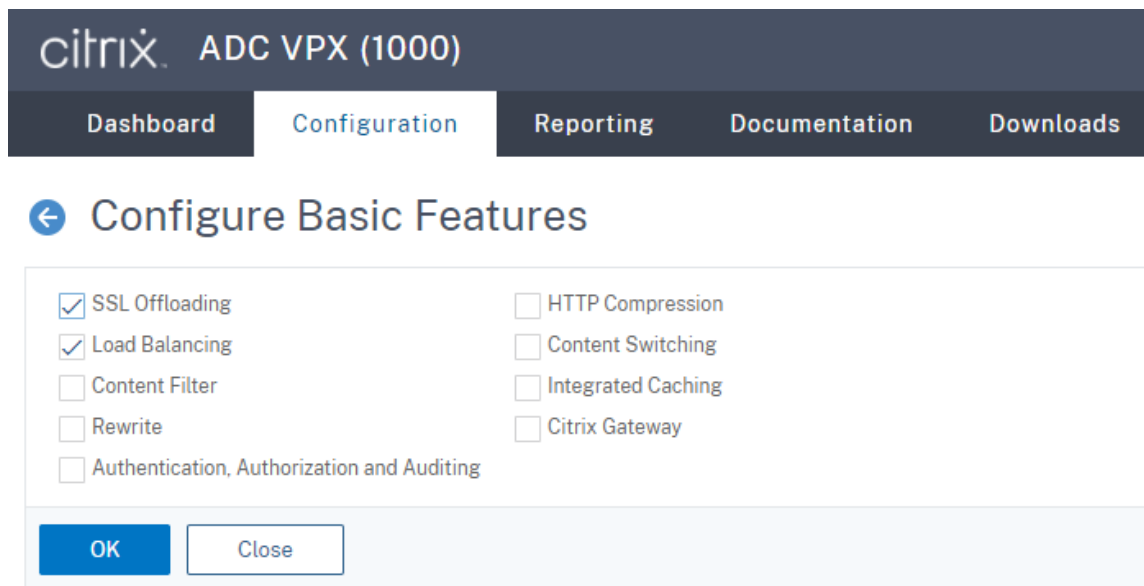


1. Melden Sie sich bei Ihrer Citrix ADC VPX-Instanz an.

2. Navigieren Sie zu **Configuration > System > Settings > Configure Basic Features**.

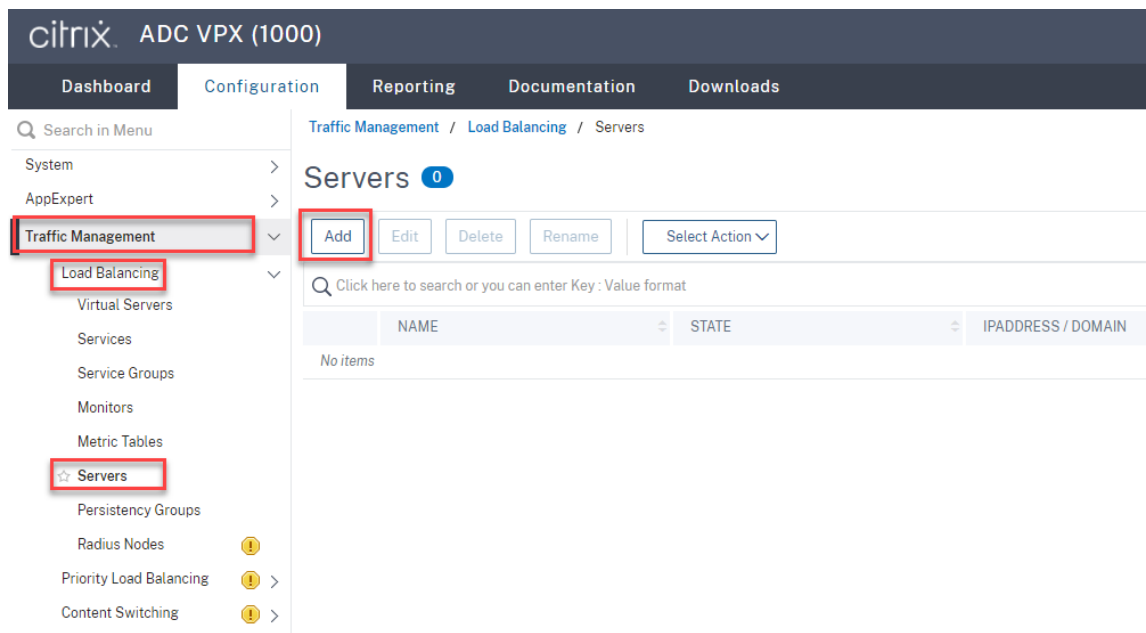


3. Wählen Sie **SSL Offloading** und **Load Balancing** und klicken Sie auf **OK**.

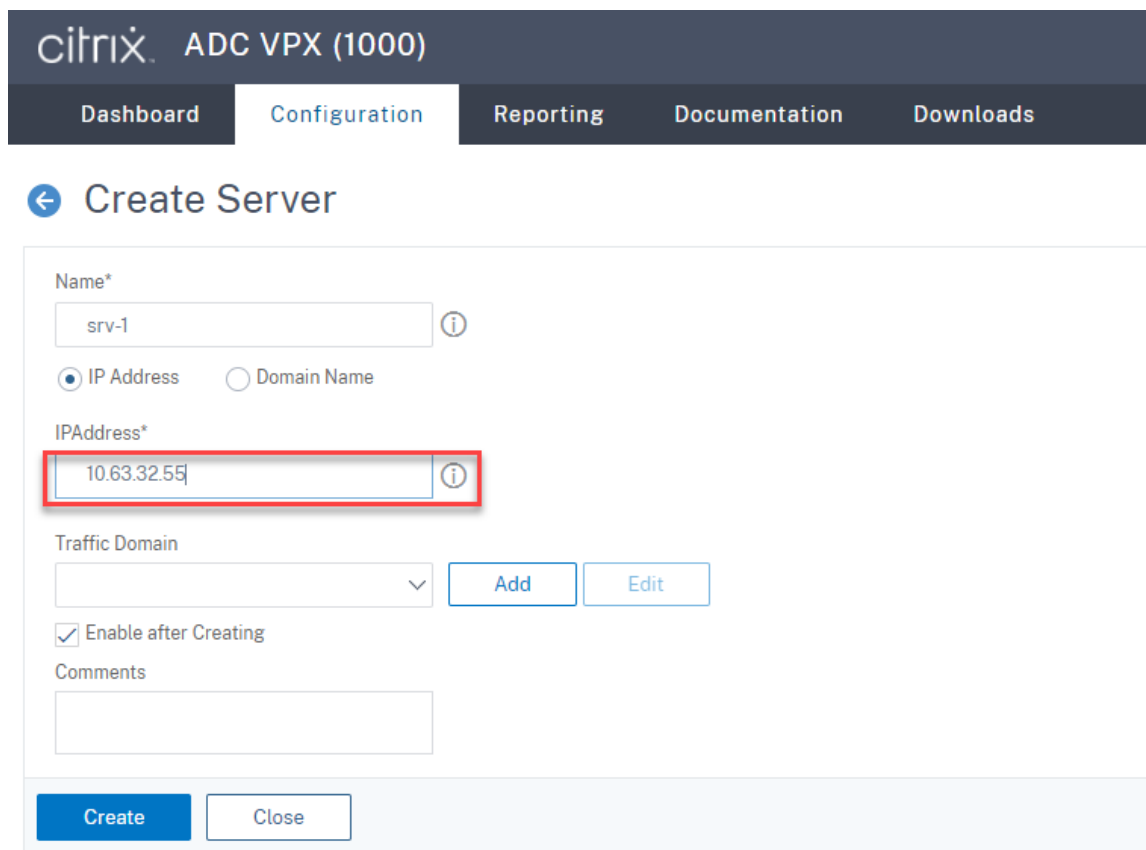


4. Fügen Sie Lastausgleichsserver hinzu.

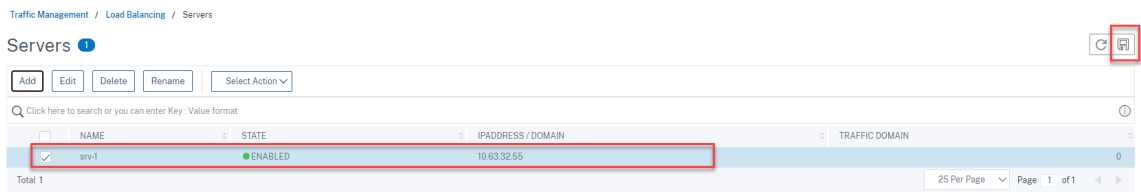
Navigieren Sie zu **Traffic Management > Load Balancing > Servers** und klicken Sie auf **Add**.



Geben Sie Namen und IP-Adresse eines Sitzungsaufzeichnungsservers ein und klicken Sie auf **Create**. Beispiel:



Klicken Sie rechts oben auf das Speichersymbol, um Ihre Änderungen zu speichern.



5. Fügen Sie Lastausgleichsdienste für jeden Sitzungsaufzeichnungsserver hinzu, den Sie im vorherigen Schritt hinzugefügt haben.

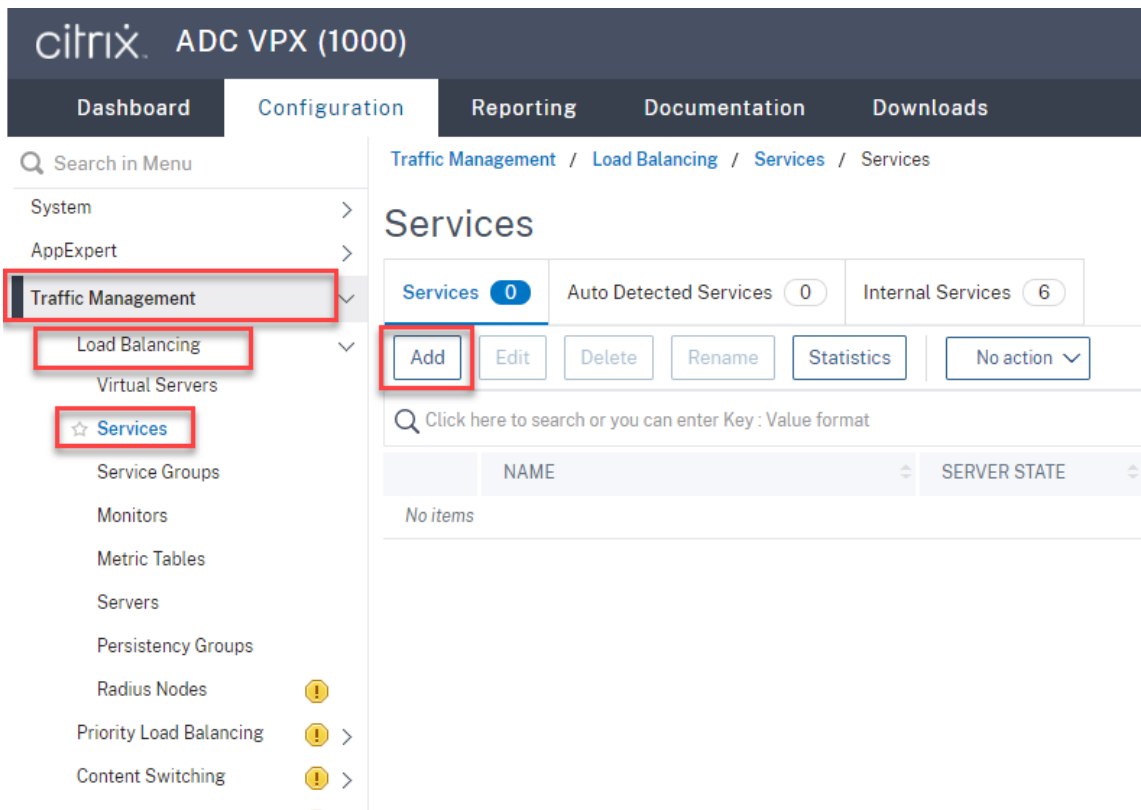
Fügen Sie die folgenden Lastausgleichsdienste für jeden Sitzungsaufzeichnungsserver hinzu:

- (Nur erforderlich, wenn Sie den WebSocket-Server Version 1.0 verwenden) SSL-Lastausgleichsdienst von Port 22334, der an den TCP-Monitor bindet
- SSL-Lastausgleichsdienst von Port 443, der an den HTTPS-Monitor bindet
- TCP-Lastausgleichsdienst von Port 1801, der an den TCP-Monitor bindet

Beispiel:

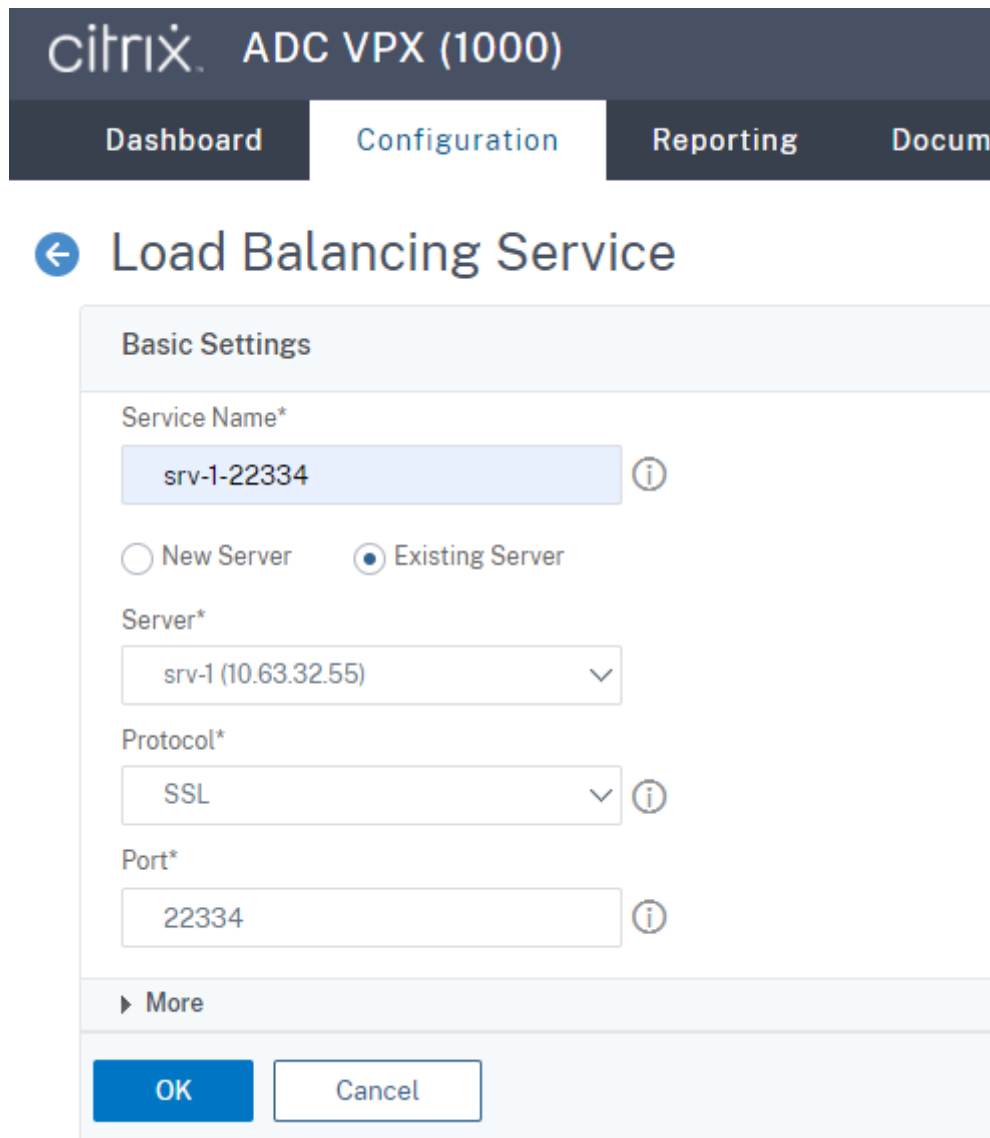


Navigieren Sie zu **Traffic Management > Load Balancing > Services** und klicken Sie auf **Add**.



**(Nur erforderlich, wenn Sie den WebSocket-Server Version 1.0 verwenden) Fügen Sie für jeden Sitzungsaufzeichnungsserver einen SSL-Lastausgleichsdienst von Port 22334 hinzu.** Geben Sie einen Namen für den Lastausgleichsdienst ein, wählen Sie **Existing Server**, wählen Sie die IP-Adresse eines Sitzungsaufzeichnungsservers, wählen Sie **SSL** als Serverprotokoll, geben Sie die Portnummer **22334** ein und klicken Sie auf **OK**.

Ein Beispiel sehen Sie im folgenden Screenshot:

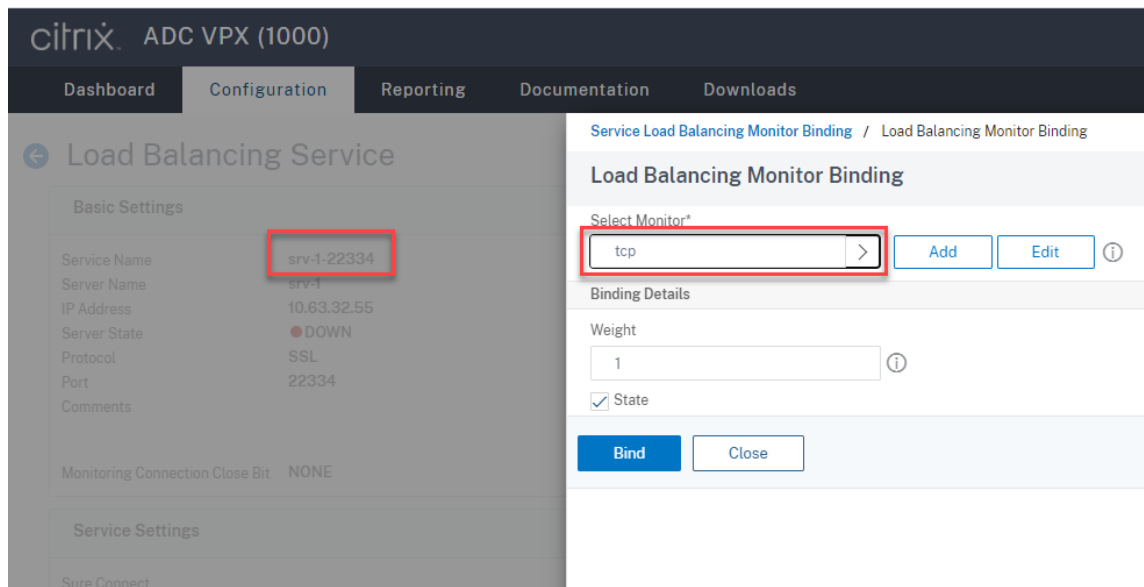


The screenshot shows the Citrix ADC VPX (1000) Configuration page. The navigation menu includes Dashboard, Configuration, Reporting, and Documents. The main heading is "Load Balancing Service". The "Basic Settings" section contains the following fields:

- Service Name\***: srv-1-22334
- Server Type**: Existing Server (selected)
- Server\***: srv-1 (10.63.32.55)
- Protocol\***: SSL
- Port\***: 22334

At the bottom, there is a "More" section and two buttons: "OK" and "Cancel".

