

Unicorn ID Manager

Active Directory 証明書サービス

インストールガイド



オープンソース・ソリューション・テクノロジ(株)

作成日: 2011年 12月 19日

リビジョン: 1.0

目次

1. 証明書サービスインストール

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

1.1.1 証明書サービスのインストール.....

2. 改版履歴

1. 証明書サービスインストール

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、証明書サービスのインストール後に、マシンの再起動が必要となります。

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。

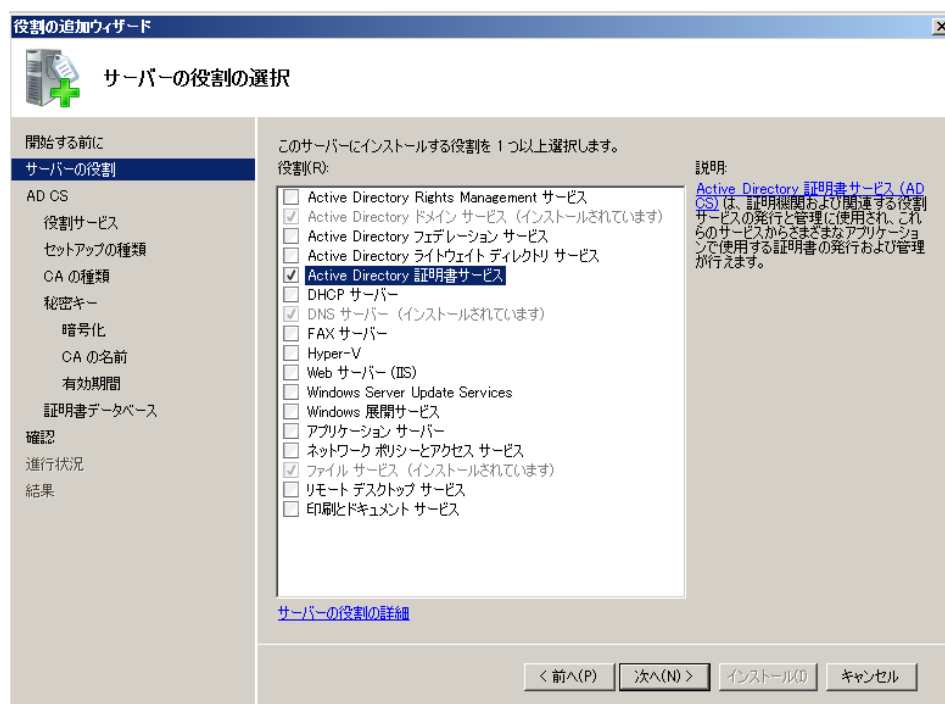
証明書サービスのインストール後には、**Windows サーバーの再起動**が必要となります。

1.1.1 証明書サービスのインストール

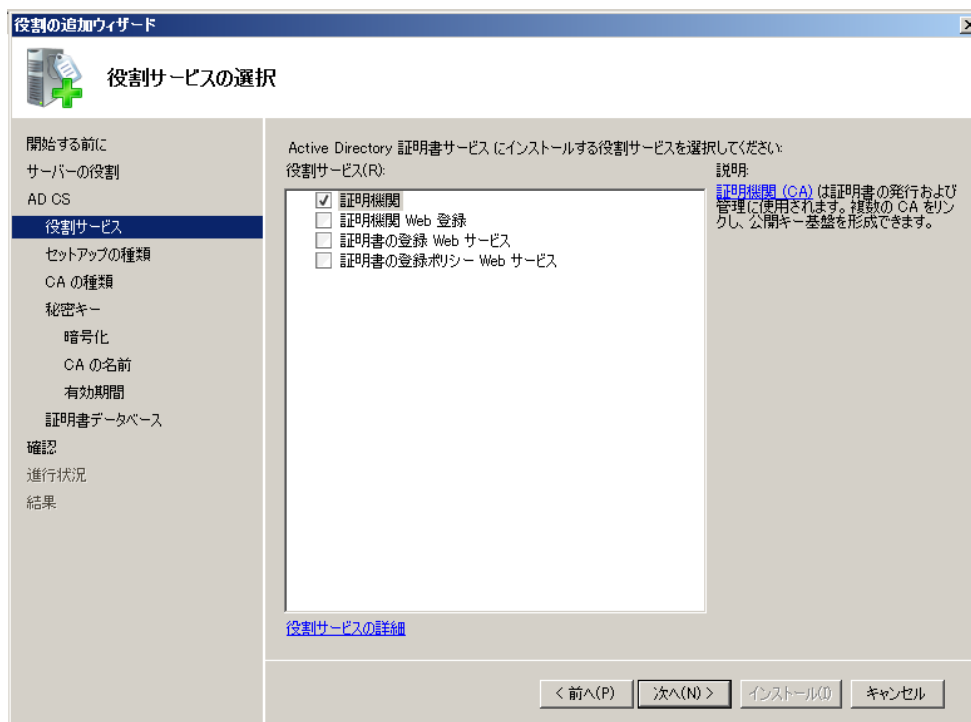
「スタート」 - 「管理ツール」 - 「サーバーマネージャー」で、サーバーマネージャーを起動し、「役割の概要」から、「役割の追加」を選択します。



