citrix

アダプティブ認証サービス

Machine translated content

Disclaimer

このコンテンツの正式なバージョンは英語で提供されています。Cloud Software Group ドキュメントの コンテンツの一部は、お客様の利便性のみを目的として機械翻訳されています。Cloud Software Group は 機械翻訳されたコンテンツを管理していないため、誤り、不正確な情報、不適切な用語が含まれる場合 があります。英語の原文から他言語への翻訳について、精度、信頼性、適合性、正確性、またはお使い の Cloud Software Group 製品またはサービスと機械翻訳されたコンテンツとの整合性に関する保証、該 当するライセンス契約書またはサービス利用規約、あるいは Cloud Software Group とのその他すべての 契約に基づき提供される保証、および製品またはサービスのドキュメントとの一致に関する保証は、明 示的か黙示的かを問わず、かかるドキュメントの機械翻訳された範囲には適用されないものとします。 機械翻訳されたコンテンツの使用に起因する損害または問題について、Cloud Software Group は責任を負 わないものとします。

Contents

リリースノート	2
アダプティブ認証サービスの設定	3
関連する適応認証構成	15
インスタンスのディスク容量管理	32
アダプティブ認証の問題のトラブルシューティング	34
アダプティブ認証を使用したスマートアクセス	39
サイジングとパフォーマンスのガイドライン	52
データガバナンス	53

リリースノート

June 19, 2024

アダプティブ認証リリースノートは、NetScaler リリースノートのサブセットです。アダプティブ認証をご利用のお 客様は、NetScaler リリースノートを使用して、アダプティブ認証サービスの機能強化、修正された問題、および既 知の問題について確認する必要があります。

注:

このドキュメントの日付は、サービスの最終アップグレード日を示しています。

16 Jan 2024

新機能

• アダプティブ認証インスタンスの自動アップグレード

アダプティブ認証インスタンスは、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 以降に自動的にアップグレードされます。

26 Sep 2023

新機能

• アダプティブ認証インスタンスの自動アップグレード

アダプティブ認証インスタンスは、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 以降に自動的にアップグレードされます。

2023年7月18日

新機能

• アダプティブ認証インスタンスの自動アップグレード

アダプティブ認証インスタンスは、CTX561482に記載されているセキュリティの脆弱性に対処するビルド 13.1-49.101 以降に自動的にアップグレードされます。

2023年4月28日

新機能

ロードバランシングによる LDAP と LDAPS のサポート
 Citrix アダプティブ認証インスタンスは、負荷分散仮想サーバーを使用して LDAP と LDAPS をサポートします。詳細については、「LDAP と LDAPS の負荷分散設定の例」を参照してください。

[AAUTH-2067]

• 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の場所のマッピング

管理者は、バックエンドの AD および RADIUS サーバーにアクセスするためのコネクタを選択できます。詳細 については、「アダプティブ認証のプロビジョニング」を参照してください。

解決された問題

• アダプティブ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 にあ りません。

[AAUTH-68]

既知の問題

アダプティブ認証インスタンスの場合、LDAP プロファイル(NetScaler 管理 GUI)の「接続テスト」オプションを使用して接続を確認すると、LDAP サーバーにアクセスできない場合でも、LDAP サーバーにアクセス可能と誤って表示されます。

[AAUTH-2111]

アダプティブ認証サービスの設定

June 19, 2024

アダプティブ認証サービスの設定には、次の大まかな手順が含まれます。

- 1. アダプティブ認証をプロビジョニング
- 2. アダプティブ認証ポリシーを構成する
- 3. Workspace のアダプティブ認証を有効にする

前提条件

- アダプティブ認証インスタンスの FQDN を予約します。たとえば aauth.xyz.com、xyz.com は会社のドメインであると仮定します。この FQDN は、このドキュメントではアダプティブ認証サービス 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、[証明書のアップロード] ステップでプロビジョニングした後に取得されます。
- aauth.xyz.com の証明書を入手します。証明書には SAN 属性が含まれている必要があります。それ以外の 場合、証明書は受け付けられません。
- アダプティブ認証 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、「中間証明書の設定」を参照してください。
- オンプレミスの AD/RADIUS 接続の接続タイプを選択します。次の2つのオプションを使用できます。データ センターの到達可能性を望まない場合は、コネクタ接続タイプを使用します。
 - Citrix Cloud Connector 詳細については、「Citrix Cloud Connector」を参照してください。
 - Azure VNet ピアリング -詳細については、「Azure VNet ピアリングを使用したオンプレミス認証サーバーへの接続のセットアップ」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、「システムクロックをネットワーク上のサーバーと同期させる方法」を参照してください。

注意事項

- Citrix では、アダプティブ認証インスタンスに対して clear config を実行したり、証明書を含むプレフィックスAA付きの構成(AAuthAutoConfig など)を変更したりしないことをお勧めします。これにより、アダプティブ認証の管理が中断され、ユーザーアクセスが影響を受けます。回復する唯一の方法は、再プロビジョニングを行うことです。
- アダプティブ認証インスタンスには SNIP やその他のルートを追加しないでください。
- ・顧客 ID がすべて小文字でない場合、ユーザー認証は失敗します。ID をすべて小文字に変換し、コマン ドset cloud parameter -customerID <all_lowercase_customerid>を使用し て NetScaler インスタンスに設定できます。
- Citrix Workspace または Citrix Secure Private Access サービスに必要な nFactor 構成は、顧客がインス タンスで直接作成することになっている唯一の構成です。現在のところ、NetScaler には、管理者がこれらの 変更を行うことを妨げるチェックや警告はありません。
- すべてのカスタム構成は、アダプティブ認証インスタンスで直接行うのではなく、ユーザーインターフェイス で行うことをお勧めします。これは、インスタンスに加えられた変更がユーザーインターフェイスと自動同期 されないため、変更が失われるためです。
- アダプティブ認証インスタンスをランダムな RTM ビルドにアップグレードしないでください。すべてのアッ プグレードは Citrix Cloud によって管理されます。

- Windows ベースの Cloud Connector のみがサポートされています。このリリースでは、Connector Appliance はサポートされていません。
- Citrix Cloud の既存のお客様で、Azure AD(またはその他の認証方法)をすでに構成している場合、アダプ ティブ認証(Device Posture チェックなど)に切り替えるには、認証方法としてアダプティブ認証を構成 し、アダプティブ認証インスタンスで認証ポリシーを構成する必要があります。詳しくは、「Citrix Cloud を Azure AD に接続する」を参照してください。
- 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 サーバー内の RADIUS クライアントとして追加します。
- 現在のリリースでは、外部の ADM エージェントは許可されていないため、Citrix Analytics (CAS) はサポ ートされていません。
- NetScaler Application Delivery Management サービスは、アダプティブ認証インスタンスのバックアッ プを収集します。ADM からバックアップを抽出するには、ADM サービスをオンボーディングします。詳細に ついては、「構成のバックアップと復元」を参照してください。Citrix は、アダプティブ認証サービスからバッ クアップを明示的に取得しません。お客様は、必要に応じて、アプリケーション配信管理サービスから構成の バックアップを取る必要があります。
- ・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を確立できません。そのため、アダプティブ認証のプロキシ構成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ことがあります。そのため、すべてのクレームに合格するには、NOAUTH などの要素を2要素認証構成に追加することをお勧めします。
- 通常の操作中はデバッグログレベルを無効のままにし、必要な場合にのみ有効にすることをお勧めします。デバッグログレベルが常に有効になっていると、管理 CPU に多大な負荷がかかります。これにより、トラフィック負荷が高いときにシステムがクラッシュする可能性があります。詳しくは、CTX222945を参照してください。

アダプティブ認証サービスの構成方法

アダプティブ認証のユーザーインターフェイスにアクセスする

アダプティブ認証ユーザーインターフェイスには、次のいずれかの方法でアクセスできます。

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

認証に成功すると、アダプティブ認証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 とアクセス管理] に移動します。
- •「認証」タブの [アダプティブ認証] で、省略記号メニューをクリックし、[管理] を選択します。

アダプティブ認証の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構成に関連する手順を示しています。

Adaptive Authentication	
Complete these tasks to prepare and deploy Adaptive Authentication.	About Adaptive Authentication:
Provision Adaptive Authentication instances Provision Adaptive Authentication instances and optionally configure a connection with your on-premises network. Complete this step before proceeding to the next step Provision	((ϕ) Connect Adaptive Auth Configure policies Configure Co
Configure authentication policies Create and apply policies for authentication, conditional access, device posture, and more using the management console. Complete this step before proceeding to the next step	With the Adaptive Authentication service, you can authenticate Workspace subscribers based on policies for conditional authentication and contextual access. These policies evaluate conditions such as device posture and network location to allow only authorized users to again to Workspace. You can also connect to vour existing hested defaults provider on corresponse or in a volke cloud learn
Enable Adaptive Authentication for Workspace Select Adaptive Authentication as your preferred authentication method for subscribers signing in to Citrix Workspace. Complete this step before proceeding to the next step <u>Take me to authentication in Workspace Configuration</u>	more
Connect an identity provider to access its user directory Make sure the identity provider of the directory you wish to access for user lookup and resource assignment is connected. Take me to identity and access management.	