Binden Sie den TCP-Monitor an den soeben hinzugefügten SSL-Lastausgleichsdienst.



**Fügen Sie einen SSL-Lastausgleichsdienst von Port 443 für jeden Sitzungsaufzeichnungsserver hinzu.** Geben Sie einen Namen für den Lastausgleichsdienst ein, wählen Sie **Existing Server**, wählen Sie die IP-Adresse eines Sitzungsaufzeichnungsservers, wählen Sie **SSL** als Serverprotokoll, geben Sie die Portnummer 443 ein und klicken Sie auf **OK**.



**citrix ADC VPX (1000)**

Dashboard Configuration Reporting De

## ← Load Balancing Service

**Basic Settings**

Service Name\*  
srv-1-443 ⓘ

New Server  Existing Server

Server\*  
srv-1 (10.63.32.55) ▾

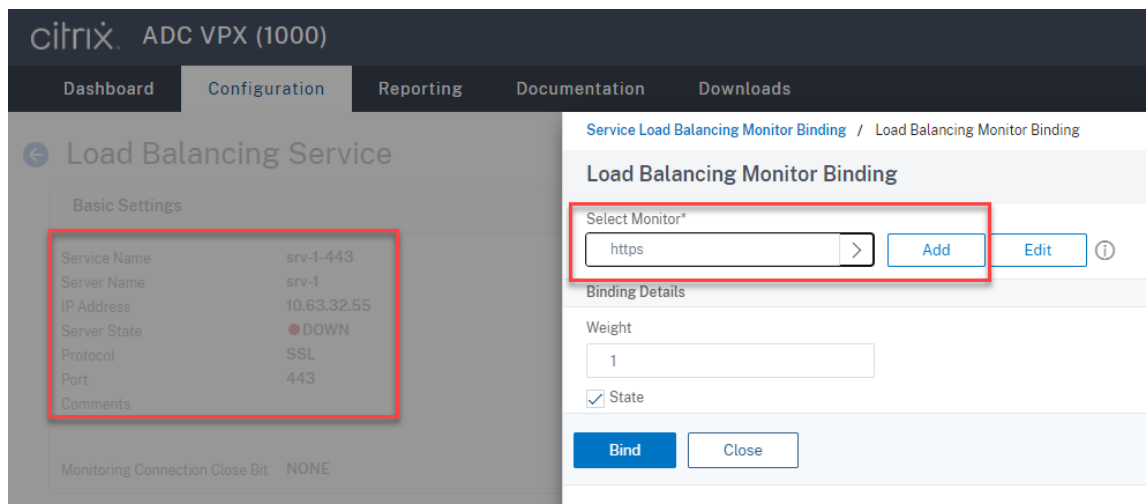
Protocol\*  
SSL ▾

Port\*  
443 ⓘ

▶ More

**OK** Cancel

Binden Sie den HTTPS-Monitor an den soeben hinzugefügten SSL-Lastausgleichsdienst.



**Fügen Sie einen TCP-Lastausgleichsdienst von Port 1801 für jeden Sitzungsaufzeichnungsserver hinzu.** Geben Sie einen Namen für den Lastausgleichsdienst ein, wählen Sie **Existing Server**, wählen Sie die IP-Adresse eines Sitzungsaufzeichnungsservers, wählen Sie **TCP** als Serverprotokoll, geben Sie die Portnummer 1801 ein und klicken Sie auf **OK**.

**citrix ADC VPX (1000)**

Dashboard Configuration Reporting Documentat

## ← Load Balancing Service

**Basic Settings**

Service Name\*  
srv-1-1801 ⓘ

New Server  Existing Server

Server\*  
srv-1 (10.63.32.55) ▾

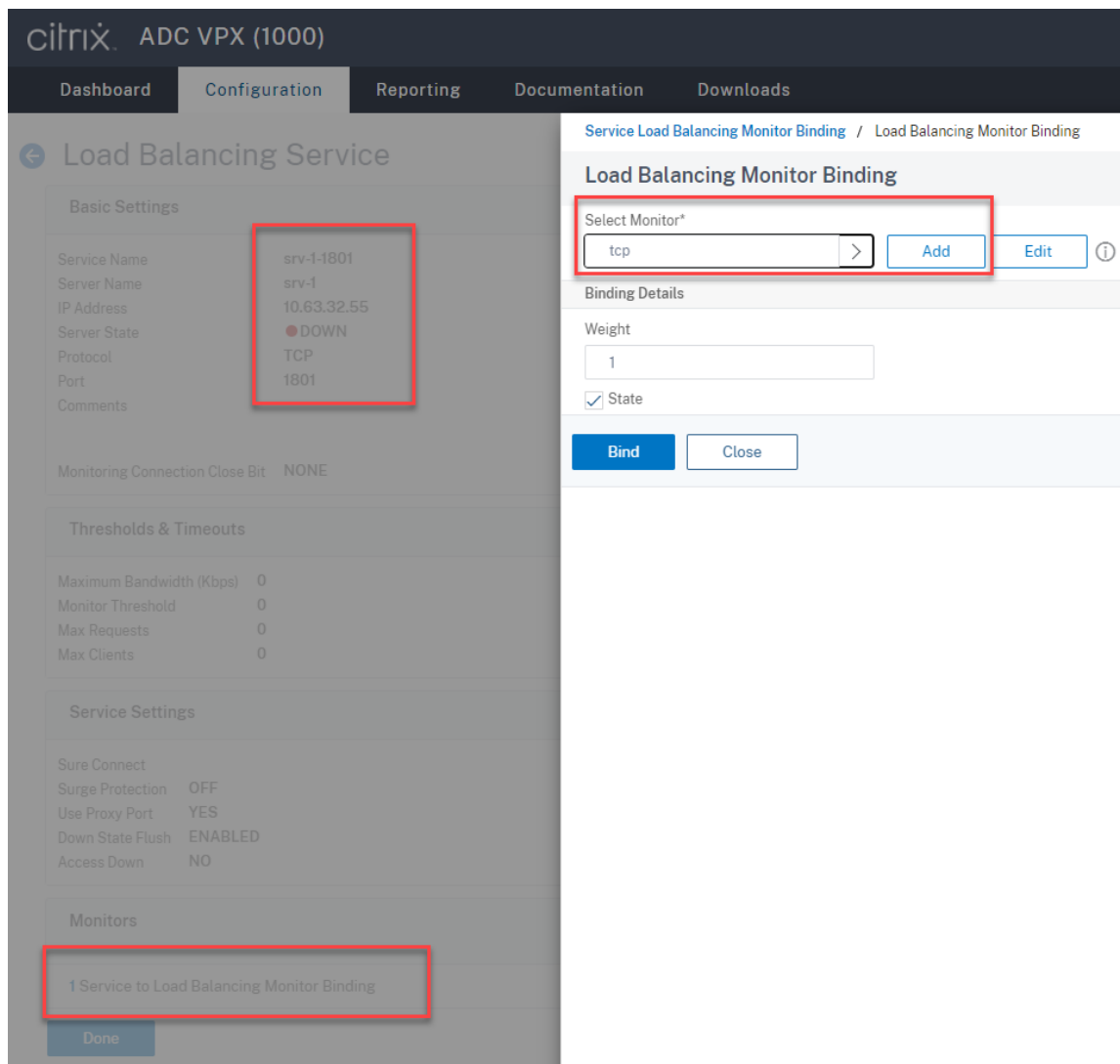
Protocol\*  
TCP ▾ ⓘ

Port\*  
1801 ⓘ

▶ More

**OK** Cancel

Binden Sie den TCP-Monitor an den soeben hinzugefügten TCP-Lastausgleichsdienst.



6. (Nur erforderlich, wenn Sie den WebSocket-Server Version 1.0 verwenden) Fügen Sie ein HTTP-Profil für jeden SSL-Lastausgleichsdienst von Port 22334 hinzu.

Navigieren Sie zu **System > Profiles > HTTP Profiles** und klicken Sie auf **Add**.

The screenshot shows the Citrix ADC VPX (1000) configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The left sidebar has a search function and a 'System' menu with various options. The 'Profiles' option is highlighted. The main content area is titled 'Profiles' and shows a summary of profile counts: TCP Profiles (13), HTTP Profiles (3), Database Profiles (0), and SSL Profiles (0). Below this, there are 'Add', 'Edit', and 'Delete' buttons. A search bar is present with the text 'Click here to search or you can enter Key : Value format'. A table lists the profiles with columns for 'NAME', 'DROP INVALID', and 'INVALIDATE HTTP'. The table contains three rows of data.

<input type="checkbox"/>	NAME	DROP INVALID	INVALIDATE HTTP
<input type="checkbox"/>	nshttp_default_profile	✘	✘
<input type="checkbox"/>	nshttp_default_strict_validation	✔	✔
<input type="checkbox"/>	nshttp_default_internal_apps	✔	✔

Total 3

Aktivieren Sie das Kontrollkästchen **Enable WebSocket connections** und akzeptieren Sie die anderen Standardeinstellungen.

HTTP/2 Initial Window Size		
<input type="text" value="65535"/>		
HTTP/2 Maximum Concurrent Streams		
<input type="text" value="100"/>		
HTTP/2 Maximum Frame Size		
<input type="text" value="16384"/>		
HTTP/2 Minimum Server Connections		
<input type="text" value="20"/>		
HTTP/2 Maximum Header List Size		
<input type="text" value="24576"/>		
HTTP/2 Maximum Ping Frames Per Minute		
<input type="text"/>		
HTTP/2 Maximum Reset Frames Per Minute		
<input type="text"/>		
HTTP/2 Maximum Empty Frames Per Minute		
<input type="text"/>		
HTTP/2 Maximum Settings Frames Per Minute <span style="float: right;">(i)</span>		
<input type="text"/>		
<input type="checkbox"/> Alternative Service	<input checked="" type="checkbox"/> Connection Multiplexing	<input type="checkbox"/> Drop invalid HTTP requests
<input type="checkbox"/> Mark HTTP/0.9 requests as invalid	<input type="checkbox"/> Mark CONNECT Requests as Invalid	<input type="checkbox"/> Mark TRACE Requests as Inva
<input type="checkbox"/> Mark RFC7230 Non-Compliant Transaction as Invalid	<input type="checkbox"/> Mark HTTP Header with Extra White Space as Invalid	<input type="checkbox"/> Compression on PUSH packet
<input checked="" type="checkbox"/> Drop extra CRLF	<input checked="" type="checkbox"/> Enable WebSocket connections (i)	<input type="checkbox"/> Enable RTSP Tunnel
<input type="checkbox"/> Drop extra data from server	<input checked="" type="checkbox"/> HTTP Weblogging	<input type="checkbox"/> Persistent ETag
<input type="checkbox"/> Adaptive Timeout		
<input type="button" value="Create"/> <input type="button" value="Close"/>		

Geben Sie einen Namen für das HTTP-Profil ein (zum Beispiel `websocket_SSL`).

Kehren Sie zu jedem SSL-Lastausgleichsdienst von Port 22334 zurück (zum Beispiel `srv-1-22334`). Klicken Sie auf **+ Profiles**.

**citrix ADC VPX (1000)** HA Status Not configured Partition default nsroot

Dashboard Configuration Reporting Documentation Downloads

### Load Balancing Service

**Basic Settings**

Service Name	srv-1-22334	Traffic Domain	0
Server Name	srv-1	Number of Active Connections	-
IP Address	10.63.32.55	Hash ID	-
Server State	DOWN	Server ID	None
Protocol	SSL	Clear Text Port	-
Port	22334	Cache Type	SERVER
Comments		Cacheable	NO
		Health Monitoring	YES
		AppFlow Logging	ENABLED
Monitoring Connection Close Bit	NONE		

**Advanced Settings**

- + Thresholds & Timeouts
- + Profiles
- + Policies
- + SSL Profile
- + SSL Policies
- + Certificate

**Service Settings**

Sure Connect		Use Source IP Address	NO
Surge Protection	OFF	Client Keep-Alive	NO
Use Proxy Port	YES	TCP Buffering	NO

Wählen Sie das HTTP-Profil (zum Beispiel `websocket_SSL`), klicken Sie auf **OK** und dann auf **Done**.

**Profiles**

Net Profile

TCP Profile

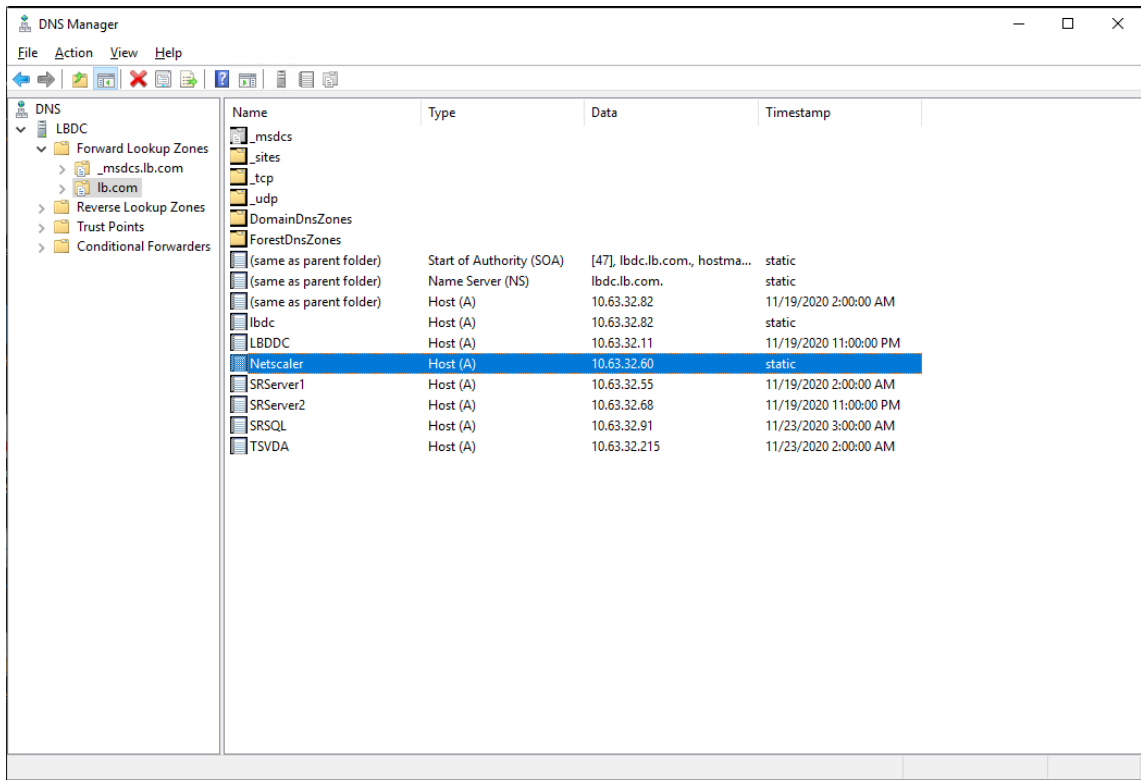
HTTP Profile

DNS Profile Name

**OK**

Done

- (Nur erforderlich, wenn Sie den WebSocket-Server Version 2.0 verwenden) Fügen Sie ein HTTP-Profil für jeden SSL-Lastausgleichsdienst von Port 443 hinzu.
- Erstellen Sie einen Hostdatensatz für die Citrix ADC VIP-Adresse auf dem Domänencontroller.

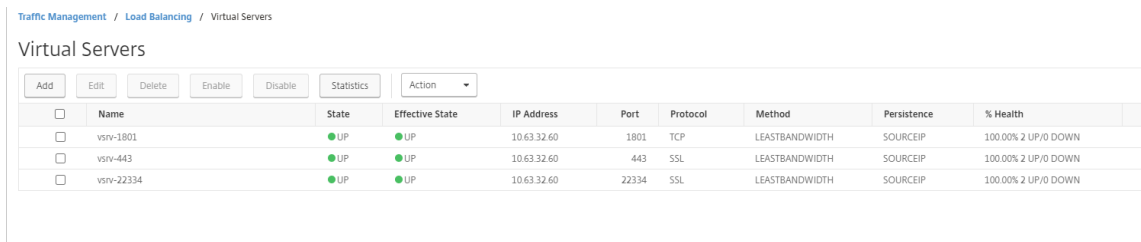


9. Fügen Sie virtuelle Lastausgleichsserver hinzu.

Fügen Sie die folgenden virtuellen Lastausgleichsserver mit der Citrix ADC VIP-Adresse hinzu.

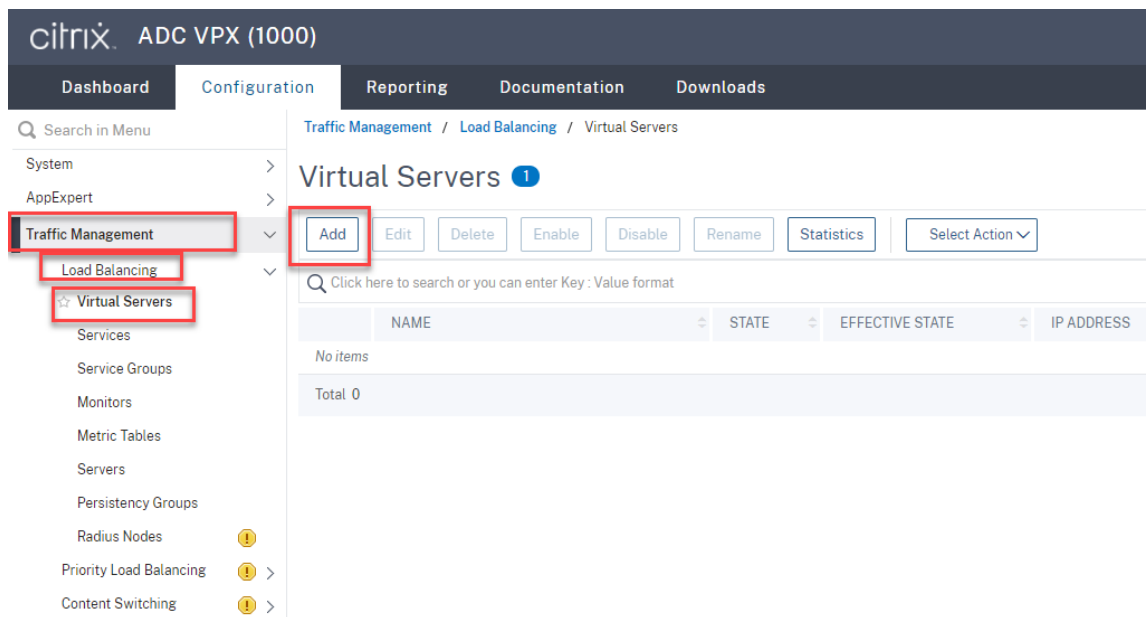
- (Nur erforderlich, wenn Sie den WebSocket-Server Version 1.0 verwenden) Virtueller Lastausgleichsserver von Port 22334 auf SSL-Basis
- Virtueller Lastausgleichsserver von Port 443 auf SSL-Basis
- Virtueller Lastausgleichsserver von Port 1801 auf TCP-Basis

Ein Beispiel sehen Sie im folgenden Screenshot:

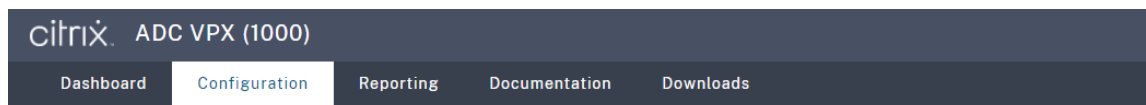


Navigieren Sie zu **Traffic Management > Load Balancing > Virtual Servers** und klicken Sie auf **Add**.