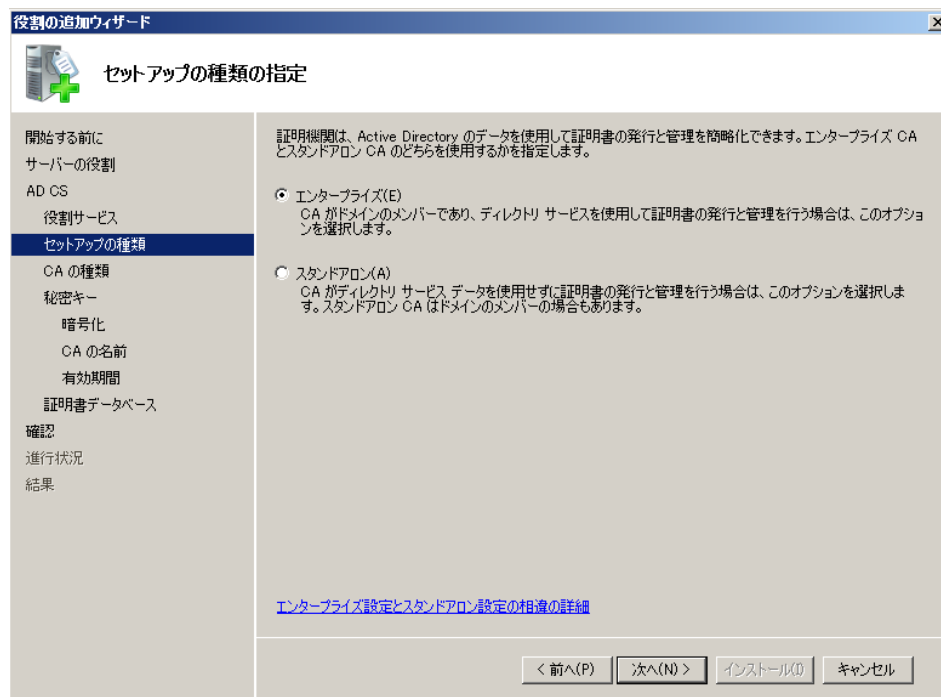
「役割の追加ウィザード」が起動しますので、「サーバーの役割の選択」画面で、「Active Directory 証明書サービス」を有効にします。



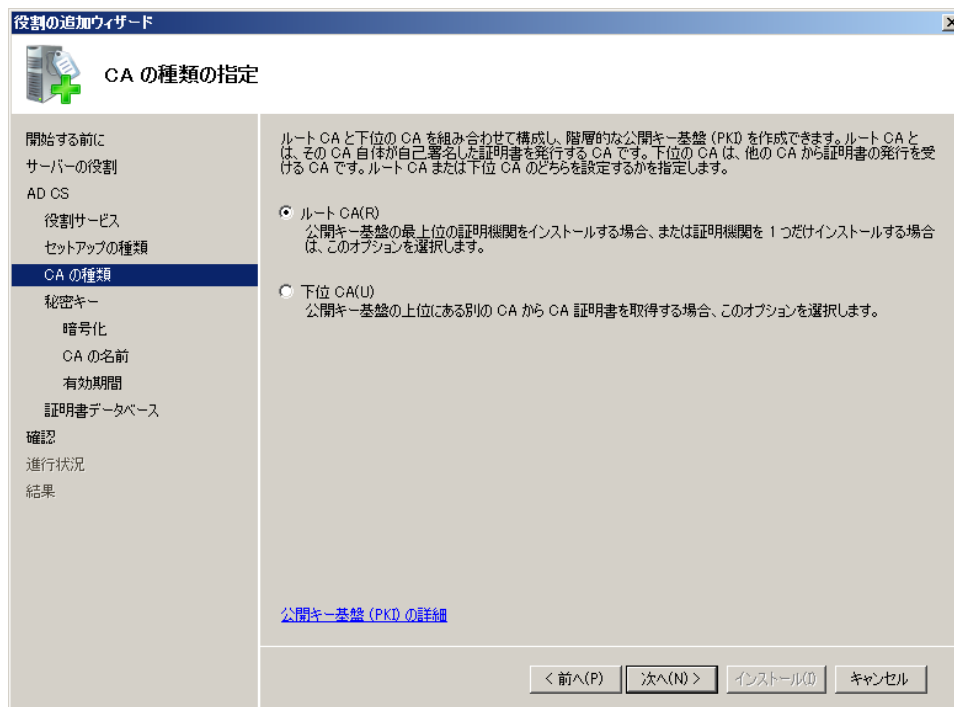
「役割サービスの選択」で、デフォルトの「証明機関」が有効になっている状態で、「次へ」を押します。



