リリースノート

Adaptive Authentication のリリースノートは、NetScaler のリリースノートのサブセットです。Adaptive Authentication のお客様は、Adaptive Authentication サービスにおける機能強化、修正された問題、および既知の問題について知るために、NetScaler のリリースノート を使用する必要があります。

2026年10月

以下のセクションでは、2026年10月リリースに関する詳細情報を提供します。

新機能

- **セキュリティアップデート**

  Adaptive Authentication インスタンスは、CTX697191 で説明されているセキュリティ脆弱性に対処するビルド 14.1–73.46 以降に自動アップグレードされます。

  Adaptive Authentication サービスのこのリリースにおける機能強化、修正された問題、および既知の問題に関する詳細については、NetScaler のリリースノート を参照してください。

- **セキュリティアップデート**

  Adaptive Authentication インスタンスは、CTX697174 で説明されているセキュリティ脆弱性に対処するビルド 14.1–73.41 以降に自動アップグレードされます。

  Adaptive Authentication サービスのこのリリースにおける機能強化、修正された問題、および既知の問題に関する詳細については、NetScaler のリリースノート を参照してください。

2026年9月

以下のセクションでは、2026年9月リリースに関する詳細情報を提供します。

新機能

- **セキュリティアップデート**

  Adaptive Authentication インスタンスは、CTX697096 で説明されているセキュリティ脆弱性に対処するビルド 14.1–73.37 以降に自動アップグレードされます。

Adaptive Authentication サービスのこのリリースにおける機能強化、修正された問題、および既知の問題の詳細については、NetScaler リリースノート を参照してください。

2026 年 8 月

以下のセクションでは、2026 年 8 月のリリースに関する詳細情報を提供します。

新機能

- **セキュリティ更新**

  Adaptive Authentication インスタンスは、CTX696939 で説明されているセキュリティ脆弱性に対処するビルド 14.1–73.33 以降に自動アップグレードされます。

  Adaptive Authentication サービスのこのリリースにおける機能強化、修正された問題、および既知の問題の詳細については、NetScaler リリースノート を参照してください。

2026 年 6 月

以下のセクションでは、2026 年 6 月のリリースに関する詳細情報を提供します。

新機能

- **セキュリティ更新**

  Adaptive Authentication インスタンスは、CTX696604 で説明されているセキュリティ脆弱性に対処するビルド 14.1–72.61 以降に自動アップグレードされます。

  Adaptive Authentication サービスのこのリリースにおける機能強化、修正された問題、および既知の問題の詳細については、NetScaler リリースノート を参照してください。

2026 年 3 月

以下のセクションでは、2026年3月リリースに関する詳細情報を提供します。

新機能

- **セキュリティアップデート**

  Adaptive Authenticationインスタンスは、CTX696300に記載されているセキュリティ脆弱性に対処するビルド14.1–66.59以降に自動アップグレードされます。

- **Adaptive Authenticationインスタンス用のLASライセンス**

Adaptive Authenticationインスタンスは、LASベースのライセンスに自動的に再ライセンスされます。この変更により、エンタイトルメントのプレミアムクォータで割り当てられたNetScaler VPX数から2つのVPXと、100 Mbpsの帯域幅が消費されます。

Adaptive Authenticationサービスのこのリリースにおける機能強化、修正された問題、および既知の問題の詳細については、NetScalerリリースノートを参照してください。

2025年11月

以下のセクションでは、2025年11月リリースに関する詳細情報を提供します。

新機能

- **セキュリティアップデート**

  Adaptive Authenticationインスタンスは、CTX695486に記載されているセキュリティ脆弱性に対処するビルド14.1–56.73以降に自動アップグレードされます。

  Adaptive Authenticationサービスのこのリリースにおける機能強化、修正された問題、および既知の問題の詳細については、NetScalerリリースノートを参照してください。

2025年6月

以下のセクションでは、2025年6月リリースに関する詳細情報を提供します。

新機能

- **セキュリティ更新**

  Adaptive Authenticationインスタンスは、CTX693420およびCTX694788で説明されているセキュリティ脆弱性に対処するビルド14.1–47.46以降に自動アップグレードされます。

  Adaptive Authenticationサービスのこのリリースにおける機能強化、修正された問題、および既知の問題の詳細については、NetScalerリリースノートを参照してください。

修正された問題

- メモリリークにより利用可能なメモリが徐々に枯渇すると、NetScaler®は応答しなくなり、アクセスできなくなる可能性があります。

2024年10月

以下のセクションでは、2024年10月リリースについて詳しく説明します。

新機能

- **セキュリティ更新**

  Adaptive Authenticationインスタンスは、CTX691608で説明されているセキュリティ脆弱性に対処するビルド14.1–34.101以降に自動アップグレードされます。

  Adaptive Authenticationサービスのこのリリースにおける機能強化、修正された問題、および既知の問題の詳細については、NetScalerリリースノートを参照してください。

- **RADIUSの負荷分散サポート**

  Citrix Adaptive Authenticationインスタンスは現在、RADIUSによる負荷分散をサポートしています。詳細については、RADIUS負荷分散構成の例を参照してください。

- **オンプレミスsyslogサーバーへのログのトンネリングのサポート**

  Adaptive Authenticationの展開では、お客様はデータセンター内のsyslogサーバーにログを送信できるようになりました。syslogサーバーを構成する際は、プライベートクラスIPアドレス（RFC1918）を使用してください。追加の構成は不要です。

2024年1月

以下のセクションでは、2024年1月リリースに関する詳細情報を提供します。

新機能

- **セキュリティ更新**

  Adaptive Authenticationインスタンスは、CTX584986で説明されているセキュリティ脆弱性に対処するビルド14.1–12.35以降に自動アップグレードされます。

  Adaptive Authenticationサービスのこのリリースにおける機能強化、修正された問題、および既知の問題の詳細については、NetScalerリリースノートを参照してください。

2023年9月

以下のセクションでは、2023年9月リリースに関する詳細情報を提供します。

新機能

- **セキュリティ更新**

  Adaptive Authenticationインスタンスは、CTX579459で説明されているセキュリティ脆弱性に対処するビルド14.1–8.50以降に自動アップグレードされます。

  Adaptive Authenticationサービスのこのリリースにおける機能強化、修正された問題、および既知の問題の詳細については、NetScalerリリースノートを参照してください。

2023年7月

以下のセクションでは、2023年7月リリースに関する詳細情報を提供します。

新機能

- **セキュリティ更新**

  Adaptive Authenticationインスタンスは、CTX561482で説明されているセキュリティ脆弱性に対処するビルド13.1–49.101以降に自動アップグレードされます。

  Adaptive Authenticationサービスのこのリリースにおける機能強化、修正された問題、および既知の問題の詳細については、NetScalerリリースノートを参照してください。

2023年4月

以下のセクションでは、2023年4月リリースに関する詳細情報を提供します。

新機能

- **ロードバランシングによるLDAPおよびLDAPSのサポート**

  Citrix Adaptive Authenticationインスタンスは、ロードバランシング仮想サーバーを使用してLDAPおよびLDAPSをサポートします。詳細については、LDAPおよびLDAPSロードバランシング構成の例を参照してください。

- **バックエンドADまたはRADIUSサーバーのサブネットとリソースロケーションのマッピング**

  管理者は、バックエンドADおよびRADIUSサーバーに到達するために使用するコネクタを選択できます。詳細については、Adaptive Authenticationのプロビジョニングを参照してください。

修正済みの問題

- 適応型認証用に構成されたスマートアクセス ポリシーとOAuth認証ポリシーが、NetScaler GUIに表示されません。

既知の問題

- 適応型認証インスタンスの場合、LDAPプロファイル（NetScaler管理GUI）で「**接続テスト**」オプションを使用して接続性を確認すると、実際には到達できないにもかかわらず、LDAPサーバーが到達可能であると誤って表示されます。

Adaptive Authentication サービスを構成する

Adaptive Authentication サービスを構成するには、次の手順を実行します。

1. Adaptive Authentication をプロビジョニングする
2. Adaptive Authentication ポリシーを構成する
3. Adaptive Authentication を有効にする

Adaptive Authentication サービスを構成する方法

Adaptive Authentication ユーザーインターフェイスにアクセスする

以下のいずれかの方法で Adaptive Authentication ユーザーインターフェイスにアクセスできます。

- URL `<https://adaptive-authentication.cloud.com>` を手動で入力します。
- 資格情報を使用してログインし、顧客を選択します。

  認証が正常に完了すると、Adaptive Authentication ユーザーインターフェイスにリダイレクトされます。

または

- **Citrix Cloud™ > IDおよびアクセス管理** に移動します。
- タブの で、省略記号メニューをクリックし、 を選択します。

Adaptive Authentication ユーザーインターフェイスが表示されます。

次の図は、アダプティブ認証の設定に関わる手順を示しています。

メインページのプロビジョニング(/en-us/adaptive-authentication/media/adaptive-authentication-provisioning-main-page1.png)

> **注:**

- いずれのアダプティブ認証インスタンスに対しても、クリア設定を実行しないでください。
- プレフィックス `AA` を持つ設定（例：AAuthAutoConfig）は、証明書を含め、変更しないでください。これにより、アダプティブ認証の管理が中断され、ユーザーアクセスに影響が出ます。
- アダプティブ認証インスタンスはSNIP設定を必要としません。
- 顧客のセットアップでプロキシが設定されている場合、アダプティブ認証インスタンスはトンネルの確立に失敗します。したがって、アダプティブ認証のプロキシ設定を無効にすることをお勧めします。
- SAMLなどのサードパーティ認証サービスを使用している場合、すべてのクレームが見つからないと認証が失敗する可能性があります。したがって、すべてのクレームを渡すために、多要素認証設定でNOAUTHなどの追加要素を追加することをお勧めします。

前提条件

- 適応型認証のプロビジョニングのアクセスを要求します。詳細については、「クラウドネイティブ条件付き認証とNetscalerベースの適応型認証の比較」を参照してください。
- 適応型認証インスタンスのFQDNを予約します。たとえば、`xyz.com` が会社のドメインであると仮定すると、`aauth.xyz.com` です。このFQDNは、このドキュメントでは適応型認証サービスFQDNと呼ばれ、インスタンスのプロビジョニング時に使用されます。FQDNをIdP仮想サーバーのパブリックIPアドレスにマッピングします。このIPアドレスは、プロビジョニング後、「**証明書のアップロード**」ステップで取得されます。
- aauth.xyz.com の証明書を調達します。証明書にはSAN属性が含まれている必要があります。そうでない場合、証明書は受け入れられません。
- 適応型認証UIは、証明書バンドルのアップロードをサポートしていません。中間証明書をリンクするには、「中間証明書の構成」を参照してください。
- タイムスキューを回避するために、ネットワークタイムプロトコル（NTP）サーバーを構成します。詳細については、「ネットワーク上のサーバーとシステムクロックを同期する方法」を参照してください。

