Adaptive Authentifizierung

Machine translated content

Disclaimer

Contents

Versionshinweise

June 19, 2024

Die Versionshinweise zur adaptiven Authentifizierung sind ein Teil der NetScaler-Versionshinweise. Kunden von Adaptive Authentication müssen die NetScaler-Versionshinweise verwenden, um sich über die Verbesserungen, behobenen Probleme und die bekannten Probleme im Adaptive Authentication Service zu informieren.

> **Hinweis:**
>
> Das Datum in diesem Dokument bezieht sich auf das Datum des letzten Upgrades des Dienstes.

16 Jan 2024

Was ist neu

- **Automatisches Upgrade der Adaptive Authentication-Instanzen**

Adaptive Authentication-Instanzen werden automatisch auf Build 14.1—12.35 und höher aktualisiert, wodurch die in CTX584986 beschriebenen Sicherheitslücken behoben werden.

26 Sep 2023

Was ist neu

- **Automatisches Upgrade der Adaptive Authentication-Instanzen**

Adaptive Authentication-Instanzen werden automatisch auf Build 14.1—8.50 und höher aktualisiert, wodurch die in CTX579459 beschriebenen Sicherheitslücken behoben werden.

18 July 2023

Was ist neu

- **Automatisches Upgrade der Adaptive Authentication-Instanzen**

Adaptive Authentication-Instanzen werden automatisch auf Build 13.1—49.101 und höher aktualisiert, wodurch die in CTX561482 beschriebenen Sicherheitslücken behoben werden.

28. April 2023

Was ist neu

- **LDAP- und LDAPS-Unterstützung mit Load Balancing**

  Die Citrix Adaptive Authentication-Instanz bietet LDAP- und LDAPS-Unterstützung mithilfe eines virtuellen Load-Balancing-Servers. Weitere Informationen finden Sie unter Beispiel für eine LDAP- und LDAPS-Load-Balancing-Konfiguration.

  [AAUTH-2067]

- **Zuordnung von Backend-AD- oder RADIUS-Serversubnetzen zu Ressourcenstandorten**

  Admins können die Connectors auswählen, über die Backend-AD- und RADIUS-Server erreicht werden müssen. Weitere Informationen finden Sie unter Bereitstellung Adaptiver Authentifizierung.

Behobene Probleme

- Smart Access-Richtlinien und OAuth-Authentifizierungsrichtlinien, die für Adaptive Authentication konfiguriert wurden, fehlen in der NetScaler-GUI.

  [AAUTH-68]

Bekannte Probleme

- Wenn Sie bei einer Adaptiven Authentifizierungsinstanz die Option **Verbindung testen** im LDAP-Profil (NetScaler Admin-GUI) verwenden, um die Konnektivität zu überprüfen, wird der LDAP-Server fälschlicherweise als erreichbar angezeigt, obwohl er nicht erreichbar ist.

  [AAUTH-2111]

Adaptiven Authentifizierungsdienst konfigurieren

June 19, 2024

Die folgenden allgemeinen Schritte sind für die Konfiguration des Adaptiven Authentifizierungsdienstes erforderlich.

1. Adaptive Authentifizierung bereitstellen
2. Richtlinien für die adaptive Authentifizierung konfigurieren
3. Adaptive Authentifizierung für Workspace aktivieren

Voraussetzungen

- Reservieren Sie einen FQDN für Ihre Instanz der adaptiven Authentifizierung. Beispiel: `aauth.xyz.com`, dabei wird angenommen, dass `xyz.com` Ihre Unternehmensdomäne ist. Dieser FQDN wird in diesem Dokument als FQDN des Adaptive Authentication Service bezeichnet und bei der Bereitstellung der Instanz verwendet. Ordnen Sie den FQDN der öffentlichen IP-Adresse des virtuellen IdP-Servers zu. Diese IP-Adresse wird nach der Bereitstellung im Schritt **Zertifikat hochladen** abgerufen.
- Beschaffen Sie sich ein Zertifikat für aauth.xyz.com. Zertifikate müssen das SAN-Attribut enthalten. Andernfalls werden die Zertifikate nicht akzeptiert.
- Die Benutzeroberfläche für die adaptive Authentifizierung unterstützt das Hochladen von Zertifikatspaketen nicht. Informationen zum Verknüpfen eines Zwischenzertifikats finden Sie unter Zwischenzertifikate konfigurieren.
- Wählen Sie Ihren Konnektivitätstyp für die on-premises AD/RADIUS-Konnektivität. Die folgenden zwei Optionen sind verfügbar. Wenn Sie keine Erreichbarkeit des Rechenzentrums wünschen, verwenden Sie den Konnektivitätstyp Connector.
  - **Citrix Cloud Connector** —Einzelheiten finden Sie unter Citrix Cloud Connector.
  - **Azure VNet-Peering** —Einzelheiten finden Sie unter Konnektivität zu on-premises Authentifizierungsservern mithilfe von Azure VNet-Peering einrichten.
- Konfigurieren Sie einen NTP-Server (Network Time Protocol), um Zeitversatz zu vermeiden. Einzelheiten finden Sie unter Synchronisieren der Systemuhr mit Servern im Netzwerk.

Wichtige Hinweise

- Citrix empfiehlt, Clear Config für keine Adaptive Authentication-Instanz auszuführen oder Konfigurationen mit dem Präfix `AA` (z. B. AAuthAutoConfig), einschließlich Zertifikaten, zu ändern. Dadurch wird die Verwaltung der adaptiven Authentifizierung gestört und der Benutzerzugriff wird beeinträchtigt. Die einzige Möglichkeit zur Wiederherstellung ist die erneute Bereitstellung.
- Fügen Sie kein SNIP oder zusätzliche Routen auf der Adaptive Authentication-Instanz hinzu.
- Die Benutzerauthentifizierung schlägt fehl, wenn die Kundennummer nicht in Kleinbuchstaben geschrieben ist. Sie können Ihre ID in Kleinbuchstaben umwandeln und sie auf der NetScaler-Instanz mit dem Befehl `set cloud parameter -customerID <all_lowercase_customerid>` festlegen.
- Die nFactor-Konfiguration, die für den Citrix Workspace- oder den Citrix Secure Private Access Service erforderlich ist, ist die einzige Konfiguration, die Kunden direkt auf den Instanzen erstellen sollten. Derzeit gibt es in NetScaler keine Prüfungen oder Warnungen, die Administratoren daran hindern, diese Änderungen vorzunehmen.

- Es wird empfohlen, dass alle benutzerdefinierten Konfigurationen in der Benutzeroberfläche und nicht direkt auf den Adaptive Authentication-Instanzen vorgenommen werden. Dies liegt daran, dass die an den Instanzen vorgenommenen Änderungen nicht automatisch mit der Benutzeroberfläche synchronisiert werden und die Änderungen daher verloren gehen.
- Aktualisieren Sie die Adaptive Authentication-Instanzen nicht auf zufällige RTM-Builds. Alle Upgrades werden von Citrix Cloud verwaltet.
- Nur ein Windows-basierter Cloud-Connector wird unterstützt. Connector-Appliance wird in dieser Version nicht unterstützt.
- Wenn Sie bereits Citrix Cloud-Kunde sind und Azure AD (oder andere Authentifizierungsmethoden) bereits konfiguriert haben, müssen Sie Adaptive Authentication als Authentifizierungsmethode konfigurieren und die Authentifizierungsrichtlinien in der Adaptive Authentication-Instanz konfigurieren, um zur adaptiven Authentifizierung zu wechseln (z. B. Gerätezustandsprüfung). Einzelheiten finden Sie unter Verbinden von Citrix Cloud mit Azure AD.
- Fügen Sie für die Bereitstellung eines RADIUS-Servers alle privaten Connector-IP-Adressen als RADIUS-Clients im RADIUS-Server hinzu.
- In der aktuellen Version ist der externe ADM-Agent nicht zulässig und daher wird Citrix Analytics (CAS) nicht unterstützt.
- Der NetScaler Application Delivery Management Service sammelt das Backup für Ihre Adaptive Authentication-Instanz. Integrieren Sie den ADM Service, um das Backup aus ADM zu extrahieren. Einzelheiten finden Sie unter Konfiguration Backup und wiederherstellen. Citrix nimmt die Backups nicht explizit vom Adaptive Authentication Service. Kunden müssen bei Bedarf die Backup ihrer Konfigurationen vom Application Delivery Management Service erstellen.
- Die Adaptive Authentication-Instanzen können den Tunnel nicht einrichten, wenn im Setup des Kunden ein Proxy konfiguriert ist. Daher wird empfohlen, die Proxykonfiguration für die adaptive Authentifizierung zu deaktivieren.
- Wenn Sie Authentifizierungsdienste von Drittanbietern wie SAML verwenden, schlägt die Authentifizierung möglicherweise fehl, wenn nicht alle Ansprüche gefunden werden. Daher wird Kunden empfohlen, der Konfiguration der Multifaktor-Authentifizierung einen zusätzlichen Faktor wie NOAUTH hinzuzufügen, um alle Ansprüche zu erfüllen.
- Es wird empfohlen, das Debug-Log-Level während des normalen Betriebs deaktiviert zu lassen und nur bei Bedarf zu aktivieren. Wenn das Debug-Log-Level immer aktiviert ist, verursacht dies eine enorme Belastung der Management-CPU. Dies kann bei hoher Verkehrsbelastung zu Systemabstürzen führen. Weitere Informationen finden Sie unter CTX222945.

So konfigurieren Sie den Adaptiven Authentifizierungsdienst

Zugreifen auf die Benutzeroberfläche für Adaptive Authentication

Sie können mit einer der folgenden Methoden auf die Benutzeroberfläche für Adaptive Authentication zugreifen.

- Geben Sie die URL manuell ein https://adaptive-authentication.cloud.com.
- Melden Sie sich mit Ihren Zugangsdaten an und wählen Sie einen Kunden aus.

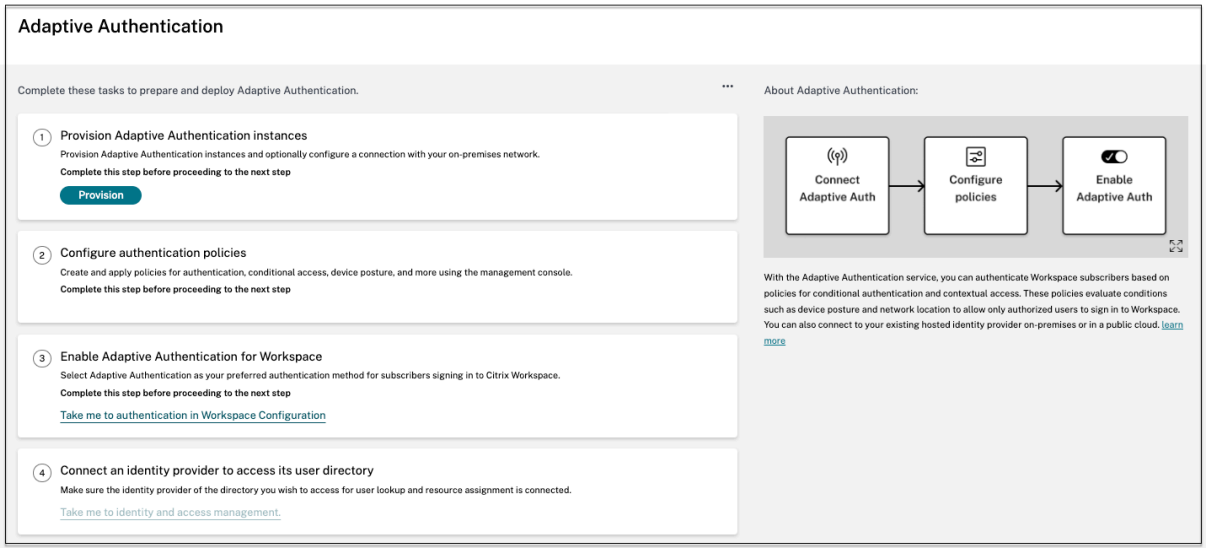
  Nachdem Sie erfolgreich authentifiziert wurden, werden Sie zur Benutzeroberfläche der adaptiven Authentifizierung weitergeleitet.

ODER

- Navigieren Sie zu **Citrix Cloud > Identitäts- und Zugriffsmanagement**.
- Klicken Sie auf der Registerkarte Authentifizierung unter **Adaptive Authentifizierung** auf das Ellipsenmenü und wählen Sie **Verwalten** aus.

Die Benutzeroberfläche der adaptiven Authentifizierung wird angezeigt.

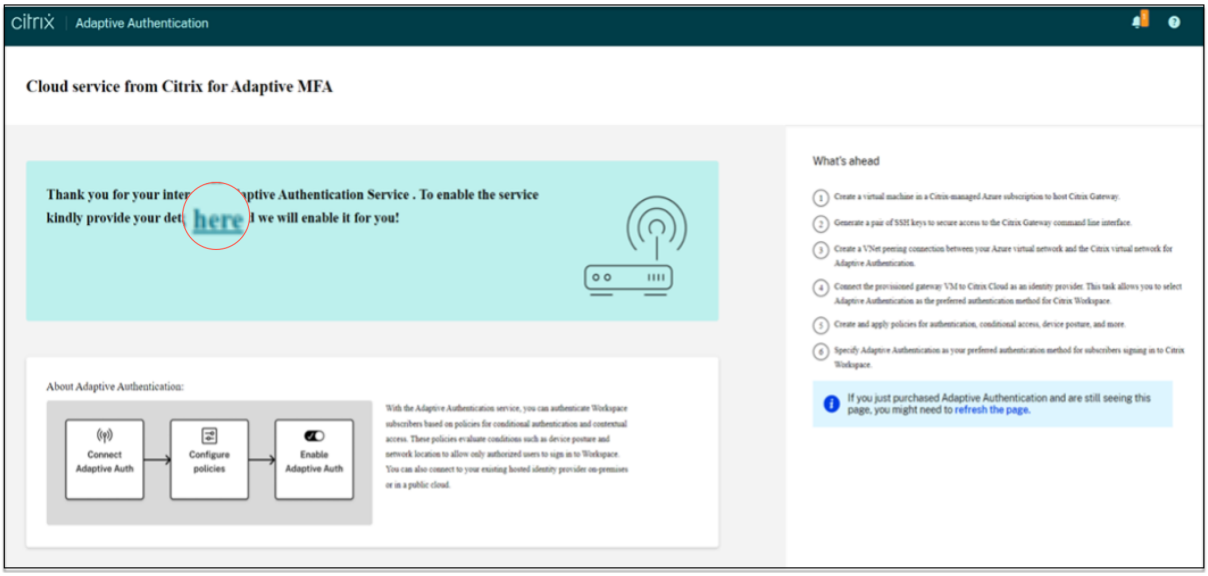
Die folgende Abbildung zeigt die Schritte, die beim Konfigurieren der adaptiven Authentifizierung erforderlich sind.



Schritt 1: Adaptive Authentifizierung bereitstellen

> **Wichtig:**
>
> Kunden, die am Adaptive Authentication Service interessiert sind, müssen auf den Link klicken, wie im folgenden Screenshot gezeigt, und das Podio-Formular ausfüllen. Das Citrix Adaptive

> Authentication-Team aktiviert dann die Bereitstellung von Adaptive Authentication-Instanzen.



Gehen Sie wie folgt vor, um die Adaptive Authentication-Instanz bereitzustellen:

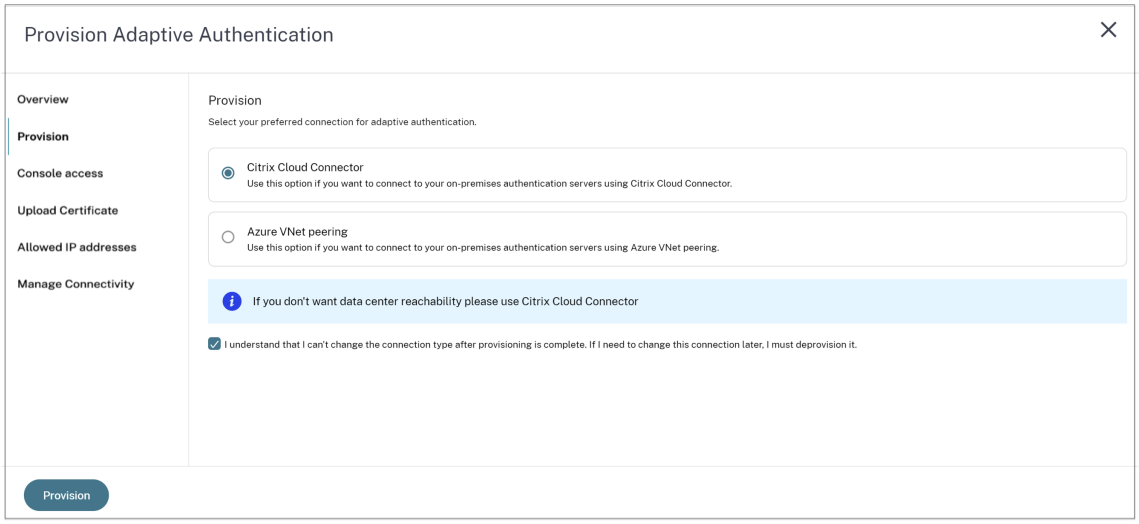
1. Klicken Sie auf der Benutzeroberfläche für **adaptive Authentifizierung** auf **Bereitstellen**.
2. Wählen Sie die bevorzugte Verbindung für die adaptive Authentifizierung aus.

    - **Citrix Cloud Connector:** Für diesen Verbindungstyp müssen Sie einen Connector in Ihrem on-premises Netzwerk einrichten. Citrix empfiehlt, dass Sie mindestens zwei Citrix Cloud Connectors in Ihrer Umgebung bereitstellen, um die Verbindung mit dem auf Azure gehosteten Citrix Gateway einzurichten. Sie müssen Ihrem Citrix Cloud Connector den Zugriff auf die Domäne/URL gewähren, die Sie für die Instanz der adaptiven Authentifizierung reserviert haben. Erlauben Sie beispielsweise https://aauth.xyz.com/*.

      Einzelheiten zu Citrix Cloud Connector finden Sie unter Citrix Cloud Connector.

    - **Azure VNet-Peering** —Sie müssen die Konnektivität zwischen den Servern mit VNet-Peering von Azure einrichten.

        - Stellen Sie sicher, dass Sie über ein Azure-Abonnementkonto verfügen, um die Konnektivität einzurichten.
        - Für das Kunden-VNet, das Peered wird, muss bereits ein Azure VPN-Gateway bereitgestellt sein. Einzelheiten finden Sie unter https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal.



So fügen Sie einen Citrix Cloud Connector als Ihre bevorzugte Verbindung hinzu:

Führen Sie die folgenden Schritte durch.

- Wählen Sie die Option **Citrix Cloud Connector** aus und aktivieren Sie dann das Kontrollkästchen Endbenutzervereinbarung.
- Klicken Sie auf **Provisioning**. Es kann bis zu 30 Minuten dauern, das Provisioning einzurichten.

> **Hinweis:**
>
> Stellen Sie für den Konnektivitätstyp des Connectors sicher, dass Ihr FQDN für Adaptive Authentication nach der Bereitstellung von der virtuellen Connector-Maschine

So richten Sie Azure VNet-Peering ein:

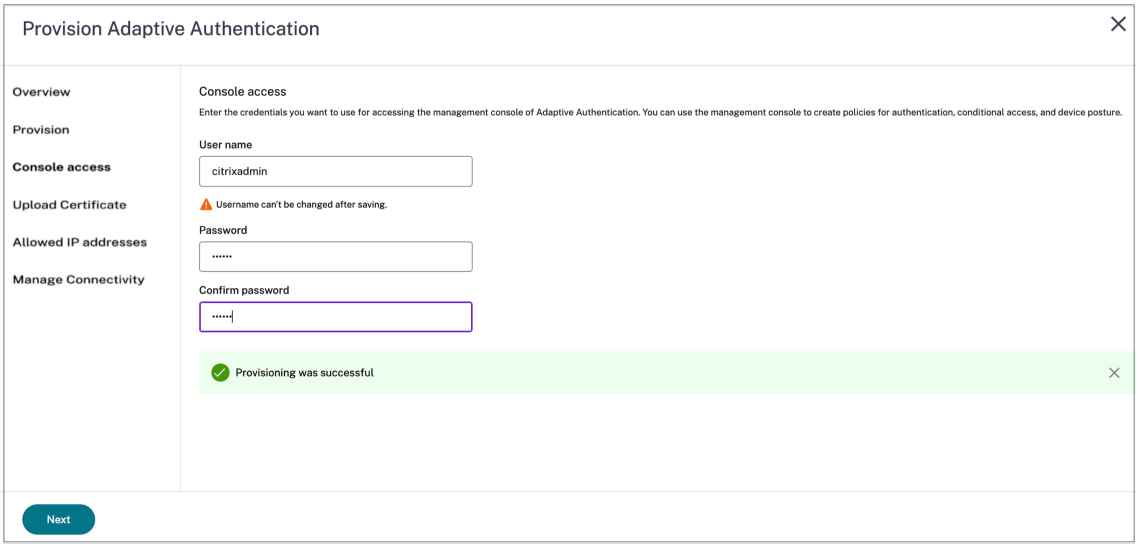
Wenn Sie **Azure VNet-Peering** als Verbindung auswählen, müssen Sie einen Subnetz-CIDR-Block hinzufügen, der zum Bereitstellen der Adaptive Authentication-Instanz verwendet werden muss. Sie müssen auch sicherstellen, dass sich der CIDR-Block nicht mit den anderen Netzwerkbereichen Ihres Unternehmens überschneidet.

Einzelheiten finden Sie unter Einrichten der Konnektivität zu On-Premises-Authentifizierungsservern mit Azure VNet-Peering.

3. Richten Sie Anmeldeinformationen für den Zugriff auf die Instanzen ein, die Sie für die adaptive Authentifizierung aktiviert haben. Sie benötigen den Zugriff auf die Verwaltungskonsole, um Richtlinien für die Authentifizierung, den bedingten Zugriff usw. zu erstellen.

   a) Geben Sie im Bildschirm für den **Zugriff auf die Konsole** den Benutzernamen und das Kennwort ein.
   b) Klicken Sie auf **Weiter**.

> **Hinweis:**
>
> Benutzer, die über den **Konsolenzugriffsbildschirm** erstellt wurden, erhalten "SuperUser"-Rechte, die über den Shell-Zugriff verfügen.