「セットアップの種類」で、「エンタープライズ」を選択します。



「役割の追加ウィザード」で、「ルート CA」を選択します。



「秘密キーの設定」で、「新しい秘密キーを作成する」を選択します。

役割の追加ウィザード

秘密キーの設定

開始する前に

サーバーの役割

AD CS

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 の名前

有効期間

証明書データベース

確認

進行状況

結果

証明書を生成してクライアントに発行するには、CA に秘密キーが必要です。新しい秘密キーを作成するか、既存の秘密キーを使用するかを指定します。

- ☒ 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してセキュリティを強化する場合は、このオプションを使用します。このオプションを選択すると、暗号化サービス プロバイダーを選択し、秘密キーのキーの長さを指定するように求められます。新しい証明書を発行するには、さらにハッシュ アルゴリズムも選択する必要があります。
- ☐ 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(G)
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ポ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から秘密キーを保持した場合、または代替ソースから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。

[公開キーと秘密キーの詳細](#)

< 前へ(P)

次へ(N) >

インストール(I)

キャンセル

「CA の暗号化を構成」で、デフォルトの「RSA#Microsoft Software Key storage Provider」「2048」、「SHA1」を選択したまま、「次へ」を押します。

役割の追加ウィザード

CA の暗号化を構成

開始する前に

サーバーの役割

AD CS

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 の名前

有効期間

証明書データベース

確認

進行状況

結果

新しい秘密キーを作成するには、発行する証明書の用途に合った適切な暗号化サービス プロバイダー、ハッシュ アルゴリズム、およびキーの長さを先に選択する必要があります。キーの長さに大きな値を選択すると、セキュリティは強固になりますが、署名処理に要する時間が長くなります。

暗号化サービス プロバイダー (CSP) を選択(C):

RSA#Microsoft Software Key Storage Provider

キーの長さ(K):
2048

この CA から発行された証明書の署名に使用するハッシュ アルゴリズムを選択(H):

SHA256

SHA384

SHA512

SHA1

☐ 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る(A)

[CA の暗号化オプションの詳細](#)

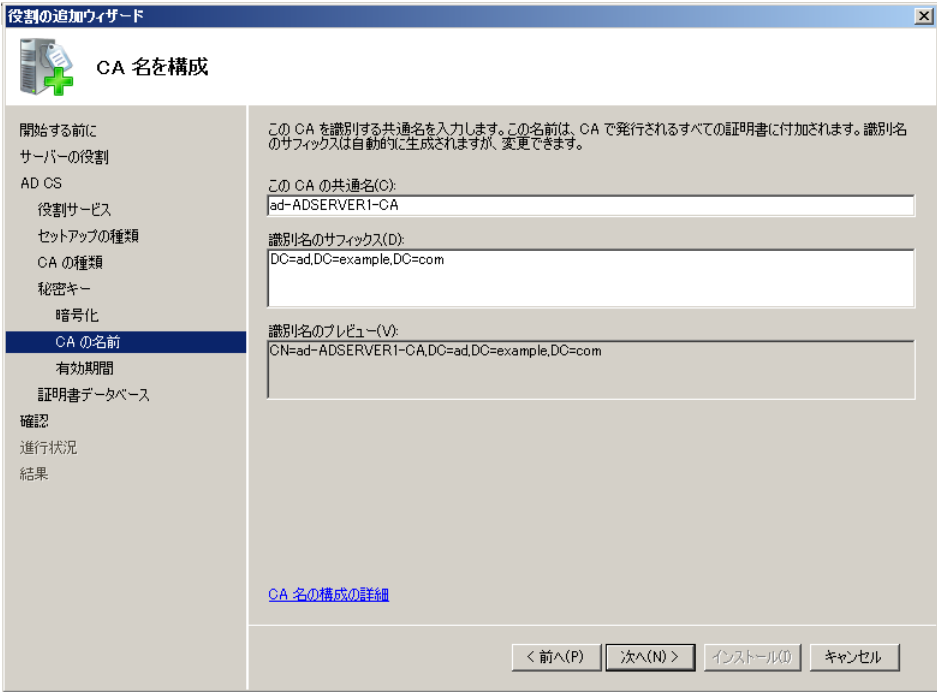
< 前へ(P)

