

# OpenAM 技術 Tips

## Vol.3

### Window デスクトップ SSO の実現手順

執筆者： 和田 広之(株式会社野村総合研究所),

田村 広平(フリーランス)

監修:OpenAM コンソーシアム

当技術 Tips コンテンツは、OpenAM コンソーシアム監修のもと、OpenAM コンソーシアム開発ワーキンググループに属する各企業の担当者により、執筆、編集されたものであり、各記事の著作権は執筆者に帰属いたします。

また、当記事のライセンスは、Creative Commons 4.0 の BY-NC-SA (表示、非営利、継承) とし、執筆者のクレジット(氏名、作品タイトル)を表示し、かつ非営利目的に限り、また改変を行った際には元の記事と同じ組み合わせの CC ライセンスで公開することを主な条件に、改変したり再配布したりすることができるものとします。

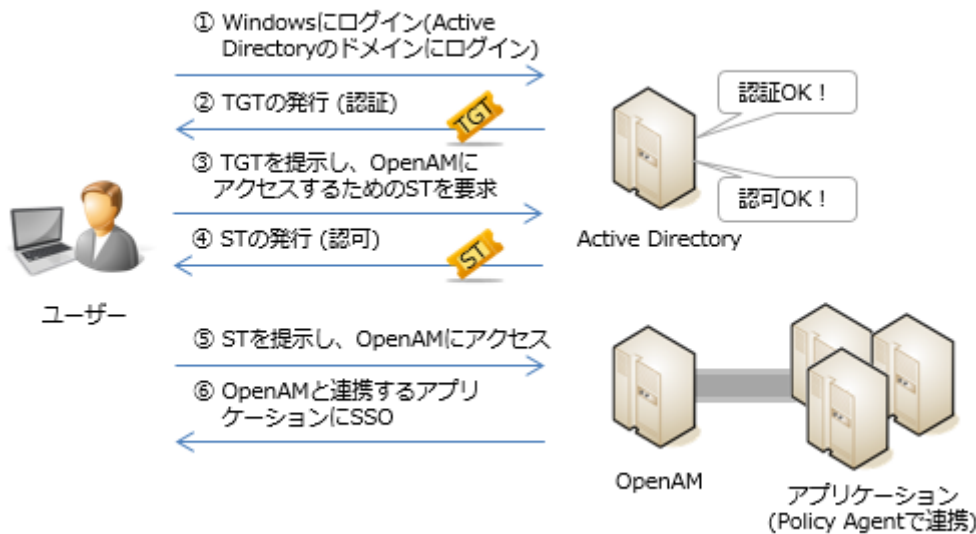
## 目次

1.	はじめに.....	3
2.	目的.....	4
3.	推奨環境.....	5
4.	事前準備.....	6
5.	名前解決の設定.....	7
6.	ファイアウォールの設定.....	8
7.	OpenAM 連携用ユーザーと一般ユーザーの作成 .....	9
8.	Kerberos 認証用の keytab ファイルの生成.....	18
9.	「データストア」の設定 (Active Directory 連携) .....	20
10.	「認証連鎖」の設定 (Windows デスクトップ SSO 認証の設定) .....	30
11.	クライアント PC (Windows) の設定 .....	42
12.	動作確認.....	47
13.	トラブルシューティングの方法 .....	48
14.	付録1: Active Directory のインストールと設定 .....	50
15.	付録2: DNS サーバーの設定 .....	70
16.	付録3: Firefox と Chrome の設定.....	88
17.	参考資料.....	89

## 1. はじめに

OpenAM は、Active Directory ドメインにログインしているユーザーを、OpenAM と連携する全てのアプリケーションに、再ログイン無しでシングルサインオンする仕組みを提供しています。この仕組みを「Windows デスクトップ SSO」と言います。

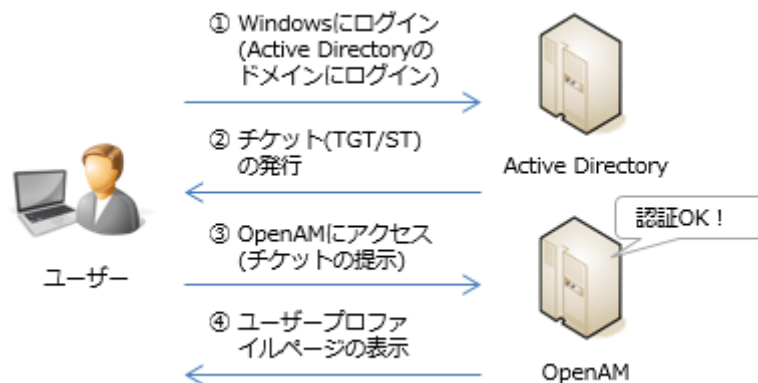
Windows デスクトップ SSO は、OpenAM の認証モジュールの 1 つであり、「統合 Windows 認証 (Kerberos 認証)」の仕組みを利用しています。Windows デスクトップ SSO の動作原理(シーケンス)は、以下のようになります。



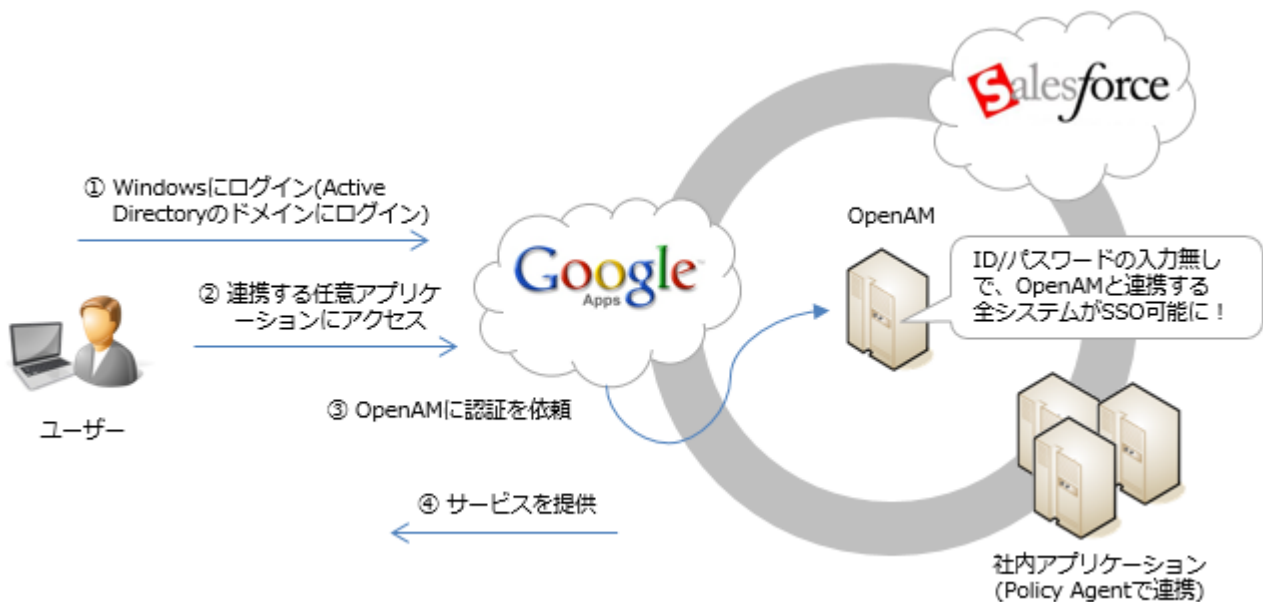
まず、ユーザーはWindowsにActive Directoryのドメインを指定して、ログインします(①)。ログイン時に入力したユーザーIDとパスワードが正しいと、Active DirectoryサーバーはTGT (Ticket Granting Ticket : チケット保証チケット)といわれるチケットを発行します(②)。ユーザーは、利用したいサービスがある場合、このチケットを再度Active Directoryサーバーに提示して(③)、ST(サービスチケット)といわれるチケットを取得します(④)。STは、利用したいサービス(OpenAM)へのアクセス許可を証明するチケットで、ユーザーはこれをOpenAMに提示する(⑤)ことでOpenAMが連携するアプリケーションへシングルサインオンできるようになります(⑥)。

## 2. 目的

本構築手順を実施することで、Active Directory ドメインに参加する Windows ユーザーであれば、再ログインを要求されることなく、OpenAM にログイン可能な環境を構築することができます。



今回はこのような OpenAM と Active Directory のみの構成ですが、さらに OpenAM と連携するアプリケーションを追加すれば、以下のように Windows 端末にログインするだけで、社内アプリケーションや Google Apps などのクラウドサービスにもシングルサインオンができるようになります。



### 3. 推奨環境

OpenAM をインストールするサーバー環境の推奨環境は以下の通りです。


- ・サーバーOS : Linux、Windows、UNIX
- ・メモリ : 2GB 以上 (JVM ヒープサイズ)
- ・JDK : 1.6 以上
- ・アプリケーションコンテナ (例. Apache Tomcat、JBoss、…etc.)

詳細については ForgeRock 社サイト (OpenAM Release Notes) をご参照下さい。

本構築手順では以下環境を前提としています。

#### OpenAM サーバー

- ・サーバーOS : CentOS 6.5
- ・メモリ : 2GB
- ・JDK : OpenJDK 1.7.0\_79
- ・アプリケーションコンテナ : Apache Tomcat 6.0.24
- ・OpenAM : OpenAM-12.0.0.war

 ForgeRock 社でビルドされた OpenAM 12.0.0.war を本番環境で利用する場合は、ForgeRock 社のサブスクリプションが必要です。

#### Active Directory サーバー

- ・サーバーOS : Windows Server 2012 R2 Standard (評価版)
- ・メモリ : 2GB

#### 4. 事前準備

本手順書では、以下の OpenAM サーバーが既にインストールされているものと仮定しています。

項目	値
URI	http://sso1.example.com:8080/openam

インストール手順に関しては、技術 Tips Vol.1 「OpenAM インストール手順」を参照下さい。

<http://www.openam.jp/category/member/techtips>

また、以下の Active Directory サーバーが既にインストールされているものと仮定しています。


項目	値
ホスト名	ad.example.local
LDAP ポート	389
LDAP 組織 DN	cn=Users, dc=example, dc=local
LDAP バインド DN	cn=admin, cn=Users, dc=example, dc=local

インストール手順に関しては、「14. 付録1: Active Directory のインストールと設定」を参照下さい。

## 5. 名前解決の設定

各 Windows クライアントから OpenAM サーバーの名前解決と、OpenAM - Active Directory 間の相互の名前解決ができるように DNS サーバーや hosts ファイルを設定する必要があります。


Windows Server の DNS サービスによりこれを実施する場合は、「15. 付録 2 : DNS サーバーの設定」を参照して下さい。

 クライアントが数台しかない場合であれば、hosts ファイルでの運用も可能です。

## 6. ファイアウォールの設定

OpenAM との通信のためには、88 番ポート (TCP/UDP) を開放しておかなければなりません。また、その他にも Active Directory を利用するにあたって、いくつかの TCP/UDP ポートを解放する必要があります。

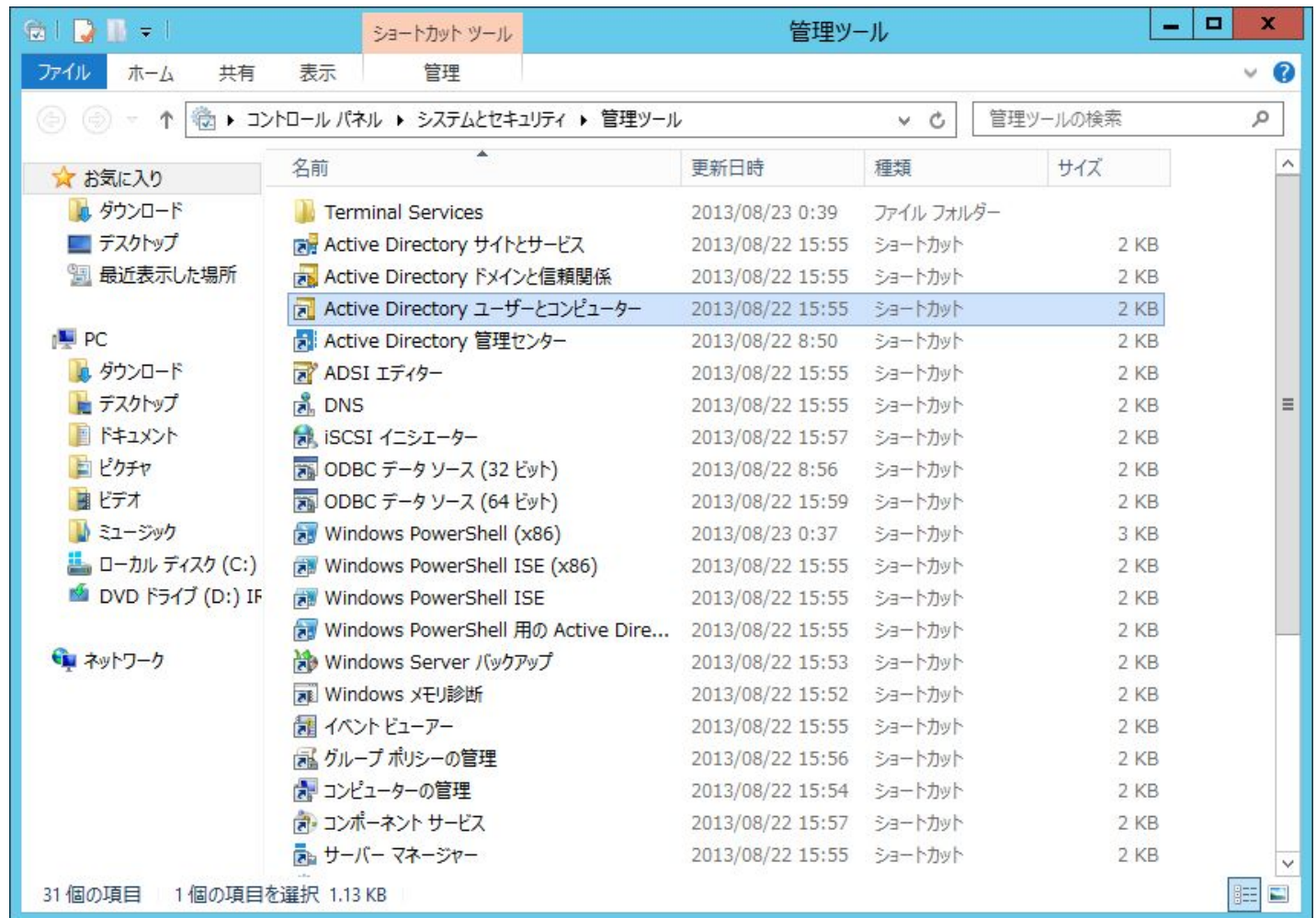
起動しているサービスが必要とするポートの解放が自動的に行われるように、Windows ファイアウォールの自動設定を有効化して下さい (デフォルトは有効)。自動設定を有効化できない場合は、手動で見直しが必要です。

