citrix

フェデレーション認証サービス 2103

Contents

フェデレーション認証サービス 2103	2
フェデレーション認証サービス 2103	2
解決された問題	2
既知の問題	3
サードパーティ製品についての通知	3
システム要件	3
インストールと構成	4
詳細な構成	21
証明機関の設定	21
秘密キー保護	28
セキュリティとネットワークの構成	45
パフォーマンスカウンター	59
Windows ログオンの問題のトラブルシューティング	60
PowerShell コマンドレット	77
展開アーキテクチャ	77
ADFS の展開	87
Azure AD の統合	91

フェデレーション認証サービス 2103

June 23, 2023

フェデレーション認証サービス 2103 (PDF ダウンロード)

この製品バージョンのドキュメントは最新リリースではありません。最近更新されたコンテンツについては、フェデ レーション認証サービスの最新リリースに関するドキュメントを参照してください。

注:

PDF から外部サイトへのリンクは正しいサイトに移動しますが、ドキュメント内を移動するリンクは無効になっています。

フェデレーション認証サービス 2103

November 9, 2021

フェデレーション認証サービス 2103 には、次の新機能が含まれています。修正プログラムについて詳しくは、「解決 された問題」を参照してください。

Citrix_SmartcardLogon 証明書テンプレートの強化

Citrix_SmartcardLogon 証明書テンプレートのアプリケーションポリシーの拡張に、「クライアント認証」および 「スマートカードによるログオン」が含まれるようになりました。[AUTH-812]

パフォーマンスカウンターの向上

Windows パフォーマンスモニターに表示されるカウンター名やカウンター機能など、さまざまな面での FAS パフォ ーマンスカウンターの向上。「パフォーマンスカウンター」を参照してください。

解決された問題

June 29, 2021

フェデレーション認証サービス 2103 で解決された問題はありません。

既知の問題

June 29, 2021

フェデレーション認証サービス 2103 には既知の問題はありません。

レジストリエントリの変更を伴う回避策については、次の点に注意してください:

警告:

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再 インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックス では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レ ジストリファイルのバックアップを作成してから、レジストリを編集してください。

サードパーティ製品についての通知

November 9, 2021

フェデレーション認証サービスのこのリリースには、次のドキュメントで定義された条件の下でライセンスが有効に なったサードパーティのソフトウェアが含まれている可能性があります:

- Citrix Virtual Apps and Desktops サードパーティ製品についての通知 (PDF ダウンロード)
- Non-Commercial Software Disclosures For FlexNet Publisher 2017 (11.15.0.0) (PDF のダウンロード) (英語)
- FLEXnet Publisher Documentation Supplement Third Party および FlexNet Publisher 11.15.0 で 使用されるオープンソースソフトウェア(PDFのダウンロード)(英語)

システム要件

September 30, 2021

- フェデレーション認証サービス(FAS)は、次の Windows Server バージョンでサポートされています:
 - Windows Server 2019 の Standard Edition、Datacenter Edition、および Server Core オプショ ン付き
 - Windows Server 2016 の Standard Edition、Datacenter Edition、および Server Core オプショ ン付き

- FAS は、ほかの Citrix コンポーネントを含まないサーバーにインストールすることをお勧めします。
- Windows サーバーはセキュリティ保護されている必要があります。Windows サーバーには登録機関の証明 書および秘密キーへのアクセス権限があり、ドメインユーザーに対して自動的に証明書を発行できます。また、 これらのユーザー証明書および秘密キーへのアクセス権限もあります。
- FAS PowerShell コマンドレットを使用するには、Windows PowerShell 64 ビットが FAS サーバーにイ ンストールされている必要があります。
- ユーザー証明書を発行するには、Microsoft エンタープライズ証明機関(ルートまたは下位)が必要です。

Citrix Virtual Apps サイトまたは Citrix Virtual Desktops サイトの要件:

 Delivery Controller、Virtual Delivery Agent (VDA)、StoreFront サーバーはすべて現在サポートされて いるバージョンを使用する必要があります。

注:

FAS は XenApp および XenDesktop 7.6 長期サービスリリース (LTSR) ではサポートされていません。

マシンカタログを作成する前に、フェデレーション認証サービスのグループポリシー構成が適切に VDA に適用されている必要があります。詳しくは、「グループポリシーの構成」セクションを参照してください。

このサービスの展開を計画する場合は、「セキュリティに関する注意事項」セクションを参照してください。

インストールと構成

November 9, 2021

インストールとセットアップの順序

- 1. フェデレーション認証サービスのインストール (FAS)
- 2. StoreFront ストアでの FAS プラグインの有効化
- 3. Delivery Controller の構成
- 4. グループポリシーの構成
- 5. FAS 管理コンソールを使用して、以下を行います:
 - a) 証明書テンプレートの展開
 - b) 証明機関のセットアップ
 - c) 証明機関を使用するための FAS の認証
 - d) ルールの構成
 - e) FAS の Citrix Cloud への接続(オプション)

フェデレーション認証サービスのインストール

セキュリティ上の理由により、フェデレーション認証サービス(FAS)は、ドメインコントローラーや証明機関と同 様にセキュリティ保護されている専用サーバーにインストールすることをお勧めします。FAS は次のいずれかの方法 でインストールできます:

- Citrix Virtual Apps and Desktops インストーラー(ISO の挿入時に自動実行されるスプラッシュスクリーンの[フェデレーション認証サービス]ボタンから)を使用、または
- スタンドアロンの FAS インストーラーファイル(Citrix ダウンロードから MSI ファイルでダウンロード)を 使用。

以下のコンポーネントをインストールします:

- フェデレーション認証サービス
- 詳細な FAS 構成用のPowerShell スナップインコマンドレット
- FAS 管理コンソール
- FAS のグループポリシーテンプレート (CitrixFederatedAuthenticationService.admx/adml)
- 証明書テンプレートファイル
- パフォーマンスカウンターおよびイベントログ

FAS のアップグレード

インプレースアップグレードで FAS を新しいバージョンにアップグレードできます。アップグレード前に、以下に注 意してください:

- インプレースアップグレードを行った場合、FAS サーバーの設定はすべて保持されます。
- FAS をアップグレードする前に、FAS 管理コンソールが閉じていることを確認してください。
- 1台以上の FAS サーバーを常に利用可能な状態に維持してください。フェデレーション認証サービスに対応した StoreFront サーバーから到達可能なサーバーがない場合、ユーザーはログオンやアプリケーションの起動を行えなくなります。

アップグレードを開始するには、Citrix Virtual Apps and Desktops インストーラーまたはスタンドアロンの FAS インストーラーファイルを使用して FAS をインストールします。

StoreFront ストアでの FAS プラグインの有効化

注:

FAS を Citrix Cloud でのみ使用する場合は、この手順は必要ありません。

StoreFront ストアで FAS の統合を有効にするには、管理者アカウントで以下の PowerShell コマンドレットを実行します。ストア名が異なる場合は、\$StoreVirtualPathを変更します。

```
1 Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
2 $StoreVirtualPath = "/Citrix/Store"
3 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
4 $auth = Get-STFAuthenticationService -StoreService $store
5 Set-STFClaimsFactoryNames -AuthenticationService $auth -
ClaimsFactoryName "FASClaimsFactory"
6 Set-STFStoreLaunchOptions -StoreService $store -
VdaLogonDataProvider "FASLogonDataProvider"
7 <!--NeedCopy-->
```

FAS の使用を停止するには、以下の PowerShell スクリプトを使用します:

```
1 Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module
2 $StoreVirtualPath = "/Citrix/Store"
3 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
4 $auth = Get-STFAuthenticationService -StoreService $store
5 Set-STFClaimsFactoryNames -AuthenticationService $auth -
ClaimsFactoryName "standardClaimsFactory"
6 Set-STFStoreLaunchOptions -StoreService $store -
VdaLogonDataProvider ""
7 <!--NeedCopy-->
```

Delivery Controllerの構成

注:

FAS を Citrix Cloud でのみ使用する場合は、この手順は必要ありません。

FAS を使用するには、このサービスに接続可能な StoreFront サーバーを信頼するように Citrix Virtual Apps また は Citrix Virtual Desktops の Delivery Controller を構成します。PowerShell コマンドレット **Set-BrokerSite** -**TrustRequestsSentToTheXmlServicePort \$true** を実行します。サイト内の Delivery Controller の数に かかわらず、これを実行するのはサイトごとに一度のみです。

グループポリシーの構成

FAS のインストール後は、インストールで提供されたグループポリシーテンプレートを使用して、グループポリシー 内の FAS サーバーの完全修飾ドメイン名(FQDN)を指定する必要があります。

重要:

チケットを要求する StoreFront サーバーおよびチケットを使用する Virtual Delivery Agent (VDA) に、グ ループポリシーオブジェクトによって適用されるサーバーの自動番号設定を含む、同じ FQDN 構成を行う必要 があります。

説明をシンプルにするために、以下の例ではすべてのマシンに適用されるドメインレベルで単一のポリシーを構成し ていますが、これは必須ではありません。StoreFront サーバー、VDA、および FAS 管理コンソールを実行している マシンで同じ FQDN の一覧が参照されている限り、FAS は機能します。手順 6 を参照してください。 手順 1: FAS をインストールしたサーバーで、C:\Program Files\Citrix\Federated Authentication Service\PolicyDefinitions\CitrixFederatedAuthenticationService.admx ファイル、CitrixBase.admx ファイル、および en-US フォルダーを見つけます。

₩	PolicyDefinit	ions				X
€ 🗇 ▼ ↑ 퉱 «	Search Policy	Definitions	Q,			
⊿ 🚖 Favorites	Name	Date modified	Туре	Size		
📃 Desktop	_ 📔 en-US	22/07/2019 09:04	File folder			
🗼 Downloads	CitrixBase.admx	19/07/2019 12:28	ADMX File	2 KB		
📃 Recent places	CitrixFederatedAuthenticationService.admx	19/07/2019 12:28	ADMX File	4 KB		
▷ I This PC 3 items	v					

手順 **2**: これらをドメインコントローラーにコピーして、C:\Windows\PolicyDefinitions および en-US サブフォ ルダーに配置します。

手順 3: コマンドラインから Microsoft 管理コンソールを実行します (mmc.exe)。メニューバーから、[ファイル]
 [スナップインの追加と削除]の順に選択します。グループポリシー管理エディターを追加します。

グループポリシーオブジェクトを入力するための画面が開いたら、[参照]を選択してから[既定のドメインポリシ ー]を選択します。または、任意のツールを使用して、環境に応じたポリシーオブジェクトを作成して選択すること もできます。このポリシーは、影響を受ける Citrix ソフトウェア(VDA、StoreFront サーバー、管理ツール)を実 行しているすべてのマシンに適用する必要があります。

	Console1 - [Console	Root]	_ 🗆 X
🚟 File Action View Favorites Window Help			_ <i>8</i> ×
(+ - + 🗊 🔒 🖬 🖬	Select Group P	olicy Object 🛛 🗙	
Console Root Name	Welcome to the Group Policy Wizard		Actions
Add			Console Root
You can select snap-ins (you can configure which extensions). Available snap-ins: Snap-in Yen A Device Manager Micr Disk Management Micr Disk Management Micr Disk Management Micr Disk Polder Micr Croup Policy Management Micr Group Policy Object Editor Micr Group Policy Object Editor Micr Description: This snap-in allows you to edit Group Policy Objects which or stored on a computer.	Group Pol or on a loc Use the B Group Pol Chang only ap	by Objects can be stored in the Active Directory al computer. owse button to select a Group Policy Object. by Object: Browse for a Group Pol Domaina/OUs Sites All Look in: Bichtstest net Domains, OUs and linked Group Policy Objects: Name Domain Controllers.otridest net Policy Default Domain Policy	More Actions
			OK Capcel
			Canour

手順 4: Computer Configuration/Policies/Administrative Templates/Citrix Components/Authentica-

tion にあるフェデレ-	-ション認証サー	-ビスポリシ-	ーに移動します。
---------------	----------	---------	----------

Group Policy Management Editor			-	×
File Action View Help				
💠 🔶 🙍 📷 🔒				
Default Damia Paicy (DW-0-CDM ATT Poly) Default Damia Paicy (DW-0-CDM ATT Poly) Default Damia Settings default Setting	Authentication Federated Authentication Service Edit and Authentication Service Edit and Authentication Service Edit and Authentication Service Edit and Authentication Service Servers numming the Federated Authentication Service Insurgery one for the service Insurgery on the service Insurgery on the service Insurgery one for the service Insurgery on the service Insurgery on the service Insurgery one for the service Insurgery on the service In	Setting Contrarts Authority: Hon Server Control ASS Rule In-session Behavior		
	Saudad (Burdard /	٢		3
· /	(Extended / standard /			

注:

フェデレーション認証サービスのポリシー設定は、CitrixBase.admx または CitrixBase.adml テンプレート ファイルを PolicyDefinitions フォルダーに追加する際に、ドメイン GPO でのみ使用できます。手順 3 の後、 フェデレーション認証サービスのポリシー設定は、[管理用テンプレート] > [Citrix コンポーネント] > [認証] フォルダーに表示されます。

手順 **5**:フェデレーション認証サービスポリシーを開き、[有効]を選択します。これにより、FAS サーバーの FQDN を構成する [表示] ボタンを選択できるようになります。

💭 Federated Authenticati	on Service	- 🗆 X	
Federated Authenticati	on Service	Previous Setting Next Setting	
Not Configured Con Enabled Disabled Sup	ported on:	~	
	Show Contents	– 🗆 X 🗸	
Options: List the installed servers in ; FQDNs Show	FQDNs Volue fas1cbridget.net		· · · · · · · · · · · · · · · · · · ·
		DK Centel	

手順 6: FAS サーバーの FQDN を入力します。

重要:

複数の FQDN を入力する場合は、VDA、StoreFront サーバー(存在する場合)と FAS サーバー間で一覧の順 番が統一されている必要があります。「グループポリシー設定」を参照してください。

手順 7: [OK] をクリックしてグループポリシーウィザードを終了し、グループポリシーの変更を適用します。変更 を反映させるには、マシンを再起動(またはコマンドラインから gpupdate /force を実行)する必要がある場合が あります。

In-session Behavior

このポリシーはセッション内証明書、承認、ロック時の切断をサポートするユーザーの VDA セッションでエージェン トプロセスをアクティブ化します。セッション内証明書はこのポリシーが有効かつ証明書の作成に使用される FAS ル ールでセッション内使用が許可されている場合のみ使用できます。「ルールの構成」を参照してください。



Enable によってこのポリシーが有効になり FAS エージェントプロセスがユーザーの VDA セッションで実行できます。

Disable によってこのポリシーが無効になり FAS エージェントプロセスが実行を停止します。

メッセージのスコープ このポリシーが有効な場合、**Prompt Scope** によってアプリケーションでセッション内証 明書を使用を許可するかというメッセージをユーザーに表示する方法を制御できます。3 つのオプションがありま す。

- No consent required—このオプションはセキュリティメッセージを無効にし、ユーザーが操作する必要な く秘密キーが使用されます。
- Per-process consent-実行中のプログラムごとに個別に承認メッセージが表示されます。
- Per-session consent-ユーザーが一度 [OK] をクリックすると、セッションのすべてのプログラムに適用されます。

承認のタイムアウト このポリシーが有効になると、**Consent Timeout**によって承認が表示される期間を秒単位 で制御できます。たとえば、5分ごとに 300 秒間メッセージが表示される、などです。この値が0の場合、秘密キー の操作ごとにユーザーにメッセージが表示されます。

ロック時の切断 このポリシーを有効にすると、ユーザーが画面をロックしたときにセッションが自動的に切断され ます。この機能では「スマートカードの取り出し時の切断」ポリシーと同様の動作になるため、ユーザーが Active Directory ログオン資格情報を持っていない場合に便利です。 注:

ロック時の切断ポリシーは、VDA 上のすべてのセッションに適用されます。

フェデレーション認証サービス管理コンソールの使用

注:

大半の展開には FAS 管理コンソールが適していますが、PowerShell インターフェイスにはより詳細なオプションもあります。FAS PowerShell コマンドレットについて詳しくは、「PowerShell コマンドレット」を参照 してください。

FAS 管理コンソールは FAS の一部としてインストールされます。[スタート] メニューにアイコン (Citrix Federated Authentication Service) が配置されます。

管理コンソールの初回使用時は、証明書テンプレートの展開、証明機関のセットアップ、および FAS への証明機関の 使用権限の付与を行う手順が表示されます。一部の手順は、OS 構成ツールを使用して手動で完了することもできま す。

FAS 管理コンソールは、デフォルトでローカルの FAS サービスに接続されます。必要に応じ、コンソールの右上に表示される [Connect to another server] を使用してリモートサービスに接続できます。

#		(Citrix FAS Administration Console - connected to localhost		
Initial Setup	Rules	Advanced		Connect to another server	Refresh
Complete these set	tup steps:				
Dep	loy cer	tificate temp	plates	Deploy	
Deploy	the certif	icate templates ir	Active Directory.		
Set u	ıp a ce	rtificate aut	hority	Publish	
Publisł	n the temp	lates on a certific	ate authority.		
Auth	orize t	his service		Authorize	2
Create	an author	ization certicate f	or this service.		
Crea	te a ru	le		Create	
A rule	defines a s	smartcard-class ce	rtificate that signs users into a Citrix environment.		
You ha	ive no rule	es configured.			
Coni	nect to	Citrix Cloud	1	Connect	
Compl	ete this st	ep if you wish to u	use this FAS service with Citrix Cloud.		

証明書テンプレートの展開

他のソフトウェアとの相互運用性の問題を避けるため、FAS では、独自の目的で使用する 3 つの Citrix 証明書テンプ レートが用意されています。

- Citrix_RegistrationAuthority_ManualAuthorization
- Citrix_RegistrationAuthority
- Citrix_SmartcardLogon

これらのテンプレートは、Active Directory で登録する必要があります。[**Deploy**] をクリックしてから、[**OK**] を クリックします。

#	Deploy Certificate Templates
	Important:
	When you click "OK" the following certificate templates are deployed to Active Directory:
	- Citrix_RegistrationAuthority_ManualAuthorization - Citrix_RegistrationAuthority - Citrix_SmartcardLogon
	Deploying certificate templates may require you run this tool as a Domain or Enterprise Administrator.
	This step can also be performed manually. For more information, consult the online documentation.
	OK Cancel

テンプレートの構成は、以下のフォルダーに FAS と一緒にインストールされた、拡張子「.certificatetemplate」の XML ファイル内にあります:

C:\Program Files\Citrix\Federated Authentication Service\CertificateTemplates

	ine i ov(e) i nogninnez i entre i readorea manentariariari	ee - connencromp		* 0
	Name	Date modified	Type	Size
	Citrix_RegistrationAuthority.certificatetemplate	2/10/2020 5:25 AM	CERTIFICATETEM	6 KI
	Citrix_RegistrationAuthority_ManualAuthorization.certificatetemplate	2/10/2020 5:25 AM	CERTIFICATETEM	7 KJ
٢.	Citrix_SmartcardLogon.certificatetemplate	2/10/2020 5:25 AM	CERTIFICATETEM	5 KJ

これらのテンプレートファイルをインストールする権限がない場合は、テンプレートファイルを Active Directory 管理者に渡してください。

テンプレートが含まれるフォルダーから以下の PowerShell コマンドを実行すると、テンプレートを手動でインスト ールできます:

2	\$CertEnrol = New-Object -ComObject X509Enrollment.
	CX509EnrollmentPolicyWebService
3	<pre>\$CertEnrol.InitializeImport(\$template)</pre>
4	<pre>\$comtemplate = \$CertEnrol.GetTemplates().ItemByIndex(0)</pre>
5	<pre>\$writabletemplate = New-Object -ComObject X509Enrollment.</pre>
	CX509CertificateTemplateADWritable
6	<pre>\$writabletemplate.Initialize(\$comtemplate)</pre>
7	<pre>\$writabletemplate.Commit(1, \$NULL)</pre>
8	NeedCopy

Active Directory 証明書サービスのセットアップ

Citrix 証明書テンプレートのインストール後は、これらのテンプレートを1つまたは複数の Microsoft エンタープラ イズ証明機関サーバーで公開する必要があります。Active Directory 証明書サービスの展開方法について詳しくは、 Microsoft 社のドキュメントを参照してください。

どのサーバーでもテンプレートが公開されていない場合は、**Set Up Certificate Authority** を使用して公開でき ます。これは、証明機関の管理権限のあるユーザーとして実行する必要があります。

(証明書テンプレートは、Microsoft 証明機関コンソールを使用して公開することもできます。)

🛱 Citrix	FAS Administration Console - connec	ted to localhost	- 🗆 X
Initial 9	Setup Rules Advanced		Connect to another server Refresh
Complete	e these setup steps: Deploy certificate temp The required templates are dep Set up a certificate au The authorization templates are Click "Publich" to publich the te	Set Up Certificate Authority X Important: When you click "OK" the following certificate templates are published on the certificate authority selected below:	Deploy Publish A.
	Authorize this service Create an authorization certicat Create a rule A rule defines a smartcard-class	Citrix_RegistrationAuthority_ManualAuthorization Citrix_RegistrationAuthority Citrix_SmartcardLogon Publishing certificate templates may require you run this tool as a Domain Administrator. This step can also be configured manually. For more information consult the online documentation.	Authorize Create
	You have no rules configured.	Certificate Authority:	
	Connect to Citrix Clo Complete this step if you wish t	– – – – – – – – – – – – – – – – – – –	Connect

フェデレーション認証サービスへの権限付与

この手順により、FASの認証が開始されます。管理コンソールは、Citrix_RegistrationAuthority_ManualAuthorization テンプレートを使用して証明書の要求生成し、この要求をテンプレートを公開する証明機関のいずれかに送信しま す。

		Citrix FAS Administration Console - connected to localhost	_ D X
nitial Set	tup Rules Advanced		Connect to another server Refres
omplete the	ese setup steps:		
\ [Deploy certificate te	Authorize Service	Deploy
т	The required templates are de		
<u> </u>	Set up a certificate a	Click "OK" to submit a certificate request for a Registration Authority certificate to the selected Microsoft Certificate Authority.	Publish
T C	The authorization templates a Click "Publish" to publish the	The CA Administrator must sign in to the Microsoft Certificate Authority console to issue the pending request.	
ļ	Authorize this servic	For more information, consult the online documentation.	Authorize
0	Create an authorization certic	Certificate authority	
(Create a rule		Create
A	A rule defines a smartcard-cla	OK Cancel	
Y	/ou have no rules configured		
(Connect to Citrix Clou	d	Connect
C	Complete this step if you wish to	use this FAS service with Citrix Cloud.	

要求は、送信後、FAS マシンアカウントから保留中の要求として Microsoft 証明機関コンソールの [保留中の要求] リストに表示されます。FAS の構成を続行するには、証明機関の管理者が要求の発行または拒否を選択する必要があ ります。

FAS 管理コンソールは、管理者が [Issue] または [Deny] を選択するまで処理中の「スピナー」アイコンを表示 します。

Microsoft 証明機関コンソールで [すべてのタスク] を右クリックしてから、証明書要求に対して [Issue] または [Deny] を選択します。[Issue] を選択すると、FAS 管理コンソールが認証証明書を表示します。[Deny] を選択す ると、コンソールはエラーメッセージを表示します。

ي. ا	cer	tsrv - [Certificat	ion Authority (Local))\citrixtest	t-CA-1-CA\Pendin	g Requests]	_	
File Action View Help Image: Second S								
Certification Authority (Local) d a citrixtest-CA-1-CA	Request ID	Binary Request	Request Status Code	Request L	Disposition Message	Request Submission Date	CITRIXTEST\FAS-15	Request C
 Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates 			All Tasks Refresh Help	•	View Attributes/Exten Export Binary Data Issue Deny	sions		
Contains actions that can be performe	d on the item		ш					>

FAS 管理コンソールにより、このプロセスの完了が自動的に検出されます。この処理には数分かかることがありま

す。

#	Citrix FAS Administration Console - connected to localhost	_ D X					
Initial S	etup Rules Advanced	Connect to another server Refresh					
Complete	these setup steps:						
	Deploy certificate templates	Deploy					
	The required templates are deployed in Active Directory.						
1	Set up a certificate authority	Publish					
•	The authorization templates are published on: ca-1.citrixtest.net\citrixtest-CA-1-CA.						
	Click "Publish" to publish the templates on another certificate authority.						
\bigcirc	Authorize this service	Authorize					
	There is a pending authorization request on ca-1.citrixtest.net\citrixtest-CA-1-CA. Cancel request						
	Create a rule	Create					
	A rule defines a smartcard-class certificate that signs users into a Citrix environment.						
	You have no rules configured.						
	-						
	Connect to Citrix Cloud	Connect					
	Complete this step if you wish to use this FAS service with Citrix Cloud.						