ステップ 1: アダプティブ認証をプロビジョニングする

重要:

アダプティブ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、 Podio フォームに記入する必要があります。その後、Citrix アダプティブ認証チームは、アダプティブ認証イ ンスタンスのプロビジョニングを有効にします。

計口文 Adaptive Authentication 4						
Cloud service from Citrix for Adaptive MFA						
Thank you for your interprive Authentication Service . To enable the service kindly provide your det here I we will enable it for you!	What's ahead ① Crear a virtual muchine in a Critic managed Azuer subscription to best Critic Gateway. ② Generate a pair of 5531 keys to secare access to the Critic Gateway command line interface. ③ Creare a VSRe presing connection between your Azuer visual antwork and the Critic visual antwork for Administration. ④ Creare a VSRe presing connection between your Azuer visual antwork and the Critic visual antwork for Administration. ④ Operate of pervision Edge greency VSH to Critic Clinid as an identity previder. This task allows you to select Adaptive Architections as the preferend anthenications method for Circs Winkapace.					
About Adaptive Authentication:	Create and apply policies for authentication, conditional across, derive pooler, and ener. Specify Adaptive Authentication as your performed authentication method for subscribers signing in to Christ Waterse. If you just purchased Adaptive Authentication and are still seeing this page, you might need to refresh the page.					

以下の手順を実行して、アダプティブ認証インスタンスをプロビジョニングします。

- 1. アダプティブ認証 UI で、[プロビジョニング] をクリックします。
- 2. アダプティブ認証の優先接続を選択します。

Citrix Cloud Connector: この接続タイプでは、オンプレミスネットワークにコネクタを設定する必要があります。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には、環境に少なくとも2つの Citrix Cloud Connector を展開することをお勧めします。Citrix Cloud Connector が、アダプティブ認証インスタンス用に予約したドメイン/URL にアクセスすることを許可する必要があります。たとえば、https://aauth.xyz.com/*を許可します。

Citrix Cloud Connector について詳しくは、「Citrix Cloud Connector」を参照してください。

- Azure VNet ピアリング -Azure の VNet ピアリングを使用してサーバー間の接続を設定する必要があ ります。
 - 接続をセットアップするための Azure サブスクリプションアカウントがあることを確認します。
 - ピアリングされる顧客 VNet には、Azure VPN ゲートウェイがすでにプロビジョニングされている必要があります。詳しくは、https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portalを参照してください。

Provision Adaptive	Authentication	×
Overview Provision Console access	Provision Select your preferred connection for adaptive authentication.	
Upload Certificate Allowed IP addresses	Use this option if you want to connect to your on-premises authentication servers using Citrix Cloud Connector. Azure VNet peering Use this option if you want to connect to your on-premises authentication servers using Azure VNet peering.	
Manage Connectivity	 If you don't want data center reachability please use Citrix Cloud Connector I understand that I can't change the connection type after provisioning is complete. If I need to change this connection later, I must deprovision it. 	
Provision		

Citrix Cloud Connector を優先接続として追加するには:

以下の手順を実行します。

- Citrix Cloud Connector オプションを選択し、「エンドユーザー契約」チェックボックスを選択します。
- [プロビジョニング]をクリックします。プロビジョニングのセットアップには最大 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は、プロビジョニング後にアダプティブ認証 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。
```

Azure VNet ピアリングを設定するには:

接続として Azure VNet ピアリングを選択した場合は、アダプティブ認証インスタンスのプロビジョニング に使用する必要があるサブネット CIDR ブロックを追加する必要があります。また、CIDR ブロックが組織の 他のネットワーク範囲と重複しないようにする必要があります。

詳しくは、「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。

- 3. 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認証情報を設定します。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。
 - a) 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。
 - b) [次へ] をクリックします。

注:

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。

Provision Adaptive	Authentication >	<
Overview Provision Console access Upload Certificate Allowed IP addresses Manage Connectivity	Console access Enter the credentials you want to use for accessing the management console of Adaptive Authentication. You can use the management console to create policies for authentication, conditional access, and device posture User name itrixadmin ▲ Username can't be changed after saving. Password 	
Next	Provisioning was successful	

- 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。
 パブリックにアクセス可能な認証サーバーに対して、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 は公に解決可能でなければなりません。
 - 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用に PFX、PEM、DER タイプの 証明書をサポートします。
 - 証明書バンドルは PEM タイプの証明書でのみサポートされます。他の種類のバンドルについては、 Citrix で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お勧めします。