4. Fügen Sie den FQDN des Adaptive Authentication Service hinzu und laden Sie das Zertifikatschlüssel
   Sie müssen den FQDN des Adaptive Authentication Service Ihrer Wahl für den öffentlich zugänglichen Authentifizierungsserver eingeben. Dieser FQDN muss öffentlich auflösbar sein.

   a) Geben **Sie im Bildschirm „Zertifikat hochladen** "den FQDN ein, den Sie für die adaptive Authentifizierung reserviert haben.

   b) Wählen Sie den Zertifikatstyp aus.

      - Der Adaptive Authentication Service unterstützt Zertifikate vom Typ PFX, PEM, DER für die Bereitstellung von Instanzen.
      - Das Zertifikatspaket wird nur für Zertifikate des Typs PEM unterstützt. Für andere Pakettypen empfiehlt Citrix, die Stamm- und Zwischenzertifikate zu installieren und sie mit dem Serverzertifikat zu verknüpfen.

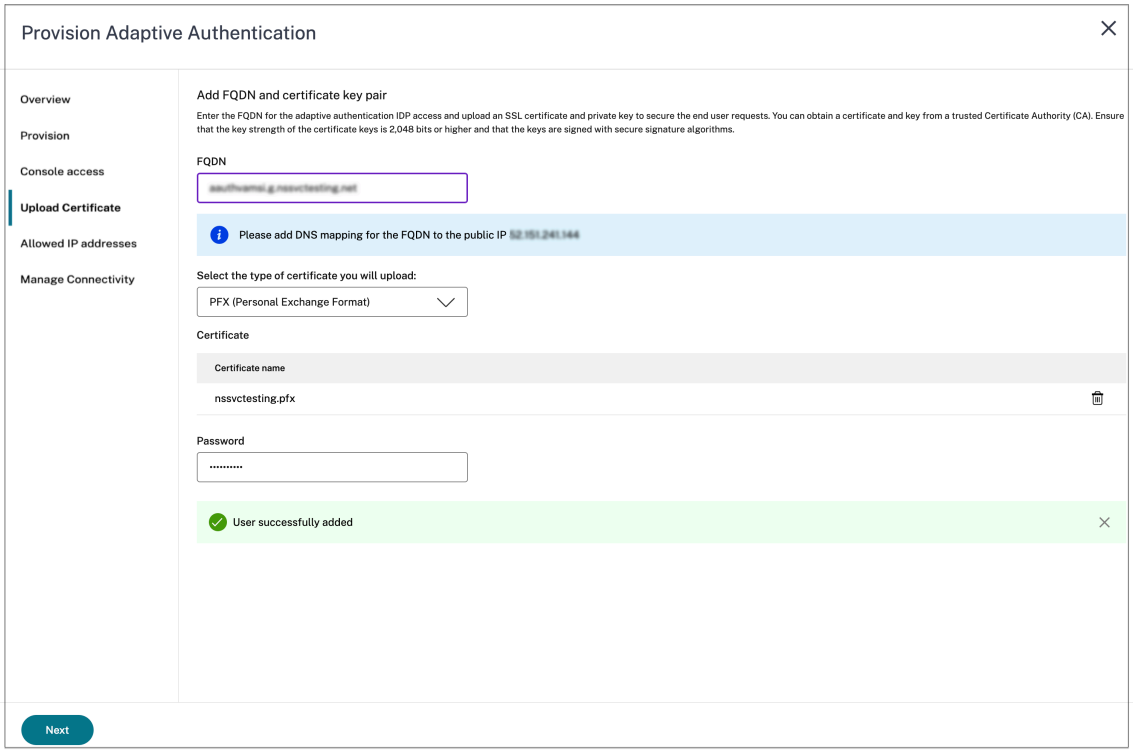
   c) Laden Sie das Zertifikat und den Schlüssel hoch.

> **Hinweis:**
>
> - Installieren Sie Ihr Zwischenzertifikat auf der Adaptive Authentication-Instanz und verknüpfen Sie es mit dem Serverzertifikat
>
> ```
> 1. Melden Sie sich bei der Adaptive Authentication-Instanz
>    1. Navigieren Sie zu **Traffic Management > SSL**.
> Einzelheiten finden Sie unter [Konfigurieren von
> ```



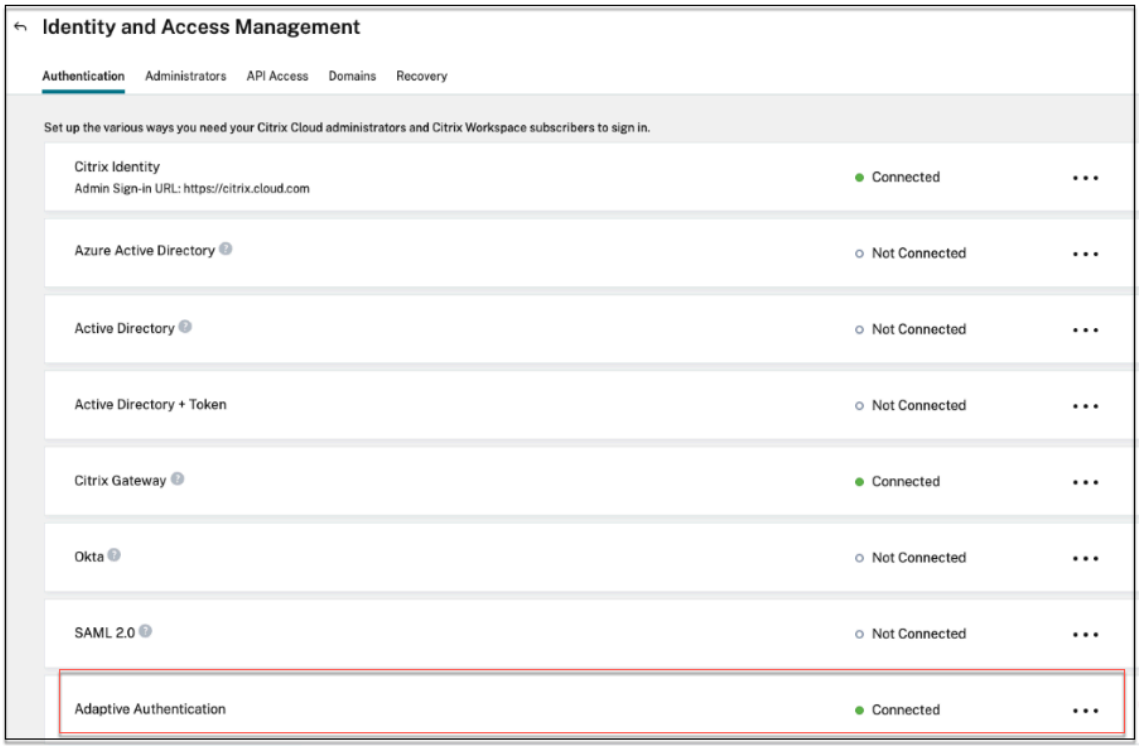
```
Zwischenzertifikaten](/en-us/citrix-gateway/current-
release/install-citrix-gateway/certificate-management-on
-citrix-gateway/configure-intermediate-certificate.html)
.
```

- Es werden nur öffentliche Zertifikate akzeptiert. Von privaten oder unbekannten Zertifizierungsstellen signierte Zertifikate werden nicht akzeptiert.
- Die Zertifikatkonfiguration oder Zertifikatsupdates dürfen nur über die Adaptive Authentication-Benutzeroberfläche durchgeführt werden. Ändern Sie es nicht direkt auf der Instanz, da dies zu Inkonsistenzen führen kann.



5. Laden Sie das Zertifikat und den Schlüssel hoch.

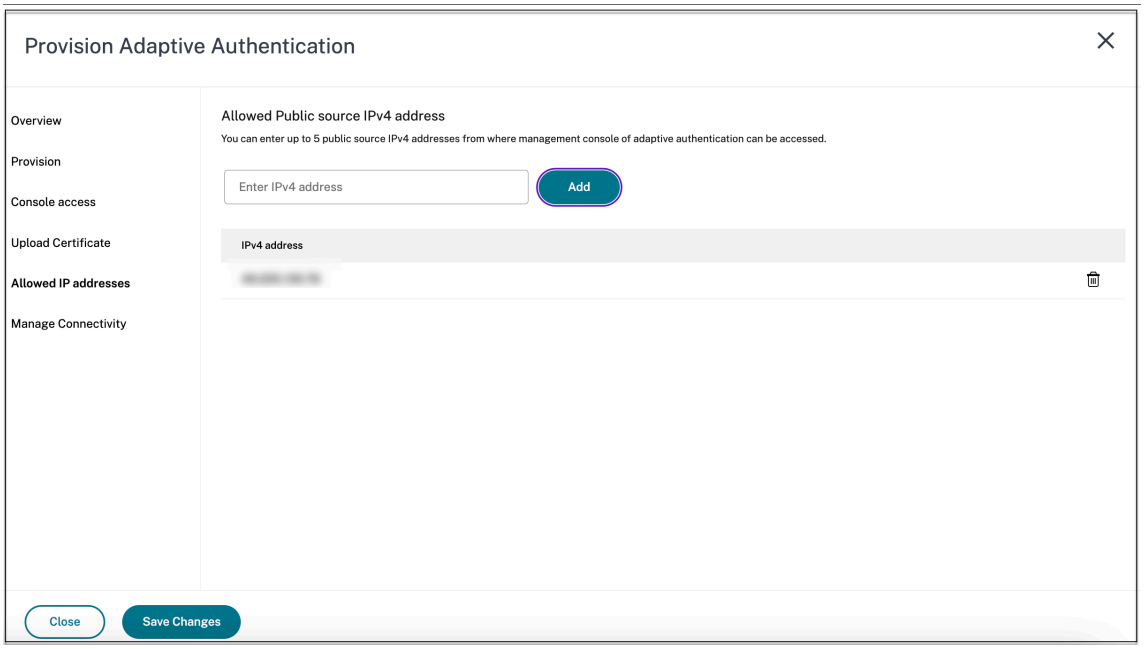
   Die Adaptive Authentication-Instanz ist jetzt mit dem Identity and Access Management-Dienst verbunden. Der Status der **adaptiven Authentifizierungsmethode** wird als **Verbunden**angezeigt.



6. Richten Sie eine IP-Adresse ein, über die auf die Managementkonsole für die Adaptive Authentifizierung zugegriffen werden kann.

    a) Geben Sie im Bildschirm **Zulässige IP-Adressen** für jede Instanz eine öffentliche IP-Adresse als Verwaltungs-IP-Adresse ein. Um den Zugriff auf die Management-IP-Adresse einzuschränken, können Sie mehrere IP-Adressen hinzufügen, die auf die Managementkonsole zugreifen dürfen.

    b) Um mehrere IP-Adressen hinzuzufügen, müssen Sie auf **Hinzufügen**klicken, die IP-Adresse eingeben und dann auf **Fertig**klicken. Dies muss für jede IP-Adresse erfolgen. Wenn Sie nicht auf die Schaltfläche **Fertig** klicken, werden die IP-Adressen nicht zur Datenbank hinzugefügt, sondern nur in der Benutzeroberfläche hinzugefügt.



7. Wenn Sie den Konnektivitätstyp Connector verwenden, geben Sie eine Reihe von Ressourcenstandorten (Connectors) an, über die AD- oder RADIUS-Server erreicht werden können. Wenn Sie den Konnektivitätstyp VNet-Peering verwenden, können Sie diesen Schritt überspringen.

   Admins können die Connectors auswählen, über die Backend-AD- und RADIUS-Server erreicht werden müssen. Um diese Funktion zu aktivieren, können Kunden eine Zuordnung zwischen ihren AD/RADIUS-Serversubnetzen im Back-End einrichten, sodass, wenn der Authentifizierungsverkehr unter ein bestimmtes Subnetz fällt, dieser Verkehr an den bestimmten Ressourcenstandort weitergeleitet wird. Wenn ein Ressourcenstandort jedoch keinem Subnetz zugeordnet ist, können Administratoren angeben, dass der Ressourcenstandort mit Platzhaltern für diese Subnetze verwendet werden soll.

   Bisher wurde der Adaptive Authentication-Verkehr für On-Premises-AD/RADIUS mit der Round-Robin-Methode an jeden verfügbaren Ressourcenstandort geleitet. Dies führte zu Problemen für Kunden mit mehreren Ressourcenstandorten.

   a) Klicken Sie auf der Benutzeroberfläche der adaptiven Authentifizierung auf **Konnektivität verwalten**.

   b) Geben Sie die Subnetzdetails ein und wählen Sie den entsprechenden Ressourcenstandort aus.

      > **Hinweis:**
      >
      > Wenn Sie das Kontrollkästchen **Alle verfügbaren Ressourcenstandorte für verbleibende Subnetze verwenden** deaktivieren, wird nur der an die konfigurierten Subnetze gerichtete Datenverkehr getunnelt.

c) Klicken Sie auf **Hinzufügen** und dann auf **Änderungen speichern**.

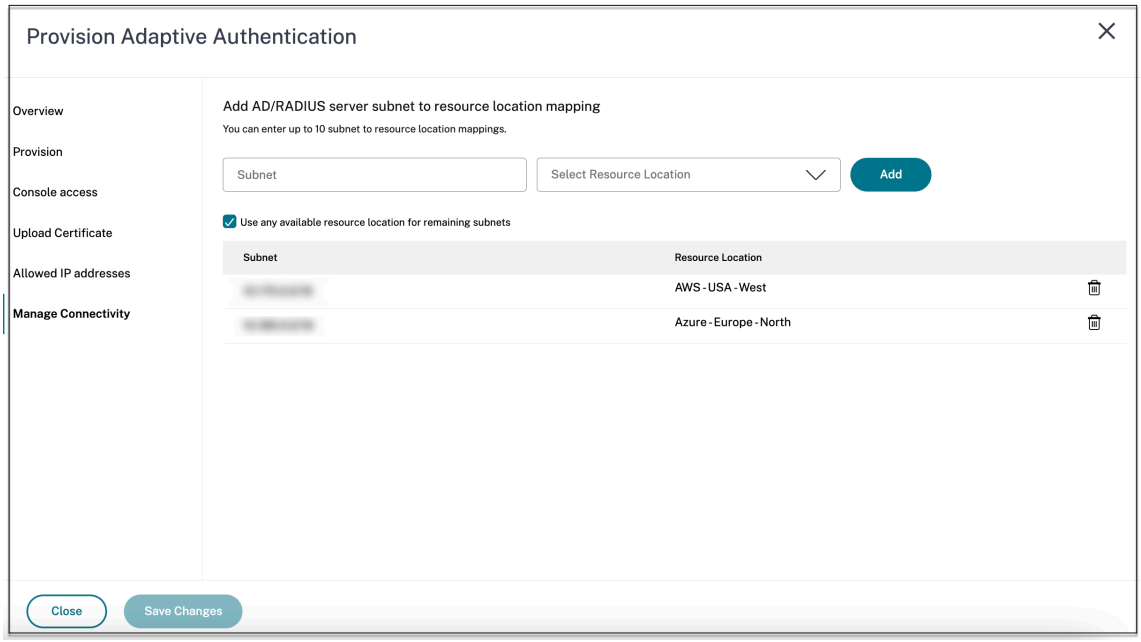
Hinweis:

- Nur RFC1918-IP-Adress-Subnetze sind zulässig.
- Die Anzahl der Subnetzressourcen-Standortzuordnungen pro Kunde ist auf 10 begrenzt.
- Einem Ressourcenstandort können mehrere Subnetze zugeordnet werden.
- Doppelte Einträge sind für dasselbe Subnetz nicht zulässig.
- Um den Subnetzeintrag zu aktualisieren, löschen Sie den vorhandenen Eintrag, und aktualisieren Sie dann.
- Wenn Sie den Ressourcenstandort umbenennen oder entfernen, stellen Sie sicher, dass Sie den Eintrag aus dem Bildschirm „ **Konnektivität verwalten** “der Benutzeroberfläche von Adaptive Authentication entfernen.
- Alle Änderungen, die mithilfe der folgenden CLI-Befehle an der Ressourcenstandortzuordnung vorgenommen wurden, werden durch die Änderungen überschrieben, die über die Benutzeroberfläche übertragen werden (**Adaptive Authentication Provisioning > Konnektivität verwalten**).

```
- set cloudtunnel parameter -subnetResourceLocationMappings


- set policy expression aauth_allow_rfc1918_subnets
   <>

- set policy expression aauth_listen_policy_exp <>
```

> Das Provisioning der adaptiven Authentifizierung ist jetzt abgeschlossen.

Schritt 2: Richtlinien für die adaptive Authentifizierung konfigurieren

So stellen Sie eine Verbindung zu Ihrer Adaptive Authentication-Instanz her:

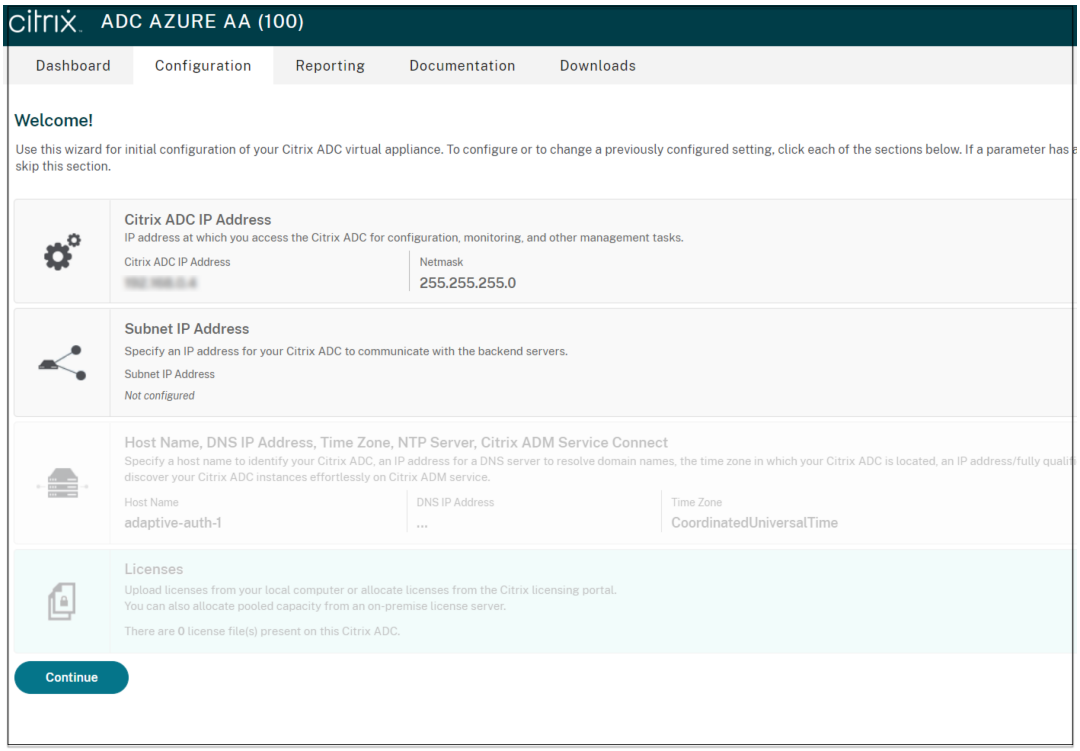
Nach der Bereitstellung können Sie direkt auf die Verwaltungs-IP-Adresse für Adaptive Authentication zugreifen. Sie können über den FQDN oder Ihre primäre IP-Adresse auf die Adaptive Authentication-Managementkonsole zugreifen.

> **Wichtig:**
>
> - In einem Hochverfügbarkeitssetup werden die Zertifikate im Rahmen des Synchronisationsprozesses ebenfalls synchronisiert. Stellen Sie also sicher, dass Sie das Wildcard-Zertifikat verwenden.
> - Wenn Sie für jeden Knoten ein eindeutiges Zertifikat benötigen, laden Sie die Zertifikatsdateien und Schlüssel in einen beliebigen Ordner hoch, der nicht synchronisiert wird (erstellen Sie beispielsweise einen separaten Ordner (nosync_cert) im Verzeichnis nsconfig/SSL) und laden Sie das Zertifikat dann einmalig auf jeden Knoten hoch.

Zugreifen auf die Verwaltungskonsole für die adaptive Authentifizierung:

- Informationen zum Zugriff auf die Adaptive Authentication-Managementkonsole über den FQDN finden Sie unter Konfigurieren von SSL für den ADC Admin-Benutzeroberflächenzugriff.
- Gehen Sie wie folgt vor, um mit Ihrer Primäradresse auf die adaptive Authentifizierung zuzugreifen:

1. Kopieren Sie die primäre IP-Adresse aus dem Abschnitt **Authentifizierungsrichtlinien konfigurieren** in der GUI und greifen Sie in Ihrem Browser auf die IP-Adresse zu.
2. Melden Sie sich mit den Anmeldeinformationen an, die Sie bei der Bereitstellung eingegeben haben.
3. Klicken Sie auf **Weiter**.



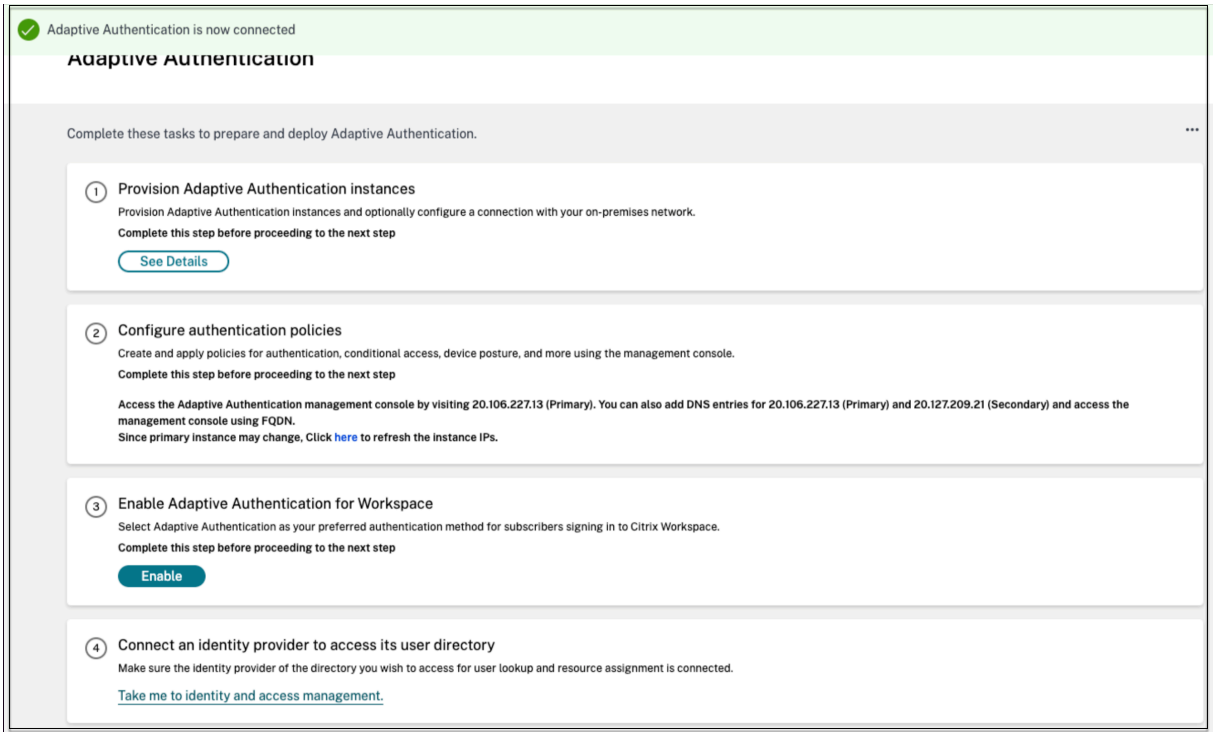
4. Navigieren Sie zu **Konfiguration > Sicherheit > AAA - Anwendungsverkehr > Virtuelle Server**.
5. Fügen Sie die Authentifizierungsrichtlinien hinzu. Für verschiedene Anwendungsfälle siehe Beispielauthentifizierungskonfigurationen.