 テスト目的であれば、全てのポートを解放しても構いません。

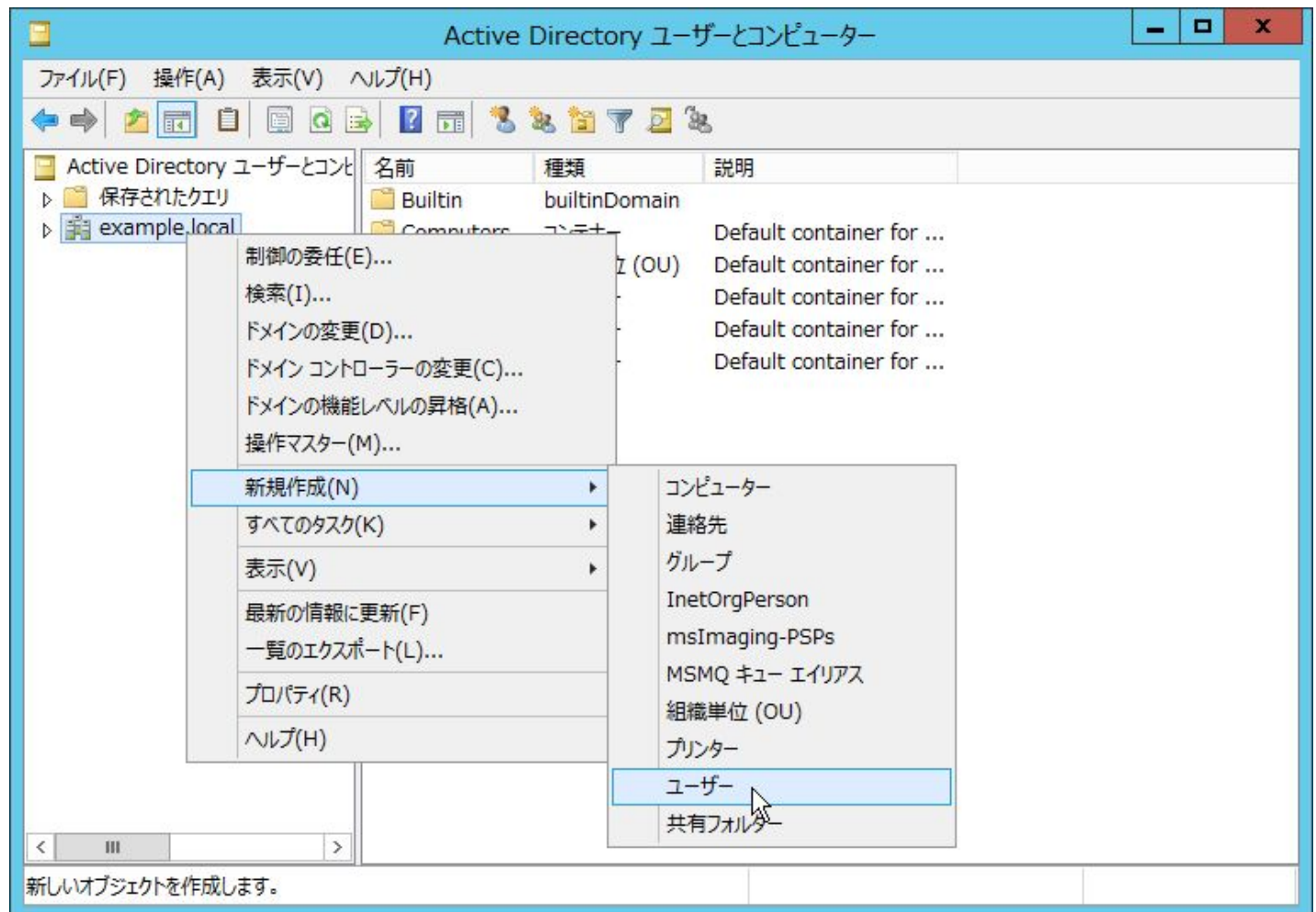


## 7. OpenAM 連携用ユーザーと一般ユーザーの作成

OpenAM から Kerberos 認証を行うための、ユーザーを作成します。「管理ツール」 > 「Active Directory ユーザーとコンピューター」をクリックします。



example.local で右クリックし、新規ユーザーを作成します。



まずは OpenAM 連携用ユーザーを作成します。ここでは、「openam」というユーザー名にしています。

新しいオブジェクト - ユーザー

作成先: example.local/

姓(L): openam

名(F):                      イニシャル                     

フルネーム(A): openam

ユーザー ログオン名(U):  
openam @example.local

ユーザー ログオン名 (Windows 2000 より前)(W):  
EXAMPLE¥ openam

< 戻る(B)    次へ(N) >    キャンセル

「ユーザーは次回ログオン時にパスワード変更が必要」のチェックは解除し、「パスワードを無期限にする」にチェックをします。



新しいオブジェクト - ユーザー

作成先: example.local/

パスワード(P): ●●●●●●●●

パスワードの確認入力(C): ●●●●●●●●

☐ ユーザーは次回ログオン時にパスワード変更が必要(M)

☐ ユーザーはパスワードを変更できない(S)

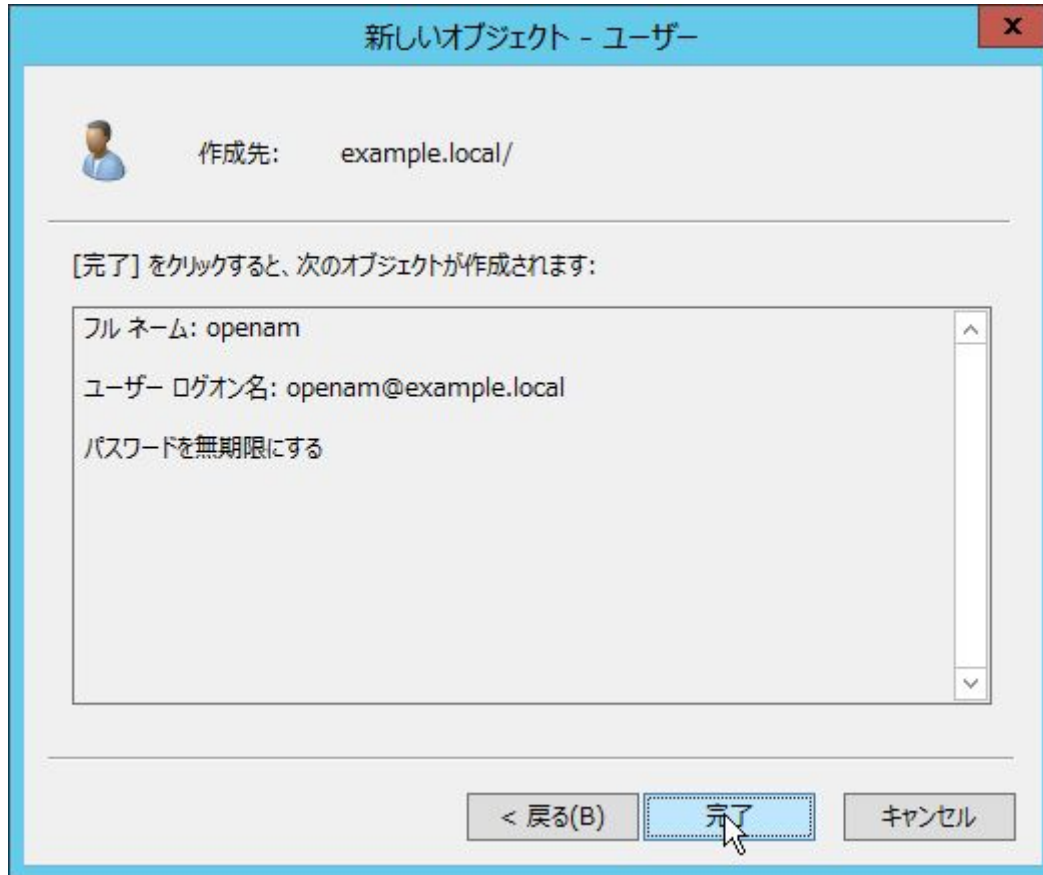
☒ パスワードを無期限にする(W)

☐ アカウントは無効(O)

< 戻る(B)    次へ(N) >    キャンセル

「パスワードを無期限にする」をチェックしておくことで、パスワードの有効期限が過ぎてもデスクトップSSOが失敗することが無くなります。

内容を確認して、「完了」ボタンをクリックして下さい。



新しいオブジェクト - ユーザー

作成先: example.local/

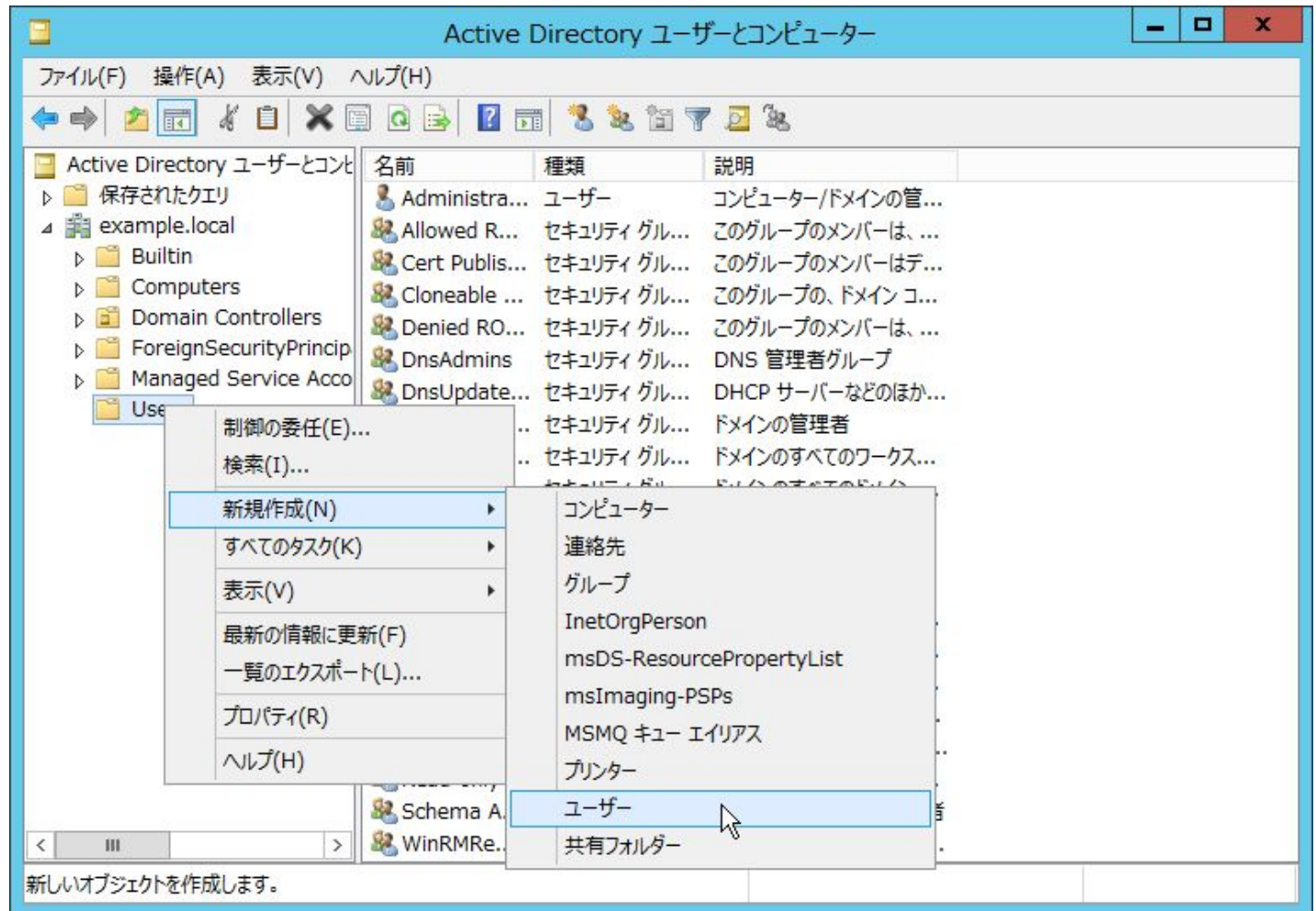
[完了] をクリックすると、次のオブジェクトが作成されます:

- フルネーム: openam
- ユーザー ログオン名: openam@example.local
- パスワードを無期限にする

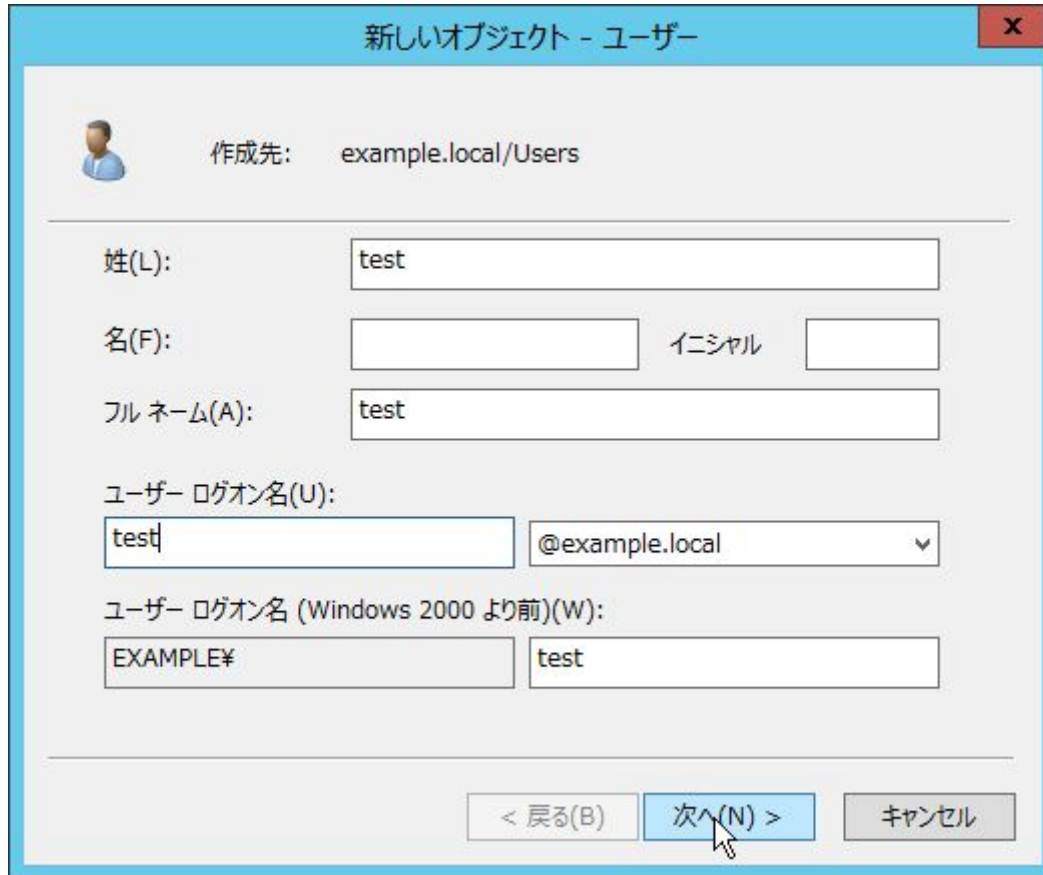
< 戻る(B)    完了    キャンセル



example.local ドメインに参加する一般ユーザーを作成します。example.local/Users で右クリックし、新規ユーザーを作成します。



先ほど同様にユーザーを作成して下さい。



新しいオブジェクト - ユーザー

作成先: example.local/Users

姓(L): test

名(F):                      イニシャル                     

フルネーム(A): test

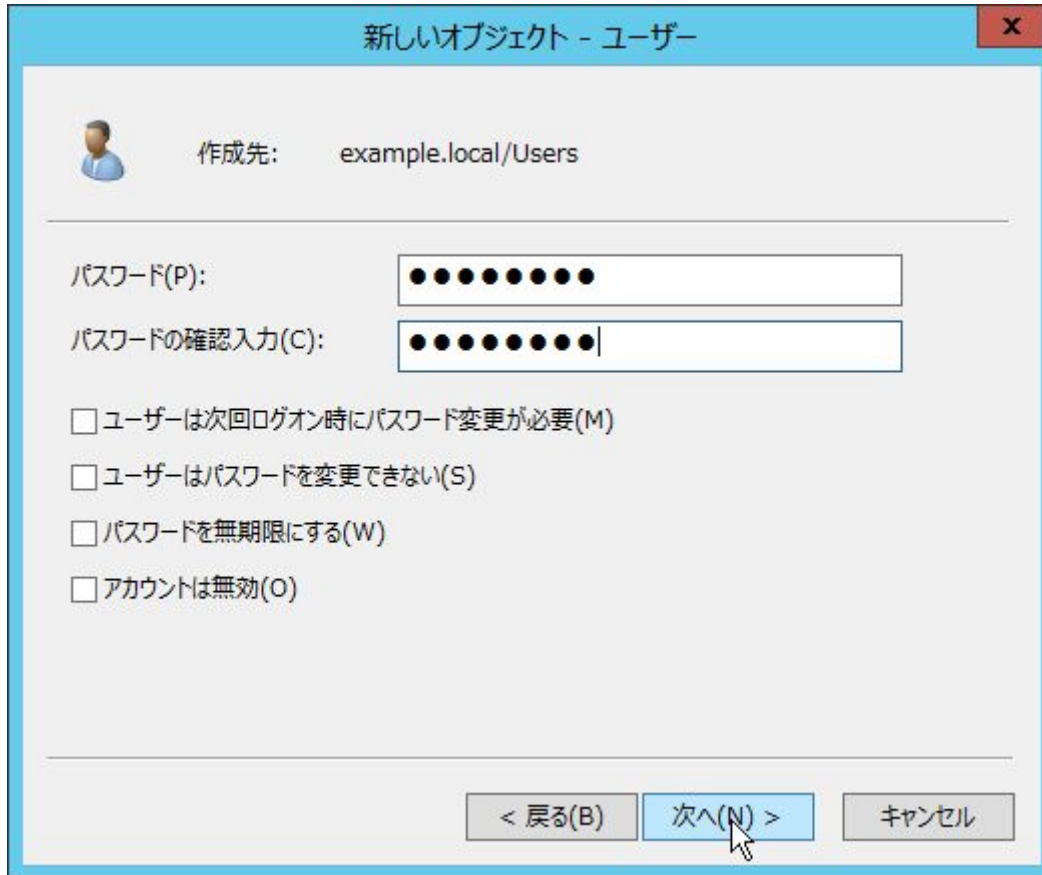
ユーザー ログオン名(U): test @example.local

ユーザー ログオン名 (Windows 2000 より前)(W): EXAMPLE¥ test

< 戻る(B)    次へ(N) >    キャンセル

ここでは、ユーザー名を「test」としています。

「ユーザーは次回ログオン時にパスワード変更が必要」のチェックは解除します。



新しいオブジェクト - ユーザー

作成先: example.local/Users

パスワード(P):

パスワードの確認入力(C):

☐ ユーザーは次回ログオン時にパスワード変更が必要(M)