```
c) 証明書とキーをアップロードします。
```

注:

- Adaptive Authentication インスタンスに中間証明書をインストールし、サーバー証明書とリン クします。
 - アダプティブ認証インスタンスにログインします。 1. [** トラフィック管理] > [SSL**] に移動します。 詳細について は、「[中間証明書を構成する](/en-us/citrix-gateway/ current-release/install-citrix-gateway/certificatemanagement-on-citrix-gateway/configure-intermediatecertificate.html)」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 CA または未知の CA によって署名された証明 書は受け付けられません。
- 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。矛盾が生じる可能性があります。

Provision Adaptive	e Authentication	×
Overview Provision Console access Upload Certificate	Add FQDN and certificate key pair Enter the FQDN for the adaptive authentication IDP access and upload an SSL certificate and private key to secure the end user requests. You can obtain a certificate and key from a trusted Certificate Authority (CA that the key strength of the certificate keys is 2,048 bits or higher and that the keys are signed with secure signature algorithms.	4). Ensure
Allowed IP addresses	Please add DNS mapping for the FQDN to the public IP	
Manage Connectivity	Select the type of certificate you will upload: PFX (Personal Exchange Format) V Certificate V	
	Certificate name	
	Password	<u> </u>
	Suser successfully added	×
Next		

5. 証明書とキーをアップロードします。

これで、アダプティブ認証インスタンスが ID およびアクセス管理サービスに接続されました。アダプティブ 認証方法のステータスが [接続済み]と表示されます。

∽ Id	lentity a	nd Access	Manager	nent			
Au	thentication	Administrators	API Access	Domains	Recovery		
Se	t up the variou	is ways you need y	our Citrix Cloud	d administra	tors and Citrix Workspace subscribers to sign in.		
	Citrix Ider Admin Sigr	ntity n-in URL: https://cit	rix.cloud.com			Connected	
	Azure Act	tive Directory 🚱				Not Connected	
	Active Dir	ectory 💿				Not Connected	
	Active Dir	ectory + Token				Not Connected	
	Citrix Gat	eway 💿				Connected	
	Okta 🕖					Not Connected	
	SAML 2.0	0				 Not Connected 	
	Adaptive	Authentication				Connected	

- 6. アダプティブ認証管理コンソールにアクセスするための 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、管理 IP アドレスとしてパブリック IP アドレ スを入力します。管理 IP アドレスへのアクセスを制限するために、管理コンソールへのアクセスを許可 する複数の 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、[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。

Provision Adaptiv	e Authentication	×			
Overview Provision	Allowed Public source IPv4 address You can enter up to 5 public source IPv4 addresses from where management console of adaptive authentication can be accessed.				
Console access	Enter IPv4 address				
Upload Certificate	IPv4 address				
Allowed IP addresses	A10.01	Ē			
Manage Connectivity					
Close Save Cha	Close Save Changes				

 コネクタ接続タイプを使用している場合は、AD または RADIUS サーバーにアクセスできるリソースの場所 (コネクタ)のセットを指定します。VNet ピアリング接続タイプを使用している場合は、この手順を省略でき ます。

管理者は、バックエンドの AD および RADIUS サーバーにアクセスするためのコネクタを選択できます。この 機能を有効にするには、お客様はバックエンドの AD/RADIUS サーバーのサブネット間のマッピングを設定 して、認証トラフィックが特定のサブネットに含まれる場合に、そのトラフィックが特定のリソースの場所に 転送されるようにします。ただし、リソースの場所がサブネットにマップされていない場合、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の場所を使用するように指定できます。

以前は、オンプレミス AD/RADIUS のアダプティブ認証トラフィックは、ラウンドロビン方式を使用して使用 可能な任意のリソースの場所に転送されていました。これにより、複数のリソースの場所を持つお客様に問題 が発生しました。

- a) アダプティブ認証 UI で、「接続を管理」をクリックします。
- b) サブネットの詳細を入力し、それぞれのリソースの場所を選択します。
 - 注:

[残りのサブネットに利用可能なリソースの場所を使用する]チェックボックスをオフにすると、 設定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リングされます。

c) [追加]をクリックし、[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。

- 顧客ごとのサブネットとリソースのロケーションマッピングの数は 10 に制限されています。
- 複数のサブネットを1つのリソースの場所にマッピングできます。
- 同じサブネットに重複したエントリは許可されません。
- 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。
- リソースの場所の名前を変更したり削除したりする場合は、必ずアダプティブ認証ユーザーインタ ーフェースの「接続管理」画面からエントリを削除してください。
- 次の CLI コマンドを使用してリソースの場所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(アダプティブ認証 Provisioning>接続管理)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 <>

Provision Adaptiv	e Authentication		×
Overview Provision Console access	Add AD/RADIUS server subnet You can enter up to 10 subnet to resource Subnet	to resource location mapping elocation mappings. Select Resource Location Add	
Allowed IP addresses	Subnet	Resource Location	A
Manage Connectivity	1.00.000	Avrs - USA - West Azure - Europe - North	U D
Close Save Cha	anges		

アダプティブ認証の Provisioning が完了しました。

ステップ 2: アダプティブ認証ポリシーを構成する

アダプティブ認証インスタンスに接続する方法:

プロビジョニング後、アダプティブ認証管理 IP アドレスに直接アクセスできます。アダプティブ認証管理コンソール には、FQDN またはプライマリ IP アドレスを使用してアクセスできます。

重要:

- 高可用性セットアップでは、同期プロセスの一環として、証明書も同期されます。そのため、必ずワイル ドカード証明書を使用してください。
- ノードごとに固有の証明書が必要な場合は、同期されない任意のフォルダーに証明書ファイルとキーを アップロードし (たとえば、NSConfig/SSL ディレクトリに別のフォルダー (nosync_cert) を作成しま す)、その証明書を各ノードに一意にアップロードします。

アダプティブ認証管理コンソールにアクセスします。

- FQDN を使用してアダプティブ認証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 の 設定」を参照してください。
- プライマリアドレスを使用してアダプティブ認証にアクセスするには、次の操作を行います。
 - 1. GUI の [認証ポリシーの設定] 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 IP アドレスにアクセスします。
 - 2. プロビジョニング時に入力した認証情報を使用してログインします。
 - 3. [続行] をクリックします。

Dashboard	Configuration	Reporting	Documentation	Downloads
Welcome! Use this wizard f skip this section	ior initial configuration of you	ır Citrix ADC virtual	appliance. To configure or	to change a previously configured setting, click each of the sections below. If a parameter
¢°	Citrix ADC IP Address IP address at which you accord Citrix ADC IP Address	ess the Citrix ADC for	configuration, monitoring, a Netmask 255,255,255,0	nd other management tasks.
	Subnet IP Address Specify an IP address for yo Subnet IP Address Not configured	our Citrix ADC to comm	nunicate with the backend so	ervers.
	Host Name, DNS IP Ac Specify a host name to iden discover your Citrix ADC ins	ddress, Time Zono tify your Citrix ADC, a tances effortlessly on	e, NTP Server, Citrix Al n IP address for a DNS serve I Citrix ADM service.	DM Service Connect If to resolve domain names, the time zone in which your Citrix ADC is located, an IP address/fully (
	Host Name adaptive-auth-1		DNS IP Address	Time Zone CoordinatedUniversalTime
	Licenses Upload licenses from your lo You can also allocate pooled There are 0 license file(s) pr	ocal computer or alloc d capacity from an on- resent on this Citrix Al	ate licenses from the Citrix I premise license server. DC.	licensing portal.

- 4. 設定>セキュリティ>AAA-アプリケーショントラフィック>仮想サーバにナビゲートして下さい。
- 5. 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、「認証設定の例」を参照してください。

注:

IP 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することは信頼できないため、多くのブラウ ザは警告を表示してアクセスをブロックします。セキュリティ上の障壁を避けるため、アダプティブ認証管理 コンソールには FQDN を使用してアクセスすることをお勧めします。Adaptive Authentication 管理コンソ ール用の FQDN を予約し、プライマリおよびセカンダリの管理 IP アドレスにマッピングする必要があります。

たとえば、アダプティブ認証インスタンスの IP が 192.0.2.0 で、セカンダリ IP が 192.2.2.2 の場合:

- primary.domain.com は 192.0.2.0 にマッピングできます
- ・ secondary.domain.com は 192.2.2.2 にマッピングできます

ステップ 3: Workspace の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、[Workspace のアダプティブ認証を有効にする] セクションの [** 有効化] をクリ ックして、Workspace の認証を有効にできます ** 。

Adaptive A	uthentication is now connected	
Ааа	prive Autnentication	
Comple	te these tasks to prepare and deploy Adaptive Authentication.	
0	Provision Adaptive Authentication instances Provision Adaptive Authentication instances and optionally configure a connection with your on-premises network. Complete this step before proceeding to the next step See Details	
2	Configure authentication policies Create and apply policies for authentication, conditional access, device posture, and more using the management console. Complete this step before proceeding to the next step Access the Adaptive Authentication management console by visiting 20.106.227.13 (Primary). You can also add DNS entries for 20.106.227.13 (Primary) and 20.127.209.21 (Secondary) and access the management console using FQDN. Since primary instance may change, Click here to refresh the instance IPs.	
3	Enable Adaptive Authentication for Workspace Select Adaptive Authentication as your preferred authentication method for subscribers signing in to Citrix Workspace. Complete this step before proceeding to the next step Enable	
4	Connect an identity provider to access its user directory Make sure the identity provider of the directory you wish to access for user lookup and resource assignment is connected. Take me to identity and access management.	

注:

これで、アダプティブ認証の設定は完了です。ワークスペース URL にアクセスすると、アダプティブ認証 FQDN にリダイレクトされる必要があります。

関連参考文献

• FQDN を編集する

- 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
- アダプティブ認証インスタンスのプロビジョニングを解除する
- ゲートウェイへの安全なアクセスを可能にする
- 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
- カスタムワークスペース URL またはバニティ URL
- 構成のバックアップと復元
- 負荷分散された LDAPS 構成の例
- 認証方法をアダプティブ認証に移行する
- 認証設定の例

関連する適応認証構成

October 21, 2024

FQDN を編集する

ワークスペース構成で認証方法として アダプティブ認証 が選択されている場合は、FQDN を編集できません。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 アドレスにマップされてい 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 Adaptive Authentication に移行する必要があります。詳細については、「認証方法を Adaptive Authentication 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. 適応認証から別の認証方法に切り替えます。

4	Workspace Configuration							
	Access	Authentication	Customize	Service Integrations	Sites			
	Work	space Authenti	cation					
	Selec	t how subscribers	will authentica	ate to sign in to their wo	rkspace.			
	Active Directory Active Directory + Token							
		Azure Active Dir	rectory					
		Okta						
	Citrix Gateway SAML 2.0 Adaptive Authentication							

2. 加入者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 ログインが影響を受け、Adaptive Authentication が再度有効になるまで、認証に Adaptive Authentication は使用されません。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。

Provision Adaptiv	e Authentication
Overview Provision	Add FQDN and certificate key pair Enter the FQDN for the adaptive authentication IDP access and upload an SSL certificate and private key to secure the end user requests. You can obtain a certificat that the key strength of the certificate keys is 2,048 bits or higher and that the keys are signed with secure signature algorithms.
Console access	ex: aauth.xyz.com
5 Allowed IP addresses	i Please add DNS mapping for the FQDN to the public IP
	Select the type of certificate you will upload: PEM (Privacy Enhanced Mail) Certificate
	Upload certificate Key Upload key
	Password for key (only required if key is encrypted) Key Password
	User successfully added

4. 変更を保存をクリックします。

重要:

FQDN を編集する場合は、証明書も再度アップロードする必要があります。

1. Adaptive Authentication ホームページで 有効 (手順 3) をクリックして、Adaptive Authentication 方式 を再度有効にします。

3	Enable Adaptive Authentication for Workspace
-	Select Adaptive Authentication as your preferred authentication method for subscribers signing in to Citrix Workspace.
	Complete this step before proceeding to the next step
	Enable

2. [更新]をクリックします。

カスタムワークスペース URL またはバニティ URL

カスタム ワークスペース URL を使用すると、選択したドメインを使用して Citrix Workspace ストアにアクセスで きます。ユーザーは、デフォルトのワークスペース URL またはカスタム ワークスペース URL、あるいはその両方を 使用してワークスペースにアクセスできます。

カスタム ワークスペース URL またはバニティ URL を構成するには、次の手順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。

 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ち、リダイレクト URL が異なる新しい OAuthIDP プロ ファイルを構成します。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:

現在のプロフィール:

```
-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
```

新しいプロフィール:

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_Cu
-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 Adaptive Authentication 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なくなります。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。

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では、アップグレードのメンテナンス ウィンドウを選択できます。

重要:

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しないでください。すべ てのアップグレードは Citrix Cloud によって管理されます。

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。

Comple	ete these tasks to prepare and deploy Adaptive Authentication.	Schodulo upgradas
1	Provision Adaptive Authentication instances Provision Adaptive Authentication instances and optionally configure a connection with your on-premises network. Complete this step before proceeding to the next step See Details	Deprovision Secure Management Access
(2)	Configure authentication policies Create and apply policies for authentication, conditional access, device posture, and more using the management console. Complete this step before proceeding to the next step Access the Adaptive Auth admin console by visiting the IPs, or access by FQDN after adding dns entries (Active),	
3	Enable Adaptive Authentication for Workspace Select Adaptive Authentication as your preferred authentication method for subscribers signing in to Citrix Workspace. Complete this step before proceeding to the next step Take me to authentication in Workspace Configuration	
4	Connect an identity provider to access its user directory Make sure the identity provider of the directory you wish to access for user lookup and resource assignment is connected. Complete this step before proceeding to the next step Take me to identity and access management.	

- 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。

Schedule Upgrades ×					
Set the time and	day for	future u	pgrades to Adaptive Authentic	cation.	
Upgrade sche	duled s	ucces	sfully.		
Sunday			\sim		
At this time:			Select time zone:		
09:00	AM	PM	America/New_York	\sim	

Adaptive Authentication インスタンスのプロビジョニングを解除する

お客様は、以下の場合および 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。

- このシナリオは発生しない可能性がありますが、Adaptive Authentication インスタンスにはアクセスできません (特にスケジュールされたアップグレード後)。
- 顧客が VNet ピアリング モードからコネクタ モードに切り替える必要がある場合、またはその逆の場合。
- ・ 顧客が VNet ピアリング モードのプロビジョニング時に間違ったサブネットを選択した場合 (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します)。

注意:

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 インスタンスをプロビジョニング解除する前に、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 インスタンスをプロビジョニング解除するには、次の手順を実行します。

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。

Adaptive Authentication	
Complete these tasks to prepare and deploy Adaptive Authentication.	Schedule upgrades Deprovision Secure Management Access
(2) Configure authentication policies Create and apply policies for authentication, conditional access, device posture, and more using the management console. Complete this step before proceeding to the next step Access the Adaptive Auth admin console by visiting the IPs, or access by FQDN after adding dns entries (Active),	
Enable Adaptive Authentication for Workspace Select Adaptive Authentication as your preferred authentication method for subscribers signing in to Citrix Workspace. Complete this step before proceeding to the next step Take me to authentication in Workspace Configuration	
Connect an identity provider to access its user directory Make sure the identity provider of the directory you wish to access for user lookup and resource assignment is connected. Complete this step before proceeding to the next step Take me to identity and access management.	

2. プロビジョニング解除をクリックします。

注意:

プロビジョニングを解除する前に、Citrix Gateway をワークスペース構成から切断する必要があります。

1. Adaptive Authentication インスタンスをプロビジョニング解除するには、顧客 ID を入力します。

Deprovision	
Are you sure you want to deprovision adaptive authentication instances? Confirm by giving below information: Customer ID II understand that all Adaptive Authentication resources that Citrix provisioned or managed are deleted, including Citrix- managed VNets, VNet peering, public IP addresses, and gateway VMs. No customer-managed resources are affected. I understand that deprovisioning Adaptive Authentication deletes only resources that Citrix provisioned or managed. My customer-managed resources will remain intact. I understand that deprovisioning is going to remove configuration as well as the configuration backup of Adaptive Authentication instances and I confirm that I have taken the configuration backup for adaptive authentication instances.	
Deprovision	

- ゲートウェイへの安全なアクセスを有効にする
 - 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. セキュア管理アクセスをクリックします。

Secure Access to the gateway	×
Generate a private key to secure access to the Citrix Gateway command line interface.	
Keys should expire in:	
SSH Private Key Use this key with your SSH client so you can connect securely with the gateway.	
Generate and Download Key	

- 3. キーの有効期限はで、新しい SSH キーの有効期限を選択します。
- キーの生成とダウンロードをクリックします。SSH 秘密キーはページを閉じると表示されないため、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を使用して 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。

重要:

- Windows 上で 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 ロードした秘密キーを PEM に変換する必要があります。詳しくは、https://www.puttygen.com/c onvert-pem-to-ppkを参照してください。
- MAC のターミナルまたは Windows (バージョン 10) の PowerShell/コマンド プロンプト経由で 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 <path-to-private-key> authadmin@<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、そのユーザーを新し い管理者として LDAP グループに追加する必要があります。詳しくは、https://support.citrix.com/a rticle/CTX123782を参照してください。その他のすべての構成では、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。

Azure VNet ピアリングを使用してオンプレミスの認証サーバーへの接続を設定する

接続タイプとして Azure VNet ピアリングを選択した場合のみ、この構成を設定する必要があります。

注意:

Okta、Azure AD、Ping などのサードパーティの IDP を使用している場合、この手順は必要ありません。

1. Connect Adaptive Authentication UI で、**Provision** をクリックし、次に **Azure VNet Peering** をク リックします。

Provision Adaptive	e Authentication X
🕗 Overview	VNet peering
Provision	 Associate the Citrix managed service principal to your Viet The Citrix managed service principal is the application identity of the Citrix Viet in Azure. Completing this step allows the Citrix Viet to connect to your on-premises network through your Azure Viet. To complete this step, copy the service principal and assign an access role to it to grant access to your Viet.
Console access	Citrix Managed Service Principal: 72ft0741-5664-45b-aaf4-98cc91729ee8
Add FQDN	Copy service principal
Allowed IP addresses	2. Add your VNet
6 VNet peering	Enter your Azure tenant IU and then click retich to retrieve your customer-managea vivet resource lus, rrom the Azure porta, your Azure tenant IU is located in the Azure AU properties or your Azure subscription. Tenant ID
	Enter tenant ID Fetch
	3. Select a resource ID Select the resource ID for the VNet that you want to peer.
	🗷 Use Azure VPN Gateway
	Customer managed VNet Resource ID
	Select a resource ID V Add
	🔗 IP addresses successfully added.
Back Done	

Citrix マネージド サービス プリンシパル フィールドには、Citrix が顧客向けに作成した Azure サービス プリンシパルのアプリケーション ID が含まれます。このサービス プリンシパルは、Citrix がサブスクリプションおよびテナント内の VNet に VNet ピアリングを追加できるようにするために必要です。

このサービス プリンシパルが顧客テナントにログインできるようにするには、顧客サイトの管理者 (テナントのグローバル管理者) が次の PowerShell コマンドを実行して、SPN をテナントに追加する必要があり ます。CloudShell も使用可能です。Connect-AzureAD New-AzureADServicePrincipal -AppId \$App_ID ここで、\$App_ID は、Citrix によって共有される SPN アプリケーション ID で す。

注意:

- 前述のコマンドは、ロールの割り当てに使用する必要のあるサービス プリンシパル名を出力します。
- このサービス プリンシパルが Azure VNet ピアリングを追加できるようにするには、顧客サイトの管理者(グローバル管理者に限定されません)が、Citrix 管理 VNet にリンクする必要がある VNet に「ネットワーク共同作成者」ロールを追加する必要があります。
- SPN は、Azure 内の Citrix 仮想ネットワークを関連付けるために使用される一意の識別子です。SPN

を VNet に関連付けると、Citrix 仮想ネットワークは Azure の VNet を介して顧客のオンプレミス ネットワークに接続できるようになります。

1. VNet ピアリングを作成します。

• 前の手順を実行したテナント ID を入力し、[取得] をクリックします。

これにより、SPN のネットワーク コントリビューター ロールが追加される候補 VNet が、顧客管理の VNet リソース ID に入力されます。VNet が表示されない場合は、前の手順が正しく実行されていることを確認する か、手順を繰り返します。

注意:

テナント ID を見つける方法の詳細については、https://docs.microsoft.com/en-us/azure/activedirectory/fundamentals/active-directory-how-to-find-tenantを参照してください。

- 1. オンプレミス ネットワークを Azure に接続するには、Azure VPN Gateway の使用 を選択します。
- 2. 顧客管理 VNet リソース ID で、ピアリング用に識別された VNet を選択し、追加をクリックします。VNet は、最初は 進行中のステータスでテーブルに追加されます。ピアリングが正常に完了すると、ステータスが 完 了に変わります。
- 3. [完了] をクリックします。
- 4. 設定を続行します。「ステップ1: 適応型認証のプロビジョニング」を参照してください。

重要:

- Citrix 管理 VNet とオンプレミス ネットワークの間でトラフィックを流すには、オンプレミスでファイ アウォールとルーティング ルールを変更して、トラフィックを Citrix 管理 VNet に誘導する必要があり ます。
- 一度に追加できる VNet ピアは 1 つだけです。現在、複数の VNet ピアリングは許可されていません。必要に応じて、VNet ピアリングを削除したり、作成したりできます。

Adaptive A	Authentication is now connected
Ааа	ptive Authentication
Comple	ete these tasks to prepare and deploy Adaptive Authentication.
1	Provision Adaptive Authentication instances Provision Adaptive Authentication instances and optionally configure a connection with your on-premises network. Complete this step before proceeding to the next step See Details
2	Configure authentication policies Create and apply policies for authentication, conditional access, device posture, and more using the management console. Complete this step before proceeding to the next step Access the Adaptive Authentication management console by visiting 20.106.227.13 (Primary). You can also add DNS entries for 20.106.227.13 (Primary) and 20.127.209.21 (Secondary) and access the management console using FQDN. Since primary instance may change, Click here to refresh the instance IPs.
3	Enable Adaptive Authentication for Workspace Select Adaptive Authentication as your preferred authentication method for subscribers signing in to Citrix Workspace. Complete this step before proceeding to the next step Enable
4	Connect an identity provider to access its user directory Make sure the identity provider of the directory you wish to access for user lookup and resource assignment is connected. Take me to identity and access management.

設定のバックアップと復元

アプリケーション配信管理サービスは、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。

1.「アプリケーション配信管理」タイルで、「管理」をクリックします。

2. インフラストラクチャ>インスタンスに移動して、バックアップにアクセスします。

注意:

オンボードされたサービスが表示されない場合は、Application Delivery Management サービスをオンボ ードします。詳細については、「はじめに」を参照してください。

LDAP および LDAPS 負荷分散構成のサンプル

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 LDAP/LDAPS サポートを提供します。

注意:

- LDAP/LDAPS の負荷分散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 サーバー用のサービスまたはサーバーを作成しないでください。
- LDAP の負荷分散を使用している場合は、サービス グループを作成し、それをスタンドアロン サービス

ではなく負荷分散サービスにバインドします。

- 認証に負荷分散仮想サーバーを使用する場合は、LDAP アクションに実際の LDAP サーバー IP アドレスではなく、負荷分散仮想サーバーの 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、TCP モニターは作成したサービスにバインドされます。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 モニターの使用をお勧めします。

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、ダミーの IP アドレスにすることができます。

負荷分散 LDAP サーバー

負荷分散 LDAP サーバーの場合は、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。 LDAP サーバーの負荷分散用のサービスを作成しないでください。

NetScaler CLI を使用して LDAP を構成します。

LDAP を構成するには、次の CLI コマンドを参考にすることができます。

- 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 グループに構成さ 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 を構成します。

- 1. トラフィック管理>負荷分散に移動し、仮想サーバーをクリックします。
- 2. タイプ TCP およびポート 389 の仮想サーバーを作成します。

SSL/SSL_TCP タイプの負荷分散仮想サーバーを作成しないでください。

3. トラフィック管理>負荷分散に移動し、サービス グループをクリックします。

- 4. タイプ TCP およびポート 389 のサービス グループを作成します。
- 5. 手順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設定」を参照してください。

負荷分散 LDAPS サーバー

LDAPS サーバーの負荷分散では、Adaptive Authentication インスタンスへの内部 SSL 暗号化または復号化を回 避するために、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 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を作成しないでください。

NetScaler CLI を使用して LDAPS を構成します。

LDAPS を設定するには、次の CLI コマンドを参考にしてください。

- 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 を構成します。

- 1. トラフィック管理>負荷分散に移動し、仮想サーバーをクリックします。
- 2. タイプ TCP およびポート 636 の仮想サーバーを作成します。

SSL/SSL_TCP タイプの負荷分散仮想サーバーを作成しないでください。

- 3. トラフィック管理>負荷分散に移動し、サービスをクリックします。
- 4. SSL_TCP タイプとポート 636 のサービスを作成します。
- 5. 手順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、「基本的な負荷分散の設定」を参照してください。

カスタムモニターを作成する

NetScaler GUI を使用してカスタム モニターを作成します。

1. Traffic Management > Load Balancing > Monitors 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 秒に設定し、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。

最大 15 個の管理 IP アドレスを追加可能

Adaptive Authentication サービスを使用すると、最大 15 個のパブリック IP サブネットと個別の IP アドレスを 入力して、Adaptive Authentication 管理コンソールにアクセスできます。

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 ~/32.B の範囲内であることを確認します。
- エントリ間に重複がないことを確認してください。

例:

- 192.0.2.0/24 と 192.0.2.8 は受け入れられません。192.0.2.8 は 192.0.2.0/24 内にあるためです。
- 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ときに、IP アドレス値としてネットワーク IP アドレスを入力します。
 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。

この機能を有効にするには、Citrix サポートにお問い合わせください。

認証方法を適応認証に移行する

認証方法を **Citrix Gateway** として Adaptive Authentication をすでに使用しているお客様は、**Adaptive Authentication** を移行し、Adaptive Authentication 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、切断をクリックします。

4	Identity a	nd Access	Manager	nent									
	Authentication	Administrators	API Access	Domains	Recovery								
	Set up the vario	us ways you need y	our Citrix Cloue	d administrat	ors and Citrix	Workspace	e subscribers t	o sign in.					
	Citrix Ide Admin Sig	ntity n-in URL: https://cit	trix.cloud.com						•	Connect	ed		
	Azure Ac	tive Directory 🚱							0	Not Con	nected		
	Active Dir	rectory 💿							0	Not Con	nected		
	Active Dir	rectory + Token							0	Not Con	nected		
	Citrix Gat	teway 💿							•	Connect	ed		
	Okta 🕑								0	Not Con	Manage sub Disconnect	scriber a	access
	SAML 2.0	0							0	Not Con	nected		
	Adaptive	Authentication							0	Not Con	nected		(

3. 加入者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 ログインが影響を受け、Adaptive Authentication が再度有効になるまで、認証に Adaptive Authentication は使用されません。

4. Adaptive Authentication 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>
1
    rm authentication oauthIdpPolicy <oauthIdpPolName>
2
3
```