適応型認証インスタンスのプロビジョニング

重要:

適応型認証サービスに関心のあるお客様は、以下のスクリーンショットに示すリンクをクリックし、フォームを完了する必要があります。その後、Citrix 適応型認証チームが適応型認証インスタンスのプロビジョニングを有効にします。

プロビジョニング

1. **Adaptive Authentication** UIで、**プロビジョニング**をクリックします。
2. Adaptive Authenticationの推奨される接続として、**Citrix Cloud Connector™**を選択します。

   接続の種類(/en-us/adaptive-authentication/media/adaptive-authentication-step11.png)

   この接続の種類の場合、オンプレミスネットワークにコネクタをセットアップする必要があります。Citrixは、AzureでホストされているCitrix Gatewayへの接続をセットアップするために、環境に少なくとも2つのCitrix Cloud Connectorを展開することを推奨します。Adaptive Authenticationインスタンス用に予約したドメイン/URLにCitrix Cloud Connectorがアクセスできるようにする必要があります。例: `<https://aauth.xyz.com/*>`を許可します。Citrix Cloud Connectorのプロビジョニングには、セットアップに最大30分かかる場合があります。

   注:

   コネクタ接続タイプの場合、プロビジョニング後、Adaptive Authentication FQDNがコネクタ仮想マシンから到達可能であることを確認してください。

   Citrix Cloud Connectorの詳細については、Citrix Cloud Connectorを参照してください。
3. **次へ**をクリックして、コンソールアクセスセクションに進みます。

コンソールアクセス

アダプティブ認証を有効にしたインスタンスにアクセスするための資格情報を設定します。認証、条件付きアクセスなどのポリシーを作成するには、管理コンソールアクセスが必要です。

1. 「**コンソールアクセス**」画面で、ユーザー名とパスワードを入力します。

   注記：

> 「**コンソールアクセス**」画面から作成されたユーザーには、シェルアクセス権を持つ「SuperUser」権限が付与されます。



2. **次へ**をクリックして、「証明書のアップロード」セクションに進みます。

証明書のアップロード

> **注：**

> 証明書のアップロード設定は、NetScaler® 上で直接（GUI または CLI を使用して）行うのではなく、アダプティブ認証ポータルのユーザーインターフェイスを通じて行うことをお勧めします。NetScaler で行われた変更は、アダプティブ認証ポータルと自動的に同期されず、失われる可能性があります。

1. アダプティブ認証サービスの FQDN を追加し、証明書とキーのペアをアップロードします。公開アクセス可能な認証サーバーには、選択したアダプティブ認証サービスの FQDN を入力する必要があります。この FQDN は、公開で解決可能である必要があります。
   a. **証明書のアップロード**画面で、アダプティブ認証用に予約した FQDN を入力します。
   b. 証明書の種類を選択します。
      - アダプティブ認証サービスは、インスタンスのプロビジョニングのために PFX、PEM、DER タイプの証明書をサポートしています。
      - 証明書バンドルは、PEM タイプの証明書のみサポートされています。その他のバンドルタイプの場合、Citrix® はルート証明書と中間証明書をインストールし、それらをサーバー証明書にリンクすることを推奨します。
   c. 証明書とキーをアップロードします。

> **注：**

> - 中間証明書をアダプティブ認証インスタンスにインストールし、サーバー証明書にリンクします。

a. アダプティブ認証インスタンスにログインします。

b. **Traffic Management > SSL** に移動します。 詳細については、「中間証明書の構成」を参照してください。

- 公開証明書のみが受け入れられます。プライベートまたは不明な CA によって署名された証明書は受け入れられません。
- 証明書の設定または証明書の更新は、アダプティブ認証 UI のみを使用して行う必要があります。インスタンスで直接変更しないでください。不整合が発生する可能性があります。



2. 証明書とキーをアップロードします。

   証明書のアップロードが成功すると、アダプティブ認証サービスはIDPとしてCitrix Cloud™に自動的に接続します。アダプティブ認証サービスのステータスは、**IDおよびアクセス管理** UIから確認できます。



3. 「次へ」をクリックして、許可されたIPアドレスセクションに移動します。

許可されたIPアドレス

Adaptive Authenticationサービスでは、Adaptive Authentication NetScaler®管理コンソールにアクセスするために、最大15個のパブリックIPサブネットと個々のIPアドレスを入力できます。

IPアドレス/サブネットを入力する際の注意点:

- パブリックIPサブネットのCIDRが/20から/32.Bの間であることを確認してください。
- エントリ間に重複がないことを確認してください。

例:

- 192.0.2.8は192.0.2.0/24の範囲内にあるため、192.0.2.0/24と192.0.2.8は受け入れられません。
- 重複するサブネット: 192.0.2.0/24と192.0.0.0/20は、サブネットが重複しているため受け入れられません。
- ネットワークサブネット値を入力する際は、ネットワークIPアドレスをIPアドレス値として入力してください。

例:

- 192.0.2.2/24は正しくありません。代わりに191.0.2.0/24を使用してください。
- 192.0.2.0/20は正しくありません。代わりに192.0.0.0/20を使用してください。

1. Adaptive Authentication管理コンソールにアクセスできるIPアドレスを設定します。
   a. **許可されたIPアドレス**画面で、インスタンスごとにパブリックIPアドレスを管理IPアドレスとして入力します。管理IPアドレスへのアクセスを制限するには、管理コンソールへのアクセスが許可されている複数のIPアドレスを追加できます。
   b. 複数のIPアドレスを追加するには、**追加**をクリックし、IPアドレスを入力してから**完了**をクリックする必要があります。これはすべてのIPアドレスに対して行う必要があります。**完了**ボタンをクリックしない場合、IPアドレスはデータベースに追加されず、ユーザーインターフェイスにのみ追加されます。

   許可されたIPアドレス(/en-us/adaptive-authentication/media/adaptive-authentication-allowed-ip-addresses1.png)
2. 「**次へ**」をクリックして、「接続管理」セクションに進みます。

接続管理

ADまたはRADIUSサーバーに到達できる一連のリソースロケーション（コネクタ）を指定できます。管理者は、バックエンドのADおよびRADIUSサーバーに到達するために使用するリソースロケーションを選択できます。

この機能を有効にするには、顧客はバックエンドのAD/RADIUSサーバーサブネット間のマッピングを設定し、認証トラフィックが特定のサブネットに属する場合、そのトラフィックが特定のリソースロケーションに転送されるようにします。ただし、リソースロケーションがサブネットにマッピングされていない場合、管理者はそれらのサブネットにワイルドカードリソースロケーションを使用するように指定できます。

> **注:**
>
> 接続管理設定は、NetScaler® (GUIまたはCLIを使用) で直接行うのではなく、Adaptive Authenticationポータルのユーザーインターフェイスを介して実行することをお勧めします。NetScalerで行われた変更は、Adaptive Authenticationポータルと自動的に同期されず、失われる可能性があります。

1. Adaptive Authentication UIで、**接続管理**をクリックします。
2. サブネットの詳細を入力し、該当するリソースロケーションを選択します。

> **注:**
>
> **残りのサブネットに利用可能なリソースロケーションを使用**チェックボックスをオフにすると、構成されたサブネットに向けられたトラフィックのみがトンネルされます。

3. **追加**をクリックし、次に**変更を保存**をクリックします。

> **注:**
>
> - RFC1918 IPアドレスサブネットのみが許可されます。
> - 顧客あたりのサブネットとリソースロケーションのマッピング数は10に制限されています。
> - 複数のサブネットを単一のリソースロケーションにマッピングできます。
> - サブネットエントリを更新するには、既存のエントリを削除してから更新します。
> - リソースロケーションの名前を変更または削除する場合は、Adaptive Authenticationユーザーインターフェイスの**接続管理**画面からエントリを削除してください。
> - 以下のCLIコマンドを使用してリソースロケーションマッピングに加えられた変更は、ユーザーインターフェイス（**Adaptive Authentication Provisioning > Manage Connectivity**）からプッシュされた変更によって上書きされます。
>
>   > ◦ set cloudtunnel parameter -subnetResourceLocationMappings
>   > ◦ set policy expression aauth_allow_rfc1918_subnets <>
>   > ◦ set policy expression aauth_listen_policy_exp <>

4. インスタンス管理セクションに進むには、**次へ**をクリックします。

インスタンス管理

Adaptive Authenticationチームは、Adaptive Authenticationインスタンスのすべてのアップグレードとメンテナンスを管理します。したがって、Adaptive Authenticationインスタンスをランダムな RTMビルドにアップグレードまたはダウングレードしないことをお勧めします。Citrix®は、デフォルトでAdaptive Authenticationインスタンスを管理します。

インスタンスのアップグレードには、VARディレクトリに最低7 GBの空き容量が必要です。そのため、Adaptive Authenticationサービスチームは、アップグレードを適用する前にインスタンスのディスクスペースをクリアします。以下のディレクトリには、機密情報、専有情報、または個人情報を保管しないことをお勧めします。

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

> **注:**

> - アップグレード中に、まず/var/nsinstallディレクトリがクリアされ、次に/var/tmpディレクトリがクリアされます。それでも最小スペース要件が満たされない場合は、他のディレクトリ（/var/core、/var/crash、/var/nstracem、および/var/nslog）もクリアされます。
> - NetScaler®のディスクスペースの管理とディスククリーンアップは、お客様の責任です。

> **ディスクスペースを自分で管理するオプション:**

CitrixはデフォルトでAdaptive Authenticationインスタンスを管理しますが、インスタンスのディスクスペースを自分でクリーンアップすることもできます。デフォルトの方法からオプトアウトするには、次の手順を実行します。

1. Adaptive Authenticationナビゲーションペインで、 をクリックします。
2. 「**ディスク領域を自分で管理する**」を選択し、確認メッセージダイアログボックスで「**確認**」をクリックします。
3. 「**変更を保存**」をクリックします。

ディスク領域の管理(/en-us/adaptive-authentication/media/adaptive-auth-manage-disk-space.png)

注:

顧客のトラフィックに応じてアップグレードをスケジュールすることもできます。その後、Citrix Cloud™チームがそれに応じてインスタンスをアップグレードします。 アップグレードのスケジュール設定については、「アダプティブ認証インスタンスのアップグレードをスケジュールする」を参照してください。

ポリシーを構成する

Adaptive Authentication NetScaler®インスタンス（OAuth、スマートアクセス、syslogなど）のすべてのポリシーは、Adaptive Authenticationインスタンスで構成されます。

注:

- LDAPまたはRADIUSアクションのデフォルトのタイムアウトは3秒に設定されています。タイムアウトを15秒に増やすことをお勧めします。
- RADIUSサーバーの展開では、すべてのコネクタプライベートIPアドレスをRADIUSサーバーのRADIUSクライアントとして追加します。

Adaptive Authenticationインスタンスへの接続方法:

プロビジョニング後、Adaptive Authentication管理IPアドレスに直接アクセスできます。FQDNまたはプライマリIPアドレスを使用して、Adaptive Authentication管理コンソールにアクセスできます。

重要:

FQDNを使用してAdaptive Authentication管理コンソールにアクセスするには、ADC管理UIアクセス用のSSLを構成するを参照してください。

Adaptive Authentication管理コンソールにアクセスする:

- プライマリIPアドレスを使用してAdaptive Authenticationにアクセスするには、次の手順を実行します。

  a. GUIの**認証ポリシーの構成**セクションからプライマリIPアドレスをコピーし、ブラウザでそのIPアドレスにアクセスします。

  b. プロビジョニング時に入力した資格情報を使用してログインします。

  c. **続行**をクリックします。

  d. **構成 > セキュリティ > AAA - アプリケーション トラフィック > 仮想サーバー**に移動します。

  e. 認証ポリシーを追加します。さまざまなユースケースについては、LDAP および LDAPS 負荷分散構成の例および認証構成の例を参照してください。

LDAPおよびLDAPSロードバランシング構成の例

シトリックス アダプティブ認証インスタンスは、ロードバランシング仮想サーバーを使用してLDAP/LDAPSサポートを提供します。

注:

- LDAP/LDAPSにロードバランシングを使用していない場合は、Adaptive Authenticationトンネルが破損する可能性があるため、LDAPサーバーのサービスまたはサーバーを作成しないでください。
- LDAPにロードバランシングを使用している場合は、サービスグループを作成し、スタンドアロンサービスではなくロードバランシングサービスにバインドしてください。
- 認証にロードバランシング仮想サーバーを使用する場合は、LDAPアクションで実際のLDAPサーバーIPアドレスの代わりにロードバランシング仮想サーバーIPアドレスを追加してください。
- デフォルトでは、作成したサービスにTCPモニターがバインドされます。Adaptive Authentication NetScaler®インスタンスでは、TCPモニターが使用されている場合、サービスはデフォルトでUPとしてマークされます。
- 監視には、カスタムモニターを使用することをお勧めします。

前提条件

ロードバランシング仮想サーバーのプライベートIPアドレス（RFC1918アドレス）。このアドレスは内部構成に使用されるため、ダミーIPアドレスでも構いません。

LDAPサーバーのロードバランシング

LDAPサーバーのロードバランシングを行うには、サービスグループを作成し、ロードバランシング仮想サーバーにバインドします。LDAPサーバーのロードバランシング用のサービスは作成しないでください。

NetScaler CLIを使用してLDAPを構成する:

LDAPを構成するための参照として、以下のCLIコマンドを使用できます。

1. `add serviceGroup <serviceGroupName> <serviceType>`
2. `bind servicegroup <serviceGroupName> (<IP> | <serverName>) <port>`
3. `add lb vserver <name> <serviceType> <ip> <port>` - ポートは389である必要があります。このポートは内部通信に使用され、オンプレミスサーバーへの接続は、サービスグループに設定されたポートに基づいてSSL経由で行われます。
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`

NetScaler GUIを使用してLDAPを構成する:

1. **Traffic Management > Load Balancing** に移動し、次に **Virtual Servers** をクリックします。
2. タイプTCPでポート389の仮想サーバーを作成します。

   タイプSSL/SSL_TCPの負荷分散仮想サーバーは作成しないでください。
3. **Traffic Management > Load Balancing** に移動し、次に **Service Groups** をクリックします。
4. タイプTCPでポート389のサービスグループを作成します。
5. ステップ1で作成した仮想サーバーにサービスグループをバインドします。

手順の詳細については、基本的な負荷分散のセットアップを参照してください。

LDAPSサーバーの負荷分散

LDAPSサーバーの負荷分散を行うには、Adaptive Authenticationインスタンスへの内部SSL暗号化または復号化を避けるため、TCPタイプの負荷分散仮想サーバーを作成する必要があります。この場合、負荷分散仮想サーバーがTLSの暗号化/復号化を処理します。SSLタイプの負荷分散仮想サーバーは作成しないでください。

NetScaler CLIを使用してLDAPSを構成する:

LDAPSを構成するための参考として、以下のCLIコマンドを使用できます。

1. `add lb vserver <name> <serviceType> <ip> <port>` - ポートは636である必要があります。
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`

NetScaler GUIを使用してLDAPSを構成する:

1. **Traffic Management > Load Balancing** に移動し、**Virtual Servers** をクリックします。
2. タイプTCP、ポート636の仮想サーバーを作成します。

   タイプSSL/SSL_TCPの負荷分散仮想サーバーは作成しないでください。
3. **Traffic Management > Load Balancing** に移動し、**Service** をクリックします。
4. タイプSSL_TCP、ポート636のサービスを作成します。
5. ステップ1で作成した仮想サーバーにサービスをバインドします。

手順の詳細については、基本ロードバランシングのセットアップを参照してください。

カスタムモニターの作成

NetScaler GUIを使用してカスタムモニターを作成します。

1. **トラフィック管理 > ロードバランシング > モニター** に移動します。
2. LDAPタイプのモニターを作成します。モニタープローブ間隔を15秒、応答タイムアウトを10秒に設定してください。

3. このモニターをサービスにバインドします。

詳細については、カスタムモニターを参照してください。

RADIUS負荷分散構成の例

Citrix Adaptive Authenticationインスタンスは、負荷分散仮想サーバーを使用してRADIUSをサポートします。

注:

- RADIUSに負荷分散を使用しない場合は、Adaptive Authenticationトンネルが破損する可能性があるため、RADIUSサーバーのサービスまたはサーバーを作成しないでください。
- RADIUSに負荷分散を使用する場合は、サービスグループを作成し、RADIUSサーバーをそれにバインドします。
- 認証に負荷分散仮想サーバーを使用する場合は、RADIUSアクションで実際のRADIUSサーバーIPアドレスの代わりに負荷分散仮想サーバーIPアドレスを追加するようにしてください。
- デフォルトでは、作成したサービスにpingモニターがバインドされます。Adaptive Authentication NetScaler®インスタンスでは、pingモニターを使用してもサービスは起動しません。RADIUSモニターを作成し、作成したサービスグループにバインドする必要があります。
- 監視には、カスタムモニターを使用することをお勧めします。
- Pingモニターはサポートされていません。RADIUSモニターを作成する必要があります。

前提条件

負荷分散仮想サーバーのプライベートIPアドレス（RFC1918アドレス）。このアドレスは内部構成に使用されるため、ダミーIPアドレスでも構いません。

RADIUSサーバーの負荷分散

RADIUSサーバーの負荷分散には、サービスグループを作成し、それを負荷分散仮想サーバーにバインドします。RADIUSサーバーの負荷分散のためにサービスを作成しないでください。

NetScaler CLIを使用してRADIUSを構成する

RADIUSを構成するための参照として、以下のCLIコマンドを使用できます。

1. `add serviceGroup <serviceGroupName> <serviceType>`
2. `bind servicegroup <serviceGroupName> (<IP> | <serverName>) <port>`
3. `add lb vserver <name> <serviceType> <ip> <port>`
4. `bind lb vserver <name> <serviceGroupName>`
5. `add authentication radiusAction <name> {-serverIP} <ip_addr> | {-serverName <string>}} <lb vserver ip>`
6. `add authentication policy <radius_policy_name> -rule <expression> -action <string>`
7. `bind authentication vserver auth_vs -policy <radius_policy_name> -priority <radius_policy_priority> -gotoPriorityExpression NEXT`

NetScaler GUI を使用して RADIUS を構成する

1. **Traffic Management > Load Balancing** に移動し、**Virtual Servers** をクリックします。
2. タイプが **RADIUS** の仮想サーバーを作成します。
3. **Traffic Management > Load Balancing** に移動し、**Service Groups** をクリックします。
4. タイプが **RADIUS** のサービスグループを作成します。
5. ステップ 1 で作成した仮想サーバーにサービスグループをバインドします。

手順の詳細については、「基本的な負荷分散のセットアップ」を参照してください。

NetScaler GUI を使用してカスタムモニターを作成する

1. **トラフィック管理 > 負荷分散 > モニター**に移動します。
2. RADIUSタイプのモニターを作成します。モニタープローブ間隔を15秒に、応答タイムアウトを10秒に設定してください。
3. このモニターをサービスグループにバインドします。

詳細については、カスタムモニターを参照してください。

サンプル認証構成

顧客は、任意の認証ポリシーを設定し、それを認証仮想サーバーにバインドできます。認証仮想サーバーには認証プロファイルのバインディングは必要ありません。認証ポリシーのみを設定できます。以下にいくつかのユースケースを示します。

> **重要:**

> 認証構成はプライマリノードでのみ実行する必要があります。

条件付き認証による多要素認証

- デュアルファクタスキーマを使用したLDAPおよびRADIUSによる二要素認証（ユーザー入力は1回のみ）
- 組織内のユーザーの部署（従業員、パートナー、ベンダー）に応じた認証ログオン方法（部署を選択するためのドロップダウンメニュー付き）
- ドロップダウンメニュー付きのユーザーのドメインに応じた認証ログオン方法
- 最初の要素としてメールID（またはユーザー名）入力を設定し、最初の要素でメールIDを使用したグループ抽出に基づく条件付きアクセスを行い、各グループに異なるログオンタイプを提供する
- ユーザー証明書を持つユーザーには証明書認証を、非証明書ユーザーにはネイティブOTP登録を使用した多要素認証
- ユーザーのホスト名入力に応じた条件付き認証による異なる認証タイプ
- ネイティブOTP認証による二要素認証

多要素認証とのサードパーティ統合

- Azure ADをSAML IdPとして構成（次の要素をLDAPポリシー - NO_AUTHとして構成し、OAuth信頼を完了）
- 最初の要素をSAMLとし、SAML属性に基づいて証明書またはLDAPへのカスタムログインを行う条件付き認証
- Web認証ログインを第一要素とし、その後にLDAP

デバイスポスチャスキャン (EPA)

- バージョンチェックのためのデバイスポスチャチェック、その後に準拠ユーザー (RADIUS) および非準拠ユーザー (LDAP) 向けのカスタマイズされたログイン
- LDAP認証、その後に必須のデバイスポスチャスキャン
- AD認証の前後にデバイスポスチャチェック - 要素としての事前および事後EPA
- EPA要素としてのデバイス証明書

