Unicorn ID Manager

Active Directory 証明書サービス

インストールガイド





OSSTech(株)	
作成日:	2021 年 12 月 06 日
リビジョン:	1.0

目次

1.	はじめに		1
1.	Windows	: Server 2019 での設定手順	2
1	.1 Acti	ve Directory サーバーへの証明書サービスのインストール	2
	1.1.1	証明書サービスのインストール	2
	1.1.2	Active Directory 証明書サービスの構成	4
2.	改版履歴		12

1. はじめに

本文書は、Unicorn ID Manager で Active Directory を連携する際に必要となる証明書サービスのインストール手順について説明します。

Unicorn ID Manager と連携するためには、Windows サーバーに「証明書サービス」をインストール後にマシンの再起動が必要となります。

1. Windows Server 2019 での設定手順

Windows Server 2019 への証明書サービスインストール手順を以下に示します。

1.1 Active Directory サーバーへの証明書サービスのインストール

Unicorn ID Manager から Active Directory と LDAPS 通信を行うために、Unicorn ID Manager の通信相手となる Windows サーバーに証明書サービスをインストールする必要があります。証明書サービスのインストール後は、Windows サーバーの再起動が必要となります。

1.1.1 証明書サービスのインストール

「スタート」-「管理ツール」-「サーバーマネージャー」で、サーバーマネージャーを起動し、 「役割と機能の追加」を選択します。

「開始する前に」の画面で「次へ」を押します。

🏊 サー	バーマネージャー		-	
E	◎ - サーバーマ:	ネージャー・ダッシュボード ・ ②丨 🍢 音理(M) ッ-ル() 表示(V)	へルプ(H)
III 3	「ッシュボード	サーバー マネージャーへようこそ		
1 L	🟊 役割と機能の追加ウイザード	- • ×		
	開始する前に	対象サーバー		
	 開始する前に インストールの種類 ウーパーの選択 ウーパーの役割 機能 確認 結果 	このウィザードを使用すると、役割、役割サービス、または機能をインストールできます。ドキュメントの共有や Web サイトの ホストなどの組織のコンビューティング ニーズに応じて、インストールする役割、役割サービス、または機能を決定します。 役割、役割サービス、または機能を削除するには、次の手順を実行します: 役割と機能の削除ウィザードの起動 続行する前に、次のタスクが完了していることを確認してください。 ・ 管理者アカウントに強力なパスワードが設定されている ・ 静的 IP アドレスなどのネットワークの設定が構成されている ・ Windows Update から最新のセキュリティ更新プログラムがインストールされている 前提条件が完了していることを確認する必要がある場合は、ウィザードを閉じて、それらの作業を完了してから、ウィザー ドを再度実行してください。 続行するには、[次へ] をクリックしてください。	非表	1
		□ 既定でこのページを表示しない(S) < 前へ(P) 次へ(N) > インストール(I) キャンセル		

「インストールの種類」の画面で「役割ベースまたは機能ベースのインストール」を選択し「次 へ」を押します。

「サーバーの選択」の画面で「サーバープールからサーバーを選択」を選択し「次へ」を押しま す。 「サーバーの役割」の画面で「Active Directory 証明書サービス」を選択し「機能の追加」をクリックし「次へ」を押します。

サーバーの役割の選	3.42		対象 サ−バ−
9-11-01支討の選	▶ 役割と機能の追加ウイザード	×	×
開始する前に インストールの種類 サーバーの選択 サーバーの役割	Active Directory 証明書サービス に必要な機能を追加しま すか? この機能を管理するには次のツールが必要ですが、同じサーバーにインストールす		ctory 証明書サービス (AD ぎまなアブリケーションにおいて
機能確認認識	 ↓リモートサーバー管理ツール ▲ 役割管理ツール ▲ Active Directory 証明書サービス ツール [ツール] 証明機関管理ツール 		「したり、それを管理するため」。
	✓ 管理ツールを含める(存在する場合) 機能の追加 キャンセル		
	< 前へ(P) 次へ(N) >		- (ンストール(I) キャンセル