rm authentication oauthIdpProfile <oauthIdpProfName>

GUI を使用する場合:

- a) セキュリティ > AAA-アプリケーショントラフィック > 仮想サーバに移動します。
- b) OAuth ポリシーのバインドを解除します。
- 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。[認証] タブの [適応型認証] で、省略 記号メニューをクリックし、[管理]を選択します。

または、https://adaptive-authentication.cloud.comにアクセスします。

6. 詳細を見るをクリックします。

- 7. 証明書のアップロード 画面で、次の操作を行います。
 - アダプティブ認証 FQDN を追加します。
 - 証明書とキーファイルを削除して再度アップロードしてください。

Provision Adaptiv	e Authentication
Overview	Add FQDN and certificate key pair
Provision	Enter the FQDN for the adaptive authentication IDP access and upload an SSL certificate and private key to secure the end user requests. You can obtain a certifica that the key strength of the certificate keys is 2,048 bits or higher and that the keys are signed with secure signature algorithms.
Console access	FQDN
4 Upload Certificate	
5 Allowed IP addresses	Please add DNS mapping for the FQDN to the public IP
	Select the type of certificate you will upload: PEM (Privacy Enhanced Mail)
	Certificate Upload certificate
	Key Upload key
	Password for key (only required if key is encrypted) Key Password
	User successfully added

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 方式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。ポリシーは指定された優先度にすで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バインド解除すること はできません。
- 8. 変更を保存をクリックします。

この時点で、Identity and Access Management では、**Adaptive Authentication** が 接続済み として 表示され、Adaptive Authentication インスタンスには OAuth プロファイルが自動的に構成されます。

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) セキュリティ > **AAA**-アプリケーショントラフィック > 仮想サーバに移動します。OAuth IdP プロファ イルが作成された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。適応認証は 接続済み 状態で す。
- 9. Adaptive Authentication ホームページで 有効 (手順 3) をクリックして、Adaptive Authentication 方式 を再度有効にします。
 - Enable Adaptive Authentication for Workspace
 Select Adaptive Authentication as your preferred authentication method for subscribers signing in to Citrix Workspace.
 Complete this step before proceeding to the next step

この手順により、ワークスペース構成で認証方法として Adaptive Authentication が有効になります。

10. 有効をクリックした後、手順3でワークスペース リンクをクリックします。認証方法が Adaptive Authentication に変更されていることを確認する必要があります。

注意:

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。

認証構成のサンプル

顧客は、選択した認証ポリシーを構成し、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 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。以下に使用例をいくつか示しま 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 と RADIUS によるデュアル ファクタ認証 (ユーザー入力は1回のみ)
- 組織内のユーザーの部門(従業員、パートナー、ベンダー)に応じた認証ログオン方法(部門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によるユーザードメインに応じた認証ログオン方法
- 電子メール ID (またはユーザー名) 入力を最初の要素として設定し、電子メール ID を最初の要素としてグループ抽出に基づく条件付きアクセスを設定し、グループごとに異なるログオン タイプを提供します。
- ユーザー証明書を持つユーザーの場合は証明書認証を使用し、証明書を持たないユーザーの場合はネイティブ OTP 登録を使用する多要素認証
- ユーザーのホスト名入力に応じて条件付き認証を行う異なる認証タイプ
- ネイティブ OTP 認証による二要素認証
- Google 再 CAPTCHA

多要素認証によるサードパーティ統合

- Azure AD を SAML IdP として構成します (次の要素を LDAP ポリシーとして構成 OAuth 信頼を完了する には NO_AUTH を使用します)
- 最初の要素として SAML を使用した条件付き認証、その後 SAML 属性に基づいて証明書または LDAP にカス タム ログインする
- 最初の要素は Web 認証ログイン、次に LDAP

デバイス姿勢スキャン (EPA)

- デバイスポスチャチェックによるバージョンチェックの後、準拠ユーザー (RADIUS) と非準拠ユーザー (LDAP)のカスタマイズされたログインを実行します。
- LDAP 認証に続いて必須のデバイスポスチャスキャン
- AD 認証前後のデバイスポスチャチェック EPA 前後を要因として
- EPA 要素としてのデバイス証明書

その他のシナリオ

- 認証付き EULA を追加する
- nFactor ポリシーラベル、ログインスキーマをカスタマイズする

インスタンスのディスク容量管理

June 19, 2024

アダプティブ認証チームは、アダプティブ認証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。 そのため、アダプティブ認証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。デフォルトでは、Citrix がアダプティブ認証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容量をクリアします。 機密情報、専有情報、または個人情報を次のディレクトリに保存しないことをお勧めします:

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

注記:

- /var/nsinstall ディレクトリはアップグレード中に最初にクリアされ、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。
- お客様は、NetScalerのディスク容量とディスククリーンアップを管理および保守する責任を負います。

ディスク容量を自分で管理するオプション

デフォルトでは、Citrix がアダプティブ認証インスタンスを管理しますが、インスタンスのディスク容量を自分でク リーンアップすることもできます。次の手順を実行して、デフォルトの方法をオプトアウトできます。

- 1. アダプティブ認証ナビゲーションペインで、[インスタンス管理]をクリックします。
- 2. [自分でディスク容量を管理する]を選択し、確認メッセージダイアログボックスの [確認] をクリックします。
- 3. [変更の保存] をクリックします。

Provision Adaptive	e Authentication ×
Overview Provision Console access	Disk space management As part of Adaptive Authentication management, disk space on Adaptive Authentication instances must be cleared by Citrix before applying upgrades. For this reason, do not keep any sensitive, proprietary, or personal information in in directories /var/tmp and /var/nsinstall. Read more I prefer Citrix to manage diskspace.
Upload Certificate Allowed IP addresses	I preter to manage diskspace myselt.
Manage Connectivity Instance Management	
Close Save Char	nges

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 チームは、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について詳しくは、「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。 アダプティブ認証の問題のトラブルシューティング

June 19, 2024

問題は、設定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問題
- AD/RADIUS 接続と認証に関する問題
- 認証に関する問題
- 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 を使用して問題のトラブルシューティングを行うこともできます。CLI に接続するには、次の 操作を行います。

- putty/securecrt などの SSH クライアントをマシンに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。
- 認証情報でログインします。

詳しくは、「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には、必ずログレベルを有効にしてください。

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 CLI にログインします。
- 2. PuTTY を使用して、管理認証情報を入力します。
- 3. コマンドset audit syslogParams logLevel ALLを実行する

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. [構成]>[システム]>[監査]に移動します。
- 3. [監査] ページの [設定] で、[監査 Syslog 設定の変更] をクリックします。
- 4.「ログレベル」で「すべて」を選択します。

プロビジョニングに関する問題

• アダプティブ認証 **UI** にアクセスできません

顧客 ID/テナントで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 分以上動かなくなる

エラーのスクリーンショットを収集し、Citrix サポートにお問い合わせください。

- VNet ピアがダウンしています
 - このピアリングに対応するアラートが Azure Portal にあるかどうかを確認し、推奨されるアクション を実行します。
 - ピアリングを削除し、アダプティブ認証 UI から再度追加します。
- プロビジョニング解除は完了していません

Citrix サポートに連絡してください。

インスタンスのアクセシビリティ問題

- 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どうかを確認します。
 - 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あるかどうかを検証します。
- インスタンスにログインできません

プロビジョニング中に入力した認証情報で、管理者アクセスが正常に機能していることを確認します。

• エンドユーザーには完全な権限がない

ユーザーを追加するときに、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。 詳しくは、「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の問題:

- 顧客管理の Azure VNet がアダプティブ認証インスタンスから到達可能かどうかを確認します。
- 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かどうかを確認します。
- オンプレミスから Azure VNet にトラフィックを誘導するために、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 で利用でき、各ログには [NS_AAUTH_TUNNEL] という接頭 辞が付いています。

- ログの ConnectionId を使用して、さまざまなトランザクションを相互に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ます。その IP アドレスはコネクタのソース IP アドレスだからです。

認証要求ごとに、アダプティブ認証インスタンス(NS-AAAD プロセス)と認証サーバの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ます。

• コネクタはインストールされているが、オンプレミス接続が失敗する。

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"

次のサンプルログが認証要求の ns.log ファイルに出力されない場合は、トンネルの確立中に問題が発生して いるか、コネクタ側から何らかの問題がある可能性があります。

ログの詳細を確認し、適切なアクションを実行してください。

ログの詳細	修正アクション
接頭辞[NS_AAUTH_TUNNEL]の付いたログはログ ファイルに含まれません	show cloudtunnel vserverコマンドを実行 します。このコマンドは、状態が UP の両方 (TCP と UDP) のクラウドトンネル仮想サーバーを一覧表示する 必要があります。
[NS_AAUTH_TUNNEL] Waiting for outbound from connector このログで、次 の応答が受信されなかった場合: [NS-AAUTH- TUNNEL] Received connect command from connector and client connection lookupsucceeded"	コネクタマシンがアダプティブ認証 FQDN に到達でき るかどうかを確認するか、またはコネクタ側のファイア ウォールでアダプティブ認証 FQDN へのアウトバウン ド接続を確認します。

ログの詳細	修正アクション
[NS_AAUTH_TUNNEL] Server is down or couldn't create connection to ip 0.0.0.0# & & [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。
bailing out"	

コネクタから応答がありません:

- アダプティブ認証 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ます。
- Adaptive Authentication インスタンス上のサーバー証明書にバインドされ、リンクされた中間証明書があることを確認します。

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 アドレスの場合は、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、次の手順を実行します。

```
1 set policy expression aauth_allow_rfc1918_subnets "(CLIENT.IP.DST
.BETWEEN(10.0.0,10.255.255.255) || 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、次の手順を実行します。
 - 1. [Appexpert] > [式] に移動します。
 - 2. aauth_allow_rfc1918_subnets という式を追加します。

トンネルが確立されても認証に失敗する場合は、次の手順を使用して問題のトラブルシューティングを行います。

LDAP:

- バインド DN の詳細を検証します。
- 接続テスト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。