その他のシナリオ

- 認証とともにEULAを追加
- nFactorポリシーラベル、ログインスキーマのカスタマイズ

カスタムストアURLのサポート

カスタムストアURLを使用すると、選択したドメインを使用してクラウドストアにアクセスできます。ユーザーは、クラウドストアURL、カスタムストアURL、またはその両方を使用してアクセスできます。

カスタムURLを構成するには、以下を実行する必要があります。

1. カスタムドメインを構成します。詳細については、「カスタムドメインの構成」を参照してください。
2. 現在のプロファイルまたはデフォルトのプロファイル (AAuthAutoConfig_oauthIdpProf) と同じクライアントID、シークレット、およびオーディエンスを持つ新しいOAuthIDPプロファイルを構成しますが、リダイレクトURLは異なるものにします。詳細については、「OAuthポリシーとプロファイルの構成」を参照してください。

   例:

   現在のプロファイル:

   ```
   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
   ```

   新しいプロファイル:

   ```
   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_Custom1 -priority 101 -gotoPriorityExpression
NEXT
```

重要:

- OAuthポリシーとプロファイルは、プロビジョニングフェーズ中に適応型認証サービスによって作成されます。その結果、Citrix Cloud管理者は暗号化されていないクライアントシークレットにアクセスできません。暗号化されたシークレットはns.confファイルから取得できます。OAuthプロファイルを作成するには、暗号化されたシークレットを使用し、CLIコマンドのみを使用してプロファイルを作成する必要があります。
- NetScaler®ユーザーインターフェイスを使用してOAuthプロファイルを作成することはできません。

アダプティブ認証を使用したスマートアクセスへの対応

Citrix Cloud™ のお客様は、アダプティブ認証をクラウドストアへのIdPとして使用することで、Citrix DaaSリソース（仮想アプリおよびデスクトップ）またはSecure Private Accessサービスへのスマートアクセス（アダプティブアクセス）を提供できます。

スマートアクセス機能により、アダプティブ認証サービスはユーザーに関するすべてのポリシー情報をCitrix DaaSに提供できます。アダプティブ認証サービスは、デバイスの姿勢（EPA）、ネットワークロケーション（企業ネットワーク内または外、地理的位置）、ユーザーグループなどのユーザー属性、時刻、またはこれらのパラメーターの組み合わせをポリシー情報の一部として提供できます。Citrix DaaS管理者は、このポリシー情報を使用して、仮想アプリおよびデスクトップへのコンテキストアクセスを構成できます。仮想アプリおよびデスクトップは、以前のパラメーター（アクセスポリシー）に基づいて列挙される場合とされない場合があります。クリップボードアクセス、プリンターリダイレクト、クライアントドライブ、USBマッピングなどの一部のユーザーアクションも制御できます。

使用例：

- 管理者は、企業ネットワークなどの特定のネットワークロケーションからのみ表示またはアクセスされるアプリのグループを構成できます。
- 管理者は、企業が管理するデバイスからのみ表示またはアクセスされるアプリのグループを構成できます。たとえば、EPAスキャンは、デバイスが企業管理デバイスかBYODかをチェックできます。EPAスキャン結果に基づいて、関連するアプリをユーザーに列挙できます。

前提条件

- クラウドストアの認証方法としてアダプティブ認証を構成します。詳細については、「アダプティブ認証サービス」を参照してください。
- Citrix DaaSと連携するアダプティブ認証サービスが稼働していること。
- アダプティブアクセス機能が有効になっていること。詳細については、「アダプティブアクセスを有効にする」を参照してください。

スマートアクセスのイベントフローを理解する

1. ユーザーはクラウドストアにログインします。
2. ユーザーは、IdPとして構成されたアダプティブ認証サービスにリダイレクトされます。
3. ユーザーは事前認証（EPA）または認証を求められます。
4. ユーザーは正常に認証されます。
5. スマートアクセス ポリシーは構成に従って評価され、タグはユーザーセッションに関連付けられます。
6. Adaptive Authentication サービスはタグを Citrix Graph サービスにプッシュします。ユーザーはストアのランディングページにリダイレクトされます。
7. StoreFront Cloud はこのユーザーセッションのポリシー情報をフェッチし、フィルターに一致させ、列挙する必要があるアプリまたはデスクトップを評価します。
8. 管理者は、ユーザーの ICA® アクセスを制限するために、Citrix DaaS でアクセス ポリシーを構成します。

Adaptive Authentication インスタンスでのスマートアクセス ポリシーの構成

Adaptive Authentication インスタンスでスマートアクセス ポリシーを構成するには、2つのステップがあります。

1. Adaptive Authentication インスタンスでスマートアクセス タグを使用してスマートアクセス ポリシーを定義します。例については、「*ステップ1*」を参照してください。
2. リソースアクセス用に、DaaS/Secure Private Access で同じタグを定義します。例については、「*ステップ2*」を参照してください。

ユースケース 1: Chrome ブラウザからログインするユーザーへのアクセスを許可し、クリップボードアクセスをブロックするスマートアクセス ポリシーを構成する

ステップ1: Adaptive Authentication インスタンスでスマートタグを使用してスマートアクセス ポリシーを構成する:

1. Adaptive Authentication インスタンスにログインします。
2. アダプティブ認証仮想サーバー (**Security > AAA - Application Traffic > Virtual Servers**) に移動します。
3. 認証仮想サーバーを選択し、**Edit** をクリックします。
4. **Smart Access Policies** をクリックします。
5. 要件に応じてポリシーの式を定義します。

    a. **Add Binding** をクリックします。

    b. **Select Policy** で、**Add** をクリックします。

    c. スマートアクセスポリシーの名前を入力します。

    d. 式を定義します。

    Chromeブラウザからログインするユーザーへのアクセスを許可する例として、式 `HTTP.REQ.HEADER("User-Agent").CONTAINS("Chrome")` を入力します。

    同様に、時間、ユーザーログイン、認証および承認グループ、その他のオプションに基づいて式を作成できます。

    

6. 次に、スマートタグを作成し、これらのタグをスマートアクセスポリシーにバインドします。

    a. **Action** で、**Add** をクリックします。

    b. **Name** で、スマートアクセスプロファイルの名前を入力します。

    c. **Tags** でスマートアクセスタグを定義します。例として、TAG-CHROME。

    

    a. **Create** をクリックします。

    b. スマートアクセスポリシーを選択し、**Add Binding** をクリックします。

    c. このスマートアクセスタグを、以前に作成したスマートアクセスポリシーにバインドします。

    

> **注:**

> **Security >AAA - Application Traffic > Policies > Authentication > Advanced Policies > Smart Access > Policies** からスマートアクセスポリシーを作成し、認証仮想サーバーにバインドすることもできます。

> **ステップ2：DaaS Studioでスマートアクセスタグを定義する:**

1. スマートタグ「TAG-CHROME」でポリシーを追加します。詳細については、「Citrix Studioでタグを定義する」を参照してください。

ユースケース2：認証後のEPA結果に基づいてスマートアクセスポリシーを構成する

ステップ1：Adaptive Authenticationインスタンスでスマートタグを使用してスマートアクセスポリシーを構成する:

エンドポイント分析などの条件に基づくスマートアクセスの場合、nFactorフローを構成し、EPAアクションを定義してから、デフォルトグループを追加します。

nFactorフローでEPAを要素として構成するには、「EPAを要素として構成する」を参照してください。

論理フロー:

1. ユーザーはWebブラウザまたはCitrix Workspaceアプリでストアurlを開きます。
2. ユーザーは認証/EPAのためにAdaptive Authenticationにリダイレクトされます。
3. エンドユーザーに対してエンドポイント分析が実行され、ユーザーを定義されたデフォルトグループに追加することで結果が保存されます。
4. ユーザーは次の認証フローを求められます。
5. スマートアクセスポリシーが評価され、ユーザーにスマートアクセスタグが割り当てられます。

設定:

アンチウイルスがインストールされているマシンからアクセスするユーザーは、準拠としてマークされ、フルアクセスが提供される必要があります。ただし、アンチウイルスがインストールされていないユーザーのマシンは、非準拠としてマークされ、制限付きアクセスが提供される必要があります。

1. EPA 用の nFactor ポリシーを作成します。詳細については、EPA を要素として構成するを参照してください。

   nFactor フローでは、最初の要素がユーザー認証要素であることを確認してください。

2. アンチウイルスが存在するかどうかを確認するために、EPA 式を選択します。
3. EPA アクションでデフォルトグループを定義します。

   EPA が正常に実行された場合、ユーザーはこのデフォルトグループに追加されます。
4. 次に、スマートアクセスポリシーを作成します。

   a. Adaptive Authentication インスタンスにログインします。
   b. Adaptive Authentication 仮想サーバーに移動します (**セキュリティ > AAA - アプリケーショントラフィック > 仮想サーバー**)。
   c. Adaptive Authentication 仮想サーバーを選択し、**編集**をクリックします。
   d. **スマートアクセスポリシー**をクリックします。
   e. 次の式を使用して、2つのスマートアクセスポリシーを作成します。

      - AAA.USER.IS_MEMBER_OF (“Compliant”) - ユーザーの EPA 合格条件の場合
      - !AAA.USER.IS_MEMBER_OF (“Compliant”) – ユーザーのEPA失敗条件の場合

   f. これら両方のポリシーに対してスマートアクセスタグを定義します。

      例:

      - `AAA.USER.IS_MEMBER_OF (“Compliant”)` の場合、タグ名 `SmartTag1` にタグ COMPLIANT を付けます
      - `!AAA.USER.IS_MEMBER_OF (“Compliant”)` の場合、タグ名 `SmartTag2` にタグ NONCOMPLIANT を付けます

スマートアクセス用のEPAを条件とするアダプティブ認証インスタンスの設定が完了しました。

要件に応じてタグと式を設定できます。

ステップ2: DaaS Studioでスマートアクセスタグを構成する:

スマートタグ「COMPLIANT」と「NONCOMPLIANT」を付けて、それぞれのデリバリーグループにポリシーを追加します。詳細については、Citrix Studioでタグを定義するを参照してください。

DaaS Studioでタグを定義する

ユーザーのアプリケーション列挙を制限するために、デリバリーグループでタグを定義します。

例: BranchOfficeユーザーは、すべてのアプリケーションを含む**Adaptive Access Delivery group**からのアプリケーションを見る必要があります。 一方、WorkfromHomeユーザーは**WFH Delivery Group**からのアプリケーションを見る必要があります。

1. Citrix Cloudにサインインします。
2. **マイサービス > DaaS**を選択します。
3. 「**管理**」をクリックします。
4. 要件に応じてデリバリーグループを作成します。詳細については、「デリバリーグループの作成」を参照してください。
5. 作成したデリバリーグループを選択し、「**デリバリーグループの編集**」をクリックします。