> **Hinweis:**
>
> Der Zugriff auf die Adaptive Authentication-Instanz mithilfe der IP-Adresse ist nicht vertrauenswürdig und viele Browser blockieren den Zugriff mit Warnungen. Wir empfehlen, dass Sie mit FQDN auf die Adaptive Authentication-Managementkonsole zugreifen, um Sicherheitsbarrieren zu vermeiden. Sie müssen den FQDN für die Verwaltungskonsole für Adaptive Authentication reservieren und ihn der primären und sekundären Management-IP-Adresse zuordnen.
>
> Wenn Ihre Adaptive Authentication-Instanz beispielsweise die IP-Adresse 192.0.2.0 und die sekundäre IP-Adresse 192.2.2.2 lautet, dann
>
> - primary.domain.com kann 192.0.2.0 zugeordnet werden

- secondary.domain.com kann 192.2.2.2 zugeordnet werden

Schritt 3: Adaptive Authentifizierung für Workspace aktivieren

Nach Abschluss der Bereitstellung können Sie die Authentifizierung für Workspace aktivieren, indem Sie im Abschnitt **Adaptive Authentifizierung für Workspace aktivieren** auf **Aktivieren** klicken.



Hinweis:

Damit ist die Konfiguration der adaptiven Authentifizierung abgeschlossen. Wenn Sie auf Ihre Workspace-URL zugreifen, müssen Sie zum FQDN für adaptive Authentifizierung umgeleitet werden.

Verwandte Referenzen

- FQDN bearbeiten
- Upgrade Ihrer Adaptive Authentication-Instanzen planen
- Provisioning Ihrer Adaptive Authentication-Instanzen aufheben
- Sicheren Zugriff auf das Gateway aktivieren
- Mit Azure VNet-Peering Konnektivität zu lokalen Authentifizierungsservern einrichten
- Benutzerdefinierte Workspace-URL oder Vanity-URL
- Backup und Wiederherstellung der Konfiguration
- Beispiel für eine LDAPS-Konfiguration mit Lastausgleich

- Authentifizierungsmethode auf Adaptiven Authentifizierung migrieren
- Beispielkonfigurationen zur Authentifizierung

Verwandte Konfigurationen der adaptiven Authentifizierung

June 19, 2024

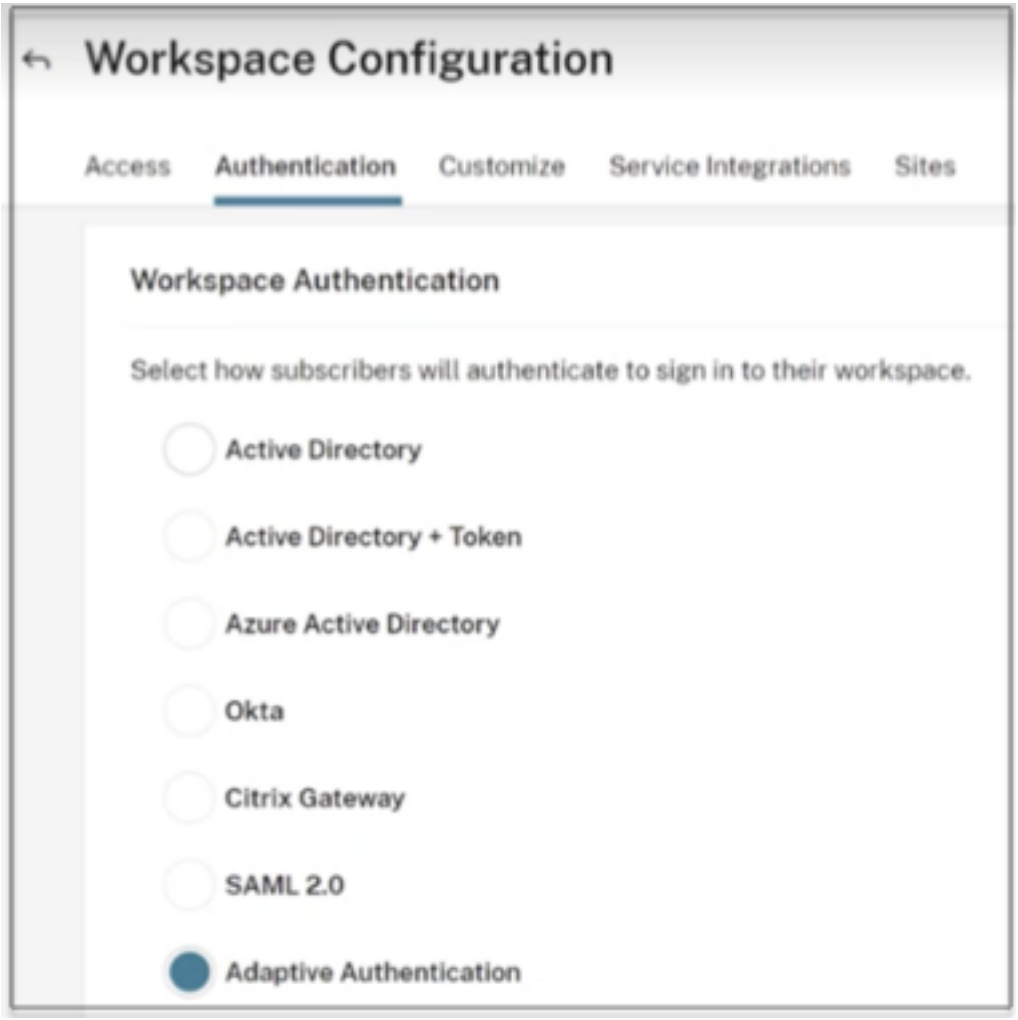
FQDN bearbeiten

Sie können einen FQDN nicht bearbeiten, wenn **Adaptive Authentication** als Authentifizierungsmethode in der Workspace-Konfiguration ausgewählt ist. Sie müssen zu einer anderen Authentifizierungsmethode wechseln, um den FQDN zu bearbeiten. Sie können das Zertifikat jedoch bei Bedarf bearbeiten.

> **Wichtig:**
>
> - Stellen Sie vor dem Ändern des FQDN sicher, dass der neue FQDN der öffentlichen IP-Adresse des virtuellen IdP-Servers zugeordnet ist.
> - Bestehende Benutzer, die mithilfe von OAuth-Richtlinien mit **NetScaler Gateway** verbunden sind, müssen Ihre Authentifizierungsmethode auf **Adaptive Authentication** migrieren. Einzelheiten finden Sie unter Migrieren Ihrer Authentifizierungsmethode zu Adaptive Authentication.

Gehen Sie wie folgt vor, um einen FQDN zu bearbeiten:

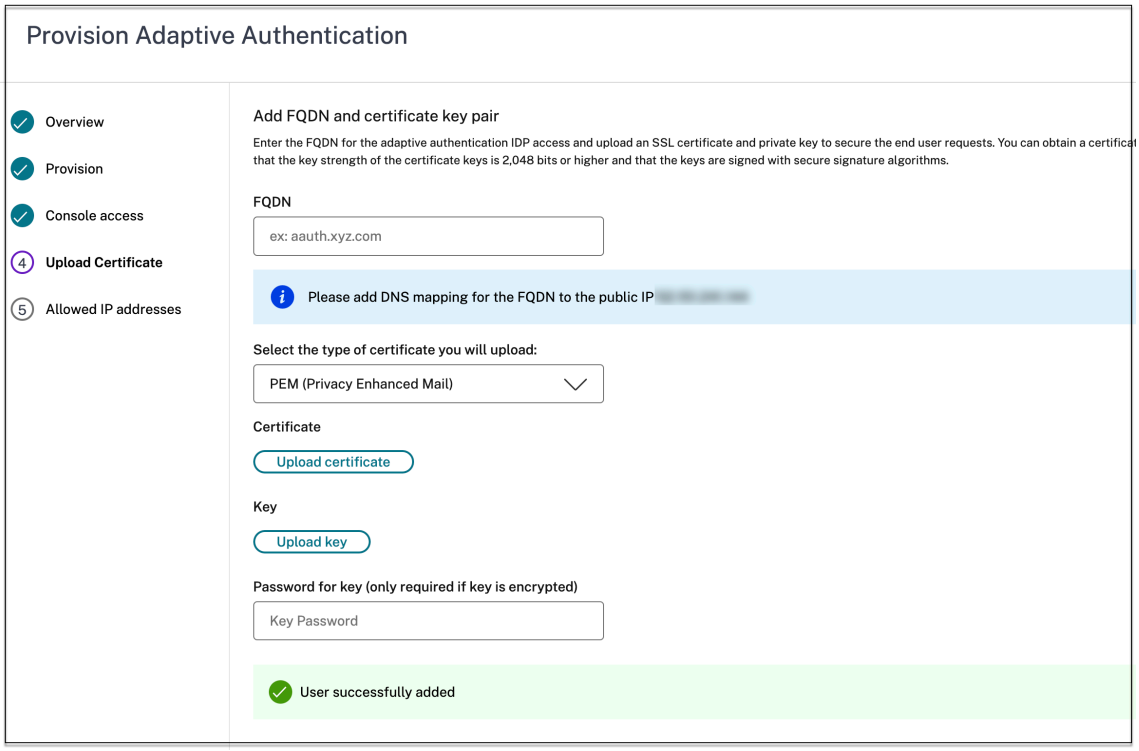
1. Wechseln Sie zu einer anderen Authentifizierungsmethode als **Adaptive Authentication**.



2. Wählen Sie **Ich verstehe die Auswirkungen auf das Abonnentenerlebnis aus,** und klicken Sie dann auf **Bestätigen** .

   Wenn Sie auf **Bestätigen** klicken, wirkt sich dies auf die Workspace-Anmeldung bei Endbenutzern aus und die adaptive Authentifizierung wird erst dann für die Authentifizierung verwendet, wenn Adaptive Authentication Daher wird empfohlen, den FQDN während eines Wartungsfensters zu ändern.

3. Ändern Sie im Fenster **Zertifikat hochladen** den FQDN.



4. Klicken Sie auf **Änderungen speichern**.

> **Wichtig:**
>
> Wenn Sie einen FQDN bearbeiten, müssen Sie das Zertifikat auch erneut hochladen.

5. Aktivieren Sie die Methode Adaptive Authentication erneut, indem Sie auf der Homepage der adaptiven Authentifizierung auf **Aktivieren** (Schritt 3) klicken

6. Klicken Sie auf **Aktualisieren**.

Benutzerdefinierte Workspace-URL oder Vanity-URL

Mit einer benutzerdefinierten Workspace-URL können Sie eine Domain Ihrer Wahl verwenden, um auf Ihren Citrix Workspace Store zuzugreifen. Benutzer können über die standardmäßige Workspace-URL oder die benutzerdefinierte Workspace-URL oder beides auf Workspace zugreifen.

Um eine benutzerdefinierte Workspace-URL oder Vanity-URL zu konfigurieren, müssen Sie wie folgt vorgehen:

1. Konfigurieren Sie Ihre benutzerdefinierte Domain. Einzelheiten finden Sie unter Konfiguration Ihrer benutzerdefinierten Domain.
2. Konfigurieren Sie ein neues OAuthIdp-Profil mit derselben Client-ID, demselben Geheimnis und derselben Zielgruppe wie Ihr aktuelles oder Standardprofil (AAuthAutoConfig_OAuthIdpProf), aber mit einer anderen Umleitungs-URL. Einzelheiten finden Sie unter Konfiguration von OAuth-Richtlinien und-Profilen.

   Beispiel:

   Aktuelles Profil:

   ```
   -add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf
    -clientID xxxx -clientSecret yyyy -encrypted -encryptmethod
   ENCMTHD_3 -kek -suffix 2023_07_09_20_09_30 -redirectURL "https
   ://accounts-internal.cloud.com/core/login-cip"-audience zzzz -
   sendPassword ON

   add authentication OAuthIdPPolicy AAuthAutoConfig_oauthIdpPol -
   rule true -action AAuthAutoConfig_oauthIdpProf

   bind authentication vserver auth_vs -policy AAuthAutoConfig_oauthIdpPol
    -priority 100 -gotoPriorityExpression NEXT
   ```

   Neues Profil:

   ```
   add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf_Custom1
    -clientID xxxx -clientSecret yyyy -encrypted -encryptmethod
   ENCMTHD_3 -kek -suffix 2023_07_09_20_09_30 -redirectURL "https://
   custom_domain/core/login-cip"-audience zzzz -sendPassword ON

   add authentication OAuthIdPPolicy AAuthAutoConfig_oauthIdpPol_Custom1
    -rule true -action AAuthAutoConfig_oauthIdpProf_Custom1

   bind authentication vserver auth_vs -policy AAuthAutoConfig_oauthIdpPol_Cu
    -priority 101 -gotoPriorityExpression NEXT
   ```

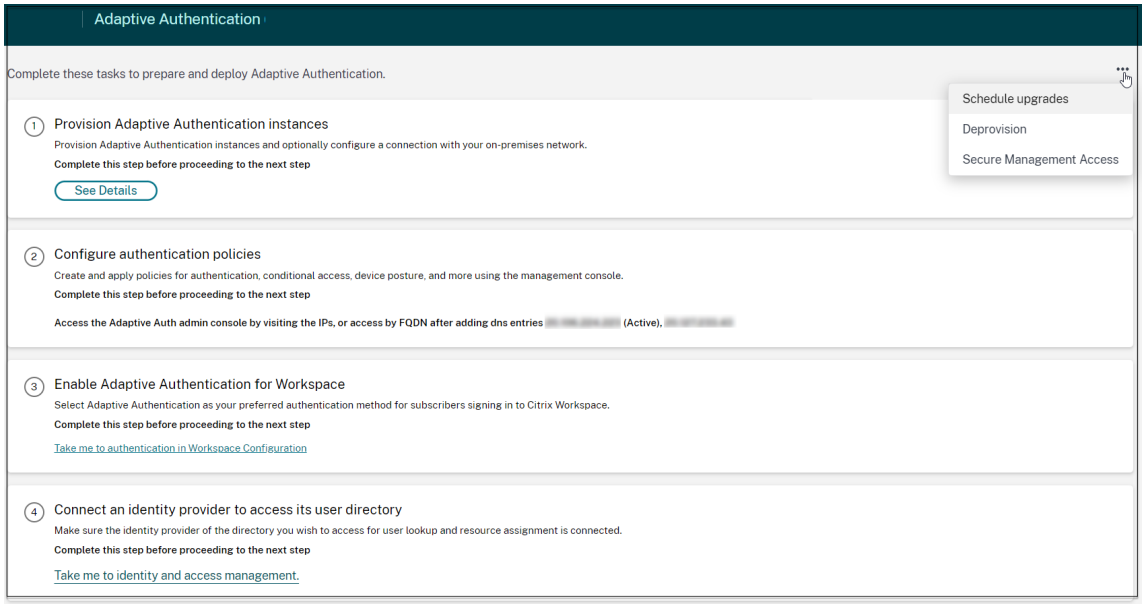
> **Wichtig:**
>
> - Die OAuth-Richtlinie und das Profil werden vom Adaptive Authentication Service während der Bereitstellungsphase erstellt. Daher hat der Citrix Cloud-Administrator keinen Zugriff auf das unverschlüsselte Client-Geheimnis. Sie können das verschlüsselte Geheimnis aus der Datei ns.conf abrufen. Um ein OAuth-Profil zu erstellen, müssen Sie das verschlüsselte Geheimnis verwenden und das Profil nur mit den CLI-Befehlen erstellen.
> - Sie können kein OAuth-Profil mit der NetScaler-Benutzeroberfläche erstellen.

Upgrade Ihrer Adaptive Authentication-Instanzen planen

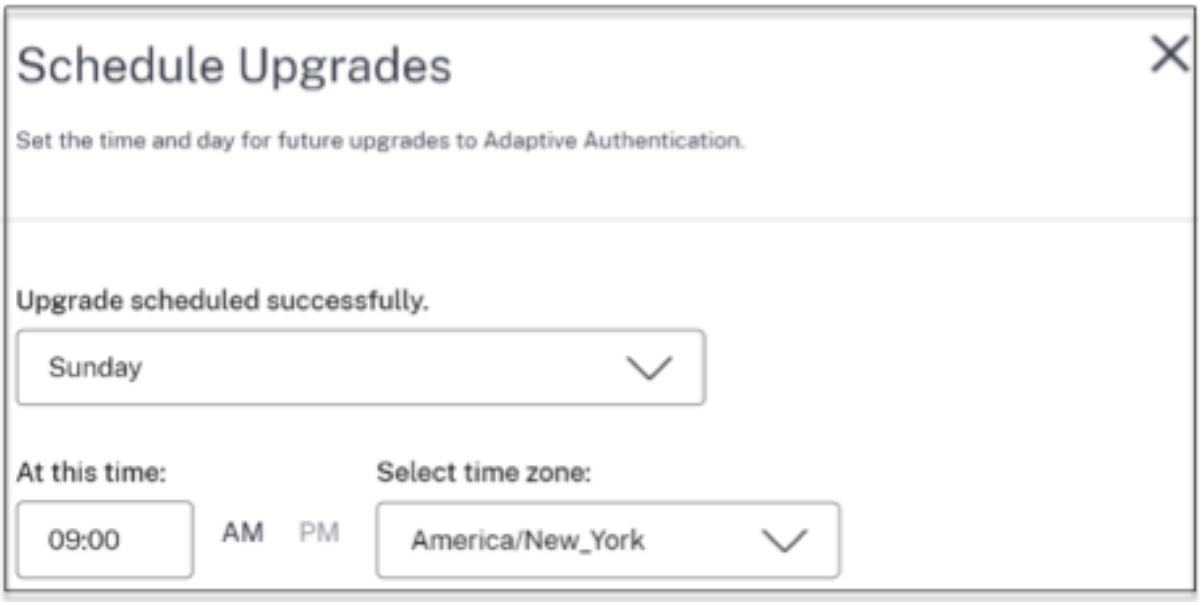
Für die aktuelle Site oder Bereitstellung können Sie das Wartungsfenster für das Upgrade auswählen.

> **Wichtig:**
>
> Aktualisieren Sie die Adaptive Authentication-Instanzen nicht auf zufällige RTM-Builds. Alle Upgrades werden von Citrix Cloud verwaltet.

1. Klicken Sie auf der Benutzeroberfläche der **adaptiven Authentifizierung** im Abschnitt **Adaptive Authentication-Instanzen bereitstellen** auf die Schaltfläche mit den Auslassungspunkten.



2. Klicken Sie auf **Upgrades planen**.
3. Wählen Sie den Tag und die Uhrzeit für das Upgrade aus.



Provisioning Ihrer Adaptive Authentication-Instanzen aufheben

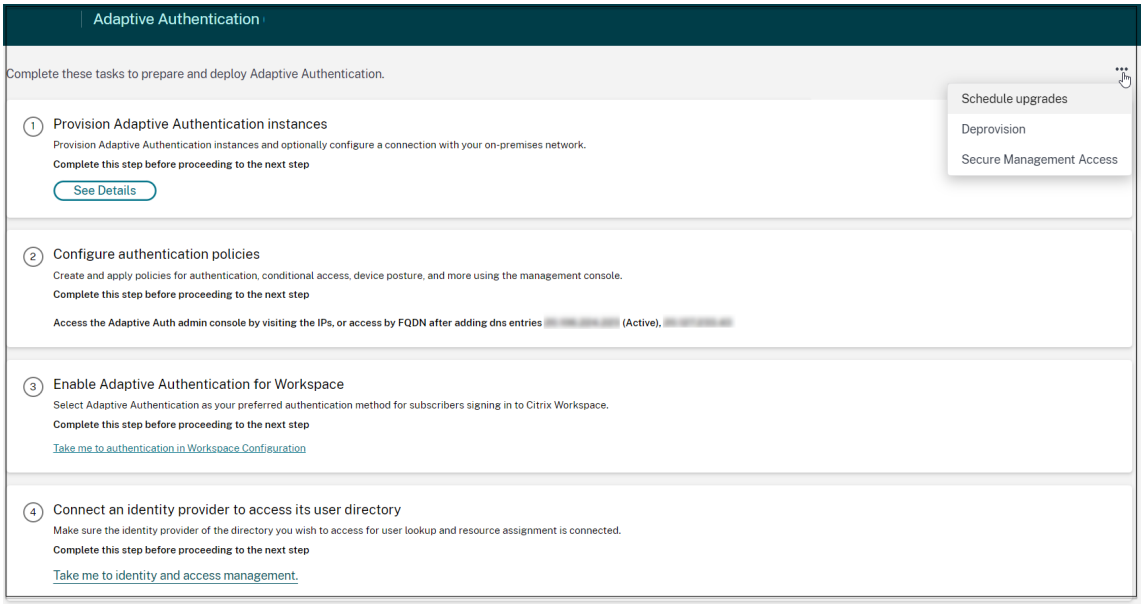
Kunden können die Adaptive Authentication-Instanzen in den folgenden Fällen und gemäß dem Vorschlag des Citrix-Supports deaktivieren.

- Auf die Instanzen der adaptiven Authentifizierung kann nicht zugegriffen werden (insbesondere nach einem geplanten Upgrade), obwohl dieses Szenario möglicherweise nicht auftritt.
- Wenn der Kunde vom VNet-Peering-Modus in den Connector-Modus oder umgekehrt wechseln muss.
- Wenn der Kunde zum Zeitpunkt der Bereitstellung des VNet-Peering-Modus ein falsches Subnetz ausgewählt hat (das Subnetz steht in Konflikt mit anderen Subnetzen in seinem Rechenzentrum oder Azure VNet).