```
1 shell
```

```
2 cd /tmp
```

```
3 cat aaad.debug
```

一般的な LDAP エラー:

- サーバータイムアウト-LDAP クエリに対する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、https://support.citrix.com/article/CTX138663を参照してください。

Radius:

 コネクタ IP アドレスは、RADIUS サーバ構成で 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 のアサーションエラーを投稿する
 - 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件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。
 - 1 cat /var/log/ns.log
 - OAuth プロファイルパラメータを検証します。
- Azure AD 認証がアサーション後にスタックする

認証をオフに設定して、次の要素として AD 認証を追加します。これは、認証を成功させるために必要なすべ ての要求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ていますが、プラグインをダウンロードするように求めるプロンプトがユーザーに表示されます。

考えられる原因: バージョンの不一致またはファイルの破損

- 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のバージョ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 のクライアントバージョンが、クライアントマシンのクライアントバージョンと同じである ことを確認します。

NetScaler のクライアントを更新します。

アダプティブ認証インスタンスで、[**Citrix Gateway**] > [グローバル設定] > [クライアントライブラ リの更新] に移動します。

Citrix ダウンロードの EPA プラグインライブラリページには、詳細情報が表示されます。

- バージョンが更新されても、要求が 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、「https://support.citrix.com/article/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に EPA の設定 ([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ています。
 - 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設定した後、アプリケーションは利用できません
 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タグが定義されていることを確認します。

Workspace デリバリーグループにタグがすべて大文字で追加されていることを確認します。

これが機能しない場合は、ns.logを収集し、Citrix サポートに連絡することができます。

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、インサイト分析のためにSDX および VPX アプライアンスか ら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。詳しくは、「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。

アダプティブ認証を使用したスマートアクセス

June 19, 2024

Citrix Cloud のお客様は、Citrix Workspace への IdP として適応型認証を使用して、Citrix DaaS リソース (Virtual Apps and Desktops) へのスマートアクセス (アダプティブアクセス) または Secure Private Access サ ービスを提供できます。 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 Workspace または Citrix DaaS に表示できます。適応型認証サービスでは、デバイスポスチャ (EPA)、ネットワー クロケーション (企業ネットワークの内部または外部、位置情報)、ユーザーグループなどのユーザー属性、時間帯、 またはこれらのパラメータ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。その後、Citrix DaaS 管理者は このポリシー情報を使用して、Virtual Apps and Desktops へのコンテキストアクセスを構成できます。Virtual Apps and Desktops は、以前のパラメーター (アクセスポリシー) に基づいて列挙することも、基にしないことも できます。クリップボードアクセス、プリンタリダイレクト、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。

ユースケースの例:

- 管理者は、アプリのグループを、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 はアクセスするように構成できます。
- 管理者は、企業の管理対象デバイスからのみアプリグループを表示またはアクセスするように設定できます。
 たとえば、EPA スキャンでは、デバイスが企業管理か BYOD かを確認できます。EPA のスキャン結果に基づいて、ユーザーに関連するアプリを列挙できます。

前提条件

- IdP としてのアダプティブ認証は、Citrix Workspace 用に構成する必要があります。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 によるアダプティブ認証サービスが稼働しています。
- アダプティブアクセス機能が有効になっています。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ためのイベントの流れを理解する

- 1. ユーザーは Citrix Workspace にログインします。
- 2. ユーザは IdP として設定された適応型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した。
- 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. アダプティブ認証サービスはタグを Citrix Graph サービスにプッシュします。ユーザーは Citrix Workspace のランディングページにリダイレクトされます。
- 7. Citrix Workspace は、このユーザーセッションのポリシー情報を取得し、フィルターを照合して、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、Citrix DaaS のアクセスポリシーを構成して、ユーザーの ICA アクセスを制限します。

適応型認証インスタンスでのスマートアクセスポリシーの設定

適応型認証インスタンスでのスマートアクセスポリシーの設定は、次の2段階のプロセスです:

- アダプティブ認証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。
 たとえば、ステップ1を参照してください。
- 2. リソースアクセス用の DaaS/Secure Private Access にも同じタグを定義します。たとえば、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にはアクセスを許可し、クリップボードへのアクセス はブロックするようにスマートアクセスポリシーを構成する

ステップ1:アダプティブ認証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設定する

- 1. アダプティブ認証インスタンスにログインします。
- 2. 適応型認証仮想サーバに移動します([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])。
- 3. 認証仮想サーバーを選択し、[編集]をクリックします。
- 4.「スマートアクセスポリシー」をクリックします。
- 5. 要件に応じてポリシーの表現を定義します。
 - a) [Add Binding] をクリックします。
 - b)「ポリシーの選択」で、「追加」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にアクセスを許可する例として、次の式を入力します。 HTTP.REQ.HEADER("User-Agent").CONTAINS("Chrome")

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

Authentication Smart Access Policy Binding > Smart Access Policies > Create Authentication Smart Access Policy	
Create Authentication Smart Access Policy	
Name*	
SmartAccessPolicy	
Action*	
citrixtagroup V Add Edit	
Expression*	xpression Editor
Select V Select V	
HTTPREQ.HEADER("User-Agent").CONTAINS("Chrome")	
	Eveluate
	Evaluate
Comments	
Create Close	

- 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) [アクション]で[追加]をクリックします。
 - b) [名前] に、スマートアクセスプロファイルの名前を入力します。
 - c)「タグ」で、スマートアクセスタグを定義します。たとえば、TAG-CHROME。

Authentication Smart Access Policy > Policy Binding > Smart Access Policies > Create Authentication Smart Access Policy > Create Authentication Smart Access Policy	ile
Create Authentication Smart Access Profile	
Name* SmartTag1 Tags* TAG-CHROME Comment	
Create	

- 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、[バインドの追加]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。

Authentic	ation Smart Access Policy > Policy Binding > Smart Access Polic	cies								
Smart	Access Policies 🕕									×
Select	Add Edit Delete Show Bindings									
Q Click he	re to search or you can enter Key : Value format									0
	NAME		EXPRESSION		REQUEST SERVER					
۲	SmartAccessPolicy		HTTP.REQ.HEADER("User-Agent").CONTAINS("Chrome	7						
Total 1						25 Per Page	\sim	Page	1 of 1	 $ \mathbf{b} $

注:

[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]>[詳細ポリシー]>[スマート アクセス]>[ポリシー]からスマートアクセスポリシーを作成し、それを認証仮想サーバ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」を使用してポリシーを追加します。詳しくは、「Citrix Studio でのタグの定 義」を参照してください。

ユースケース 2: EPA の結果に基づいて認証後のスマートアクセスポリシーを設定

ステップ **1:** アダプティブ認証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設定する エンドポイント分析などの条件に基づいてスマートアクセスするには、nFactor フローを設定し、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。

EPA を nFactor フローのファクターとして構成するには、「EPA をファクターとして構成する」を参照してください。

ロジカルフロー

- 1. ユーザーはワークスペース URL にアクセスします。
- 2. ユーザは、認証/EPA の適応型認証にリダイレクトされます。
- 3. エンドポイント分析はエンドユーザーで行われ、結果は定義済みのデフォルトグループにユーザーを追加する ことによって保存されます。
- 4. ユーザーは次の認証フローに進むように求められます。
- 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。

構成

ウイルス対策がインストールされたマシンからアクセスするユーザーには、準拠していることを示すマークを付け、 フルアクセスを許可する必要があります。ただし、ウイルス対策ソフトがインストールされていないユーザーマシン は、非対応としてマークし、アクセスが制限されている必要があります。

- EPA の nFactor ポリシーを作成します。詳細については、「要素としての EPA の設定」を参照してください。
 nFactor フローでは、最初のファクターがユーザー認証ファクターであることを確認します。
- 2. EPA 式を選択して、ウイルス対策ソフトウェアが存在するかどうかを確認します。
- 3. EPA アクションで、デフォルトグループを定義します。

Name	
EPA-client-scan	
Default Group	
Compliant	\odot
Quarantine Group	
(ill Process	
Delete Files	
xpression *	
Select V Select	✓ Select ✓
sys.client_expr("app_0_ANTIVIR_0_0)_VERSION_<_1.2_AUTHENTIC_==_TRUE_RTP_==_TRUE[COMMENT: Generic Antivirus Product Scan]")

EPA が正常に実行されると、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) アダプティブ認証インスタンスにログインします。
 - b) 適応型認証仮想サーバに移動します([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])。
 - c) 適応型認証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) 次の式で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 (「準拠」)-ユーザー EPA 合格条件用
 - ・ !AAA.USER.IS_MEMBER_OF (「準拠」) ユーザー EPA 障害状態の場合
 - f) これらのポリシーの両方にスマートアクセスタグを定義します。

例:

- AAA.USER.IS_MEMBER_OF ("Compliant")の COMPLIANT タグが付いたタグ 名SmartTag1
- !AAA.USER.IS_MEMBER_OF ("Compliant")NONCOMPLIANT タグが付いたタ グ名SmartTag2

スマートアクセス用の EPA を条件とする適応型認証インスタンスの設定が完了しました。

必要に応じてタグと式を設定できます。

Authentication Smart Access Policy		
Add Binding Unbind Regenerate Priorities No action V		
Q Click here to search or you can ente		
PRIORITY POLICY NAME	© EXPRESSION © ACTION	GOTO EXPRESSION
90 compliant-EPA-pass	AAA.USER.IS_MEMBER_OF("Compliant") SmartTag1	END
110 noncompliant-EPA-fail	IAAA.USER.IS_MEMBER_OF("Compliant") SmartTag2	END
Close		
Authentication Smart Access Policy > Configure Authentication Smart Access Profile Configure Authentication Smart Access Profile	Authentication Smart Access Policy > Configure Authentication Smart Access Profile	
Name SmartTag1 Tags* COMPLIANT Comment	Name SmartTag2 Tags* NONCOMPLIANT Comment	
CK Close	OK Close	

ステップ **2: DaaS Studio** でスマートアクセスタグを設定する スマートタグ「準拠」と「非準拠」のポリシーを それぞれのデリバリーグループに追加します。詳しくは、「Citrix Studio でのタグの定義」を参照してください。

DaaS Studio でタグを定義

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

例:BranchOffice ユーザーは、すべてのアプリケーションを含むアダプティブ・アクセス・デリバリー・グループの アプリケーションを確認する必要があります。

一方、WorkFromHome ユーザーは、WFH デリバリーグループ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。詳しくは、「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。

Edit Delivery Group)			×
Users	Access Policy			
Desktops	You can restrict access for users made through Citrix Gateway. Fo	through Smart Acce or example, you can re	ss policy expressions that filter user estrict machine access to a subset of	connections fusers and
Application Prelaunch	specify allowed user devices.			
Application Lingering	Policy		Status	
	Citrix Gateway connections	Default	Enabled	0
User Settings	Non-Citrix Gateway connect	ions Default	Enabled	0
StoreFront				
App Protection				
Scopes				
Access Policy				
Restart Schedule				
License Assignment				
	Add			

- 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、次の手順を実行して、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してください:
 - 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、[任意に一致]を選択して、条件を追加 します。

Connections meeting the following criteria	
O Match all O Match any	
Filter:	Value:
Workspace	LOCATION_TAG_HOME
+ Add criterion	

WorkFromHome ユーザーの場合は、それぞれの Delivery Controller に次の値を入力します。

ファーム: ワークスペース

フィルター: LOCATION_TAG_HOME

BranchOffice ユーザーの場合は、各 Delivery Controller で次の値を入力します。

フィルター: ワークスペース

値: ロケーション _ タグ _ ブランチオフィス

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。

提供されているアプリケーションへのアクセスの種類を制限する

例: 在宅勤務のユーザーにはクリップボード権限があってはなりません。

- 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。

Edit Policy Disable-clipborad-Home		×
Select Settings	Assign Policy To	
2 Assign Policy To	Selected user and machine objects All objects in the site	
3 Summary	User and machine objects: 1 selected	View selected only
	 Access control Applies to user settings only Allow - Workspace, LOCATION_TAG_HOME Apply policy based on the access control conditions through which a client connects. 	Edit Unassign
	> Citrix SD-WAN Applies to user settings only	Assign
	 Client IP address Applies to user settings only 	Assign
	 Client name Applies to user settings only 	Assign
	> Delivery Group Applies to all settings	Assign
	> Delivery Group type Applies to all settings	Assign
	 Organizational Unit (OU) Applies to all settings 	Assign
	Tag Applies to all settings	Assign
	> User or group Applies to user settings only	Assign

- 7. 次の詳細を含む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:-ワークスペース
 - アクセス条件:LOCATION_TAG_HOME (すべて大文字)

Assign Policy Access control				
Apply policy ba Access control	ased on the access control condition	ns through which a client connects.		
Mode	Connection type	Gateway farm name	Access condition	
Allow	With Citrix Gateway	Workspace	LOCATION_TAG_I +	🗸 Enable

- 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。

Summary						
Enable policy						
View a summary of the settings you configured and provide a name for your new policy. Policy name:						
Description:	Disable clipboard access for users working from home					
Settings configu	ured: 1	Assigned to: 1 user and machine objects				
Client clipboa User setting - Prohibited (De	ard redirection ICA efault: Allowed)	Access control Applies to user settings only				

これで、アクセスをテストする準備が整いました。

よくあるエラーのトラブルシューティング

• 問題: 「リクエストを完了できません」というメッセージが表示される。

解像度

- 1. アダプティブアクセスが有効になっていることを確認します。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。
- 2. この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、スマートタグがアダプティブ認証からワークスペースにプッシュされない場合や、DaaS または Secure Private Access で受信され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ヒットしていないか確認してください。詳しくは、https://support.citr ix.com/article/CTX138840を参照してください。
- Citrix アダプティブ認証インスタンスがcas.citrix.comに接続できるかどうかを確認します。
- スマートタグの詳細については、アダプティブ認証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で LogLevel パラメータ ーがALLに設定されていることを確認します。
 - * puttyを使用して適応型認証プライマリ・インスタンスにログインします。

タイプ: シェル

- cd /var/log
- cat ns.log | more or cat ns.log | grep -I "smartaccess"
- それでも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設定変更

次のディレクトリの高可用性セットアップでは、ファイル同期が遅れることがあります。その結果、Citrix ADM 登録 中に作成されたキーは時間どお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を解決するには、次の手順を実行してセカンダリでset cloudコマンドを再実行します。