ルールの構成

FAS のルールにより、StoreFront の指示に従って、VDA ログオンおよびセッション中の使用に関する証明書発行の 権限が付与されます。各ルールでは、証明書の要求を信頼する StoreFront サーバー、証明書を要求できる一連のユ ーザー、および証明書の使用を許可する一連の VDA マシンを指定します。

FAS では、最低 1 つのルールを作成し構成する必要があります。StoreFront は FAS にアクセスしたとき「デフォルト」という名前のルールを要求するため、「デフォルト」という名前のルールを作成することをお勧めします。

追加のカスタムルールを作成して、さまざまな証明書テンプレートおよび証明機関を参照し、各種プロパティや権限 が含まれるように構成することができます。これらのルールは、さまざまな StoreFront サーバーや Workspace で 使用するために構成できます。グループポリシー構成オプションを使用して、カスタムルールを名前で要求できるよ うに StoreFront サーバーを構成します。

[**Create**](または「Rules」タブの [**Create rule**])をクリックしてルールを作成するための情報を収集するルール 作成ウィザードを開始します。[Rules] タブは各ルールの概要を表示します。

#		(Citrix FAS Administration Console	- connected to localhost			
Initial Setup	Rules	Advanc	red		Connect to another server	Refresh	
A rule defines a smartcard-class certificate that signs users into a Citrix environment.							
+ Create rule	è						
Default	0	Ŷ ⑪	Summary				
			Rule name:	Default			
			Status:	ОК			
			Template:	Citrix_SmartcardLogon			
			Certificate authorities:	ca-1.citrixtest.net\citrixtest	-CA-1-CA		
			Certificate available in-session:	No			
			Access control:	Configured			
			Restrictions:	Not configured			
			Cloud rule:	No			

ウィザードによって次の情報が収集されます:

テンプレート:ユーザー証明書の発行に使用される証明書テンプレート。これは Citrix_SmartcardLogon テンプ レートか、その変更されたコピーである必要があります(「証明書テンプレート」を参照してください)。

証明機関:ユーザー証明書を発行する証明機関。テンプレートは証明機関によって公開される必要があります。FAS では、フェールオーバーおよび負荷分散のために、複数の証明機関の追加することができます。選択した証明機関の ステータスが「Template available」であることを確認してください。「証明機関の管理」を参照してください。

セッション内使用: [セッション内使用を許可] オプションにより、証明書を VDA へのログオン後に使用できるかど うかを制御します。

- Allow in-session use が選択されていない場合(デフォルトで推奨)—証明書はログオンまたは再接続にの み使用され、認証後、ユーザーは証明書にアクセスできなくなります。
- Allow in-session use が選択されている場合--認証後、ユーザーは証明書にアクセスできます。通常の場合、 お客様はこのオプションを選択しないでください。イントラネット Web サイトやファイル共有など、VDA セ ッション内からアクセスされるリソースには、Kerberos を使用したシングルサインオンでアクセスできるた め、セッション内証明書は必要ありません。

Allow in-session use を選択した場合は、In-session Behaviorグループポリシーも有効にして VDA に適 用する必要があります。これにより、ログオン後にアプリケーションが使用できるようにユーザーの個人証明 書ストアに証明書が配置されます。たとえば、VDA セッション内で Web サーバーへの TLS 認証が必要な場合、証明書は Internet Exploler によって使用されます。

アクセス制御:ユーザーのログオンまたは再接続用に証明書を要求する権限が付与された、信頼済み StoreFront サ ーバーの一覧。これらのすべてのアクセス許可に対して、個々の AD オブジェクトまたはグループを追加できます。

重要:

[アクセス制御] 設定はセキュリティ上非常に重要であり、慎重に管理する必要があります。

注:

FAS サーバーを Citrix Cloud でのみ使用する場合は、アクセス制御を構成する必要はありません。ただし、 Citrix Cloud でルールが使用される場合、StoreFront のアクセス許可は無視されます。Citrix Cloud とオン プレミスの StoreFront 環境で、同じルールを使用できます。StoreFront のアクセス許可は、ルールがオンプ レミスの StoreFront で使用される場合には適用されます。

デフォルトのアクセス許可(「Assert Identity」を許可)では、すべてが拒否されます。したがって、Storefront サ ーバーを明示的に許可する必要があります。

Permissions for St	oreFront Ser	vers 🛛 🗙
Security		
Group or user names:		
STF-1 (CITRIXTEST\STF-1\$)		
	Add	Remove
	/////	Hellove
Permissions for STF-1	Allow	Deny
Assert Identity	✓	
ОК	Cancel	Apply

制限:ユーザーが FAS を使用してログオンできる VDA マシンのリストと、FAS を介して証明書を発行できるユーザーのリスト。

- VDA 権限の管理では、FAS を使用してユーザーをログオンさせる VDA を指定できます。VDA の一覧のデフ ォルトはドメインコンピューターになります。
- ユーザー権限の管理では、FAS を使用して VDA にサインインするユーザーを指定できます。ユーザーの一覧のデフォルトはドメインユーザーになります。

注:

FAS サーバーが VDA およびユーザーのドメインとは異なるドメインにある場合は、デフォルトの制限を変更す る必要があります。

🐌 Perm	ission	s for VDAs		x				
Security								
Group or user names:								
🍇 Domain Computers (0	CITRIXT	EST\Domain Con	nputers)					
				1				
		Add	Remove	4				
Permissions for Domain Computers		Allow	Deny					
Relying Party		~						
	OK	Canad	Analy					
	UK	Cancel	Арріу					

Permissions	for Users	x
Security		
Group or user names:		
& Domain Users (CITRIXTEST\E	Domain Users)	
		-
	Add	Remove
Permissions for Domain Users	Add Allow	Deny
Permissions for Domain Users User Authentication	Add Allow	Deny
Permissions for Domain Users User Authentication	Add Allow	Deny
Permissions for Domain Users User Authentication	Add Allow	Deny
Permissions for Domain Users User Authentication	Add Allow	Deny
Permissions for Domain Users User Authentication	Add Allow	Deny
Permissions for Domain Users User Authentication	Add Allow	Deny
Permissions for Domain Users User Authentication	Add Allow	Deny
Pemissions for Domain Users User Authentication	Add Allow	Deny

Cloud ルール: Citrix Workspace から ID アサーションを受信したときに、このルールが適用されるかを示します。 Citrix Cloud に接続するときに、Citrix Cloud で使用するルールを選択します。[**Connect to Citrix Cloud**] セ クションのリンクから Citrix Cloud に接続した後、ルールを変更することもできます。

#	Citrix FAS Administration Console - connected to localhost	_ □ X
Initial S	etup Rules Advanced	Connect to another server Refresh
Complete	these setup steps:	
	Deploy certificate templates	Deploy
ľ	The required templates are deployed in Active Directory.	
\checkmark	Set up a certificate authority	Publish
	The authorization templates are published on: ca-1.citrixtest.net\citrixtest-CA-1-CA.	
	Click "Publish" to publish the templates on another certificate authority.	
	Authorize this service	Reauthorize
•	An authorization certificate is configured.	
	Deauthorize this service.	
\checkmark	Create a rule	Create
	You have a rule configured: Default	
	Connect to Citrix Cloud	Connect
	Complete this step if you wish to use this FAS service with Citrix Cloud.	

Citrix Cloud への接続

FAS サーバーを Citrix Cloud に接続して、Citrix Workspace で使用できます。このCitrix Workspace の記事を 参照してください。

1. [Initial Setup] タブの [Connect to Citrix Cloud] で [Connect] をクリックします。



2. [**Sign in to Citrix Cloud**] をクリックし、接続先の Cloud 顧客の管理者資格情報を使用して Citrix Cloud にサインインします。

Citrix Cloud [®]		
	· · · · ·	
	Choose a resource location:	
	Benchmark at BARLAR	

3. 必要に応じて顧客アカウントを選択して、FAS サーバーを接続するリソースの場所を選択します。[Continue] をクリックし、確認用のウィンドウを閉じます。

# Connect to Citrix Clo	ed .	-		×
Connect to Citri	(Cloud			
Sign in	Choose a FAS rule to use with Citrix Cloud.			
Choose a rule	 I will configure a rule later 			
Summary	Create a rule when this wizard finishes			
	 Use an existing rule: 			
	Default			
	The rule you use for Citrix Cloud can also be used with on-premises StoreFront.			
	Back Next		Cance	

- FAS 管理コンソールで、Citrix Workspace から ID アサーションを受信したときに適用するルールを選択す るか、このウィザードの終了時に [Create a rule] を選択します([Rules] タブで、選択または作成したル ールの Cloud rule の値は「Yes」です)。
- 5. [Summary] タブで [Finish] をクリックして Citrix Cloud 接続を完了します。

Citrix Cloud で FAS サーバーが登録され、Citrix Cloud アカウントの [リソースの場所] ページに表示されます。

Citrix Cloud からの切断

このCitrix Workspace の記事の説明に従って Citrix Cloud のリソースの場所から FAS サーバーを削除した 後、[Connect to Citrix Cloud] で [Disable] を選択します。

詳細な構成

September 28, 2021

このセクションの記事では、フェデレーション認証サービス(FAS)の高度な構成および管理について説明します。

関連情報

- FAS のインストールと初期セットアップについては、「インストールと構成」を参照してください。
- •「展開アーキテクチャ」では、FAS の主要アーキテクチャの概要を説明し、より複雑なアーキテクチャに関する そのほかの記事へのリンクを掲載しています。

証明機関の設定

November 9, 2021

この記事では、フェデレーション認証サービス(FAS)を証明機関(CA)サーバーと統合するための詳細設定につい て説明します。これらの設定の大半は FAS 管理コンソールでサポートされていません。この説明では、FAS が提供す る PowerShell API を使用します。この記事に記載されている説明を実行する前に、PowerShell の基礎知識を確認 してください。

FAS で使用するための複数 **CA** サーバーのセットアップ

🗱 Edit F	Rule	-		×
Edit ru	ule "Default"			
Tem	iplate tificate authority	Choose the certificate authority (CA) where user certificates will be generated. You can choose multiple certificate authorities for load balancing and failover.	Refres	sh
in-s	ession use	Name Status		
Acc	ess control	Template available		
Resi	trictions 1mary	✓ Template available		
		☑ Only show CAs publishing Citrix_SmartcardLogon (recommended).		
		Apply	Cancel	

FAS 管理コンソールを使用して、複数の証明機関で FAS を構成し、ルールを作成または編集できます:

選択したすべての CA が Citrix_SmartcardLogon 証明書テンプレート(またはルールで選択したテンプレート)を 公開する必要があります。

使用するいずれかの CA が必要なテンプレートを公開していない場合、CA の証明機関をセットアップする手順を実行します。

注:

この手順で構成された認証証明書はどの CA でも使用できるため、すべての CA でこのサービスを認証する手順 を実行する必要はありません。

想定される動作の変更

FAS サーバーを複数の CA サーバーで構成した後は、ユーザー証明書の生成は構成済みのすべての CA サーバー間で 配信されます。さらに、構成済みの CA サーバーのうちいずれかでエラーが発生すると、FAS サーバーは別の使用可 能な CA サーバーに切り替えます。

Microsoft 証明機関を TCP アクセス用に構成する

デフォルトでは、Microsoft 証明機関はアクセスに DCOM を使用します。この場合、ファイアウォールの実装が 複雑になるため、静的 TCP ポートに切り替えることができます。Microsoft 証明機関で DCOM 構成パネルを開 き、「CertSrv 要求」DCOM アプリケーションのプロパティを編集します:

CertSrv Request Properties ? X					
General Location Security Endpoints Identity					
DCOM Protocols and endpoints:					
T default system protocols					
Select DCOM protocol and endpoint					
Select the DCOM network protocol sequence that you want to add. Enter the endpoint details and click OK when you have finished.					
Protocol Sequence: Connection-oriented TCP/IP V					
Disable protocol sequence. Use default endpoints. Use static endpoint 900 Use intranet range of dynamic endpoints. Use intermet range of dynamic endpoints.					
OK Cancel					
Learn more about setting these properties.					
OK Cancel Apply					

[エンドポイント]を変更して静的エンドポイントを選択し、TCP ポート番号を指定します (上の図では 900 です)。

Microsoft 証明機関を再起動して、証明書要求を送信します。「netstat -a -n -b」を実行する場合は、certsvr がポート 900 をリスンしていることを確認する必要があります:

TCP 0.0.0.0:636	dc:0	LISTENING
TCP 0.0.0.0:900	dc:D	LISTENING
[certsrv.exe] TCP 0.0.0.0:3268	dc:0	LISTENING
[lsass.exe] TCP 0.0.0.0:3269	dc : D	LISTENING

DCOM には RPC ポートを使用するネゴシエーションステージがあるため、FAS サーバー(または証明機関を使用す るその他のマシン)を構成する必要はありません。クライアントが DCOM を使用する必要がある場合、クライアント は証明書サーバーの DCOM RPC Service に接続して特定の DCOM サーバーへのアクセスを要求します。これによ ってポート 900 が開かれ、DCOM サーバーは FAS サーバーに接続方法を指示します。

ユーザー証明書の事前生成

ユーザー証明書が FAS サーバー内で事前生成されると、ユーザーのログオンにかかる時間が大幅に短縮されます。次のセクションでは、単一または複数の FAS サーバーでユーザー証明書を事前生成する方法について説明します。

Active Directory ユーザーの一覧を取得します

AD に対してクエリを実行し、ユーザーの一覧を次の例のようにファイル(.csv ファイルなど)に保存することにより、証明書の生成を改善することができます。

```
1 Import-Module ActiveDirectory
2
3 $searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for
      Users, leave it blank to search all
4 $filename = "user_list.csv" # Filename to save
5
6 if ($searchbase -ne ""){
7
       Get-ADUser -Filter {
8
9
   (UserPrincipalName -ne "null") -and (Enabled -eq "true") }
10
     -SearchBase $searchbase -Properties UserPrincipalName | Select
        UserPrincipalName | Export-Csv -NoTypeInformation -Encoding utf8 -
        delimiter "," $filename
11
   }
12
    else {
13
14
       Get-ADUser -Filter {
    (UserPrincipalName -ne "null") -and (Enabled -eq "true") }
15
    -Properties UserPrincipalName | Select UserPrincipalName | Export-Csv
16
         -NoTypeInformation -Encoding utf8 -delimiter "," $filename
17
    }
18
19 <!--NeedCopy-->
```

Get-ADUser は、ユーザーの一覧を要求するための標準コマンドレットです。上述の例には、UserPrincipalName を持ちステータスが「有効」のユーザーのみを一覧表示するフィルター引数が含まれています。

SearchBase 引数によって、AD のユーザー検索が制限されます。すべてのユーザーを AD に含めたい場合、これを 省略できます。注: このクエリによって、多数のユーザーが返される可能性があります。

CSV の外観は、次のようになります。

📕 user_list.csv - Notepad	
File Edit Format View Help	
"UserPrincipalName" "testuser1@bvt.local" "testuser2@bvt.local" "testuser3@bvt.local" "testuser4@bvt.local" "ucs38@bvt.local"	

FAS サーバー

以下の PowerShell スクリプトでは、以前生成されたユーザーの一覧を使用してユーザー証明書の一覧が作成されます。

```
1 Add-PSSnapin Citrix.A*
2 $csv = "user_list.csv"
3 $rule = "default" # rule/role in your admin console
4 $users = Import-Csv -encoding utf8 $csv
5 foreach ( $user in $users )
6 {
7
8
       $server = Get-FasServerForUser -UserPrincipalNames $user.
          UserPrincipalName
9
       if( $server.Server -ne $NULL) {
10
11
           New-FasUserCertificate -Address $server.Server -
              UserPrincipalName $user.UserPrincipalName -
              CertificateDefinition $rule"_Definition" -Rule $rule
12
        }
13
14
       if( $server.Failover -ne $NULL) {
15
           New-FasUserCertificate -Address $server.Failover -
              UserPrincipalName $user.UserPrincipalName -
              CertificateDefinition $rule"_Definition" -Rule $rule
17
        }
18
19
    }
20
21 <!--NeedCopy-->
```

複数の FAS サーバーが存在する場合は、特定のユーザーの証明書がメインサーバーで1回、フェールオーバーサーバ ーで1回の合計2回生成されます。

上述のスクリプトは、「default」という名前の規則の場合のものです。規則名が異なる場合(「hello」など)は、ス クリプトの \$rule 変数を変更してください。

#				Citrix FAS Administr	ation Console - con	nected to localhos
Initial Setup	Rules	٨d	/ance	d		
A rule defines a smartcard-class certificate that signs users into a Citrix environment. + Create rule						
Default	6	1	Î	Summary		
hello	ć	1	<u>Î</u>	Rule name:	hello]
				Status:	ОК	
				Template:	Citrix_S	martcardLogon

登録機関証明書を更新します

複数の FAS サーバーを使用中の場合は、ログオン中のユーザーに影響することなく FAS 認証証明書を更新できます。

注:

GUI を使用して FAS を再認証することもできます:

8		Ci	trix FAS Administration Console - connected to localhost	_	o x
Initial Setup	Rules A	Advanced		Connect to another server	Refres
Complete these se	etup steps:				
V Dep	oloy certif	icate temp	lates	Deploy	
The re	equired templ	lates are deploye	ed in Active Directory.		
🗸 Set	up a cert	ificate auth	nority	Publish	
The a	uthorization t	emplates are pu	blished on: ca-1.citrixtest.net\citrixtest-CA-1-CA.		
Click '	"Publish" to p	ublish the templ	lates on another certificate authority.		
🗸 Aut	horize thi	is service		Reauthori	ize
An au	thorization ce	ertificate is config	gured.		
Deaut	thorize this se	rvice.			
Crea	ate a rule			Create	
You h	ave 2 rules co	onfigured.			

以下の手順を実行します。

- 1. 新しい認証証明書を作成します。New-FasAuthorizationCertificate
- 2. 次のコマンドによって返される新しい認証証明書のGUIDをメモします:Get-FasAuthorizationCertificate
- 3. FAS サーバーをメンテナンスモードにします: Set-FasServer -Address <FAS server> MaintenanceMode \$true
- 4. 新しい認証証明書を置換します。Set-FasCertificateDefinition _AuthorizationCertificate <GUID>
- 5. FAS サーバーのメンテナンスモードを解除します。Set-FasServer -Address <FAS server
 > -MaintenanceMode \$false
- 6. 古い認証証明書を削除します。Remove-FasAuthorizationCertificate

関連情報

- FAS のインストールと構成については、「インストールと構成」の記事を参照してください。
- 一般的な FAS 環境については、「展開アーキテクチャ」を参照してください。
- その他の具体的な手順については、「詳細な構成」を参照してください。

秘密キー保護

November 9, 2021

はじめに

秘密キーは Network Service アカウントを使用して保存され、デフォルトでエクスポート不可としてマークされま す。

秘密キーには2つの種類があります。

- 登録機関証明書に関連付けられている、Citrix_RegistrationAuthority 証明書テンプレートからの秘密キー
- ユーザー証明書に関連付けられている、Citrix_SmartcardLogon 証明書テンプレートからの秘密キー

登録機関証明書には Citrix_RegistrationAuthority_ManualAuthorization(デフォルトで 24 時間有効)および Citrix_RegistrationAuthority(デフォルトで 2 年間有効)の 2 つの種類があります。

フェデレーション認証サービス (FAS) 管理コンソールの [初回セットアップ] タブの手順3で、管理者 が [許可する] をクリックすると、FAS サーバーによってキーペアが生成され、証明書署名要求が Citrix_RegistrationAuthority_ManualAuthorization 証明書の証明機関に送信されます。これは一時的な証明 書であり、デフォルトで24 時間有効です。証明機関は自動的に証明書を発行しません。証明書を発行するに は、管理者による証明機関での手動の権限許可が必要です。証明書が FAS サーバーに発行されると、FAS は Citrix_RegistrationAuthority_ManualAuthorization 証明書を使用して Citrix_RegistrationAuthority 証明 書 (デフォルトで2 年間有効) を自動的に取得します。FAS サーバーは、Citrix_RegistrationAuthority 証明書を 取得するとすぐに、Citrix_RegistrationAuthority_ManualAuthorization の証明書とキーを削除します。

登録機関証明書ポリシーは秘密キーを所有するものすべてに対して、テンプレートで構成されたユーザーセットに対 する証明書要求の発行を許可するため、登録機関証明書に関連付けられた秘密キーは特に機密です。結果として、こ のキーを管理するものはだれでも、セット内のユーザーと同様、環境に接続できます。

次のいずれかを使用して、組織のセキュリティ要件に準拠して秘密キーが保護されるように FAS サーバーを構成できます:

- Microsoft Enhanced RSA、AES Cryptographic Provider、または Microsoft ソフトウェアキー記憶域プロバイダー(登録機関証明書およびユーザー証明書両方の秘密キー用)
- トラステッドプラットフォームモジュール(TPM)チップを使用した Microsoft プラットフォームキー記憶 域プロバイダー(登録機関証明書の秘密キー用)、および Microsoft Enhanced RSA、AES Cryptographic Provider、または Microsoft ソフトウェアキー記憶域プロバイダー(ユーザー証明書の秘密キー用)
- ハードウェアセキュリティモジュール(HSM)ベンダーのHSMデバイスを使用した暗号サービスまたはキー 記憶域プロバイダー(登録機関証明書およびユーザー証明書両方の秘密キー用)

秘密キーの構成設定

3 つのオプションのうちいずれかを使用して FAS を構成します。テキストエディターを使用して、Citrix.Authentication.FederatedAuthenticationService.exe.config ファイルを編集します。ファイルのデフ ォルトの場所は FAS サーバーの Program Files\Citrix\Federated Authentication Service フォルダーです。

<pre><rr></rr></pre> version="1.0" encoding="utf=8"
<configuration></configuration>
<appsettings></appsettings>
This option switch between CAPI API (true) and CNG API (false) Cryptographic Providers
<add <pre="">key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLegacyCsp" value="false"/></add>
Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name
add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/
Specify the Cryptographic Service Provider Type (only for CSP - not KSP). For example: PROV RSA AES is 24
add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/
Specify Private Key protection [NoProtection GenerateNonExportableKey GenerateTPMProtectedKey]
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateNonExportableKey"></add>
Specify RSA Key length
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"></add>
Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational)
add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" /
Logging: Event IDs to not log (comma separated)
add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" /
Logging: Disable Key Management logs
add key="Citrix.TrustFabric.Logging.SystemLog" value=""/
<startup><supportedruntime sku=".NETFramework,Version=v4.5.1" version="v4.0"></supportedruntime></startup>

FAS は、サービスの起動時にのみ構成ファイルを読み込みます。いずれかの値が変更された場合、新しい設定を反映 させるために FAS を再起動する必要があります。

Citrix.Authentication.FederatedAuthenticationService.exe.config ファイルの関連する値を次のとおり設定 します:

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp**(CAPIと CNG API の切り替 え)

 值	コメント
true	CAPI API を使用
false(デフォルト)	CNG API を使用

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderName**(使用するプロバイダーの名前)

值	ーイメト
Microsoft Enhanced RSA および AES	デフォルトは CAPI プロバイダーです
Cryptographic Provider	
Microsoft ソフトウェアキー記憶域プロバイダー	デフォルトは CNG プロバイダーです

值	コメント
Microsoft プラットフォームキー記憶域プロバイダー	デフォルトは TPM プロバイダーです。TPM はユーザー キーにはお勧めしません。TPM は登録機関キーにのみ使
	用します。FAS サーバーを仮想化環境で実行する予定の 場合は、TPM およびハイパーバイザーのベンダーに仮想 化がサポートされているかどうかを確認してください。
HSM_Vendor CSP/Key 記憶域プロバイダー	HSM ベンダーによって提供されます。値はベンダーに よって異なります。FAS サーバーを仮想化環境で実行す る予定の場合は、HSM ベンダーに仮想化がサポートさ れているかどうかを確認してください。

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType (CAPI API の場合のみ必要)

 值	コメント
24	Default。Microsoft KeyContainerPermissionAc-
	cessEntry.ProviderType Property
	PROV_RSA_AES 24 を参照します。CAPI で HSM を使
	用する場合、および HSM ベンダーで別のタイプを指定
	されている場合以外は、常に 24 である必要があります。

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyProtection**(FAS が秘密キー操作を実行する必要がある場合は、ここで使用されている値を使用します)。秘密キーの「エクスポート可能」フラグを制御します。ハードウェアでサポートされている場合は、TPM キーストレージの使用が許可されます。

	コメント
NoProtection	秘密キーをエクスポートできます。
GenerateNonExportableKey	Default。秘密キーをエクスポートできません。
GenerateTPMProtectedKey	秘密キーは TPM を使用して管理されます。秘密キーは ProviderName で指定した ProviderName(例: Microsoft プラットフォームキー記憶域プロバイダー)
	を介して格納されます

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**KeyLength**(秘密キーのサイズをビット単位で指 定)

值	コメント
2048	デフォルト値です。1024 または 4096 を使用すること
	もできます。

構成ファイルの設定を以下に図解します(インストール時のデフォルト設定は赤で示しています)。



構成シナリオの例

例 **1**

この例では、Microsoft ソフトウェアキー記憶域プロバイダーを使用して格納されている登録機関証明書の秘密キー およびユーザー証明書の秘密キーについて説明します。

これはデフォルトのインストール後の構成です。追加の秘密キー構成は不要です。

例 **2**

この例は、Microsoft プラットフォームキー記憶域プロバイダーを使用して FAS サーバーのマザーボードのハード ウェア TPM に格納されている登録機関証明書秘密キー、および Microsoft ソフトウェアキー記憶域プロバイダーを 使用して格納されているユーザー証明書秘密キーを示しています。 このシナリオでは、FAS サーバーのマザーボード上の TPM は TPM の製造元のドキュメントに基づいて BIOS で有効 化され、その後 Windows で初期化されているものとみなしています。詳しくは、https://docs.microsoft.com/enus/previous-versions/windows/it-pro/windows-vista/cc749022(v=ws.10)を参照してください。

PowerShellの使用(推奨) PowerShell を使用して、登録機関証明書をオフラインで要求できます。これは、証 明機関がオンラインの証明書署名要求で登録機関証明書を発行しないようにする組織にお勧めです。FAS 管理コンソ ールを使用してオフラインで登録機関証明書の署名要求を行うことはできません。

手順 1: 管理コンソールを使用した初回 FAS 構成時には、最初の「証明書テンプレートの展開」および「証明機関の セットアップ」の2つの手順だけを完了します。

#			C	itrix FAS Administration Console - connected to localhost		X			
Initial S	etup	Rules	Advanced		Connect to another server	Refresh			
Complete 1	Complete these setup steps:								
\checkmark	Deploy certificate templates Deploy								
	The req	uired tem	plates are deploy	ed in Active Directory.					
\checkmark	Set u	p a ce	rtificate aut	nority	Publish				
	The aut	horization	n templates are p	ublished on: ca-1.citrixtest.net\citrixtest-CA-1-CA.					
	Click "P	ublish" to	publish the temp	lates on another certificate authority.					
	Authorize this service Authorize								
	Create an authorization certicate for this service.								
	Create a rule Create								
	A rule o	defines a s	martcard-class ce	rtificate that signs users into a Citrix environment.					
	You ha	ve no rule	s configured.						
	Conr	nect to	Citrix Cloud	I	Connect				
	Comple	ete this ste	ep if you wish to u	se this FAS service with Citrix Cloud.					