Fügen Sie jeden virtuellen Server mit der Citrix ADC VIP-Adresse hinzu. Geben Sie einen Servernamen ein, wählen Sie **TCP** oder **SSL** und wählen Sie die entsprechende Portnummer wie zuvor beschrieben.



### ← Load Balancing Virtual Server

**Basic Settings**

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public network (WAN), the VIP is usually a private (ICANN non-routable) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name\*  
 ⓘ

Protocol\*  
 ⓘ

IP Address Type\*  
 ⓘ

IP Address\*  
 ⓘ

Port\*  
 ⓘ

▶ More

Binden Sie jeden virtuellen Server an den Lastausgleichsdienst desselben Ports. Beispiel:

The screenshot displays the Citrix ADC VPX (1000) configuration interface. The main panel is titled 'Load Balancing Virtual Server' and shows the following settings:

- Name: vsrv-443
- Protocol: SSL
- State: DOWN
- IP Address: 10.63.32.60
- Port: 443
- Traffic Domain: 0

The sidebar on the right shows the 'Service Binding / Service' configuration. It includes a 'Service' count of 3 and buttons for 'Select', 'Add', and 'Edit'. A search bar is present with the text 'Click here to search or you can enter'. Below the search bar is a table of services:

<input type="checkbox"/>	NAME
<input type="checkbox"/>	srv-1-22334
<input checked="" type="checkbox"/>	srv-1-443
<input type="checkbox"/>	srv-1-1801

The total number of services is 3. The 'Continue' button is visible at the bottom of the main panel.

**Tipp:**

Der Lastausgleichsdienst von Port 22334 ist nur erforderlich, wenn Sie den WebSocket-Server Version 1.0 verwenden.

Wählen Sie eine Lastausgleichsmethode.

### Method

Method is a load balancing algorithm that the Citrix ADC uses to s

Load Balancing Method\*

LEASTBANDWIDTH  ⓘ

New Service Startup Request Rate

0

Backup LB Method\*

ROUNDROBIN

New Service Request unit\*

PER\_SECOND

Increment Interval

Konfigurieren Sie Persistenz auf jedem virtuellen Server. Wir empfehlen die Auswahl von **SOURCEIP** als Persistenztyp. Weitere Informationen finden Sie unter [Persistenzeinstellungen](#).

### Persistence

Configure persistence to route all connections from the same user persistence type fails.

**Select Persistence Type\***

SOURCEIP  
  RULE  
  OTHERS  
 i

Time-out (mins)\*

2

IPv4 Netmask

255 . 255 . 255 . 255

IPv6 Mask Length

128

OK

(Nur erforderlich, wenn Sie den WebSocket-Server Version 1.0 verwenden) Fügen Sie ein HTTP-Profil für den virtuellen Lastausgleichsserver von Port 22334 hinzu.

Profiles
×

A profile is a collection of settings that can be applied to a NetScaler entity, such as a virtual server or service. You can apply the same profile to multiple entities of the same type.

Net Profile

▼
+
✎

TCP Profile

▼
+
✎

LB Profile

▼
+
✎

HTTP Profile

▼
+
✎
?

DB Profile

▼
+
✎

DNS Profile Name

▼
+
✎

OK

10. Installieren Sie ein SAN-Zertifikat in Citrix ADC.

Beziehen Sie ein SAN-Zertifikat im PEM-Format von einer vertrauenswürdigen Zertifizierungsstelle. Navigieren Sie zu **Traffic Management > SSL > Server Certificate Wizard**, und extrahieren und laden Sie das Zertifikat und die privaten Schlüsseldateien in Citrix ADC hoch.

Weitere Informationen finden Sie unter [SSL-Zertifikate](#).

### 4 Install Certificate

Certificate-Key Pair Name\*

Certificate File Name\*  
  ?

Key File Name\*  
  ?

Password\*  
 ?

Notify When Expires

---

**No** SNMP Trap destination found. Notification will not be sent until a trap destination is configured.

---

Notification Period

11. Binden Sie ein SAN-Zertifikat an jeden virtuellen SSL-Lastausgleichsserver.

Navigieren Sie zu **Traffic Management > Load Balancing > Virtual Servers**, wählen Sie einen virtuellen SSL-Lastausgleichsserver und klicken Sie auf **Server Certificate**.

The screenshot shows the Citrix ADC VPX (1000) Configuration page for a Load Balancing Virtual Server. The navigation bar includes Dashboard, Configuration (selected), Reporting, Documentation, and Downloads. The page title is "Load Balancing Virtual Server" with a back arrow icon. Below the title, there is a link "Export as a Template".

The "Basic Settings" section displays the following information:

Name	vsrv-443
Protocol	SSL
State	● DOWN
IP Address	10.63.32.60
Port	443
Traffic Domain	0

The "Services and Service Groups" section shows:

- 1 Load Balancing Virtual Server Service Binding
- No Load Balancing Virtual Server ServiceGroup Binding

The "Certificate" section shows:

- No Server Certificate (highlighted with a red box)
- No CA Certificate

A "Continue" button is located at the bottom of the configuration page.

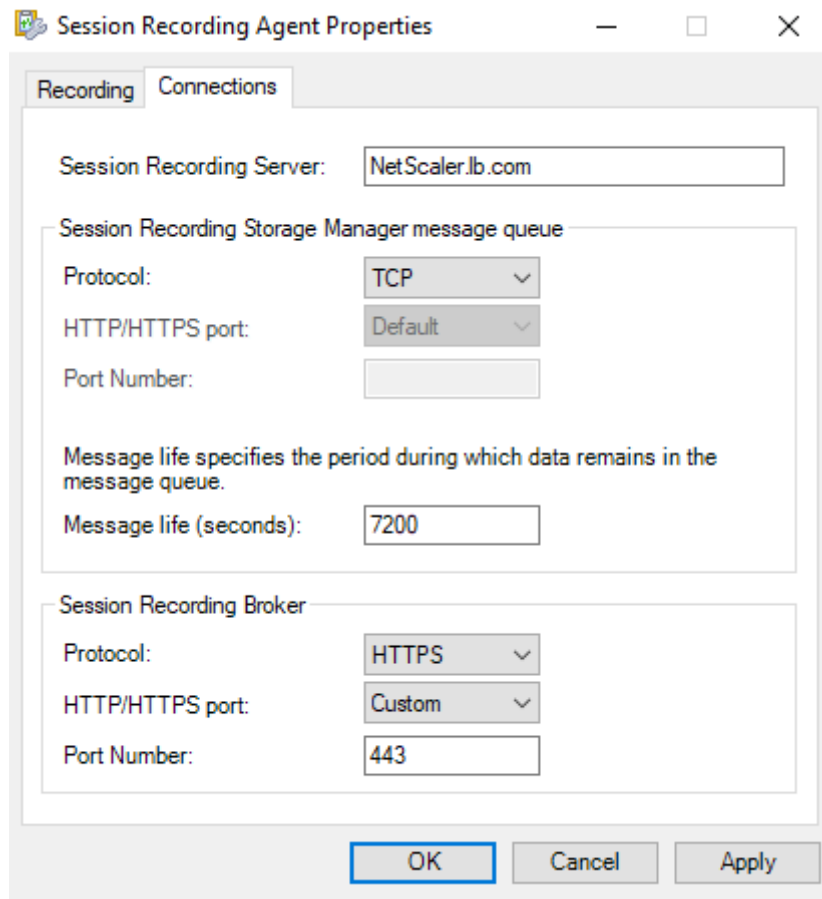
Fügen Sie das zuvor erwähnte SAN-Zertifikat hinzu und klicken Sie auf **Bind**.

#### Schritt 4: Konfigurieren eines vorhandenen Sitzungsaufzeichnungsagent für den Lastausgleich

1. Melden Sie sich mit einem Domänenadministratorkonto beim Sitzungsaufzeichnungsagent an.
2. Öffnen Sie **Sitzungsaufzeichnungsagent - Eigenschaften**.

3. Führen Sie diesen Schritt aus, wenn Sie Microsoft Message Queuing (MSMQ) über TCP verwenden.

Geben Sie den FQDN Ihrer Citrix ADC VIP-Adresse in das Feld **Sitzungsaufzeichnungsserver** ein.

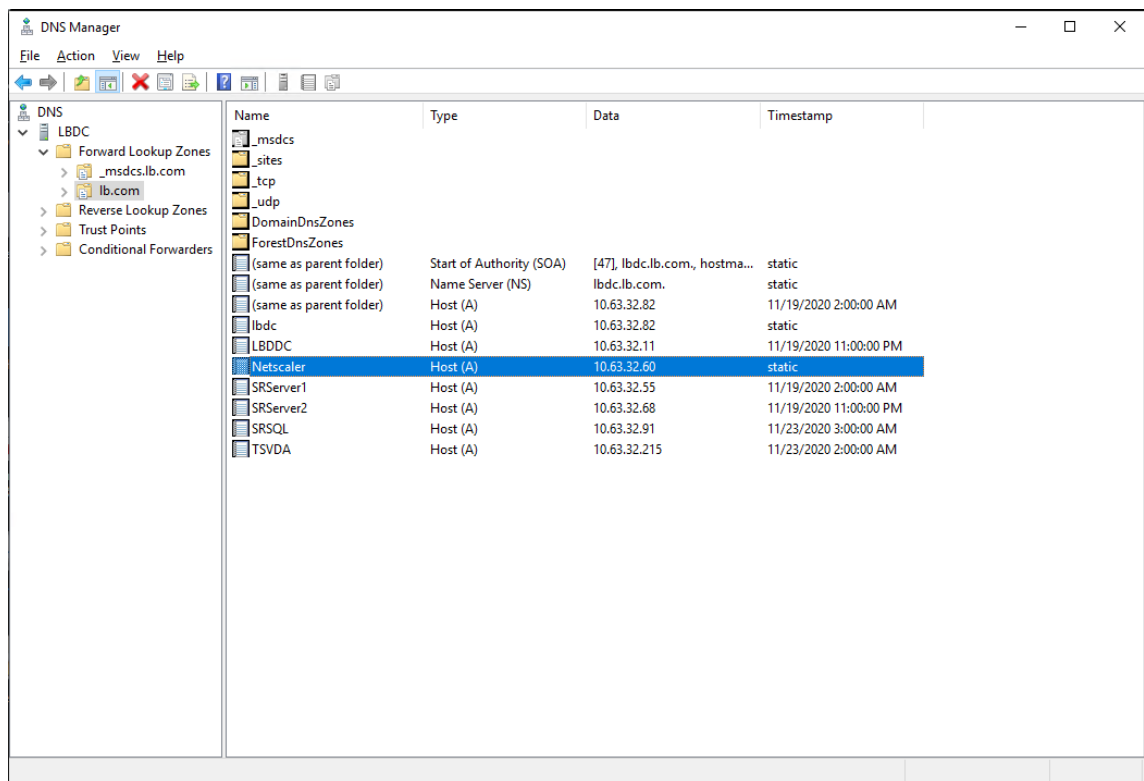


The screenshot shows the 'Session Recording Agent Properties' dialog box with the 'Connections' tab selected. The 'Recording' tab is also visible. The 'Session Recording Server' field contains 'NetScaler.lb.com'. The 'Session Recording Storage Manager message queue' section has 'Protocol' set to 'TCP', 'HTTP/HTTPS port' set to 'Default', and 'Port Number' empty. The 'Message life (seconds)' field is set to '7200'. The 'Session Recording Broker' section has 'Protocol' set to 'HTTPS', 'HTTP/HTTPS port' set to 'Custom', and 'Port Number' set to '443'. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom.

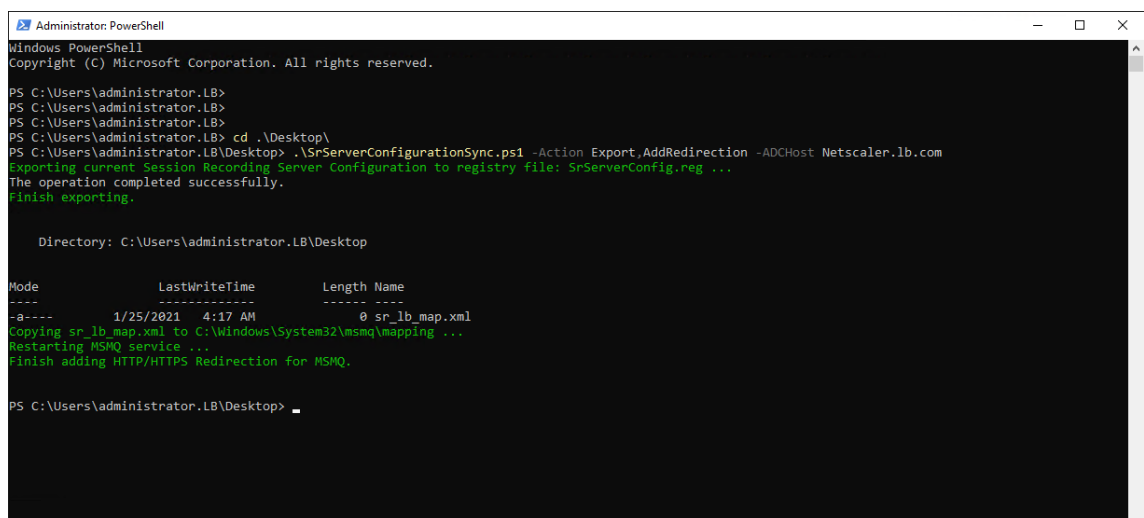
Fügen Sie auf jedem Sitzungsaufzeichnungsserver unter `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters` den DWORD-Wert `IgnoreOSNameValidation` hinzu und legen Sie ihn auf 1 fest. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX248554](#).

4. Führen Sie diesen Schritt aus, wenn Sie MSMQ über HTTP oder HTTPS verwenden.

(Überspringen Sie den Abschnitt, falls dieser Schritt bereits abgeschlossen ist.) Erstellen Sie einen Hostdatensatz für die Citrix ADC VIP-Adresse auf dem Domänencontroller.



Führen Sie auf jedem Sitzungsaufzeichnungsserver den Befehl `powershell.exe -file SrServerConfigurationSync.ps1 -Action AddRedirection -ADCHost <ADCHost>` aus, um Umleitungen von Citrix ADC zum lokalen Host hinzuzufügen. <ADCHost> ist der FQDN der Citrix ADC VIP-Adresse. Eine Umleitungsdatei (zum Beispiel `sr_lb_map.xml`) wird unter `C:\Windows\System32\msmq\Mapping` erstellt.

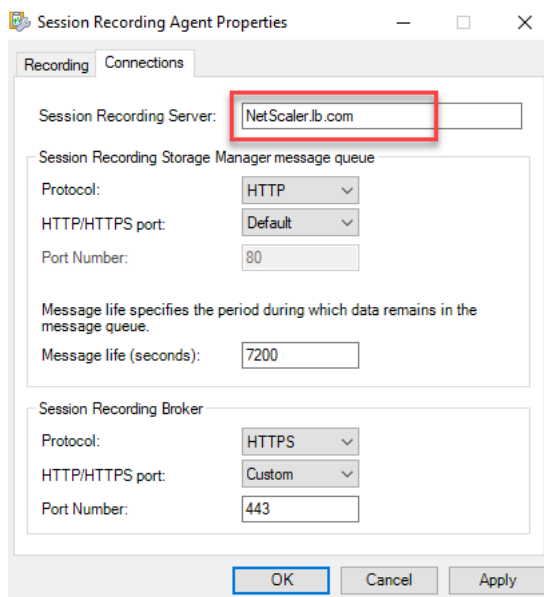


**Hinweis:** Wechseln Sie zum Ordner, in dem sich `SrServerConfigurationSync.ps1` befindet, wenn Sie PowerShell.exe ausführen.

Geben Sie den FQDN Ihrer Citrix ADC VIP-Adresse in das Feld **Sitzungsaufzeichnungsserver** ein.



Beispiel:



### **Schritt 5: Konfigurieren eines vorhandenen Sitzungsaufzeichnungsplayers für den Lastausgleich**

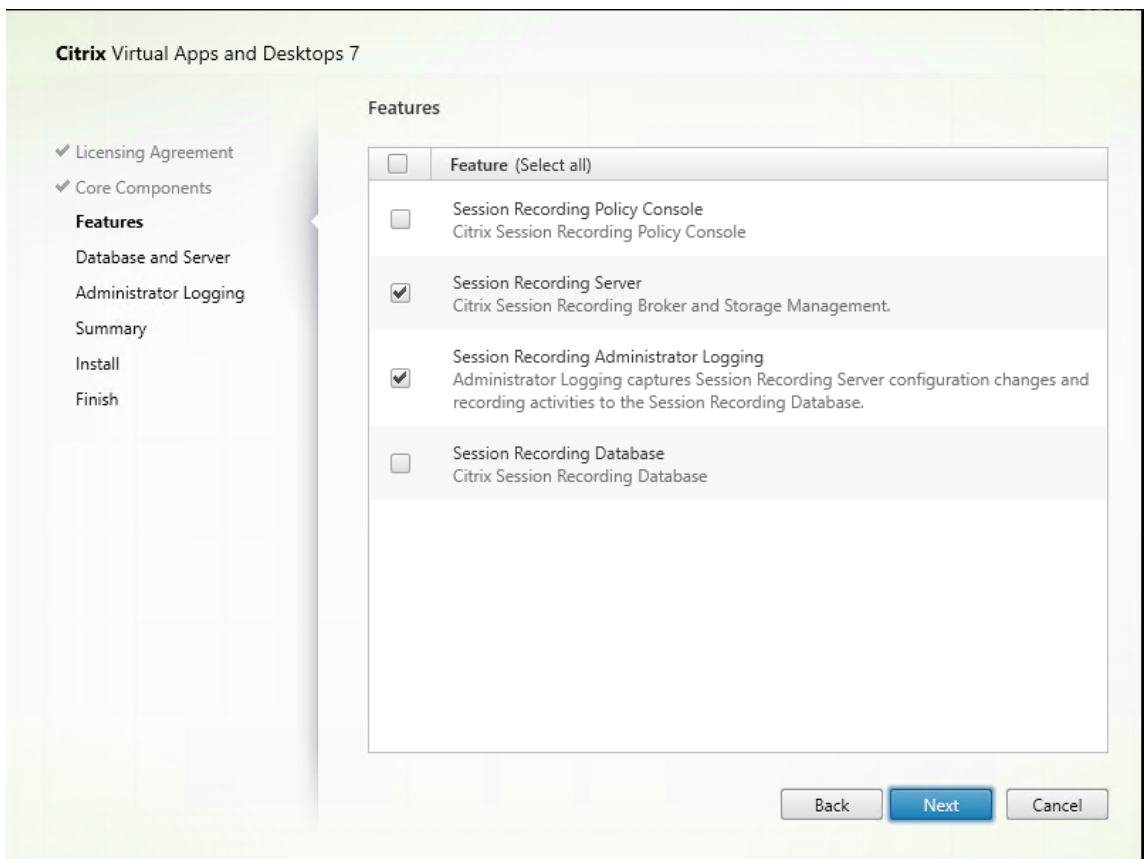
Fügen Sie auf jeder Maschine, auf der ein Sitzungsaufzeichnungsplayer installiert ist, die Citrix ADC VIP-Adresse oder ihren FQDN als den verbundenen Sitzungsaufzeichnungsserver hinzu.