「機能」の画面はデフォルトのまま「次へ」を押します。

「AD CS」の画面で「次へ」を押します。

🚹 役割と機能の追加ウイザード		- 🗆 X
役割サービスの運	択	对象サーバー
開始する前に インストールの種類	Active Directory 証明書サービス のインストール 役割サービス	する役割サービスを選択します 19日日
サーバーの選択 サーバーの役割 機能 AD CS 役割サービス 確認 結果	✓ 部時限間	証明機関(CA)は、証明書を発行および 管理するために使用されます。複数の CA をリンクさせることで公開キー基盤を構成 できます。
		: 前へ(P) 次へ(N) > インストール(I) キャンセル

「役割サービス」の画面で「証明機関」を選択し「次へ」を押します。

「確認」の画面で「必要に応じて対象サーバーを自動的に再起動する」にチェックをいれ、「は

い」を選択し、インストールをクリックします。

🏊 役割と機能の追加ウィザード	- D X
インストール オプシ	32の確認 対象サーバー
開始する前に	選択したサーバーに次の役割、役割サービス、または機能をインストールするには、[インストール] をクリックしてください。
インストールの種類	✓ 必要に応じて対象サーバーを自動的に再起動する
サーバーの選択 サーバーの役割	オブションの機能 (管理ツールなど)は、自動的に選択されるため、このページに表示されている可能性があります。これら のオブションの機能をインストールしない場合は、(前へ)をクリックして、チェック ボックスをオフにしてください。
機能 AD CS	Active Directory 証明書サービス 証明機関
役割サービス 確認	リモート 役割と機能の追加ウイザード × 役
結果	必要に応じて、このサーバーは通知なしで自動的に再起動されます。自動的 に再起動しますか?
	はい(Y) いいえ(N)
	構成設定のエクスポート 代替ソース バスの指定
	< 前へ(P) 次へ(N) > インストール(I) キャンセル

機能のインストールが完了したら、「閉じる」を押します。

≧ 役割と機能の追加ウィザード			-		×
インストールの進行	状況			対象サ-	-/(-
開始する前に インストールの種類	インストールの進行状況の表示 機能のインストール				
サーバーの選択 サーバーの役割	構成が必要です。	でインストールが正常	常に完了しまし	た。	
リーハーの反当 機能 AD-CS 役割サービス 確認	Active Directory 証明書サービス 対象サーバーに Active Directory 証明書サービ 対象サーバーに Active Directory 証明書サービ 証明機関 リモート サーバー管理ツール 役割管理ツール Active Directory 証明書サービス ツー 証明機関管理ツール	Rを構成するには、さらに手順を実行 Rを構成する ル	する必要があ	ります	
	このウィザードを閉じても、実行中の処理が中 ページを再度開いたりするには、コマンドパーの 構成設定のエクスポート	断されることはありません。 処理の進) [通知] をクリックし、 [タスクの詳細	行状況を表示] をクリックしま	示したり、こ ます。	.o
	< 前^	√(P) 次へ(N) >	閉じる	キャンセ	JI.

|| 1.1.2 Active Directory 証明書サービスの構成

「サーバーマネージャー」-「タスクの詳細」-「フラグ(旗のアイコン)」-「対象サーバーに Active Directory 証明書サービスを構成する」を押します。

				- 1	⊐ ×
€∋ サーバーマ	ネージャー・ ダッシュボ-	۴ 🔹 🖒 ۲	管理(M) ツ	ール(T) 表示(V)	ヘルプ(H)
 ダッシュポード ローカル サーバー 夏 オペてのサーバー 愛 AD CS AD DS	サーバー マネージャーへようこそ 1 5 <i>クイック スタート</i> (Q) 星新情報(W) 4 5	 		非表	· 示

「資格情報」の画面で、デフォルトの状態のまま「次へ」を押します。

📥 AD CS の構成	- 🗆 X
資格情報	対象サーバー miyabi220.miyabidom3.example.com
<u>資格情報</u> 役割サービス 確認 進行状況 結果	役割サービスを構成するための証明書を指定してください 次の役割サービスをインストールするには、ローカルの Administrators グループに属している必要があります: ・ スタンドアロン証明機関 ・ 近り用機関 Web 登録 ・ オンラインレスポンダー 次の役割サービスをインストールするには、Enterprise Admins グループに属している必要があります: ・ エンタープライズ証明機関 ・ 証明書の登録がリシー Web サービス ・ 証明書の登録がリシー Web サービス ・ 証明書の登録 Web サービス ・ オットワーク デバイス登録サービス 資格情報:
	AD CS サーパーの役割の詳細
	< 前へ(P) 次へ(N) > 構成(C) キャンセル