6. 「**アクセスポリシー**」をクリックします。
7. Citrix Workspaceプラットフォーム内でアダプティブアクセスを使用しているお客様は、デリバリーグループのアクセスを内部ネットワークのみに制限するために、次の手順を実行します。

   a. デリバリーグループを右クリックし、「**編集**」を選択します。
   b. 左ペインでアクセスポリシーを選択します。
   c. 編集アイコンをクリックして、デフォルトのCitrix Gateway接続ポリシーを変更します。
   d. ポリシーの編集ページで、「**次の条件を満たす接続**」を選択し、「**いずれかに一致**」を選択してから、条件を追加します。



   在宅勤務ユーザーの場合は、それぞれのデリバリーコントローラーに次の値を入力します。

   ファーム: Workspace

   フィルター: LOCATION_TAG_HOME

   支社ユーザーの場合は、それぞれのデリバリーコントローラーに次の値を入力します。

   フィルター: ワークスペース

   値: LOCATION_TAG_BRANCHOFFICE

これらのタグを使用して、アプリケーションへのアクセスを制限できるようになりました。

提供されたアプリケーションのアクセスタイプを制限する

例: 在宅勤務のユーザーはクリップボードの権限を持つべきではありません。

1. DaaS Studio で、**ポリシー**に移動し、**ポリシーの作成**をクリックします。
2. **ポリシーの作成**ページで、アクセスを許可または禁止する設定を選択します。
3. **選択**をクリックします。



4. **設定の編集**ページで、**許可**または**禁止**をクリックし、**保存**をクリックします。
5. **次へ**をクリックします。
6. **ポリシーの割り当て先**ページで、**アクセス制御**を選択し、**次へ**をクリックします。



7. 次の詳細でポリシーを定義します。
   - **モード**: - 許可
   - **接続タイプ**: - Citrix Gatewayを使用
   - **ファーム名**: - Workspace
   - **アクセス条件**: LOCATION_TAG_HOME (すべて大文字)



8. **次へ**をクリックし、ポリシーの名前を入力します。
9. **完了**をクリックします。



これで、アクセスのテストの準備が整いました。

一般的なエラーのトラブルシューティング

- **問題:** 「Cannot Complete your Request」というメッセージが表示されます。

  解決策

  a. Adaptive Accessが有効になっていることを確認してください。詳細については、「Adaptive Accessを有効にする」を参照してください。

  b. 機能が有効になっていない場合は、Citrixサポートにお問い合わせください。

- **問題:** アプリまたはデスクトップが公開されていません。

この問題は、スマートタグがAdaptive Authenticationからワークスペースにプッシュされていないか、DaaSまたはSecure Private Accessで受信されていない場合に発生する可能性があります。

解決策:

- スマートアクセスポリシーが適用されているか確認します。詳細については、<CTX138840を参照してください。
- Citrix Adaptive Authenticationインスタンスが`cas.citrix.com`に接続できるか確認します。
- スマートタグの詳細については、Adaptive Authenticationインスタンスを確認してください。
  - `set audit syslogParams`コマンドで、すべてのインスタンスのlogLevelパラメータが`ALL`に設定されていることを確認してください。
  - puttyを使用してAdaptive Authenticationプライマリインスタンスにログインします。

    shellと入力します

    `cd /var/log`

    `cat ns.log | more or cat ns.log | grep -I “smartaccess”`
- これらで問題が解決しない場合は、Citrixサポートにお問い合わせください。

高可用性セットアップの構成変更

高可用性セットアップでは、以下のディレクトリでファイル同期が遅延する場合があります。その結果、Citrix ADM登録中に作成されたキーが時間通りに読み取られません。

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

ファイル同期の問題に対処するため、セカンダリで`set cloud`コマンドを再実行するには、次の手順を実行します。

```
> shell cat /var/mastools/conf/agent.conf

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
```

```
<mps_agent>

<uuid>temp_str</uuid>

<url>fuji.agent.adm.cloud.com</url>

<customerid>customer_id</customerid>

<instanceid>instance_id</instanceid>

<servicename>MAS</servicename>

<download_service_url>download.citrixnetworkapistaging.net</
download_service_url>

<abdp_url>fuji.agent.adm.cloud.com</abdp_url>

<msg_router_url>fuji.agent.adm.cloud.com</msg_router_url>

</mps_agent> Done

> set cloud param -CustomerID customer_id -InstanceID instance_id
-Deployment Production
```

アダプティブ認証を有効にする

プロビジョニングが完了したら、**Enable Adaptive Authentication for Workspace**セクションで**Enable**をクリックして、クラウドストアの認証を有効にできます。

注：

これにより、アダプティブ認証の設定が完了します。エンドユーザーがストアにアクセスすると、アダプティブ認証のFQDNにリダイレクトされます。

認証方法をアダプティブ認証に移行する

認証方法として**Citrix Gateway**を使用してアダプティブ認証をすでに利用しているお客様は、**アダプティブ認証**を移行し、アダプティブ認証インスタンスからOAuth構成を削除する必要があります。

1. Citrix Gateway以外の別の認証方法に切り替えます。
2. **Citrix Cloud™ > Identity and Access Management**で、Citrix Gatewayに対応する省略記号ボタンをクリックし、**Disconnect**をクリックします。

   ゲートウェイを切断する(/en-us/adaptive-authentication/media/adaptive-authentication-different-authentication-method.png)
3. **I understand the impact on the subscriber experience**を選択し、**Confirm**をクリックします。

   Confirmをクリックすると、アダプティブ認証が再度有効になるまで、アダプティブ認証は認証に使用されません。
4. アダプティブ認証インスタンス管理コンソールで、OAuth関連の構成を削除します。

   CLIを使用する場合：

   ```
   unbind authentication vs <authvsName> -policy <oauthIdpPolName>

   rm authentication oauthIdpPolicy <oauthIdpPolName>

   rm authentication oauthIdpProfile <oauthIdpProfName>
   ```

   GUIを使用する場合：

   a. **Security > AAA - Application Traffic > Virtual Servers** の画面に移動します。
   b. OAuthポリシーをアンバインドします。
   c. **セキュリティ > AAA - アプリケーショントラフィック > ポリシー > 認証 > 高度なポリシー > OAuth IDP** に移動します。
   d. OAuthポリシーとプロファイルを削除します。
5. **Citrix Cloud > Identity and Access Management**に移動します。 Authenticationタブの Adaptive Authenticationで、省略記号メニューをクリックし、**Manage**を選択します。

   または `<https://adaptive-authentication.cloud.com>` にアクセスします
6. をクリックします。

7. 画面で、次の操作を行います。

   - Adaptive Authentication FQDNを追加します。
   - 証明書とキーファイルを削除し、再度アップロードします。

   > **重要:**
   >
   > **Adaptive Authentication** に移行せずにFQDNまたは証明書とキーのペアを直接編集すると、Identity and Access Management への接続が失敗し、次のエラーが表示されます。これらのエラーを修正するには、Adaptive Authentication メソッドに移行する必要があります。
   >
   > - ADCコマンドがエラーで失敗しました。ポリシーはすでに指定された優先度にバインドされています。
   > - ADCコマンドがエラーで失敗しました。バインドされていないポリシーをアンバインドすることはできません。

8. をクリックします。

   この時点で、Identity and Access Management は **Adaptive Authentication** を **Connected** と表示し、Adaptive Authentication インスタンスにはOAuthプロファイルが自動構成されます。

   これはGUIから検証できます。

   a. Adaptive Authentication インスタンスにアクセスし、資格情報を使用してログインします。
   b. **> >** に移動します。OAuth IdPプロファイルが作成されていることを確認する必要があります。
   c. **Citrix Cloud > Identity and Access Management** に移動します。アダプティブ認証は**接続済み**ステータスです。

9. アダプティブ認証のホームページで、**有効にする**（ステップ3）をクリックして、アダプティブ認証方法を再度有効にします。

   認証を有効にする(/en-us/adaptive-authentication/media/adaptive-authentication-enable.png)

この手順により、クラウドストアに対して認証方法がアダプティブ認証として有効になります。

10. **有効にする**をクリックした後、ステップ3のStoreFront Cloudリンクをクリックします。認証方法がアダプティブ認証に変更されていることを確認する必要があります。

> **注:**
>
> 新規ユーザーは、OAuth関連の構成を削除する手順を除いて、同じ手順に従う必要があります。

Adaptive Authenticationインスタンスのアップグレードとメンテナンス

Adaptive Authenticationインスタンスのすべてのアップグレードとメンテナンスは、Citrix Cloudチームによって管理されます。Adaptive Authenticationインスタンスを任意のRTMビルドにアップグレードまたはダウングレードしないことをお勧めします。お客様のトラフィックに応じてアップグレードをスケジュールできます。詳細については、「Adaptive Authenticationインスタンスのアップグレードをスケジュールする」を参照してください。その後、Citrix Cloudチームがお客様のインスタンスを適切にアップグレードします。

重要:

- Citrix Cloud™チームは、インスタンスへの通信を定期的にチェックします。切断が発生した場合、Adaptive Authenticationサポートチームがインスタンスの管理を再開するために連絡する場合があります。インスタンス管理の問題が解決されない場合、Adaptive Authenticationチームはアップグレードを管理できません。その結果、脆弱なバージョンを実行することになる可能性があります。
- 資格の有効期限とディスク領域の使用状況の詳細に関するメールを受信するには、メール通知を有効にすることをお勧めします。詳細については、「通知」を参照してください。
- Adaptive AuthenticationインスタンスのアップグレードはCitrixによって管理されるため、お客様はアップグレードのためにVARディレクトリに十分なスペース（最低7 GB）があることを確認する必要があります。VARディレクトリのスペースを解放する方法の詳細については、「VARディレクトリのスペースを解放する方法」を参照してください。
- 高可用性ステータスをENABLEDからSTAY PRIMARYまたはSTAY SECONDARYに変更しないでください。Adaptive Authenticationでは、高可用性ステータスはENABLEDである必要があります。
- Adaptive Authenticationインスタンスのユーザー（authadmin）のパスワードを変更しないでください。パスワードが変更された場合、Adaptive Authenticationチームはアップグレードを管理できません。

Adaptive Authenticationインスタンスのアップグレードをスケジュールする

現在のサイトまたは展開の場合、アップグレードのメンテナンス期間を選択できます。

> **重要：**
>
> Adaptive Authenticationインスタンスをランダムなビルドにアップグレードしないでください。すべてのAdaptive Authenticationインスタンスのアップグレードは Citrix によって管理されます。

1. **Adaptive Authentication** UIで、**Adaptive Authenticationインスタンスのプロビジョニング**セクションにある省略記号ボタンをクリックします。