手順2:証明機関サーバーで、証明書テンプレート MMC スナップインを追加します。Citrix_RegistrationAuthority_ManualAu テンプレートを右クリックし、「テンプレートの複製」を選択します。

[一般] タブを選択します。テンプレート名と有効期間を変更します。この例では、テンプレート名は Offline_RA、有 効期間は 2 年間です。

Properties of New Template X									
Subject Name Server Issuance Requirements									
Superseded Templa	tes	es Extensions Security							
Compatibility General	Request	Handling	Cryptography	Key Attestation					
Template display name:	Template display name:								
Offline_RA									
Template name: Offline_RA									
Validity period: 2 years V 0 days V									
2 years 0 days Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory Directory Directory Directory Directory									
OK	(Cancel	Apply	Help					

手順 **3**: 証明機関サーバーで、証明機関 MMC スナップインを追加します。3. [証明書テンプレート] を右クリック します。[新規作成] を選択し、[発行する証明書テンプレート] をクリックします。作成したばかりのテンプレート を選択します。

手順 4: FAS サーバーで次の PowerShell コマンドレットを読み込みます。

1 Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

手順 **5**: RSA キーペアを FAS サーバーの TPM 内で生成し、FAS サーバーで次の PowerShell コマンドレットを入 力して証明書署名要求を作成します。注: 一部の TPM ではキーの長さが制限されます。デフォルトのキーの長さは、 2048 ビットです。ハードウェアでサポートされているキーの長さを指定してください。

```
1 New-FasAuthorizationCertificateRequest -UseTPM $true -address \<FQDN of
FAS Server>
```

次に例を示します:

1 New-FasAuthorizationCertificateRequest -UseTPM \$true -address fashsm. auth.net

以下が表示されます。

Id	: 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address TrustArea	: [Offline CSR] :
CertificateRequest	:BEGIN CERTIFICATE REQUEST MIICaDCCAVACAQIWIZEhMB86CgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq hki69w0BAQEFAAOCAQBAMIIB6gKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZU3wTHFR0XW lhCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAf1bInFPgrz+ vbG3YjKuKtX35JpGqWiJUEDzXiQFaob3Dkh/pwP3U7DcEYthx88CfbaN9MH0EFbepoSYOCAfunXW smu1bXD91c/fGyH/3f9Af5bHrjE10Hc+4UJ/WS9PgRgcq3XBwFjpcj0g00WbJS9g220VSPwD77 7f7vZvoQkRy5NXXATJ+xxYEPLp9JuJaE1WXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB oAAwDQYJKoZIhvcHAQENBQADggEBAJJU8jR9XWH1vztpjxPeJzAUOsrLp0sCfMdvYn9u+17J8Gsr 4tuLjuQ+An4Y2Rw7b6pZxEICU8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c YIITNOtmcHFK4Loz5U55+tQw39MProEj3p7GwF7HrGY-Q5bFU38rbL19Z5cfNYYMbsgyMgAB8F 3SmaqQjN3C81yqT8z1if4132xImQrP/4XQvr1F+T015PM5Fxjj6PEKWopWTVZXGzSC1ufxevc01K +tTH9tQYJM6xw3+6TIcfuW0jrd8KJjTdCSSMu7LJuIajTNZ5Z+1eM61TAT03X6/AB7o= END CERTIFICATE REQUEST
Status	: WaitingForApproval

PS C:\Users\Administrator.AUTH> _

メモ:

- Id GUID(この例では「5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39」)は後続の手順で必要です。
- この PowerShell コマンドレットは、登録機関証明書の秘密キーの生成に使用される一時的な「上書き」 と認識してください。
- このコマンドレットを実行する場合、FAS が開始されるときに構成ファイルから読み込まれる値がチェックされ、使用するキーの長さが決定されます(デフォルトは 2048 です)。
- この手動の PowerShell によって開始される登録機関証明書秘密キー操作で-UseTPM が \$true に設定 されているため、ファイルからの値で TPM の使用に必要な設定に一致しないものは無視されます。
- このコマンドレットの実行によって、構成ファイルの設定が変更されることはありません。
- FAS で開始される後続のユーザー証明書秘密キー自動操作の実行中は、FAS が開始したときにファイル から読み込まれた値が使用されます。
- FAS サーバーがユーザー証明書を発行するときに構成ファイルで KeyProtection 値を GenerateTPM-ProtectedKey に設定して、TPM で保護されるユーザー証明書秘密キーを生成することもできま す。

TPM がキーペアの生成に使用されたことを確認するには、FAS サーバー上でキーペアが生成された時間の Windows

イベントビューアーのアプリケーションログをチェックします。

Information	22/07/2019 12:59:42	Citrix.Fas.PkiCore	14	None
Information	22/07/2019 12:59:41	Citrix.Fas.PkiCore	16	None
Information	22/07/2019 12:59:41	Citrix.Authentication.FederatedAuthenticationService	15	None

Event 15, Citrix.Authentication.FederatedAuthenticationService

General Details

[S15] Administrator [CITRIXTEST\Administrator] creating certificate request [TPM: True] [correlation: e61a73d7-bb61-44af-8d21-1159d864d82e]

注:「[TPM: True]」となっています。

ログは以下のように続きます。

Application Number of events: 3									
Level	Date and Time	Source	Event ID	Task C					
(i) Information	22/07/2019 12:59:42	Citrix.Fas.PkiCore	14	None					
(i) Information	22/07/2019 12:59:41	Citrix.Fas.PkiCore	16	None					
(i) Information	22/07/2019 12:59:41	Citrix.Authentication.FederatedAuthenticationService	15	None					
L									
Event 16, Citrix,Fas.PkiCore									
Course De la 1									
General Details									
[S16] PrivateKey::Create [Identifier afae7c8d-53ff-4cf6-bd96-75fa3e606d3e_TWIN][MachineWide: False][Provider:									
[CNG] Microsoft Platform Crypto Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable:									
[False]									

注:「Provider: CNG M[icr]osoft Platform Crypto Provider」となっています。

手順6:証明書要求セクションをテキストエディターにコピーし、テキストファイルとしてディスクに保存します。
usmcertreq - Notepad	-		x
File Edit Format View Help			
BEGIN CERTIFICATE REQUEST			~
MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXN0RmFicmljMIIBI	jANE	Bgkq	
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3w	TNfF	ROXW	
lhCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAf1bI	nFPg	grz+	
vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V70cEYthxB8CfbaN9MH0EFbepoSY0	CAfu	unXW	
snwIbXD91c/fGyN/3f94P4fbNrjEIOHc+40y/WsPgPRgcq9XBwRjzpGjOgOWRoJS9g220	Y5P _W	vD77	
7f7vZvoQkRy5NXXXATJ+xxYEPLp9JuJaE1WXrTJG+XP3SnG/oCCPit7iUIIc9FjGa3qTU	QIDA	AQAB	
oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9XWH1vztpjxPeJzAV0srLpOsCfNdvYn9u+	1738	BGsr	
4tuLjuQ+An4Y2Rw7b6pZxEICV8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bF	egLH	ls8c	
Y1ITNOtmcHFKt4Loz505E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsg	yMgd	IR8F	
3SmagQjN3C81yqT8z1iF4132x1mQrP/4XQvr1F+T015PM5Fxjj6PEKWopWTYZXGzSC1uf	xevo	:01K	
+tTH9tQYJM6xw3+6TIcfuW0jrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TAT03XG/AB7o=			
END CERTIFICATE REQUEST			
			*

手順 7:以下のコマンドを FAS サーバーの PowerShell に入力して、証明書署名要求を証明機関に送信します:

1 certreq -submit -attrib "certificatetemplate:\<certificate template
 from step 2>" \<certificate request file from step 6>

次に例を示します:

1 certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\
 Administrator.AUTH\Desktop\usmcertreq.txt

以下が表示されます。

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
{&F76160E-DBDC-4D21-A&FD-2E29502177C2}
ldap:
```

この時点で、「証明機関の一覧」ウィンドウが表示される可能性があります。この例の証明機関では http(上部)お よび DCOM(下部)登録の両方が有効です。使用できる場合は DCOM オプションを選択します。

Certification A	uthority List ? ×
Select Certification Authority	
CA	Computer
CG-DC-2-ER-CA (Kerberos)	https://cg-dc-2.auth.local/CG-D(
GG-DC-2-ER-CA (Kerberos)	cg-dc-2.auth.local
< 111	>
	OK Cancel

証明機関が指定されると、PowerShell によって RequestID が表示されます。



手順 8: 証明機関サーバーの証明機関 MMC スナップインで [Pending Requests] をクリックします。要求 ID を 記録します。要求を右クリックし、[発行] を選択します。

手順 9: [発行した証明書] ノードを選択します。発行したばかりの証明書(要求 ID が一致する証明書)を見つけま す。証明書をダブルクリックして開きます。[詳細] タブをクリックします。[ファイルヘコピー] をクリックします。 証明書のエクスポートウィザードが開きます。[次へ] をクリックします。次のファイル形式のオプションを選択しま す。

Certificate Export Wizard
Export File Format Certificates can be exported in a variety of file formats.
Select the format you want to use:
O DER encoded binary X.509 (.CER)
O Base-64 encoded X.509 (.CER)
Oryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 Include all certificates in the certification path if possible
O Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
 Microsoft Serialized Certificate Store (.SST)
Next Cancel

形式は [**Cryptographic Message Syntax Standard- PKCS #7** 証明書(**.P7B**)]を選択し、[証明のパスにあ る証明書を可能であればすべて含む]をオンにする必要があります。

手順 10: エクスポートされた証明書を FAS サーバーにコピーします。

手順 **11**: FAS サーバー上で次の PowerShell コマンドレットを入力して、登録機関証明書を FAS サーバーにイン ポートします:

```
Import-FasAuthorizationCertificateResponse -address <FQDN of FAS server> -Id <ID
GUID from step 5> -Pkcs7CertificateFile <Certificate file from step 10>
```

次に例を示します:

```
Import-FasAuthorizationCertificateResponse -address fashsm.auth.net -Id 5ac3d8bd-
b484-4ebe-abf8-4b2cfd62ca39 -Pkcs7CertificateFile
C:\Users\Administrator.AUTH\Desktop\TPM_FAS_Cert.p7b
```

以下が表示されます。

PS C:\Users\Admini:	strator.AUTH> Import-UcsAuthorizationCertificateResponse -address ucshsm.auth.local -Id 5ac3d8bd-b484-
4ebe-abf8-4b2cfd62	ca39 -Pkcs7CertificateFile C:\Users\Administrator.AUTH\Desktop\TPM_UCS_Cert.p7b
Id Address TrustArea CertificateRequest Status	: 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39 : [Dffline CSR] : a5c27fcc-1dd7-4c2b-8963-16ec311D2Dfc : 0k

手順 12: FAS 管理コンソールを終了して再起動します。

#			(itrix FAS Administration Console - connected to localhost		_ D X	
Initial S	Setup	Rules	Advanced		Connect to an	other server Refresh	۱
							٦
Complete	these setu	up steps:					_
\checkmark	Deple	oy cert	tificate temp	plates		Deploy	
	The req	uired tem	plates are deploy	red in Active Directory.			
	Set u	p a ce	rtificate aut	hority		Publish	-
*	The aut	horizatio	n templates are p	ublished on: ca-1.citrixtest.net\citrixtest-CA-1-CA.			
	Click "P	ublish" to	publish the tem	plates on another certificate authority.			
	Auth	orizo t	his convico			Poputhorizo	
	Auth	orization	riis service	iourad		Reautionze	
	Angua			gurea.			
	Deauth	orize this	service.				-
	Creat	te a ru	le			Create	
	A rule d	lefines a s	smartcard-class co	rtificate that signs users into a Citrix environment.			
	You hav	/e no rule	es configured.				
	Conn	act to	Citrix Clour	1		Connect	-
	Commette this step if you wish to use this EAS service with Citrix Cloud			eonneot			
	comple		cp ii you wish to t				-

注: [このサービスを認証する] 手順には緑色のチェックマークが付いています。

手順 **13**: FAS 管理コンソールで [ルール] タブを選択し、「インストールと構成」の記述に従って設定を編集します。

FAS 管理コンソールの使用 FAS 管理コンソールではオフラインの証明書署名要求を実行できないため、組織で登録機関証明書のオンラインの証明書署名要求が許可されない限り、FAS 管理コンソールの使用はお勧めしません。

FAS の初回のセットアップ手順の実行中、証明書テンプレートを展開して証明機関をセットアップした後、サービス を許可(構成順序の手順 3)する前に次を行います:

手順1:以下の行を次のとおり変更して、構成ファイルを編集します。

<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateTPMProtectedKey"/>

ファイルは以下のように表示されます。

<?xml version="1.0" encoding="utf-8"?> configuration> <appSettings> <!-- This option switch between CAPI API (true) and CNG API (false) Cryptographic Providers <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderLeqacyCsp" value="false"/> <!-- Specify the Cryptographic Service Provider (CSP) / Key Storage Provider (KSP) Name. <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="Microsoft Software Key Storage Provider"/ --> <!-- Specify the Cryptographic Service Provider Type (only for CSP - not KSP). For example: PROV RSA AES is 24 --> <!-- add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderType" value="24"/ --> <!-- Specify Private Key protection [NoProtection]GenerateNonExportableKey|GenerateTPMProtectedKey] --> <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection" value="GenerateTPMProtectedKey"/> <!-- Specify RSA Key length --> <add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyLength" value="2048"/> <!-- Logging: Event log Verbosity (0 Disabled, 1 Errors, 2 Warnings, 3 Informational) --> <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.LogLevel" value="3" / --> <!-- Logging: Event IDs to not log (comma separated) --> <!-- add key="Citrix.Authentication.UserCredentialService.SystemLog.Supress" value="" / --> <!-- Logging: Disable Key Management logs --> <!-- add key="Citrix.TrustFabric.Logging.SystemLog" value=""/ --> </appSettings> <startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/></startup></configuration>

ー部の TPM ではキーの長さが制限されています。デフォルトのキーの長さは、2048 ビットです。お使いのハードウ ェアでサポートされる長さのキーを指定してください。

手順2:サービスを許可します。

手順 3: 証明機関サーバーから、保留中の証明書要求を手動で発行します。登録機関証明書が取得されたら、管理コ ンソールのセットアップ順序の手順3が緑色に変わります。この時点で、登録機関証明書の秘密キーは TPM で生成 されています。証明書はデフォルトで2年間有効です。

手順4:次のように構成ファイルを編集し直します。

<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.KeyProtection"
value="GenerateNonExportableKey"/>

注:

FAS は TPM で保護されたキーでユーザー証明書を生成できますが、TPM は大規模の展開には速度が遅すぎる 可能性があります。

手順 5: FAS を再起動します。これにより、サービスによる構成ファイルの再読み込みが強制され、変更された値が 反映されます。後続の自動秘密キー操作はユーザー証明書キーに影響します。これらの操作では TPM に秘密キーが 保存されませんが、Microsoft ソフトウェアキー記憶域プロバイダーが使用されます。

手順 6: FAS 管理コンソールで [ルール] タブを選択し、「インストールと構成」の記述に従って設定を編集します。

例 3

この例では、HSM に格納されている登録機関証明書の秘密キーおよびユーザー証明書の秘密キーについて説明しま す。この例では、構成済みの HSM を想定しています。HSM にはプロバイダー名(「HSM_Vendor's Key Storage Provider」など)が含まれます。

FAS サーバーを仮想化環境で実行する予定の場合は、HSM ベンダーにハイパーバイザーがサポートされているかどうかを確認してください。

手順 **1**:管理コンソールを使用した FAS の初期セットアップ時には、最初の「証明書テンプレートの展開」および「証明機関のセットアップ」の2つの手順だけを完了します。

#			(itrix FAS Administration Console - connected to localhost			x
Initial S	ial Setup Rules Advanced Connect to another		r server	Refresh			
Complete	these setu	ıp steps:					
\checkmark	Deploy certificate templates Deploy						
	The req	uired tem	plates are deploy	ed in Active Directory.			
\checkmark	Set u	p a ce	rtificate aut	NORITY		Publish	
	Click "Pu	ublish" to	publish the temp	lates on another certificate authority.			
	Authorize this service Authorize				2		
	Create a	an author	ization certicate f	or this service.			
	Creat	e a ru	e			Create	
	A rule d	efines a s	martcard-class ce	rtificate that signs users into a Citrix environment.			
	You hav	e no rule	s configured.				
	Conn	ect to	Citrix Cloud	I		Connect	
	Complete this step if you wish to use this FAS service with Citrix Cloud.						

手順 **2**: HSM ベンダーのドキュメントで、HSM の ProviderName の値を確認します。HSM が CAPI を使用して いる場合、プロバイダーはドキュメントで暗号化サービスプロバイダー(CSP)と記述されている可能性があります。 HSM が CNG を使用している場合、プロバイダーはキー記憶域プロバイダー(KSP)と記述されている可能性があり ます。

手順3:構成ファイルを次のように編集します。

```
<add key="Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.ProviderName" value="HSM_Vendor's Key Storage Provider"/>
```

ファイルは以下のように表示されます。

このシナリオでは、HSM が CNG を使用していると想定しているため、ProviderLegacyCsp の値は false に設定 されています。HSM が CAPI を使用している場合は、ProviderLegacyCsp の値は true に設定されます。HSM ベ ンダーのドキュメントで、HSM が CAPICN と CNG のどちらを使用しているかを確認してください。また、非対称 RSA キー生成でサポートされているキーの長さについても、HSM ベンダーのドキュメントで確認してください。こ の例では、キーの長さはデフォルトの 2048 ビットに設定されています。指定したキーの長さがお使いのハードウェ アでサポートされていることを確認してください。

手順 4: Citrix フェデレーション認証サービスを再起動して、構成ファイルからの値を読み込みます。

手順 5: HSM 内で RSA キーペアを生成し、FAS 管理コンソールの [Initial Setup] タブで [Authorize] をク リックして証明書署名要求を作成します。

手順 **6**: Windows イベントログのアプリケーションエントリをチェックして、キーペアが HSM 内で生成されていることを確認します。

[S16] PrivateKey::Create [Identifier e1608812-6693-4c54-a937-91a2e27df75b_TWIN][MachineWide: False][Provider: [CNG] HSM_Vendor's Key Storage Provider][ProviderType: 0][EllipticCurve: False][KeyLength: 2048][isExportable: False]

注: [Provider: [CNG] HSM_Vendor's Key Storage Provider] となっています。

手順 7: 証明機関サーバーで、証明機関 MMC で [Pending Requests] ノードを選択します。

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region
🙀 107	BEGIN NE	The operation compl	Taken Under Submission	07/04/2016 14:04	AUTH\UCSHSM\$	

要求を右クリックし、[発行]を選択します。

注: [このサービスを認証する] 手順には緑色のチェックマークが付いています。

#	Citrix FAS Administration Console - connected to localhost	
Initial S	etup Rules Advanced	Connect to another server Refresh
Complete	these setup steps:	
	Deploy certificate templates	Deploy
*	The required templates are deployed in Active Directory.	
\checkmark	Set up a certificate authority	Publish
Ť	The authorization templates are published on: ca-1.citrixtest.net\citrixtest-CA-1-CA.	
	Click "Publish" to publish the templates on another certificate authority.	
\checkmark	Authorize this service	Reauthorize
	An authorization certificate is configured.	
	Deauthorize this service.	
	Create a rule	Create
	A rule defines a smartcard-class certificate that signs users into a Citrix environment.	
	You have no rules configured.	
	Connect to Citrix Cloud	Connect
	Complete this step if you wish to use this FAS service with Citrix Cloud.	

手順 8: FAS 管理コンソールで [ルール] タブを選択し、「インストールと構成」の記述に従って設定を編集します。

FAS 証明書ストレージ

FAS では、証明書の保存に FAS サーバー上の Microsoft 証明書ストアを使用しません。埋め込みデータベースを使用します。

登録機関証明書の GUID を特定するには、FAS サーバーで次の PowerShell コマンドレットを入力します:

```
1 Add-pssnapin Citrix.a\*
2 Get-FasAuthorizationCertificate - address \<FAS server FQDN>
```

たとえば、「Get-FasAuthorizationCertificate -address cg-fas-2.auth.net」と入力します:

PS C:\Users\Adminis	strator.AUTH> Get-UcsAuthorizationCertificate -address cg-ucs-2.auth.local
Id Address TrustArea CertificateRequest Status	: a3958424-b8c3-4cac-ba0d-7eb3ce24591c : cg-dc-2.auth.local\CG-DC-2-ER-CA : 3df77088-00e0-4dca-a47a-28060dc16986 : : MaintenanceDue
Id Address TrustArea CertificateRequest	<pre>: fcb185f9-5069-4e34-8625-a333ac126535 : [Offline CSR] : BEGIN CERTIFICATE REQUEST MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXN0RmFicmljMIIBIjANBgkq hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyNzaiWX8DhUnOZMS2YVSDhr36AV5BGeIYOGVCFKvZPe Rmm/x0VM6cNKsLbew3dYlbo+vdgWg86DFRVxT0RhollV86iazDZy0iYGgxe9/s8YZzCspVWN1nB1 zX0UJfo1qo9UsmImYr7MR/dhGAtkfsFUoPcd2+zcezmg0fq/4vmCIuerwqzRR5T/p4og7+IjR1se ECz/CbXR00uiDhW+VWbjcsgklcavzvC/jR33F9dZSXNgKRiGHgfd/lBb3elZKA400oi90u64Q916 3ba9BnihqxIgvwWIL0myUfjJmCgbhLJV4TPBopOdKz/axZEIO5p5XYVjCcpXqhqL7PpnwIDAQAB oAAwDQYJKoZIhvcNAQENBQADggEBAJhdvw6yrLGBMtAgo3oPL608/at+IqHjHKqgcJNJ0/MU7/7X bZB46drLPFzpzF88DkmfoCEg0xlbzFX9waaiFs9CHC/AcEzblN925y1gqljsfC3l5TCKBAeLFoM1 PSEkfYMQU0SBYCuLlKFn1LXLSeQ3qJTZSvptYR0awFmUMQLffwLSR1v0uS8DJSrpASrwdXJk3T0a Gl0/xJo/NRM0wMH+AvGbBsgp31+jnDjXED5RudqARfgVgcW714JP+XIeFrE1TZmUL2skNIXEPNHC H8eAHdYD26caFigydfefbjx4fbaJDFHJs5+1tnrTZ9knCrawhUiIy0MLGZ00aiER+z8= END CERTIFICATE REQUEST</pre>
Status	: WaitingForApproval

ユーザー証明書の一覧を取得するには、以下を入力します:

1 Get-FasUserCertificate - address \<FAS server FQDN>

例: Get-FasUserCertificate -address cg-fas-2.auth.net

PS C:\Users\Administrator.AUTH> Get-UcsUserCertificate -address cg-ucs-2.auth.local

ThumbPrint UserPrincipalName Role CertificateDefinition ExpiryDate	7BA22879F40EE92125A2F96E7DD2D52C73820459 walter@adfs.ext default default
--	---

注:

HSM を使用して秘密キーを保存する場合、HSM コンテナーは GUID で識別されます。HSM 内の秘密キーの GUID は、次のコマンドレットで取得できます。「FQDN of FAS Server」は、FAS サーバーの FQDN です。:

```
1 Get-FasUserCertificate - address \<FAS server FQDN> -KeyInfo $true
```

次に例を示します:

1 Get-FasUserCertificate - address fas3.djwfas.net -KeyInfo \$true

PS C:\Users\administra	<pre>stor> Get-FasUserCertificate -Address fas3.djwfas.net -KeyInfo \$true</pre>
PrivateKeyIdentifier PrivateKeyProvider PrivateKeyIsCng ThumbPrint UserPrincipalName Role CertificateDefinition SecurityContext ExpiryDate	: 38405c4d-63af-43e4-9135-2412246b1112 : Microsoft Software Key Storage Provider : True : AD2441F050A02966AA4DB190BA084976528DB667 : joe@djwfas.net : default : default : default_Definition : : 19/01/2018 09:18:48

関連情報

- FAS のインストールと構成については、「インストールと構成」を参照してください。
- 一般的な FAS 環境については、「Federated Authentication Service のアーキテクチャの概要」を参照してください。
- その他の具体的な手順については、「詳細な構成」を参照してください。

セキュリティとネットワークの構成

September 2, 2022

フェデレーション認証サービス(FAS)は、Microsoft Active Directory および Microsoft 証明機関と密接に統合 しています。ドメインコントローラーやそのほかの重要なインフラストラクチャと同様に、セキュリティポリシーを 展開することによって、システムの適切な管理と保護を行うことが重要です。

このドキュメントでは、FASを展開する場合に考慮する、セキュリティ問題の概要について説明します。また、イン フラストラクチャのセキュリティ保護に役立つ利用可能な機能の概要についても説明します。

ネットワークアーキテクチャ

次の図は、FAS 展開で使用される主要なコンポーネントとセキュリティ境界を示しています。

FAS サーバーは、証明機関やドメインコントローラーと共に、セキュリティ上重要なインフラストラクチャの一部と して扱われる必要があります。フェデレーション環境では、Citrix Gateway および Citrix StoreFront が、ユーザ ー認証を行うことが信頼されたコンポーネントです。そのほかの Citrix Virtual Apps and Desktops コンポーネン トは、FAS 導入の影響を受けません。

WIICTOSOTE	Citrix	Microsoft	Microsoft
ADFS Server (with Web Access Proxy)	Federated Authenti- cation Server	Certificate Authority	Domain Controlle
Windows Server	Windows Server	Vindows Server	Windows Server
TLS Server Certificate	FAS Authorization Certificate FAS User Certificates	FAS User Certificate Template FAS Authorization Certificate Township	UPN walter@auth.loc. Alternative UPN walter@adfs.ext
Encryption Certificate (not used)	s	For	
Citrix	Citrix	Gitrix	Citrix
	StoreFront	Delivery Controller	VDA
Citrix Gateway			
Citrix Gateway	Windows Server	Windows Server & Desktop Operating Systems	rberos ating Systems
Citrix Gateway	S Windows Server	TLS Windows Server & Deskton Operating Systems Ke	Process Server & Desl ating Systems FAS User Certificate

ファイアウォールとネットワークセキュリティ

Citrix Gateway、StoreFront、および Delivery Controller コンポーネント間の通信は、ポート 443 上で TLS に よって保護される必要があります。StoreFront サーバーは発信接続のみを行い、Citrix Gateway は、HTTPS のポ ート 443 を使用したインターネット上の接続のみを受け入れるようにする必要があります。

StoreFront サーバーは相互認証された Kerberos を使用して、ポート 80 で FAS サーバーと通信します。認証には、 FAS サーバーの Kerberos HOST/fqdn ID、および StoreFront サーバーの Kerberos マシンアカウント ID が使用 されます。これにより、Citrix の Virtual Delivery Agent(VDA)がユーザーにログオンするのに必要な、1 回限り 有効の「資格情報ハンドル」が生成されます。

HDX セッションが VDA に接続されると、VDA もポート 80 で FAS サーバーと通信します。認証には、FAS サーバー の Kerberos HOST/fqdn ID、および VDA の Kerberos マシン ID が使用されます。また、VDA は、証明書と秘密 キーへのアクセスに「資格情報ハンドル」を提供する必要があります。

Microsoft 証明機関は、固定 TCP ポートの使用を構成できる、Kerberos 認証の DCOM を使用して、接続を受け入 れます。また、証明機関は、FAS サーバーに信頼された登録エージェント証明書による署名済みの CMC パケットを 提供するよう要求します。

サーバー	ファイアウォールポート
フェデレーション認証サービス	[in] StoreFront および VDA から HTTP 経由で
	Kerberos、[out] DCOM から Microsoft 証明機関
Citrix Gateway	[in] クライアントマシンから HTTPS、[in/out]
	HTTPS と StoreFront サーバー間、[out] HDX から
	VDA
StoreFront	[in] NetScaler から Citrix Gateway、[out] HTTPS
	から Delivery Controller、[out] Kerberos から
	HTTP 経由で FAS
Delivery Controller	[in] StoreFront サーバーから HTTPS、[in/out] VDA
	から HTTP 経由で Kerberos
VDA	[in/out] Delivery Controller から HTTP 経由で
	Kerberos、[in] Citrix Gateway から HDX、[out]
	Kerberos から HTTP 経由で FAS
Microsoft 証明機関	[in]DCOM と、FAS からの署名

Citrix フェデレーション認証サービスと Citrix Cloud の接続

コンソールと FAS は、それぞれユーザーのアカウントとネットワークサービスアカウントを使用して次のアドレスに アクセスします。

- ユーザーアカウントの下の FAS 管理コンソール
 - *.cloud.com
 - *.citrixworkspacesapi.net
 - サードパーティの ID プロバイダーが必要とするアドレス(環境で使用されている場合)
- ネットワークサービスアカウントの下の FAS サービス: *.citrixworkspacesapi.net

環境にプロキシサーバーが含まれている場合は、FAS 管理コンソールのアドレスを使用してユーザープロキシを構成 します。また、ネットワークサービスアカウントのアドレスが netsh または同様のツールを使用して構成されている ことを確認します。

セキュリティに関する注意事項

FAS には、FAS がドメインユーザーの代わりに自律的に証明書を発行できるようにする、登録機関の証明書がありま す。このため、セキュリティポリシーを作成および実装して FAS サーバーを保護し、権限を制限することは重要で す。

委任された登録エージェント

FAS は登録エージェントとして機能することによってユーザー証明書を発行します。Microsoft 証明機関により、登録エージェント、証明書テンプレート、および登録エージェントが証明書を発行できるユーザーを制限できます。

cit	rixtest-DC-C	A Prope	rties	?	x
Extensions	Storage Certifica		Certificate M	anagers Med de	
Enrolment Agents	Auditing	Pecover	Acente	Sec	
Enforment Agents	Auditing	Hecover	y Agents	360	лу
For more informatio	n see <u>Delegate</u>	d Enrollme	ent Agents.		
 Do not restrict enrol 	lment agents				
Restrict enrolment	agents				
Enrolment agents:					
Everyone				Add	
				- MAN	
				Remov	е
Conflored Translate					
Certificate Templati	es:				_
5762				Add	
				Remov	e
					_
Permissions:					_
Name		Acce	:55	Add	
Everyone		Allow		Romau	
				TVEHIOV	
				Dom	
Deny					
OK	Cance	1	Apply	He	þ

このダイアログボックスを使用して、次のことを確認してください:

- [Enrollment agents] の一覧に FAS サーバーのみが含まれている。
- [Certificate Templates] の一覧に FAS テンプレートのみが含まれている。
- [*Permissions*] の一覧に FAS の使用が許可されているユーザーのみが含まれている。たとえば、管理グルー プまたは保護されたユーザーのグループに属するユーザーに FAS が証明書を発行できないようにすることを お勧めします。

アクセス制御リストの構成

「ルールの構成」セクションで説明しているように、証明書が発行された場合の FAS に対するユーザー ID の承認を信 頼する StoreFront サーバーの一覧を構成する必要があります。同様に、証明書の発行対象となるユーザー、および ユーザーが認証可能な VDA マシンを制限することができます。この操作は、標準で構成を行う Active Directory ま たは証明機関のセキュリティ機能に追加で行います。 ファイアウォールの設定

FAS サーバーへのすべての通信では、相互認証された Windows Communication Foundation (WCF) Kerberos ネットワーク接続がポート 80 で使用されます。

イベントログの監視

FAS および VDA は、Windows イベントログに情報を書き込みます。これは、情報の監視および監査に使用できま す。「イベントログ」セクションに、生成される可能性のあるイベントログの一覧を示します。

ハードウェアセキュリティモジュール

FAS によって発行されたユーザー証明書の秘密キーを含むすべての秘密キーは、Network Service アカウントによってエクスポート不可の秘密キーとして保存されます。FAS は、セキュリティポリシーで暗号化ハードウェアセキュリティモジュールが必要とされる場合、このモジュールの使用をサポートします。

FederatedAuthenticationService.exe.config ファイルでは、低レベルの暗号化構成が使用可能です。これらの 設定は、秘密キーが最初に作成されたときに適用されます。そのため、登録機関の秘密キー(4096 ビット、TPM 保 護など)およびランタイムのユーザー証明書には異なる設定が使用されることがあります。

パラメーター	説明
ProviderLegacyCsp	true に設定した場合、FAS では Microsoft CryptoAPI (CAPI) が使用されます。false に設定した場合、FAS で は Microsoft Cryptography Next Generation
ProviderName	は Microsoft Cryptography Next Generation (CNG) API が使用されます。 使用する CAPI または CNG プロバイダーの名前。
ProviderType	Microsoft KeyContainerPermissionAccessEn-
	おいていいのロックション そうしょう おいの ALS 24 を 参照します。CAPI で HSM を使用する場合、および HSM ベンダーで別のタイプを指定されている場合以外
	は、常に24 である必要があります。
KeyProtection	秘密キーの「エクスポート可能」フラグを制御します。 さらに、ハードウェアでサポートされている場合は、ト
	ラステッドプラットフォームモジュール(TPM)のキー ストレージの使用も許可されます。
KeyLength	RSA 秘密キーのキー長。サポートされる値は 1024、 2048、および 4096 です(デフォルトは 2048 です)。

管理の責任

環境の管理は、次のグループに分かれます。

名前	責任
エンタープライズ管理者 ドメインの管理者	フォレスト内の証明書テンプレートのインストールおよ び保護 グループポリシー設定の構成
証明機関の管理者	証明機関の設定
FAS 管理者	FAS サーバーのインストールと構成
StoreFront/Citrix Gateway 管理者	ユーザー認証の構成
Citrix Virtual Desktops 管理者	VDA およびコントローラーの構成

各管理者は、セキュリティモデル全体のさまざまな面を制御し、システムのセキュリティ保護のための、徹底した防 御対策のアプローチを実現します。

グループポリシー設定

信頼された FAS マシンは、グループポリシーで構成済みの「index number -> FQDN」のルックアップテーブルで 識別されます。FAS サーバーに接続する場合、クライアントは FAS サーバーのHOST \ < fqdn>Kerberos ID を検 証します。FAS サーバーにアクセスするすべてのサーバーは、同じインデックスに同一の FQDN を持つ必要があり ます。そうでない場合は、StoreFront および VDA が別の FAS サーバーに接続することがあります。

構成ミスを防ぐために、環境内のすべてのマシンに、単一のポリシーを適用することをお勧めします。FAS サーバー の一覧に変更を加える場合、特にエントリの削除や順序の変更は、注意して行ってください。

この GPO の管理は、FAS サーバーのインストールおよび運用停止を担当する FAS 管理者(またはドメイン管理者) に限定する必要があります。FAS サーバーの運用停止直後に、その FQDN を再度使用しないように注意してください。

証明書テンプレート

FAS から提供される Citrix_SmartcardLogon 証明書テンプレートを使用しない場合、証明書のコピーを変更でき ます。以下の変更がサポートされています。

証明書テンプレートの名前の変更

Citrix_SmartcardLogon の名前を変更する場合、所属組織のテンプレート命名標準に従って、以下を行う必要があります。

- 証明書テンプレートのコピーを作成し、所属組織のテンプレート命名標準に従ってその名前を変更します。
- 管理ユーザーインターフェイスではなく、管理 FAS への FAS PowerShell コマンドを使用します。(管理ユ ーザーインターフェイスは、Citrix のデフォルトのテンプレート名での使用のみを対象としています。)
 - Microsoft MMC 証明書テンプレートスナップインか Publish-FasMsTemplate コマンドを使用して、 自身のテンプレートを公開し、
 - New-FasCertificateDefinition コマンドにより、自身のテンプレートの名前を使用して FAS を構成 します。

全般プロパティの変更

証明書テンプレートの有効期間を変更できます。

更新期間は変更しないでください。FAS は証明書テンプレートのこの設定を無視します。FAS は有効期間の半ばで証 明書を自動的に更新します。

要求処理プロパティの変更

これらのプロパティは変更しないでください。FAS は証明書テンプレートのこれらの設定を無視します。FAS では常に、「秘密キーのエクスポートを許可する」と [同一キーで更新する] はオフにされています。

暗号プロパティの変更

これらのプロパティは変更しないでください。FAS は証明書テンプレートのこれらの設定を無視します。 FAS で提供される該当の設定については、「秘密キー保護」を参照してください。

キーの構成証明プロパティの変更

これらのプロパティは変更しないでください。FAS ではキーの構成証明はサポートされません。

優先テンプレートプロパティの変更

これらのプロパティは変更しないでください。FAS では優先テンプレートはサポートされません。

拡張プロパティの変更

所属組織のポリシーに合わせてこれらの設定を変更できます。

注: 不適切な拡張設定を行うと、セキュリティの問題が発生したり、証明書が使用できなくなる場合があります。

セキュリティプロパティの変更

FAS サーバーのマシンアカウントにのみ読み取り権限および登録権限が許可されるように、これらの設定を変更する ことをお勧めします。FAS サービスには、それ以外の権限は必要ありません。ただし、他の証明書テンプレートと同 様、次の項目も追加できます:

- 管理者がテンプレートに対して読み取りまたは書き込みできるようにする
- 認証ユーザーがテンプレートに対して読み取りできるようにする

	Citrix_	Smartc	ardLogo	n Propertie	s ? X
	Subject Name			ssuance Requi	rements
General	Compatibility	Request	Handling	Cryptography	Key Attestation
Supers	seded Template	s	Extensions	Security	Server
<u>G</u> roup o	rusernames:				
🎎 Au	thenticated Use	ers			
🚨 Do	main Admins (D	JWFAS\[Domain Adm	ins)	
Do Do	main Computer	s (DJWFA	.S∖Domain (Computers)	
				A <u>d</u> d	Remove
		. .			
Permiss	ions for Domain	Computer	s	Allow	Deny
Full C	Control				
Kead	1				
Forol	1				
Autor	enroll				
For ener	cial nemieeione	or advary	ced settings	dick	
Advanc	Advanced. Advanced settings, click Advanced				
	ОК		Cancel	Apply	Help
	0.0			CPP0	

サブジェクト名プロパティの変更

Citrix では、これらのプロパティを変更しないことをお勧めします。

テンプレートで [Active Directory の情報から構築する]が選択されているため、証明機関は証明書拡張にユーザーの SID を含めます。これにより、ユーザーの Active Directory アカウントへの強力なマッピングが提供されます。

サーバープロパティの変更

推奨はされませんが、必要に応じて、所属組織のポリシーに合わせてこれらの設定を変更できます。

発行要件プロパティの変更

これらの設定は変更しないでください。これらは以下のように設定する必要があります。

Citrix_SmartcardLogon Properties ? ×				
General Compatibility Request Handling Countography Key Attestation				
Superseded Templates Extensions Security Server				
Subject Name Issuance Requirements	1			
Require the following for appellment:				
CA est/Seate masses assessed				
✓ This number of authorized signatures: 1				
If you require more than one signature, autoenrollment is not allowed.				
Policy type required in signature:				
Application policy				
Application policy:				
Certificate Request Agent				
Issuance policies:				
Add				
Bemove				
Require the following for recordiment:				
Same criteria as for enrollment				
Valid existing certificate				
Allow key based renewal (*)				
Requires subject information to be provided within the certificate				
request.				
* Control is disabled due to compatibility settings,				
OK Cancel Apply Help]			

互換性プロパティの変更

これらの設定は変更できます。この設定は、**Windows Server 2003 CA**(スキーマバージョン 2)以上とする必要 があります。ただし、FAS がサポートするのは Windows Server 2008 以降の CA のみです。上記の説明のとおり、 **Windows Server 2008 CA**(スキーマバージョン 3)または **Windows Server 2012 CA**(スキーマバージョン 4)を選択することにより使用可能となる追加設定は、FAS では無視されます。

証明機関の管理

証明機関の管理者の任務は、証明機関サーバーの構成、および証明機関サーバーが使用する証明書用秘密キーの発行 です。

テンプレートの公開

エンタープライズ管理者の提供するテンプレートに基づいた証明書を証明機関が発行するには、証明機関の管理者が テンプレートの公開を選択する必要があります。

シンプルなセキュリティ対策としては、FAS サーバーのインストール時にのみ登録機関証明書テンプレートを公開す るか、またはオフラインの証明書発行手続きを選択することです。いずれの場合も、証明機関の管理者は登録機関証 明書の要求の承認において全面的なコントロールを維持し、FAS サーバーの承認に関するポリシーを持つ必要があり ます。

ファイアウォールの設定

一般的に、証明機関の管理者は、証明機関のネットワークファイアウォール設定も管理して、受信接続の制御を行い ます。証明機関の管理者は、DCOM TCP およびファイアウォールルールを構成し、FAS サーバーだけが証明書を要 求できるようにすることができます。

登録の制限

デフォルトでは、登録機関証明書のすべての保持者が、アクセス可能な証明書テンプレートを使用して、ユーザーに 証明書を発行することができます。これを、証明機関プロパティの「登録エージェントの制限」で、特権のないユー ザーグループに制限する必要があります。

cit	rixtest-DC-CA	Prope	rties	? X
Extensions	Storage		Certificate M	lanagers
General	Policy Modul	e .	Ext	Module
Enrolment Agents	Audting	Recover	y Agents	Security
For more information	on see Delegated I	nrollme	nt Agents,	
Do not restrict enro	llment agents			
Restrict enrollment	agents			
Enrollment agents:				
				Add
				Remove
				THOMPTO
Certificate Templat	es:			
				Add
				Remove
Permissions:				
Name		Acce	88	Add
				Remove
				Allow
01	Creard		Analy	Usla

ポリシーモジュールと監査

高度な展開には、カスタムセキュリティモジュールを使用して、証明書の発行の追跡と拒否を行うことができます。

FAS の管理

FAS にはいくつかのセキュリティ機能があります。

アクセス制御リスト(ACL)による StoreFront、ユーザー、および VDA の制限

FAS セキュリティモデルの中心となるのが、機能にアクセスできる Kerberos アカウントの管理です。

アクセスベクトル	説明
StoreFront [IdP]	これらの Kerberos アカウントは、ユーザーが正しく認
	証されたと宣言することを信頼されています。
	Kerberos アカウントのいずれかが危害を受けた場合に
	は、証明書が作成され、FAS の構成で許可されたユーザ
	ーに証明書が使用されます。
VDA [証明書利用者]	これらは、証明書および秘密キーへのアクセスが許可さ
	れたマシンです。このグループ内の危害を受けた VDA ア
	カウントによるシステム攻撃の範囲が制限されるよう、
	ldP が取得した資格情報ハンドルも必要です。
ユーザー	ldP がどのユーザーをアサートするかを管理します。証
	明機関の「制限付き登録エージェント」構成オプション
	と重複していることに注意してください。一般的に、ア
	クセス制御リストには、特権のないアカウントのみを加
	えることをお勧めします。これにより、危害を受けた
	StoreFront アカウントが、権限をより高い管理者レベ
	ルに高めることを防ぎます。特に、ドメイン管理者のア
	カウントは、このアクセス制御リストで許可されるべき
	ではありません。

ルールの構成

独立した複数の Citrix Virtual Apps または Citrix Virtual Desktops の展開で同じ FAS サーバーインフラストラク チャが使用されている場合には、ルールが役立ちます。各ルールにはそれぞれの構成オプションセットがあり、特に Kerberos アクセス制御リスト(ACL)は、個別に構成することができます。

証明機関とテンプレートの設定

証明書テンプレートおよび CA は、それぞれ異なるアクセス権のために構成することができます。高度な構成は、環 境に応じて、権限の度合いが異なる証明書を使用するよう選択する場合があります。たとえば、「外部」と識別された ユーザーには、「内部」ユーザーよりも権限が弱い証明書が発行されることがあります。

セッション中および認証の証明書

FAS 管理者は、認証に使用された証明書を、ユーザーのセッションで使用するかどうか管理します。たとえば、より 権限のある「ログオン」証明書はログオン時にのみ使用するように、セッションでは「署名」証明書のみ使用可能に することができます。

秘密キー保護およびキー長

FAS 管理者は、FAS が秘密キーをハードウェアセキュリティモジュール(HSM)、またはトラステッドプラットフォ ームモジュール(TPM)に保存するよう構成できます。少なくとも登録機関証明書の秘密キーは、TPM に保存して 保護することをお勧めします。このオプションは、「オフライン」証明書要求手続きの中で提供されます。

同様に、ユーザー証明書の秘密キーも TPM または HSM に保存できます。すべてのキーは「エクスポート不可能」と して生成し、キー長は 2048 ビット以上でなければなりません。

イベントログ

FAS サーバーによって、詳細な構成およびランタイムイベントのログが提供されるため、監査と侵入検出に役立てる ことができます。

管理アクセスと管理ツール

FAS には、リモート管理の機能(相互認証の Kerberos)およびツールが含まれています。「ローカルの Administrators グループ」のメンバーは、FAS の構成に対するフルコントロール権限を付与されています。この一覧は、注意して維 持する必要があります。

Citrix Virtual Apps 管理者、Citrix Virtual Desktops 管理者、VDA 管理者

「Active Directory パスワード」は FAS の「資格情報ハンドル」にそのまま置き換えられるため、一般的には、 FAS の利用によって Delivery Controller や VDA 管理者のセキュリティモデルが変更されることはありません。 Controller および VDA の管理グループのメンバーは、信頼されたユーザーに限定する必要があります。監査とイベ ントログを維持する必要があります。

一般的な Windows サーバーセキュリティ

すべてのサーバーにパッチを完全に適用し、標準のファイアウォールとアンチウィルスソフトウェアを使用する必要 があります。セキュリティ上重要なインフラストラクチャのサーバーは、物理的に安全な場所に設置し、ディスクの 暗号化や仮想マシンのメンテナンスオプションにも十分配慮する必要があります。

監査データとイベントログは、リモートマシンに安全に保存する必要があります。

RDP アクセスは、承認された管理者のみに制限する必要があります。可能な場合は、ユーザーアカウント、特に証明 機関およびドメイン管理者のアカウントでは、スマートカードを使用したログオンが要求されるようにする必要があ ります。

関連情報

- FAS のインストールと構成については、「インストールと構成」を参照してください。
- FAS アーキテクチャについては、「展開アーキテクチャ」を参照してください。
- その他の具体的な手順については、「詳細な構成」を参照してください。

パフォーマンスカウンター

November 9, 2021

FASには、	負荷の追跡用の・	一連のパフォー	·マンスカウン	ターが含まれます。
--------	----------	---------	---------	-----------

🚳 Performance Monito	r	_	\Box \times
🔊 File Action View	Window Help		_ 8 ×
🗢 🄿 🖄 📊 🛅			
 Performance Monitoring Tools 	Add Counters	×	
Efformance Data Collector Se Reports	Available counters Select counters from computer: Clocal computer> Browse Citrix Federated Authentication Service Citrix Federated Authentication Service Certificate Signing Request Millseconds Certificate Signing Request Count High Load Level Low Load Level Pool Key Count Tinstances of selected object:	22222	
	Search Add >> Show description OK Cancel Show Color Scale Counter Instance Parent Object	20 Ition Compu	12:08:15 1:40 uter

次の表は、使用可能なカウンターの一覧です。特に明記されていない限り、各カウンターは 10 秒ごとに更新されます。

名前	説明
Average Certificate Signing Request Milliseconds	直前の1分のデータを使用して計算された、証明書署名 要求の平均期間(ミリ秒単位)。
Certificate Count	フェデレーション認証サービスで管理されている証明書 の数。
Certificate Signing Requests Per Minute	直前の1分のデータを使用して計算された、フェデレー ション認証サービスによって発行された1分あたりの証 ^{明書} 署名要求の数
Concurrent Certificate Signing Request Count	の首者ロ安尔の奴。 フェデレーション認証サービスで同時に処理されている 証明書署名要求の数。
Pool Key Count	事前に生成された、証明書署名要求に使用できるキープ ール内のキーペアの数。
Private Key Operations Per Minute	直前の1分のデータを使用して計算された、フェデレー ション認証サービスによって実行された1分あたりの証 明書秘密キー操作の数。
Session Count	フェデレーション認証サービスによって追跡されている VDA セッションの数。
Low/Medium/High Load Level	フェデレーション認証サービスが1分あたりの証明書署 名要求に関して許容できる負荷の推定値。推定値は、前 の1分のデータを使用して、毎分更新されます。「高負
	荷」しきい値を超過すると、公開アプリまたはデスクト ップの起動に失敗することがあります。

Windows ログオンの問題のトラブルシューティング

November 9, 2021

ここでは、ユーザーが証明書やスマートカードを使用してログオンするときに、Windows が提供するログおよびエ ラーメッセージについて説明します。これらのログには、認証の失敗をトラブルシューティングするために使用でき る情報が含まれています。

証明書と公開キー基盤

Windows Active Directory は、ユーザーのログオン用証明書を管理するいくつかの証明書ストアを保守しています。

- NTAuth 証明書ストア: Windows への認証のため、ユーザー証明書をすぐに発行する証明機関(つまりチェ ーンはサポートされません)を NTAuth ストアに配置する必要があります。これらの証明書を表示するには、 certutil プログラムから次のように入力します。certutil -viewstore -enterprise NTAuth
- ルートおよび中間証明書ストア:通常、証明書ログオンシステムは単一の証明書のみを提供できるため、チェ ーンが使用中の場合、すべてのマシン上の中間証明書ストアがこれらの証明書を含んでいる必要があります。 ルート証明書は信頼されたルートストアに、最後から2番目の証明書はNTAuthストアにある必要があります。
- ログオン証明書拡張とグループポリシー: EKU や他の証明書ポリシーを強制的に検証するように Windows を構成できます。Microsoft のドキュメントサイトを参照してください: https://docs.microsoft.com/enus/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)。

レジストリポリシー	説明
AllowCertificatesWithNoEKU	無効にすると、証明書にスマートカードログオン拡張キ ー使用法(Extended Key Usage:EKU)が含まれる必 要があります。
AllowSignatureOnlyKeys	デフォルトで、Windows は、RSA 復号化を許可しない 証明書秘密キーを拒否します。このオプションは、その フィルターを上書きします。
AllowTimeInvalidCertificates	デフォルトで、Windows は期限切れの証明書を拒否し ます。このオプションは、そのフィルターを上書きしま す。
EnumerateECCCerts	楕円曲線認証を有効化します。
X509HintsNeeded	証明書に一意のユーザープリンシパル名(UPN)が含ま れないか、複数の解釈が可能な場合、このオプションを 使用すると、ユーザーが手動で Windows ログオンアカ ウントを指定できます。
UseCachedCRLOnlyAnd、	失効チェックを無効にします(通常ドメインコントロー
IgnoreRevocationUnknownErrors	ラー上で設定)。

ドメインコントローラー証明書: Kerberos 接続を認証するには、すべてのサーバーが適切な「ドメインコントローラー」証明書を持っている必要があります。これらは、[Local Computer Certificate Personal Store] MMC スナップインメニューを使用して要求できます。

UPN 名と証明書マッピング

ユーザー証明書は、一意のユーザープリンシパル名(UPN)をサブジェクトの別名拡張機能に含めることをお勧めし ます。

Active Directory での UPN 名

デフォルトで、Active Directory のすべてのユーザーは、パターン <samUsername>@<domainNetBios> お よび <samUsername>@<domainFQDN> に基づく暗黙的 UPN を持っています。利用できるドメインおよび FQDN は、フォレストに対応する RootDSE エントリに含まれています。RootDSE で、単一のドメインに対して複 数の FQDN アドレスが登録されていることがあることに注意してください。

また、Active Directory のすべてのユーザーは明示的な UPN と altUserPrincipalNames を持っています。これ らはユーザーの UPN を指定する LDAP エントリです。

UPN でユーザーを検索する場合、Windows は、まず(UPN を参照するプロセスの ID に基づいて)現在のドメイン で明示的な UPN を、続けて代替 UPN を探します。一致するものがない場合、暗黙的 UPN を探しますが、これはフ ォレストの異なるドメインで解決されることがあります。

証明書マッピングサービス

証明書に明示的な UPN が含まれない場合、Active Directory は各使用に対して正確な公開証明書を 「x509certificate」 属性に保管するオプションを持っています。そのような証明書をユーザーに解決するために、コ ンピューターは直接この属性を問い合わせることができます(デフォルトでは単一のドメインで)。

用意されているオプションを使用すると、ユーザーがユーザーアカウントを指定してこの検索の速度を上げたり、こ の機能がクロスドメイン環境で使用されるようにしたりできます。

フォレストに複数のドメインがあり、ユーザーがドメインを明示的に指定しない場合、Active Directory の rootDSE が証明書マッピングサービスの場所を指定します。これは通常グローバルカタログマシンに置かれ、フォレスト内の すべての x509certificate 属性のキャッシュビューを持っています。このコンピューターは、証明書だけに基づいて 任意のドメインでユーザーアカウントを効率的に検出するために使用できます。

ログオンドメインコントローラーの選択制御

ある環境に複数のドメインコントローラーが含まれる場合、認証にどのドメインコントローラーが使用されているか を把握して制限すると、ログを有効化して取得するのに便利です。

ドメインコントローラーの選択制御

Windows に対して、ログオンで特定の Windows ドメインコントローラーを強制的に使用させるために、lmhosts ファイル (\Windows\System32\drivers\etc\lmhosts)を構成することで、Windows マシンが使用するドメイ ンコントローラーのリストを明示的に設定することができます。

通常その場所には「lmhosts.sam」という名のサンプルファイルがあります。単に次の1行を追加します。

1.2.3.4 dcnetbiosname #PRE #DOM:mydomai

ここで、「1.2.3.4」は、「mydomain」ドメインで「dcnetbiosname」という名前が付けられているドメインコン トローラーの IP アドレスです。

再起動後に、Windows マシンはその情報を使用して mydomain にログオンします。デバッギングが完了したら、 この構成を取り消す必要があることに注意してください。

使用中のドメインコントローラーの識別

Windows はログオン時に、ユーザーをログオンさせたドメインコントローラーを MSDOS 環境変数に設定します。 これを参照するには、コマンドプロンプトで「**echo %LOGONSERVER%**」を実行します。

認証に関するログは、このコマンドで返されたコンピューターに保存されます。

アカウント監査イベントの有効化

デフォルトで、Windows ドメインコントローラーは完全なアカウント監査ログを有効化していません。これは、グ ループポリシーエディターで、セキュリティ設定の監査ポリシーを介して制御できます。有効化すると、ドメインコ ントローラーはセキュリティログファイル内に追加のイベントログ情報を作成します。

S	Local Group Polic	cy Editor	_ D X
File Action View Help			
 Local Computer Policy Computer Configuration Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) Security Settings Security Settings Account Policies Account Lockout Policy Kerberos Policy Local Policies Audit Policy Security Options Windows Firewall with Advance 	rad Sacurity	Policy Audit account logon events Audit account management Audit directory service access Audit logon events Audit object access Audit policy change Audit privilege use Audit process tracking Audit system events	Security Setting Success, Failure No auditing Success, Failure No auditing Success, Failure Failure No auditing Success, Failure

証明書検証ログ

証明書の有効性チェック

スマートカード証明書が DER 証明書(秘密キー不要)としてエクスポートされた場合、次のコマンドで検証できます。certutil –verify user.cer

CAPI ログの有効化

ドメインコントローラーとユーザーマシンでは、イベントビューアーを開いて、Microsoft/Windows/-CAPI2/Operational Logs のロギングを有効化します。

CAPI ログは、次のレジストリキーで制御できます。CurrentControlSet\Services\crypt32

 值	説明
DiagLevel (DWORD)	詳細度レベル(0~5)
DiagMatchAnyMask (QUADWORD)	イベントフィルター(すべてに 0xffffff を使用)
DiagProcessName (MULTI_SZ)	プロセス名(たとえば、LSASS.exe)によるフィルター

CAPI のログ

メッセージ	説明
チェーンの構築	LSA が CertGetCertificateChain をコールしました
	(結果含む)
失効確認	LSA が CertVerifyRevocation をコールしました(結
	果含む)
X509 オブジェクト	詳細モードでは、証明書と証明書失効リスト(CRL)が
	AppData\LocalLow\Microsoft\X509Objects にダン
	プされます
チェーンポリシーの検証	LSA が CertVerifyChainPolicy をコールしました(パ
	ラメーター含む)

エラーメッセージ

エラーコード	説明
信頼されていない証明書	スマートカード証明書を、証明書を使用してコンピュー
	ターの中間証明書ストアおよび信頼できるルート証明書
	ストアに作成できませんでした。

エラーコード	説明
証明書失効のチェックエラー	証明書 CRL 配布ポイントによって指定されたアドレス
	からスマートカードの CRL をダウンロードできません
	でした。失効チェックが必須の場合、これが原因となっ
	てログオンが失敗します。証明書と公開キー基盤」を参
	照してください。
証明書使用状況エラー	証明書がログオンに適していません。たとえば、サーバ
	一証明書または署名証明書の可能性があります。

Kerberos ログ

Kerberos ログを有効化するには、ドメインコントローラーおよびエンドユーザーマシン上で次のレジストリ値を作 成します。

ハイブ	値の名前	値 [DWORD]
CurrentControlSet\Control\Lsa\Ke	erbgræs/ælarameters	0x1
CurrentControlSet\Control\Lsa\Ke	kleebdæ\Bagdeveters	0xffffffff
CurrentControlSet\Services\Kdc	KdcDebugLevel	0x1
CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

Kerberos ログはシステムイベントログに出力されます。

- •「信頼できない証明書」などのメッセージは診断が簡単です。
- 次の2つのエラーコードは情報提供目的のもので、無視しても問題ありません。
 - KDC_ERR_PREAUTH_REQUIRED(以前のドメインコントローラーとの後方互換性のために使用)
 - 不明なエラー 0x4b

イベントログメッセージ

ここでは、ユーザーが証明書を使用してログオンした場合にドメインコントローラーおよびワークステーションに出 力されるログエントリの例について説明します。

- ドメインコントローラー CAPI2 ログ
- ドメインコントローラーセキュリティログ
- Virtual Delivery Agent (VDA) セキュリティログ
- VDA CAPI ログ
- VDA システムログ

ドメインコントローラー **CAPI2** ログ

ログオン時にドメインコントローラーは発信者の証明書を検証し、一連のログエントリを次の形式で作成します。

Operational Number of	events: 6			
Level	Date and Time	Source	Event ID	Task Category
Information	21/06/2016 15:14:54	CAPI2	30	Verify Chain Policy
Information	21/06/2016 15:14:54	CAPI2	11	Build Chain
Information	21/06/2016 15:14:54	CAPI2	90	X509 Objects
Information	21/06/2016 15:14:54	CAPI2	41	Verify Revocation
Information	21/06/2016 15:14:54	CAPI2	40	Verify Revocation
 Information 	21/06/2016 15:14:54	CAPI2	10	Build Chain
J				

最終イベントログメッセージは、VDA によって提供される証明書に基づいてチェーンを作成するドメインコントロー ラー上に lsass.exe を表示し、その妥当性(失効など)を検証します。結果は「ERROR_SUCCESS」として戻され ます。

- CertVerifyCertificateChainPolicy
 - Policy