### **Schritt 6: Funktionskontrolle des Lastausgleichs für den konfigurierten vorhandenen Sitzungsaufzeichnungsserver**

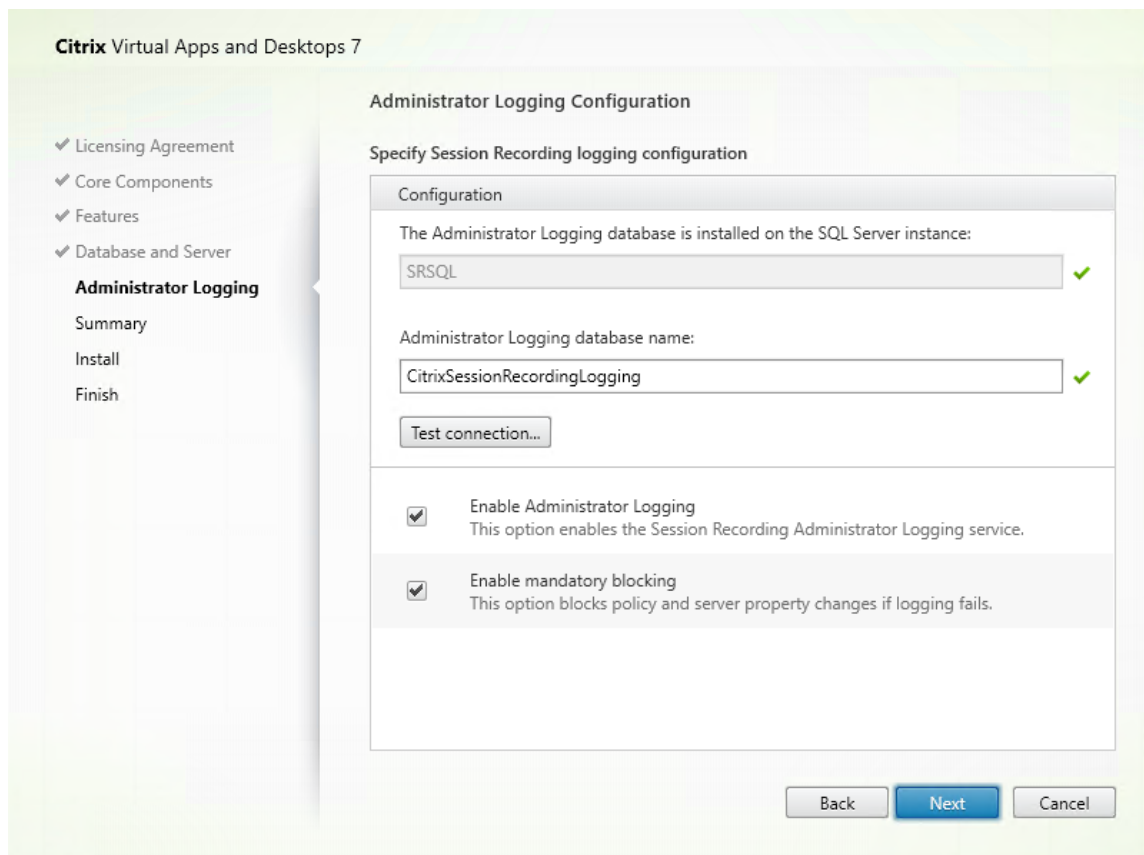
1. Starten Sie eine virtuelle Citrix-Sitzung.
2. Prüfen Sie, ob die Sitzung aufgezeichnet werden kann.
3. Prüfen Sie, ob Webplayer und Sitzungsaufzeichnungsplayer die Aufzeichnungsdatei wiedergeben können.

### **Schritt 7: Hinzufügen weiterer Sitzungsaufzeichnungsserver**

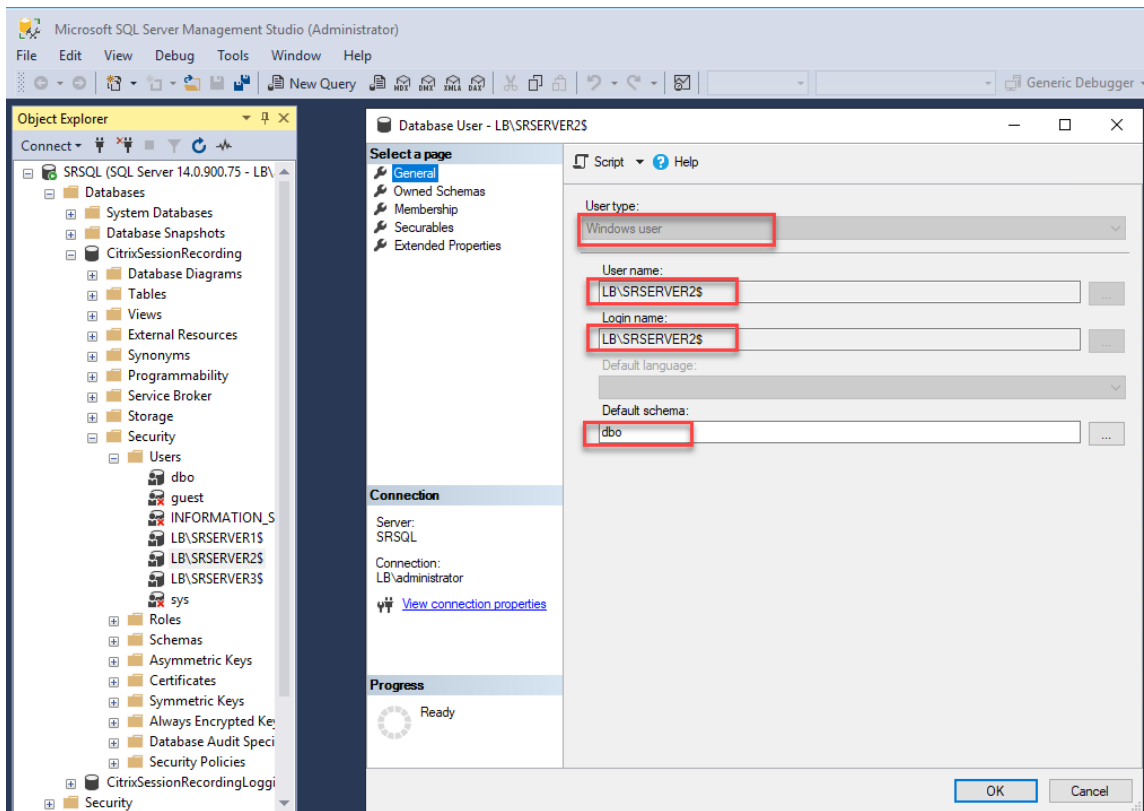
1. Bereiten Sie eine Maschine in derselben Domäne vor und installieren Sie darauf nur die Module "Sitzungsaufzeichnungsserver" und "Sitzungsaufzeichnung - Administratorprotokollierung".

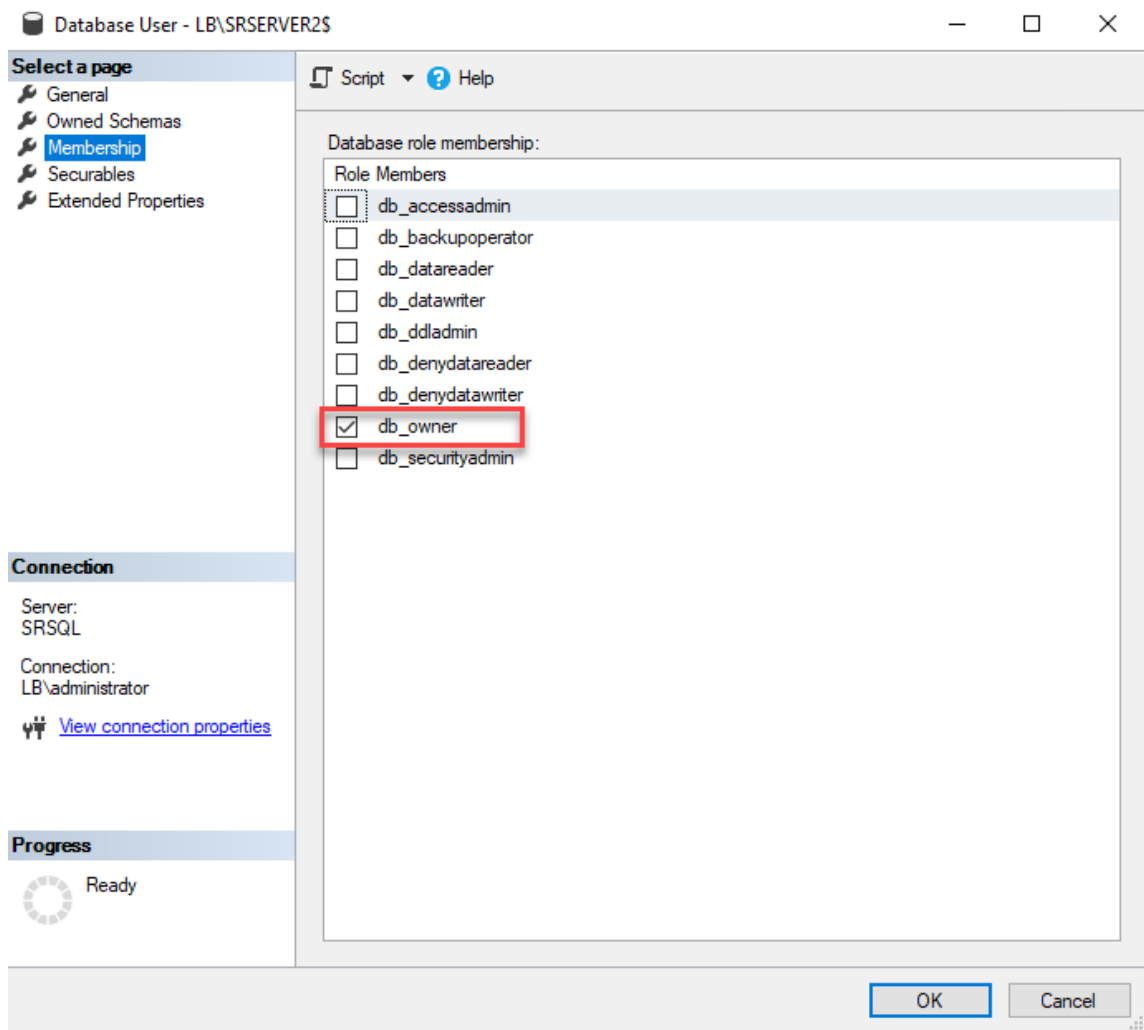


2. Verwenden Sie dieselben Datenbanknamen wie der vorhandene Sitzungsaufzeichnungsserver.  
Beispiel:



3. Deaktivieren Sie die Netzwerkfirewall auf der Maschine.
4. Fügen Sie auf dem SQL-Server, auf dem die Datenbank für die Sitzungsaufzeichnung installiert ist, alle Maschinenkonten des Sitzungsaufzeichnungsservers zur freigegebenen Datenbank für die Sitzungsaufzeichnung hinzu und weisen Sie ihnen die Berechtigung `db_owner` zu. Beispiel:





5. Erteilen Sie dem Maschinenkonto des neuen Sitzungsaufzeichnungsservers (zum Beispiel LB \SRServer2\$) Lese-/Schreibrechte für die Ordner zum Speichern und Wiederherstellen von Aufzeichnungen (zum Beispiel *SessionRecording* und *SessionRecordingsRestored* ). Das Dollarzeichen \$ ist erforderlich.
6. Wiederholen Sie [Schritt 3](#), um Lastausgleichsdienste für den neuen Sitzungsaufzeichnungsserver hinzuzufügen und vorhandene virtuelle Server zu bearbeiten, um Bindungen zu den Lastausgleichsdiensten hinzuzufügen. Es müssen keine weiteren virtuellen Server hinzugefügt werden. Beispiel:

**citrix ADC VPX (1000)**

Dashboard Configuration Reporting Documentation Downloads

Search in Menu

- System >
- AppExpert >
- Traffic Management** >
  - Load Balancing >
    - Virtual Servers
    - Services
    - Service Groups
    - Monitors
    - Metric Tables
    - ☆ Servers
    - Persistency Groups
    - Radius Nodes

Traffic Management / Load Balancing / Servers

### Servers 2

Add Edit Delete Rename Select Action

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	STATE	IPADDRESS / DOMAIN
<input type="checkbox"/>	srv-1	● ENABLED	10.63.32.55
<input type="checkbox"/>	srv-2	● ENABLED	10.63.32.74
Total 2			

**citrix ADC VPX (1000)**

Dashboard Configuration Reporting Documentation Downloads

Search in Menu

- System >
- AppExpert >
- Traffic Management** >
  - Load Balancing >
    - Virtual Servers
    - ☆ Services
    - Service Groups
    - Monitors
    - Metric Tables
    - Servers
    - Persistency Groups
    - Radius Nodes
    - Priority Load Balancing
    - Content Switching
    - Cache Redirection
    - DNS >
    - GSLB
    - SSL >
    - Subscriber >
    - Service Chaining >
    - User >

Traffic Management / Load Balancing / Services / Services

### Services

Services 8 Auto Detected Services 0 Internal Services 6

Add Edit Delete Rename Statistics No action

Click here to search or you can enter Key : Value format

<input type="checkbox"/>	NAME	SERVER STATE	IP ADDRESS/DOMAIN NAME	PORT	PROTOCOL
<input type="checkbox"/>	srv-1-80	● UP	10.63.32.55	80	TCP
<input type="checkbox"/>	srv-1-443	● UP	10.63.32.55	443	TCP
<input type="checkbox"/>	srv-1-1801	● UP	10.63.32.55	1801	TCP
<input type="checkbox"/>	srv-1-22334	● UP	10.63.32.55	22334	TCP
<input type="checkbox"/>	srv-2-443	● UP	10.63.32.74	443	TCP
<input type="checkbox"/>	srv-2-80	● UP	10.63.32.74	80	TCP
<input type="checkbox"/>	srv-2-1801	● UP	10.63.32.74	1801	TCP
<input type="checkbox"/>	srv-2-22334	● UP	10.63.32.74	22334	TCP
Total 8					

The screenshot shows the Citrix ADC VPX (1000) configuration interface. The main navigation bar includes Dashboard, Configuration, Reporting, Documentation, and Downloads. The left sidebar shows a search menu and a tree view of configuration categories, with 'Virtual Servers' under 'Load Balancing' highlighted. The main content area is titled 'Virtual Servers' and features a toolbar with buttons for Add, Edit, Delete, Enable, Disable, Rename, Statistics, and Select Action. Below the toolbar is a search bar and a table of virtual servers. The table has columns for NAME, STATE, EFFECTIVE STATE, and IP ADDRESS. The row for 'vsrv-22334' is selected, indicated by a checked checkbox and a blue background. The total number of servers is 4.

<input type="checkbox"/>	NAME	STATE	EFFECTIVE STATE	IP ADDRESS
<input type="checkbox"/>	vsrv-80	● UP	● UP	10.63.32.60
<input type="checkbox"/>	vsrv-1801	● UP	● UP	10.63.32.60
<input type="checkbox"/>	vsrv-443	● UP	● UP	10.63.32.60
<input checked="" type="checkbox"/>	vsrv-22334	● UP	● UP	10.63.32.60

Total 4

The screenshot shows the Citrix ADC VPX (1000) Configuration page for a Load Balancing Virtual Server. The main configuration area is dimmed, and a modal window titled "Load Balancing Virtual Server Service Binding" is open. The modal contains a table with two service bindings, both highlighted with a red box. The table has columns for SERVICE NAME, IP ADDRESS, PORT, and PROTOCOL. The first row shows "srv-1-22334" with IP address "10.63.32.55" and port "22334" on "TCP". The second row shows "srv-2-22334" with IP address "10.63.32.74" and port "22334" on "TCP". The modal also includes buttons for "Add Binding", "Edit Binding", "Unbind", "Edit Service", "Bound Monitors", "No action", and "Close".

	SERVICE NAME	IP ADDRESS	PORT	PROTOCOL
<input type="checkbox"/>	srv-1-22334	10.63.32.55	22334	TCP
<input type="checkbox"/>	srv-2-22334	10.63.32.74	22334	TCP

7. Kopieren Sie die Konfigurationsdatei der Autorisierungskonsole für die Sitzungsaufzeichnung, `SessionRecordingAzManStore.xml`, vom vorhandenen Sitzungsaufzeichnungsserver auf den neuen Sitzungsaufzeichnungsserver. Die Datei wird unter `<Session Recording Server installation path>\App_Data` gespeichert.
8. Um für den neuen Sitzungsaufzeichnungsserver MSMQ über HTTP oder HTTPS zu verwenden, führen Sie folgende Schritte aus, um Registrierungseinstellungen des aktuell funktionierenden Sitzungsaufzeichnungsservers zu importieren.

Führen Sie auf dem vorhandenen Sitzungsaufzeichnungsserver (zum Beispiel `SrServer1`) den Befehl `powershell.exe -file SrServerConfigurationSync.ps1 -Action Export -ADCHost <ADCHost >` aus, wobei `<ADCHost>` der FQDN der Citrix ADC VIP-Adresse ist. Es wird eine exportierte Registrierungsdatei `SrServerConfig.reg` erstellt.

Kopieren Sie die Datei `SrServerConfig.reg` auf den neuen Sitzungsaufzeichnungsserver und führen Sie den Befehl `powershell.exe -file SrServerConfigurationSync.ps1 -Action Import,AddRedirection -ADCHost <ADCHost>` aus. Der Wert **EnableLB** wird dem Registrierungsschlüssel des neuen Sitzungsaufzeichnungsservers in `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server` hinzugefügt, und unter `C:\Windows\System32\msmq\Mapping` wird eine Datei `sr_lb_map.xml` hinzugefügt.



9. Wiederholen Sie den Vorgang, um einen weiteren Sitzungsaufzeichnungsserver hinzuzufügen.

### Problembehandlung

- Sitzungen werden nicht aufgezeichnet, wenn Sie einen CNAME-Datensatz oder einen ALIAS-Datensatz für einen Sitzungsaufzeichnungsserver verwenden. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX248554](#).
- Aufzeichnungsdateien können zwar lokal gespeichert werden, die Speicherung in einem UNC-Pfad ist jedoch nicht möglich. Um dieses Problem zu beheben, ändern Sie den Startmodus des Citrix Speichermanagers der Sitzungsaufzeichnung in **Automatisch (Verzögerter Start)**.

## Bereitstellen und Lastausgleich der Sitzungsaufzeichnung in Azure

January 15, 2024

### Voraussetzungen

- Sie haben Citrix Virtual Apps and Desktops bereits in Azure installiert.
- Sie haben ein Azure-Konto.

### Schritt 1: Hochladen des Installationsprogramms für Citrix Virtual Apps and Desktops in Azure

#### Hinweis:

Überspringen Sie Schritt 1, wenn Sie sich mit Ihrem Citrix-Konto bei der Citrix Virtual Apps and Desktops-Downloadseite anmelden und die ISO-Datei des Produkts in eine VM in Azure herunterladen.