次へ(N) >

インストール(I)

キャンセル

「CA 名を構成」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。



役割の追加ウィザード

CA 名を構成

開始する前に
サーバーの役割
AD CS
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 の名前
有効期間
証明書データベース
確認
進行状況
結果

この 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されます。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。

この CA の共通名(C):
ad-ADSERVER1-CA

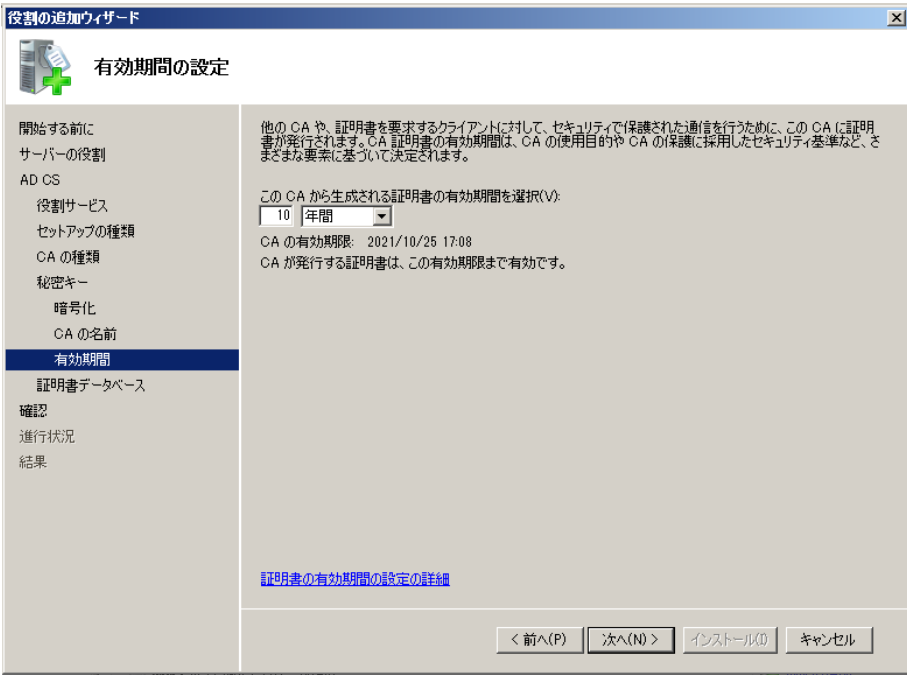
識別名のサフィックス(D):
DC=ad,DC=example,DC=com

識別名のプレビュー(V):
CN=ad-ADSERVER1-CA,DC=ad,DC=example,DC=com

[CA 名の構成の詳細](#)

< 前へ(P) 次へ(N) > インストール(O) キャンセル

「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）



役割の追加ウィザード

有効期間の設定

開始する前に
サーバーの役割
AD CS
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 の名前
有効期間
証明書データベース
確認
進行状況
結果

他の CA や、証明書を要求するクライアントに対して、セキュリティで保護された通信を行うために、この CA に証明書が発行されます。CA 証明書の有効期間は、CA の使用目的や CA の保護に採用したセキュリティ基準など、さまざまな要素に基づいて決定されます。

この CA から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: 2021/10/25 17:08
CA が発行する証明書は、この有効期限まで有効です。

[証明書の有効期間の設定の詳細](#)

< 前へ(P) 次へ(N) > インストール(O) キャンセル



以降の画面は、「次へ」で設定を進めてください。

証明書サービスのインストール後、Windows サーバーを再起動します。

以上で証明書サービスのインストールは完了です。

2. 改版履歷

- 2011 年 12 月 19 日
 - 初版作成