☐ ユーザーはパスワードを変更できない(S)

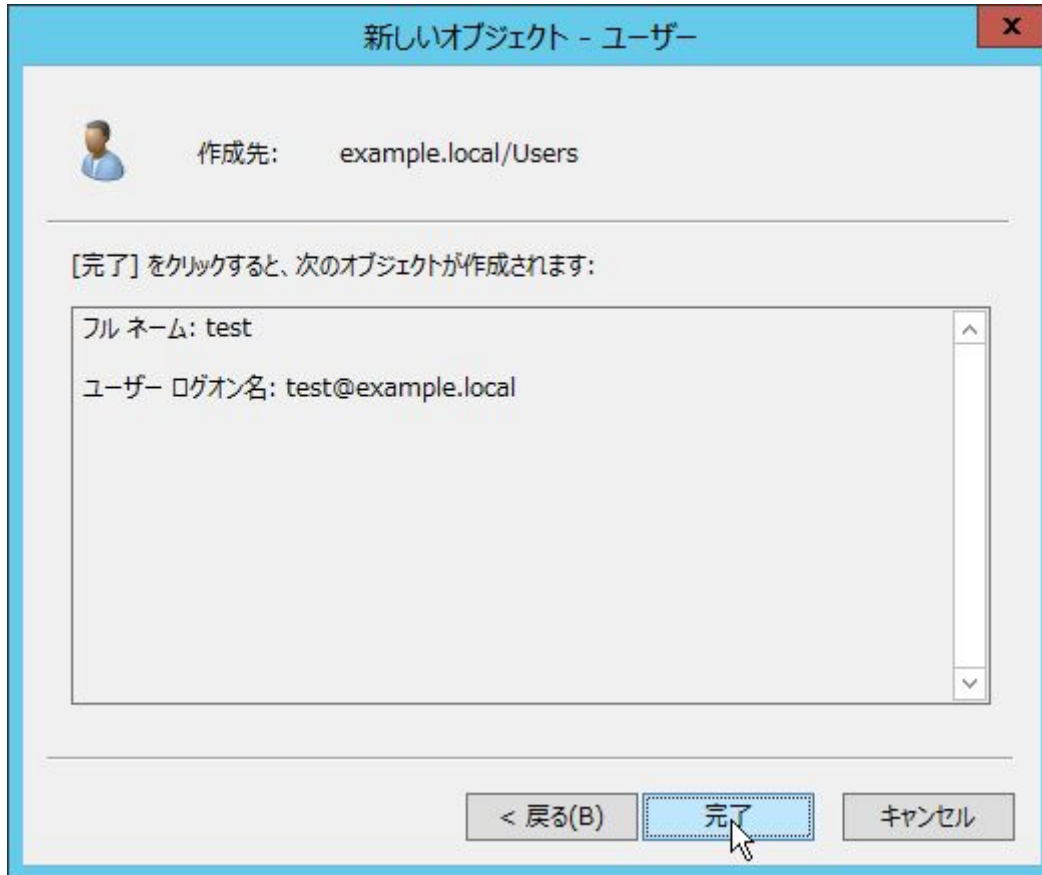
☐ パスワードを無期限にする(W)

☐ アカウントは無効(O)

< 戻る(B)    次へ(N) >    キャンセル



内容を確認して、「完了」ボタンをクリックして下さい。



新しいオブジェクト - ユーザー

作成先: example.local/Users

[完了] をクリックすると、次のオブジェクトが作成されます:

フルネーム: test  
ユーザー ログオン名: test@example.local

< 戻る(B)    完了    キャンセル

## 8. Kerberos 認証用の keytab ファイルの生成

OpenAM の Windows デスクトップ SSO 認証では、Kerberos 認証用の keytab ファイルが必要になります。keytab ファイルは、Windows の ktpass コマンドにより生成します。Active Directory サーバーでコマンドプロンプトを起動し、以下のコマンドを実行します。

```
> ktpass -out desktopsso.HTTP.keytab  
        -princ HTTP/sso1.example.com@EXAMPLE.LOCAL  
        -ptype KRB5_NT_PRINCIPAL  
        -pass Password1  
        -mapuser openam
```

各オプションについて説明します。

-out keytab ファイルのファイル名

出力される keytab ファイルのファイル名です。

-princ サービス主体

Kerberos 認証での「サービス主体」を指定します。

HTTP/"OpenAM の FQDN"@Active Directory のドメイン名の大文字で設定します。

-ptype KRB5\_NT\_PRINCIPAL

固定値 (KRB5\_NT\_PRINCIPAL) を指定します。

-pass OpenAM 連携用ユーザーのパスワード


OpenAM 連携用ユーザーのパスワードを指定します。

-mapuser OpenAM 連携用ユーザーの ID


OpenAM 連携用ユーザーの ID を指定します。

実行結果は以下のようになります。

```
> ktpass -out desktopsso.HTTP.keytab -princ HTTP/sso1.example.com@EXAMPLE.LOCAL -ptype
KRB5_NT_PRINCIPAL -pass Password1 -mapuser openam
Targeting domain controller: WIN-DTOKQDBDE2J.example.local
Using legacy password setting method
Successfully mapped HTTP/sso1.example.com to openam.
Key created.
Output keytab to desktopsso.HTTP.keytab:
Keytab version: 0x502
keysize 79 HTTP/sso1.example.com@EXAMPLE.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4-
HMAC) keylength 16 (0x64f12cddaa88057e06a81b54e73b949b)
```

 エラーが出る場合は `-Target AD のドメイン名` をオプションに追加して下さい。

出力された `desktopsso.HTTP.keytab` ファイルは、OpenAM サーバーの任意のディレクトリに転送しておきます。  
ここでは、`/home/tomcat/desktopsso.HTTP.keytab` に配置したと仮定します。

 **keytab ファイルは任意のパスに配置できますが、Tomcat の実行ユーザーが参照できるディレクトリでなければなりません。**

## 9. 「データストア」の設定（Active Directory 連携）

Active Directory を OpenAM のユーザーデータストアとして使用するための設定を行います。  
OpenAM の管理コンソールに amadmin でログインして下さい。

OpenAM - Login - Mozilla Firefox

OpenAM - Login

sso1.example.com:8080/openam/XUI/#login/ Invalid initial he: →

FORGEROCK

OpenAM へのサインイン

ユーザー名: amadmin

パスワード: .....

☒ Remember my username

Log in

[info@forgerock.com](mailto:info@forgerock.com)

Copyright © 2010-14 ForgeRock AS, all rights reserved.

「アクセス制御」タブをクリックします。

OpenAM - Mozilla Firefox

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

共通タスク **アクセス制御** 連携 設定 セッション

### SAMLv2 プロバイダを作成

これらのワークフローを使用して、SAMLv2 連携のホストまたはリモートのアイデンティティとサービスプロバイダを作成します。

- ホストアイデンティティプロバイダの作成
- ホストサービスプロバイダの作成
- リモートアイデンティティプロバイダを登録
- リモートサービスプロバイダを登録

### OAuth2 の設定

このタスクはレルムごとに OAuth2 を設定します。レルム単位に認可サーバとして動作することができます。

- OAuth2 の設定

### Fedlet を作成

Fedlet を作成して、OpenAM のこのインスタンスでホストされているアイデンティティプロバイダと、連携ソリューションのないリモートサービスプロバイダ間で、連携を有効にします。最初に、ホストアイデンティティプロバイダを設定する必要があります。

- Fedlet を作成

### Google Apps の設定

OpenAM と Google Apps Web アプリケーションを統合して、シングルサインオン環境を作成します。最初に、ホストアイデンティティプロバイダとトラストサークルを設定する必要があります。

### Salesforce CRM の設定

OpenAM と Salesforce CRM を統合して、シングルサインオン環境を作成します。最初に、SAMLv2 ホストアイデンティティプロバイダとトラストサークルを設定する必要があります。

- Salesforce CRM の設定

### Configure Social Authentication

Add social authentication options per realm. This task configures authentication through third parties such as Facebook, Google and Microsoft.

- Configure Facebook Authentication
- Configure Google Authentication
- Configure Microsoft Authentication
- Configure Other Authentication

### 連携の接続性をテスト

この自動化されたテストを使用して、連携の接続が成功するかどうかを判断し、どこに問題があるかを確認します。

- 連携の接続性をテスト

### 製品マニュアルを取得

OpenAM 製品マニュアルのページを起動します。

- 製品マニュアルを取得

sso1.example.com:8080/openam/task/Home?Home.tab...FRhYklkdAABMHQAekN1cnJlbnRQcm9maWxlVmllld3QAAS94

「/(最上位のレルム)」のリンクをクリックします。

OpenAM - Mozilla Firefox

OpenAM

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

共通タスク アクセス制御 連携 設定 セッション

レルムは、OpenAM が設定情報の整理に使用する単位です。レルム内では、認証プロパティ、承認ポリシー、データストア、対象、その他のデータを定義できます。最上位のレルムは、OpenAM の配備時に作成されます。最上位のレルムは、OpenAM インスタンスの root で OpenAM 設定データを含んでいます。

### レルム

\* 検索

レルム (1 項目)

新規... 削除

レルム名	場所
<a href="#">/(最上位のレルム)</a>	/

sso1.example.com:8080/openam/realms/RMRealm?RMR...iSWR0AAExdAASQ3VycmVudFByb2ZpbGVWaWV3cQB-ABp4

「データストア」をクリックします。

The screenshot shows the OpenAM console interface in a Mozilla Firefox browser window. The address bar displays the URL `sso1.example.com:8080/openam/realm/RMRealm?RM`. The page header includes the OpenAM logo and the FORGEROCK logo. The navigation menu at the top contains tabs: 一般, 認証, サービス, データストア (selected), 権限, ポリシー, 対象, エージェント, and STS. The main content area shows the configuration for the 'Data Store' tab. It includes a section for 'レلم属性' (Realm Properties) with radio buttons for 'アクティブ' (Active) and '非アクティブ' (Inactive). Below this is a section for 'レلمまたは DNS のエイリアス' (Realm or DNS Alias) with a list of current values: 'sso1.example.com' and 'openam'. A '新しい値' (New Value) input field and an '追加' (Add) button are also present. The bottom of the page shows the browser's status bar with the full URL.

OpenAM - Mozilla Firefox

OpenAM

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

一般 認証 サービス **データストア** 権限 ポリシー 対象 エージェント STS

/ (最上位のレلم)

(最上位のレلم) - プロパティー

保存 リセット アクセス制御 へ戻る

レلم属性

レلمの状態: ☒ アクティブ ☐ 非アクティブ

このレلمを有効または無効にします。

レلمまたは DNS のエイリアス

現在の値

sso1.example.com  
openam

削除

新しい値

追加

このレلمに関連付けられた DNS ドメインのリスト。

sso1.example.com:8080/openam/realm/RealmProperti...YklkcQB-AAN0ABJDdXjyZW50UHJvZmlsZVZpZXdxAH4AHng\$

「新規」ボタンをクリックします。

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

一般 認証 サービス データストア 権限 ポリシー 対象 エージェント STS

/ (最上位のレルム)

(最上位のレルム) - データストア アクセス制御 へ戻る

データストア (1 項目)

新規... 削除

<input checked="" type="checkbox"/>	名前	タイプ
<input type="checkbox"/>	embedded	OpenDJ



任意の名前(本書では ActiveDirectory)を入力し、タイプは「Active Directory」を選択して、「次へ」ボタンをクリックします。

OpenAM - Mozilla Firefox

OpenAM

sso1.example.com:8080/openam/realms/IDRepo

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

ステップ 1/2: データストアのタイプを選択

戻る 次へ 取消し

必須入力フィールド

名前: ActiveDirectory

タイプ:

- ☒ Active Directory
- ☐ Active Directory アプリケーションモード (ADAM)
- ☐ OpenAM スキーマを含んだ Sun Directory Server
- ☐ OpenDJ
- ☐ Tivoli Directory Server
- ☐ データベースリポジトリ (アーリーアクセス)
- ☐ 汎用 LDAPv3

Active Directory をデータストアとして利用するための設定画面が表示されます。

OpenAM - Mozilla Firefox

OpenAM

sso1.example.com:8080/openam/realm/IDRepoSelect

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

ステップ 2/2: 新規データストア - Active Directory

戻る 終了 取消し

\* 必須入力フィールド

\* 名前: ActiveDirectory

完了時にスキーマを読み込み: ☒

サーバー設定

\* LDAP サーバー

現在の値 ad.example.local:389 削除

新しい値 追加

形式: LDAP サーバーのホスト名:ポート | server\_ID | site\_ID

LDAP バインド DN: CN=Administrator,CN=Users,dc=openam,dc=for  
サポートされる操作を実行できる適切なアクセス権を持つユーザーまたは管理者。

LDAP バインドパスワード: .....

LDAP バインドパスワード (確認): .....

\* LDAP 組織 DN: dc=openam,dc=forgerock,dc=org

LDAP SSL: ☐ 有効

以下の設定を行います。

項目	値
LDAP サーバー	ad.example.local:389 ※デフォルトで設定されている値は削除して、上記値を追加して下さい。
LDAP バインド DN	cn=administrator, cn=Users, dc=example, dc=local
LDAP バインドパスワード	[administrator のパスワード]
LDAP バインドパスワード (確認)	[administrator のパスワード]
LDAP 組織 DN	cn=Users, dc=example, dc=local
LDAPv3 プラグイン検索範囲	SCOPE_SUB
LDAP ユーザー検索属性	sAMAccountName
LDAP ピープルコンテナネーミング属性	(空にする)
LDAP ピープルコンテナ値	(空にする)
グループメンバーシップの属性名	memberOf
持続検索ベース DN	dc=example, dc=local

データストア「ActiveDirectory」を作成したら、デフォルトの embedded データストアは削除して下さい。

OpenAM - Mozilla Firefox

OpenAM

sso1.example.com:8080/openam/realms/IDRepoAdd

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

一般 認証 サービス データストア 権限 ポリシー 対象 エージェント STS

/ (最上位のレルム)

(最上位のレルム) - データストア [アクセス制御 へ戻る](#)

データストア (2 項目)

新規... 削除

<input checked="" type="checkbox"/>	名前	タイプ
<input type="checkbox"/>	ActiveDirectory	Active Directory
<input checked="" type="checkbox"/>	embedded	OpenDJ

対象タブをクリックし、Active Directory サーバー上のユーザーアカウントが表示されていることを確認します。

OpenAM - Mozilla Firefox

OpenAM

sso1.example.com:8080/openam/authentication/Auth

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

一般 認証 サービス データストア 権限 ポリシー 対象 エージェント STS

ユーザー グループ

/ (最上位のレルム)

ユーザー

アクセス制御 へ戻る

\* 検索

ユーザー (7 ユーザー)

新規... 削除

<input checked="" type="checkbox"/>	名前	汎用 ID
<input type="checkbox"/>	Administrator	Administrator
	amAdmin	amAdmin
<input type="checkbox"/>	anonymous	anonymous
<input type="checkbox"/>	demo	demo
<input type="checkbox"/>	Guest	Guest
<input type="checkbox"/>	krbtgt	krbtgt
<input type="checkbox"/>	test	test

## 10. 「認証連鎖」の設定 (Windows デスクトップ SSO 認証の設定)

OpenAM の認証の方式を Windows デスクトップ SSO 認証に変更します。

「認証」タブをクリックして、認証画面を表示します。

OpenAM - Mozilla Firefox

OpenAM

sso1.example.com:8080/openam/authentication

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

一般 認証 サービス データストア 権限 ポリシー 対象 エージェント STS

/ (最上位のレルム)

(最上位のレルム) - プロパティ

保存 リセット アクセス制御 へ戻る

レルム属性

レルムの状態: ☒ アクティブ ☐ 非アクティブ

このレルムを有効または無効にします。

レルムまたは DNS のエイリアス

現在の値

sso1.example.com	削除
openam	

新しい値

追加

このレルムに関連付けられた DNS ドメインのリスト。

sso1.example.com:8080/openam/realms/RealmProperties...EFCUXRPRGsxT0RZeE5qa3pNekF3TkRRMU5ETXIOUS4uKng\$

モジュールインスタンスのセクションにある「新規」ボタンをクリックします。

OpenAM - Mozilla Firefox

OpenAM

ssol.example.com:8080/openam/realm/RealmPrc

Invalid initial he: →

### コア

すべてのコア設定...

組織認証設定: ldapService

ユーザーのデフォルト認証連鎖。

管理者認証設定: ldapService

管理者のデフォルトの認証連鎖。

ログイン成功時に返すデフォルトの URL

現在の値: /openam/console

削除

新しい値:

追加

ログイン成功後にこの URL へ転送します。

先頭に戻る

### モジュールインスタンス

モジュールインスタンス (7 項目)

新規 削除

名前	タイプ
<input type="checkbox"/> HOTP	HOTP
<input type="checkbox"/> LDAP	LDAP
<input type="checkbox"/> OATH	OATH
<input type="checkbox"/> SAE	SAE
<input type="checkbox"/> WSSAuthModule	WSSAuth

「Windows デスクトップ SSO」を選択し、任意の名前(本書では DesktopSSO)を付けて「了解」ボタンをクリックして下さい。

The screenshot shows the OpenAM console interface in Mozilla Firefox. The browser address bar shows the URL `sso1.example.com:8080/openam/authentication/Auth`. The page title is "OpenAM - Mozilla Firefox". The OpenAM logo and "FORGEROCK" branding are visible. The user is logged in as "amAdmin" on the server "sso1.example.com".