```
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

サイジングとパフォーマンスのガイドライン

June 19, 2024

適応型認証では、顧客はデータセンターに展開された Cloud Connector または Azure VNet Peering のいずれか を使用してオンプレミスの認証サーバーにアクセスできます。これは、顧客が管理する VNet からデータセンターの 到達可能性がすでに確立されている場合に備えます。このトピックには、Citrix Cloud Connector と Azure VNet ピアリングの両方の展開メントのパフォーマンス数値に関する情報と、Citrix Cloud Connector マシンの推奨スケ ールとサイズの構成に関する情報も含まれています。

ユーザー認証レート

サイズが2のvCPUと7GB RAMのコネクタ仮想マシンは、1秒あたり14人の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4認証/秒を超え ると、コネクタサービスが失敗します。この速度は、障害がいくつ発生してもコネクタサービスを再起動するように 構成することで実現できます(**Citrix Netscaler Cloud Gateway >** リカバリ **>** サービスの再起動)。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 Connector を使用する場合のトラフィックレイテンシーとユーザー認証レート

次の表は、Citrix Cloud Connector を使用する場合のトラフィックレイテンシーとユーザー認証率を示しています:

		1秒あたりの認証またはユーザーロ
認証の種類	認証待ち時間 (p95) (ミリ秒)	グインレート
LDAP	5.99	14
RADIUS	3.17	14
LDAP+RADIUS	4.59	14
LDAPS	26.75	14
LDAPS+RADIUS	15.61	14

Azure VNet ピアリングを使用する場合のトラフィックレイテンシーとユーザー認証レート

次の表は、Azure VNet ピアリングを使用する場合のトラフィック遅延とユーザー認証率を示しています:

		1秒あたりの認証またはユーザーロ
認証の種類	リクエスト遅延 (p95) (ミリ秒)	グインレート
LDAP	6.95	17.54
LDAPS	7.19	16.98

データガバナンス

June 19, 2024

このトピックでは、Citrix Adaptive Authentication Service 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、および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](https://www.citrix.com/en-in/buy/licensing/agreements.html)

0

- アダプティブ認証サービス: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。
- アダプティブ認証インスタンス:管理者がユーザー認証を管理できるようにするために、アダプティブ認証サ ービスによって展開された NetScaler ADC 仮想マシン。

データ所在地

アダプティブ認証サービス

Citrix アダプティブ認証サービスの顧客コンテンツデータは、Azure クラウドサービス東部リージョンにあります。 これらは、可用性と冗長性のために次の 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

以下は、サービス構成ログとランタイムログの異なる宛先です。

- 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を対 象としています。
- 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 システムログサービス。詳しくは、「Citrix Cloud Services の顧客コンテンツとログの処理」および「地理的な考慮事項」を参照してください。

アダプティブ認証インスタンス

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 アダプティブ認証サービスを使用すると、顧客管理者はアダプティブ認証 UI を介してサービスを構成し、コ ンソールからコンパニオン Connector Appliance を介してサービスを構成できます。次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) と IP アドレス。
 - IP アドレス/範囲、ポート、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、ネットワークコントリビューターロールを持つサービスプリンシパル。
 詳しくは、「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。詳しくは、「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、およびリソースの場所の識別子
 - 内部プロキシ設定

サービスコンポーネントによって収集されたランタイムログの場合、重要な情報は次のもので構成されます。

- クライアント IP アドレスとポート
- 送信先 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
- 要求バイト数
- 応答バイト数
- 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)

バーチャルマシン名

データ送信

Citrix アダプティブ認証サービスは、トランスポート層セキュリティで保護された宛先(Splunk)にログを送信します。

データ管理

Citrix アダプティブ認証サービスは現在、ログの送信をオフにしたり、お客様のコンテンツがグローバルに複製され ないようにした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いて、お客様の構成データは、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。

ログの宛先は、サービス固有のデータ保持ポリシーを維持します。

- NetScaler Application Delivery Management に保存されているイベント用。NetScaler ADM のデータ ガバナンスを参照してください。
- Splunk ログはアーカイブされ、90日 (約3か月)後に削除されます。
- アダプティブ認証インスタンスは、サブスクリプションの有効期限が切れてから 30 日 (約 4 週間半)後に割り 当てが解除されます。

データのエクスポート

いくつかのタイプのログには、さまざまなデータエクスポートオプションがあります。

- 管理者監査ログには、Citrix Cloud システムログコンソールからアクセスできます。
- Splunk のログは顧客には使用できません。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、Citrix がサービスを実行するためのアクセス権を与えられているお客様の環境内のスト レージまたはデータのために顧客アカウントにアップロードされる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、および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、お客様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。

citrix

© 2024 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.