「構成する役割サービスの選択」で「証明機関」にチェックを入れ、「次へ」を押します。

淕 AD CS の構成		-	
役割サービス			対象サーバー
資格情報 役割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA 名 有効期間 証明書データベース 確認 進行状況 詰果	構成する役割サービスの選択 ☑ 証明機関 ■ 証明機関 Web 登録 ■ オンラインレスポンダー ■ ネットワークデバイス登録サービス ■ 証明書の登録 Web サービス ■ 証明書の登録ポリシー Web サービス		
	AD CS サーバーの役割の詳細		
	<前へ(P) 次へ(N) > 構成	戎(C)	キャンセル

「CA のセットアップの種類の指定してください」で、「エンタープライズ」を選択します。

📥 AD CS の構成	- 🗆 X
セットアップの種類	対象サーバー
資格情報 役割サービス セットアップの種類 CA の種類 秘密キー 暗号化 CA 名 宿効期間 証明書データベース 確認 進行状況 結果	 CAのセットアップの種類を指定してください エンターブライズ証明機関(CA)は、Active Directoryドメインサービス(AD DS)を使用して証明書の管理を簡略化できます。スタンドアロン CAでは、AD DSを使用して証明書を発行または管理することはありません。 エンターブライズ CA(E) エンターブライズ CA(E) エンターブライズ CA(はドメインメンバーである必要があり、証明書または証明書ポリシーを発行するために通常はオンラインです。 スタンドアロン CA(A) スタンドアロン CA(A) スタンドアロン CA(はワークグループまたはドメインのメンバーとなることができます。スタンドアロン CA(は AD DS を必要とせず、ネットワーク接続なし(オフライン)で使用できます。
	セットアップの種類の詳細
	<前へ(P) 次へ(N) > 構成(C) キャンセル

「CA の種類を指定してください」で、「ルート CA」を選択します。



「秘密キーの種類を指定してください」で、「新しい秘密キーを作成する」を選択します。

📥 AD CS の構成	- 🗆 X
秘密キ-	対象サーバー
資格情報 役割サービス セットアップの種類 CA の種類 秘密キー	秘密キーの種類を指定してください 証明書を生成してクライアントに発行するには、証明機関 (CA) に秘密キーが必要です。 ● 新しい秘密キーを作成する(R) 秘密キーがない場合、または新しい秘密キーを作成する場合は、このオブションを使用します。
暗号化 CA 名 有効期間 証明書データベース 確認 進行状況 結果	 既存の秘密キーを使用する(U) CA の再インストール時に、以前に発行された証明書との連続性を確保する場合は、このオプションを使用します。 証明書を選択し、関連付けられている秘密キーを使用する(C) このコンピューターに既存の証明書がある場合、または証明書をインボートしてそれに関連付けられている秘密キーを使用する場合は、このオプションを選択します。 このコンピューターの既存の秘密キーを選択する(E) 以前のインストールの秘密キーを保持している場合、または代替ソースからの秘密キーを使用する場合は、このオプションを選択します。
	秘密キーの詳細 < 前へ(P) 次へ(N) > 構成(C) キャンセル

「CA の暗号化」で、デフォルトの「RSA#Microsoft Software Key Storage Provider」「2048」、 「SHA256」を選択し、「次へ」を押します。

ADCSの構成				-		>
Aの暗号化					対象サー	-バ-
資格情報 役割サービス	暗号化オプションを指定してください					
ヤットアップの種類	暗号化プロバイダーの選択(C):		キー長(K):			
CA の種類	RSA#Microsoft Software Key Storage Provider	¥	2048			v
秘密キー		(+ 192 + T /)				
暗号化	この CA から発行された証明書の著名に使用するハッシュアルコリス	ムを選択(F	():			
CA 名	SHA256 SHA384	-				
有効期間	SHA512					
証明書データベース	SHA1					
	MD5	\sim				
進行状況	□ CA が秘密キーにアクセスするときに、管理者による操作を許可す	ວີ. (A)				
结果						
	暗号化の詳細					
	明方化の計構					

「CA 名の名前」で、「この CA の共通名」をデフォルト値、もしくは、この Active Directory に 構築された CA であることが分かる名称を設定します。