1. Erstellen Sie im [Azure-Portal](#) ein Speicherkonto vom Typ **Allgemein v2** und akzeptieren Sie die voreingestellte Leistungsstufe **Standard**.

Der gesamte Zugriff auf den Azure-Speicher erfolgt über ein Speicherkonto.

Microsoft Azure

Home > Storage accounts >

## Create storage account

Azure Storage is a Microsoft managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*   
[Create new](#)

### Instance details

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

Storage account name \*

Location \*

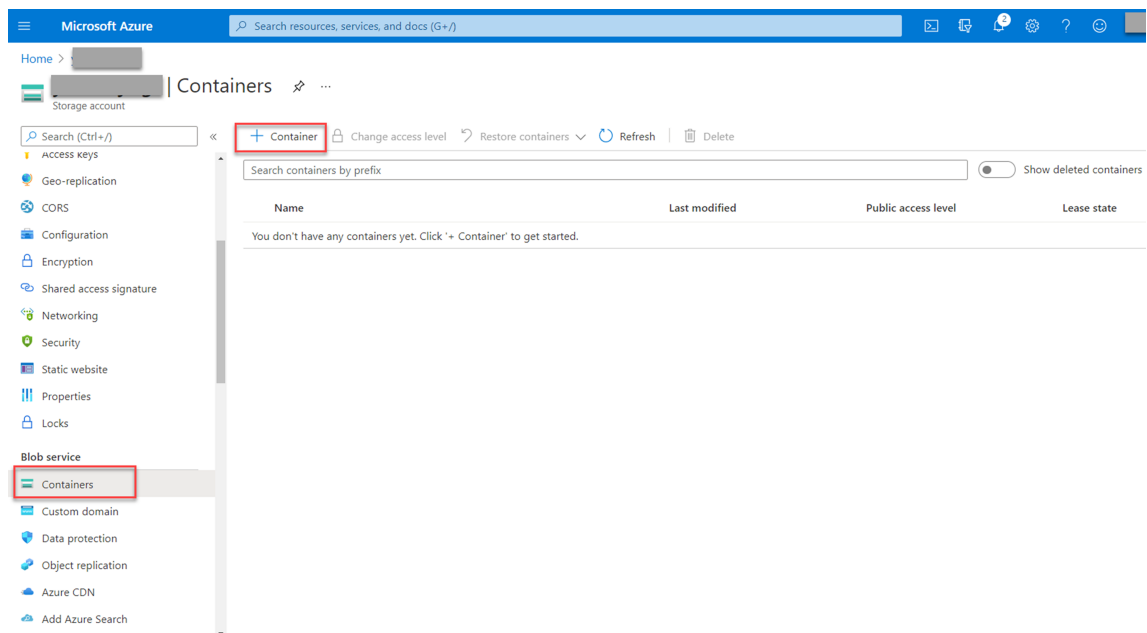
Performance  Standard  Premium

Account kind

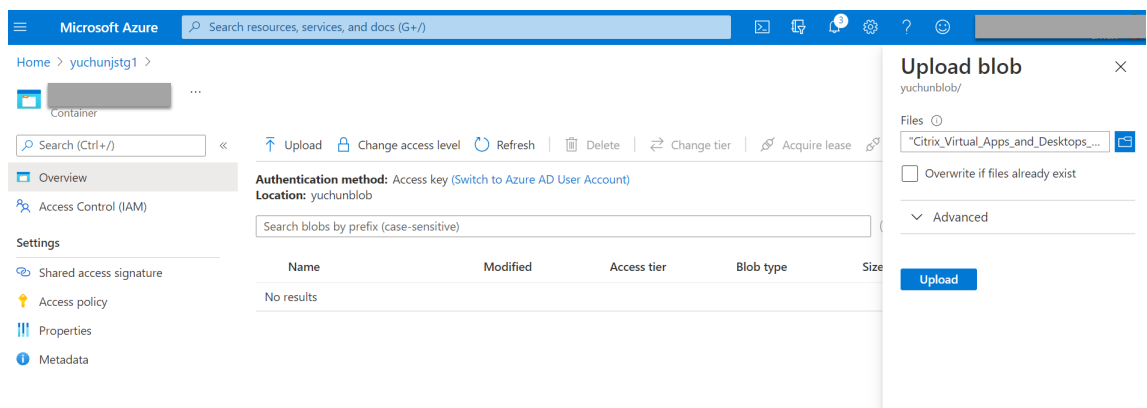
Replication

[Review + create](#) [< Previous](#) [Next: Networking >](#)

2. Navigieren Sie zu Ihrem neuen Speicherkonto und wählen Sie unter **Blob-Dienst** die Option **Container**, um einen Container zu erstellen.



3. Laden Sie das Installationsprogramm für Citrix Virtual Apps and Desktops in den Container hoch.



## Schritt 2: Erstellen einer verwalteten SQL-Instanz im Azure-Portal

Weitere Informationen finden Sie unter [Erstellen einer verwalteten Azure SQL-Instanz](#).

## Schritt 3: Erstellen virtueller Azure-Maschinen (VMs)

Wählen Sie als Image **Windows Server 2019 Datacenter –Gen1** und als Größe **Standard\_D4as\_v4 – 4 vcpus, 16GiB memory**. Weitere Informationen finden Sie unter [Erstellen einer virtuellen Windows-Maschine im Azure-Portal](#).

portal.azure.com/#create/Microsoft.VirtualMachine

Microsoft Azure Search resources, services, and docs (G+)

All services > Virtual machines >

## Create a virtual machine

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ cse-dev-03-ca

Resource group \* ⓘ (New) Resource group  
[Create new](#)

### Instance details

Virtual machine name \* ⓘ

Region \* ⓘ (US) East US

Availability options ⓘ No infrastructure redundancy required

Image \* ⓘ Windows Server 2019 Datacenter - Gen1  
[See all images](#)

Azure Spot instance ⓘ

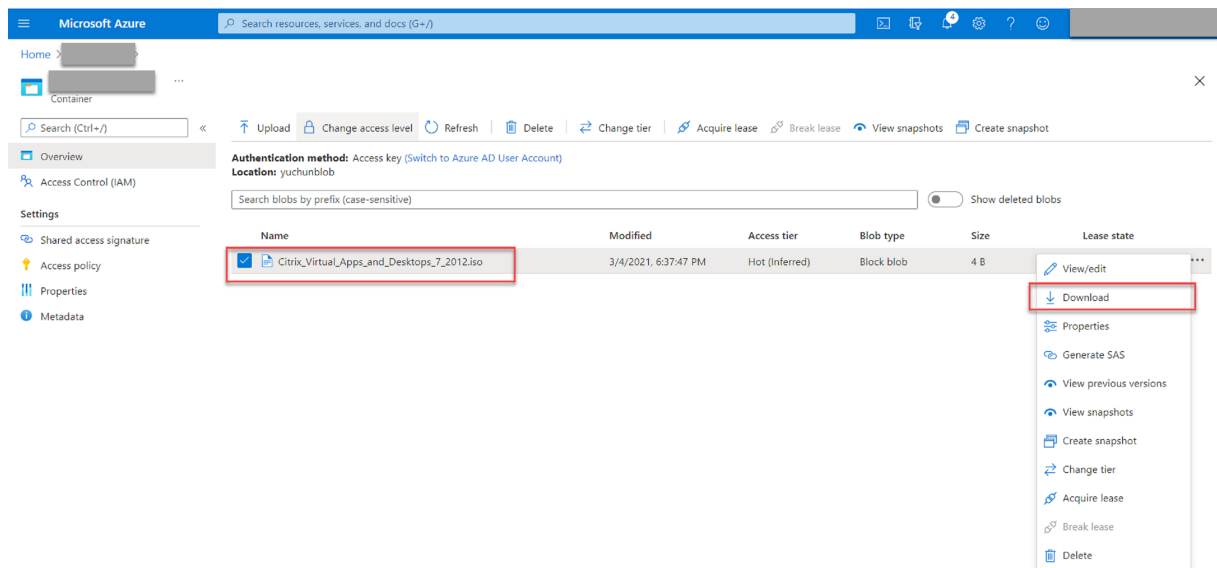
Size \* ⓘ Standard\_D4s\_v3 - 4 vcpus, 16 GiB memory (\$83.22/month)  
[See all sizes](#)

### Administrator account

Username \* ⓘ

[Review + create](#) < Previous Next : Disks >

## Schritt 4: Remote-Desktop und Download des Installationsprogramms für Citrix Virtual Apps and Desktops auf die Azure-VMs



## Schritt 5: Ausführen des Installationsprogramms zur Installation der Komponenten der Sitzungsaufzeichnung auf die Azure-VMs

Weitere Informationen finden Sie unter [Installieren der Verwaltungskomponenten der Sitzungsaufzeichnung](#).

## Schritt 6: Konfigurieren einer Azure-Dateifreigabe zum Speichern von Aufzeichnungen

Führen Sie folgende Schritte aus, um eine Azure-Dateifreigabe zum Speichern von Aufzeichnungen zu erstellen:

1. Erstellen Sie im [Azure-Portal](#) zuerst ein Speicherkonto und dann eine Azure-Dateifreigabe.

Eine Kurzanleitung finden Sie unter [Erstellen und Verwalten von Azure-Dateifreigaben mit dem Azure-Portal](#). Die folgende Tabelle enthält empfohlene Konfigurationen.

Größe der Aufzeichnungsdatei (MB/Stunde)	Anzahl aufgezeichneter Sitzungen pro Tag	Typ der Dateifreigabe	Kontingent der Dateifreigabe (TB)	Sitzungsaufzeichnung –Serveranzahl	Sitzungsaufzeichnung –Servergröße
< 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
ca. 10	< 1.000	HDD Standard (StorageV2)	3	1	Standard D4as_v4
ca. 10	1.000–2.500	SSD Premium	6	1	Standard D4as_v4
ca. 10	2.500–4.000	SSD Premium	10	2	Standard D4as_v4

Das Kontingent für Dateifreigaben wird basierend auf acht Stunden pro Tag, 23 Arbeitstagen pro Monat und einer einmonatigen Aufbewahrungsdauer für jede Aufzeichnungsdatei berechnet.

2. Fügen Sie dem Host, auf dem Sie den Sitzungsaufzeichnungsserver installiert haben, die Anmeldeinformationen der Azure-Dateifreigabe hinzu.

a) Starten Sie eine Eingabeaufforderung als Administrator und ändern Sie das Laufwerk in den Ordner **<Installationspfad des Sitzungsaufzeichnungsservers>\Bin**.

Standardmäßig wird der Sitzungsaufzeichnungsserver in `C:\Program Files\Citrix\SessionRecording\Server` installiert.

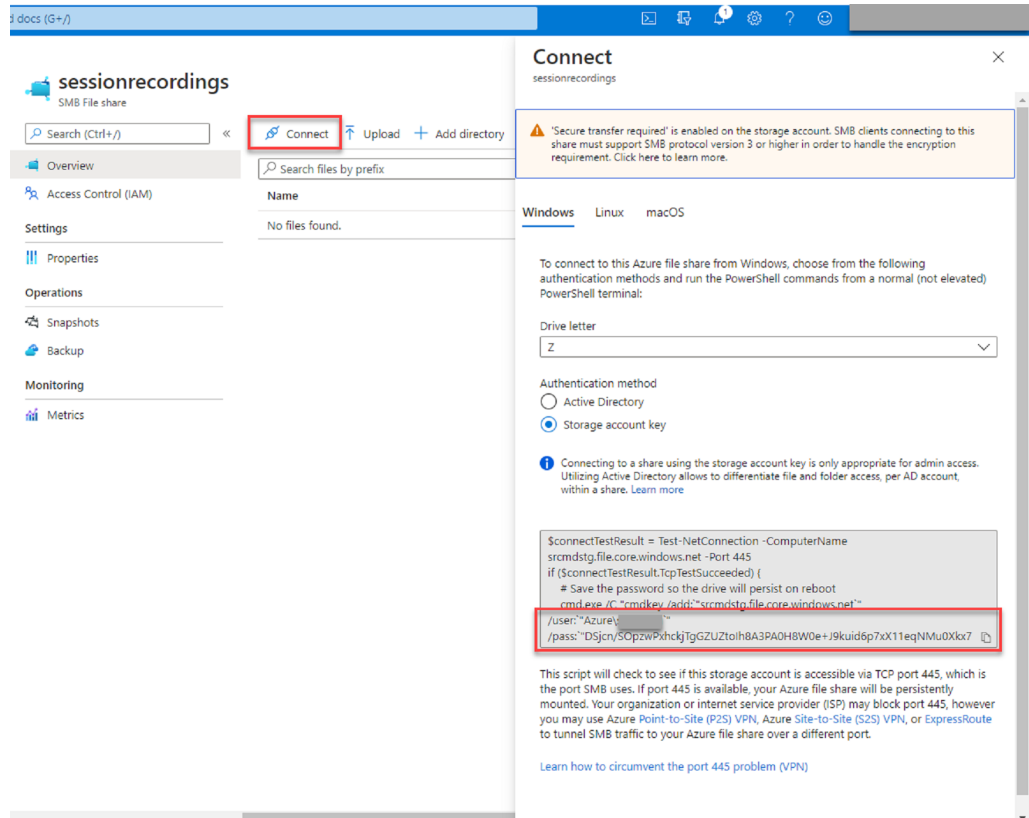
b) Führen Sie den Befehl **SsRecUtils.exe -AddAzureFiles <storageAccountName> <fileShareName> <accesskey>** aus.

Hierbei gilt:

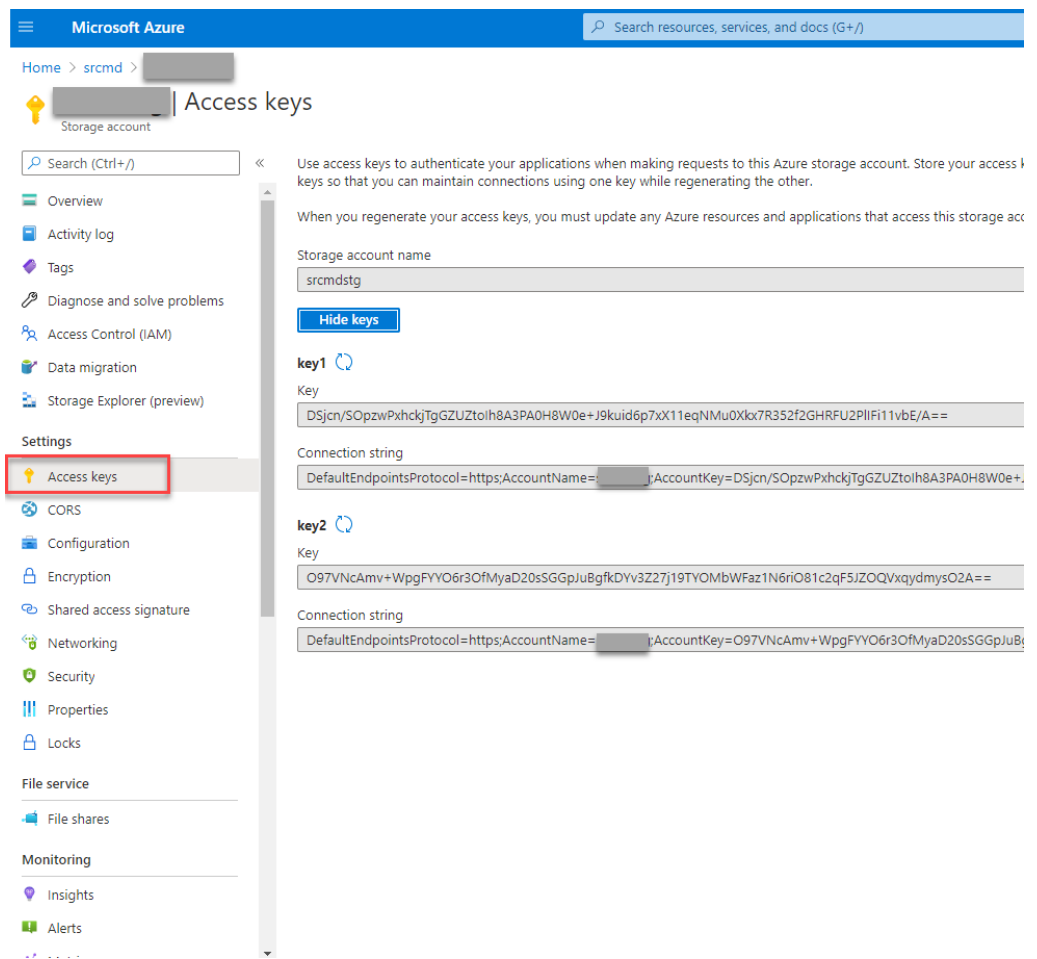
- **<storageaccountname>** ist der Name Ihres Speicherkontos in Azure.
- **<filesharename>** ist der Name der Dateifreigabe, die in Ihrem Speicherkonto enthalten ist.
- **<accesskey>** ist Ihr Speicherkontoschlüssel, der für den Zugriff auf die Dateifreigabe verwendet werden kann.

Sie haben zwei Möglichkeiten, Ihren Speicherkontoschlüssel abzufragen:

- Sie finden den Speicherkontoschlüssel in der angezeigten Verbindungszeichenfolge, wenn Sie auf der Dateifreigabeseite auf die Schaltfläche **Verbinden** klicken.



- Sie können den Speicherkontoschlüssel auch abrufen, indem Sie links in der Speicherkontoseite auf **Zugriffsschlüssel** klicken.



Microsoft Azure

Home > srcmd > [Storage account]

### Access keys

Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account.

Storage account name: srcmdstg

**Hide keys**

**key1**

Key: DSjcn/SOpzwPxxckjTgGZUZtoIh8A3PA0H8W0e+J9kuid6p7xX11eqNMu0Xkx7R352f2GHRFU2PllFi11vbe/A==

Connection string: DefaultEndpointsProtocol=https;AccountName=[Storage account name];AccountKey=DSjcn/SOpzwPxxckjTgGZUZtoIh8A3PA0H8W0e+...

**key2**

Key: O97VncAmv+WpgFY06r3OfMyaD20sSGGpJuBgfkDYv3Z27j19TYOMbWfz1N6riO81c2qF5ZQOQxqydmysO2A==

Connection string: DefaultEndpointsProtocol=https;AccountName=[Storage account name];AccountKey=O97VncAmv+WpgFY06r3OfMyaD20sSGGpJuB...

c) Stellen Sie die Azure-Dateifreigabe auf dem Host bereit, auf dem Sie den Sitzungsaufzeichnungsserver installiert haben.