> **Hinweis:**
>
> Beim Deprovisioning wird auch das Konfigurationsbackup der Instanzen gelöscht. Daher müssen Sie die Backupdateien herunterladen und speichern, bevor Sie die Bereitstellung Ihrer Adaptive Authentication-Instanzen aufheben.

Führen Sie Folgendes aus, um die Bereitstellung einer Adaptive Authentication-Instanz

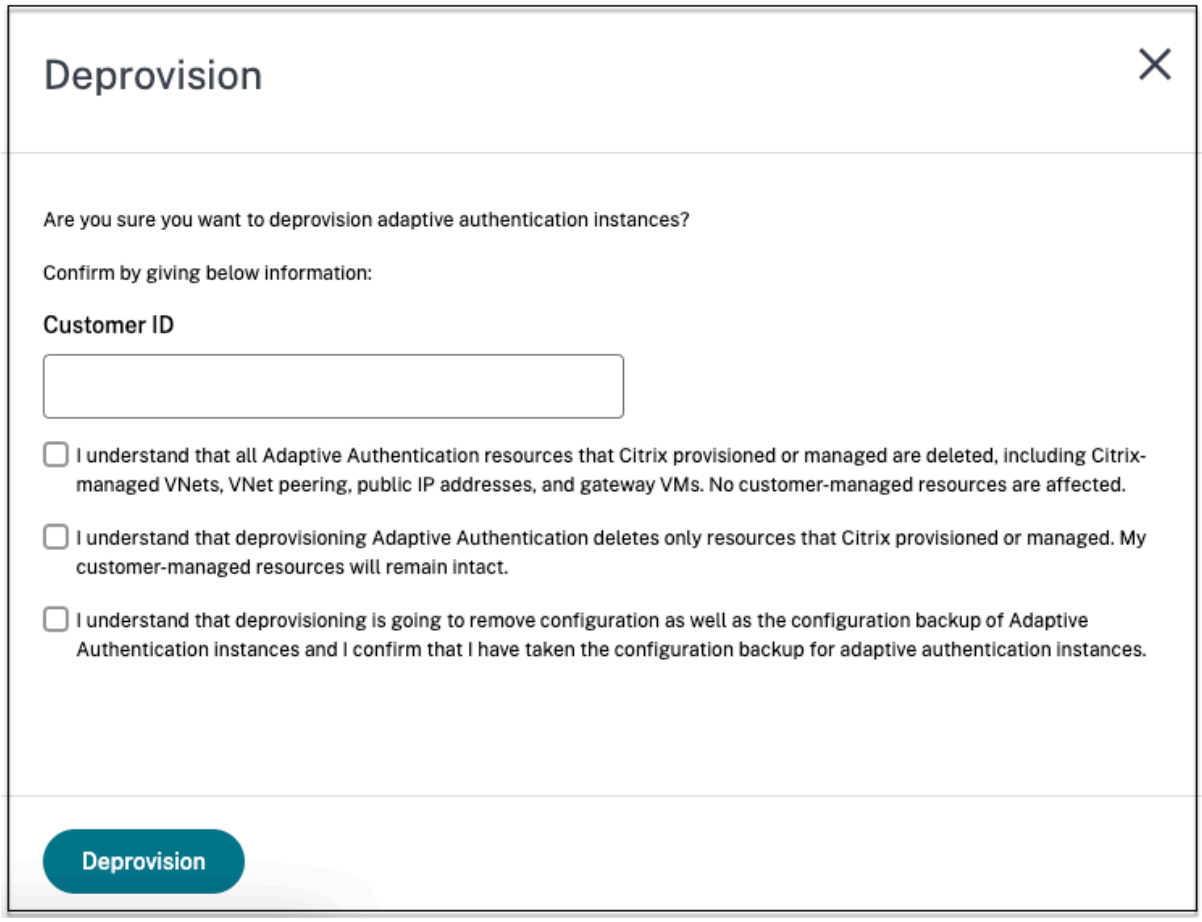
1. Klicken Sie auf der Benutzeroberfläche der **adaptiven Authentifizierung** im Abschnitt **Adaptive Authentication-Instanzen bereitstellen** auf die Schaltfläche mit den Auslassungspunkten.



2. Klicken Sie auf **Deprovision**.

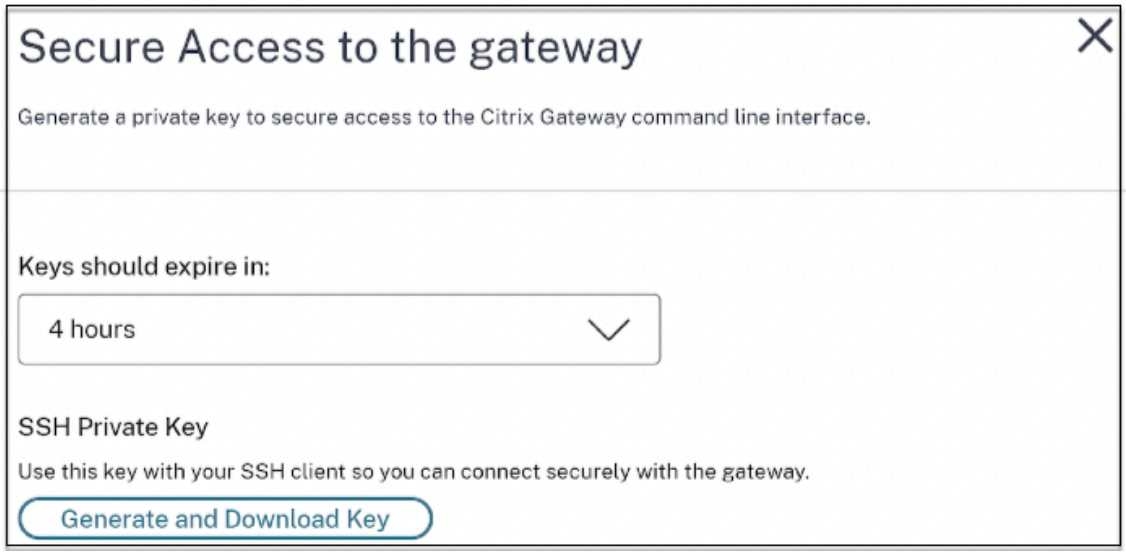
> **Hinweis:**
>
> Vor dem Aufheben der Bereitstellung müssen Sie **NetScaler Gateway** von der Workspace-Konfiguration trennen.

3. Geben Sie die Kunden-ID ein, um die Bereitstellung der Instanzen für Adaptive



Sicheren Zugriff auf das Gateway aktivieren

1. Klicken Sie auf der Benutzeroberfläche der **adaptiven Authentifizierung** im Abschnitt **Adaptive Authentication-Instanzen bereitstellen** auf die Schaltfläche mit den Auslassungspunkten.
2. Klicken Sie auf **Secure Management Access**.



3. Wählen Sie unter **Schlüssel sollten ablaufen in** eine Ablaufdauer für den neuen SSH-Schlüssel aus.
4. Klicken Sie auf **Schlüssel generieren und herunterladen**.
   Kopieren Sie den privaten SSH-Schlüssel oder laden Sie ihn zur späteren Verwendung herunter, da er nach dem Schließen der Seite nicht angezeigt wird. Dieser Schlüssel kann verwendet werden, um sich mit dem Benutzernamen bei den Adaptive Authentication-Instanzen anzumelden `authadmin`.

   Sie können auf **Schlüssel generieren und herunterladen** klicken, um ein neues Schlüsselpaar zu erstellen, falls das frühere Schlüsselpaar abläuft. Es kann jedoch nur ein Schlüsselpaar aktiv sein.
5. Klicken Sie auf **Fertig**.

Wichtig:

- Wenn Sie PuTTY unter Windows verwenden, um eine Verbindung zu Adaptive Authentication-Instanzen herzustellen, müssen Sie den heruntergeladenen privaten Schlüssel in PEM konvertieren. Einzelheiten finden Sie unter https://www.puttygen.com/convert-pem-to-ppk.
- Es wird empfohlen, den folgenden Befehl zu verwenden, um über das Terminal über den MAC oder die PowerShell/Eingabeaufforderung von Windows (Version 10) eine Verbindung zu den Instanzen der adaptiven Authentifizierung herzustellen.
  `ssh -i <path-to-private-key> authadmin@<ip address of ADC>`
- Wenn Sie möchten, dass die AD-Benutzer auf die GUI für Adaptive Authentication zugreifen können, müssen Sie sie als neue Administratoren zur LDAP-Gruppe hinzufügen. Einzelheiten finden Sie unter https://support.citrix.com/article/CTX123782.
  Für alle anderen Konfigurationen empfiehlt Citrix, dass Sie die GUI für Adaptive Authenti-

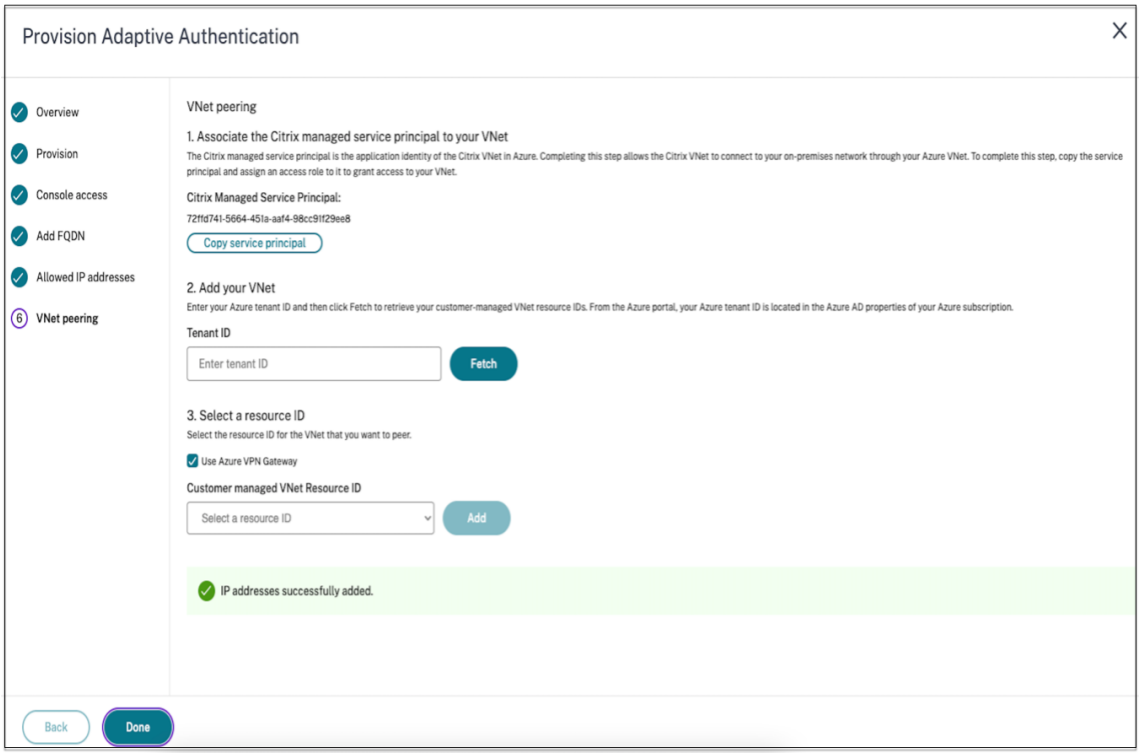
> cation und nicht die CLI-Befehle verwenden.

Mit Azure VNet-Peering Konnektivität zu lokalen Authentifizierungsservern einrichten

Sie müssen diese Konfiguration nur einrichten, wenn Sie den Konnektivitätstyp als Azure VNet-Peering ausgewählt haben.

> **Hinweis:**
>
> Wenn Sie Drittanbieter-IDPs wie Okta, Azure AD, Ping verwenden, ist dieser Schritt nicht erforderlich.

1. Klicken Sie auf der Benutzeroberfläche von Connect Adaptive Authentication auf **Provision**und dann auf **Azure VNet Peering**.



Das Feld **Citrix Managed Service Principal** enthält die Anwendungs-ID eines Azure Service Principal, der von Citrix für Ihren Kunden erstellt wurde. Dieser Dienstprinzipal ist erforderlich, damit Citrix ein VNet-Peering zu einem VNet in Ihrem Abonnement und Mandanten hinzufügen kann.

Damit sich dieser Dienstprinzipal beim Kundenmandanten anmelden kann, muss der Administrator am Kundenstandort (globaler Administrator des Mandanten) die folgenden PowerShell-Befehle ausführen, um den SPN zum Mandanten hinzuzufügen. CloudShell kann auch verwendet werden.

```
Connect-AzureAD
```



```
New-AzureADServicePrincipal -AppId $App_ID
```

Dabei ist `$App_ID` eine SPN-Anwendungs-ID, die von Citrix mitgeteilt wurde.

> **Hinweis:**
>
> - Der zuvor erwähnte Befehl gibt einen Dienstprinzipalnamen aus, der für die Rollenzuweisungen verwendet werden muss.
> - Damit dieser Dienstprinzipal ein Azure VNet-Peering hinzufügen kann, muss der Administrator am Kundenstandort (nicht auf globale Administratoren beschränkt) dem VNet eine Rolle "Network Contributor"hinzufügen, die mit dem Citrix Managed VNet verknüpft sein muss.
> - SPN ist eine eindeutige Kennung, die verwendet wird, um das virtuelle Citrix-Netzwerk in Azure zuzuordnen. Durch die Verknüpfung des SPN mit VNet kann das virtuelle Citrix Netzwerk über das VNet von Azure eine Verbindung mit on-premises Netzwerk des Kunden herstellen.

2. Erstellen Sie ein VNet-Peering.

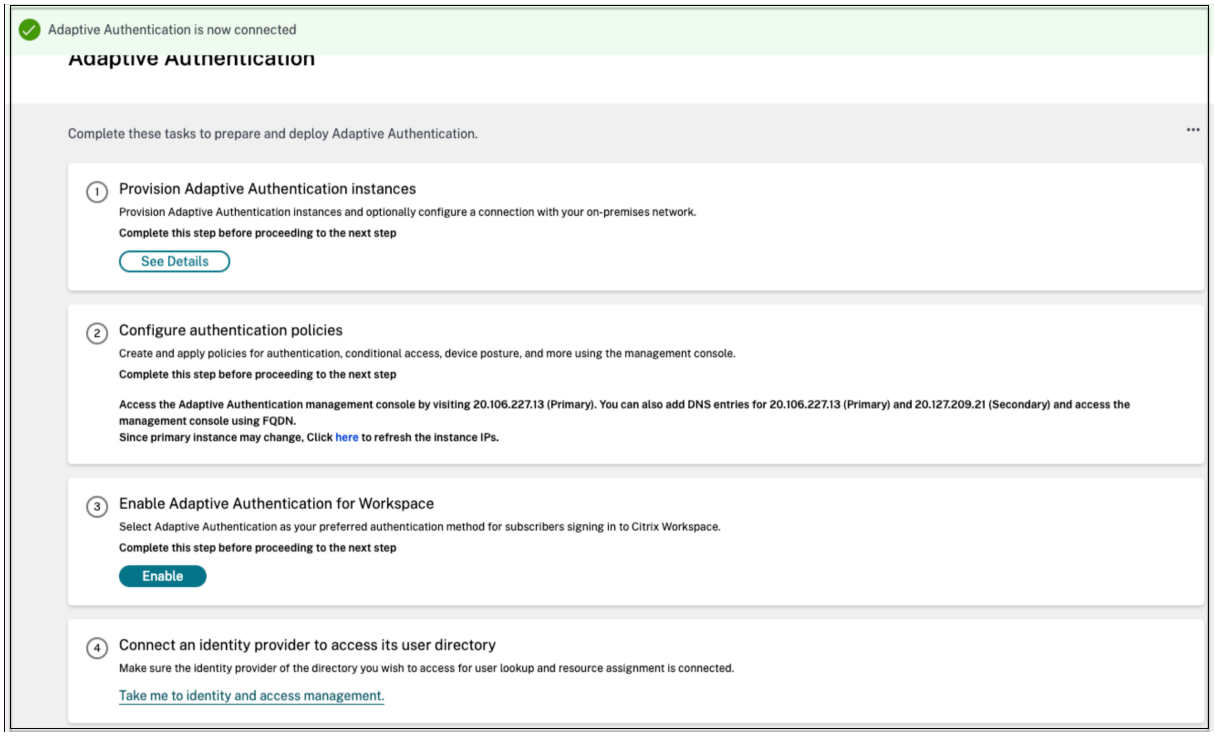
   - Geben Sie die Mandant-ID ein, für die die vorherigen Schritte ausgeführt wurden, und klicken Sie auf **Abrufen**.

   Dadurch wird die vom Kunden verwaltete VNet-Ressourcen-ID mit den möglichen VNets aufgefüllt, für die die Netzwerkbeitragsrolle für den SPN hinzugefügt wird. Wenn Sie Ihr VNet nicht sehen, stellen Sie sicher, dass die vorherigen Schritte korrekt ausgeführt wurden, oder wiederholen Sie die Schritte.

   > **Hinweis:**
   >
   > Einzelheiten zum Auffinden Ihrer Mandanten-ID finden Sie unter https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-to-find-tenant.

3. Wählen Sie **Azure VPN Gateway verwenden**, um Ihre on-premises Netzwerke mit Azure zu verbinden.
4. Wählen Sie **unter Customer managed VNet Resource ID**das für Peering identifizierte VNet aus und klicken Sie auf **Hinzufügen**.
   Das VNet wird der Tabelle mit dem anfänglichen Status **In Bearbeitung**hinzugefügt. Sobald das Peering erfolgreich abgeschlossen wurde, ändert sich der Status in **Fertig**.
5. Klicken Sie auf **Fertig**.
6. Fahren Sie mit der Konfiguration fort, siehe Schritt 1: Bereitstellen der adaptiven Authentifizierung.

> **Wichtig:**
>
> - Damit der Datenverkehr zwischen dem von Citrix verwalteten VNet und dem lokalen Netzwerk fließen kann, können die Firewall- und Routing-Regeln on-premises geändert werden, um den Datenverkehr an das Citrix Managed VNet zu leiten.
> - Sie können jeweils nur einen VNet-Peer hinzufügen. Mehrere VNet-Peerings sind derzeit nicht zulässig. Sie können ein VNet-Peering löschen oder nach Bedarf erstellen.



Backup und Wiederherstellung der Konfiguration

Der Application Delivery Management Service führt die Backupverwaltung für die Adaptive Authentication-Instanzen Einzelheiten finden Sie unter Backup und Wiederherstellen von NetScaler-Instanzen.

1. Klicken Sie auf der Kachel Application Delivery Management auf **Verwalten** .
2. Navigieren Sie zu **Infrastruktur > Instanzen** und greifen Sie auf die Backups zu.

> **Hinweis:**
>
> Wenn der Service nicht integriert ist, integrieren Sie den Application Delivery Management Service. Einzelheiten finden Sie unter Erste Schritte.

Beispiel für eine LDAP- und LDAPS-Load-Balancing-Konfiguration

Die Citrix Adaptive Authentication-Instanz bietet LDAP/LDAPS-Unterstützung über einen virtuellen Lastausgleichsserver.

> **Hinweis:**
>
> - Wenn Sie keinen Load Balancing für LDAP/LDAPS verwenden, vermeiden Sie es, einen Dienst oder Server für einen LDAP-Server zu erstellen, da dies den adaptiven Authentifizierungstunnel beschädigen könnte.
> - Wenn Sie Load Balancing für LDAP verwenden, erstellen Sie eine Dienstgruppe und binden Sie sie an den Lastausgleichsdienst und nicht an einen eigenständigen Dienst.
> - Wenn Sie den virtuellen Lastausgleichsserver für die Authentifizierung verwenden, stellen Sie sicher, dass Sie in der LDAP-Aktion die IP-Adresse des virtuellen Lastausgleichsservers anstelle der tatsächlichen IP-Adresse des LDAP-Servers hinzufügen.
> - Standardmäßig ist ein TCP-Monitor an den Dienst gebunden, den Sie erstellen. Auf den NetScaler-Instanzen von Adaptive Authentication ist der Dienst standardmäßig als AKTIV markiert, wenn ein TCP-Monitor verwendet wird.
> - Für die Überwachung wird empfohlen, benutzerdefinierte Monitore zu verwenden.

Voraussetzungen

Private IP-Adresse (RFC1918-Adresse) des virtuellen Load-Balancing-Servers. Es kann sich um eine Schein-IP-Adresse handeln, da diese Adresse für die interne Konfiguration verwendet wird.

LDAP-Server mit Lastausgleich

Erstellen Sie für LDAP-Server mit Lastausgleich eine Dienstgruppe und binden Sie sie an den virtuellen Lastausgleichsserver. Erstellen Sie keinen Dienst für den Lastausgleich von LDAP-Servern.

Konfigurieren Sie LDAP mithilfe der NetScaler-CLI:

Sie können die folgenden CLI-Befehle als Referenz für die Konfiguration von LDAP verwenden.

1. `add serviceGroup <serviceGroupName> <serviceType>`
2. `bind servicegroup <serviceGroupName> (<IP> | <serverName>)<port>`
3. `add lb vserver <name> <serviceType> <ip> <port>` - Der Port muss 389 sein. Dieser Port wird für die interne Kommunikation verwendet und die Verbindung zu einem on-premises Server erfolgt über SSL, basierend auf dem für die Dienstgruppe konfigurierten Port.
4. `bind lb vserver <name> <serviceGroupName>`
5. `add authentication ldapAction <name> { -serverIP } <ip_addr> | { -serverName <string> } } <lb vserver ip>`

6. `add authentication policy <ldap_policy_name> -rule <expression> -action <string>`
7. `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority <ldap_policy_priority> -gotoPriorityExpression NEXT`

Konfigurieren Sie LDAP mithilfe der NetScaler-GUI:

1. Navigieren Sie zu **Traffic Management > Load Balancing** und klicken Sie dann auf **Virtuelle Server**.
2. Erstellen Sie einen virtuellen Server vom Typ TCP und Port 389.

   Erstellen Sie keinen virtuellen Lastausgleichsserver vom Typ SSL/SSL_TCP.
3. Navigieren Sie zu **Traffic Management > Load Balancing** und klicken Sie dann auf **Service Groups**.
4. Erstellen Sie eine Dienstgruppe vom Typ TCP und Port 389.
5. Binden Sie die Dienstgruppe an den virtuellen Server, den Sie in Schritt 1 erstellt haben.

Einzelheiten zu den Verfahren finden Sie unter Grundlegendes Load-Balancing einrichten.