The main section is titled "新規モジュールインスタンス" (New Module Instance). It contains the following fields and options:

- 名前:** DesktopSSO
- タイプ:** A list of radio buttons for selecting the module type. The selected option is "Windows デスクトップ SSO".

The list of available module types includes:

- Active Directory
- Device Id (Match)
- Device Id (Save)
- HOTP
- HTTP 基本
- JDBC
- LDAP
- MSISDN
- OATH
- OAuth 2.0
- OpenID Connect id\_token bearer
- RADIUS
- SAE
- Scripted Module
- SecurID
- Windows NT
- Windows デスクトップ SSO** (selected)
- WSSAuth
- アダプティブリスク
- データストア
- メンバーシップ
- 持続 Cookie
- 証明書
- 匿名
- 連携

At the top right, there are two buttons: "了解" (OK) and "取消し" (Cancel). A red asterisk and the text "必須入力フィールド" (Required input field) are shown next to the "了解" button.



モジュールインスタンスの一覧から、作成された Windows デスクトップ SSO 認証モジュールを選択します。

OpenAM - Mozilla Firefox

OpenAM

sso1.example.com:8080/openam/realm/RealmPrc

Invalid initial he: →

### コア

すべてのコア設定...

組織認証設定: ldapService

ユーザーのデフォルト認証連鎖。

管理者認証設定: ldapService

管理者のデフォルトの認証連鎖。

ログイン成功時に返すデフォルトの URL

現在の値: /openam/console

削除

新しい値:

追加

ログイン成功後にこの URL へ転送します。

先頭に戻る

### モジュールインスタンス

モジュールインスタンス (8 項目)

新規 削除

名前	タイプ
DataStore	データストア
DesktopSSO	Windows デスクトップ SSO
Federation	連携
HOTP	HOTP
LDAP	LDAP

Windows デスクトップ SSO 認証モジュールに、以下の設定を行います。

OpenAM - Mozilla Firefox

OpenAM

sso1.example.com:8080/openam/authentication/Auth

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

### Windows デスクトップ SSO

保存 リセット 認証 へ戻る

#### レルム属性

サービス主体: HTTP/sso1.example.com@EXAMPLE.LOCAL  
認証時に使用される Kerberos 主体の名前

Keytab ファイル名: /home/tomcat/desktopsso.HTTP.keytab  
AD の keytab ファイルのパス

Kerberos レルム: EXAMPLE.LOCAL  
認証に使用される Kerberos (Active Directory) のレルムの名前。

Kerberos サーバー名: ad.example.local  
Kerberos (Active Directory) サーバーのホスト名/ IP アドレス。

ドメイン名を含む主体を返す: ☐ 有効  
単なるユーザー名ではなく、認証済みユーザーの完全修飾名を返します。

認証レベル: 0  
この認証モジュールで認証成功時に設定される認証レベルです。

レルム内のユーザー検索: ☐ 有効  
ユーザーがデータストアで構成されたユーザープロフィールと一致していることを検証します。

保存 リセット 認証 へ戻る

項目	値
サービス主体	HTTP/sso1.example.com@EXAMPLE.LOCAL
Keytab ファイル名	/home/tomcat/desktopsso.HTTP.keytab
Kerberos レルム	EXAMPLE.LOCAL
Kerberos サーバー名	ad.example.local
ドメイン名を含む主体を返す	チェックなし
認証レベル	0
レルム内のユーザー検索	チェックなし

この例では、Keytab ファイル (desktopsso.HTTP.keytab) を /home/tomcat/ に配置しています。

次に、Windows デスクトップ SSO 認証モジュールを含む認証連鎖を作成します。  
認証連鎖のセクションにある「新規」ボタンをクリックして下さい。

OpenAM - Mozilla Firefox

OpenAM

ssol.example.com:8080/openam/authentication/ Invalid initial he: →

ログイン成功後にこの URL へ転送します。

先頭に戻る

### モジュールインスタンス

モジュールインスタンス (8 項目)

新規 削除

<input checked="" type="checkbox"/>	<input type="checkbox"/>	名前	タイプ
<input type="checkbox"/>		DesktopSSO	Windows デスクトップ SSO
<input type="checkbox"/>		Federation	連携
<input type="checkbox"/>		HOTP	HOTP
<input type="checkbox"/>		LDAP	LDAP
<input type="checkbox"/>		OATH	OATH
<input type="checkbox"/>		SAE	SAE
<input type="checkbox"/>		WSSAuthModule	WSSAuth
<input type="checkbox"/>		DataStore	データストア

このレلمに使用可能な認証モジュールのリスト

先頭に戻る

### 認証連鎖

認証連鎖 (1 項目)

新規 削除

<input checked="" type="checkbox"/>	<input type="checkbox"/>	名前
<input type="checkbox"/>		ldapService

このレلمに使用可能な認証連鎖のリスト

先頭に戻る

任意の名称(本書では desktopssochain)で認証連鎖を作成します。

OpenAM - Mozilla Firefox

OpenAM

sso1.example.com:8080/openam/authentication/Auth

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

新規認証連鎖

了解 取消し

\* 必須入力フィールド

\* 名前: desktopssochain

認証連鎖は以下のようなモジュール構成にします。

インスタンス	条件	オプション
DesktopSSO	十分	

OpenAM - Mozilla Firefox

OpenAM

sso1.example.com:8080/openam/authentication/Auth

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

desktopssochain - プロパティ

保存 リセット 認証 へ戻る

(1 項目)

追加 削除 並べ替え

<input checked="" type="checkbox"/>	インスタンス	条件	オプション
<input type="checkbox"/>	DesktopSSO	十分	

このテーブルには、この認証連鎖を構成する認証モジュールのリストを表示します。

ログイン成功時に返す URL

現在の値

新しい値

追加

ログイン成功後、次のURLに転送されます。

ログイン失敗時に返す URL

現在の値

この設定の場合、OpenAM は Windows デスクトップ SSO 認証が成功すれば、ログインを許可します。つまり、Active Directory ドメインに参加している Windows にログインしているユーザーは、ログイン画面で ID とパスワードを入力することなく、OpenAM にシングルサインオンできることになります。

最後に作成した認証連鎖を有効にします。「認証タブ」の「コア」セクションにある「組織認証設定」をデフォルトの ldapservice から作成した認証連鎖(desktopssochain)に変更し、「保存」をクリックします。

OpenAM - Mozilla Firefox

OpenAM

sso1.example.com:8080/openam/authentication/Auth

バージョン ログアウト

ユーザー: amAdmin サーバー: sso1.example.com

FORGEROCK

一般 認証 サービス データストア 権限 ポリシー 対象 エージェント STS

/ (最上位のレルム)

(最上位のレルム) - 認証

保存 リセット アクセス制御 へ戻る

コア

すべてのコア設定...

組織認証設定: desktopssochain

ユーザーのデフォルト認証連鎖。

管理者認証設定: ldapService

管理者のデフォルトの認証連鎖。

ログイン成功時に返すデフォルトの URL


現在の値 /openam/console 削除

新しい値 追加

ログイン成功後にこの URL へ転送します。

以上で、OpenAM の設定は終了です。完了したら、アプリケーションコンテナを再起動して下さい。



 「組織認証設定」の認証を変更したため、OpenAM サーバーへアクセスすると Windows 統合認証となり OpenAM のログイン画面が表示されなくなります。

OpenAM 管理コンソールを操作するために amAdmin でログインする場合は、OpenAM へアクセスする URL のクエリストリングに service=adminconsole service を付けてアクセスするようにして下さい。

<http://sso1.example.com:8080/openam/UI/Login?service=adminconsole service>

## 1.1. クライアント PC (Windows) の設定

通常は、Active Directory のグループポリシーのブラウザの設定テンプレートにクライアント PC の共通設定を行います。本手順書では動作検証用のクライアント PC の設定を変更します。Active Directory の設定を変更している場合は、このセクションを読み飛ばして下さい。

ドメインに参加していない端末は、DNS 設定とドメインへの参加設定が必要です。TCP/IP の設定で、Active Directory サーバーの IP アドレスを DNS サーバーとして指定します。

インターネット プロトコル バージョン 4 (TCP/IPv4) のプロパティ

全般 代替の構成

ネットワークでこの機能がサポートされている場合は、IP 設定を自動的に取得することができます。サポートされていない場合は、ネットワーク管理者に適切な IP 設定を問い合わせてください。

☒ IP アドレスを自動的に取得する(O)

☐ 次の IP アドレスを使う(S):

IP アドレス(I):

サブネット マスク(U):

デフォルト ゲートウェイ(D):

☐ DNS サーバーのアドレスを自動的に取得する(B)

☒ 次の DNS サーバーのアドレスを使う(E):

優先 DNS サーバー(P): 172 . 26 . 22 . 53

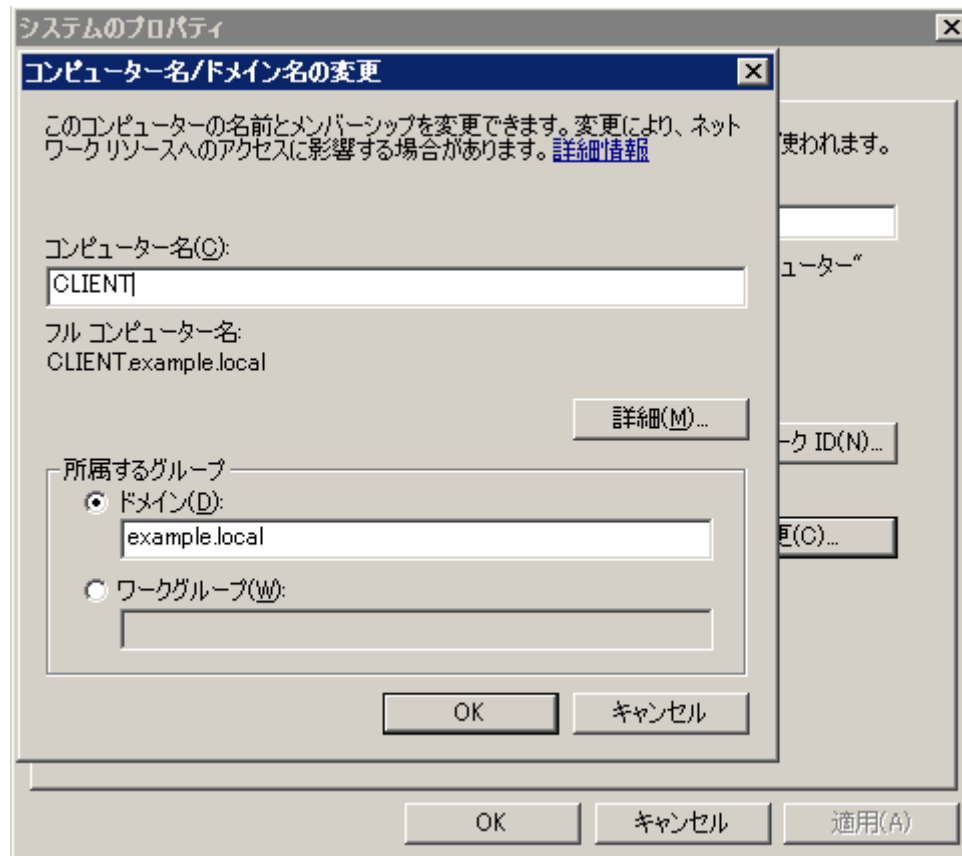
代替 DNS サーバー(A):

☐ 終了時に設定を検証する(L)

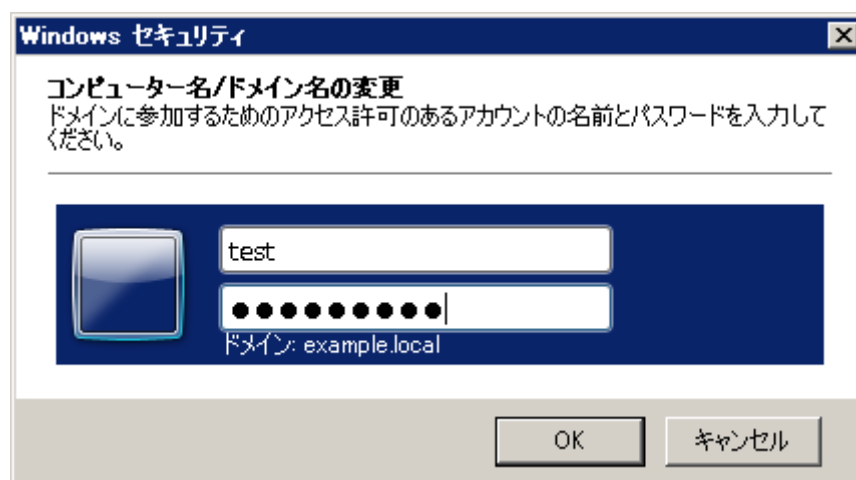
詳細設定(V)...

OK キャンセル

次にドメイン参加の設定を行います。コンピュータ名変更のダイアログより、ドメインを入力して「OK」ボタンをクリックして下さい。



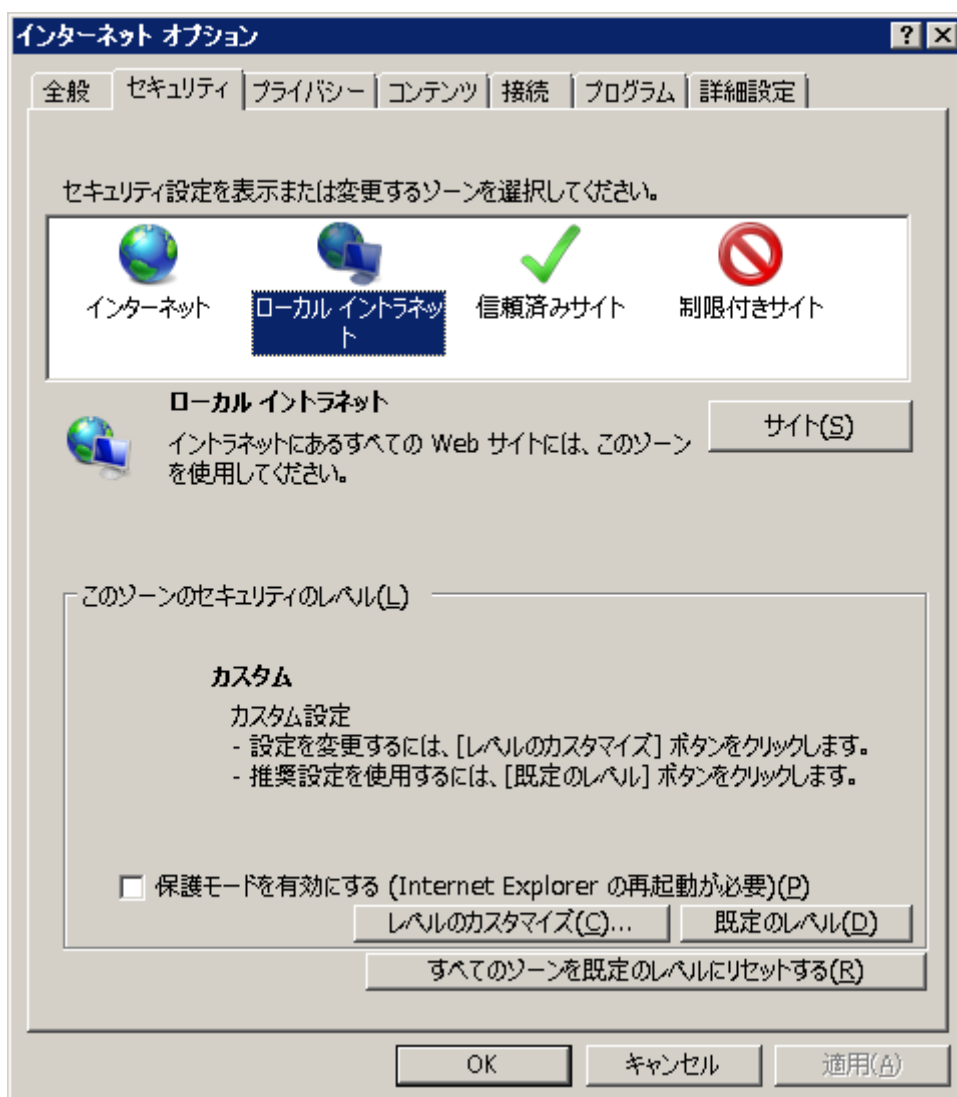
以下の認証ダイアログが表示されるので、Active Directoryに登録したユーザーIDとパスワードを入力します。