📥 AD CS の構成	– 🗆	×
CA の名前	対象サ	-バ-
資格情報 役割サービス	CA の名前を指定してください	
セットアップの種類 CA の種類	この証明機関 (CA)を識別する共通名を入力します。この名前は、CA で発行されるすべての証明書に付加 ます。識別名のサフィックスは自動的に生成されますが、変更できます。	され
秘密キー 暗号化	この CA の共通名(C):	
CA 名 有効期間	識別名のサフィックス(D):	
確認 進行状況	識別名のブレビュー(V):	
結果		
	CAの名前の詳細	
	< 前へ(P) 次へ(N) > 構成(C) キャンセ	211

「有効期間」の設定で、有効期間を設定します。有効期間が短い場合、証明書の期限切れが発生 して、Unicorn ID Manager との連携が行えなくなりますので、本システムを利用する期間を満 たす十分に長い期間を指定してください。(例: 10 年間など)

	a AD CS の構成	- □ >
 資格情報 役割サービス セットアップの憧頻 CAの憧頻 必密キー 階号化 CA の有効期間: 2031/12/07 19:44:00 この CA 証明書に対して構成する有効期間は、その CA が発行する証明書の有効期間を超えている必要か ます。 	有効期間	対象サーバー
右动期間の詳細	 資格情報 役割サービス セットアップの種類 CAの種類 秘密キー 暗号化 CA名 有効期間 証明書データベース 確認 進行状況 結果 	有効期間を指定してください この証明機関 (CA) に対して生成される証明書の有効期間を選択(V): 10 年間 CA の有効期限: 2031/12/07 19:44:00 この CA 証明書に対して構成する有効期間は、その CA が発行する証明書の有効期間を超えている必要があり ます。
FF XUTADIEUV/ST 4W		有効期間の詳細

デフォルトの状態のまま「次へ」を押します。

CA データベース 資格情報 デ 役割サービス ご セットアップの種類 ご CA の種類 ご 秘密キー 証 暗号化 ご CA 名 ご	-タベースの場所を指定してくださし		対象サ-	-バー
 資格情報 デ 役割サービス セットアップの種類 C4 の種類 C3 秘密キー 暗号化 C4 C4 	-タベースの場所を指定してください			
有効期間 証明 音デ-タベース 確認 進行状況 結果	月音データベースの場所(C): Windows¥system32¥CertLog 月音データベース ログの場所(E): Windows¥system32¥CertLog			
	アークハース(U)s+物ム 			

「構成」を押します。

📥 AD CS の構成			-		Х
確認				対象サー	-バー
資格情報 役割サービス セットアップの種類 CA の種類 秘密キー	次の役割、役割サービス、または機能 Active Directory 証明書サー 証明機関 CA の種類: 暗号化プロバイダー:	を構成するには、[構成] をクリックします。 ビス スタンドアロン ルート RSA#Microsoft Software Key Storage Provider			
暗号化 CA 名 有効期間 証明書データベース 確認 進行状況 結果	 ハッシュアルゴリズム: キー長: 管理者による対話操作を許可する: 証明書の有効期間: 識別名: 証明書データベースの場所: 証明書データベースログの場所: 	SHA256 2048 無効 2031/12/07 19:44:00 CN= C:¥Windows¥system32¥CertLog C:¥Windows¥system32¥CertLog			
		<前へ(P) 次へ(N) > 橿成(C)		キャンヤ	JU

構成に成功しましたと表示された「閉じる」を押します。

≞ AD CS の構成		-		>
結果			対象サー	-バー
資格情報	次の役割、役割サービス、または機能が構成されました:			
役割サービス	(へ) Active Directory 証明書サービス			
セットアップの種類 CA の種類 秘密キー 暗号化 CA 名 有効期間 証明書データベース 確認 進行状況 結果	証明機関 CA 機成の詳細			
	<前へ(P) 次へ(N) > 目	見じる	キャンセ	:JV

作業完了後、Windows サーバーを再起動します。

「スタート」の「電源ボタン」を押し、「再起動」を選択します。



「この PC をシャットダウンする理由に一番近い項目を選んでください」では、「その他(計画外)」 を選択し、「続行」を押します。



以上で証明書サービスのインストールは完了です。

2. 改版履歴

2023 年 12 月 06 日
 初版作成