```
[type] CERT_CHAIN_POLICY_NT_AUTH
[constant] 6
```

- Certificate

```
[fileRef] 23BC65AFB7F18787ADAAAD5CEF09CC7505C4176F.cer
[subjectName]fred
```

- CertificateChain

[chainRef] {FF03F79B-52F8-4C93-877A-5DFFE40B9574}

- Flags

[value] 0

- Status

[chainIndex] -1 [elementIndex] -1

- EventAuxInfo

[ProcessName] lsass.exe

- CorrelationAuxInfo

```
[Taskid] {F5E7FD3F-628F-4C76-9B1C-49FED786318F}
```

- [SeqNumber] 1
- Result

```
[value] 0
```

ドメインコントローラーセキュリティログ

ドメインコントローラーは一連のログオンイベントを表示します。主要なイベントは 4768 で、証明書を使用して Kerberos Ticket Granting Ticket(krbtgt)を発行します。

これより前のメッセージは、ドメインコントローラーに対して認証するサーバーのマシンアカウントを表示します。 これより後のメッセージは、ドメインコントローラーに対して認証するために使用される新しい krbtgt に属するユ ーザーアカウントを表示します。

Keywords Date	e and Time	Source	Event ID	Task Category	^	
Audit Success 21/0	06/2016 15:14:56	Security-Auditing	4624	Logon		
Audit Success 21/0	06/2016 15:14:56	Security-Auditing	4624	Logon		
Audit Success 21/0	06/2016 15:14:54	Security-Auditing	4769	Kerberos Service Ticket Operations	.	
Audit Success 21/0	06/2016 15:14:54	Security-Auditing	4768	Kerberos Authentication Service		
Audit Success 21/0	06/2016 15:14:54	Security-Auditing	4769	Kerberos Service Ticket Operations		
Audit Success 21/0	06/2016 15:14:54	Security-Auditing	4634	Logoff		
Audit Success 21/0	06/2016 15:14:54	Security-Auditing	4624	Logon		
Audit Success 21/0	06/2016 15:14:54	Security-Auditing	4624	Logon	Y	
Event 4768, Security-Auditing					×	
General Details						
Friendly View O XML Vie	ew					
+ System						
- EventData						
TargetUserName	e fred					
TargetDomainNa	ame CITRIXTEST.NE	т				
TargetSid	S-1-5-21-3907317	715-1143989709	-1377117006-1	106		
ServiceName	krbtgt					
ServiceSid	ServiceSid S-1-5-21-390731715-1143989709-1377117006-502					
TicketOptions	0x40810010					
Status	0x0					
TicketEncryption	nType0x12					
PreAuthType	PreAuthType 16					
IpAddress	IpAddress ::ffff:192.168.0.10					
IpPort	49348					
CertIssuerName citrixtest-DC-CA						
CertSerialNumber 5F0001D1FCA2AC30F36879CEEC00000001D1FC						
CertThumbprint	23BC65AFB7F187	87ADAAAD5CEF	9CC7505C417	6F		

VDA セキュリティログ

ログオンイベントに対応する VDA セキュリティ監査ログはイベント ID が 4648 のエントリで、winlogon.exe により記録されます。

Security Number of events: 24						
Keywords Date and Tim	e	Source	Event ID	Task Category		
Audit Success 21/06/2016 15	:14:54	Security-Auditing	4648	Logon		
<		Ш		>		
Event 4648, Security-Auditing				×		
General Details						
Friendly View O XML	View					
+ System				^		
- EventData						
SubjectUserSid	S-1-5-18					
SubjectUserNa	me VDA79\$	5				
SubjectDomai	nName CITR	RIXTEST				
SubjectLogon	d 0x3e7					
LogonGuid	{0000000	00-0000-0000-0000-00	00000000	00}		
TargetUserName fred						
TargetDomain	Name CITRI	XTEST				
TargetLogonG	uid (51B22B	CC-9F90-CE55-6E44-2	1D7EEC216	52C}		
TargetServerN	ame localho	st				
TargetInfo	localhost					
Processid	0x126c					
ProcessName	C:\Windo	ws\System32\winlogo	n.exe			
IpAddress	192.168.	0.9				
lpPort	51171			~		

VDA CAPI ログ

このサンプルの VDA CAPI ログは、lsass.exe から単一のチェーンビルドおよび検証シーケンスを示しており、ドメ インコントローラー証明書(dc.citrixtest.net)を検証しています。

(1) Information	21/06/2016 15:14:54	CAPI2	30 Verify Chain P
Information	21/06/2016 15:14:54	CAPI2	11 Build Chain
Information	21/06/2016 15:14:54	CAPI2	90 X509 Objects
Information	21/06/2016 15:14:54	CAPI2	41 Verify Revocat
Information	21/06/2016 15:14:54	CAPI2	40 Verify Revocat
(i) Information	21/06/2016 15:14:54	CAPI2	10 Build Chain

- UserData - CertVerifyCertificateChainPolicy - Policy [type] CERT_CHAIN_POLICY_NT_AUTH [constant] 6 - Certificate [fileRef] 813C6D12E1E1800E61B8DB071E186EB912B7 [subjectName] dc.citrixtest.net - CertificateChain [chainRef] {84E0B3D1-A4D4-4AC7-BA99-5291415B343 - Flags [value] 0 - Status [chainIndex] -1

VDA システムログ

Kerberos ログが有効化されている場合、システムログは、エラー KDC_ERR_PREAUTH_REQUIRED(無視して かまいません)と、Kerberos ログオンが成功したことを示す Winlogon からのエントリを表示します。

 Information 	21/06/2016 15	:14:56	Winlogon	7001
Error	21/06/2016 15	:14:54	Security-Kerberos	3
<		Ш		>
Event 7001, Winlogon				
General Details				
Friendly View	○ <u>X</u> ML View			
- System				^
- Prov	vider			
	[Name] [Guid]	Microso (DBE9B)	oft-Windows-Winlogon 383-7CF3-4331-91CC-A3CB16	A3B538)
Eve	ntID	7001		
Vers	sion	0		
Leve	el	4		
Task	c	1101		
Орс	ode	0		
Key	words	0x2000	00000000000	~
. Tim	eCreated			

イベントログ

次の表は、FAS で生成されるイベントログエントリの一覧です。

管理イベント [フェデレーション認証サービス]

[イベントソース: Citrix.Authentication.FederatedAuthenticationService]

これらのイベントは、FAS サーバーでの構成変更に応じて記録されます。

ログコード

[S001] アクセス拒否: ユーザー [{0}] は管理者グループのメンバーではありません

[S002] アクセス拒否: ユーザー [{0}] はロール [{1}] の管理者ではありません

[S003] 管理者 [{0}] は保守モードを [{1}] に設定しています

[S004] 管理者 [{0}] は CA [{1}] テンプレート [{2} および {3}] で登録しています

[S005] 管理者 [{0}] は CA [{1}] の権限を取り消しています

[S006] 管理者 [{0}] は新しい証明書定義 [{1}] を作成しています

[S007] 管理者 [{0}] は証明書定義 [{1}] を更新しています

[S008] 管理者 [{0}] は証明書定義 [{1}] を削除しています

[S009] 管理者 [{0}] は新しいロール [{1}] を作成しています

[S010] 管理者 [{0}] はロール [{1}] を更新しています

[S011] 管理者 [{0}] はロール [{1}] を削除しています

[S012] 管理者 [{0}] は証明書を作成しています [UPN: {1} sid: {2} ロール: {3}][Certificate Definition: {4}][セ キュリティコンテキスト: {5}]

[S013] 管理者 [{0}] は証明書を削除しています [UPN: {1} ロール: {2} 証明書定義: {3} セキュリティコンテキスト: {4}]

[S015] 管理者 [{0}] は証明書要求を作成しています [TPM: {1}]

[S016] 管理者 [{0}] は認証証明書をインポートしています [参照: {1}]

[S050] 管理者 [{0}] は新しいクラウド構成を作成しています: [{1}]

[S051] 管理者 [{0}] はクラウド構成を更新しています: [{1}]

[S052] 管理者 [{0}] はクラウド構成を削除しています

ログコード

[S401] 構成アップグレードを実行中です-[開始バージョン {0}][to version {1}]
[S402] エラー: Citrix フェデレーション認証サービスは Network Service として実行する必要があります [現在は {0} として実行中]
[S404] Citrix フェデレーション認証サービスのデータベースを強制的に消去しています
[S405] レジストリからデータベースへのデータの移行中にエラーが発生しました: [{0}]
[S406] レジストリからデータベースへのデータ移行が完了しました(注: ユーザー証明書は移行されない)
[S407] データベースが既に存在していたため、レジストリベースのデータはデータベースに移行されませんでした
[S408] 構成をダウングレードできません-[バージョン {0} 以降][to version {1}]
[S409] ThreadPool MinThreads は [ワーカー: {0} 完了: {1}] から [ワーカー: {2} 完了: {3}] に変更されました
[S410] ThreadPool MinThreads を [ワーカー: {0} 完了: {11] から [ワーカー: {2} 完了: {3}] に変更できません
でした
[S411] FAS サービスの開始エラー: [{0}]

ID アサーションの作成 [フェデレーション認証サービス]

[イベントソース: Citrix.Authentication.FederatedAuthenticationService]

これらのイベントは、信頼済みのサーバーがユーザーログオンをアサートすると、ランタイム時に FAS サーバーに記 録されます。

ログコード

[S101] サーバー [{0}] にはロール [{1}] の ID をアサートする権限がありません

[S102] サーバー [{0}] は UPN [{1}] のアサートに失敗しました(例外: {2}{3})

[S103] サーバー [{0}] は UPN [{1}]、SID {2} を要求しましたが、検索で SID {3} が返されました

[S104] サーバー [{0}] は UPN [{1}] のアサートに失敗しました(UPN はロール [{2}] によって許可されていません)

[S105] サーバー [{0}] は ID のアサーションを発行しました [UPN: {1}、ロール: {2}、セキュリティコンテキスト: [{3}]]

[S120] [UPN: {0}、ロール: {1}、セキュリティコンテキスト: [{2}]] に対して証明書を発行しています

[S121] 証明書が [UPN: {0} ロール: {1}] に [認証局: {2}] から発行されました

[S122] 警告: サーバー過負荷です [UPN: {0}、ロール: {1}] [1 分あたりの要求 {2}]。

[S123] [UPN: {0} ロール: {1}] の証明書の発行に失敗しました [例外: {2}]

[S124] [認証局: {2}]の[UPN: {0} ロール: {1}]の証明書の発行に失敗しました[例外: {3}]
```
証明書利用者の行動 [フェデレーション認証サービス]
```

[イベントソース: Citrix.Authentication.FederatedAuthenticationService]

これらのイベントは、VDA にユーザーがログオンすると、ランタイム時に FAS サーバーに記録されます。

ログコード

[S201] 証明書利用者 [{0}] にはパスワードへのアクセス権がありません。

[S202] 証明書利用者 [{0}] には証明書へのアクセス権がありません。

[S203] 証明書利用者 [{0}] にはログオン CSP へのアクセス権がありません

[S204] 証明書利用者 [{0}] が [{4}] によって承認されたログオン CSP にアクセスしています [UPN: {1}] 役割: [{2}] [操作: {3}]

[S205] 呼び出しアカウント [{0}] はロール [{1}] の証明書利用者ではありません

[S206] 呼び出しアカウント [{0}] は証明書利用者ではありません

[S208] 秘密キーの処理が失敗しました [操作: {0}] [UPN: {1}、ロール: {2}、証明書定義 {3}] [エラー {4} {5}]

セッション内証明書サーバー [フェデレーション認証サービス]

[イベントソース: Citrix.Authentication.FederatedAuthenticationService]

これらのイベントは、ユーザーはセッション内証明書を使用すると、FAS サーバーで記録されます。

ログコード

[S301] アクセス拒否: ユーザー [{0}] には仮想スマートカードへのアクセス権がありません

[S302] ユーザー [{0}] は不明な仮想スマートカードを要求しました [拇印: {1}]

[S303] アクセス拒否:ユーザーが [{0}] 仮想スマートカードと [UPN: {1}] 一致しません

[S304] コンピューター [{2}] でプログラム [{1}] を実行中のユーザー [{0}] は秘密キー処理 [{6}] のために仮想スマー トカードを使用しています [UPN: {3}、ロール: {4}、拇印: {5}]