LDAPS-Server mit Lastausgleich

Für LDAPS-Server mit Lastausgleich müssen Sie einen virtuellen Lastausgleichsserver vom Typ TCP erstellen, um eine interne SSL-Verschlüsselung oder -Entschlüsselung in der Adaptive Authentication-Instanz zu vermeiden. Der virtuelle Load-Balancing-Server übernimmt in diesem Fall die TLS-Verschlüsselung/Entschlüsselung. Erstellen Sie keinen virtuellen Lastausgleichsserver vom Typ SSL.

Konfigurieren Sie LDAPS mithilfe der NetScaler-CLI:

Sie können die folgenden CLI-Befehle als Referenz für die Konfiguration von LDAPS verwenden.

1. `add lb vserver <name> <serviceType> <ip> <port>` - Der Port muss 636 sein.
2. `bind lb vserver <name> <serviceGroupName>`
3. `add authentication ldapAction <name> { -serverIP } <ip_addr> | { -serverName <string> } } <lb vserver ip>`
4. `add authentication policy <ldap_policy_name> -rule <expression> -action <string>`
5. `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority <ldap_policy_priority> -gotoPriorityExpression NEXT`

Konfigurieren Sie LDAPS mithilfe der NetScaler-GUI:

1. Navigieren Sie zu **Traffic Management > Load Balancing** und klicken Sie dann auf **Virtuelle Server**.
2. Erstellen Sie einen virtuellen Server vom Typ TCP und Port 636.

   Erstellen Sie keinen virtuellen Lastausgleichsserver vom Typ SSL/SSL_TCP.
3. Navigieren Sie zu **Traffic Management > Load Balancing** und klicken Sie dann auf **Service**.
4. Erstellen Sie einen Dienst vom Typ SSL_TCP und Port 636.
5. Binden Sie den Dienst an den virtuellen Server, den Sie in Schritt 1 erstellt haben.

Einzelheiten zu den Verfahren finden Sie unter Grundlegendes Load-Balancing einrichten.

Erstellen Sie benutzerdefinierte Monitore

Erstellen Sie benutzerdefinierte Monitore mithilfe der NetScaler-GUI:

1. Navigieren Sie zu **Traffic Management > Load Balancing > Monitore** .
2. Erstellen Sie einen Monitor vom Typ LDAP. Stellen Sie sicher, dass Sie das Monitortastintervall auf 15 Sekunden und das Reaktionszeitlimit auf 10 Sekunden einstellen.
3. Binden Sie diesen Monitor an Ihren Dienst.

Weitere Informationen finden Sie unter Benutzerdefinierte Monitore.

Möglichkeit, bis zu 15 Admin-IP-Adressen hinzuzufügen

Mit dem Adaptive Authentication-Dienst können Sie bis zu 15 öffentliche IP-Subnetze und einzelne IP-Adressen eingeben, um auf die Adaptive Authentication-Verwaltungskonsole zuzugreifen.

Hinweise, die Sie bei der Eingabe der IP-Adressen/Subnetze beachten sollten:

- Stellen Sie sicher, dass die CIDRs der öffentlichen IP-Subnetze zwischen /20 und /32.B liegen.
- Stellen Sie sicher, dass sich die Einträge nicht überschneiden.

Beispiele:

- 192.0.2.0/24 und 192.0.2.8 werden nicht akzeptiert, da 192.0.2.8 innerhalb von 192.0.5.0/24 liegt.
- Überlappende Subnetze: 192.0.2.0/24 und 192.0.0.0/20 werden nicht akzeptiert, da sich die Subnetze überschneiden.
- Geben Sie bei der Eingabe eines Netzwerk-Subnetzwerts die Netzwerk-IP-Adresse als IP-Adresswert ein.

  Beispiel:

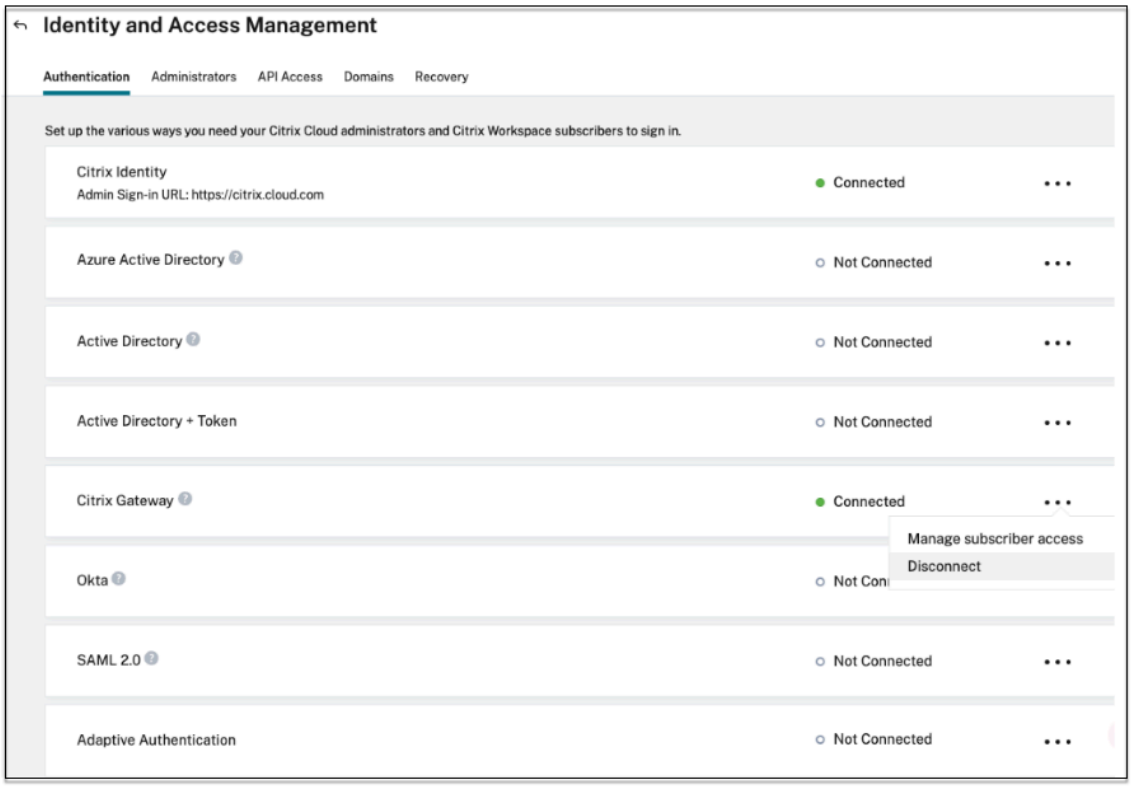
- 192.0.2.2/24 ist falsch, verwenden Sie stattdessen 191.0.2.0/24
- 192.0.2.0/20 ist falsch, verwenden Sie stattdessen 192.0.0.0/20

Um diese Funktion zu aktivieren, wenden Sie sich an den Citrix Support.

Authentifizierungsmethode auf Adaptiven Authentifizierung migrieren

Kunden, die bereits Adaptive Authentication mit Authentifizierungsmethode **NetScaler Gateway** verwenden, müssen **Adaptive Authentication** migrieren und dann die OAuth-Konfiguration aus der Adaptive Authentication-Instanz entfernen.

1. Wechseln Sie zu einer anderen Authentifizierungsmethode als NetScaler Gateway.
2. Klicken Sie in **Citrix Cloud > Identitäts- und Zugriffsmanagement**auf die Ellipsenschaltfläche für NetScaler Gateway, und klicken Sie dann auf **Trennen**.



3. Wählen Sie **Ich verstehe die Auswirkungen auf das Abonnentenerlebnis**und klicken Sie dann auf **Bestätigen**.

   Wenn Sie auf **Bestätigen** klicken, wirkt sich dies auf die Workspace-Anmeldung bei Endbenutzern aus und die adaptive Authentifizierung wird erst dann für die Authentifizierung verwendet, wenn Adaptive Authentication

4. Entfernen Sie in der Verwaltungskonsole der Adaptive Authentication-Instanz die OAuth-bezogene Konfiguration.

   Mit der CLI:

   ```
   unbind authentication vs <authvsName> -policy <oauthIdpPolName>
   rm authentication oauthIdpPolicy <oauthIdpPolName>
   rm authentication oauthIdpProfile <oauthIdpProfName>
   <!--NeedCopy-->
   ```

   Durch die Verwendung der GUI:

   a) Navigieren Sie zu **Sicherheit > AAA —Anwendungsdatenverkehr > Virtuelle Server**.
   b) Lösen Sie die OAuth-Richtlinie.
   c) Navigieren Sie zu **Sicherheit > AAA —Anwendungsdatenverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > OAuth IDP**.
   d) Löschen Sie die OAuth-Richtlinie und das Profil.

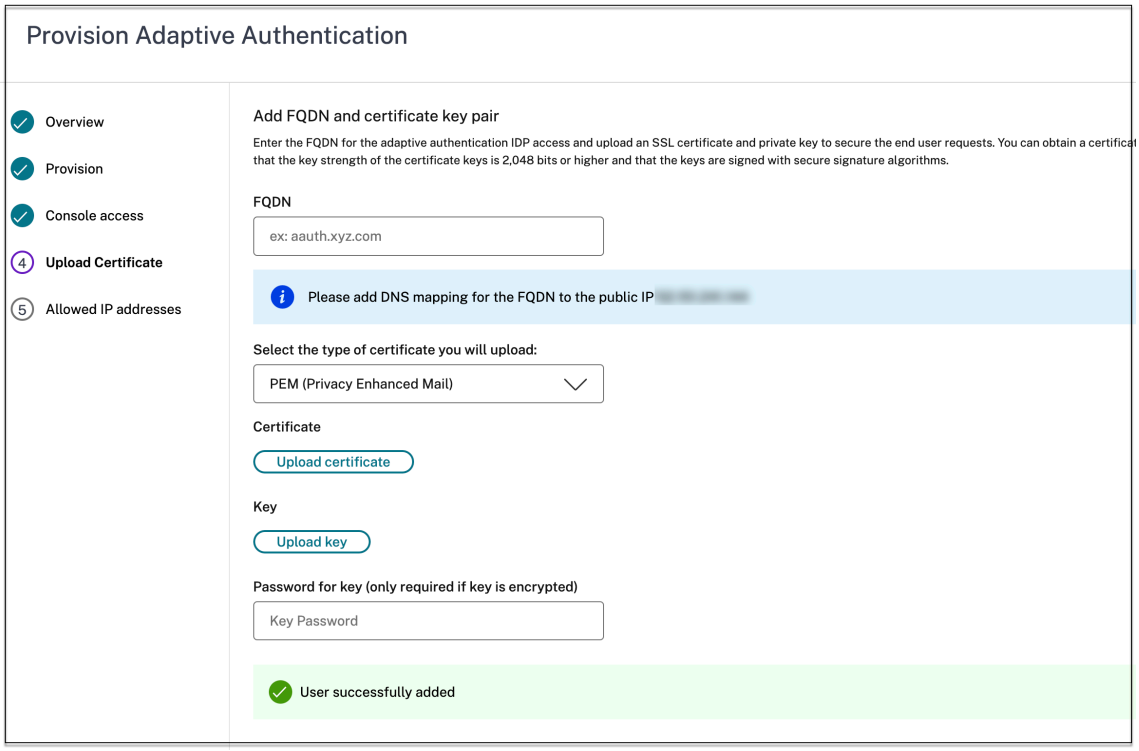
5. Navigieren Sie zu **Citrix Cloud > Identitäts- und Zugriffsmanagement**.
   Klicken Sie auf der Registerkarte Authentifizierung unter Adaptive Authentifizierung auf das Ellipsenmenü und wählen Sie **Verwalten** aus.

   ODER greifen Sie auf https://adaptive-authentication.cloud.com zu

6. Klicken Sie auf **Details anzeigen**.

7. Gehen Sie im Fenster **Zertifikat hochladen** wie folgt vor:

   - Fügen Sie den FQDN für adaptive Authentifizierung hinzu
   - Entfernen Sie die Zertifikate und Schlüsseldateien und laden Sie sie erneut hoch.



> **Wichtig:**
>
> Wenn Sie einen FQDN oder das Zertifikatschlüsselpaar direkt bearbeiten, ohne auf **Adaptive Authentication**zu migrieren, schlägt die Verbindung zur Identitäts- und Zugriffsverwaltung fehl und die folgenden Fehler werden angezeigt. Sie müssen zur Adaptive Authentication-Methode migrieren, um diese Fehler zu beheben.
>
> - ADC-Befehl ist mit einem Fehler fehlgeschlagen. Eine Richtlinie ist bereits an die angegebene Priorität gebunden.
> - ADC-Befehl ist mit einem Fehler fehlgeschlagen. Die Bindung einer Richtlinie, die nicht gebunden ist, kann nicht aufgehoben werden.

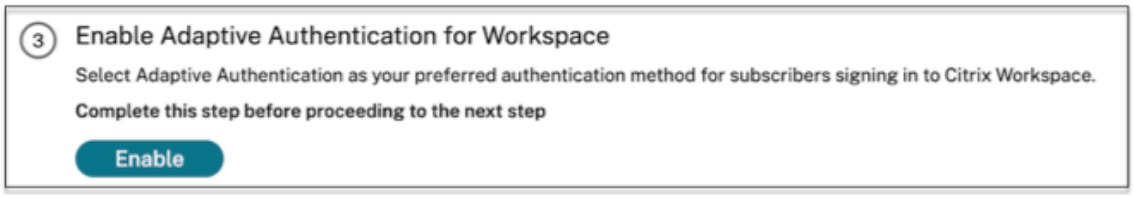
8. Klicken Sie auf **Änderungen speichern**.

   Zu diesem Zeitpunkt zeigt das Identitäts- und Zugriffsmanagement die **adaptive Authentifizierung** als **Verbunden** an, und für die Adaptive Authentication-Instanz ist das OAuth-Profil automatisch konfiguriert.

   Sie können dies von der GUI aus überprüfen.

   a) Greifen Sie auf Ihre Adaptive Authentication-Instanz zu und melden Sie sich
   b) Navigieren Sie zu **Sicherheit > AAA —Anwendungsdatenverkehr > Virtuelle Server**. Sie müssen sehen, dass das OAuth-IdP-Profil erstellt wurde.
   c) Navigieren Sie zu **Citrix Cloud > Identitäts- und Zugriffsmanagement**. Adaptive Authentifizierung befindet sich im Status **Verbunden** .

9. Aktivieren Sie die Methode Adaptive Authentication erneut, indem Sie auf der Homepage der adaptiven Authentifizierung auf **Aktivieren** (Schritt 3) klicken



   Dieser Schritt aktiviert die Authentifizierungsmethode als Adaptive Authentication in Ihrer Workspace-Konfiguration.

10. Klicken Sie in Schritt 3 auf den Workspace-Link, nachdem Sie auf **Aktivieren**ge Sie müssen sehen, dass die Authentifizierungsmethode in Adaptive Authentication geändert wurde.

> **Hinweis:**
>
> Neue Benutzer müssen dieselben Schritte ausführen, mit Ausnahme des Schritts zum Entfernen der OAuth-bezogenen Konfiguration.

Beispielkonfigurationen zur Authentifizierung

Kunden können eine Authentifizierungsrichtlinie ihrer Wahl konfigurieren und an den virtuellen Authentifizierungsserver binden. Bindungen des Authentifizierungsprofils sind für den virtuellen Authentifizierungsserver nicht erforderlich. Nur die Authentifizierungsrichtlinien können konfiguriert werden. Im Folgenden sind einige der Anwendungsfälle aufgeführt.

> **Wichtig:**
>
> Die Authentifizierungskonfiguration darf nur auf den primären Knoten erfolgen.

Multifaktor-Authentifizierung mit bedingter Authentifizierung

- Zwei-Faktor-Authentifizierung mit LDAP und RADIUS unter Verwendung eines Dual-Faktor-Schemas (Benutzereingabe nur einmal)
- Anmeldemethode für die Authentifizierung gemäß den Abteilungen des Benutzers (Mitarbeiter, Partner, Lieferant) in der Organisation mit Dropdown-Menü zur Auswahl der Abteilung
- Authentifizierungsanmeldemethode gemäß Benutzerdomänen mit Dropdownmenü
- Konfigurieren Sie die Eingabe der E-Mail-ID (oder des Benutzernamens) als ersten Faktor mit bedingtem Zugriff basierend auf der Gruppenextraktion mit E-Mail-ID im ersten Faktor und stellen Sie für jede Gruppe einen anderen Anmeldetyp bereit
- Multifaktor-Authentifizierung mit Zertifikatauthentifizierung für Benutzer mit Benutzerzertifikaten und Native OTP-Registrierung für Benutzer ohne Zertifikat

- Unterschiedlicher Authentifizierungstyp mit bedingter Authentifizierung gemäß den Eingaben des Hostnamens
- Dual-Faktor-Authentifizierung mit nativer OTP-Authentifizierung
- Google erneut CAPTCHA

Integration von Drittanbietern mit Multifaktor-Authentifizierung

- Azure AD als SAML-IdP konfigurieren (Nächsten Faktor als LDAP-Richtlinie konfigurieren - NO_AUTH zur Vervollständigung der OAuth-Vertrauensstellung)
- Bedingte Authentifizierung mit First Factor als SAML und dann benutzerdefinierter Anmeldung bei Zertifikat oder LDAP basierend auf SAML-Attributen
- Erster Faktor war Webauth-Login gefolgt von LDAP

Device Posture Scans (EPA)

- Gerätezustandsprüfung zur Versionsprüfung, gefolgt von einer benutzerdefinierten Anmeldung für konforme (RADIUS) und nicht konforme Benutzer (LDAP)
- LDAP-Authentifizierung gefolgt von einem obligatorischen Gerätezustand-Scan
- Überprüfung des Gerätestatus vor und nach der AD-Authentifizierung —vor und nach der EPA als Faktor
- Gerätezertifikat als EPA-Faktor

Verschiedene Szenarien

- EULA mit Authentifizierung hinzufügen
- Anpassen der nFactor-Richtlinienbeschriftungen,

Speicherplatzverwaltung für Instanzen

June 19, 2024

Das Adaptive Authentication-Team verwaltet alle Upgrades und Wartungsarbeiten der Adaptive Authentication-Instanzen. Daher wird empfohlen, die Adaptive Authentication-Instanzen nicht auf zufällige RTM-Builds zu aktualisieren oder herabzustufen. Citrix verwaltet standardmäßig die Adaptive Authentication-Instanzen.

Für die Instanz-Upgrades sind mindestens 7 GB Speicherplatz im VAR-Verzeichnis erforderlich. Daher räumt das Adaptive Authentication Service-Team den Speicherplatz auf den Instanzen frei, bevor Upgrades angewendet werden. Es wird empfohlen, keine sensiblen, urheberrechtlich geschützten oder persönlichen Daten in den folgenden Verzeichnissen aufzubewahren:

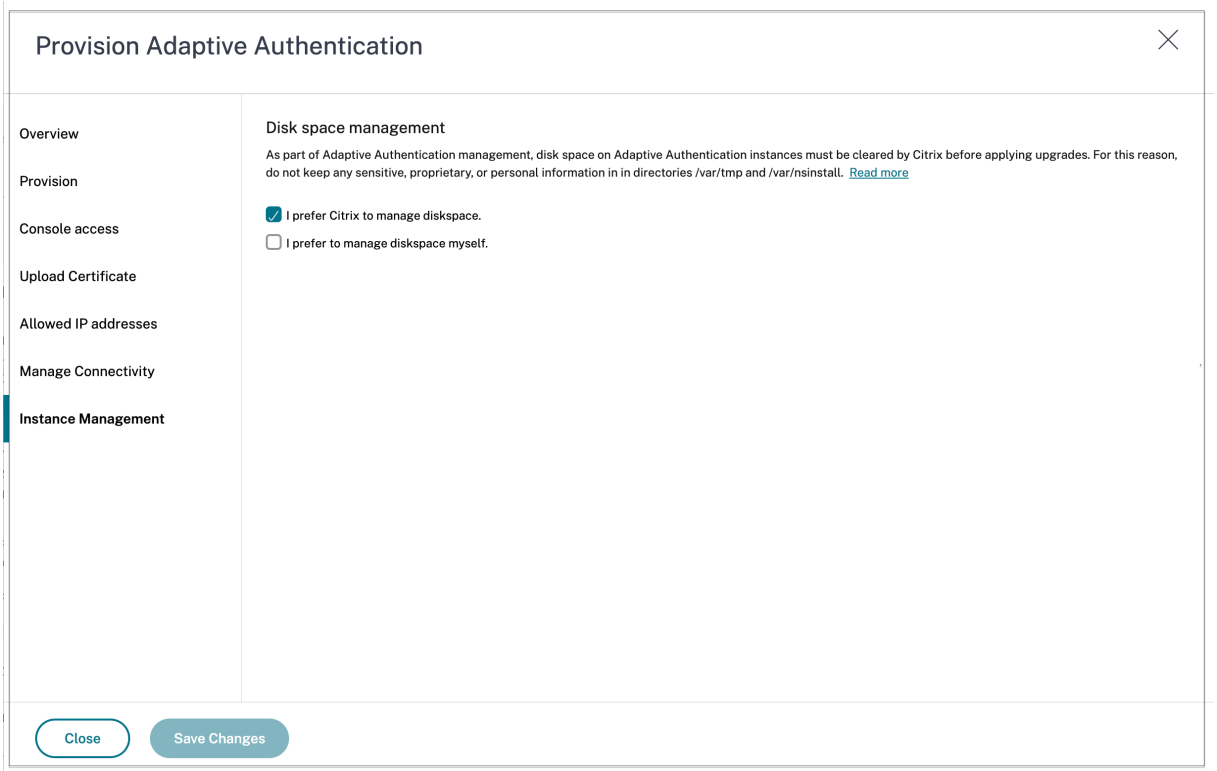
- /var/core
- /var/crash
- /var/tmp
- /var/nsinstall
- /var/nstrace
- /var/nslog

> **Hinweis:**
>
> - Das Verzeichnis /var/nsinstall wird während des Upgrades zuerst gelöscht, gefolgt vom Verzeichnis /var/tmp. Wenn der Mindestspeicherbedarf immer noch nicht erfüllt ist, werden auch die anderen Verzeichnisse (/var/core, /var/crash, /var/nstracem und /var/nslog) gelöscht.
> - Der Kunde ist für die Verwaltung und Wartung des NetScaler-Datenträgerspeichers und die Datenträgerbereinigung verantwortlich.