最後にブラウザの設定を変更します。通常は、Active Directory のグループポリシーのブラウザの設定テンプレートにクライアント PC の共通設定を行います。本手順書では動作検証用のクライアント PC の設定を変更します。Active Directory の設定を変更している場合は、このセクションを読み飛ばして下さい。

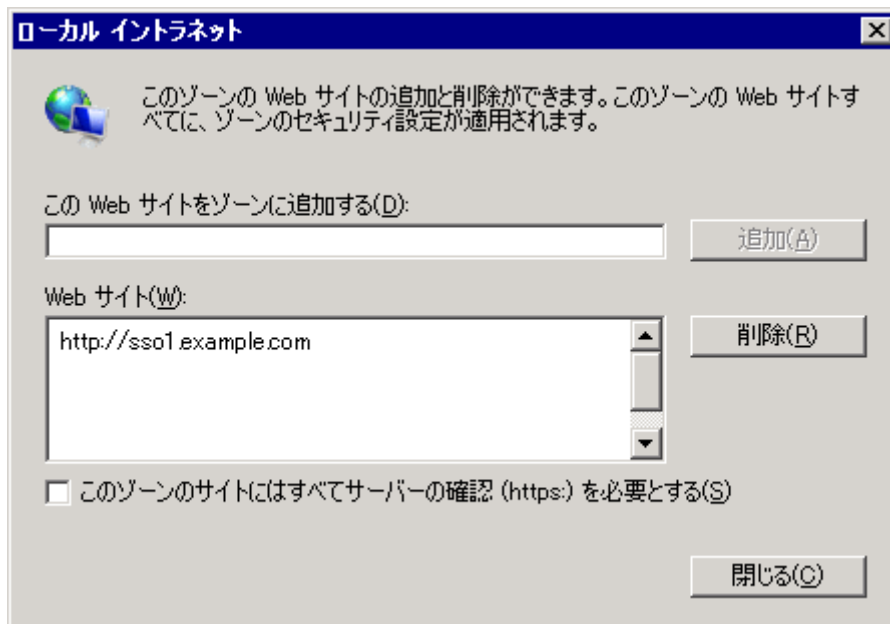
以下は Internet Explorer 11 の場合ですが、Microsoft Edge でも同様です。それ以外のブラウザの設定については、「16. 付録3: Firefox と Chrome の設定」を参照して下さい。

インターネットオプションの「セキュリティ」タブをクリックし、「ローカル イントラネット」を選択して下さい。

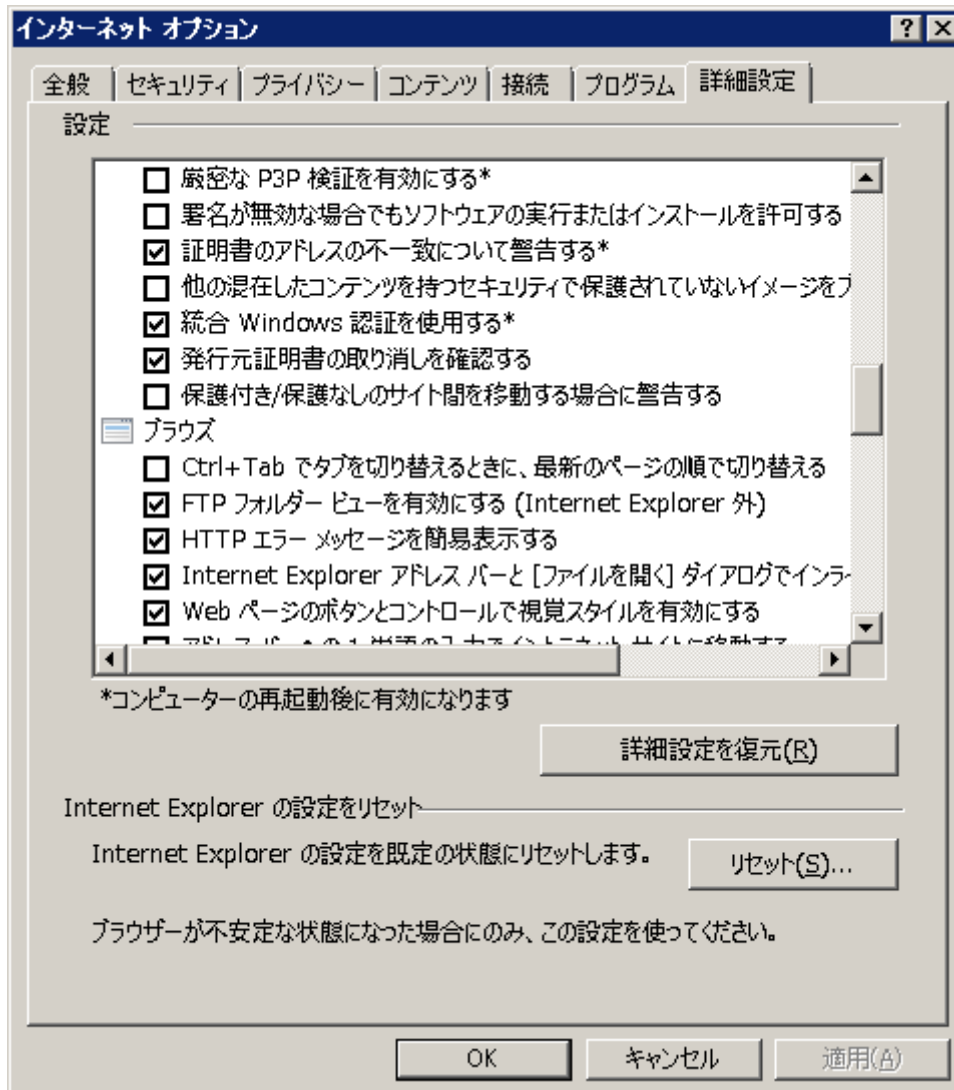


「サイト」ボタンをクリックして開いたダイアログの「詳細設定」ボタンをクリックすると、以下のようなダイアログが表示されます。

ここに OpenAM サーバーの URL を追加して下さい。



「詳細設定」タブをクリックし、「統合 Windows 認証を使用する」にチェックが入っていることを確認して下さい。



以上で、クライアントの設定は完了です。

## 1 2. 動作確認

それでは実際に動作確認をしてみましょう。

Active Directory に作成した一般ユーザー「test」で、Windows にログインします。その際のドメインは「example.local」になるので、ユーザーID は「test¥example.local」になります。Windows にログインしたら、OpenAM (<http://sso1.example.com:8080/openam>) の URI にアクセスします。全ての設定に問題が無ければ、ログイン画面は表示されず、以下のようなユーザープロフィール画面が表示されます。

### 13. トラブルシューティングの方法

Windows デスクトップ認証が正常に動作しない場合、まずは OpenAM のデバッグログを確認して下さい。デバッグログの出力先は、管理コンソールの **設定 > サーバーおよびサイト > [サーバー名] > 一般** の「デバッグ」セクションで確認できます。

OpenAM - Mozilla Firefox

OpenAM

sso1.example.com:8080/openam/service/ServerSite? Invalid initial he

親サイト: なし

先頭に戻る

#### システム

ベースインストールディレクトリ: /usr/share/tomcat6/openam  
製品のデータが存在するベースディレクトリ。(プロパティ名: com.ipplanet.services.configpath)

デフォルトのロケール: en\_US  
製品のデフォルトのロケール。(プロパティ名: com.ipplanet.am.locale)

通知 URL:  
通知サービスエンドポイントの場所。これは、通常、製品の配備 URI または notificationsservice です。(プロパティ名: com.sun.identity.client.notification.url)

XML 検証: off  
XML 文書の解析時に検証が必要かどうかを指定します。(プロパティ名: com.ipplanet.am.util.xml.validating)

先頭に戻る

#### デバッグ

デバッグレベル: エラー  
製品のすべてのコンポーネントのデバッグレベル。(プロパティ名: com.ipplanet.services.debug.level)

デバッグファイルのマージ: オフ  
オン: デバッグデータをすべて 1 つのファイル (debug.out) に転送します。オフ: コンポーネントごとに個別のデバッグファイルを作成します (プロパティ名: com.sun.services.debug.mergeall)

デバッグディレクトリ: %BASE\_DIR%/SERVER\_URI%/debug  
デバッグファイルが存在するディレクトリ。(プロパティ名: com.ipplanet.services.debug.directory)

先頭に戻る

#### メールサーバー

メールサーバーのホスト名: localhost  
(プロパティ名: com.ipplanet.am.smtphost)

メールサーバーのポート番号: 25  
(プロパティ名: com.ipplanet.am.smtpport)

先頭に戻る

デバッグログから詳細な情報が得られない場合は、デバッグレベルをメッセージに変更して下さい。



Windows デスクトップ認証に関するログは、主に以下のファイルに出力されます。

debug/Authentication

このログを参照しても、原因が分からない場合は Wireshark などのパケット解析ツールで Kerberos 通信の内容を確認して下さい。

## 1 4. 付録 1 : Active Directory のインストールと設定

このセクションでは、Windows Server に Active Directory をインストールする手順を説明します。

 ここで記載されているのは、動作確認用の最小限のインストール、設定手順です。

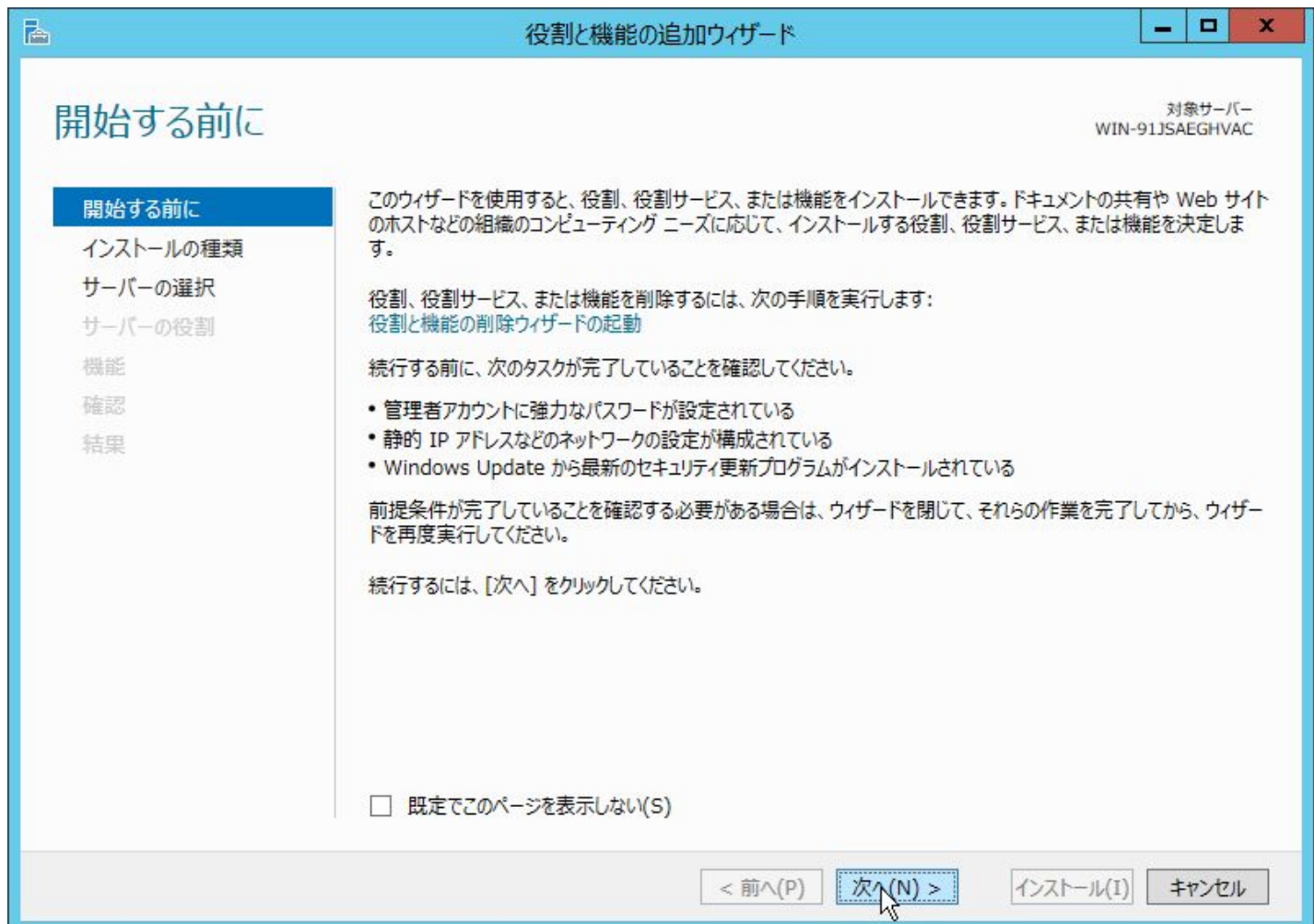
画面右下のサーバーマネージャーをクリックします。



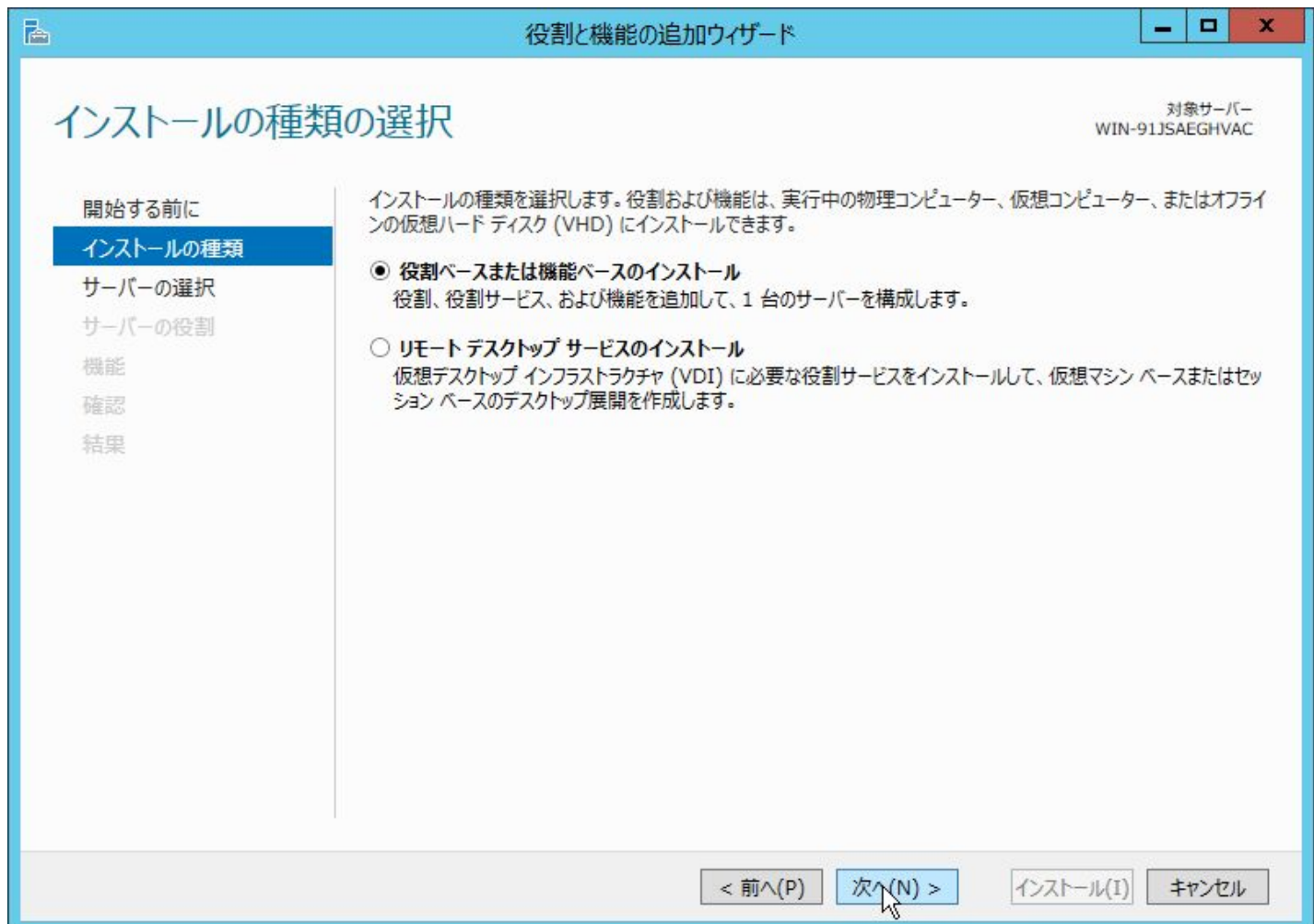
次のような画面が表示されるので、「② 役割と機能の追加」を選択します。



「次へ」ボタンをクリックします。



「役割ベースまたは機能ベースのインストール」を選択して、「次へ」ボタンをクリックします。



「サーバープールからサーバーを選択」を選択して、「次へ」ボタンをクリックします。

役割と機能の追加ウィザード

対象サーバーの選択

対象サーバー  
WIN-91JSAEGHVAC

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

機能

確認

結果

役割と機能をインストールするサーバーまたは仮想ハード ディスクを選択します。

☒ サーバー プールからサーバーを選択  
☐ 仮想ハード ディスクから選択

サーバー プール

フィルター:

名前	IP アドレス	オペレーティング システム
WIN-91JSAEGHVAC	192.168.1.8	Microsoft Windows Server 2012 R2 Standard 評価

<

|||

>

1 台のコンピューターが見つかりました

このページには、Windows Server 2012 を実行しており、サーバー マネージャーの [サーバーの追加] コマンドを使用して追加されたサーバーが表示されます。オフライン サーバーや、データ収集が完了していない、新たに追加されたサーバーは表示されません。

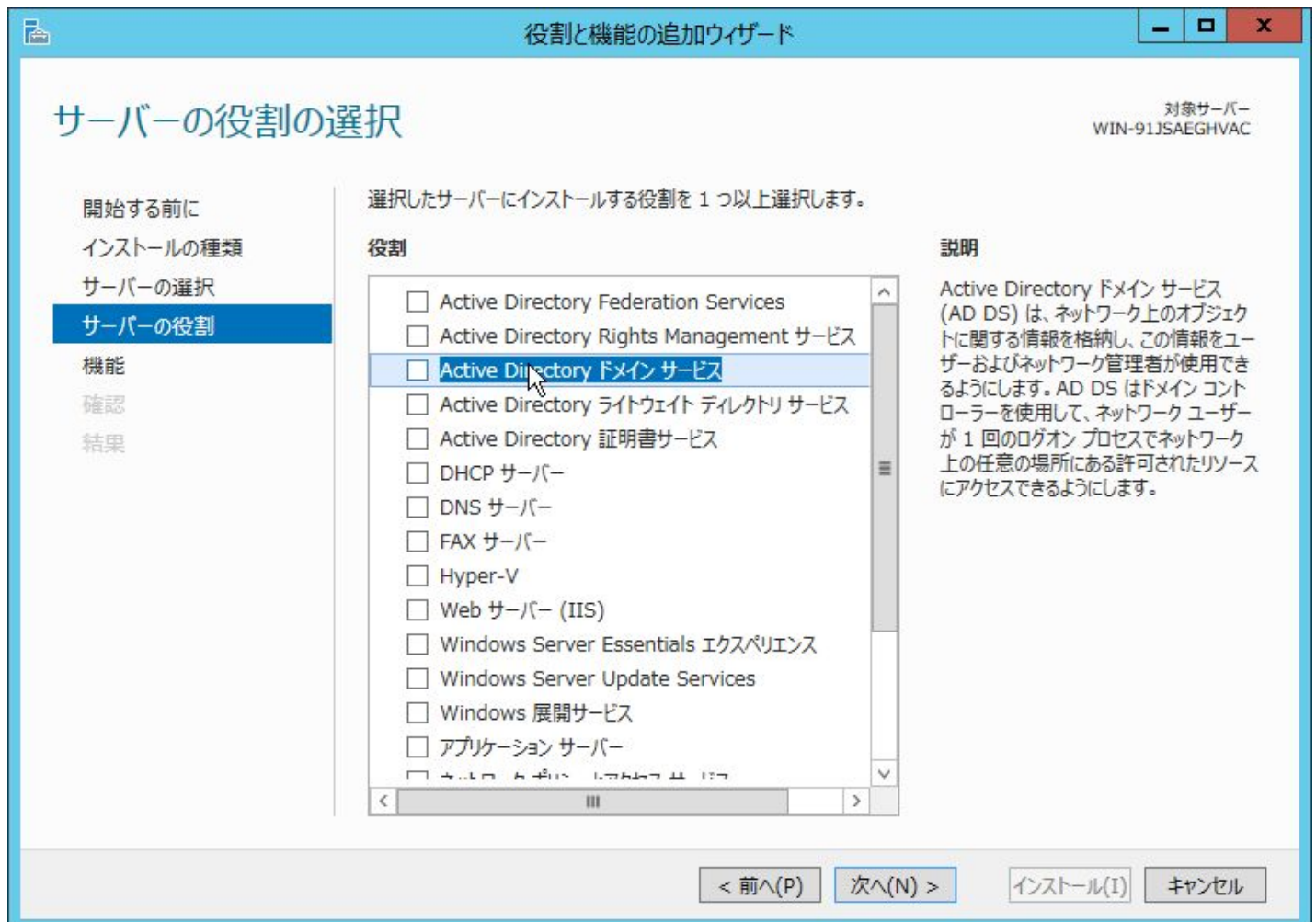
< 前へ(P)

**次へ(N) >**

インストール(I)