```
[S305]秘密キーの処理が失敗しました[操作: {0}][UPN: {1}、ロール: {2}、コンテナ名 {3}][エラー {4} {5}]。
```

FAS アサーションプラグイン [フェデレーション認証サービス]

[イベントソース: Citrix.Authentication.FederatedAuthenticationService]

これらのイベントは、FAS アサーションプラグインによって記録されます。

[S500] FAS アサーションプラグインが設定されていません

[S501] 設定された FAS アサーションプラグインをロードできませんでした [例外: {0}]

[S502FAS]FAS アサーションプラグインがロードされました [pluginId={0}] [assembly={1}] [location={2}]

[S503] サーバー [{0}] が UPN [{1}] のアサートに失敗しました(ログオン値が提供されましたがプラグイン [{2}] が 対応していません)

[S504] サーバー [{0}] が UPN [{1}] のアサートに失敗しました(ログオン値が提供されましたが、FAS プラグインが 構成されていません)

[S505] サーバーが [{0}]UPN の [{1}] アサートに失敗しました(プラグインに [{2}] よりログオン値が拒否されステ ータス [{3}] とメッセージ [{4}] が返されました)

[S506] プラグイン [{0}] がサーバー [{1}] のログオン値を UPN [{2}] として承認しメッセージ [{3}] が返されました

[S507] サーバー [{0}] は UPN [{1}] のアサートに失敗しました(プラグイン [{2}] が例外 [{3}] をスローしました)

[S507] サーバー [{0}] は UPN [{1}] のアサートに失敗しました(プラグイン [{2}] が例外 [{3}] をスローしました)

[S508] サーバー [{0}] が UPN [{1}] のアサートに失敗しました(処理へのアクセスが提供されましたがプラグイン [{2}] が対応していません)

[S509] サーバー [{0}] が UPN [{1}] のアサートに失敗しました(処理へのアクセスが提供されましたが、FAS プラグ インが構成されていません)

[S510] サーバー [{0}] が UPN [{1}] のアサートに失敗しました(プラグイン [{2}] によってアクセス処理が無効と判断されました)

Workspace 対応 FAS [フェデレーション認証サービス]

[イベントソース: Citrix.Fas.Cloud]

FAS と Workspace を組み合わせて使用している場合、これらのイベントがログに記録されています。

ログコード

[S001] Citrix Cloud サービスキーを切り替えています [FAS ID={0}]

[S002] FAS クラウドサービスを開始しています。FasHub クラウドサービス URL: {0}

[S003] FAS はクラウドに登録しました [FAS ID: {0}] [トランザクション ID: {1}]

[S004] FAS はクラウドへの登録に失敗しました [FAS ID: {0}] [トランザクション ID: {1}] [例外: {2}]

[S005] FAS はクラウドに現在の構成を送信しました [FAS ID: {0}] [トランザクション ID: {1}]

[S006] FAS はクラウドに現在の構成を送信できませんでした [FAS ID: {0}] [トランザクション ID: {1}] [例外: {2}]

[S007] FAS はクラウドから登録解除しました [FAS ID: {0}] [トランザクション ID: {1}]

[S009] FAS はクラウドからの登録解除に失敗しました [FAS ID: {0}] [トランザクション ID: {1}] [例外: {2}]

[S010] FAS サービスはクラウドメッセージング URL に接続されています: {0}

[S011] FAS サービスはクラウドに接続されていません

[S012] FAS サービスは Citrix Cloud からのシングルサインオンで利用可能です

[S013] FAS サービスは Citrix Cloud からのシングルサインオンで利用できません。[{0}] 詳しくは、管理コンソー ルを確認してください

[S014] クラウドサービス<service name>の呼び出しに失敗しました [FAS ID: {0}] [トランザクション ID: {1}] [例外: {2}]

[S015] Citrix Cloud からのメッセージは、呼び出し元が許可されていないためブロックされました [メッセージ ID {0}] [トランザクション ID {1}] [呼び出し元 {2}]

[S016] クラウドサービス<service name>の呼び出しに成功しました [FAS ID: {0}] [トランザクション ID: {1}]

[S019] FAS はクラウド [FAS ID: {0}] [トランザクション ID: {1}] から構成をダウンロードしました

[S020] FAS はクラウド [FAS ID: {0}] [トランザクション ID: {1}] [例外: {2}] から構成をダウンロードできません でした

[S021] FAS クラウドサービスを開始できませんでした。例外: {0}

[S022] FAS クラウドサービスを停止しています

ログオン **[VDA]**

[イベントソース: Citrix.Authentication.IdentityAssertion]

これらのイベントは、ログオン時に VDA で記録されます。

ログコード

[S101] ID アサーションログオンに失敗しました。認識できないフェデレーション認証サービス [ID: {0}]

[S102] ID アサーションログオンに失敗しました。{0} の SID が見つかりませんでした [例外: {1}{2}]

[S103] ID アサーションログオンに失敗しました。ユーザー {0} の SID は {1} ですが、想定された SID は {2} です

[S104] ID アサーションログオンに失敗しました。フェデレーション認証サービスへの接続に失敗しました: {0} [エ ラー: {1} {2}]

[S105] ID アサーションログオン。[ユーザー名: {0}][Domain: {1}] にログインしています

[S106] ID アサーションログオン。[証明書: {0}] にログインしています。

[S107] ID アサーションログオンに失敗しました。[例外: {0}{1}]

[S108] ID アサーションサブシステム。ACCESS_DENIED [呼び出し元: {0}]

セッション内証明書 [VDA]

[イベントソース: Citrix.Authentication.IdentityAssertion]

これらのイベントは、ユーザーがセッション内証明書を使用しようとすると、VDA に記録されます。

ログコード

[S201] 仮想スマートカードの [PID: {1} プログラム名: {2}][Certificate thumbprint: {3}] へのアクセスが [{0}]
 に認証されました
 [S203] 仮想スマートカードサブシステム。アクセスが拒否されました [呼び出し元: {0}、セッション: {1}]

[S204] 仮想スマートカードサブシステム。スマートカードのサポートが無効化されました。

証明書要求およびキーペア生成 [フェデレーション認証サービス]

[イベントソース: Citrix.Fas.PkiCore]

これらのイベントは、FAS サーバーが低レベルの暗号化操作を実行すると記録されます。

ログコード

[S001] TrustArea::TrustArea: 証明書がインストールされました [TrustArea: {0}] [証明書

{1}][TrustAreaJoinParameters{2}

[S014] Pkcs10Request::Create: PKCS10 要求が作成されました [識別名 {0}]

[S016] PrivateKey::Create [識別子 {0}][MachineWide: {1}][プロバイダー: {2}][ProviderType:

{3}][EllipticCurve: {4}][KeyLength: {5}][isExportable: {6}]

[S017] PrivateKey::Delete [CspName: {0}、識別子 {1}]

ログコード

[S104] MicrosoftCertificateAuthority::GetCredentials: {0}の使用権限が付与されました

[S105]MicrosoftCertificateAuthority::SubmitCertificateRequest エラーが応答 [{0}] を返しました

[S106] MicrosoftCertificateAuthority::SubmitCertificateRequest 証明書 [{0}] が発行されました

[S112] MicrosoftCertificateAuthority::SubmitCertificateRequest - 承認待機中 [CR_DISP_UNDER_SUBMISSION] [参照: {0}]

エンドユーザーエラーメッセージ

ここでは、Windows ログオンページでユーザーに表示される一般的なエラーメッセージの一覧を示します。

表示されるエラーメッセージ	説明および参照先
無効なユーザー名またはパスワードです。	コンピューターはユーザーが有効な証明書および秘密キ
	ーを持っていると判断していますが、Kerberos ドメイ
	ンコントローラーが接続を拒否しました。この記事の
	「 <i>Kerberos</i> ログ」を参照してください。
システムにログオンできませんでした。資格情報を確認	ドメインコントローラーに接続できないか、ドメインコ
できませんでした。/この要求は、サポートされていませ	ントローラーにスマートカード認証をサポートする証明
ho	書が構成されていません。「Kerberos 認証」、「ドメイン
	コントローラー認証」、または「ドメインコントローラ
	ー」証明書のドメインコントローラーを登録します。こ
	れは通常試す価値があります。既存の証明書が有効に見
	える場合でも同様です。
システムにログオンできませんでした。認証のために使	中間証明書とルート証明書がローカルコンピューターに
用されたスマートカード証明書が信頼できませんでした。	インストールされていません。「証明書と公開キー基盤」
	を参照してください。
不正な要求	これは通常、証明書の拡張子が正しく設定されていない
	か、RSA キーが短すぎることを示します(2048 ビット
	未満)。

関連情報

- スマートカードログオン用のドメインを構成します: http://support.citrix.com/article/CTX206156
- スマートカードログオンポリシー: https://docs.microsoft.com/en-us/previous-versions/windows /it-pro/windows-server-2008-R2-and-2008/ff404287(v=ws.10)
- CAPI ログの有効化: http://social.technet.microsoft.com/wiki/contents/articles/242.troublesho oting-pki-problems-on-windows.aspx
- Kerberos ログの有効化: https://support.microsoft.com/en-us/kb/262177
- サードパーティの証明機関を使用してスマートカードログオンを有効化するためのガイドライン: https://support.microsoft.com/en-us/kb/281245

PowerShell コマンドレット

November 9, 2021

シンプルな展開ではフェデレーション認証サービス(FAS)管理コンソールも使用できますが、PowerShell イン ターフェイスにはより詳細なオプションがあります。コンソールでは使用できないオプションを使用する場合は、 PowerShell のみを使用して構成を行うことをお勧めします。

次のコマンドによって FAS PowerShell コマンドレットが追加されます。

1 Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1

PowerShell ウィンドウでは、Get-Help < cmdlet name> を使用して、コマンドレットのヘルプを表示できます。

FAS PowerShell SDK コマンドレットについて詳しくは、https://developer-docs.citrix.com/projects/feder ated-authentication-service-powershell-cmdlets/en/latest/を参照してください。

展開アーキテクチャ

November 9, 2021

はじめに

フェデレーション認証サービス(FAS)は Active Directory 証明機関と統合して、Citrix 環境内でのシームレスなユ ーザー認証を実現する Citrix コンポーネントです。このドキュメントでは、環境に適した、さまざまな認証アーキテ クチャについて説明します。

FAS が有効化されると、信頼された StoreFront サーバーにユーザー認証の判断が委任されます。StoreFront は最 新の Web テクノロジを中心に構築されたビルトイン認証オプションの包括的なセットを搭載しており、StoreFront SDK やサードパーティの IIS プラグインを使用して容易に拡張できます。基本的な設計目標は、Web サイトへのユ ーザー認証が可能なすべての認証テクノロジを、Citrix Virtual Apps または Citrix Virtual Desktops の展開への ログインに活用することです。

このドキュメントでは、複雑さを増す上位レベルの展開アーキテクチャに関する例が記載されています。

- 内部展開
- Citrix Gateway の展開
- ADFS SAML
- B2B アカウントのマッピング
- Windows 10 Azure AD への参加

FAS 関連記事にリンクしています。すべてのアーキテクチャにおける FAS のセットアップについては「インストール と構成」を参照してください。

アーキテクチャの概要

FAS には、StoreFront の認証した Active Directory ユーザーの代わりに、スマートカードクラスの証明書を自動 的に発行する権限が付与されます。これは、管理者が物理スマートカードをプロビジョニングできるツールと同様 の API を使用します。ユーザーが Citrix Virtual Apps または Citrix Virtual Desktops の Virtual Delivery Agent (VDA) に仲介されると、マシンに証明書がアタッチされ、Windows ドメインはログオンを標準のスマートカード認 証と見なします。

ユーザーが Citrix 環境へのアクセスを要求すると、信頼済みの StoreFront サーバーが FAS にアクセスします。FAS は、単一の Citrix Virtual Apps または Citrix Virtual Desktops セッションがそのセッションの証明書で認証でき るようにするチケットを付与します。VDA でユーザーを認証する必要がある場合、VDA は FAS にアクセスしてチケ ットを使用します。ユーザー証明書の秘密キーにアクセスできるのは FAS だけです。VDA は、証明書を使用して実 行する必要のあるすべての署名処理および暗号化解除処理を、FAS に送信しなければなりません。

以下の図に、Microsoft 証明機関と統合した FAS による、StoreFront と Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA) へのサポートサービスの提供について示します。



内部展開

FAS では、さまざまな認証オプション(Kerberos シングルサインオンを含む)を使用した StoreFront への安全な ユーザー認証、および十分に認証された Citrix HDX セッションへの接続が可能です。 これにより、Windows 認証にユーザーの資格情報やスマートカードの PIN の入力が求められることはありません。 また、シングルサインオンサービスのような「保存されたパスワードの管理」機能を使用する必要もありません。こ れを使用して、Citrix Virtual Apps の旧バージョンで利用可能な Kerberos 制約付き委任のログオン機能を置き換 えることができます。

エンドポイントデバイスへのログオンにスマートカードを使用したかどうかにかかわらず、セッション内ではすべて のユーザーが、公開キー基盤(PKI)の証明書にアクセスできます。このため、スマートフォンやタブレットのよう に、スマートカードリーダーを搭載していないデバイスからも、2 要素認証モデルへの円滑な移行が可能です。

この展開では、FAS を実行する新しいサーバーが追加されますが、このサーバーにはユーザーの代わりにスマートカ ードクラスの証明書を発行する権限が付与されます。これらの証明書は、スマートカードによるログオンの代わりと して、Citrix HDX 環境でのユーザーセッションへのログオンに使用されます。



Citrix Virtual Apps または Citrix Virtual Desktops 環境は、CTX206156で説明するように、スマートカードによるログオンと同様の方法で構成する必要があります。

既存の展開では、通常、ドメインに参加する Microsoft 証明機関を利用可能にし、ドメインコントローラーにドメイン コントローラー証明書を割り当てるだけで済みます。(CTX206156 の「Issuing Domain Controller Certificates」 セクションを参照してください。)

関連情報:

- キーは、ハードウェアセキュリティモジュール(HSM)やビルトインのトラステッドプラットフォームモジュ ール(TPM)に保存できます。詳しくは、「秘密キー保護」を参照してください。
- FAS をインストールおよび構成する方法については、「インストールと構成」を参照してください。

Citrix Gatewayの展開

Citrix Gateway の展開は内部展開と似ていますが、StoreFront と組み合わせた Citrix Gateway が追加されており、認証のプライマリポイントが Citrix Gateway そのものに移動されています。Citrix Gateway には、企業 Webサイトへのリモートアクセスの保護に使用できる、認証および承認の高度なオプションが含まれています。

この展開を利用すれば、Citrix Gateway への初回認証時およびユーザーセッションへのログイン時に、何度も PIN の入力が求められることはありません。また、AD パスワードやスマートカードを必要とせずに、高度な Citrix Gateway 認証テクノロジを利用することができます。



Citrix Virtual Apps または Citrix Virtual Desktops 環境は、CTX206156で説明するように、スマートカードによるログオンと同様の方法で構成する必要があります。

既存の展開では、通常、ドメインに参加する Microsoft 証明機関を利用可能にし、ドメインコントローラーにドメイン コントローラー証明書を割り当てるだけで済みます。(CTX206156 の「Issuing Domain Controller Certificates」 セクションを参照してください。)

Citrix Gateway をプライマリ認証システムとして構成する場合は、Citrix Gateway と StoreFront 間のすべての 接続を TLS で保護するようにします。特に、この展開では Citrix Gateway サーバーの認証にコールバック URL が 使用されるため、コールバック URL が Citrix Gateway サーバーを指すよう正しく構成する必要があります。

	Add NetS	caler Gateway Appliance
StoreFront	Authentication Sett	tings how the remote user provides authentication credentials
 General Settings Secure Ticket Authority Authentication Settings Summary 	Version: VServer I₽ address: (optional) Logon type: Smart card fallback: Callback URL: (optional)	10.0 (Build 69.4) or later v10.0: SNIP or MIP, v10.1+: VIP Domain None https://NetScalerGatewayFQDN /CitrixAuthService/AuthService.asmx Men no Callback URL is specified, Smart Access is not available.
		<u>B</u> ack Cancel

関連情報:

- Citrix Gateway を構成する方法については、『How to Configure NetScaler Gateway 10.5 to use with StoreFront 3.6 and Citrix Virtual Desktops 7.6』を参照してください。
- FAS をインストールおよび構成する方法については、「インストールと構成」を参照してください。

ADFS SAML の展開

Citrix Gateway の主要な認証テクノロジにより、SAML ID プロバイダー(IdP)として機能できる、Microsoft ADFS との統合が実現します。SAML アサーションは暗号を使用して署名された XML ブロックであり、コンピュー ターシステムへのユーザーのログオンを承認する、信頼された IdP によって発行されます。つまり、FAS サーバーに よって、Microsoft ADFS サーバー(またはほかの SAML 対応 IdP)へのユーザー認証の委任が許可されます。



ADFS は、一般的にインターネットを利用して企業リソースにリモートでユーザーを安全に認証するために使用され、 たとえば、Office 365 の統合に多く利用されます。

関連情報:

- ・ 詳しい情報については、「ADFS の展開」を参照してください。
- FAS をインストールおよび構成する方法については、「インストールと構成」を参照してください。
- 構成に関する考慮事項については、この記事の「Citrix Gateway の展開」セクションを参照してください。

B2B アカウントのマッピング

2 つの会社が互いのコンピューターシステムを利用する場合、一般的なオプションは Active Directory フェデレー ションサービス(ADFS)サーバーを信頼関係でセットアップすることです。これにより、一方の会社のユーザーが、 他方の会社の Active Directory(AD)環境にシームレスに認証されるようになります。ログオン時に、各ユーザー は自社のログオン資格情報を使用します。ADFS はこれを相手の会社の AD 環境の「シャドウアカウント」に自動的 にマップします。



関連情報:

• FAS をインストールおよび構成する方法については、「インストールと構成」を参照してください。

Windows 10 Azure AD への参加

Windows 10 では、「Azure AD への参加」というコンセプトが導入されました。これは、従来の Windows ドメイ ンへの参加とコンセプトが似ていますが、「インターネット上」のシナリオに焦点を当てている点が特徴です。これ は、ラップトップおよびタブレットとうまく機能します。従来の Windows ドメイン参加と同様に、Azure AD には 企業の Web サイトやリソースで、シングルサインオンモデルを実現する機能があります。これらはすべて「インタ ーネットに対応」しているため、社内 LAN だけでなく、インターネットに接続したすべての場所から機能します。



この展開は、事実上「オフィスにいるエンドユーザー」という概念のない一例です。ラップトップコンピューターは 最新の Azure AD 機能を使用して完全にインターネット経由で登録および認証されています。

この展開では、IP アドレスが使用可能なすべての場所、つまりオンプレミス、ホストされたプロバイダー、Azure、 あるいはそのほかのクラウドプロバイダーで、インフラストラクチャが実行できる点に注意してください。Azure AD Connect の同期機能により、自動的に Azure AD に接続します。例として示した図では、簡単にするために Azure 仮想マシンを使用しています。

関連情報:

- FAS をインストールおよび構成する方法については、「インストールと構成」を参照してください。
- 詳しくは、「Azure AD の統合」を参照してください。

ADFS の展開

November 9, 2022

はじめに

このドキュメントでは、Citrix 環境を Microsoft ADFS と統合する方法について説明します。

ADFS は、多くの組織で単一の認証ポイントが必要な Web サイトへのセキュアなユーザーアクセスを管理するため に使用されます。たとえば、従業員にとって利用可能な追加のコンテンツやダウンロードがある場合、これらの場所 は、標準の Windows ログオン資格情報で保護する必要があります。

また、フェデレーション認証サービス(FAS: Federated Authentication Service) では、Citrix Gateway および Citrix StoreFront を ADFS のログオンシステムに統合できるため、企業担当者が混乱する可能性が減少します。

この展開で、Citrix Gateway は Microsoft ADFS の証明書利用者として統合されます。



注:

バックエンドリソースが Windows VDA か Linux VDA のいずれかである場合、違いはありません。

SAML の概要

SAML (Security Assertion Markup Language: セキュリティアサーションマークアップランゲージ)は、シン プルな「ログオンページへのリダイレクト」を実現する、Web ブラウザーのログオンシステムです。構成には次の項 目が含まれます。

リダイレクト URL [シングルサインオンサービス URL]

ユーザー認証の必要があることを Citrix Gateway が検出すると、NetScaler はユーザーが使用する Web ブラウザ ーに、ADFS サーバー上の SAML ログオン Web ページに HTTP POST を実行するよう指示します。この URL は通 常、次の形式のhttps://アドレスです: https://adfs.mycompany.com/adfs/ls。

この Web ページの POST には、ログオン完了時に ADFS がユーザーを返す「リターンアドレス」などの情報も含ま れます。

識別子 [発行者名/EntityID]

Entityld は、Citrix Gateway が ADFS に送信する POST データに含まれる一意の識別子です。Entityld は ADFS に、ユーザーがどのサービスにログオンしようとしているかを知らせ、必要に応じてさまざまな認証ポリシーが適用 されるようにします。発行されると、SAML 認証 XML は、Entityld の識別したサービスへのログオンのみに使用さ れます。

通常、EntityID は Citrix Gateway サーバーのログオンページの URL ですが、一般的には、Citrix Gateway および ADFS から認められればどのような URL も使用できます(例: https://ns.mycompany.com/ application/logonpage)。

リターンアドレス [応答 **URL**]

認証に成功すると、ADFS はユーザーの Web ブラウザーに、EntityID で構成された応答 URL の1つに、SAML 認証 XML を POST し返すよう指示します。この URL は、通常は元の Citrix Gateway サーバー上での次の形式 のhttps://アドレスです: https://ns.mycompany.com/cgi/samlauth。

構成された応答 URL アドレスが複数ある場合、Citrix Gateway は ADFS への元の POST 内にある 1 つを選択でき ます。

署名証明書 [IDP 証明書]

ADFS は秘密キーを使用して、SAML 認証 XML BLOB に暗号で署名します。この署名を検証するには、Citrix Gateway を構成し、証明書ファイルに含まれる公開キーを使用して、これらの署名を確認する必要があります。証 明書ファイルは、通常、ADFS サーバーから取得されるテキストファイルです。

シングルサインアウト URL [シングルログアウト URL]

ADFS および Citrix Gateway は、「中央ログアウト」システムをサポートしています。これは Citrix Gateway がポ ーリングすることがある URL であり、SAML 認証 XML BLOB が現在ログオン中のセッションをまだ示しているこ とを確認します。 これは、構成する必要がないオプション機能です。この URL は通常、次の形式のhttps://アドレスです: https://adfs.mycompany.com/adfs/logout。(シングルログオン URL と同じ場合があることに 注意してください。)

構成

セクション「Citrix Gateway の展開」では、Citrix Gateway をセットアップし、標準的な LDAP 認証オプション を処理する方法について説明します。これが正常に完了すると、SAML 認証を許可する Citrix Gateway で、新しい 認証ポリシーを作成することができます。その後、Citrix Gateway ウィザードで使用されたデフォルトの LDAP ポ リシーを置き換えることができます。

NetScaler > 1	Scaler > NetScaler Gateway > Policies > Authentication > SAML > Policies						8	
Policies	Servers							
Add	Edit	Delete	Show Bindings	Primary VPN Global Bindings			Searc	h -
Name			Expression		Request Server			
StoreFrontSAML	•		NS_TRUE		AzureAd			

SAML ポリシーの記入

ADFS 管理コンソールから前に取得した情報を使用して、新しい SAML IdP サーバーを構成します。このポリシーが 適用されると、Citrix Gateway はログオンのためにユーザーを ADFS-signed にリダイレクトし、ADFS の署名し た SAML 認証トークンを代わりに受け取ります。

Create Authentication SAML Server	5
Create Authentication SAML Server	Two Factor
Name*	O ON () OFF
AzureAd	Assertion Consumer Service Index
Authentication Tune	255
SAML	Attribute Consuming Service Index
IDP Certificate Name*	255
AzureADSAML 🖌 +	Requested Authentication Context*
Redirect URL*	
29f-4c20-9826-14d5e484c62e/saml2	EAdri
Single Logout URL	Authentication Class Types
29f-4c20-9826-14d5e484c62e/saml2	InternetProtocol InternetProtocolPassword
User Field	Signature Algorithm*
userprincipalname	C RSA-SHA1 @ RSA-SHA256
Signing Certificate Name	
~	Digest Method"
Issuer Name	O SHA1 ♥ SHA256
https://ns.citrixsamldemo.net/Citrix/s	Send Thumbprint
Reject Uprigned Assertion*	Enforce Username
	Attribute 3 Attri
Default Authentication Group	Attribute 5 Attri
Skew Time(mins)	Attribute 7 Attri
5	

関連情報

- FAS のインストールと構成については、「インストールと構成」を参照してください。
- 一般的な FAS の展開については、「展開アーキテクチャ」を参照してください。
- 具体的な手順については、「詳細な構成」を参照してください。

Azure AD の統合

November 9, 2021

はじめに

このドキュメントでは、Citrix 環境を Windows 10 Azure AD 機能と統合する方法について説明します。Windows 10 が導入した Azure AD は、ドメイン参加の新しいモデルです。これを利用すれば、管理とシングルサインオンの目 的で、ローミングラップトップを、インターネット上で企業ドメインに参加させることができます。

このドキュメントで例として示した展開では、新規ユーザーの Windows 10 ラップトップに会社のメールアドレス と登録コードが提供されるシステムを説明しています。ユーザーは [設定] パネルの [システム] > [バージョン情 報] > [Azure AD に参加] から、このコードにアクセスします。

← Settings			- 🗆 ×
🐼 SYSTEM			Find a setting P
Display	Î	PC	Î
Notifications & actions		PC name	vda-win10
Apps & features		Rename PC	
Multitasking		Organization	WORK
Tablet mode		Join a domain	
Power & sleep		Join Azure AD	
Storage		Edition	Windows 10 Enterprise
Offline maps		Product ID	00329-00000-00003-AA066
Default apps		Processor	Intel(R) Xeon(R) CPU E5-1650 0 @ 3.20GHz 3.19 GHz
		Installed RAM	2.00 GB
About		System type	64-bit operating system, x64-based processor
		Pen and touch	No pen or touch input is available for this display
	~	Change product l	ev or upgrade your edition of Windows

ラップトップが登録されると、Microsoft Edge の Web ブラウザーは、Azure SaaS アプリケーションの Web ページから、会社の Web サイトや Citrix の公開アプリケーション、および Office 365 などの Azure アプリケーション に自動的にサインオンします。

\Box Access Panel Applicatior $ imes$ +		_		×
\leftarrow \rightarrow \circlearrowright \land account.activedirectory.windowsazure.com/a	=		٩	
Microsoft Azure			ge	orge@ ^
applications profile				
citrix				
AzureStoreFront				
©2016 Microsoft Legal Privacy				, v

アーキテクチャ

このアーキテクチャでは、Azure AD や Office 365 などの最新クラウドテクノロジとの統合により、従来の企業ネットワークが Azure 内に完全に複製されます。すべてのエンドユーザーがリモートワーカーと見なされ、社内イントラネット上にはエンドユーザーが存在しないというコンセプトです。

Azure AD Connect の同期サービスが、インターネット上で Azure への橋渡しとして機能するため、既存のオンプ レミスシステムを持つ企業はこのモデルを適用することができます。



セキュアな接続やシングルサインオンといえば、従来はファイアウォールで保護された LAN や、Kerberos 認証およ び NTLM 認証でしたが、このアーキテクチャでは、Azure への TLS 接続および SAML がこれらに取って代わります。 Azure アプリケーションの Azure AD への参加により、新しいサービスが生み出されています。Active Directory を必要とする既存のアプリケーション(SQL Server データベースなど)は、Azure クラウドサービスの laaS 部分 にある、標準的な Active Directory サーバーの仮想マシンを使用して実行できます。

ユーザーが従来のアプリケーションを起動すると、Citrix Virtual Apps and Desktops の公開アプリケーションを 使用してアクセスします。Microsoft Edge のシングルサインオン機能を使用して、ユーザーの [**Azure** アプリケー ション] ページからさまざまな種類のアプリケーションが照合されます。また、Microsoft は、Azure アプリケーシ ョンの一覧表示と起動ができる Android および iOS アプリを提供しています。

DNS ゾーンの作成

Azure AD では、管理者がパブリック DNS アドレスを登録し、ドメイン名サフィックスの委任ゾーンを管理する必要 があります。これを実行するために、管理者は Azure DNS ゾーン機能を使用できます。

この例では、DNS ゾーン名 citrixsamldemo.net を使用します。

DNS zone - P CONS zone - P Settings Record s	REVIEW st Delete R	ව efresh		*	×
Essentials ^			89.	\bigcirc	