Option, den Speicherplatz selbst zu verwalten

Obwohl Citrix die Adaptive Authentication-Instanzen standardmäßig verwaltet, können Sie es vorziehen, den Speicherplatz auf den Instanzen selbst zu bereinigen. Sie können die Standardmethode wie folgt deaktivieren:

1. Klicken Sie im Navigationsbereich Adaptive Authentication auf **Instance Management**.
2. Wählen Sie **Ich bevorzuge es, den Speicherplatz selbst zu verwalten**, und klicken Sie dann im Bestätigungsdialogfeld auf **Bestätigen**.
3. Klicken Sie auf **Änderungen speichern**.



> **Hinweis:**
>
> Sie können Upgrades auch entsprechend Ihrem Kundenverkehr planen. Das Citrix Cloud-Team aktualisiert Ihre Instanzen dann entsprechend.
> Informationen zur Planung von Upgrades finden Sie unter Planen des Upgrades Ihrer Adaptive Authentication-Instanzen.

Probleme mit der adaptiven Authentifizierung beheben

June 19, 2024

Die Probleme werden basierend auf den verschiedenen Stufen der Konfiguration kategorisiert:

- Provisioning
- Problem beim Zugriff auf eine Instanz
- AD/Radius-Verbindungs- und Authentifizierungsproblem
- Probleme mit der Authentifizierung
- Probleme im Zusammenhang mit der EPA/Gerätehaltung
- Probleme im Zusammenhang mit Smarttags
- Protokollsammlung

Sie können die Probleme auch mit der Adaptive Authentication CLI beheben. Gehen Sie wie folgt vor, um eine Verbindung mit der CLI herzustellen:

- Laden Sie den SSH-Client wie putty/securecrt auf Ihren Computer herunter.
- Greifen Sie über die Verwaltungs-IP-Adresse (primäre) auf die Adaptive Authentication-Instanz
- Melden Sie sich mit Ihren Anmeldeinformationen an.

Einzelheiten finden Sie unter Zugreifen auf eine NetScaler Appliance.

Protokollierung adaptiver Authentifizierungsprotokolle aktivieren

Stellen Sie sicher, dass Sie die Protokollstufen aktivieren, um die adaptiven Authentifizierungsprotokolle zu erfassen.

Protokolle mit CLI aktivieren:

1. Melden Sie sich bei der Adaptive Authentication-Instanz an.
2. Geben Sie mit PuTTY die Verwaltungsanmeldeinformationen ein.
3. Führen Sie den Befehl aus `set audit syslogParams logLevel ALL`

Protokollierung über die GUI aktivieren:

1. Melden Sie sich mit einem Browser bei der Adaptive Authentication-Instanz an
2. Navigieren Sie zu **Konfiguration > System > Auditing**.
3. Klicken Sie auf der Seite Überwachung unter **Einstellungen** auf **Syslog-Einstellungen für Auditing ändern**.
4. Wählen Sie unter **Protokollebenen** die Option **ALLE** aus.

Provisioningprobleme

- **Zugriff auf die Benutzeroberfläche der adaptiven Authentifizierung nicht möglich**

  Prüfen Sie, ob die Berechtigung für Ihre Kunden-ID/Ihren Mandanten aktiviert ist.

- **Ich stecke länger als 45 Minuten auf der Provisioning-Seite fest**

  Sammeln Sie den Screenshot des Fehlers, falls vorhanden, und wenden Sie sich an den Citrix Support, um Unterstützung zu erhalten.

- **VNet-Peer ist ausgefallen**

  - Überprüfen Sie, ob im Azure-Portal Warnungen vorhanden sind, die diesem Peering entsprechen, und führen Sie die empfohlenen Maßnahmen aus.
  - Löschen Sie das Peering und fügen Sie es erneut über die Benutzeroberfläche der adaptiven Authentifizierung hinzu.

- **Die Aufhebung der Bereitstellung ist nicht abgeschlossen**

  Wenden Sie sich an Citrix Support, um Unterstützung zu erhalten.

Problem beim Zugriff auf eine Instanz

- **Die Management-IP-Adresse ist für die Instanz nicht zugänglich**
  - Überprüfen Sie, ob die öffentliche IP-Adresse des Clients, die für den Zugriff verwendet wird, zu den zulässigen Quell-IP-Adressen gehört.
  - Überprüfen Sie, ob ein Proxy die IP-Adresse der Client-Quelle ändert.
- **Anmeldung bei der Instanz nicht möglich**

  Stellen Sie sicher, dass der Administratorzugriff mit den Anmeldeinformationen, die Sie bei der Bereitstellung eingegeben haben, einwandfrei funktioniert.
- **Endbenutzer haben keine vollständigen Rechte**

  Stellen Sie beim Hinzufügen des Benutzers sicher, dass Sie die geeignete Befehlsrichtlinie für den Zugriff gebunden haben. Weitere Informationen finden Sie unter Benutzer, Benutzergruppen und Befehlsrichtlinien.

AD- oder RADIUS-Konnektivitätsproblem

Problem mit Azure Vnet-Peering-Konnektivitätstyp:

- Überprüfen Sie, ob das vom Kunden verwaltete Azure VNet von den Adaptive Authentication-Instanzen
- Prüfen Sie, ob die Konnektivität/Erreichbarkeit des vom Kunden verwalteten Azure VNet zu AD funktioniert.
- Stellen Sie sicher, dass geeignete Routen hinzugefügt werden, um den Datenverkehr von on-premises zu Azure VNets zu leiten.

Windows-basierter Connector:

- Alle Protokolle sind im Verzeichnis /var/log/ns.log verfügbar und jedem Protokoll wird das Präfix [NS_AAUTH_TUNNEL] vorangestellt.
- ConnectionID aus Protokollen kann verwendet werden, um verschiedene Transaktionen zu korrelieren.
- Stellen Sie sicher, dass die private IP-Adresse der virtuellen Connector-Maschine als einer der RADIUS-Clients im RADIUS-Server hinzugefügt wird, da diese IP-Adresse die Quell-IP-Adresse für den Connector ist.

Für jede Authentifizierungsanforderung wird der Tunnel zwischen der Adaptive Authentication-Instanz (NS - AAAD-Prozess) und dem Authentifizierungsserver eingerichtet. Sobald der Tunnel erfolgreich eingerichtet wurde, erfolgt die Authentifizierung.

Stellen Sie sicher, dass die virtuelle Connector-Maschine den FQDN für adaptive Authentifizierung auflösen kann.

- Connector ist installiert, die on-premises Konnektivität schlägt jedoch fehl.

  Überprüfen Sie, ob NSAUTH-TUNNEL eingerichtet wird.

  ```
  cat ns.log | grep -I “tunnel”
  ```

  Wenn das folgende Beispielprotokoll nicht in der Datei ns.log für die Authentifizierungsanforderung gedruckt wird, liegt möglicherweise ein Problem beim Aufbau eines Tunnels oder ein Problem von der Connectorseite vor.

  ```
  1  LDAP:
  2  [NS_AAUTH_TUNNEL] Entering bitpump for
  3  Connection1 => Src : 192.168.0.7:28098, Dst : 10.106.103.60:636 ,
         Connection2 => Src : 10.106.103.70:2271, Dst :
        10.106.103.80:443"
  4  RADIUS:
  5  [NS_AAUTH_UDP_TUNNEL] MUX channel established"
  6  <!--NeedCopy-->
  ```

  Überprüfen Sie die Protokolldetails und ergreifen Sie entsprechende Maßnahmen.

Angaben protokollieren	Korrekturmaßnahme
Protokolle mit Präfix `[NS_AAUTH_TUNNEL]` werden nicht in die Protokolldatei aufgenommen `[NS_AAUTH_TUNNEL] Waiting for outbound from connector` Für dieses Protokoll, wenn die folgende Antwort nicht empfangen wird: `[NS-AAUTH-TUNNEL] Received connect command from connector and client connection lookupsucceeded"`	Führen Sie den Befehl `show cloudtunnel vserver` aus. Dieser Befehl muss beide virtuellen Cloud-Tunnelserver (TCP und UDP) mit dem Status “UP”auflisten. Überprüfen Sie, ob der Connectorcomputer in der Lage ist, den FQDN für adaptive Authentifizierung zu erreichen, **ODER** überprüfen Sie die connectorseitige Firewall auf ausgehende Verbindungen zum FQDN für Adaptive

Angaben protokollieren	Korrekturmaßnahme
`[NS_AAUTH_TUNNEL] Server is down or couldn't create connection to ip 0.0.0.0` und `[NS_AAUTH_TUNNEL] Connect response code 401 is not 200 OK, bailing out"`	Wenden Sie sich an den Citrix Support.

Keine Antwort vom Connector:

- Stellen Sie sicher, dass der FQDN für adaptive Authentifizierung von der virtuellen Connector-Maschine aus erreichbar ist
- Stellen Sie sicher, dass ein Zwischenzertifikat gebunden und mit dem Serverzertifikat auf der Adaptive Authentication-Instanz verknüpft ist.

Falsche LDAP/RADIUS-Einstellungen:

Wenn die IP-Adresse Ihres AD/RADIUS-Servers eine öffentliche IP-Adresse ist, müssen Sie das Subnetz oder die IP-Adresse hinzufügen, die die Ausdrücke in NetScaler adressiert. Bearbeiten Sie nicht die vorhandenen Bereiche.

- So fügen Sie ein Subnetz oder eine IP-Adresse mit der CLI hinzu:

```
1  set policy expression aauth_allow_rfc1918_subnets "(CLIENT.IP.DST
       .BETWEEN(10.0.0.0,10.255.255.255) || CLIENT.IP.DST.BETWEEN
       (172.16.0.0,172.31.255.255) || CLIENT.IP.DST.BETWEEN
       (192.168.0.0, 192.168.255.255) || CLIENT.IP.DST.BETWEEN
       (13.14.0.0, 13.14.255.255)||CLIENT.IP.DST.EQ(1.2.5.4))"
2  <!--NeedCopy-->
```

- So fügen Sie mithilfe der GUI ein Subnetz oder eine IP-Adresse hinzu:

  1. Navigieren Sie zu **Appexpert > Expressions**.
  2. Fügen Sie den Ausdruck **aauth_allow_rfc1918_subnets**hinzu.

Wenn der Tunnel eingerichtet ist, die Authentifizierung jedoch weiterhin fehlschlägt, führen Sie die folgenden Schritte aus, um das Problem zu beheben.

LDAP:

- Überprüfen Sie die Details des Bind-DN.
- Bestätigen Sie den Fehler mithilfe der Testkonnektivität.
- Überprüfen Sie die Fehler mit `aaad`-Debug.

- Melden Sie sich mit der CLI bei der Adaptive Authentication-Instanz an.

```
shell
cd /tmp
cat aaad.debug
<!--NeedCopy-->
```

Häufige LDAP-Fehler:

- Server-Timeout —Keine Antwort vom Connector für die LDAP-Abfrage.
- Andere LDAP-Fehler finden Sie unter https://support.citrix.com/article/CTX138663.

Radius:

- Die Connector-IP-Adresse muss als Quell-IP-Adresse des RADIUS-Clients in der RADIUS-Serverkonfiguration hinzugefügt werden.

Probleme mit der Authentifizierung

- **Fehler nach der Assertion für OAuth**
  - Stellen Sie sicher, dass alle Anträge von AD bereitgestellt werden. Sie benötigen 7 Claims, um dies erfolgreich zu machen.
  - Überprüfen Sie die Protokolle in /var/log/ns.log, um den Fehler für OAuth-Fehler zu finden.

```
cat /var/log/ns.log
<!--NeedCopy-->
```

  - Überprüfen Sie die OAuth-Profilparameter.
- **Azure AD-Authentifizierung bleibt bei der Assertion hängen**

  Fügen Sie AD-Authentifizierung als nächsten Faktor hinzu, wobei die Authentifizierung auf Aus gesetzt ist. Dies dient dazu, alle erforderlichen Ansprüche für eine erfolgreiche Authentifizierung abzurufen.

EPA-bezogene Probleme

- **Das Plug-in ist bereits vorhanden, aber der Benutzer wird aufgefordert, das Plug-in herunterzuladen.**

  Mögliche Ursachen: Versionskonflikt oder beschädigte Dateien
  - Führen Sie Entwicklertools aus und überprüfen Sie, ob die Plugin-Listendatei dieselbe Version wie die des NetScaler und Ihres Client-Computers enthält.

- Stellen Sie sicher, dass die Client-Version auf dem NetScaler dieselbe ist wie auf dem Client-Computer.

  Aktualisieren Sie den Client auf dem NetScaler.

  Navigieren Sie in der Adaptive Authentication-Instanz zu **NetScaler Gateway > Globale Einstellungen > Clientbibliotheken aktualisieren**.

  Auf der Seite EPA-Plug-in-Bibliotheken auf Citrix Downloads finden Sie detaillierte Informationen.

- Manchmal kann die Anfrage auf NetScaler zwischengespeichert werden, auch wenn die Version aktualisiert wird.

  `show cache object` zeigt die Details des zwischengespeicherten Plug-ins an. Sie können es löschen, indem Sie den Befehl verwenden;

  ```
  flush cache object -locator 0x00000023345600000007
  ```

Einzelheiten zur Erfassung von EPA-Protokollen finden Sie unter https://support.citrix.com/article/CTX209148.

- **Gibt es eine Möglichkeit, die EPA-Einstellungen (Immer, Ja, Nein) zurückzusetzen, nachdem der Benutzer eine Option ausgewählt hat.**

  Derzeit erfolgt das Zurücksetzen der EPA-Einstellungen manuell.

  - Navigieren Sie auf dem Client-Computer zu C:\Users<user_name>\ AppData\ Local\ Citrix\ AGEE.
  - Öffnen Sie die Datei `config.js` und setzen Sie TrustAlways auf null - `"trustAlways":null`

Probleme mit Smart-Zugriff-Tags

- **Nach der Konfiguration des Smart Access sind Anwendungen nicht verfügbar**

  Stellen Sie sicher, dass die Tags sowohl in der Adaptive Authentication-Instanz als auch in den Citrix VDA-Bereitstellungsgruppen definiert sind.

  Vergewissern Sie sich, dass die Tags der Workspace-Bereitstellungsgruppe in Großbuchstaben hinzugefügt wurden.

  Sie können die Datei ns.log sammeln und sich an den Citrix Support wenden, falls dies nicht funktioniert.

Allgemeine Protokollsammlung für die Adaptive Authentifizierungsinstanz

- Paket für technischen Support: Weitere Informationen finden Sie unter So sammeln Sie das Paket für technischen Support von SDX- und VPX-Appliances für Insight-Analysen.
- Dateien verfolgen. Einzelheiten finden Sie unter Aufzeichnen einer Paketverfolgung auf NetScaler.

Weitere Informationen erhalten Sie vom Citrix Support.

Intelligenter Zugriff mit adaptiver Authentifizierung

June 19, 2024

Citrix Cloud-Kunden können intelligenten Zugriff (Adaptive Access) auf die Citrix DaaS-Ressourcen (virtuelle Apps und Desktops) oder den Secure Private Access Service mithilfe der adaptiven Authentifizierung als Identitätsanbieter für Citrix Workspace bereitstellen.

Die Smart Access-Funktion ermöglicht es dem Adaptive Authentication Service, alle Richtlinieninformationen über den Benutzer an Citrix Workspace oder Citrix DaaS weiterzuleiten. Der Adaptive Authentication Service kann den Gerätestatus (EPA), den Netzwerkstandort (innerhalb oder außerhalb des Unternehmensnetzwerks, Geolocation), Benutzerattribute wie Benutzergruppen, Tageszeit oder eine Kombination dieser Parameter als Teil der Richtlinieninformationen angeben. Der Citrix DaaS-Administrator kann diese Richtlinieninformationen dann verwenden, um den kontextuellen Zugriff auf die virtuellen Apps und Desktops zu konfigurieren. Die virtuellen Apps und Desktops können entweder auf der Grundlage der früheren Parameter (Zugriffsrichtlinie) aufgezählt werden oder nicht. Einige Benutzeraktionen wie der Zugriff auf die Zwischenablage, die Druckerumleitung, das Clientlaufwerk oder die USB-Zuordnung können ebenfalls gesteuert werden.

Anwendungsbeispiele:

- Der Administrator kann die Gruppe von Apps so konfigurieren, dass sie nur von bestimmten Netzwerkstandorten wie dem Unternehmensnetzwerk aus angezeigt oder aufgerufen wird.
- Der Administrator kann die Gruppe von Apps so konfigurieren, dass sie nur von unternehmensverwalteten Geräten aus angezeigt oder aufgerufen wird. EPA-Scans können beispielsweise überprüfen, ob es sich bei dem Gerät um ein vom Unternehmen verwaltetes Gerät oder BYOD handelt. Basierend auf dem EPA-Scanergebnis können die relevanten Apps für den Benutzer aufgelistet werden.

Voraussetzungen

- Adaptive Authentication als IdP muss für Citrix Workspace konfiguriert sein. Einzelheiten finden Sie unter Adaptive Authentication Service.
- Der adaptive Authentifizierungsdienst mit Citrix DaaS ist in Betrieb.
- Die Adaptive Access-Funktion ist aktiviert. Einzelheiten finden Sie unter Adaptiven Zugriff aktivieren.

Den Ablauf von Ereignissen für Smart Access verstehen

1. Der Benutzer meldet sich bei Citrix Workspace an.
2. Der Benutzer wird zum adaptiven Authentifizierungsdienst umgeleitet, der als IdP konfiguriert ist.
3. Der Benutzer wird zur Vorauthentifizierung (EPA) oder Authentifizierung aufgefordert.
4. Der Benutzer wurde erfolgreich authentifiziert.
5. Smart-Access-Richtlinien werden entsprechend der Konfiguration bewertet und Tags werden der Benutzersitzung zugeordnet.
6. Der Adaptive Authentication Service überträgt die Tags an den Citrix Graph-Dienst. Der Benutzer wird zur Citrix Workspace-Landingpage umgeleitet.
7. Citrix Workspace ruft die Richtlinieninformationen für diese Benutzersitzung ab, stimmt mit dem Filter überein und wertet die Apps oder Desktops aus, die aufgezählt werden müssen.
8. Der Administrator konfiguriert die Zugriffsrichtlinie auf Citrix DaaS, um den ICA-Zugriff für Benutzer einzuschränken.

Konfiguration von Smart-Access-Richtlinien auf Adaptive Authentication-Instanzen

Die Konfiguration von Smart-Access-Richtlinien auf einer Adaptive Authentication-Instanz erfolgt in zwei Schritten:

1. Definieren Sie Smart-Access-Richtlinien mit Smart-Access-Tags auf Adaptive Authentication-Instanzen. Siehe beispielsweise *Schritt 1*.
2. Definieren Sie dieselben Tags in Ihrem DaaS/Secure Private Access für den Ressourcenzugriff. Sehen Sie sich beispielsweise *Schritt 2* an.

Anwendungsfall 1: Konfigurieren Sie eine Smart-Access-Richtlinie, um Benutzern, die sich über den Chrome-Browser anmelden, den Zugriff auf die Zwischenablage zu gewähren und ihnen den Zugriff auf die Zwischenablage zu blockieren

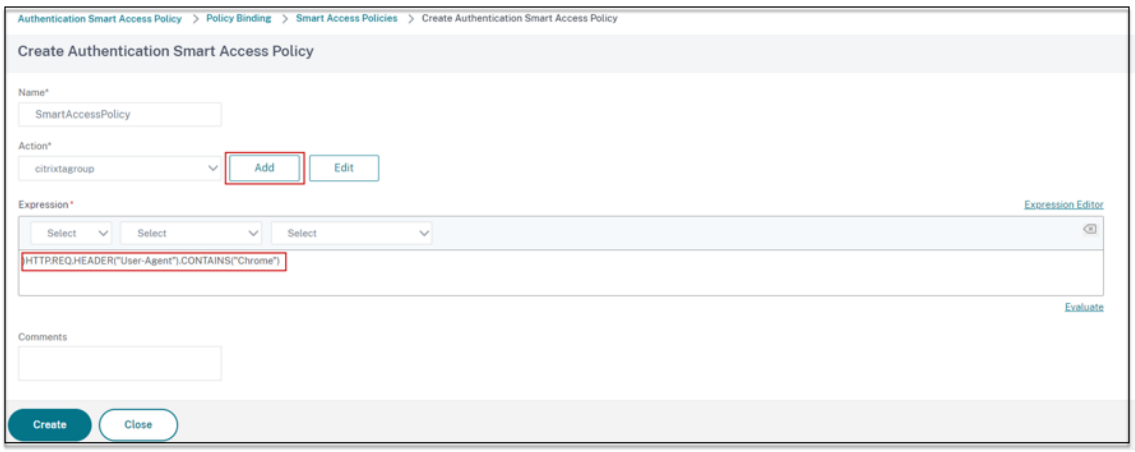
Schritt 1: Konfigurieren Sie Smart-Access-Richtlinien mit Smarttags auf der Adaptive Authentication-Instanz

1. Melden Sie sich bei der Adaptive Authentication-Instanz
2. Navigieren Sie zum virtuellen Server mit adaptiver Authentifizierung (**Sicherheit > AAA —Anwendungsdatenverkehr > Virtuelle Server**).
3. Wählen Sie den virtuellen Authentifizierungsserver aus und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie auf **Smart Access-Richtlinien**.
5. Definieren Sie den Ausdruck der Richtlinie entsprechend Ihren Anforderungen.

    a) Klicken Sie auf **Add binding**.
    b) Klicken **Sie unter Richtlinie auswählen**auf **Hinzufügen**.
    c) Geben Sie einen Namen für die Smart Access-Richtlinie ein.
    d) Definieren Sie den Ausdruck.

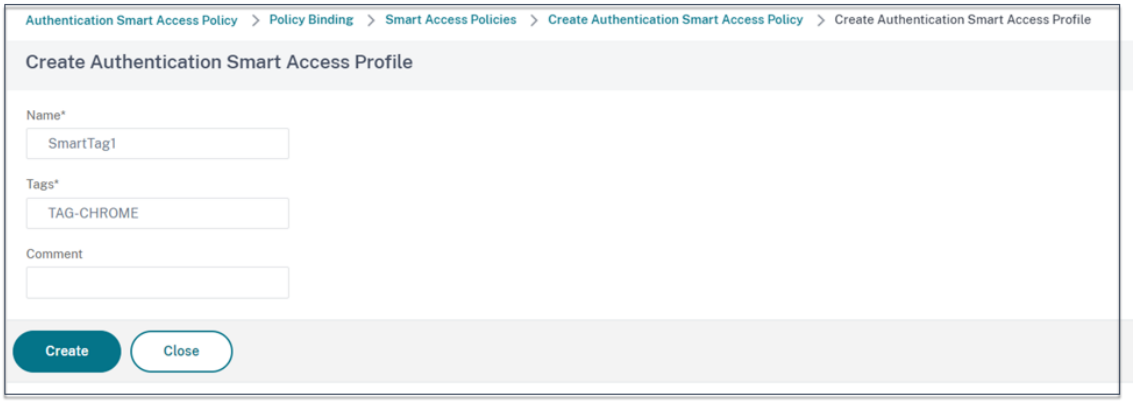
    Geben Sie als Beispiel für das Zulassen des Zugriffs für Benutzer, die sich über einen Chrome-Browser anmelden, den Ausdruck `HTTP.REQ.HEADER("User-Agent").CONTAINS("Chrome")` ein

    In ähnlicher Weise können Sie Ausdrücke erstellen, die auf der Uhrzeit, der Benutzeranmeldung, der Authentifizierungs- und Autorisierungsgruppe und anderen Optionen basieren.