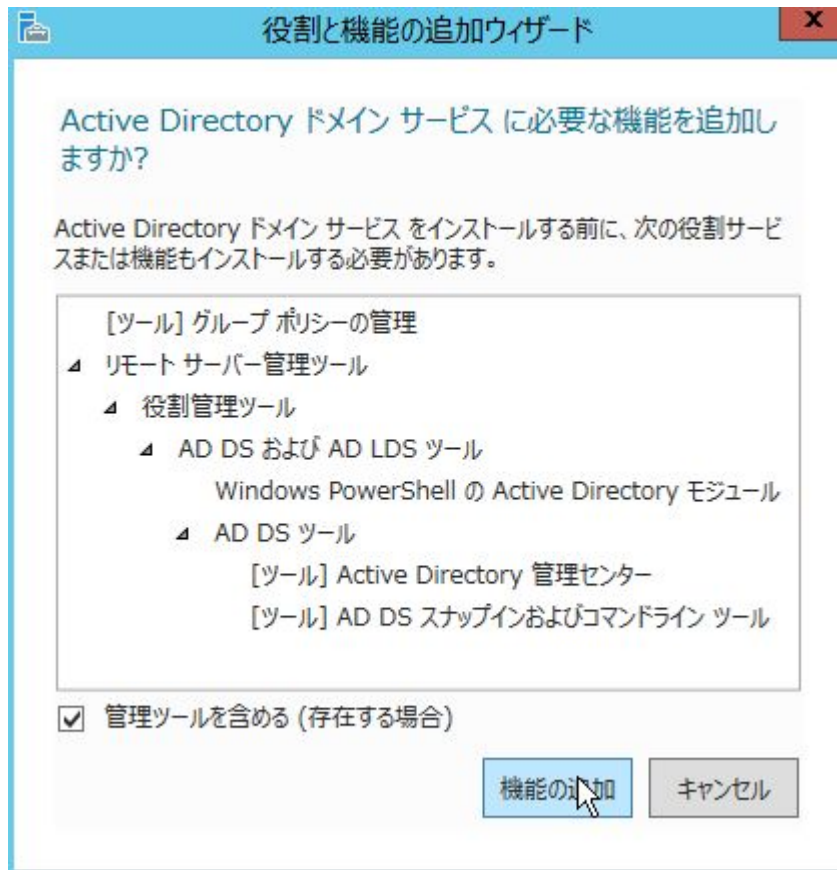
キャンセル

「Active Directory ドメインサービス」を選択します。

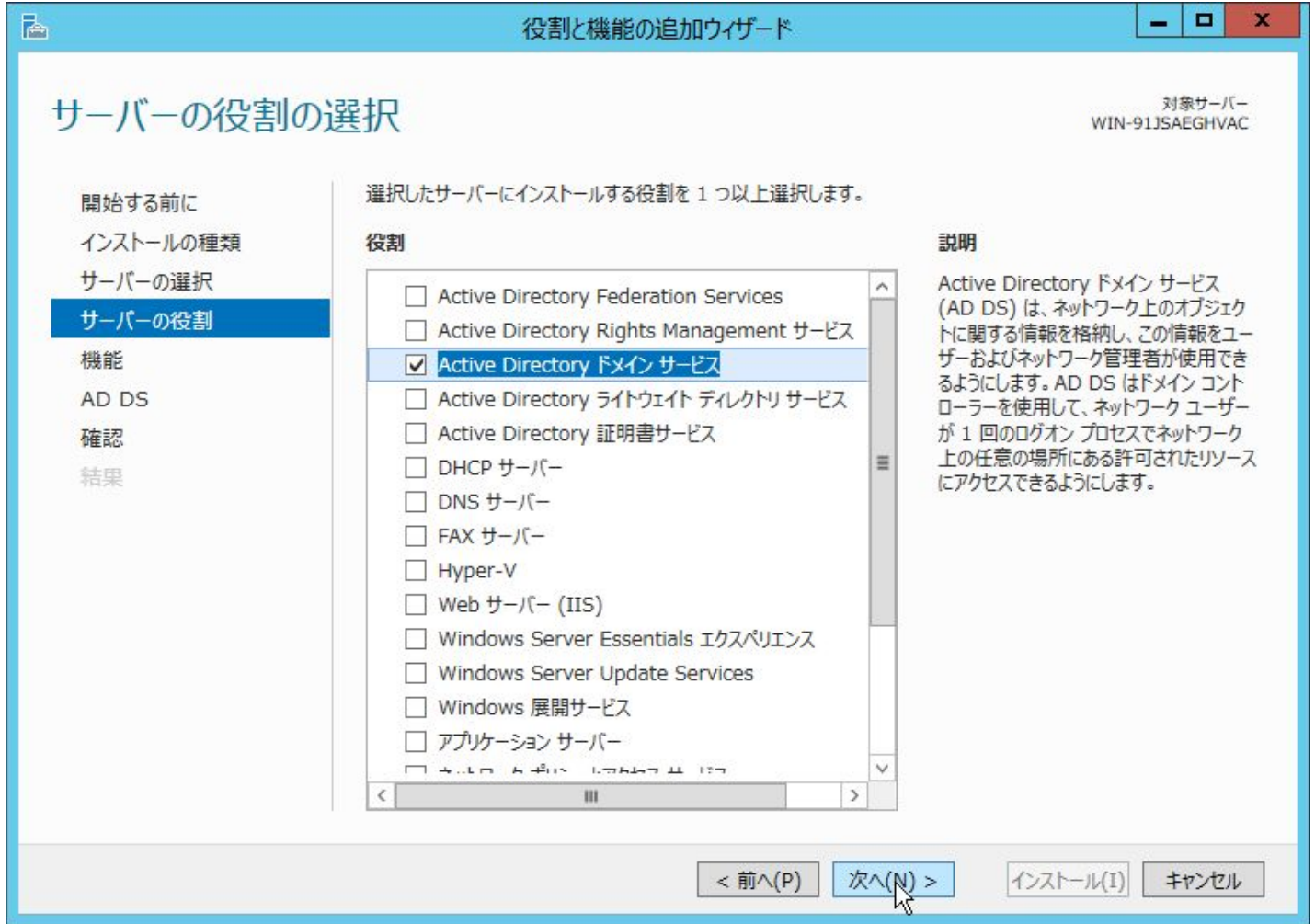




「役割と機能の追加ウィザード」が表示されるので、「管理ツールを含める（存在する場合）」にチェックした状態で、「機能の追加」ボタンをクリックします。

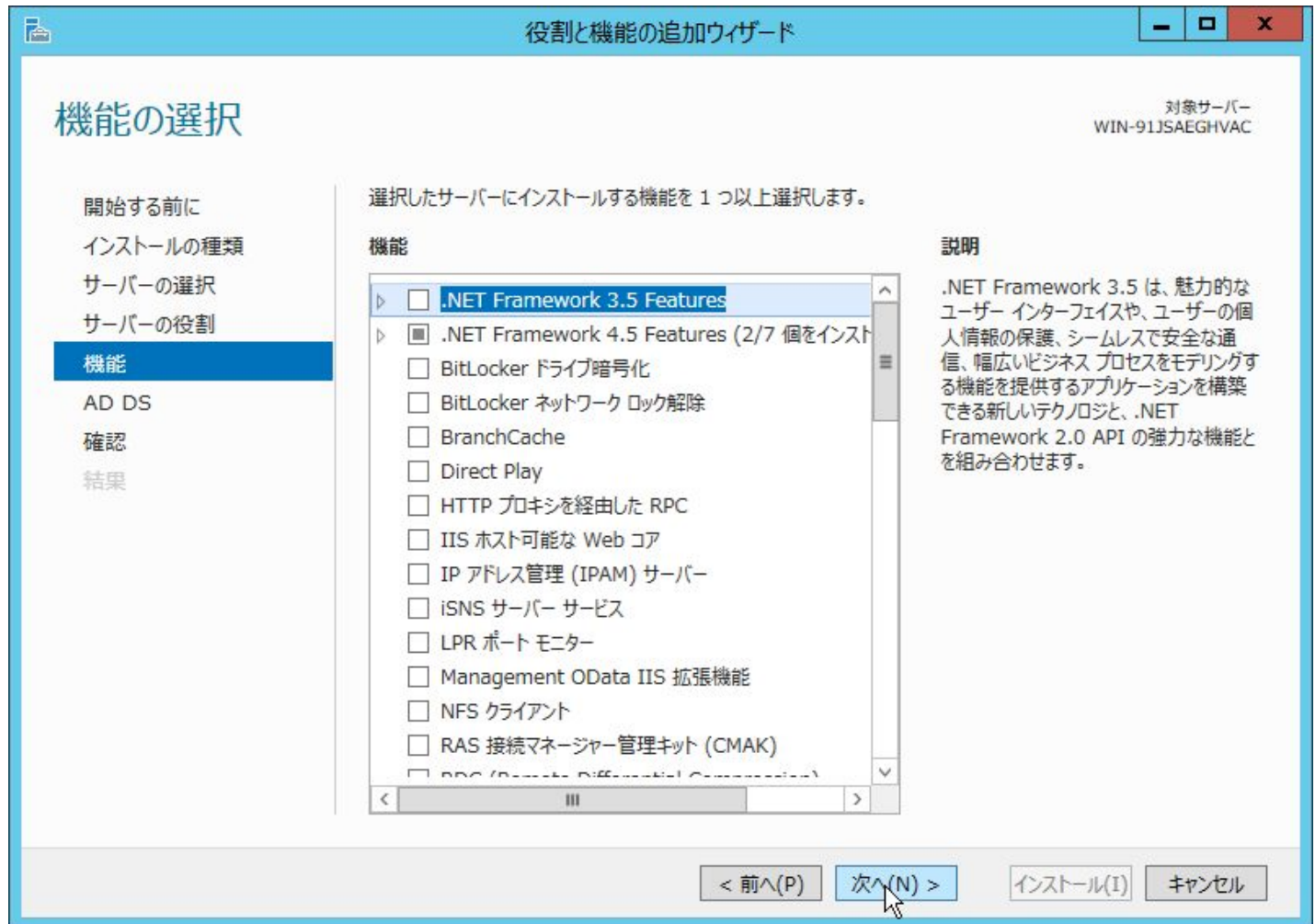


「次へ」ボタンをクリックします。

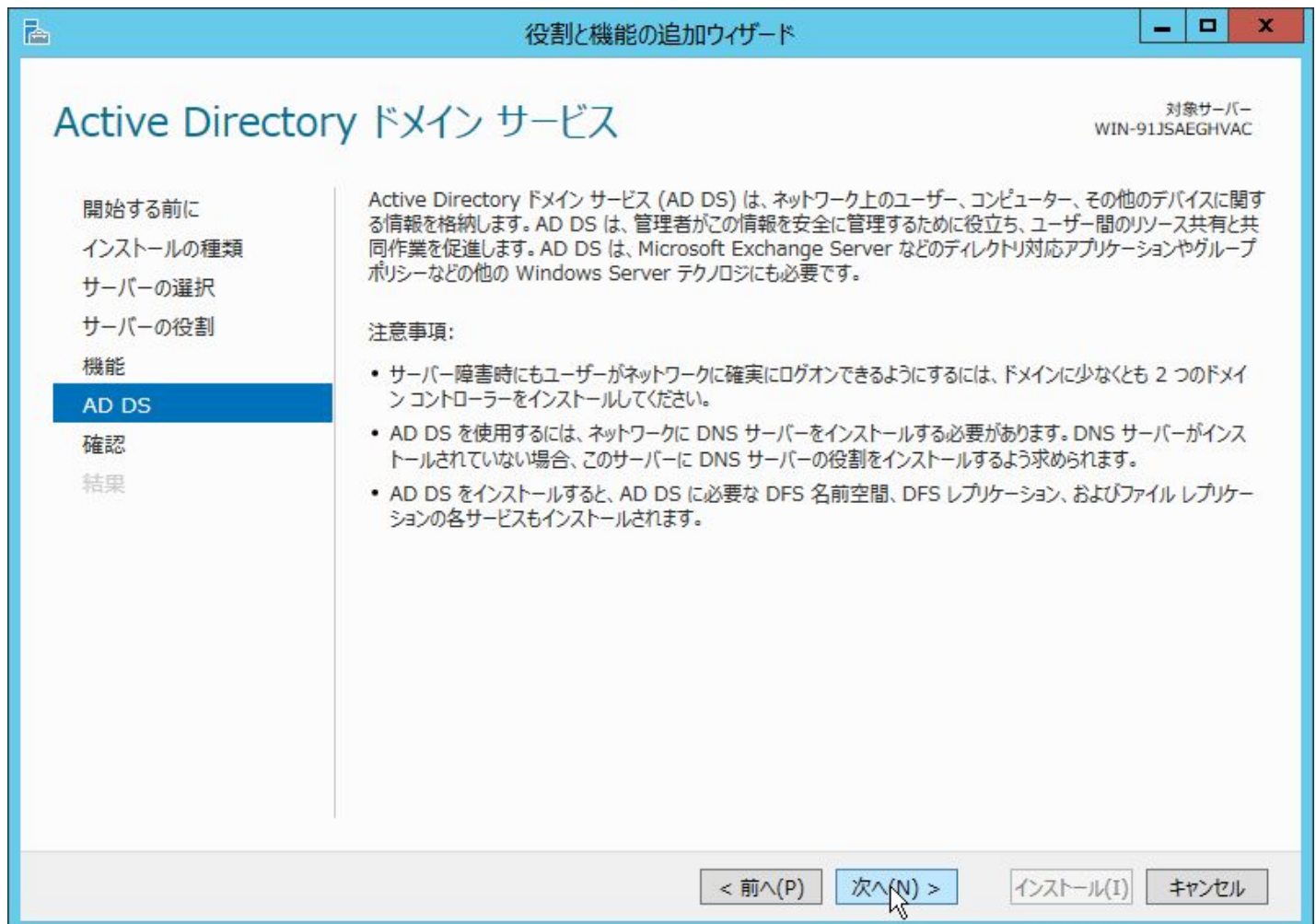




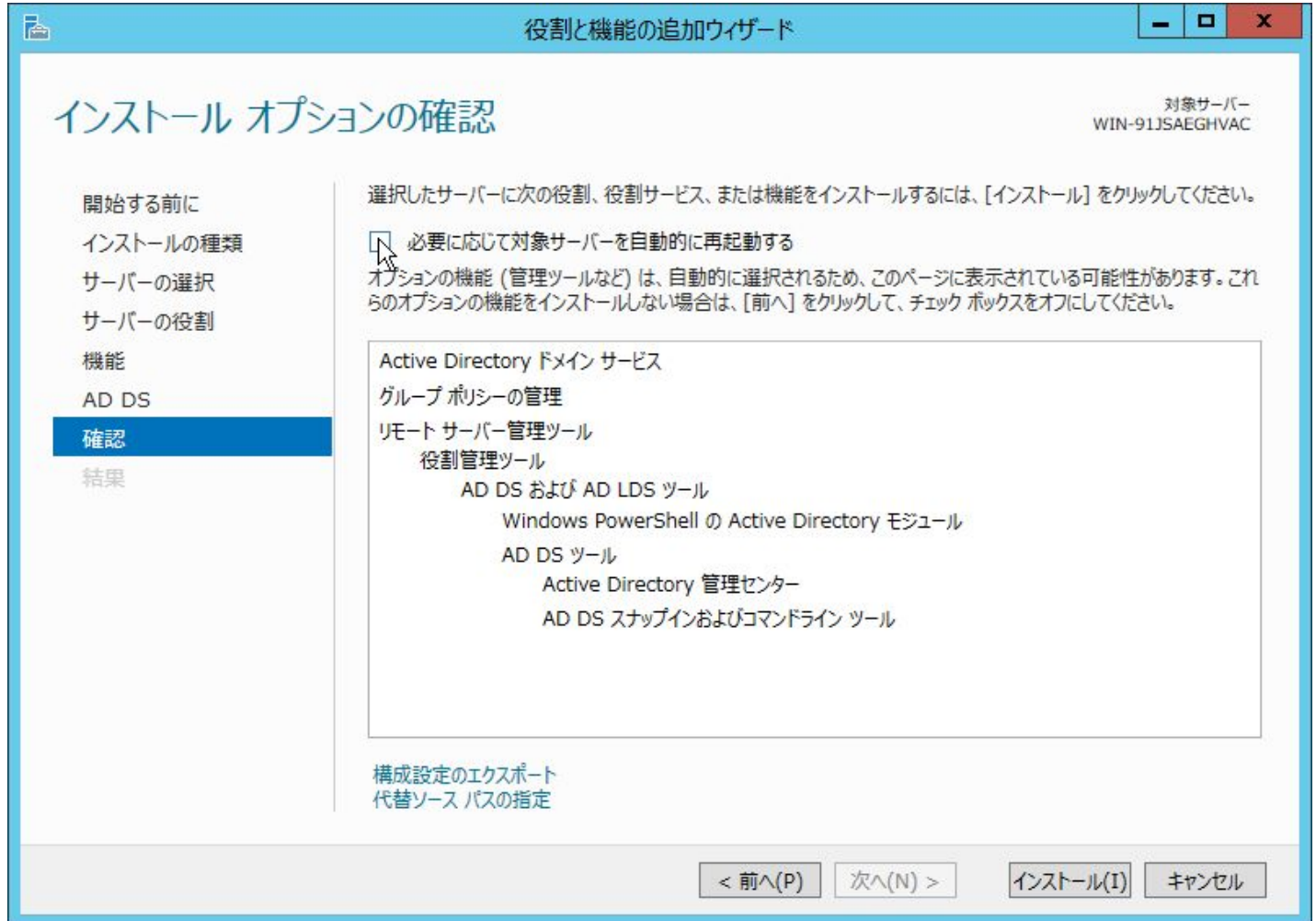
機能は追加せず、デフォルトのままで「次へ」ボタンをクリックします。



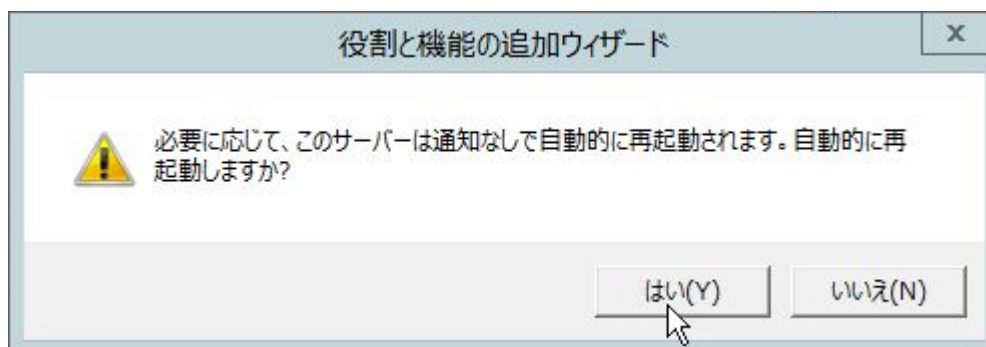
内容を確認して、「次へ」ボタンをクリックします。



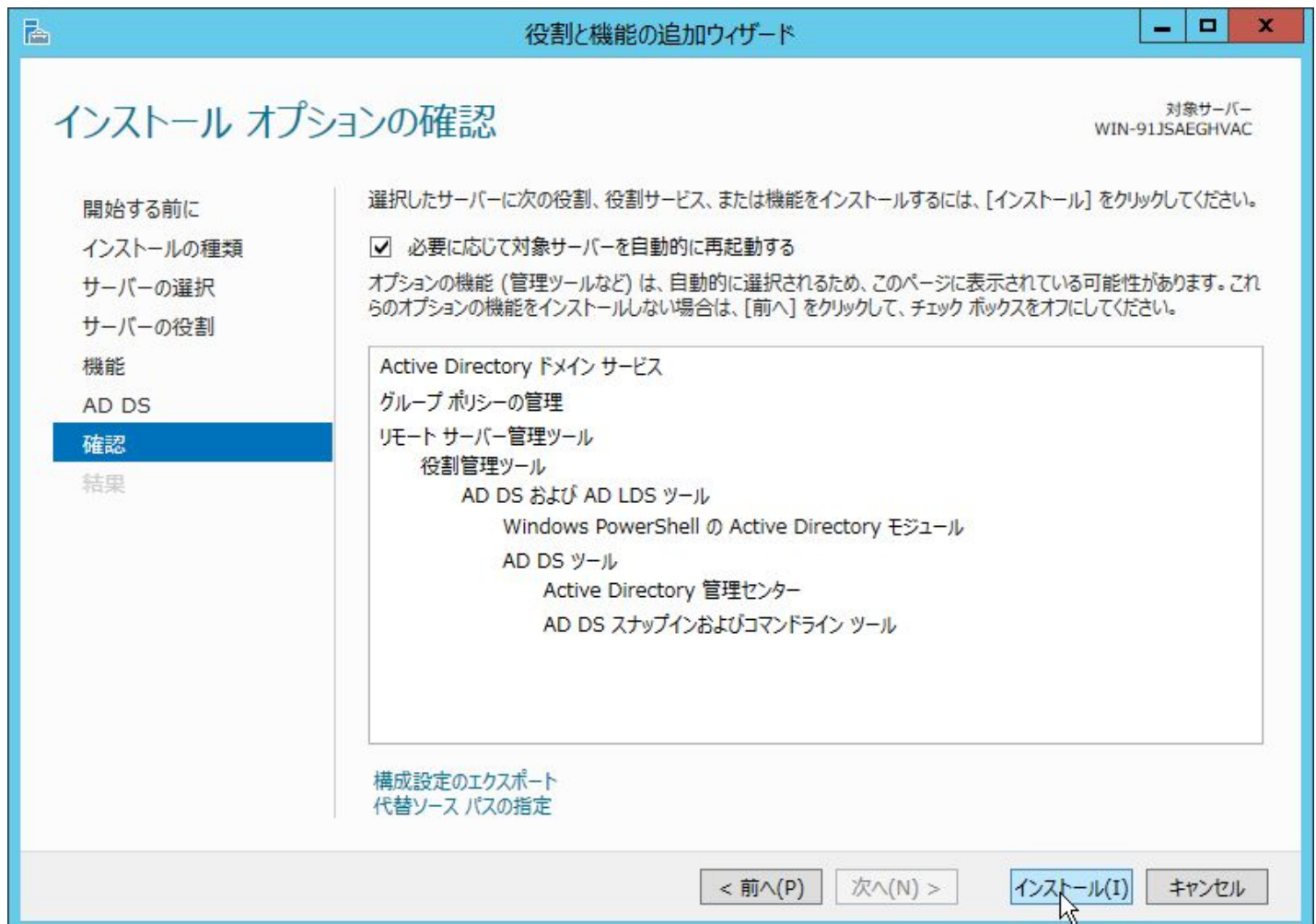
完了と同時に再起動する場合は「必要に応じて対象サーバーを自動的に再起動する」のチェックをクリックします。



確認のダイアログが表示されますので、「はい」ボタンをクリックしてチェックを有効にします。

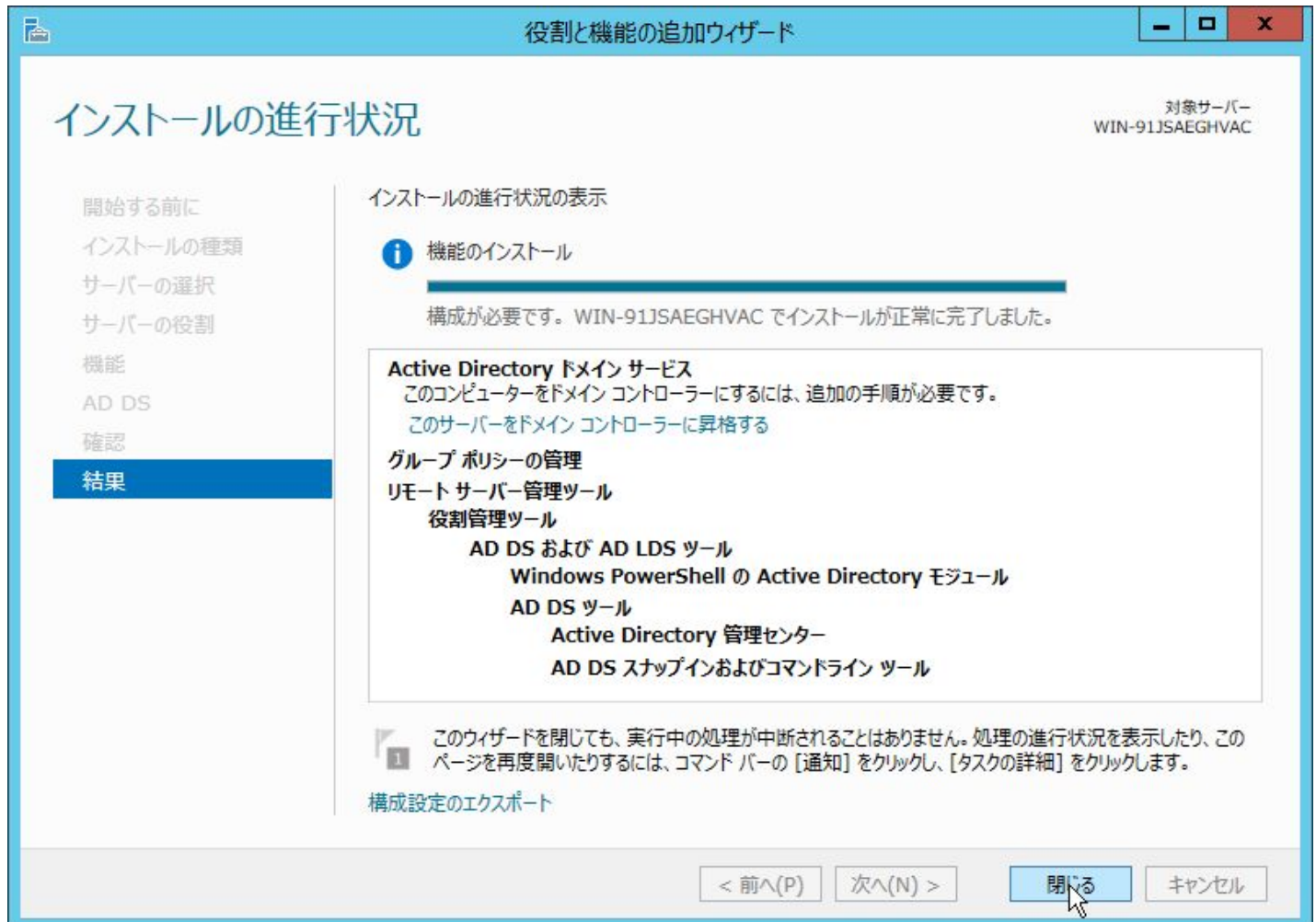


「インストール」ボタンをクリックして、インストールを開始します。





完了したら、「閉じる」ボタンをクリックします。インストール時に「必要に応じて対象サーバーを自動的に再起動する」をチェックしていた場合は自動的に再起動します。



再起動したら、再度「サーバーマネージャー」を起動して下さい。画面上部の旗のマークのところに警告マークがあるので、この中の「このサーバーをドメインコントローラーに昇格する」のリンクをクリックすると、Active Directory ドメインサービスの設定画面が表示されます。



「新しいフォレストを追加する」を選択して、「ルートドメイン名」に適切なドメイン名(本書の構成の場合は example.local)を入力します。完了したら、「次へ」ボタンをクリックして下さい。

Active Directory ドメイン サービス構成ウィザード

ターゲット サーバー  
WIN-91JSAEGHVAC

### 配置構成

配置構成

- ドメイン コントローラー オプ...
- 追加オプション
- パス
- オプションの確認
- 前提条件のチェック
- インストール
- 結果

配置操作を選択してください

- ☐ 既存のドメインにドメイン コントローラーを追加する(D)
- ☐ 新しいドメインを既存のフォレストに追加する(E)
- ☒ 新しいフォレストを追加する(F)

この操作のドメイン情報を指定してください

ルート ドメイン名(R):

詳細 配置構成

< 前へ(P)    次へ(N) >    インストール(I)    キャンセル

パスワードを入力して、「次へ」ボタンをクリックします。

The screenshot shows the 'Active Directory ドメイン サービス構成ウィザード' (Active Directory Domain Services Configuration Wizard) window. The title bar includes standard Windows window controls. The main window has a light blue header with the title 'ドメイン コントローラー オプション' (Domain Controller Options) on the left and 'ターゲット サーバー WIN-91JSAEGHVAC' (Target Server WIN-91JSAEGHVAC) on the right. A left-hand navigation pane lists the steps: '配置構成' (Configuration), 'ドメイン コントローラー オプション' (selected), 'DNS オプション' (DNS Options), '追加オプション' (Additional Options), 'パス' (Path), 'オプションの確認' (Verify Options), '前提条件のチェック' (Check Prerequisites), 'インストール' (Install), and '結果' (Results). The main content area is titled '新しいフォレストおよびルート ドメインの機能レベルを選択してください' (Select the functional level for the new forest and root domain). It contains two dropdown menus, both set to 'Windows Server 2012 R2'. Below these, it says 'ドメイン コントローラーの機能を指定してください' (Specify the features for the domain controller) and lists three options: 'ドメイン ネーム システム (DNS) サーバー(O)' (checked), 'グローバル カタログ (GC)(G)' (checked), and '読み取り専用ドメイン コントローラー (RODC)(R)' (unchecked). Further down, it prompts for the 'ディレクトリ サービス復元モード (DSRM) のパスワードを入力してください' (Enter the password for the Directory Service Restore Mode (DSRM)). There are two password input fields, both masked with dots. At the bottom of the window, there are four buttons: '< 前へ(P)' (Previous), '次へ(N) >' (Next, which is highlighted with a mouse cursor), 'インストール(I)' (Install), and 'キャンセル' (Cancel).