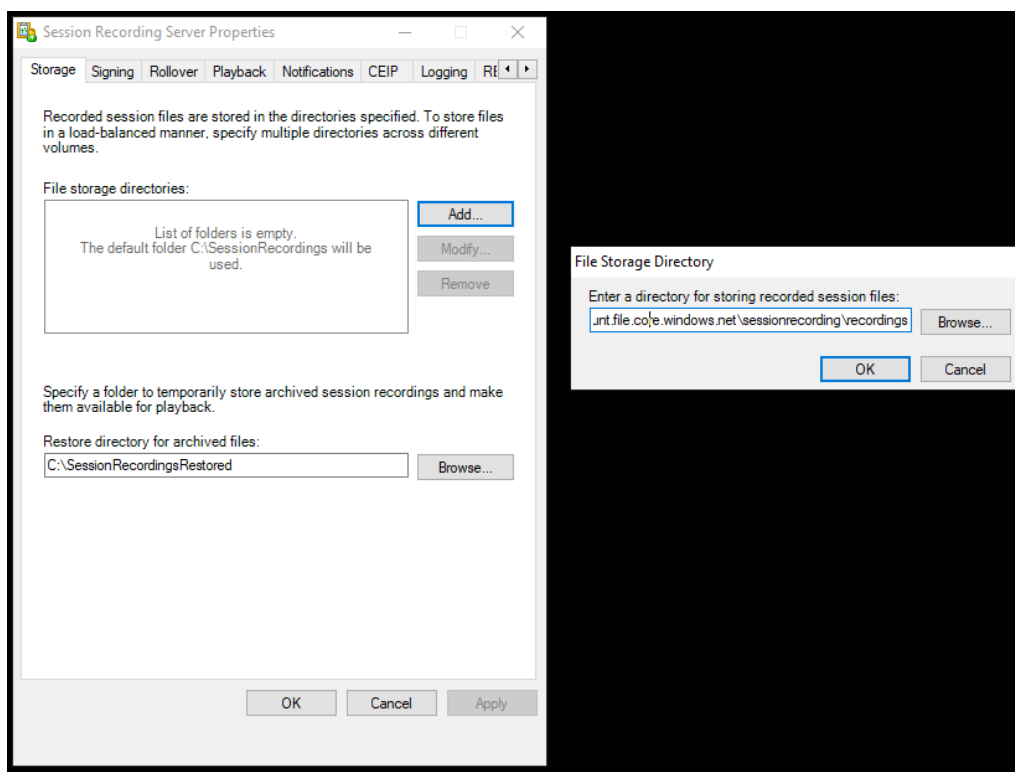
i. Öffnen Sie **Sitzungsaufzeichnungsserver - Eigenschaften**.

ii. Klicken Sie auf der Registerkarte **Speicher** auf **Hinzufügen**.

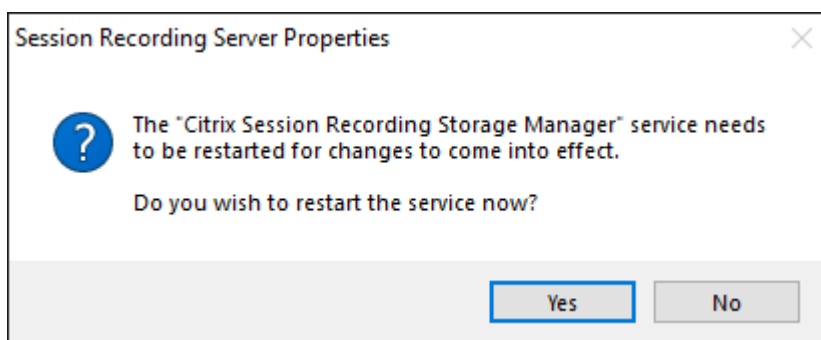
iii. Geben Sie den UNC-Pfad im Format `\\<storageaccountname>.file.core.windows.net\<fileshare>` ein.

Legen Sie unter der Dateifreigabe einen Unterordner fest, in dem Ihre Aufzeichnungsdateien gespeichert werden sollen. Der Sitzungsaufzeichnungsserver erstellt dann automatisch den Unterordner für Sie.





- iv. Klicken Sie im Dialogfeld **Verzeichnis für Dateispeicherung** auf **OK**.
- v. Klicken Sie im Fenster **Sitzungsaufzeichnungsserver - Eigenschaften** auf **Übernehmen**.
- vi. Klicken Sie auf **OK**, nachdem **Übernehmen** abgeblendet ist.
- vii. Klicken Sie auf **Ja**, wenn Sie aufgefordert werden, den Speichermanager der Sitzungsaufzeichnung neu zu starten.



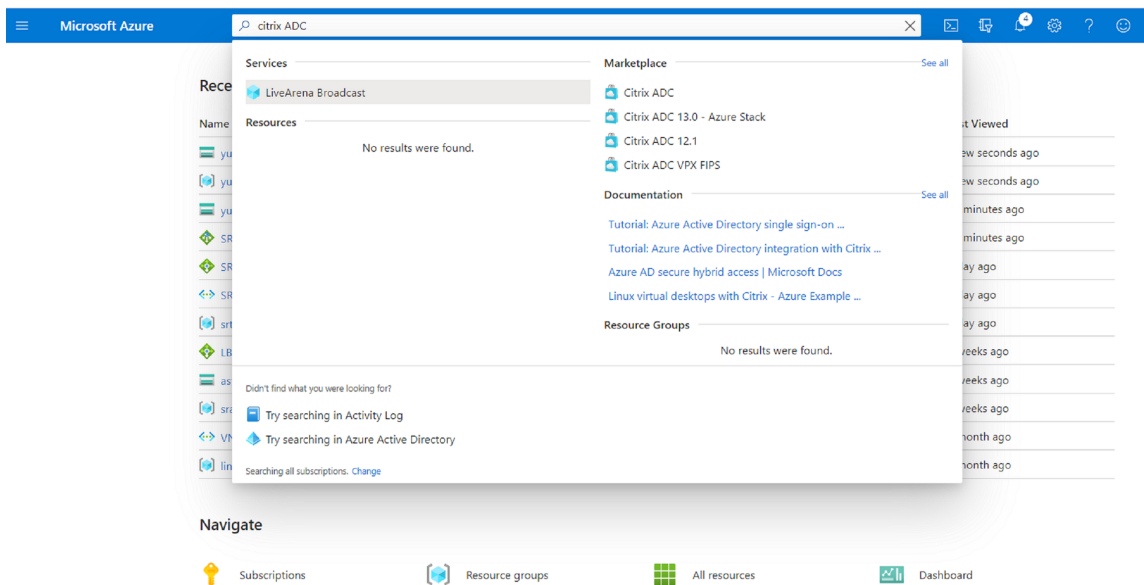
### Schritt 7: Hinzufügen eines Lastausgleichs

Bei mehreren vorhandenen Sitzungsaufzeichnungsservern sollten Sie einen Lastausgleich vor den Servern hinzufügen. Azure bietet zahlreiche Optionen für einen Lastausgleich von Datenverkehrs-

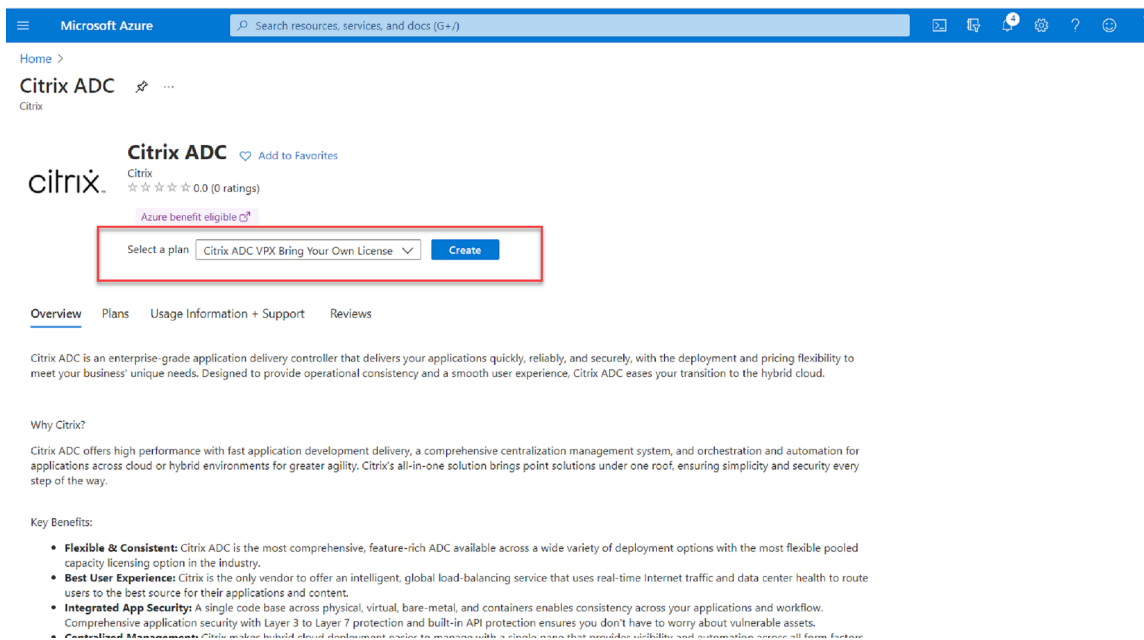
forderungen. Dieser Abschnitt erläutert, wie Sie Citrix ADC, Azure Load Balancer und Azure Application Gateway in Azure erstellen.

### Option 1: Erstellen einer Citrix ADC VPX-Instanz in Azure

1. Geben Sie im **Azure-Portal** Citrix ADC in das Suchfeld ein.

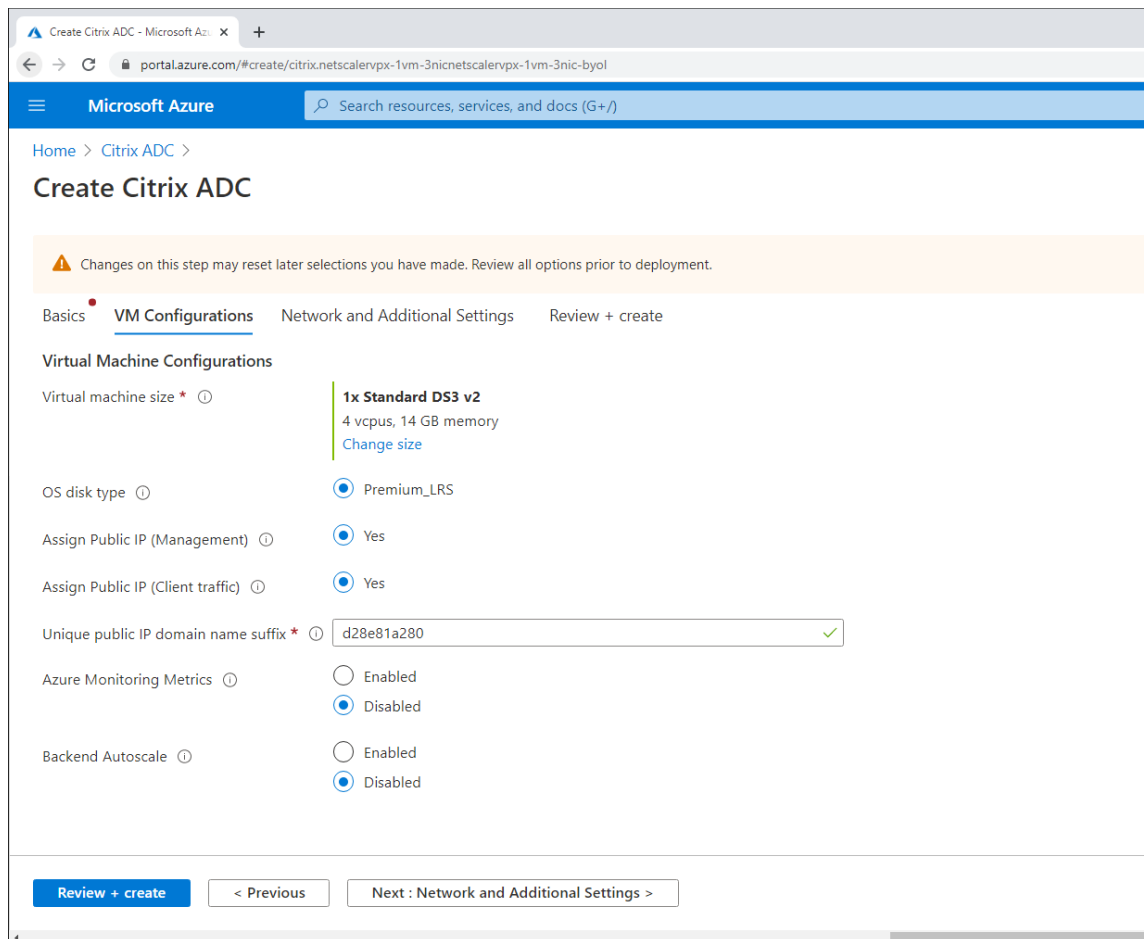


2. Wählen Sie den Plan **Citrix ADC VPX Bring Your Own License** und klicken Sie auf **Erstellen**.



3. Wählen oder erstellen Sie eine Ressourcengruppe und legen Sie die anderen Einstellungen auf der Registerkarte **Grundlagen** fest.

#### 4. Legen Sie VM-Konfigurationen fest.



#### 5. Prüfen und ändern Sie bei Bedarf die Netzwerkeinstellungen. Wählen Sie **ssh (22)**, **http (80)**, **https (443)** als öffentliche Eingangsports.

Ein virtuelles Netzwerk wird automatisch erstellt. Wenn Sie bereits eine Sitzungsaufzeichnungsumgebung installiert haben, können Sie diese Einstellungen für das virtuelle Netzwerk und das Serversubnetz verwenden.

Microsoft Azure Search resources, services, and docs (G+)

Home > Citrix ADC >

## Create Citrix ADC

**Configure virtual networks**

Virtual network \* ⓘ (new) citrix-adc-vpx-virtual-network ▼  
[Create new](#)

Management Subnet \* ⓘ (new) 01-management-subnet (10.128.0/24) ▼

Client Subnet \* ⓘ (new) 11-client-subnet (10.129.0/24) ▼

Server Subnet \* ⓘ (new) 12-server-subnet (10.130.0/24) ▼

**Public IP (Management)**

Management Public IP (NSIP) \* ⓘ (new) citrix-adc-vpx-nsip ▼  
[Create new](#)

Management Domain Name ⓘ citrix-adc-vpx-nsip-23f12ee6b2 ✓  
.eastus.cloudapp.azure.com

**Public IP (Clientside)**

Clientside Public IP (VIP) \* ⓘ (new) citrix-adc-vpx-vip ▼  
[Create new](#)

Clientside Domain Name ⓘ citrix-adc-vpx-vip-23f12ee6b2 ✓  
.eastus.cloudapp.azure.com

**Public Inbound Ports (Management only)**

Ports open for Management public IP ⓘ  None  
 ssh (22)  
 ssh (22), http (80), https (443)

Review + create < Previous Next : Review + create >

Microsoft Azure Search resources, services, and docs

Home > Citrix ADC >

## Create Citrix ADC

Basics VM Configurations **Network and Additional Settings** Review + create

**Boot diagnostics**

Diagnostics storage account \* ⓘ  [Create New](#)

**Network Settings**

**Configure virtual networks**

Virtual network \* ⓘ  [Create new](#)

Management Subnet \* ⓘ

Client Subnet \* ⓘ

Server Subnet \* ⓘ

**Accelerated Networking**

Accelerated Networking (Management Interface) ⓘ  On  Off

Accelerated Networking (Client Interface) ⓘ  On  Off

Accelerated Networking (Server Interface) ⓘ  On  Off

**Public IP (Management)**

Management Public IP (NSIP) \* ⓘ  [Create new](#)

---


[Review + create](#) [< Previous](#) [Next : Review + create >](#)

6. Klicken Sie auf **Weiter: Überprüfen + erstellen**, um die Citrix ADC VPX-Instanz zu erstellen, und warten Sie auf den Abschluss der Bereitstellung.

Microsoft Azure Search resources, services, and documentation

Home > Citrix ADC >

## Create Citrix ADC

 Validation Passed

Basics VM Configurations Network and Additional Settings Review + create

### PRODUCT DETAILS

Citrix ADC  
by Citrix  
[Terms of use](#) | [Privacy policy](#)

### TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

### Basics

Subscription	cse-dev-03-ca
Resource group	srcmdtest
Region	East US
Citrix ADC Release Version	13.0
License Subscription	Bring Your Own License
Virtual Machine name	citrix-adc-vpx
Username	nsroot
Password	*****

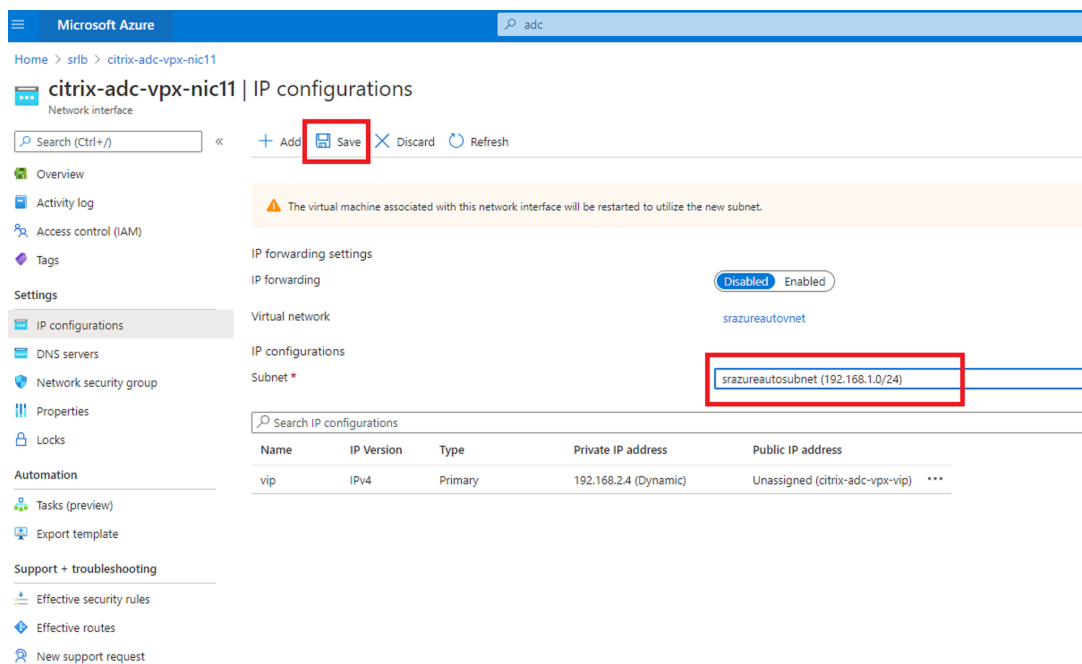
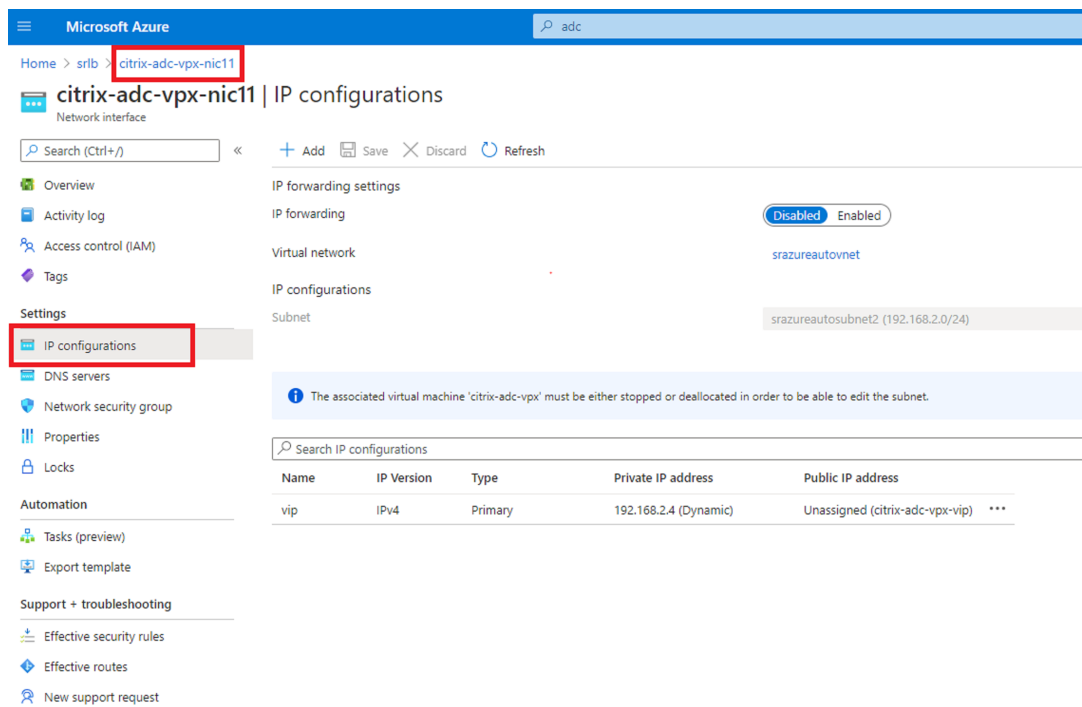
### VM Configurations

[Create](#) [< Previous](#) [Next](#) [Download a template for automation](#)

7. Richten Sie Subnetz-IP-Adresse (SNIP) und Citrix ADC VIP-Adresse so ein, dass sie sich im selben Subnetz befinden.

Die SNIP-Adresse und die VIP-Adresse müssen sich im selben Subnetz befinden. In diesem Beispiel legen wir fest, dass die VIP-Adresse im Subnetz der SNIP-Adresse ist.