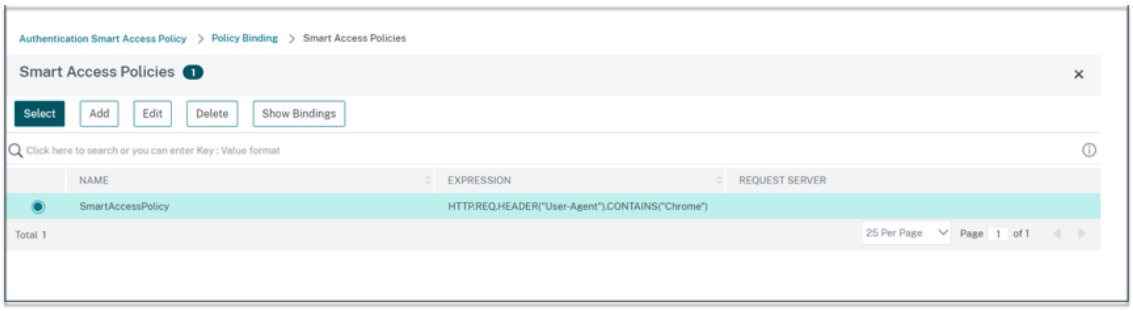


6. Erstellen Sie nun Smarttags und binden Sie diese Tags an die Smart Access-Richtlinie.

    a) Klicken Sie unter **Aktion** auf **Hinzufügen**.
    b) Geben Sie unter **Name**einen Namen für das Smart Access-Profil ein.
    c) Definieren Sie unter **Tags**die Smart Access-Tags. Zum Beispiel TAG-CHROME.



a) Klicken Sie auf **Erstellen**.
b) Wählen Sie die Smart Access-Richtlinie aus und klicken Sie auf **Bindung hinzufügen**.
c) Binden Sie dieses Smart Access-Tag an die zuvor erstellte Smart Access-Richtlinie.



> **Hinweis:**
>
> Sie können auch eine Smart-Access-Richtlinie unter **Sicherheit > AAA —Anwendungsverkehr > Richtlinien > Authentifizierung > Erweiterte Richtlinien > Smart Access > Policies** erstellen und sie dann an den virtuellen Authentifizierungsserver binden.

Schritt 2: Definieren Sie Smart Access-Tags in DaaS Studio

1. Fügen Sie die Richtlinien mit dem Smarttag “TAG-CHROME“hinzu. Einzelheiten finden Sie unter Definieren von Tags in Citrix Studio.

Anwendungsfall 2: Konfigurieren Sie Smart-Access-Richtlinien auf der Grundlage von EPA-Ergebnissen für die nachträgliche Authentifizierung

Schritt 1: Konfigurieren Sie Smart-Access-Richtlinien mit Smarttags auf der Adaptive Authentication-Instanz Für intelligenten Zugriff, der auf Bedingungen wie der Endpunktanalyse basiert, konfigurieren Sie den nFactor Flow, definieren Sie eine EPA-Aktion und fügen Sie dann die Standardgruppe hinzu.

Informationen zur Konfiguration von EPA als Faktor im nFactor-Flow finden Sie unter EPA als Faktor konfigurieren.

Logischer Ablauf

1. Der Benutzer greift auf die Workspace-URL zu.
2. Der Benutzer wird zur adaptiven Authentifizierung für die Authentifizierung/EPA weitergeleitet.
3. Die Endpunktanalyse wird für den Endbenutzer durchgeführt und die Ergebnisse werden gespeichert, indem der Benutzer zur definierten Standardgruppe hinzugefügt wird.
4. Der Benutzer wird zum nächsten Authentifizierungsablauf aufgefordert.
5. Smart-Access-Richtlinien werden evaluiert und dem Benutzer werden die Smart Access-Tags zugewiesen.

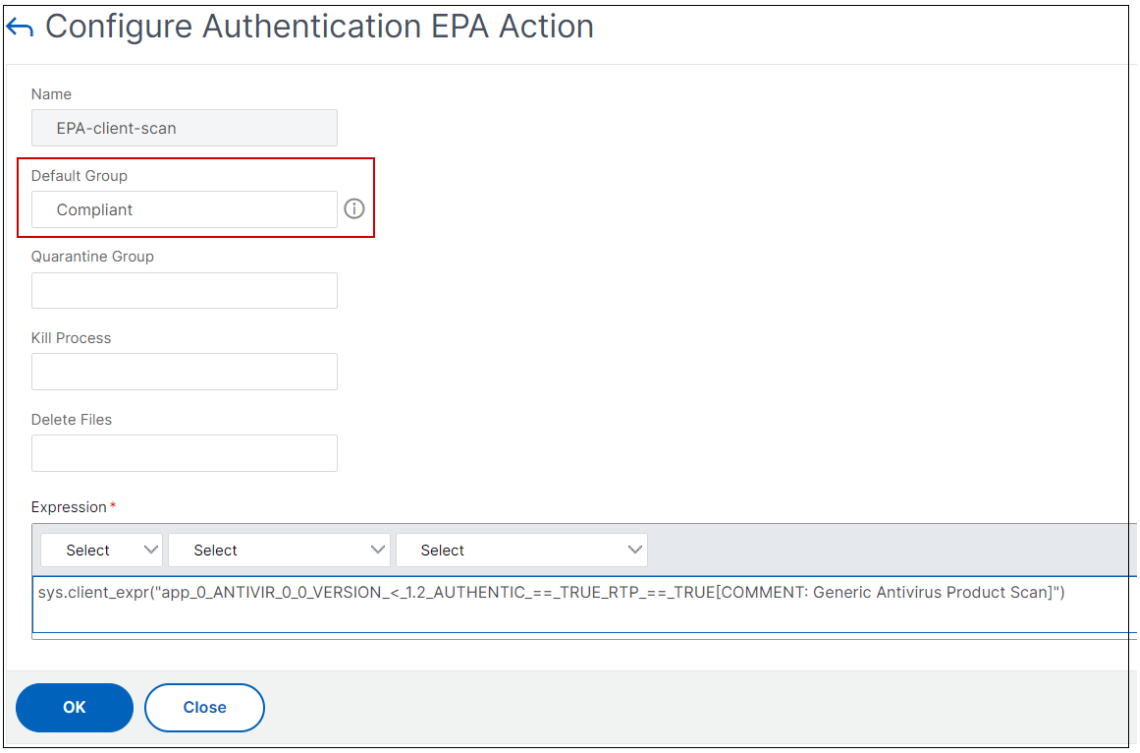
Konfiguration

Benutzer, die von einem Computer aus zugreifen, auf dem ein Antivirenprogramm installiert ist, müssen als konform markiert werden und vollen Zugriff erhalten. Benutzercomputer ohne Virenschutz müssen jedoch als nicht konform gekennzeichnet und mit eingeschränktem Zugriff versehen werden.

1. Erstellen Sie eine nFactor-Richtlinie für EPA. Einzelheiten finden Sie unter EPA als Faktor konfigurieren.

   Stellen Sie im nFactor-Flow sicher, dass der erste ein Benutzerauthentifizierungsfaktor ist.

2. Wählen Sie den EPA-Ausdruck aus, um zu überprüfen, ob das Antivirenprogramm vorhanden ist oder nicht.
3. Definieren Sie in der EPA-Aktion die Standardgruppe.



Der Benutzer wird zu dieser Standardgruppe hinzugefügt, wenn EPA erfolgreich ausgeführt wird.

4. Erstellen Sie jetzt intelligente Zugriffsrichtlinien

   a) Melden Sie sich bei der Adaptive Authentication-Instanz

   b) Navigieren Sie zum virtuellen Server mit adaptiver Authentifizierung (**Sicherheit > AAA — Anwendungsdatenverkehr > Virtuelle Server**).

   c) Wählen Sie den virtuellen Server für die adaptive Authentifizierung aus und klicken Sie auf **Bearbeiten**.

   d) Klicken Sie auf **Smart Access-Richtlinien**.

   e) Erstellen Sie zwei Smart Access-Richtlinien mit den folgenden Ausdrücken.

      - AAA.USER.IS_MEMBER_OF (“Compliant“) —Für den Benutzer EPA-Pass-Bedingung
      - ! AAA.USER.IS_MEMBER_OF (“Compliant“) —Für den Benutzer EPA-Fehlerbedingung

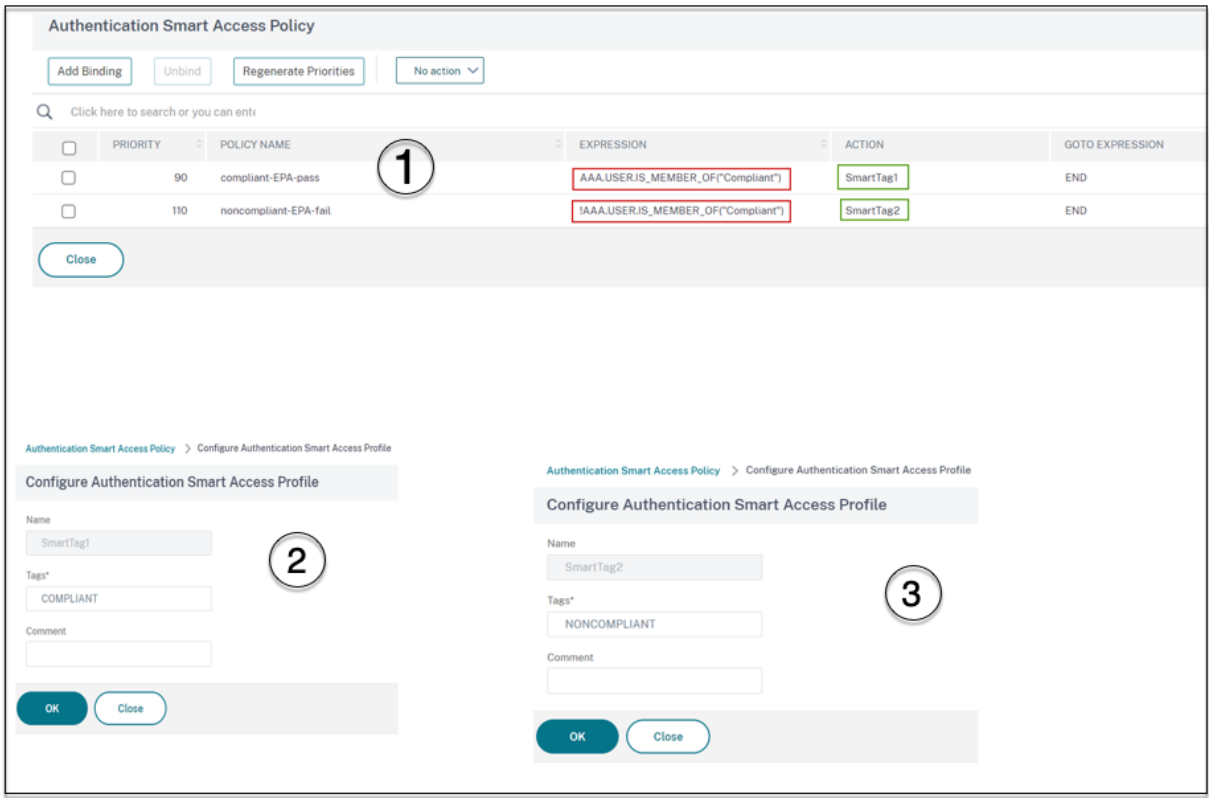
   f) Definieren Sie Smart Access-Tags für diese beiden Richtlinien.

      Beispiel:

      - Tag-Name `SmartTag1` mit dem Tag COMPLIANT für `AAA.USER.IS_MEMBER_OF (“Compliant”)`
      - Tag-Name `SmartTag2` mit dem Tag NONCOMPLIANT für `!AAA.USER.IS_MEMBER_OF (“Compliant”)`

Die Konfiguration der Adaptive Authentication-Instanz mit Bedingungen wie EPA für intelligenten Zugriff ist jetzt abgeschlossen.

Sie können die Tags und den Ausdruck entsprechend Ihren Anforderungen konfigurieren.



Schritt 2: Smart Access-Tags in DaaS Studio konfigurieren Fügen Sie die Richtlinien mit den Smarttags "COMPLIANT"und "NONCOMPLIANT"in den entsprechenden Bereitstellungsgruppen hinzu. Einzelheiten finden Sie unter Definieren von Tags in Citrix Studio.

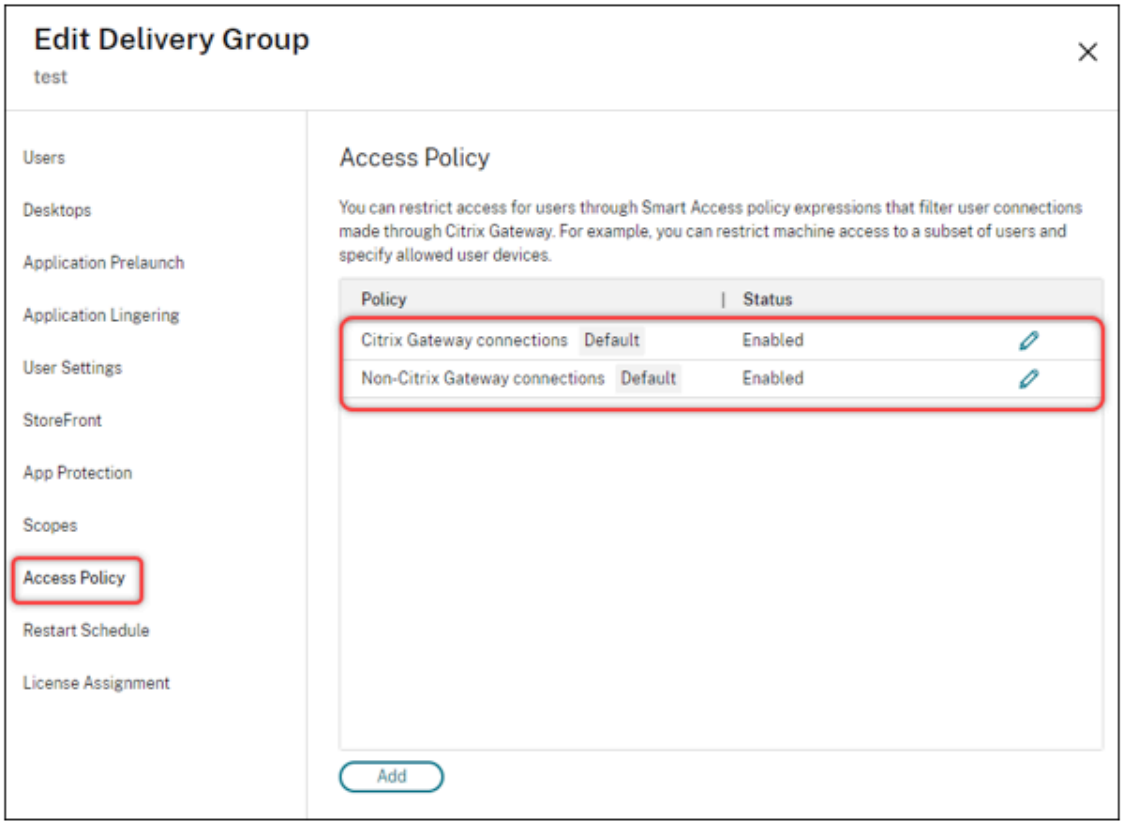
Definieren Sie Tags in DaaS Studio

Definieren Sie Tags in Bereitstellungsgruppen, um die Anwendungsaufzählung für Benutzer einzuschränken.

Beispiel: BranchOffice-Benutzer müssen Anwendungen aus der **Adaptive Access Delivery-Gruppe** sehen, die alle Anwendungen enthält.
WorkFromHome-Benutzer müssen dagegen Anwendungen der **WFH-Bereitstellungsgruppe**sehen.

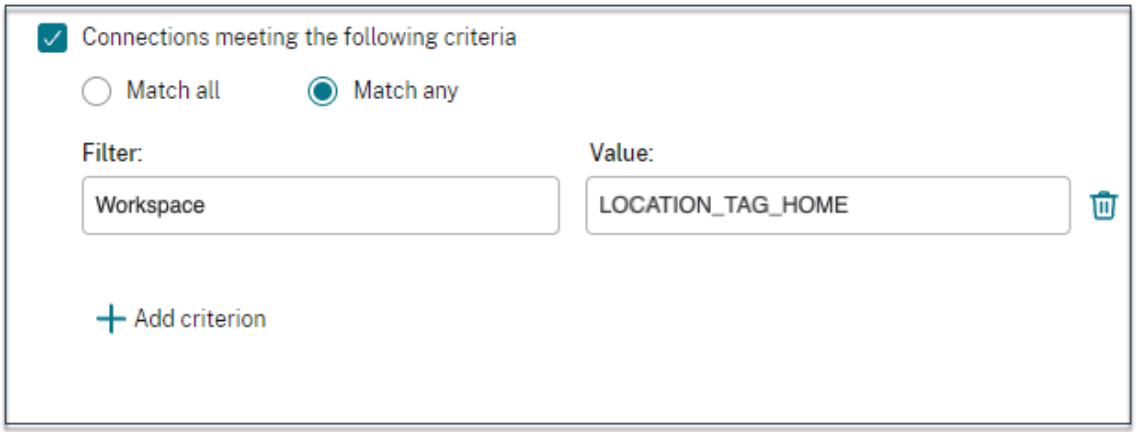
1. Melden Sie sich bei Citrix Cloud an.
2. Wählen Sie **Eigene Services > DaaS**.
3. Klicken Sie auf **Verwalten**.

4. Erstellen Sie Bereitstellungsgruppen gemäß Ihrer Anforderung. Weitere Informationen finden Sie unter Erstellen von Bereitstellungsgruppen.
5. Wählen Sie die von Ihnen erstellte Bereitstellungsgruppe aus und klicken Sie auf **Bereitstellungsgruppe bearbeiten**.



6. Klicken Sie auf **Zugriffsrichtlinie**.
7. Für Kunden, die den adaptiven Zugriff in der Citrix Workspace-Plattform verwenden, können Sie für eine Bereitstellungsgruppe den Zugriff auf interne Netzwerke wie folgt beschränken:

   a) Klicken Sie mit der rechten Maustaste auf die Bereitstellungsgruppe und wählen Sie **Bearbeiten** aus.
   b) Wählen Sie im linken Bereich die Zugriffsrichtlinie aus.
   c) Klicken Sie auf das Bearbeitungssymbol, um die standardmäßige Citrix Gateway Gateway-Verbindungsrichtlinie zu ändern.
   d) Wählen Sie auf der Seite Richtlinie bearbeiten die Option **Verbindungen aus, die die folgenden Kriterien erfüllen** , wählen Sie **Match any** aus, und fügen Sie dann die Kriterien hinzu.



Geben Sie für WorkFromHome-Benutzer die folgenden Werte in den jeweiligen Delivery Controller ein.

Farm: Workspace

Filter: LOCATION_TAG_HOME

Geben Sie für BranchOffice-Benutzer die folgenden Werte in den jeweiligen Delivery Controller ein.

Filter: Workspace

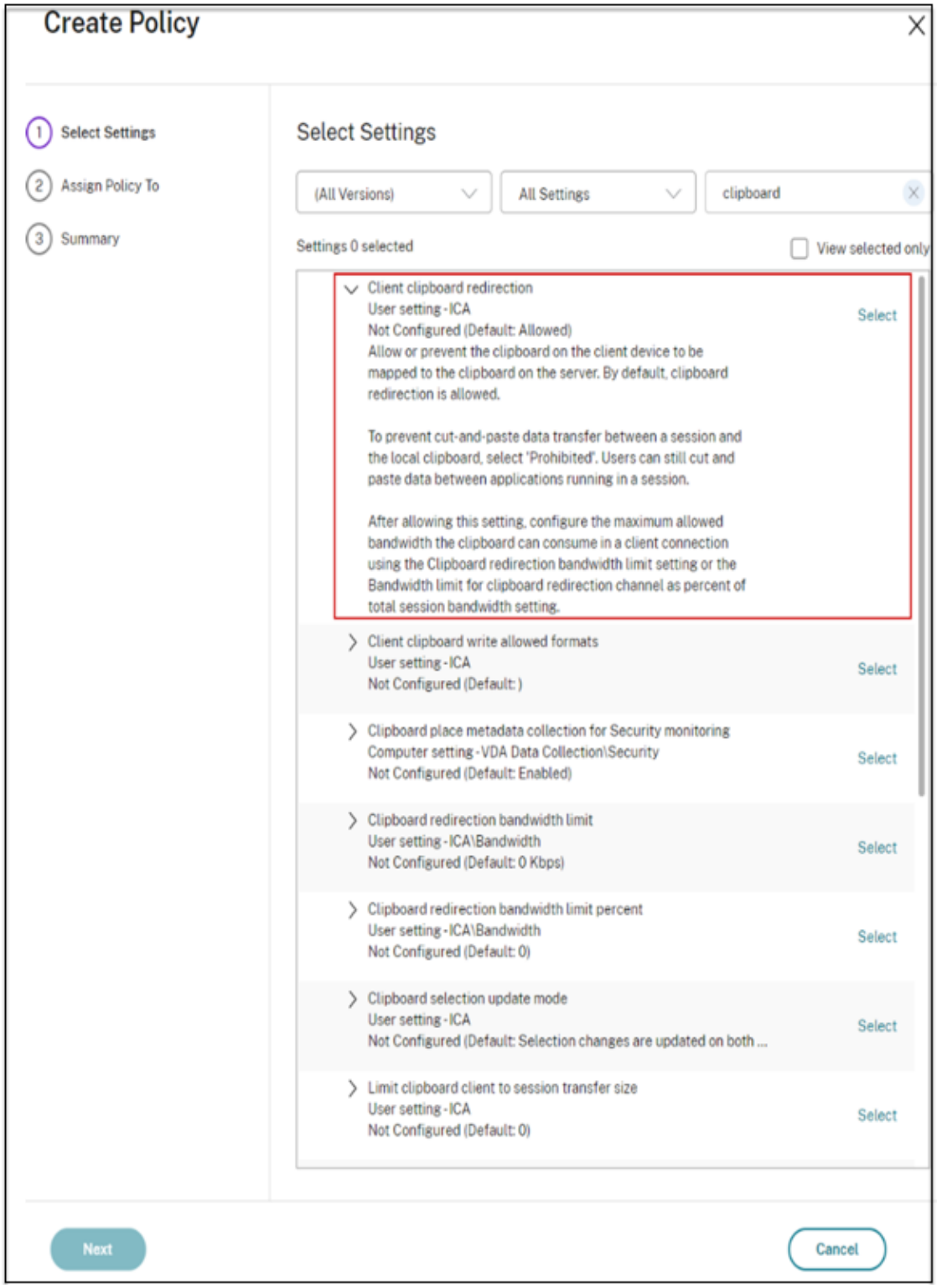
Wert: LOCATION_TAG_BRANCHOFFICE

Sie können diese Tags jetzt verwenden, um den Zugriff auf Ihre Anwendungen einzuschränken.