2. **アップグレードのスケジュール**をクリックします。
3. アップグレードの日時を選択します。



バックアップと復元を設定する

NetScaler Consoleサービスは、Adaptive Authenticationインスタンスのバックアップ管理を実行します。詳細については、NetScalerインスタンスのバックアップと復元を参照してください。

> **注:**
>
> サービスがオンボードされていない場合は、NetScaler Consoleサービスをオンボードしてください。詳細については、はじめにを参照してください。

Adaptive Authenticationインスタンスのプロビジョニング解除

お客様は、次のケースで、またCitrix®サポートからの提案に従って、Adaptive Authenticationインスタンスのプロビジョニングを解除できます。

- Adaptive Authenticationインスタンスにアクセスできない場合 (特にスケジュールされたアップグレード後)。ただし、このシナリオは発生しない可能性があります。
- お客様がVNetピアリングモードからコネクタモードへ、またはその逆に切り替える必要がある場合。
- お客様がVNetピアリングモードのプロビジョニング時に誤ったサブネットを選択した場合 (そのサブネットがデータセンターまたはAzure VNet内の他のサブネットと競合する場合)。

> **注：**

> プロビジョニング解除すると、インスタンスの構成バックアップも削除されます。したがって、Adaptive Authenticationインスタンスのプロビジョニングを解除する前に、バックアップファイルをダウンロードして保存する必要があります。

> Adaptive Authenticationインスタンスのプロビジョニングを解除するには、以下を実行します。

1. **Adaptive Authentication** UIの**Adaptive Authenticationインスタンスのプロビジョニング**セクションで、省略記号ボタンをクリックします。

   

2. **プロビジョニング解除**をクリックします。

   > **注：**

   > プロビジョニング解除する前に、**Citrix Gateway**をStoreFront Cloudから切断する必要があります。

3. 顧客IDを入力して、Adaptive Authenticationインスタンスのプロビジョニングを解除します。



セキュアな管理アクセス

> **重要:**

- Adaptive Authenticationインスタンスのプロビジョニングが完了していることを確認してください。詳細については、「Adaptive Authenticationのプロビジョニング」を参照してください。
- WindowsでPuTTYを使用してAdaptive Authenticationインスタンスに接続する場合は、ダウンロードした秘密鍵をPEMに変換する必要があります。
- MACのターミナルまたはWindows (バージョン10) のPowerShell/コマンドプロンプトからAdaptive Authenticationインスタンスに接続するには、次のコマンドを使用することをお勧めします。

```
ssh -i &lt;path-to-private-key> authadmin@&lt;ip address of ADC>
```

- ADユーザーがAdaptive Authentication GUIにアクセスできるようにするには、新しい管理者としてLDAPグループに追加する必要があります。詳細については、「CTX123782」を参照してください。
- その他のすべての構成については、Citrix®はCLIコマンドではなくAdaptive Authentication GUIを使用することをお勧めします。

ゲートウェイへのセキュアなアクセスを有効にする

1. **Adaptive Authentication** UIで、省略記号ボタンをクリックします。
2. **セキュアな管理アクセス**をクリックします。



3. **キーの有効期限**で、新しいSSHキーの有効期限を選択します。
4. **キーの生成とダウンロード**をクリックします。 SSH秘密鍵は、ページを閉じると表示されなくなるため、後で使用するためにコピーまたはダウンロードしてください。このキーは、ユーザー名`authadmin`でAdaptive Authenticationインスタンスにログインするために使用できます。

   以前のキーペアの有効期限が切れた場合は、**キーの生成とダウンロード**をクリックして新しいキーペアを作成できます。ただし、アクティブにできるキーペアは1つだけです。
5. **完了**をクリックします。

アダプティブ認証FQDNの更新

アダプティブ認証サービスをプロビジョニングする際に作成した構成を更新または編集できます。「**Provision Adaptive Authentication instances**」タブで「**See Details**」をクリックし、「**Edit**」をクリックして設定を更新します。

アダプティブ認証インスタンスの更新(/en-us/adaptive-authentication/media/update-aa-instances.png)

FQDNの編集

StoreFront Cloudで認証方法として**アダプティブ認証**が選択されている場合、FQDNを編集することはできません。FQDNを編集するには、別の認証方法に切り替える必要があります。ただし、必要に応じて証明書を編集することはできます。

> **重要:**
>
> - FQDNを変更する前に、新しいFQDNがIdP仮想サーバーのパブリックIPアドレスにマッピングされていることを確認してください。
> - OAuthポリシーを使用して**Citrix Gateway**に接続している既存のユーザーは、認証方法を**アダプティブ認証**に移行する必要があります。詳細については、「認証方法をアダプティブ認証に移行する」を参照してください。

FQDNを編集するには、次の手順を実行します。

1. **アダプティブ認証**から別の認証方法に切り替えます。

   認証方法の切り替え(/en-us/adaptive-authentication/media/adaptive-authentication-adaptive-authentication-connected.png)
2. 「**サブスクライバーエクスペリエンスへの影響を理解しています**」を選択し、「**確認**」をクリックします。

   「**確認**」をクリックすると、エンドユーザーへのワークスペースログインに影響があり、アダプティブ認証が再度有効になるまで、アダプティブ認証は認証に使用されません。したがって、メンテナンス期間中にFQDNを変更することをお勧めします。
3. 「**証明書のアップロード**」画面で、FQDNを変更します。

   FQDNの編集(/en-us/adaptive-authentication/media/adaptive-authentication-edit-fqdn.png)

4. 「**変更を保存**」をクリックします。

> **重要:**
>
> FQDNを編集した場合、証明書を再度アップロードする必要があります。

5. アダプティブ認証のホームページで、「**有効にする**」をクリックして（ステップ3）、アダプティブ認証メソッドを再度有効にします。



6. 「**更新**」をクリックします。

アダプティブ認証証明書の更新

アダプティブ認証サービスポータルで、**証明書のアップロード**タブから新規または更新された証明書をアップロードすることをお勧めします。このポータルからアップロードされた証明書は、`/nsconfig/ssl/`フォルダに「tenant-id.pfx」というデフォルト名で保存されます。この証明書を指すSSL証明書キーが、「-certkey」という名前で自動的に作成されます。デフォルトのバインドポイント（auth_vsおよびVPNグローバル）も、新しい証明書キーで自動的に更新されます。

この証明書キーを、Security Assertion Markup Language (SAML) やロードバランシング (LB) など、他の目的で使用してはなりません。証明書キーがデフォルトのバインドポイント（auth_vsおよびVPNグローバル）以外で使用されている場合、アダプティブ認証サービスポータルから証明書をアップロードする際に「failed to update certkey」エラーが発生する可能性があります。



このエラーを解決するには、他のバインドポイントから証明書キーを手動で削除し、証明書を再アップロードする必要があります。

証明書キーがLB仮想サーバーで使用されている場合にエラーを解決するための手順の例を以下に示します。

1. まだ不明な場合は、「-certkey」という証明書キーが使用されているすべてのバインドポイントを特定します。
    - Secure Shell (SSH) を使用してNetScaler®のプライマリノードにログインし、次のコマンドを実行します。

```
sh runn | grep [tenant-id]-certkey
```

次の画像では、デフォルトのバインドポイント（auth_vsおよびVPNグローバル）に加えて、証明書キーはLB仮想サーバーにもバインドされています。



2. LB仮想サーバーから証明書キーのバインドを解除します。詳細については、「CLIを使用して仮想サーバーからSSL証明書キーペアのバインドを解除する」を参照してください。
3. アダプティブ認証サービスポータルから証明書を再アップロードします。詳細については、「証明書のアップロード」を参照してください。



4. 新しい証明書キー（同じ名前「-certkey」）をLB仮想サーバーに再バインドします。詳細については、「証明書キーペアをSSL仮想サーバーにバインドする」を参照してください。

アダプティブ認証の問題をトラブルシューティングする

問題は、構成のさまざまな段階に基づいて分類されます。

- プロビジョニング
- インスタンスのアクセシビリティの問題
- AD/RADIUS接続および認証の問題
- 認証の問題
- EPA/デバイスポスチャ関連の問題
- スマートタグ関連の問題
- ログ収集

アダプティブ認証CLIを使用して問題をトラブルシューティングすることもできます。CLIに接続するには、次の手順を実行します。

- お使いのマシンにputty/securecrtのようなSSHクライアントをダウンロードします。
- 管理IP（プライマリ）アドレスを使用してアダプティブ認証インスタンスにアクセスします。
- 資格情報を使用してログインします。

詳細については、NetScalerアプライアンスへのアクセスを参照してください。

アダプティブ認証ログのロギングを有効にする

アダプティブ認証ログをキャプチャするために、ログレベルを有効にしてください。

> **注：**
>
> 通常の操作中はデバッグログレベルを無効にしておき、必要な場合にのみ有効にしてください。デバッグログレベルが常に有効になっていると、管理CPUの使用率が高くなる可能性があります。これにより、高トラフィック負荷時にシステムクラッシュが発生する可能性があります。詳細については、CTX222945を参照してください。

> **CLIを使用してログを有効にする：**

1. アダプティブ認証インスタンスのCLIにログインします。
2. PuTTYを使用して、管理資格情報を入力します。
3. コマンド `set audit syslogParams logLevel ALL` を実行します。

GUIを使用してログを有効にする：

1. ブラウザを使用してアダプティブ認証インスタンスにログインします。
2. **Configuration > System > Auditing**に移動します。
3. ページで、**Settings**の下にある**Change Auditing syslog Settings**をクリックします。
4. **Log Levels**で、**ALL**を選択します。

プロビジョニングの問題

- **アダプティブ認証UIにアクセスできません**

  お客様の顧客ID/テナントに対してエンタイトルメントが有効になっているかどうかを確認します。

- **プロビジョニングページで45分以上スタックしている**

  エラーのスクリーンショットがあれば収集し、Citrixサポートに連絡して支援を求めてください。

- **VNetピアがダウンしている**

  - Azure Portalでこのピアリングに対応するアラートがあるか確認し、推奨されるアクションを実行してください。
  - ピアリングを削除し、Adaptive Authentication UIから再度追加してください。

- **デプロビジョニングが完了していない**

  Citrixサポートに連絡して支援を求めてください。

インスタンスのアクセシビリティの問題

- **インスタンスの管理IPアドレスにアクセスできない**

  - アクセスに使用されているクライアントのパブリックIPアドレスが、許可された送信元IPアドレスに含まれているか確認してください。

    - クライアントの送信元IPアドレスを変更するプロキシがないか検証してください。

- **インスタンスにログインできない**

  プロビジョニング時に入力した資格情報で管理者アクセスが正常に機能していることを確認してください。

- **エンドユーザーが完全な権限を持っていない**

  ユーザーを追加する際に、アクセスに適したコマンドポリシーをバインドしていることを確認してください。詳細については、「ユーザー、ユーザーグループ、およびコマンドポリシー」を参照してください。