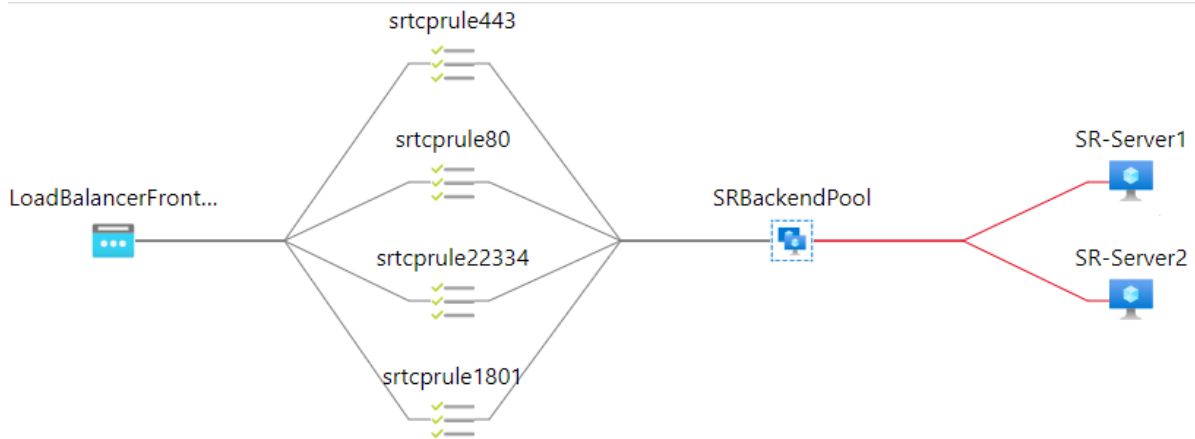
- Halten Sie die virtuelle Maschine **citrix-adc-vpx** an.
- Ändern Sie das Subnetz der VIP-Adresse.



c) Starten Sie die virtuelle Maschine **citrix-adc-vpx**.

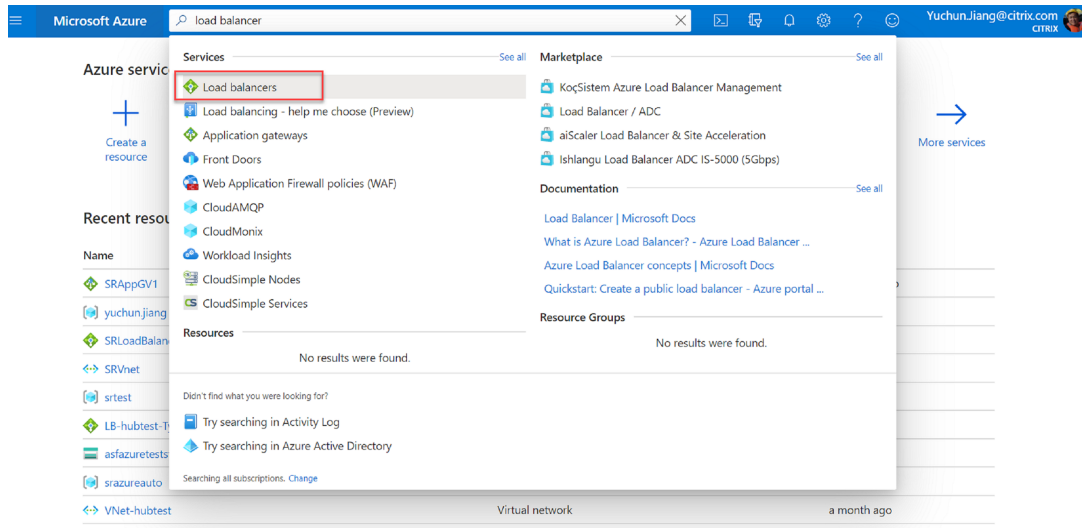
## Option 2: Erstellen eines Azure Load Balancers

Azure Load Balancer ist ein TCP-Passthrough-Dienst. Das folgende Diagramm zeigt den Lastausgleich über einen TCP-Passthrough.



1. Erstellen Sie einen Azure Load Balancer.

a) Suchen und wählen Sie im Azure-Portal **Load Balancers** im **Marketplace**.



Konfigurieren Sie auf der Registerkarte **Grundlagen** der Seite **Lastenausgleich erstellen** die Einstellungen, wie in der folgenden Tabelle beschrieben:

Einstellung	Wert
Abonnement	Wählen Sie Ihr Abonnement aus.
Ressourcengruppe	Wählen Sie zum Beispiel das zuvor erstellte <b>srlbtest</b> .
Name	Geben Sie <b>SRLoadBalance</b> ein.
Region	Wählen Sie <b>(US) East US</b> .
Typ	Wählen Sie <b>Intern</b> .
SKU	Wählen Sie <b>Standard</b> .



Einstellung	Wert
Virtuelles Netzwerk	Wählen Sie zum Beispiel das zuvor erstellte <b>srazureautovnet</b> .
Subnetz	Wählen Sie zum Beispiel das zuvor erstellte <b>srazureautosubnet</b> .
IP-Adresszuweisung	Wählen Sie <b>Dynamisch</b> .
Verfügbarkeitszone	Wählen Sie <b>Zonenredundant</b> .

Microsoft Azure

Home >

## Create load balancer

is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. [Learn more](#).

**Project details**

Subscription \*

Resource group \*  [Create new](#)

**Instance details**

Name \*  ✓

Region \*

Type \*  Internal  Public

SKU \*  Basic  Standard

**Configure virtual network.**

Virtual network \*

Subnet \*  [Manage subnet configuration](#)

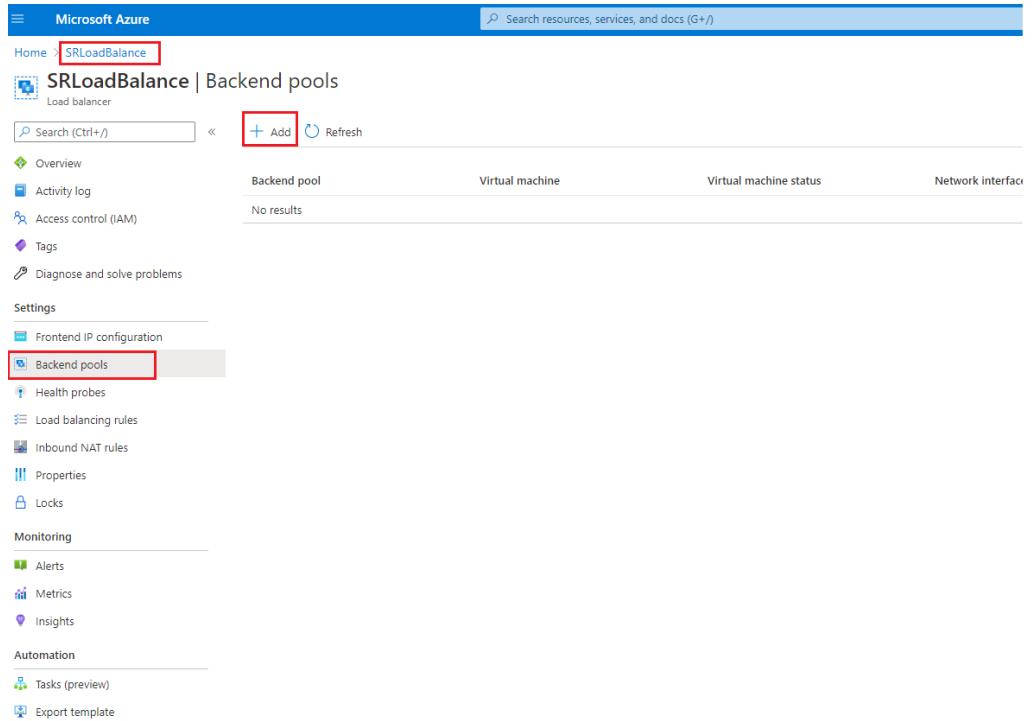
IP address assignment \*  Static  Dynamic

Availability zone \*

[Review + create](#) < Previous Next : Tags > [Download a template for automation](#)

- b) Fügen Sie Load Balancer-Ressourcen hinzu, darunter Back-End-Pools, Integritätsprüfungen und Lastausgleichsregeln.
- Fügen Sie einen Back-End-Pool hinzu.

Wählen Sie den erstellten Load Balancer aus der Ressourcenliste aus und klicken Sie in der linken Navigation auf **Back-End-Pools**. Klicken Sie auf **Hinzufügen**, um einen Back-End-Pool hinzuzufügen.



Geben Sie einen Namen für den neuen Back-End-Pool ein und klicken Sie auf **Hinzufügen**.

Microsoft Azure

Home > SRLoadBalance >

### Add backend pool

SRLoadBalance

Name \*

Virtual network

IP version  IPv4  IPv6

**Virtual machines**

You can only attach virtual machines in eastus that have a standard SKU public IP configuration or no public IP configuration. All IP configurations must be on the same virtual network.

[+ Add](#) [X Remove](#)

Virtual machine ↑↓	IP Configuration ↑↓	Availability set ↑↓
No virtual machines selected		

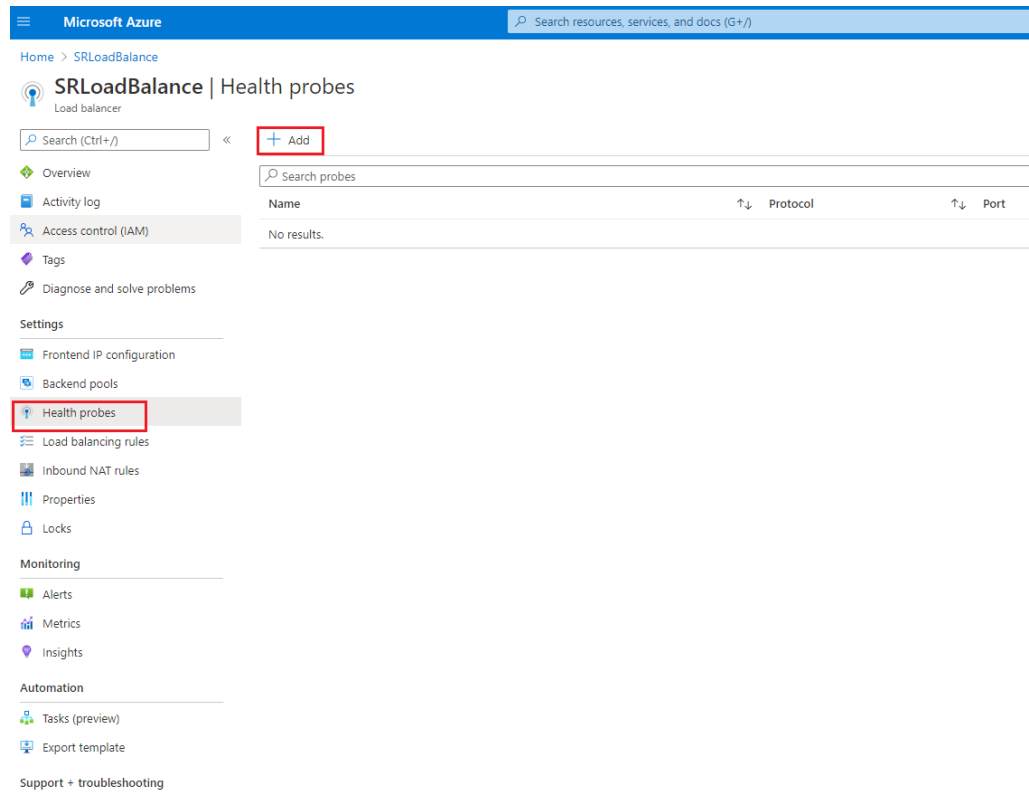
**Virtual machine scale sets**

Virtual Machine Scale Sets must be in same location as Load Balancer. Only IP configurations that have the same SKU (Basic/Standard) as the Load Balancer can be selected. All of the IP configurations have to be in the same Virtual Network.

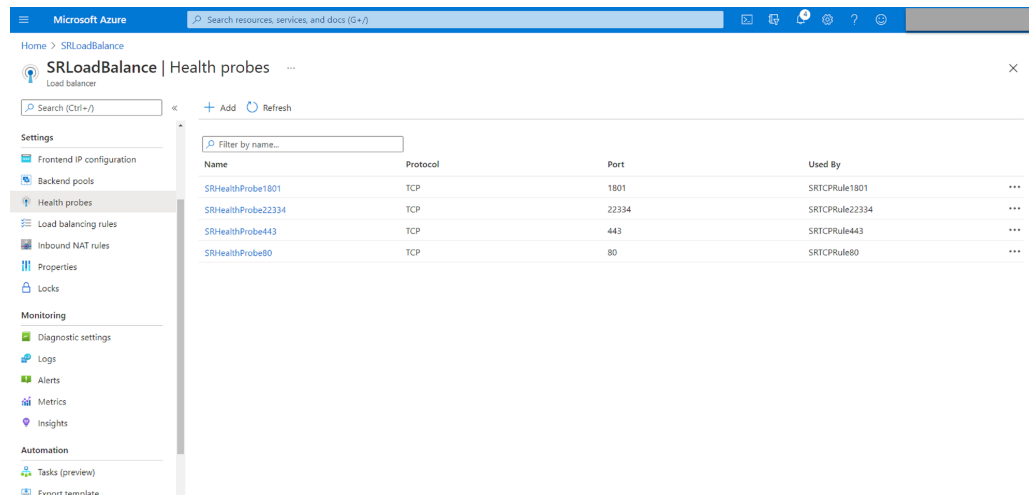
**i** No virtual machine scale set is found in eastus that matches the above criteria

[Add](#)

- Fügen Sie Integritätsprüfungen hinzu.  
Wählen Sie den von Ihnen erstellten Load Balancer aus der Ressourcenliste aus und klicken Sie in der linken Navigation auf **Integritätstests**.



Klicken Sie auf **Hinzufügen**, um Integritätsprüfungen an den Ports 80, 22334, 1801 und 443 hinzuzufügen.



Verwenden Sie beispielsweise die folgenden Einstellungen, um eine Integritätsprüfung an Port 80 zu erstellen.

Einstellung	Wert
Name	Geben Sie <b>SRHealthProbe80</b> ein.
Protokoll	Wählen Sie <b>TCP</b> .

Einstellung	Wert
Port	Geben Sie <b>80</b> ein.
Intervall	5
Fehlerschwellenwert	Wählen Sie 2 als Fehlerschwellenwert. Dies bedeutet, dass zwei Fehler aufeinanderfolgen müssen, bevor eine VM als fehlerhaft gilt.

The screenshot shows the configuration page for an SRHealthProbe in the Microsoft Azure portal. The page title is "SRHealthProbe" under the resource "SRLoadBalance". There are three action buttons: "Save", "Discard", and "Delete". The configuration fields are as follows:

- Name \***: SRHealthProbe80
- Protocol ⓘ**: TCP
- Port \***: 80
- Interval \***: 5 seconds
- Unhealthy threshold \***: 2 consecutive failures
- Used by ⓘ**: Not used

- Fügen Sie eine Lastausgleichsregel hinzu.  
Wählen Sie den von Ihnen erstellten Load Balancer aus der Ressourcenliste aus und klicken Sie in der linken Navigation auf **Lastausgleichsregel**. Klicken Sie auf **Hinzufügen**, um eine Lastausgleichsregel hinzuzufügen.

Microsoft Azure

Home > SRLoadBalance

### SRLoadBalance | Load balancing rules

Load balancer

Search (Ctrl+/) << **+ Add**

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Frontend IP configuration

Backend pools

Health probes

**Load balancing rules**

Inbound NAT rules

Properties

Locks

Monitoring

Alerts

Metrics

Insights

Automation

Tasks (preview)

Export template

Support + troubleshooting

Search load balancing rules

Name	Load balancing rule	Backend pool	Health probe
No results.			

Klicken Sie auf **Hinzufügen**, um Lastausgleichsregeln für die Ports 80, 22334, 1801 und 443 hinzuzufügen.

Microsoft Azure

Home > SRLoadBalance

### SRLoadBalance | Load balancing rules

Load balancer

Search (Ctrl+/) << + Add

Settings

Frontend IP configuration

Backend pools

Health probes

**Load balancing rules**

Inbound NAT rules

Properties

Locks

Monitoring

Diagnostic settings

Logs

Alerts

Metrics

Insights

Automation

Tasks (preview)

Export template

Search load balancing rules

Name	Load balancing rule	Backend pool	Health probe
SRTCPRule1801	SRTCPRule1801 (TCP/1801)	SRBackendPool	SRHealthProbe1801
SRTCPRule22334	SRTCPRule22334 (TCP/22334)	SRBackendPool	SRHealthProbe22334
SRTCPRule443	SRTCPRule443 (TCP/443)	SRBackendPool	SRHealthProbe443
SRTCPRule80	SRTCPRule80 (TCP/80)	SRBackendPool	SRHealthProbe80

Verwenden Sie beispielsweise die folgenden Einstellungen, um eine Lastausgleichsregel für Port 80 zu erstellen.

---

Einstellung	Wert
Name	Geben Sie einen Namen ein, z. B. <b>SRTCPRule80</b> .
IP-Version	Wählen Sie <b>IPv4</b> .
Front-End-IP-Adresse	Wählen Sie <b>LoadBalancerFrontEnd</b> .
Protokoll	Wählen Sie <b>TCP</b> .
Port	Geben Sie <b>80</b> ein.
Back-End-Port	Geben Sie <b>80</b> ein.
Back-End-Pool	Wählen Sie <b>SRBackendPool</b> .
Integritätstest	Wählen Sie <b>SRHealthProbe80</b> .
Sitzungspersistenz	Wählen Sie <b>Client-IP</b> .
Leerlaufzeitüberschreitung (Minuten)	Akzeptieren Sie den Standardwert.
TCP-Zurücksetzung	Wählen Sie <b>Aktiviert</b> aus.
Übersetzung der Quellnetzwerkadresse (SNAT) für ausgehenden Datenverkehr	Wählen Sie <b>(Empfohlen) Verwenden Sie Ausgangsregeln, um Back-End-Poolmitgliedern Zugriff auf das Internet zu gewähren</b> .