Beschränken Sie die Art des Zugriffs für die bereitgestellten Anwendungen

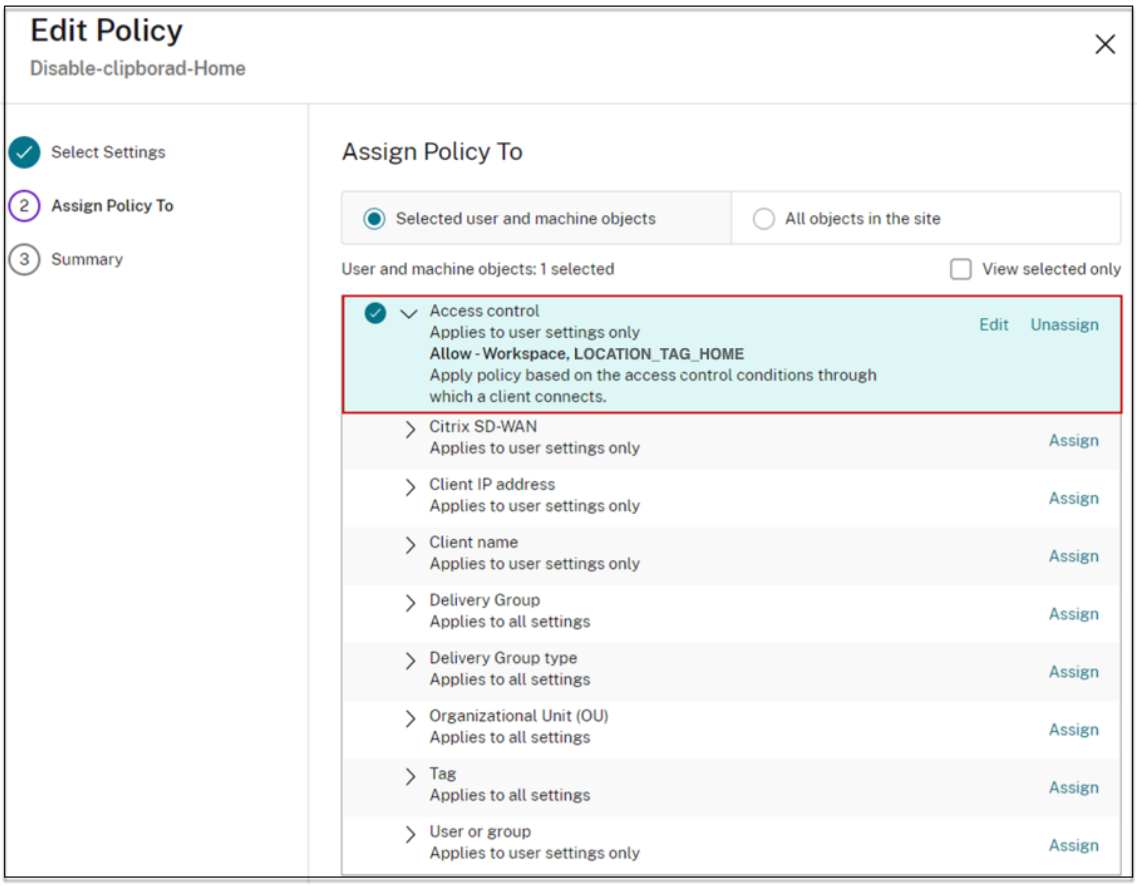
Beispiel: Benutzer, die von zu Hause aus arbeiten, dürfen keine Rechte für die Zwischenablage haben.

1. Navigieren Sie in DaaS Studio zu **Richtlinien** und klicken Sie auf **Richtlinie erstellen**.
2. Wählen Sie auf der Seite **Richtlinie erstellen** die Einstellung aus, für die Sie den Zugriff zulassen oder verbieten möchten.
3. klicken Sie auf **Auswählen**.



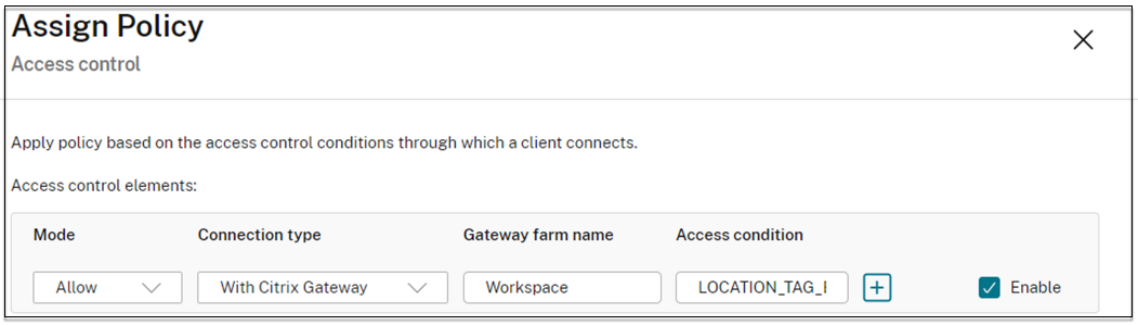
4. Klicken Sie auf der Seite **“Einstellung bearbeiten** “auf **Zulässig** oder **Verboten** und dann auf **Speichern.**
5. Klicken Sie auf **Weiter**.

6. Wählen Sie auf der Seite **Richtlinie zuweisen zu** die Option **Zugriffskontrolle** aus und klicken Sie dann auf **Weiter**.

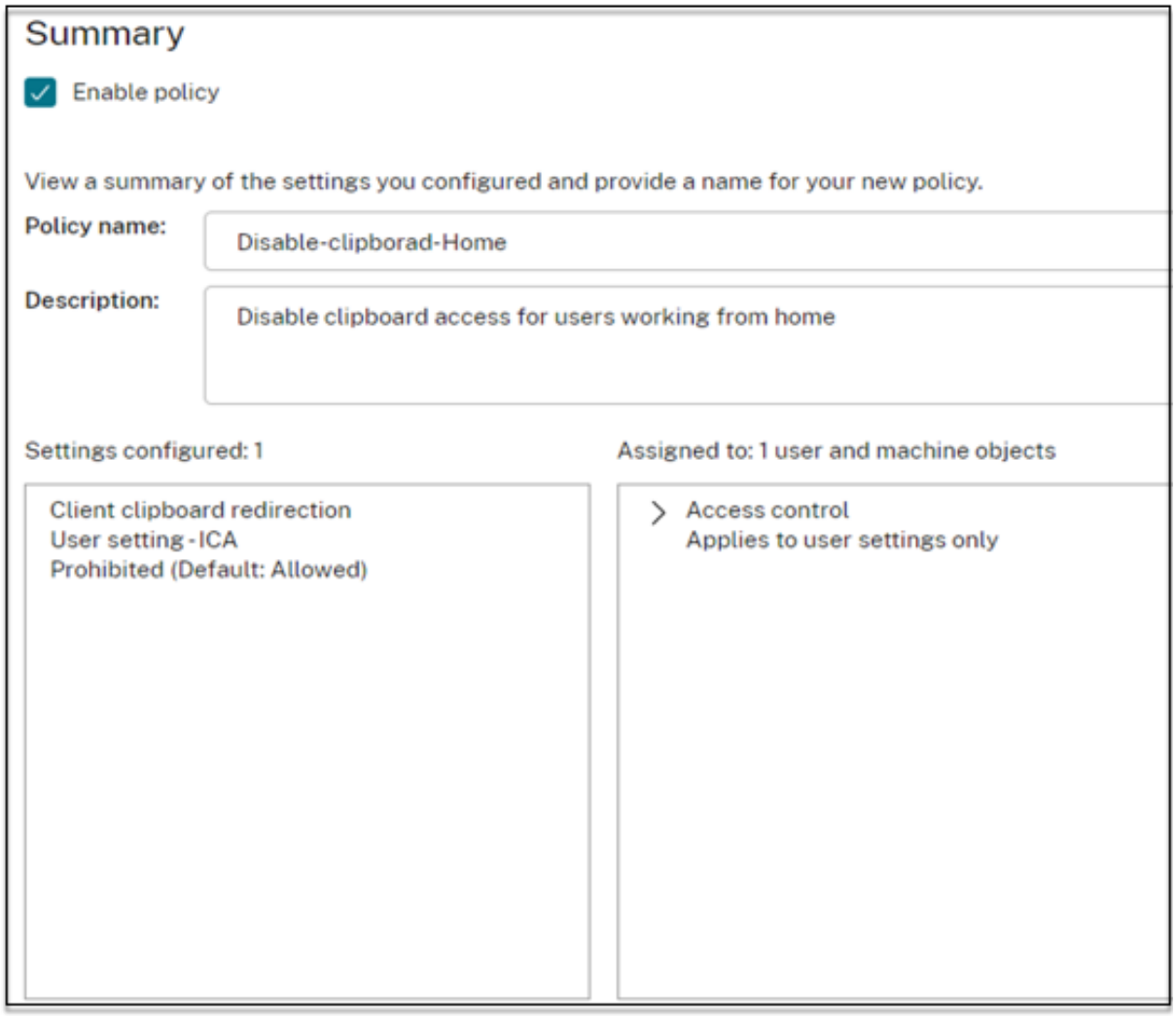


7. Definieren Sie eine Richtlinie mit den folgenden Details:

   - **Modus**: - Erlauben
   - **Verbindungstyp**: - Mit Citrix Gateway
   - **Name der Farm**: - Workspace
   - **Zugriffsbedingung**: LOCATION_TAG_HOME (alles in Großbuchstaben)



8. Klicken Sie auf **Weiter** und geben Sie einen Namen für die Richtlinie ein.
9. Klicken Sie auf **Fertigstellen**.



Sie sind jetzt bereit, Ihren Zugriff zu testen.

Behebung häufiger Fehler

- **Problem:** Sie sehen die Meldung "Ihre Anfrage kann nicht abgeschlossen werden".

  Auflösung

  1. Stellen Sie sicher, dass Adaptive Access aktiviert ist. Einzelheiten finden Sie unter Adaptiven Zugriff aktivieren.
  2. Wenn die Funktion nicht aktiviert ist, wenden Sie sich an den Citrix Support.

- **Problem:** Es werden keine Apps oder Desktops veröffentlicht.

  Dieses Problem kann auftreten, wenn die Smarttags nicht von der adaptiven Authentifizierung an den Workspace übertragen oder bei DaaS oder Secure Private Access nicht empfangen werden.

Auflösung:

- Prüfen Sie, ob Smart-Access-Richtlinien verletzt werden. Einzelheiten finden Sie unter https://support.citrix.com/article/CTX138840.
- Überprüfen Sie, ob die Citrix Adaptive Authentication-Instanz eine Verbindung herstellen kann `cas.citrix.com`.
- Einzelheiten zu den Smarttags finden Sie in der Instanz der adaptiven Authentifizierung.
  * Stellen Sie sicher, dass der LogLevel-Parameter im Befehl `set audit syslogParams` auf allen Instanzen auf `ALL` gesetzt ist.
  * Melden Sie sich mit Putty bei der primären Instanz der Adaptive Authentication an.

    Shell-Typ

    ```
    cd /var/log
    ```

    ```
    cat ns.log | more or cat ns.log | grep -I “smartaccess”
    ```
- Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den Citrix Support.

Konfigurationsänderungen für ein Hochverfügbarkeits-Setup

Manchmal kann es in einem Hochverfügbarkeits-Setup in den folgenden Verzeichnissen zu einer verzögerten Dateisynchronisierung kommen. Daher werden die Schlüssel, die während der Citrix ADM-Registrierung erstellt wurden, nicht rechtzeitig gelesen.

- /var/mastools/conf/agent.conf
- /var/mastools/trust/.ssh/private.pem
- /var/mastools/trust/.ssh/public.pem

Um das Problem mit der Dateisynchronisierung zu beheben, führen Sie die folgenden Schritte aus, um den Befehl `set cloud` auf dem sekundären Computer erneut auszuführen.

```
1  > shell cat /var/mastools/conf/agent.conf
2  <?xml version="1.0" encoding="UTF-8" standalone="no"?>
3  <mps_agent>
4  <uuid>temp_str</uuid>
5  <url>fuji.agent.adm.cloud.com</url>
6  <customerid>customer_id</customerid>
7  <instanceid>instance_id</instanceid>
8  <servicename>MAS</servicename>
9  <download_service_url>download.citrixnetworkapistaging.net</
      download_service_url>
10 <abdp_url>fuji.agent.adm.cloud.com</abdp_url>
11 <msg_router_url>fuji.agent.adm.cloud.com</msg_router_url>
12 </mps_agent> Done
```



```
13 > set cloud param -CustomerID customer_id -InstanceID instance_id -
      Deployment Production
14 <!--NeedCopy-->
```

Größen- und Leistungsrichtlinien

June 19, 2024

Adaptive Authentifizierung bietet Kunden Zugriff auf ihre on-premises Authentifizierungsserver, indem sie entweder Cloud Connectors verwenden, die in ihren Rechenzentren bereitgestellt werden, oder Azure VNet Peering, falls die Erreichbarkeit des Rechenzentrums bereits über das vom Kunden verwaltete VNet hergestellt ist. Dieses Thema enthält Informationen zu den Leistungszahlen für Citrix Cloud Connector- und Azure VNet Peering-Bereitstellungen sowie zu den empfohlenen Skalierungs- und Größenkonfigurationen für Citrix Cloud Connector-Maschinen.

Rate der Benutzerauthentifizierung

Eine virtuelle Connector-Maschine der Größe 2 vCPUs und 7 GB RAM kann 14 Benutzer/Sekunde authentifizieren.

Standardmäßig ist der Connector-Dienst so konfiguriert, dass er bei einem Ausfall oder Absturz zweimal automatisch neu gestartet wird. Bei einem nachfolgenden Ausfall oder Absturz stoppt der Dienst. Außerdem schlägt der Connector-Dienst derzeit fehl, wenn die Authentifizierungsrate über 4 Authentifizierungen/Sekunde erhöht wird. Diese Rate kann erreicht werden, indem der Connector-Dienst so konfiguriert wird, dass er nach einer beliebigen Anzahl von Fehlern neu gestartet wird (**Citrix Netscaler Cloud Gateway > Recovery > Dienst neu starten**). Wenn diese Einstellung nicht konfiguriert ist, sinkt die Rate auf 4 Authentifizierungen/Sekunde.

Verkehrslatenz und Benutzerauthentifizierungsrate bei Verwendung von Citrix Cloud Connectors

Die folgende Tabelle zeigt die Verkehrslatenz und die Benutzerauthentifizierungsrate bei Verwendung von Citrix Cloud Connectors:

Authentifizierungstyp	Authentifizierungslatenz (p95) in ms	Authentifizierungs- oder Benutzeranmelderate pro Sekunde
LDAP	5.99	14

Authentifizierungstyp	Authentifizierungslatenz (p95) in ms	Authentifizierungs- oder Benutzeranmelderate pro Sekunde
RADIUS	3.17	14
LDAP+RADIUS	4.59	14
LDAPS	26.75	14
LDAPS+RADIUS	15.61	14

Verkehrslatenz und Benutzerauthentifizierungsrate bei Verwendung von Azure VNet Peering

In der folgenden Tabelle werden die Verkehrslatenz und die Benutzerauthentifizierungsrate bei Verwendung von Azure VNet-Peering angezeigt:

Authentifizierungstyp	Anforderungslatenz (p95) in ms	Authentifizierungs- oder Benutzeranmelderate pro Sekunde
LDAP	6.95	17.54
LDAPS	7.19	16.98

Data Governance

June 19, 2024

Dieser Artikel enthält Informationen zum Sammeln, Speichern und Aufbewahren von Protokollen durch den Citrix Adaptive Authentication-Dienst und die Adaptive Authentication-Instanzen. Alle Begriffe, die nicht in Definitionen definiert sind, haben die in der Citrix Endbenutzer-Servicevereinbarungangegebene Bedeutung.

- Adaptive Authentifizierungsdienste: Citrix Cloud-Dienst, bei dem sich Administratoren anmelden können, um Adaptive Authentication-Instanzen bereitzustellen und zu verwalten.
- Adaptive Authentifizierungsinstanzen: Virtuelle NetScaler-Maschinen, die vom Adaptive Authentication-Dienst bereitgestellt werden, damit Administratoren die Benutzerauthentifizierung verwalten

Datenresidenz

Adaptive Authentifizierungsdienste

Die Kundeninhaltsdaten des Citrix Adaptive Authentication Service befinden sich in der Region Azure Cloud Services East. Sie werden aus Gründen der Verfügbarkeit und Redundanz in die folgenden Azure-Regionen repliziert:

- US West
- Nordeuropa

Im Folgenden sind die verschiedenen Ziele für die Dienstkonfiguration und die Laufzeitprotokolle aufgeführt.

- Splunk-Dienst zur Systemüberwachung und zum Debuggen von Protokollen, nur in den USA und in der EU (Europäische Union).
- NetScaler Application Delivery Management Service für die aggregierten Benutzerzugriffsprotokolle. Einzelheiten finden Sie unter NetScaler ADM Data Governance.
- Citrix Cloud System Logs-Dienst für Administratorüberwachungsprotokolle. Einzelheiten finden Sie unter Umgang mit Kundeninhalten und Protokollen von Citrix Cloud Services sowie geografische Überlegungen.

Instanzen für adaptive Authentifizierung

NetScaler Application Delivery Management Service zur Sicherung aller Konfigurationen, instanzspezifischer Artefakte. Einzelheiten finden Sie unter NetScaler ADM Data Governance.

Datensammlung

Mit dem Citrix Adaptive Authentication-Dienst können die Kundenadministratoren den Dienst über die Benutzeroberfläche der adaptiven Authentifizierung und die zugehörigen Connector-Appliances über die Konsole konfigurieren. Folgende Kundeninhalte werden gesammelt:

- Adaptive Authentifizierung
  - FQDN (vollqualifizierter Domänenname) und IP-Adresse des IdP-Endpunkts (Identitätsanbieter).
  - IP-Adressen/-bereiche, Ports und Protokolle
  - Für den Zugriff auf den virtuellen IdP-Authentifizierungsserver verwendete Zertifikate
  - Öffentliche IP-Adresse des Management-Endpunkts

  - Für Azure VNet-Peering: Dienstprinzipal mit Netzwerkbeitragsrolle. Einzelheiten finden Sie unter Einrichten der Konnektivität zu On-Premises-Authentifizierungsservern mit Azure VNet-Peering.

- Benutzerkennungen für App-Berechtigungen
- Informationen zu Citrix Cloud Connector. Weitere Informationen finden Sie unter Citrix Cloud Connector.

  - IP-Adressen oder FQDNs
  - Identifikatoren für Benutzer, Geräte und Ressourcenstandorte
  - Interne Proxykonfiguration

Für Laufzeitprotokolle, die von den Servicekomponenten gesammelt werden, bestehen die wichtigsten Informationen aus den folgenden

- IP-Adresse und Port des Clients
- Ziel-FQDN/Adresse und Port
- Kunden-Benutzer-Agent
- URL-Pfad der Anwendung
- Zugriffszeit und Dauer des Anwendungszugriffs
- Bytezahl anfordern
- Anzahl der Antwortbytes
- HTTP Transaktionsnummer
- Bereitstellungsmodus (Connector oder Azure VNet-Peering)
- Azure-Ressourcen

  - Namen von Ressourcengruppen
  - VNets (IP-Adressen, CIDRs)
  - Subnetze (IP-Adressen, CIDRs)
  - Namen virtueller Maschinen

Datenübertragung

Der Dienst Citrix Adaptive Authentication sendet Protokolle an die Ziele (Splunk), die durch die Transport Layer Security geschützt sind.

Steuerung von Daten

Der Citrix Adaptive Authentication-Dienst bietet derzeit keine Optionen, mit denen Kunden das Senden von Protokollen deaktivieren oder verhindern können, dass Kundeninhalte global repliziert werden.

Datenaufbewahrung

Basierend auf der Citrix Cloud-Datenaufbewahrungsrichtlinie werden die Kundenkonfigurationsdaten 90 Tage (ca. 3 Monate) nach Ablauf des Abonnements aus dem Dienst gelöscht.

Die Protokollziele behalten ihre dienstspezifische Datenaufbewahrungsrichtlinie bei.

- Für die in Citrix Application Delivery Management gespeicherten Ereignisse. Siehe Citrix ADM Data Governance.
- Die Splunk-Protokolle werden archiviert und schließlich nach 90 Tagen (ca. 3 Monaten) entfernt.
- Die Adaptive Authentication-Instanzen werden 30 Tage (etwa viereinhalb Wochen) nach Ablauf des Abonnements freigegeben.

Datenexport

Es gibt verschiedene Datenexportoptionen für verschiedene Arten von Protokollen.

- Auf die Administratorüberwachungsprotokolle kann über die Citrix Cloud System Log-Konsole zugegriffen werden.
- Die Splunk-Logs sind nicht für Kunden gedacht. Diese Ereignisse können auch aus Splunk als CSV-Datei exportiert werden.

Definitionen

- Kundeninhalt bezeichnet alle Daten, die zur Speicherung in ein Kundenkonto hochgeladen werden, oder Daten in einer Kundenumgebung, auf die Citrix Zugriff zur Ausführung der Dienste erhält.
- Protokoll bezeichnet eine Aufzeichnung von Ereignissen mit Bezug zu den Services, darunter Messdaten zu Leistung, Stabilität, Nutzung, Sicherheit und Unterstützung.
- Dienste bedeuten, dass die zuvor beschriebenen Citrix Cloud-Dienste zur Erleichterung der Anwendungsfälle des Kunden verwendet werden.