AD または RADIUS 接続の問題

Azure Vnet ピアリング接続タイプに関する問題:

- 顧客が管理する Azure VNet がアダプティブ認証インスタンスから到達可能であることを確認します。
- 顧客が管理する Azure VNet から AD への接続/到達可能性が機能していることを確認します。
- オンプレミスから Azure VNet へのトラフィックをルーティングするために、適切なルートが追加されていることを確認します。

Windows ベースのコネクタ:

- すべてのログはディレクトリ /var/log/ns.log にあり、各ログには がプレフィックスとして付加されています。
- ログの ConnectionID を使用して、異なるトランザクションを関連付けることができます。
- コネクタ仮想マシンのプライベート IP アドレスが RADIUS サーバーの RADIUS クライアントの1つとして追加されていることを確認してください。その IP アドレスがコネクタのソース IP アドレスとなるためです。

  すべての認証要求に対して、アダプティブ認証インスタンス (NS - AAAD プロセス) と認証サーバー間にトンネルが確立されます。トンネルが正常に確立されると、認証が行われます。

  コネクタ仮想マシンがアダプティブ認証 FQDN を解決できることを確認してください。

- コネクタはインストールされていますが、オンプレミス接続に失敗します。

  NSAUTH-TUNNEL が確立されているかどうかを検証します。

  `cat ns.log | grep -I “tunnel”`

認証要求に対して以下のサンプルログが ns.log ファイルに出力されない場合、トンネルの確立中に問題が発生しているか、コネクタ側に何らかの問題がある可能性があります。

```
LDAP:

[NS_AAUTH_TUNNEL] Entering bitpump for

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"

RADIUS:

[NS_AAUTH_UDP_TUNNEL] MUX channel established"
```

ログの詳細を確認し、適切に対応します。

ログの詳細	是正措置
`[NS_AAUTH_TUNNEL]` のプレフィックスを持つログがログファイルに含まれていません	`show cloudtunnel vserver` コマンドを実行します。このコマンドは、状態が「UP」のクラウドトンネル仮想サーバー（TCPとUDPの両方）を一覧表示する必要があります。
`[NS_AAUTH_TUNNEL] Waiting for outbound from connector` このログの場合、次の応答が受信されない場合: `[NS-AAUTH-TUNNEL] Received connect command from connector and client connection lookupsucceeded"`	コネクタマシンがAdaptive Authentication FQDNに到達できることを確認するか、**または** Adaptive Authentication FQDNへのアウトバウンド接続についてコネクタ側のファイアウォールを確認します
`[NS_AAUTH_TUNNEL] Server is down or couldn't create connection to ip 0.0.0.0` および `[NS_AAUTH_TUNNEL] Connect response code 401 is not 200 OK, bailing out"`	Citrixサポートにお問い合わせください。

コネクタからの応答なし:

- Adaptive Authentication FQDNがコネクタ仮想マシンから到達可能であることを確認してください。

- Adaptive Authenticationインスタンスで、中間証明書がサーバー証明書にバインドされ、リンクされていることを確認してください。

LDAP/RADIUS設定が正しくありません:

AD/RADIUSサーバーのIPアドレスがパブリックIPアドレスである場合、NetScalerの式にサブネットまたはIPアドレスを追加する必要があります。既存の範囲は編集しないでください。

- CLIを使用してサブネットまたはIPアドレスを追加するには:

```
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))"
```

- GUIを使用してサブネットまたはIPアドレスを追加するには：

  a. **Appexpert > Expressions** に移動します。

  b. 式 **aauth_allow_rfc1918_subnets** を追加します。

トンネルが確立されていても認証が失敗する場合は、次の手順で問題をトラブルシューティングしてください。

LDAP:

- バインドDNの詳細を検証します。
- テスト接続を使用してエラーを確認します。
- `aaad` デバッグを使用してエラーを検証します。
- CLIを使用してアダプティブ認証インスタンスにログインします。

```
shell

cd /tmp

cat aaad.debug
```

一般的なLDAPエラー:

- サーバータイムアウト – LDAPクエリに対してコネクタからの応答がありません。

- その他のLDAPエラーについては、CTX138663 を参照してください。

ラディウス:

- コネクタのIPアドレスは、RADIUSサーバー設定でRADIUSクライアントの送信元IPアドレスとして追加する必要があります。

認証に関する問題

- **OAuth のアサーション後エラー**
  - すべてのクレームが AD によって提供されていることを確認してください。これを成功させるには、7つのクレームが必要です。
  - /var/log/ns.log のログを検証して、OAuth 障害のエラーを特定します。

```
cat /var/log/ns.log
```

  - OAuth プロファイルパラメータを検証します。
- **アサーション後に停止する Azure AD 認証**

  認証をオフに設定して、AD 認証を次の要素として追加します。これは、認証を成功させるために必要なすべてのクレームを取得するためです。

EPA 関連の問題

- **プラグインは既に存在しますが、ユーザーにプラグインのダウンロードを促すプロンプトが表示されます。**

  考えられる原因：バージョン不一致またはファイル破損
  - 開発者ツールを実行し、プラグインリストファイルに NetScaler® およびクライアントマシンと同じバージョンが含まれているかどうかを検証します。
  - NetScaler 上のクライアントバージョンがクライアントマシン上のバージョンと同じであることを確認してください。

    NetScaler 上のクライアントを更新します。

    Adaptive Authentication インスタンスで、**Citrix Gateway > Global Settings > Update client libraries** に移動します。

Citrix Downloads の EPA プラグインライブラリページには、詳細情報が記載されています。

- バージョンが更新されていても、リクエストが NetScaler にキャッシュされることがあります。

  `show cache object` はキャッシュされたプラグインの詳細を表示します。コマンドを使用して削除できます。

  `flush cache object -locator 0x00000023345600000007`

EPAログ収集の詳細については、CTX209148を参照してください。

- **ユーザーがオプションを選択した後で、EPA設定 (常に、はい、いいえ) を元に戻す方法はありますか。**

  現在、EPA設定の復元は手動で行われます。

  - クライアントマシンで、C:\Users\<user_name>\AppData\Local\Citrix\AGEE に移動します。
  - `config.js` ファイルを開き、trustAlways を null に設定します - `"trustAlways":null`

スマートアクセスタグの問題

- **スマートアクセスを構成した後、アプリケーションが利用できません**

  タグがアダプティブ認証インスタンスとCitrix VDAデリバリーグループの両方で定義されていることを確認してください。

  タグがデリバリーグループにすべて大文字で追加されていることを確認してください。

  これが機能しない場合は、ns.log を収集してCitrixサポートに連絡してください。

アダプティブ認証インスタンスの一般的なログ収集

- テクニカルサポートバンドル: 詳細については、SDXおよびVPXアプライアンスからインサイト分析用のテクニカルサポートバンドルを収集する方法を参照してください。
- トレースファイル。詳細については、NetScalerでパケットトレースを記録する方法を参照してください。

ガイダンスについては、Citrixサポートにお問い合わせください。

共有セキュリティの責任

以下のセクションでは、共有セキュリティの責任について詳しく説明します。

お客様が必要とするアクション

セキュリティのベストプラクティスの一環として、お客様が行うべきアクションの一部を以下に示します。

- Adaptive Authentication UI にアクセスするための資格情報: お客様は、Adaptive Authentication UI にアクセスするための資格情報の作成と維持に責任を負います。お客様が Citrix サポートと協力して問題を解決している場合、これらの資格情報をサポート担当者と共有する必要がある場合があります。
- 多要素認証: ベストプラクティスとして、お客様はリソースへの不正アクセスを防ぐために多要素認証ポリシーを設定する必要があります。
- 認証資格情報: お客様は、一般的なセキュリティおよびパスワードの標準に従って認証資格情報を設定する必要があります。
- リモート CLI アクセスセキュリティ: Citrix はお客様にリモート CLI アクセスを提供します。ただし、お客様は実行時におけるインスタンスのセキュリティ維持に責任を負います。
- SSL プライベートキー: NetScaler® はお客様の管理下にあるため、Citrix はファイルシステムにアクセスできません。お客様は、NetScaler インスタンスでホストしている証明書とキーを保護する必要があります。
- データバックアップ: 構成、証明書、キー、ポータルのカスタマイズ、およびその他のファイルシステムの変更をバックアップします。
- NetScaler インスタンスのディスクイメージ: NetScaler のディスク領域とディスククリーンアップを維持および管理します。詳細については、「インスタンス管理」を参照してください。
- ロードバランスされた LDAPS 構成の例については、「LDAP および LDAPS ロードバランシング構成の例」を参照してください。

お客様と Citrix の両方から必要とされるアクション

- ディザスタリカバリ: サポートされている Azure リージョンでは、NetScaler の高可用性インスタンスは、データ損失から保護するために個別の可用性ゾーンにプロビジョニングされます。Azure のデータ損失が発生した場合、Citrix は Citrix 管理の Azure サブスクリプション内の可能な限り多くのリソースを回復します。

  Azure リージョン全体の損失が発生した場合、お客様は新しいリージョンで顧客管理の仮想ネットワークを再構築し、新しい VNet ピアリングを作成する責任を負います。

- パブリック管理IPアドレス経由の安全なアクセス:

  割り当てられたパブリックIPアドレスによって管理インターフェースへのアクセスを保護し、インターネットへのアウトバウンド接続を許可します。

サイジングとパフォーマンスのガイドライン

アダプティブ認証は、データセンターに展開されたCloud Connector、または顧客が管理するVNetからデータセンターへの到達可能性がすでに確立されている場合のAzure VNet Peeringのいずれかを使用して、顧客がオンプレミスの認証サーバーにアクセスできるようにします。このトピックには、Citrix Cloud Connector™とAzure VNet Peeringの両方の展開におけるパフォーマンス数値、およびCitrix Cloud Connectorマシンの推奨されるスケールとサイズ構成に関する情報が含まれています。

ユーザー認証レート

2 vCPUおよび7 GB RAMサイズのコネクタ仮想マシンは、1秒あたり14ユーザーを認証できます。

デフォルトでは、コネクタサービスは、障害またはクラッシュが発生した場合に2回自動的に再起動するように構成されています。その後の障害またはクラッシュでは、サービスは停止します。また現在、認証レートが1秒あたり4認証を超えて増加すると、コネクタサービスは失敗します。このレートは、コネクタサービスを任意の回数の障害後に再起動するように構成することで達成できます（**Citrix Netscaler Cloud Gateway > Recovery > Restart the service**）。この設定が構成されていない場合、レートは1秒あたり4認証に低下します。

Citrix Cloud™ Connectorsを使用する場合のトラフィック遅延とユーザー認証レート

次の表は、Citrix Cloud Connectorsを使用する場合のトラフィック遅延とユーザー認証レートを示しています。

認証タイプ	認証遅延 (P95) (ミリ秒)	1秒あたりの認証またはユーザーログインレート
LDAP	5.99	14
RADIUS	3.17	14
LDAP+RADIUS	4.59	14

認証タイプ	認証遅延 (P95) (ミリ秒)	1秒あたりの認証またはユーザーログインレート
LDAPS	26.75	14
LDAPS+RADIUS	15.61	14

Azure VNet Peering 使用時のトラフィック遅延とユーザー認証レート

次の表は、Azure VNet peering 使用時のトラフィック遅延とユーザー認証レートを示します。

認証タイプ	リクエスト遅延 (P95) (ミリ秒)	1秒あたりの認証またはユーザーログインレート
LDAP	6.95	17.54
LDAPS	7.19	16.98

よくある質問

以下のセクションでは、よくある質問について詳しく説明します。

Adaptive Authentication または NetScaler のアップグレード後、ユーザーがログインできません。どうすればよいですか?