Resource group citrixsamldemo Subscription name Visual Studio Prof Subscription ID df22436f-d4f9-46	fessional with M ae-be7b-6479cc	SDN daeefca	Name server 1 ns1-01.azure-dns.com. Name server 2 ns2-01.azure-dns.net. Name server 3 ns3-01.azure-dns.org. Name server 4 ns4-01.azure-dns.info.		
			All settin	ngs 🔿	•
	sets TYPE	ττι	VALUE		
0	NS	172800	ns1-01.azure-dns.com. ns2-01.azure-dns.net. ns3-01.azure-dns.org. ns4-01.azure-dns.info.		-
Ø	SOA	3600	Email: azuredns-hostmaster.microsoft Host: ns1-01.azure-dns.com. Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300		
fs	CNAME	3600	adfs-citrixsamldemo.westeurope.cloud		

コンソールに Azure DNS ネームサーバーの名前が表示されます。これらは、ゾーンの DNS 登録の NS エントリで 参照する必要があります(例: citrixsamldemo.net. NS n1-01.azure-dns.com)。 Azure で実行される仮想マシンへの参照を追加する場合は、CNAME ポインターを、Azure が管理する仮想マシンの DNS レコードに使用するのが最も簡単です。仮想マシンの IP アドレスが変更されている場合は、DNS ゾーンファイ ルを手動で更新する必要はありません。

内部および外部の DNS アドレスサフィックスは、この展開に一致します。ドメインは citrixsamldemo.net で、ス プリット DNS(内部で 10.0.0.*)を使用します。

Web アプリケーションプロキシサーバーを参照する、「fs.citrixsamldemo.net」エントリを追加します。これがこ のゾーンのフェデレーションサービスです。

クラウドサービスの作成

この例では、Azure で実行される ADFS サーバーが設置された AD 環境を含む、Citrix 環境を構成します。クラウド サービスを作成し、「citrixsamldemo」と名づけます。

NEW				×
	S WEB APP	UUICK CREATE	URL citrixsamldemo	
x		CUSTOM CREATE	.cloudapp.net REGION OR AFFINITY GROUP	
¢°۰	MOBILE SERVICE		West Europe	
\odot				
	BATCH SERVICE			

Windows 仮想マシンの作成

クラウドサービスで実行される Windows 仮想マシンを5台作成します。

- ドメインコントローラー (domaincontrol)
- Azure Connect ADFS $\forall n (adfs)$
- ADFS Web アクセスプロキシ(ドメインに参加していない Web アプリケーションプロキシ)
- ・ Citrix Virtual Apps and Desktops の Delivery Controller
- Citrix Virtual Apps and Desktops Virtual Delivery Agent (VDA)



ドメインコントローラー

- DNS サーバーおよび Active Directory ドメインサービスの役割を追加し、標準的な Active Directory 展開を作成します(この例では、citrixsamldemo.net)。ドメインの昇格が完了したら、Active Directory 証明書サービスの役割を追加します。
- テスト用に通常のユーザーアカウントを作成します(例: George@citrixsamldemo.net)。
- このサーバーでは内部 DNS が実行されるため、すべてのサーバーは DNS 解決にこのサーバーを参照する必要があります。これは、[Azure DNS 設定]ページで行います。(詳しくは、このドキュメントの付録を参照してください。)

ADFS コントローラーと Web アプリケーションプロキシサーバー

- ADFS サーバーを citrixsamldemo ドメインに参加させます。Web アプリケーションプロキシサーバーは、 分離されたワークグループにとどまる必要があるため、AD DNS で DNS アドレスを手動で登録します。
- これらのサーバーで Enable-PSRemoting Force コマンドレットを実行して、Azure AD Connect ツー ルからファイアウォール経由の PS リモーティングを有効にします。

Citrix Virtual Desktops \mathcal{O} Delivery Controller \succeq VDA

 Citrix Virtual Apps または Citrix Virtual Desktops の Delivery Controller と VDA を、citrixsamldemo に参加した残り 2 台の Windows サーバーにインストールします。

内部 DNS の構成

ドメインコントローラーのインストール後に DNS サーバーを構成し、citrixsamldemo.net の内部ビューを処理 し、外部 DNS サーバーに対してフォワーダーとして機能するように設定します(例:8.8.8.8)。

Å	DNS M	anager		 x
File Action View Help				
🗢 🔿 🙍 📰 🖾 😽 🛽				
DNS DOMAINCONTROL DOMAINCONTRO	Name msdcs sites tcp udp DomainDnsZones ForestDnsZones (same as parent folder) (same as parent folder) (same as parent folder) domaincontrol fs wap enterpriseregistration	Type Start of Authority (SOA) Name Server (NS) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A)	[24], domaincontrol. domaincontrol. 10.0.0.12 10.0.0.13 10.0.0.13 10.0.0.13 10.0.0.14 10.0.0.13	static static 5/13/201 5/13/201 static static static static

静的なレコードを追加します。

- wap.citrixsamldemo.net [Web アプリケーションプロキシの仮想マシンはドメインに参加しません]
- fs.citrixsamldemo.net [内部フェデレーションサーバーのアドレス]

• enterpriseregistration.citrixsaml.net [fs.citrixsamldemo.net と同じ]

Azure で実行されるすべての仮想マシンは、この DNS サーバーのみを使用するように構成する必要があります。これは、ネットワークインターフェイス GUI から実行できます。

netscaler530 Network interface to m Settings Delete	* _ = ×	– Settings netscalers30		DNS servers netscaler530 Save Discard
Essentials A Resource group chrissamldemo Location West Europe Subscription name Visual Studio Professional with MSDN Subscription ID df22436f-d4f9-46ae-be7b-6479cdaeefca Netscaler Attached to Netscaler	de PR ♥		> > >	DNS servers Azure DNS Custom DNS Primary DNS server 10.0.05 Secondary DNS server

デフォルトでは、内部 IP(10.0.0.9)アドレスは動的に割り当てられます。IP アドレスの設定を使用して、IP アド レスを永続的に割り当てることができます。これは、Web アプリケーションプロキシサーバーとドメインコントロー ラーで実行する必要があります。

外部 DNS アドレスの構成

仮想マシン実行時に、Azure は、仮想マシンに割り当てられた現在のパブリック IP アドレスを指す自身の DNS ゾー ンサーバーを維持します。Azure はデフォルトで各仮想マシンの起動時に IP アドレスを割り当てるため、この便利 な機能を有効にします。

אר איז	DomainControl8733 Public IF address Settings Dissociate Delete		* _ 🗆 ×	– Settings DomainControl8733	- = ×	_ Configuration DomanControll??3 Free Decard
Computer page	Essentials ^	ID addrare	CL 18 ()			Assignment Dynamic Static
DomainControl	citrixsamldemo	13.94.252.54		SUPPORT + TROUBLESHOOTING		IP address @
Operating system Windows	Location West Europe	DNS name		Audit logs	>	13.94.252.54
Size Standard DS1 v2 (1 core, 3.5 GB memory)	Subscription name Visual Studio Professional with MSDN	Associated to domaincontrol824		😩 New support request	>	Idle timeout (minutes) 🛛
Public IP address/DNS name label 13.94.252.54/ <none> Virtual network/subnet</none>	Subscription ID df22436f-d4f9-46ae-be7b-6479cdaeefca	Virtual machine DomainControl	All cottings and	GENERAL		DNS name label (optional)
citrixsamldemo/default			An seconds -	Properties	>	domaincontrol-citrixsamIdemo .westeurope.cloudapp.azure.com
All settings → Add tiles				🚔 Configuration	>	
\odot				RESOURCE MANAGEMENT		
Edit				🥏 Tags	>	
				A Locks	>	
				📲 Users	>	
				🖳 Export template	>	

この例では、DNS アドレス domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com を、ドメイ ンコントローラーに割り当てています。 リモート構成の完了時にパブリック IP アドレスを有効にする必要があるのは、Web アプリケーションプロキシと Citrix Gateway 仮想マシンだけである点に注意してください。(構成では、環境への RDP アクセスにパブリック IP アドレスが使用されます)。

セキュリティグループの構成

Azure クラウドは、セキュリティグループを使用して、インターネットから仮想マシンへの TCP および UDP アクセ スのファイアウォールルールを管理します。デフォルトでは、すべての仮想マシンで RDP アクセスが許可されます。 また、Citrix Gateway および Web アプリケーションプロキシサーバーでは、ポート 443 で TLS を許可する必要が あります。

_ E						
Settings netscaler530		Network security group	Netscaler Network security group		Settings Netscaler	
		Edit	🔅 🛅 Settings Delete			
		Network security group	Essentials 🔨	A X 🖉		
SUPPORT + TROUBLESHOOTING		Netscaler	Resource group citrixsamIdemo	Security rules 1 inbound, 0 outbound	SUPPORT + TROUBLESHOOTING	
Audit logs	>		Location West Europe	Associated with 0 subnets, 2 network interfaces	Audit logs	>
New support request	>		Subscription name Visual Studio Professional with MSDN		New support request	>
GENERAL			Subscription ID df22436f-d4f9-46ae-be7b-6479cdaeefca	10 anti-car 20	GENERAL	
Properties	>			Air settings -	Properties	>
IP addresses	>				📥 Inbound security rules	>
DNS servers	>				🚊 Outbound security rules	>
Network security group	>				Network interfaces	>
RESOURCE MANAGEMENT					<-> Subnets	>

ADFS 証明書の作成

Microsoft 証明機関で **Web** サーバー証明書テンプレートを有効にします。これにより、PFX ファイルにエクスポート(秘密キーも含む)できる、カスタム DNS アドレスを持つ証明書を作成できます。PFX ファイルを優先オプションにするには、この証明書を ADFS と Web アプリケーションプロキシサーバーの両方にインストールする必要があります。

次のサブジェクト名を使用して、Web サーバー証明書を発行します。

- Commonname:
 - adfs.citrixsamldemo.net [コンピューター名]
- SubjectAltname:
 - *.citrixsamldemo.net [ゾーン名]
 - fs.citrixsamldemo. net [DNS のエントリ]
 - enterpriseregistration.citrixsamldemo.net

Console1 - [Con:	Certificate Properties	D X
 File Action V File Action V Certificate Enrollment Console Root Certificates (Li Personal Certific Personal Certificate Enrollment Personal Computer Pointermedia Trusted Pa Trusted Pa Client Aution Remote Da Remote Da Remote Da Smart Cara Application point Validity period Show all templates	Subject General Extensions Private Key Certification Authority The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate Subject of certificate Subject of certificate The user or computer that is receiving the certificate Subject name: Add > Type: Add > Value: < Remove	

パスワードで保護された秘密キーを含め、証明書を PFX ファイルにエクスポートします。

Azure AD のセットアップ

このセクションでは、新しい Azure AD インスタンスをセットアップして、Windows 10 を Azure AD に参加させ るために使用できるユーザー ID を作成する方法について説明します。

新しいディレクトリの作成

Azure クラシックポータルにログオンして、新しいディレクトリを作成します。

DIRECTORY ACCE	SS CONTROL NAMESPACES	MULTI-FACTOR AU	TH PROVIDERS	RIGHTS N
Add directo	ry			×
DIRECTORY 👔	-			
Create new directory	~			
NAME 🕜				
CitrixSAMLDemo				
DOMAIN NAME 🕜				
citrixsamldemo	(onmicrosoft.com	n	
COUNTRY OR REGION				
United Kingdom		~		
□ This is a B2C directory	PREVIEW			\checkmark
				\smile

完了すると、概要ページが表示されます。

USERS GROUPS APPLIC NSES	CATIONS DOMAINS DIRECTORY INTEGRATION CONFIGURE REPORTS
	Your directory is ready to use. Here are a few options to get started.
	Manage Access Develop Applications
I STAKIED	
Improve user sign	-in experience
Add a custom domain so tha	at your users can sign in with familiar user names. For example, if your organization owns
'contoso.com', users can sign	n in Azure AD with user names such as 'joe@contoso.com'.
Improve user sign	-in experience
Add a custom domain so tha	at your users can sign in with familiar user names. For example, if your organization owns
'contoso.com', users can sign	n in Azure AD with user names such as 'joe@contoso.com'.
Add d	Iomain
Improve user sign	-in experience
Add a custom domain so tha	at your users can sign in with familiar user names. For example, if your organization owns
'contoso.com', users can sig	n in Azure AD with user names such as 'joe@contoso.com'.
Add d	Iomain
Integrate with you	r local directory
Improve user sign	-in experience
Add a custom domain so tha	at your users can sign in with familiar user names. For example, if your organization owns
'contoso.com', users can sign	in Azure AD with user names such as 'joe@contoso.com'.
Add d	
Integrate with you	Iomain
Use the same user accounts	Ir local directory
Download Azure AD Connect	and groups in the cloud that you already use on premises.
Inprove user sign	-in experience
Add a custom domain so tha	at your users can sign in with familiar user names. For example, if your organization owns
'contoso.com', users can sign	n in Azure AD with user names such as 'joe@contoso.com'.
Add c	Iomain
Integrate with you	Ir local directory
Use the same user accounts a	and groups in the cloud that you already use on premises.
Download Azure AD Connect	at
Get Azure AD Press	mium
Improve user sign	-in experience
Add a custom domain so tha	at your users can sign in with familiar user names. For example, if your organization owns
'contoso.com', users can sign	in Azure AD with user names such as 'joe@contoso.com'.
Add c	Iomain
Integrate with you	ar local directory
Use the same user accounts a	and groups in the cloud that you already use on premises.
Download Azure AD Connect	at
Get Azure AD Prete	mium
Improve access management	t experiences for end users and administrators, including self service password reset,
group management, sign in the	customization, and reporting.

グローバル管理者ユーザー(**AzureAdmin**)の作成

Azure でグローバル管理者を作成し(この例ではAzureAdmin@citrixsamldemo.onmicrosoft. com)、この新しいアカウントでログオンしてパスワードを設定します。

ADD USER		×
user profile		
FIRST NAME	LAST NAME	1
Azure	Admin	
DISPLAY NAME		
Azure Admin		
ALTERNATE EMAIL ADDRESS		
MULTI-FACTOR AUTHENTICATION		
Enable Multi-Factor Authentication		
Enable Multi-Factor Authentication		

Azure AD を使用したドメインの登録

デフォルトでは、ユーザーは次の形式のメールアドレスで識別されます: <user.name>@<company>. onmicrosoft.com。

このアドレスは追加の構成なしで機能しますが、エンドユーザーのメールアカウントと一致する、次の標準形式のメールアドレスをお勧めします: <user.name>@<company>.com。

[ドメインの追加]で、ユーザーの会社のドメインからのリダイレクトを構成します。この例では、citrixsamldemo .netを使用します。

ADFS をシングルサインオンにセットアップしている場合は、チェックボックスにチェックマークを入れます。

Specify a domain name	
Enter the name of a domain that your organization owns. 💿	
DOMAIN NAME	
citrixsamldemo.net	
🗹 I plan to configure this domain for single sign-on with my local Active Directory. 🐨	
add	

Azure AD Connect のインストール

Azure AD 構成 GUI の手順 2 により、Azure AD Connect の Microsoft ダウンロードページにリダイレクトされ ます。これを ADFS 仮想マシンにインストールします。[簡単設定]ではなく [カスタムインストール]を使用し、 ADFS のオプションが利用できるようにします。

Interest Area Active D	irectory Connect	-	×
Welcome Express Settings Required Components User Sign-In	Install required components Are existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed. Installing Visual C++ 2013 Redistributable Optional configuration Specify a custom installation location Use an existing SQL Server Use an existing service account Specify custom sync groups		
	Previous Install		

[AD FS とのフェデレーション] シングルサインオンオプションを選択します。



あらかじめ作成した管理アカウントで Azure に接続します。
I wicrosoft Azure Active D	irectory Connect		_ ×
Welcome Express Settings Required Components User Sign-In Connect to Azure AD	Connect to Azure AD Enter your Azure AD credentials: ? USERNAME AzureAdmin@citrixsamIdemo.onmicrosoft.com		
Sync Connect Directories Azure AD sign-in Domain/OU Filtering Identifying users Filtering Optional Features AD FS Farm Azure AD Domain Configure Verify	PASSWORD		
		Previous	Next

内部 AD フォレストを選択します。

I Microsoft Azure Active D	irectory Connect	_ ×
Welcome Express Settings Required Components User Sign-In Connect to Azure AD Sync Connect Directories Domain/OU Filtering Identifying users Filtering Optional Features AD FS Farm Azure AD Domain Configure Verify	Connection information for your on-premises directories or forests: Inter connection information for your on-premises directories or forests: Inter CONT TVE IntrixsamIdemo.cloudapp.net IntrixsamIdemo.cloudapp.net	Remove
	Previous	Next

Active Directory の従来のオブジェクトをすべて Azure AD と同期します。

Alicrosoft Azure Active D	Directory Connect	×
Welcome Express Settings Required Components User Sign-In Connect to Azure AD Sync Connect Directories	Domain and OU filtering Directory: citrixsamIdemo.cloudapp.net Sync all domains and OUs Sync selected domains and OUs CitrixsamIdemo.cloudapp.net Builtin Computers	
Identifying users Filtering Optional Features AD FS Farm Azure AD Domain Configure Verify	 Computers Computers Domain Controllers ForeignSecurityPrincipals Infrastructure LostAndFound Managed Service Accounts MTDS Quotas Program Data System Users Configuration 	
	Previous Next	

ディレクトリ構造がシンプルな場合は、ユーザー名の一意性に依存して、ログオンするユーザーを識別することがで きます。

Interest Area Active D	Directory Connect _ X
Welcome Express Settings Required Components User Sign-In Connect to Azure AD Sync Connect Directories Domain/OU Filtering Optional Features AD FS Farm Azure AD Domain Configure Verify	Uniquely identifying your users Select how users should be identified in your on-premises directories. Isers are represented only once across all directories. User identifies exist across multiple directories. Match using: Mail attribute ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes SAMAccountName and MailNickName attributes A specific attribute CUSTOM ATTRIBUTE VISTOM ATTRIBUTE ObjectGUID VISTE RNINCIPAL NAME ?
	Previous Next

デフォルトのフィルタリングオプションを使用するか、あるいはユーザーとデバイスを特定のグループセットに制限 します。

Alicrosoft Azure Active D	Icrosoft Azure Active Directory Connect _ X							
Welcome Express Settings Required Components User Sign-In Connect to Azure AD Sync Connect Directories Domain/OU Filtering Identifying users Filtering Optional Features AD FS Farm Azure AD Domain Configure Verify	Filter users and For a pilot deployment, specify a Synchronize all users and devi Synchronize selected FOREST citrixsamIdemo.cloudapp.net	d devices group containing your users and devices that will be ices GROUP Enter a name or DN of a group	synchronized.					
		Previous	Next					

必要に応じて、Azure AD パスワードを Active Directory と同期することができます。これは、通常、ADFS ベースの認証では必要ありません。



証明書の PFX ファイルを AD FS で使用するように選択します。DNS 名として fs.citrixsamldemo.net を指定します。

🚸 Microsoft Azure Active D	irectory Connect _ X
Welcome Express Settings Required Components	AD FS Farm
User Sign-In Connect to Azure AD	Use an existing Windows Server 2012 R2 AD FS farm
Connect Directories Domain/OU Filtering Identifying users Filtering	Specify the SSL certificate used to secure the communication between clients and AD FS. Provide a PFX Certificate File Use a Certificate installed on the Federation Machines CERTIFICATE FILE CERTIFICATE FILE
Optional Features	C:\Users\Fred.CITRIXSAMLDEMO\Desktop\adfs.pfx Browse
Federation Servers Proxy Servers Credentials	SUBJECT NAME SUBJECT NAME PREFIX *,titrixsamIdemo.net fs
Service account Azure AD Domain Configure Verify	https://fs.citrixsamldemo.net
	Previous Next

プロキシサーバーの選択を求める画面が表示されたら、wap.citrixsamldemo.net サーバーのアドレスを入 力します。Azure AD Connect が構成できるよう、Web アプリケーションプロキシサーバーの管理者として Enable-PSRemoting – Force コマンドレットを実行する必要がある場合があります。

🚸 Microsoft Azure Active D	irectory Connect _ X
Welcome Express Settings Required Components User Sign-In Connect to Azure AD Sync Connect Directories Domain/OU Filtering Identifying users Filtering Optional Features AD FS Farm Federation Servers	Web application proxy servers specify where to install web application proxy. SERVER Type a server name or IP address Add Browse SELECTED SERVERS
Proxy Servers Credentials Service account Azure AD Domain Configure Verify	
	Previous Next

注:

Remote PowerShell の信頼性の問題でこの手順に失敗した場合は、Web アプリケーションプロキシサーバーをドメインに参加させてみてください。

ウィザードの残りの手順については、標準の管理者パスワードを使用して、ADFS のサービスアカウントを作成します。Azure AD Connect により、DNS ゾーンの所有権の検証が求められます。



TXT レコードと MX レコードを Azure の DNS アドレスレコードに追加します。

♀ Search reco.	rd sets			
NAME	TYPE	TTL	VALUE	
ø	NS	172800	ns1-01.azure-dns.com. ns2-01.azure-dns.net. ns3-01.azure-dns.org. ns4-01.azure-dns.info.	
ē	SOA	3600	Email: azuredns-hostmaster.microsoft Host: ns1-01.azure-dns.com, Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300	
ø	TXT	3600	ms70102213	
fs	CNAME	3600	adfs-citrixsamldemo.westeurope.cloud	

Azure 管理コンソールで [検証]をクリックします。

CitrixSamlDemo

62	USERS	GROUPS	APPLICATIONS	DOMAINS D	RECTORY INTEGRATION	CONF	IGURE	REPORTS	LICENSES		
DC	MAIN NAME		TYPE		STATUS		SINGLE SI	GN-ON		PRIMARY DOMAIN	Q
cit	ixsamldemo.c	nmicrosoft.co	m Basic		🗸 Active		Not Availa	able		Yes	
cit	rixsamldemo.	net	Custom		🛕 Unverified		Not Conf	igured		No	

注:

この手順に失敗した場合は、Azure AD Connect を実行する前にドメインを検証します。

完了すると、外部アドレス fs.citrixsamldemo.net がポート 443 で接続されます。



Azure AD への参加の有効化

Windows 10 が Azure AD への参加を実行するよう、メールアドレスを入力すると、ADFS を指す必要がある CNAME DNS レコードの作成に DNS サフィックスが使用されます (enterpriseregistration.<*upnsuffix*>)。 この例では、fs.citrixsamldemo.netとなります。

enterpriseregistration.citrixsamldemo.net				
Туре				
CNAME				
* TTL	TTL unit			