---

Microsoft Azure

Home > SRLoadBalance >

### Add load balancing rule

SRLoadBalance

Name \*  
SRTCPRule80 ✓

IP Version \*  
 IPv4  IPv6

Frontend IP address \* ⓘ  
192.168.1.23 (LoadBalancerFrontEnd) ✓

HA Ports ⓘ

Protocol  
 TCP  UDP

Port \*  
80 ✓

Backend port \* ⓘ  
80 ✓

Backend pool ⓘ  
SRBackendPool ✓

Health probe ⓘ  
SRHealthProbe80 (TCP:80) ✓

Session persistence ⓘ  
Client IP ✓

Idle timeout (minutes) ⓘ  
4

TCP reset  
 Disabled  Enabled

Floating IP ⓘ

OK

- Fügen Sie dem Back-End-Pool die Azure-VMs hinzu, auf denen der Sitzungsaufzeichnungsserver installiert ist.



The screenshot shows the Azure portal interface for configuring a load balancer. The main page displays the 'SRBackendPool' under the 'Backend pools' section. A modal window titled 'Add virtual machines to backend pool' is open, showing a table of virtual machines and their IP configurations.

Virtual machine	Resource group	IP Configuration	Availability set	Tags	Notes
<input type="checkbox"/> sr-server1		ipconfig1 (10.7.1.5)	-	-	-
<input type="checkbox"/> sr-server2		ipconfig1 (10.7.1.6)	-	-	-

c) Testen Sie den Azure Load Balancer.

Wenn Sie dem Back-End-Pool einen Server nicht hinzufügen können, wird folgende Fehlermeldung angezeigt: **NetworkInterfaceAndLoadBalancerAreInDifferentAvailabilitySets**. Heben Sie in diesem Fall die Zuordnung der öffentlichen IP-Adresse der Servernetzwerkschnittstelle auf.

Microsoft Azure

Home > srlbtest > SR-Server1-ip > sr-server172 >

# ipconfig1

sr-server172

Save Discard

Public IP address settings

Public IP address

Disassociate Associate

Public IP address \*

SR-Server1-ip (20.62.236.36)

Create new

Private IP address settings

Virtual network/subnet

srazureautovnet/srazureautosubnet

Assignment

Dynamic Static

IP address

192.168.1.19

### Option 3: Erstellen eines Azure Application Gateway

#### Tipp:

Application Gateway V2 unterstützt keine Routinganforderungen über einen NTLM-fähigen Proxy.

1. Erstellen Sie ein Azure Application Gateway.

Konfigurieren Sie die folgenden Einstellungen beim Erstellen eines Anwendungsgateways.

- Wählen Sie auf der Registerkarte **Grundlagen** für **Ebene** die Einstellung **Standard**.
- Wählen Sie auf der Registerkarte **Front-Ends** für **Typ der Front-End-IP-Adresse** die Einstellung **Privat**. Das neue Anwendungsgateway wird als interner Load Balancer verwendet.

2. Fügen Sie einen Back-End-Pool hinzu.

[Home](#) > [SRAppGV1](#) >

## Edit backend pool

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machines scale sets, IP addresses, domain names, or an App Service.

Name

AGbackendpool



Add backend pool without targets

Yes

No

Backend targets

2 items

Target type	Target	
IP address or FQDN	192.168.1.13	 ...
IP address or FQDN	192.168.1.18	 ...
IP address or FQDN		

Associated rule

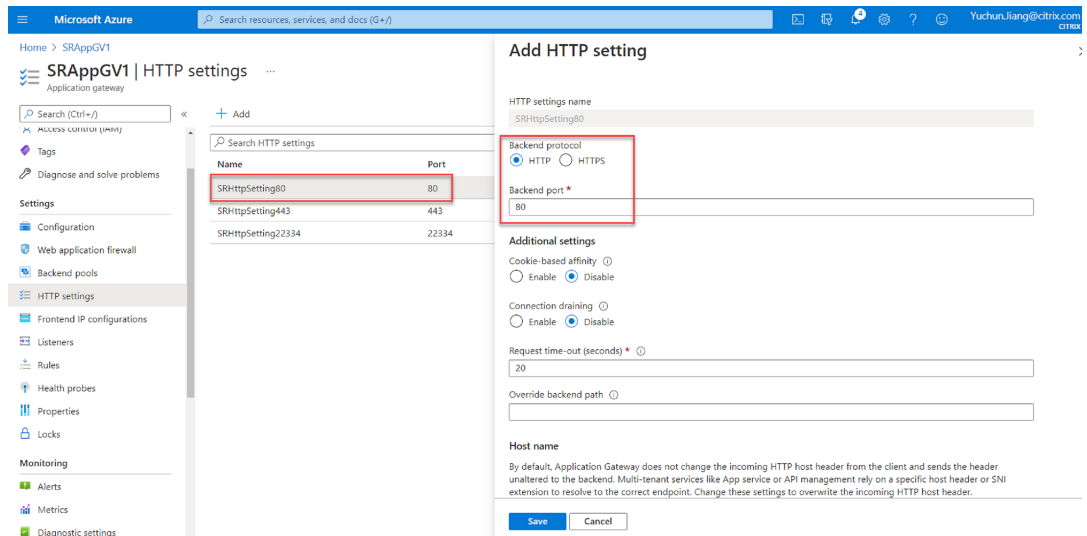
[SRHttpRule80](#)

[SRHttpRule443](#)

### 3. Erstellen Sie HTTP-Einstellungen.

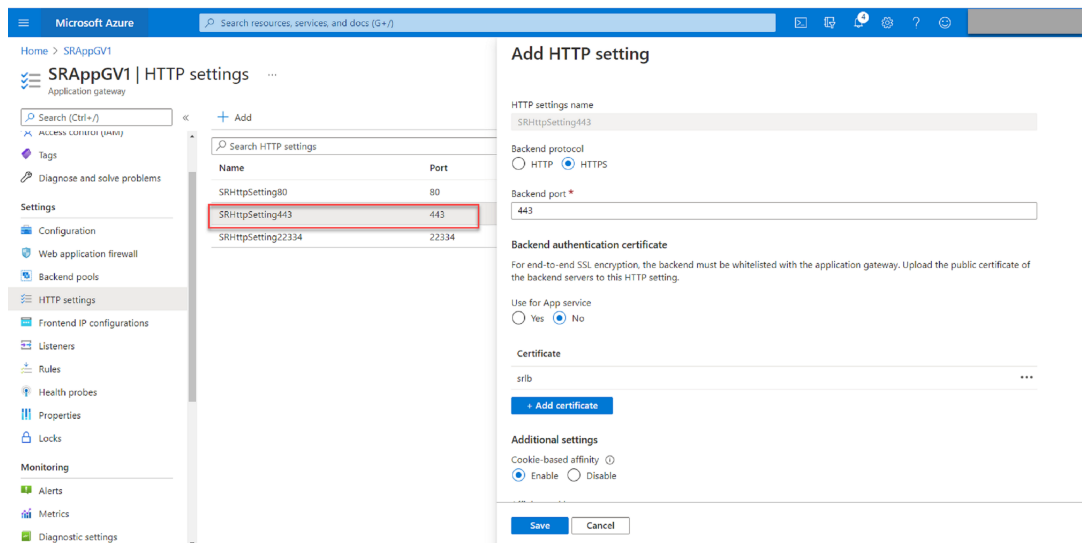
Azure Application Gateway unterstützt sowohl HTTP als auch HTTPS für Routinganforderungen an Back-End-Server. Erstellen Sie HTTP-Einstellungen für die Ports 80, 443 und 22334.

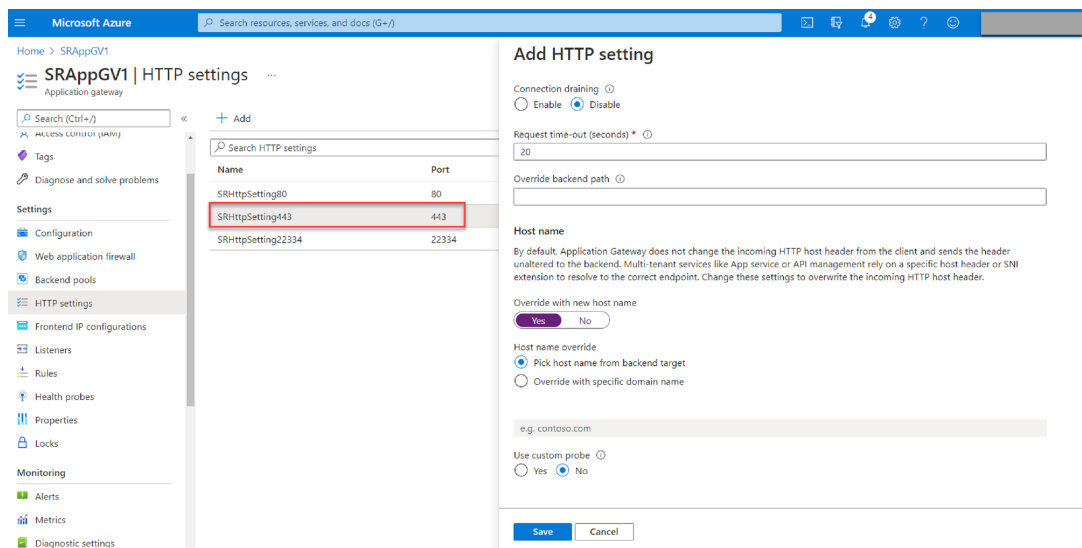
- HTTP über Port 80



- HTTP über Port 443

Ein Authentifizierungszertifikat ist erforderlich, um Back-End-Server in Application Gateway V1 zuzulassen. Das Authentifizierungszertifikat ist der öffentliche Schlüssel von Back-End-Serverzertifikaten im Base64-codierten X.509 (CER)-Format. Informationen zum Exportieren des öffentlichen Schlüssels aus dem TLS/SSL-Zertifikat finden Sie unter [Exportieren von Authentifizierungszertifikaten \(für v1-SKU\)](#).



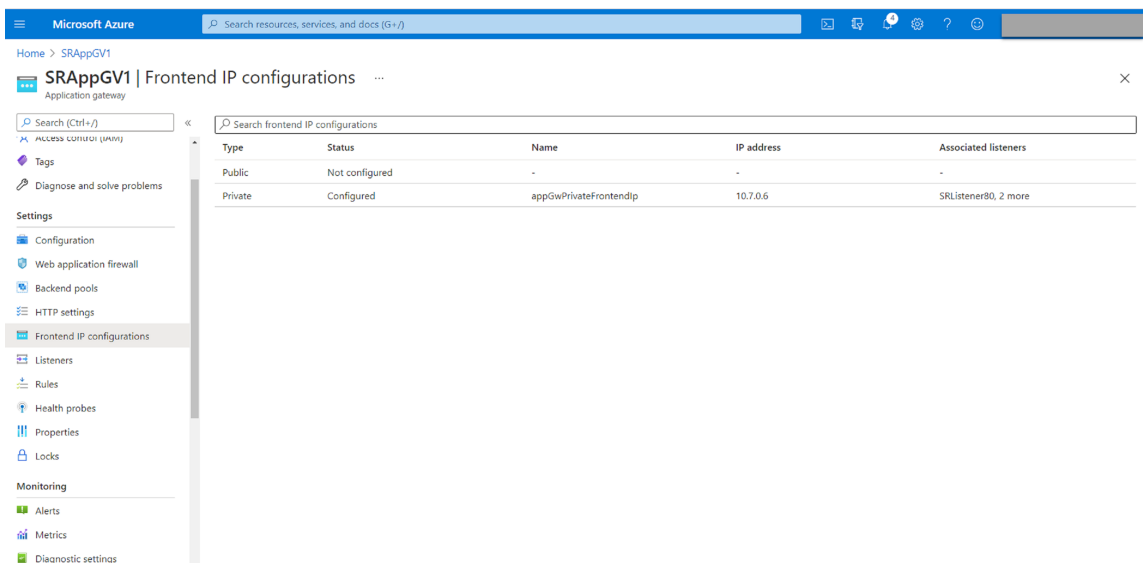


- HTTP oder HTTPS über Port 22334

Wenn WebSocket HTTP verwendet, verwenden Sie dieselbe Einstellung wie Port 80.

Wenn WebSocket HTTPS verwendet, verwenden Sie dieselbe Einstellung wie Port 443.

4. Fügen Sie eine Front-End-IP-Adresse hinzu.



5. Fügen Sie Listener hinzu.

Fügen Sie Listener an den Ports 80, 443 und 22334 hinzu, zum Beispiel:

SRAppGV1 | Listeners

Application gateway

Search (Ctrl+/) | + Add listener | Refresh

Application Gateway provides native support for WebSocket across all gateway sizes. There is no additional configuration required to enable or disable WebSocket support. If a WebSocket traffic is received on the Application Gateway, it is automatically directed to the WebSocket enabled backend server using the appropriate backend pool as specified in application gateway rules.

Search listeners

Name	Protocol	Port	Associated rule	Host name
SRListener80	HTTP	80	SRHttpRule80	-
SRListener443	HTTPS	443	SRHttpRule443	-
SRListener22334	HTTPS	22334	SRHttpRule22334	-

SSL Policy

The SSL policy defines the SSL protocol version and available ciphers. Choose from one of the predefined policies or create a custom security policy to match your organizational security requirements.

Learn more about SSL policy.

Selected SSL Policy  
Default (change)

Min protocol version  
TLSv1.0

Cipher suites

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

- Listener an Port 80

SRAppGV1

Listener name  
SRListener80

Frontend IP \*  
Private

Port \*  
80

Protocol  
 HTTP  HTTPS

Associated rule  
SRHttpRule80

Additional settings

Listener type  
 Basic  Multi site

Error page url  
 Yes  No

- Listener auf Port 443

Erstellen Sie ein selbstsigniertes Zertifikat und laden Sie das Zertifikat in das [Azure-Portal](#), wenn Sie den HTTPS-Listener erstellen. Weitere Informationen finden Sie unter [Unterstützte Zertifikate für die TLS-Beendigung](#) und [Erstellen eines selbstsignierten Zertifikats](#).

[Home](#) > [SRAppGV1](#) >

## SRListener443

SRAppGV1

Listener name ⓘ

SRListener443

Frontend IP \* ⓘ

Private

Port \* ⓘ

443

Protocol ⓘ

HTTP  HTTPS

Choose a certificate

Create new  Select existing

Certificate \*

lbdc

Renew or edit selected certificate

Associated rule

[SRHttpRule443](#)

Additional settings

Listener type ⓘ

Basic  Multi site

Error page url

Yes  No

- Listener an Port 22334

Wenn WebSocket HTTP verwendet, verwenden Sie dieselbe Einstellung wie Port 80. Wenn WebSocket HTTPS verwendet, verwenden Sie dieselbe Einstellung wie Port 443. Das folgende Beispiel zeigt die Einstellung eines HTTPS-Listeners an Port 22334.

Microsoft Azure

Home > SRAppGV1 >

## SRLListener22334

SRAppGV1

Listener name ⓘ  
SRLListener22334

Frontend IP \* ⓘ  
Private

Port \* ⓘ  
22334

Protocol ⓘ  
 HTTP  HTTPS

Choose a certificate  
 Create new  Select existing

Certificate \*  
lbdc

Renew or edit selected certificate

Associated rule  
[SRHttpRule22334](#)

**Additional settings**

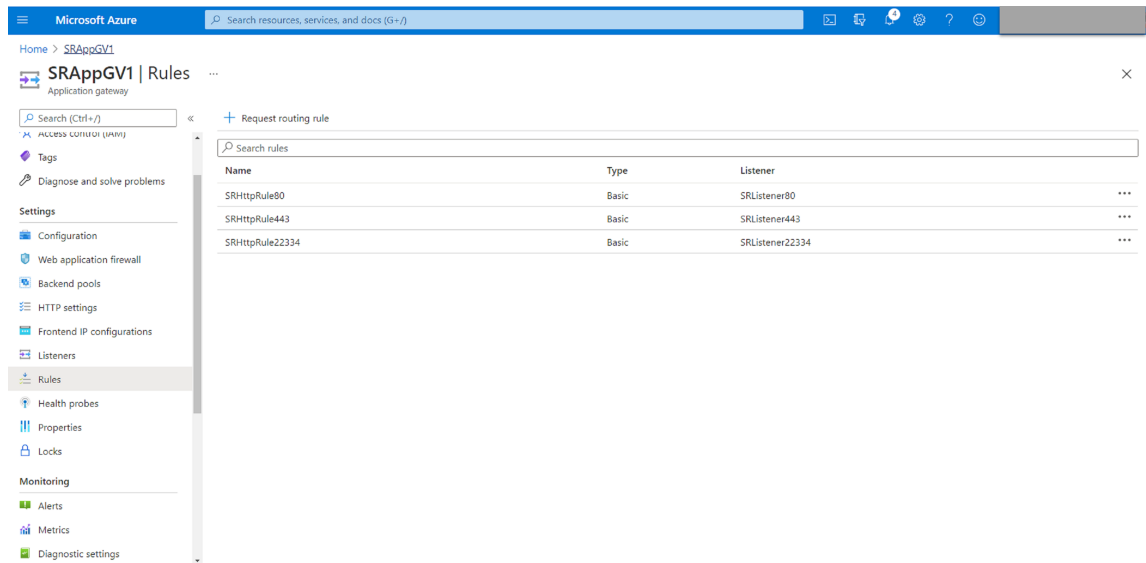
Listener type ⓘ  
 Basic  Multi site

Error page url  
 Yes  No

6. Erstellen Sie Anforderungsroutingregeln.

Erstellen Sie Regeln für die Ports 80, 443 und 22334, zum Beispiel:





- Routingregel für Port 80

## SRHttpRule80

SRAppGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name

**\* Listener** \* Backend targets

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener \*

## SRHttpRule80

SRAppGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name

\* Listener **\* Backend targets**

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

Target type  Backend pool  Redirection

Backend target \*

HTTP settings \*

- Routingregel für Port 443

### SRHttpRequest443

SRAppGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name

**\* Listener** **\* Backend targets**

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener \*

### SRHttpRequest443

SRAppGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name

**\* Listener** **\* Backend targets**

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

Target type  Backend pool  Redirection

Backend target \*

HTTP settings \*

- Routingregel für Port 22334

### SRHttpRequest22334

SRAppGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name

**\* Listener** **\* Backend targets**

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener \*

## SRHttpRule22334

SRAAppGV1

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name

\* Listener   \* Backend targets

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

Target type    Backend pool    Redirection

Backend target \* ⓘ  

HTTP settings \* ⓘ  

7. Fügen Sie dem Back-End-Pool die Azure-VMs hinzu, auf denen der Sitzungsaufzeichnungsserver installiert ist.
8. Konfigurieren Sie Sitzungsaufzeichnungsserver gemäß dem Knowledge Center-Artikel [CTX230015](#).



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).