自己診断チェック:

- Adaptive Authentication IdP FQDN にアクセスできない場合:
  - 認証仮想サーバー (auth_vs) が UP であるか確認します。
  - UP でない場合は、証明書が正しくバインドされていることを確認します。

  保存されていない構成や誤った構成により、証明書のバインドが解除されたり失われたりして、認証仮想サーバーが DOWN になる可能性があります。
- プライマリ Adaptive Authentication NetScaler CLI を使用して、クラウドトンネル仮想サーバーが UP であるか確認します: `show cloudtunnel vserver`。

  Azure IMDS の断続的な接続性の問題により、再起動後にクラウドトンネル仮想サーバーの構成が失われる可能性があります。

  回避策: もう一度再起動を実行します。
- LDAP を使用している場合は、`ldapAction` が 7〜10 秒のタイムアウト (`authTimeout`) で構成されていることを確認してください。

> **注:**
>
> この LDAP 関連のログインの問題は、アップグレードが実行されたかどうかに関係なく発生する可能性があります。

ADM/NetScaler Console で Adaptive Authentication NetScaler インスタンスが「ダウン」または「猶予期間中」と表示されるのはなぜですか?

Adaptive Authentication NetScaler インスタンスのエントリは、**Console Service > Infrastructure > Instances > NetScaler** に表示されます。

- コンソールに表示されるUP (緑) またはDOWN (赤) の状態は、Console Service と Adaptive Auth NetScaler インスタンス間の接続性を示しており、Adaptive Authentication ノードの実際の状態を示すものではありません。
- 接続状態がDOWNであっても、ユーザーのログインや機能には影響しませんが、次のような影響が生じる可能性があります。
  - Citrix は NetScaler インスタンスにアップグレードをプッシュできません。
  - 接続が30日以上DOWNのままだと、Adaptive Authentication NetScaler LAS ライセンスリース更新が失敗し、インスタンスの帯域幅が10 Mbpsに制限される可能性があります。NetScaler 管理UIに警告バナーが表示されます。

接続を復元する:

ADM/NetScaler Console で接続ステータスがDOWNと表示される場合は、復元する必要があります。以下の手順を実行するか、Citrix Support にお問い合わせください。

1. 接続ステータスがDOWNと表示されているNetScalerインスタンスにSSHで接続します。
2. シェルを実行します。
3. mastools プロセスが実行されているかどうかを確認します。

   ```
   ps -ax | grep mastools
   ```

   出力には、mastools と mastools_upgrade の両方のプロセスが実行中であることが示されている必要があります。
4. 必要に応じて、mastools を再起動します。

   ```
   cd /var/mastools/scripts
   ```

   ```
   ./mastoolsd restart
   ```

アダプティブ認証のアップグレード後、ユーザーが「Relaying party requested claims of user not found」というメッセージを受け取るのはなぜですか?

- アダプティブ認証IdPログインページが表示される前に問題が発生した場合は、Citrixサポートにお問い合わせください。
- アダプティブ認証IdPログインページが表示され、資格情報が入力された後に問題が発生した場合は、次の点を確認してください。
    - ユーザーがADに以下の7つの必須クレームをすべて持っていることを確認してください。
        - メールアドレス
        - 表示名
        - 共通名
        - sAMAccountName
        - ユーザープリンシパル名
        - オブジェクト識別子 (OID)
        - セキュリティ識別子 (SID)
    - SAMLまたはRADIUSを使用している場合は、最後にNOAUTH LDAPファクターを追加して、7つの必須クレームをすべて抽出します。

アダプティブ認証がLDAPポート389または636で動作していません。何を確認すればよいですか?

接続テスト (GUI: **ネットワーク接続のテスト**) は、プライマリノードからのみ実行されていることを確認してください。

1. `ns.log`で**Entering bitpump**ログエントリを確認して、オンプレミスADへのトンネルが成功していることを確認してください。
2. トンネルが成功した場合は、`cat /tmp/aaad.debug` を実行して認証エラーを表示します。
3. 問題が解決しない場合は、Citrixサポートにお問い合わせください。

適応型認証アプライアンスをプロビジョニングしようとしていますが、オンボーディングフローでアクセスできないフォームの入力を求められます。どうすればよいですか?

適応型認証プロビジョニングを要求するために使用されるフォームは、一部の顧客に対して「アクセス拒否」エラーを表示する場合があります。

回避策:

Citrixサポートに連絡して、プロビジョニングリクエストを直接送信してください。

フォーム提出後、適応型認証を有効にするにはどのくらいかかりますか?

最低3営業日です。

データガバナンス

このトピックでは、Citrix Adaptive Authenticationサービスおよびアダプティブ認証インスタンスによるログの収集、保存、保持に関する情報を提供します。定義で定義されていない大文字の用語は、Citrixエンドユーザーサービス契約で指定された意味を持ちます。

- Adaptive Authenticationサービス: 管理者がログインしてアダプティブ認証インスタンスを展開および管理できるCitrix Cloud™サービス。
- Adaptive Authenticationインスタンス: 管理者がユーザー認証を管理できるように、Adaptive Authenticationサービスによって展開されるNetScaler®仮想マシン。

データレジデンシー

アダプティブ認証サービス

Citrix Adaptive Authenticationサービスの顧客コンテンツデータは、Azure Cloud Services East リージョンに存在します。これらは、可用性と冗長性のために、以下のAzureリージョンにレプリケートされます。

- 米国西部
- 北ヨーロッパ

サービス構成ログとランタイムログの宛先は次のとおりです。

- システム監視およびデバッグログ用のSplunkサービス（米国およびEU（欧州連合）のロケーションのみ）。
- 集約されたユーザーアクセスログ用のNetScaler Application Delivery Managementサービス。詳細については、NetScaler ADMデータガバナンスを参照してください。
- 管理者監査ログ用のCitrix Cloud System Logsサービス。詳細については、Citrix Cloud Servicesの顧客コンテンツとログの処理および地理的考慮事項を参照してください。

Adaptive Authenticationインスタンス

すべての構成、インスタンス固有のアーティファクトをバックアップするためのNetScaler Application Delivery Managementサービス。詳細については、NetScaler ADMデータガバナンスを参照してください。

データ収集

Citrix Adaptive Authenticationサービスにより、顧客管理者はAdaptive Authentication UIを介してサービスを設定し、付属のコネクタアプライアンスをコンソールを介して設定できます。以下の顧客コンテンツが収集されます。

- アダプティブ認証サービス
  - IdP (IDプロバイダー) エンドポイントのFQDN (完全修飾ドメイン名) およびIPアドレス。
  - IPアドレス/範囲、ポート、およびプロトコル
  - IdP認証仮想サーバーへのアクセスに使用される証明書
  - 管理エンドポイントのパブリックIPアドレス
  - Azure VNetピアリングの場合、ネットワーク共同作成者ロールを持つサービスプリンシパル。詳細については、「Azure VNetピアリングを使用してオンプレミス認証サーバーへの接続をセットアップする」を参照してください。
- アプリエンタイトルメントのユーザー識別子
- Citrix Cloud Connector関連の詳細。詳細については、「Citrix Cloud Connector」を参照してください。
  - IPアドレスまたはFQDN
  - ユーザー、デバイス、およびリソースロケーション識別子
  - 内部プロキシ構成

サービスコンポーネントによって収集されるランタイムログの場合、主要な情報は次のとおりです。

- クライアントIPアドレスとポート
- 宛先FQDN/アドレスとポート
- クライアントユーザーエージェント
- アプリケーションURLパス
- アプリケーションアクセス時間と期間
- リクエストバイト数
- レスポンスバイト数
- HTTPトランザクションID
- 展開モード (コネクタまたはAzure VNetピアリング)

- Azureリソース
  - リソースグループ名
  - VNet (IPアドレス、CIDR)
  - サブネット (IPアドレス、CIDR)
  - 仮想マシン名

データ転送

Citrix Adaptive Authenticationサービスは、トランスポート層セキュリティによって保護された宛先 (Splunk) にログを送信します。

データ制御

Citrix Adaptive Authenticationサービスは現在、お客様がログ送信をオフにしたり、顧客コンテンツがグローバルに複製されるのを防いだりするオプションを提供していません。

データ保持

Citrix Cloudのデータ保持ポリシーに基づき、お客様の設定データはサブスクリプションの有効期限が切れてから90日（約3か月）後にサービスから削除されます。

ログの保存先は、サービス固有のデータ保持ポリシーを維持します。

- Citrix Application Delivery Managementに保存されているイベントについては、「Citrix ADM データガバナンス」を参照してください(/ja-jp/citrix-application-delivery-management-software/current-release/data-governance.html)。
- Splunkログは、90日（約3か月）後にアーカイブされ、最終的に削除されます。
- Adaptive Authenticationインスタンスは、サブスクリプションの有効期限が切れてから30日（約4.5週間）後に割り当て解除されます。

データエクスポート

いくつかの種類のログに対して、さまざまなデータエクスポートオプションがあります。

- 管理者監査ログは、Citrix Cloudシステムログコンソールからアクセスできます。
- Splunkログは、お客様が利用するためのものではありません。これらのイベントは、SplunkからCSVファイルとしてエクスポートすることもできます。

定義

- 顧客コンテンツとは、ストレージのためにお客様アカウントにアップロードされたデータ、またはCitrixがサービスを実行するためにアクセスを許可されているお客様環境内のデータを意味します。
- ログとは、パフォーマンス、安定性、使用状況、セキュリティ、サポートを測定する記録を含む、サービスに関連するイベントの記録を意味します。
- サービスとは、顧客のユースケースを促進する目的で前述したCitrix Cloudサービスを意味します。