1 🗸	Minutes	~		
Alias				
fs.citrixsamldemo.net		~		

パブリック証明機関を使用していない場合は、Windows が ADFS サーバーを信頼するよう、ADFS のルート証明書 を Windows 10 コンピューターにインストールします。あらかじめ生成された標準のユーザーアカウントを使用し て、Azure AD ドメインに参加します。

Let's get you signed in		
Work or school account		
George@citrixsamldemo.net	×	
Password		
forgot my password		
Which account should have?		
which account should I use?		
Sign in with the username and password	you use with Office 365 (or ot	her business
services from Microsoft).		
Privacy statement		
Privacy statement		
Privacy statement	Circo in	Deale
Privacy statement	Sign in	Back
Privacy statement	Sign in	Back

UPN は、ADFS ドメインコントローラーで認識される UPN と一致する必要があることに注意してください。

	×		×
			Q
fs.citrixsamldemo.net			
Sign in with your organizational account			
george@citrixsamldemo.net			
Password			
Sign in			
		@ 3.20GHz	
		ble for this	01
		Die for this	
© 2013 Microsoft		Vindows	
i an			
lion			
is is your organization			
policies might be turned on or other changes might be mad	e to your	PC.	
ration?			
ldemo.net			
ixsamldemo.net			
Cancel	Join		
		۽ پ	
	fs.citrixsamIdemo.net Sign in with your organizational account george@citrixsamIdemo.net Password Sign in e 2013 Microsoft tion f S S your organization uploicies might be turned on or other changes might be madation? monet ation? demo.net xsamIdemo.net	s.citrixsamldemo.net Sign in with your organizational account eorge@citrixsamldemo.net Password Sign in e 2013 Microsoft tion is is your organizational tion is is your organizational to policies might be turned on or other changes might be made to your ation? demo.net xamiddemo.net xamidemo.net xamidemo.net	fs.citrixsamldemo.net Sign in with your organizational account eeorge@citrixsamldemo.net Password Sign in @ 3.20GHz ased process ble for this tindowe tion is is your organization policies might be turned on or other changes might be made to your PC. ation? demo.net xsamldemo.net Lone Lone Lone Lone Lone Lone Lone Lone



メールアドレスを使用してマシンの再起動とログオンを行い、Azure AD への参加が正常に行われたことを検証しま す。ログオンすると Microsoft Edge が起動してhttp://myapps.microsoft.comに接続します。この Web サイト では、シングルサインオンが自動的に使用されます。

Citrix Virtual Apps または Citrix Virtual Desktops のインストール

通常の方法で、Citrix Virtual Apps または Citrix Virtual Desktops の ISO から、Delivery Controller および VDA 仮想マシンを Azure に直接インストールすることができます。

この例では、StoreFront は Delivery Controller と同じサーバーにインストールされています。VDA はスタンドアロ ンの Windows 2012 R2 用 RDS ワーカーとしてインストールされ、Machine Creation Services とは統合していま せん (ただしオプションで構成することができます)。作業を続行する前に、ユーザー George@citrixsamldemo.net がパスワードで認証できることを確認します。

ر المعادي	litrix Receiver ×	× A ★ ®
Citrix StoreFront		George User ▼
		Q Search Desktops
Details		
Azure		

StoreFront が ユ ー ザ ー 資 格 情 報 な し に 認 証 で き る よ う、**Set-BrokerSite** -**TrustRequestsSent-ToTheXmlServicePort \$true** PowerShell コマンドレットを Controller で実行します。

フェデレーション認証サービスのインストール

ADFS サーバーに FAS をインストールし、Delivery Controller が信頼できる StoreFront として機能するための ルールを構成します(この例では、StoreFront が Delivery Controller と同じ仮想マシンにインストールされてい るため)。「インストールと構成」を参照してください。

StoreFront の構成

Delivery Controller のコンピューター証明書を要求します。また、ポート 443 に IIS バインドを設定し、StoreFront のベースアドレスを https: に変更して、IIS および StoreFront で HTTPS が使用されるように構成します。

Change Base URL
Modify the base URL for services hosted on this deployment. For multiple server deployments, specify the load-balanced URL for the server group.
Base URL: https://ddc.citrixsamIdemo.net
OK Cancel

StoreFront で FAS サーバーが使用されるように構成し(「インストールと構成」の PowerShell スクリプトを使用 します)、Azure 内で内部テストを行います。FAS サーバーのイベントビューアーをチェックして、ログオンに FAS が使用されることを確認します。

8			Event Viewer				-		x
File Action V	iew Help								
🗢 🄿 🔁 🔂	? 🗊								
Event Viewer	Application Num	iber of events: 4,053					Actio	ins	
Custom V	Level	Date and Time	Source	Event ID	Task C	~	App	li 🔺	· ^
A Applic	() Information	5/31/2016 9:47:35 AM	Citrix.Authentication.FederatedAuthenticationService	204	None		100	Op	
Securit	Information	5/31/2016 9:47:35 AM	Citrix.Authentication.FederatedAuthenticationService	204	None		-	c.	
Setup	 Information 	5/31/2016 9:47:13 AM	Citrix.Authentication.FederatedAuthenticationService	105	None		1		
Systen	(i) Information	5/31/2016 9:46:19 AM	MSSQL\$MICROSOFT##WID	17137	Server			m	- 11
Forwar	 Information 	5/31/2016 9:45:44 AM	Citrix.Authentication.FederatedAuthenticationService	10	None			CI	
Applicatio	 Information 	5/31/2016 9:45:43 AM	Citrix.Authentication.FederatedAuthenticationService	7	None		7	Filt	
📑 Subscripti	 Information 	5/31/2016 9:44:39 AM	Citrix.Authentication.FederatedAuthenticationService	10	None			Pr.	
	1 Information	5/31/2016 9:44:39 AM	Citrix.Authentication.FederatedAuthenticationService	7	None		000		≡
	1 Information	5/31/2016 9:41:23 AM	MSSQL\$MICROSOFT##WID	17137	Server		88	fin	
	 Information 	5/31/2016 9:38:37 AM	Citrix.TrustFabric	16	None			Sa	
	(i) Information	5/31/2016 9:38:37 AM	Citrix.TrustFabric	16	None	\sim	·	Att	
	Event 204, Citrix.Au	thentication.FederatedAuth	enticationService			×		View)	•
	General Details	1					Q	Re	
	Course Course					~	?	Help I	,
	[S204] Relying [Operation: Sig	party [I (VDA\$] ac nHash] as authorized by [cessing the Logon CSP for [upn: george@ net] in ro \DDC\$].	le: [default]		=	Eve	nt 🔺	•
								Ev	
	Log Name:	Application				~	1	Att	
< III >							Rb.	Co 1	. 🖂

Citrix Gateway を使用するための StoreFront の構成

StoreFront 管理コンソールの [認証方法の管理] GUI を使用して、StoreFront が認証に Citrix Gateway を使用 するよう構成します。

Manage Authentication Methods - Store Service	
Select the methods which users will use to authenticate and access resources.	() Settings
Configure Delegated Authentication	
Specify whether StoreFront fully delegates credential validation to NetScaler Gates setting is applied when users log on with smart cards.	way. This
ок	Cancel
ourendeedon service seconds are meloded in the astanced options.	
ОК	Cancel

Citrix Gateway 認証オプションを統合するには、Secure Ticket Authority(STA)の構成および Citrix Gateway アドレスの構成を行います。

Configure Re	mote Access Settings - Store Service	
Enabling remote access allows u you enable remote access, add a	isers outside the firewall to securely access resources a NetScaler Gateway appliance.	. After
🗹 Enable Remote Access		
Select the permitted level of acc	ess to internal resources	
Allow users to access only re	sources delivered through StoreFront (No VPN tunn	el) 🚹
 Allow users to access all reso Users may require the NetSc NetScaler Gateway appliances: 	ources on the internal network (Full VPN tunnel) aler Gateway Plug-in to establish a full VPN tunnel.	0
Default appliance:	Add NetscalerGateway 👻]
	OK	Cancel

新しい Azure AD アプリケーションを StoreFront へのシングルサインオンに構成

このセクションでは、Azure AD SAML 2.0 シングルサインオン機能を使用します。現在は、Azure Active Directory プレミアムサブスクリプションが必要です。Azure AD 管理ツールで [新しいアプリケーション]を選択し、[ギャラ リーからアプリケーションを追加します]を選択します。

	Application gallery Add an application	for my o	organization to use	د م	ĸ
i.	FEATURED APPLICATIONS (17)		Add an unlisted application my	NAME	
	ALL (2626)		organization is using	StoreFront	
	BUSINESS MANAGEMENT (124)			Enter the name of an application you are	
	COLLABORATION (314)			integration options.	
	CONSTRUCTION (3)				
	CONTENT MANAGEMENT (97)				
	CRM (114)				
	DATA SERVICES (109)				
	DEVELOPER SERVICES (86)				

[カスタム] カテゴリの [私の組織で使用している、一覧にないアプリケーションを追加] を選択して、ユーザーが使 用する新しいカスタムアプリケーションを作成します。

アイコンの構成

縦横 215 ピクセルの画像を作成して[構成]ページにアップロードし、アプリケーションのアイコンとして使用しま す。

properties

APPLICATION TILE LOGO



SAML 認証の構成

アプリケーションダッシュボードの概要ページに戻り、[シングルサインオンの構成]を選択します。

storefront



この展開では、[Microsoft Azure AD のシングルサインオン] に対応する SAML 2.0 認証を使用します。

CONFIGURE SINGLE SIGN-ON

How would you like users to sign on to StoreFront?

- Microsoft Azure AD Single Sign-On
 Establish federation between Microsoft Azure AD and StoreFront
 Learn more
- Password Single Sign-On Microsoft Azure AD stores account credentials for users to sign on to StoreFront Learn more
- Existing Single Sign-On Configures Microsoft Azure AD to support single sign-on to StoreFront using Active Directory Federation Services or another third-party single sign-on provider. Learn more

[識別子] には任意の文字列を指定できます(Citrix Gateway に提供された構成と一致する必要があります)。この例 では、[応答 **URL**]が Citrix Gateway サーバーの */cgi/samlauth* になっています。

(CONFIGURE SINGLE SIGN-ON	
	Configure App Settings	
I	Enter the settings of AzureStoreFront application below. Learn more	
I	DENTIFIER O	
	https://ns.citrixsamldemo.net/Citrix/StoreFront 🥝	
F	REPLY URL O	
	https://ns.citrixsamldemo.net/cgi/samlauth 📀	

次のページには、Citrix Gateway を Azure AD の証明書利用者として構成するために使用される情報が含まれています。

CONFIGURE SINGLE SIGN-ON

Configure single sign-on at AzureStoreFront

To accept the SAML token issued by Azure Active Directory, your application will need the information below. Refer to your application's SAML documentation or source code for details.

 The following certificate will be used for federated single sign-on: Thumbprint: 8D1E02EBF7C111EDDBBD325F526053BA9626A73B Expiry: 05/31/2018 11:06:20 UTC

Download Certificate (Base 64 - most common)

Download Certificate (Raw)

Download Metadata (XML)

2. Configure the certificate and values in AzureStoreFront

ISSUER URL

https://sts.windows.net/b1aef21b-d29f-4c20-9826-14d5e484c62e/

SINGLE SIGN-ON SERVICE URL

https://login.windows.net/b1aef21b-d29f-4c20-9826-14d5e484c62e

SINGLE SIGN-OUT SERVICE URL

https://login.windows.net/b1aef21b-d29f-4c20-9826-14d5e484c62e

Confirm that you have configured single sign-on as described above. Checking this will enable the current certificate to start working for this application.

Base 64 の信頼された署名証明書をダウンロードして、サインオン URL とサインアウト URL をコピーします。これ らを Citrix Gateway の[構成]画面にペーストします。

ユーザーへのアプリケーションの割り当て

最後の手順では、アプリケーションを有効にして、ユーザーの「myapps.microsoft.com」コントロールページ にアプリケーションが表示されるようにします。これは[ユーザーとグループ]ページで行います。Azure AD Connect が同期したドメインユーザーアカウントへのアクセスを割り当てます。ほかのアカウントも使用できます が、<user>@<domain> パターンに従っていないため、明示的にマップする必要があります。

×

storefront

62	DASHBOARD	USERS AND GROUPS	ATTRIBUTES	CONFIGURE				
si	HOW All Users	~						\checkmark
	CDI AV MANJE		108 71		DEDUDTMENT	100500	METHOD	0

DISPLAY NAME	USER NAME	JOB TITLE	DEPARTMENT	ACCESS	METHOD	p
Azure Admin	AzureAdmin@citrivsaml	d		No	Unassigned	
Course Here	And Contract of the second design of the second des			No.	Unassigned	
George User	george@citrixsamidemo	J.net		NO	onassigned	
On-Premises Directory Sy	Sync_ADFS_21a7e8060dcf			No	Unassigned	

MyApps ページ

アプリケーションが構成されると、https://myapps.microsoft.comで、Azure アプリケーションのユーザー一覧 に表示されます。

\Box Access Panel Applicatior $ imes$ +		—		×
\leftarrow \rightarrow \circlearrowright $ $ \bigcirc account.activedirectory.windowsazure.com/aj \square \bigstar	=		٩	
Microsoft Azure			ge	orge@ ^
applications profile				
citrix				
AzureStoreFront				
©2016 Microsoft Legal Privacy				<u> </u>

Azure AD に参加している場合、ログオンしたユーザーは、Windows 10 により、Azure アプリケーションへのシン グルサインオンがサポートされます。アイコンをクリックすると、ブラウザーは前に構成した SAML cgi/samlauth Web ページに移動します。 シングルサインオン URL

Azure AD ダッシュボードのアプリケーションに戻ります。アプリケーションに利用できるシングルサインオン URL があることを確認します。この URL は、Web ブラウザーリンクの提供や、StoreFront に直接移動するための、ス タートメニューのショートカットの作成に使用されます。

→ View usage report
https://myapps.microsoft.com/signin/
SINGLE SIGN-ON URL
URL
PUBLISHER
APPLICATION TYPE Web application
quick glance

この URL を Web ブラウザーにペーストして、前に構成した Citrix Gateway cgi/samlauth Web ページに、Azure AD がリダイレクトするようにします。これが機能するのは、割り当てられたユーザーだけです。また、シングルサインオンが利用できるのは、Windows 10 の Azure AD に参加しているログオンセッションだけです。(そのほかのユ ーザーには、Azure AD の資格情報の入力が求められます。)

Citrix Gateway のインストールと構成

この例では、展開へのリモートアクセスに、NetScaler(現 Citrix Gateway)を実行する独立した仮想マシンを使用 します。仮想マシンは Azure ストアで購入できます。この例では、NetScaler 11.0 の「Bring your own License」 バージョンを使用しています。

Web ブラウザーのアドレスバーに内部 IP アドレスを入力し、ユーザー認証の際に指定された資格情報を使用して、 NetScaler 仮想マシンにログオンします。Azure AD 仮想マシンの nsroot ユーザーのパスワードを変更する必要が あることに注意してください。

ライセンスを追加し、各ライセンスファイルが追加されたら [再起動]を選択して、DNS リゾルバーが Microsoft ドメインコントローラーをポイントするようにします。

Citrix Virtual Apps and Desktops のインストールウィザードを実行する

この例では、SAML を使用しない、シンプルな StoreFront 統合を構成することから始めます。この展開が機能する ようになってから、SAML のログオンポリシーが追加されます。

XenApp/XenDesktop Setup Wizard

What is your deployment



Citrix Gateway および StoreFront の標準設定を選択します。Microsoft Azure での使用のため、この例ではポート 443 ではなく、ポート 4433 を構成します。あるいは、ポート転送したり、Citrix Gateway 管理 Web サイトを 再マップしたりすることもできます。

NetScaler Gateway Settings
NetScaler Gateway IP Address*
10 . 0 . 0 . 18
Port*
4433
Virtual Server Name*
ns.citrixsamldemo.net
Redirect requests from port 80 to secure port
Continue

この例では、簡単にするために、ファイルに保存された既存のサーバー証明書と秘密キーをアップロードします。

フェデレーション認証サービス 2103

Server Certificate
Certificate Format*
pem 🔽
Certificate File*
ns.citrixsamldemo.net Browse 👻
Private key is password protected
Private key password
•••••
Continue Do It Later

AD アカウント管理のためのドメインコントローラーの構成

ドメインコントローラーはアカウント解決に使用されるため、その IP アドレスをプライマリ認証方法に追加します。 ダイアログボックスの各フィールドで求められる形式に注意してください。

Primary authentication method*
Active Directory/LDAP
IP Address*
10 . 0 . 0 . 12 🗌 IPv6
Load Balancing Port*
389
Time out (seconds)*
3
Base DN*
CN=Users,DC= citrixsamIdemo ,DC
Service account*
CN=internaladmin,CN=Users,DC=
Group Extraction
Server Logon Name Attribute*
userPrincipalName
Password*
•••••
Confirm Password*
••••••
Secondary authentication method*
None
Continue

StoreFront アドレスの構成

この例では、HTTPS を使用して StoreFront が構成されているため、SSL プロトコルのオプションを選択します。

StoreFront
StoreFront FQDN*
ddc.citrixsamldemo.net
Site Path*
/Citrix/StoreWeb
Single Sign-on Domain*
citrixsamldemo. 🗙 🕜
Store Name*
/Citrix/StoreWeb
Secure Ticket Authority Server*
http://ddc.citrixsamldemo.net/sta +
StoreFront Server*
10 . 0 . 0 . 15 +
Protocol*
SSL 🗸
Port*
443
Load Balancing
Continue Cancel

Citrix Gateway 展開の検証

Citrix Gateway に接続し、ユーザー名とパスワードを使用して、認証と起動が正常に行われることを確認します。



Citrix Gateway SAML 認証サポートの有効化

StoreFront での SAML の使用は、ほかの Web サイトで SAMl を使用するのと同様です。NS_TRUE の式を使用して、新しい SAML ポリシーを追加します。

Configure Authentication SAML Policy
Name StoreFrontSAML
Authentication Type SAML
Server*
Expression*
Operators
NS_TRUE
OK Close

Azure AD から前に取得した情報を使用して、新しい SAML IdP サーバーを構成します。

Create Authentication SAML Server	Two Factor	
	O ON @ OFF	
Name*	Assertion Consumer Service Index	
AzureAd	255	
Authentication Type SAML	Attribute Consuming Service Index	
DP Certificate Name*	255	
AzureADSAML	Requested Authentication Context*	
Redirect URL*	Exact	~
29f-4c20-9826-14d5e484c62e/saml2	Authentication Class Types	
Single Logout URL	InternetProtocol	^
29f-4c20-9826-14d5e484c62e/saml2	InternetProtocolPassword	\sim
User Field	Signature Algorithm*	
userprincipalname	○ RSA-SHA1	
Signing Certificate Name	Digest Method*	
\checkmark	○ SHA1	
ssuer Name	Send Thumbprint	
https://ns.citrixsamIdemo.net/Citrix/	 Enforce Username 	
Paint Unright Arration*	Attribute 1	Attri
	Attribute 3	Attri
SAML Binding*		
POST	Attribute 5	
Default Authentication Group	Autorice 5	
	Attribute 7	Attri

エンドツーエンドシステムの検証

Azure AD に登録したアカウントを使用して、Azure AD に参加している Windows 10 デスクトップにログオンします。Microsoft Edge を起動してhttps://myapps.microsoft.comに接続します。

Web ブラウザーには、ユーザーの Azure AD アプリケーションが表示されます。



アイコンをクリックすると認証された StoreFront サーバーにリダイレクトされることを確認します。

同様に、シングルサインオン URL を使用した直接接続、および Citrix Gateway のサイトへの直接接続により、 Microsoft Azure との間でリダイレクトされることを確認します。

最後に、Azure AD に参加していないマシンも同じ URL で動作することを確認します(ただし、最初の接続時に、 Azure AD への明示的なサインオンが 1 回行われます)。

付録

Azure で仮想マシンをセットアップするときには、次の標準オプションを構成してください。

パブリック IP アドレスと DNS アドレスの入力

Azure は内部サブネット上で、すべての仮想マシンに IP アドレスを提供します(この例では 10.*.*.*)。デフォルトで は、動的に更新された DNS ラベルで参照できる、パブリック IP アドレスも提供されます。

フェデレーション認証サービス 2103

Netscaler Virtual machine Connect Start Restart	¥ × ■ Ē Stop Denter	Puetiscaler Puetisc ili address C X B Settings Dissociate Delete	* _ = ×	_ 🗆 × Settings _{Netcoder}
Sensing Connect Date Retact Essentials ^	200 Devel Computer name Netscaler Operating system Linux Size	Setting: Discost Denes Essentials: ^	P address DIS name All settings →	Filter settings SUPPORT + TROUBLESHOOTING Audit logs New support request SENERAL Properties Configuration Configuration Configuration
CPU percentage	svailable data.			RESOURCE MANAGEMENT Tags Locks Locks Solution Export template

[パブリック **IP** アドレス**/DNS** 名] ラベルの [構成] を選択します。仮想マシンのパブリック DNS アドレスを選択し ます。これは、ほかの DNS ゾーンファイルでの CNAME 参照に使用でき、IP アドレスが再割り当てされた場合も、 すべての DNS レコードが正しく仮想マシンをポイントするようにします。

Configuration
Save Discard
Assignment Dynamic Static
IP address 0 40.68.28.181
Idle timeout (minutes) 🛛 4
DNS name label (optional) 🛛
ns-citrixsamldemo 🗸
.westeurope.cloudapp.azure.com

ファイアウォールルールのセットアップ(セキュリティグループ)

クラウド上の各仮想マシンには、自動的に適用されたファイアウォールルールのセットがあり、このセットはセキュ リティグループとして知られています。セキュリティグループはパブリック IP アドレスからプライベート IP アドレ スに転送されるトラフィックを制御します。デフォルトでは、Azure はすべての仮想マシンへの RDP の転送を許可 します。また、Citrix Gateway サーバーおよび ADFS サーバーは、TLS トラフィック(443)を転送する必要があ ります。

仮想マシンの [ネットワークインターフェイス] を開いて [ネットワークセキュリティグループ] ラベルをクリック します。[受信セキュリティ規則] を構成し、適切なネットワークトラフィックを許可します。

netscaler530			Netscaler Network security group			Settings Netscaler	
🔅 🛅 Settings Delete			🔅 🛅 Settings Delete				
Essentials ^		A 18 🖉	Essentials 🔿	À	89. 🖉		
Resource group citrixsamldemo	Private IP address 10.0.0.9		Resource group citrixsamidemo	Security rules 1 inbound, 0 outbound		SUPPORT + TROUBLESHOOTING	
Location West Europe	Virtual network/subnet citrixsamldemo/default		Location West Europe	Associated with 0 subnets, 1 network interfaces		Audit logs	>
Subscription name Visual Studio Professional with MSDN	Public IP address 40.68.28.181 (Netscaler)		Subscription name Visual Studio Professional with MSDN			New support request	>
Subscription ID df22436f-d4f9-46ae-be7b-6479cdaeefca	Network security group Netscaler		Subscription ID df22436f-d4f9-46ae-be7b-6479cdaeefca			GENERAL	
	Netscaler				All settings →	Properties	>
		All settings 🔿				📥 Inbound security rules	>
						🚊 Outbound security rules	>

関連情報

- FAS のインストールと構成については、「インストールと構成」を参照してください。
- 一般的な FAS の展開については、「展開アーキテクチャ」を参照してください。
- 具体的な手順については、「詳細な構成」を参照してください。



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).

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