Active Directory ドメイン サービス構成ウィザード

ドメイン コントローラー オプション

ターゲット サーバー  
WIN-91JSAEGHVAC

配置構成  
ドメイン コントローラー オプション  
DNS オプション  
追加オプション  
パス  
オプションの確認  
前提条件のチェック  
インストール  
結果

新しいフォレストおよびルート ドメインの機能レベルを選択してください

フォレストの機能レベル: Windows Server 2012 R2

ドメインの機能レベル: Windows Server 2012 R2

ドメイン コントローラーの機能を指定してください

☒ ドメイン ネーム システム (DNS) サーバー(O)  
☒ グローバル カタログ (GC)(G)  
☐ 読み取り専用ドメイン コントローラー (RODC)(R)

ディレクトリ サービス復元モード (DSRM) のパスワードを入力してください

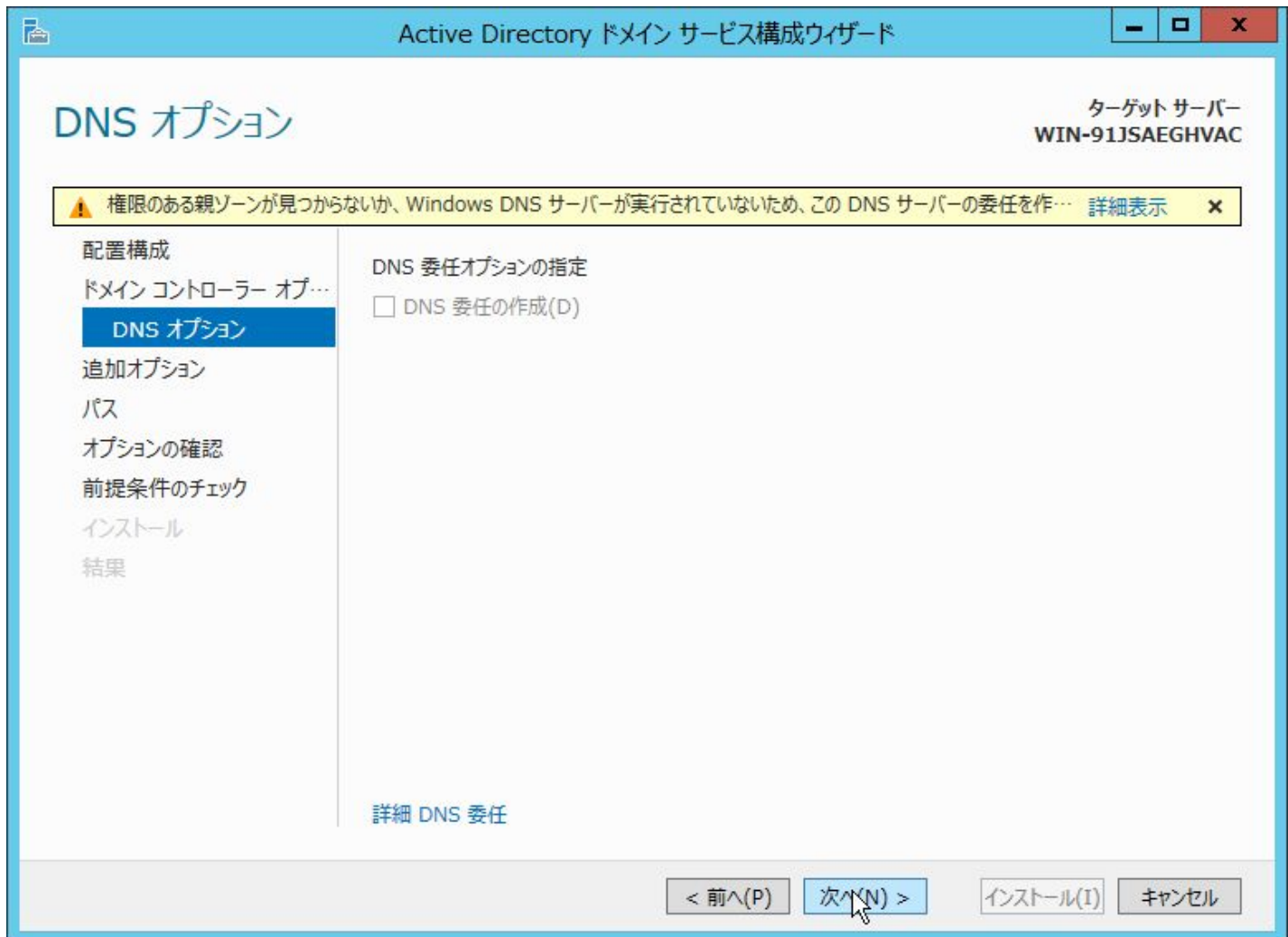
パスワード(D):  
パスワードの確認入力(C):

詳細 ドメイン コントローラー オプション

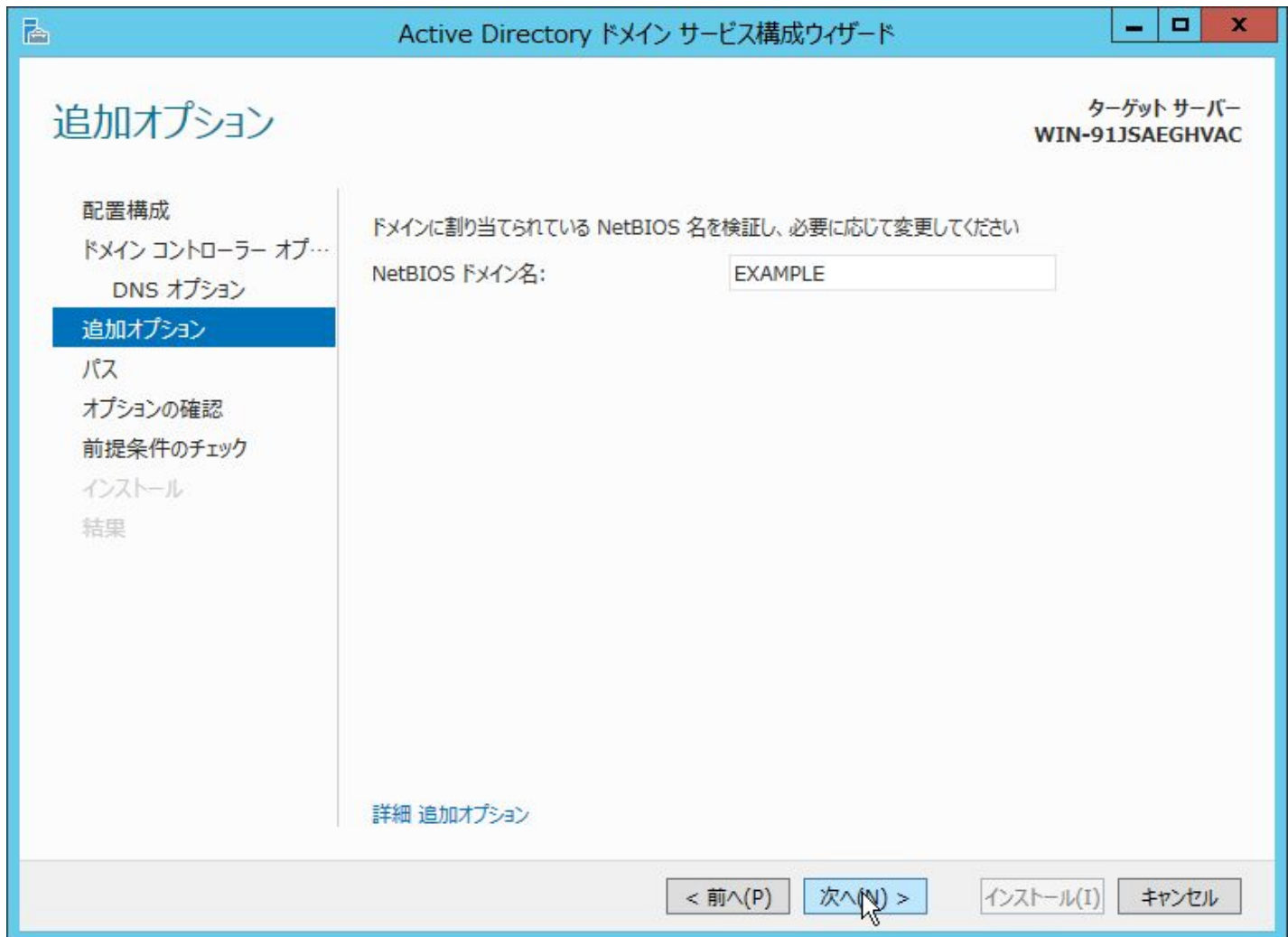
< 前へ(P) 次へ(N) > インストール(I) キャンセル



そのまま「次へ」ボタンをクリックします。



デフォルトのまま（本書の構成の場合は EXAMPLE）、「次へ」ボタンをクリックします。



データベースファイルなどの出力先を変更する場合は、変更して「次へ」ボタンをクリックして下さい。

Active Directory ドメイン サービス構成ウィザード

ターゲット サーバー  
WIN-91JSAEGHVAC

パス

配置構成  
ドメイン コントローラー オブ…  
DNS オプション  
追加オプション  
**パス**  
オプションの確認  
前提条件のチェック  
インストール  
結果

AD DS データベース、ログ ファイル、および SYSVOL の場所を指定してください

データベースのフォルダー(D): C:\Windows\NTDS ...

ログ ファイルのフォルダー(L): C:\Windows\NTDS ...

SYSVOL フォルダー(Y): C:\Windows\SYSVOL ...

詳細 Active Directory のパス

< 前へ(P) 次へ(N) > インストール(I) キャンセル

内容を確認して、「次へ」ボタンをクリックします。

The screenshot shows the 'Active Directory ドメイン サービス構成ウィザード' (Active Directory Domain Services Configuration Wizard) window. The title bar includes standard Windows window controls. The main window has a light blue header and a sidebar on the left. The sidebar contains a list of steps: '配置構成' (Configuration), 'ドメイン コントローラー オプション' (Domain Controller Options), 'DNS オプション' (DNS Options), '追加オプション' (Additional Options), 'パス' (Pass), 'オプションの確認' (Options Confirmation - currently selected), '前提条件のチェック' (Prerequisites Check), 'インストール' (Install), and '結果' (Results). The main area is titled 'オプションの確認' (Options Confirmation) and shows the target server as 'WIN-91JSAEGHVAC'. It lists the following configuration details: '新しいフォレストの最初の Active Directory ドメイン コントローラーとしてこのサーバーを構成します。' (Configure this server as the first Active Directory domain controller for the new forest), '新しいドメイン名は "example.local" です。これは新しいフォレスト名にもなります。' (The new domain name is "example.local", which will also be the new forest name), 'ドメインの NetBIOS 名: EXAMPLE' (Domain NetBIOS name: EXAMPLE), 'フォレストの機能レベル: Windows Server 2012 R2' (Forest functional level: Windows Server 2012 R2), and 'ドメインの機能レベル: Windows Server 2012 R2' (Domain functional level: Windows Server 2012 R2). Under '追加オプション:' (Additional options:), it shows 'グローバル カタログ: はい' (Global catalog: Yes), 'DNS サーバー: はい' (DNS server: Yes), and 'DNS 委任の作成: いいえ' (Create DNS delegation: No). At the bottom of the main area, it states 'これらの設定は、追加のインストールを自動化する Windows PowerShell スクリプトにエクスポートできます' (These settings can be exported to a Windows PowerShell script to automate additional installation) with a 'スクリプトの表示(V)' (View script(V)) button. A link '詳細 インストール オプション' (More install options) is also present. The bottom of the window features four buttons: '< 前へ(P)' (Previous), '次へ(N) >' (Next - highlighted with a mouse cursor), 'インストール(I)' (Install), and 'キャンセル' (Cancel).

Active Directory ドメイン サービス構成ウィザード

ターゲット サーバー  
WIN-91JSAEGHVAC

### オプションの確認

配置構成  
ドメイン コントローラー オプション  
DNS オプション  
追加オプション  
パス  
オプションの確認  
前提条件のチェック  
インストール  
結果

次の選択を確認してください:

新しいフォレストの最初の Active Directory ドメイン コントローラーとしてこのサーバーを構成します。

新しいドメイン名は "example.local" です。これは新しいフォレスト名にもなります。

ドメインの NetBIOS 名: EXAMPLE

フォレストの機能レベル: Windows Server 2012 R2

ドメインの機能レベル: Windows Server 2012 R2

追加オプション:

グローバル カタログ: はい

DNS サーバー: はい

DNS 委任の作成: いいえ

これらの設定は、追加のインストールを自動化する Windows PowerShell スクリプトにエクスポートできます

スクリプトの表示(V)

詳細 インストール オプション

< 前へ(P)    次へ(N) >    インストール(I)    キャンセル

「インストール」ボタンをクリックして、インストールを開始します。



完了すると自動的に Windows Server が再起動します。

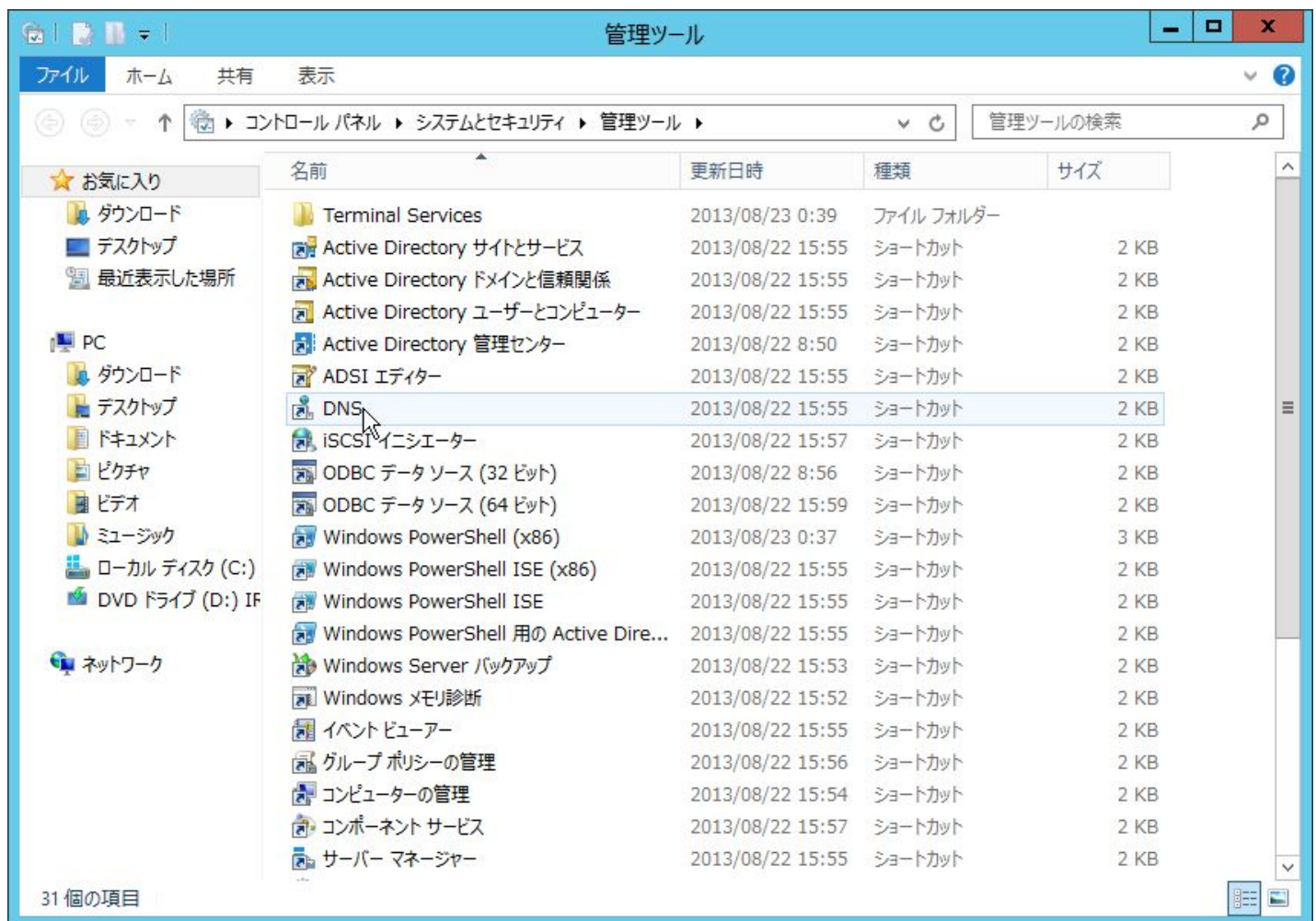
以上で、Active Directory サーバーの設定は完了です。



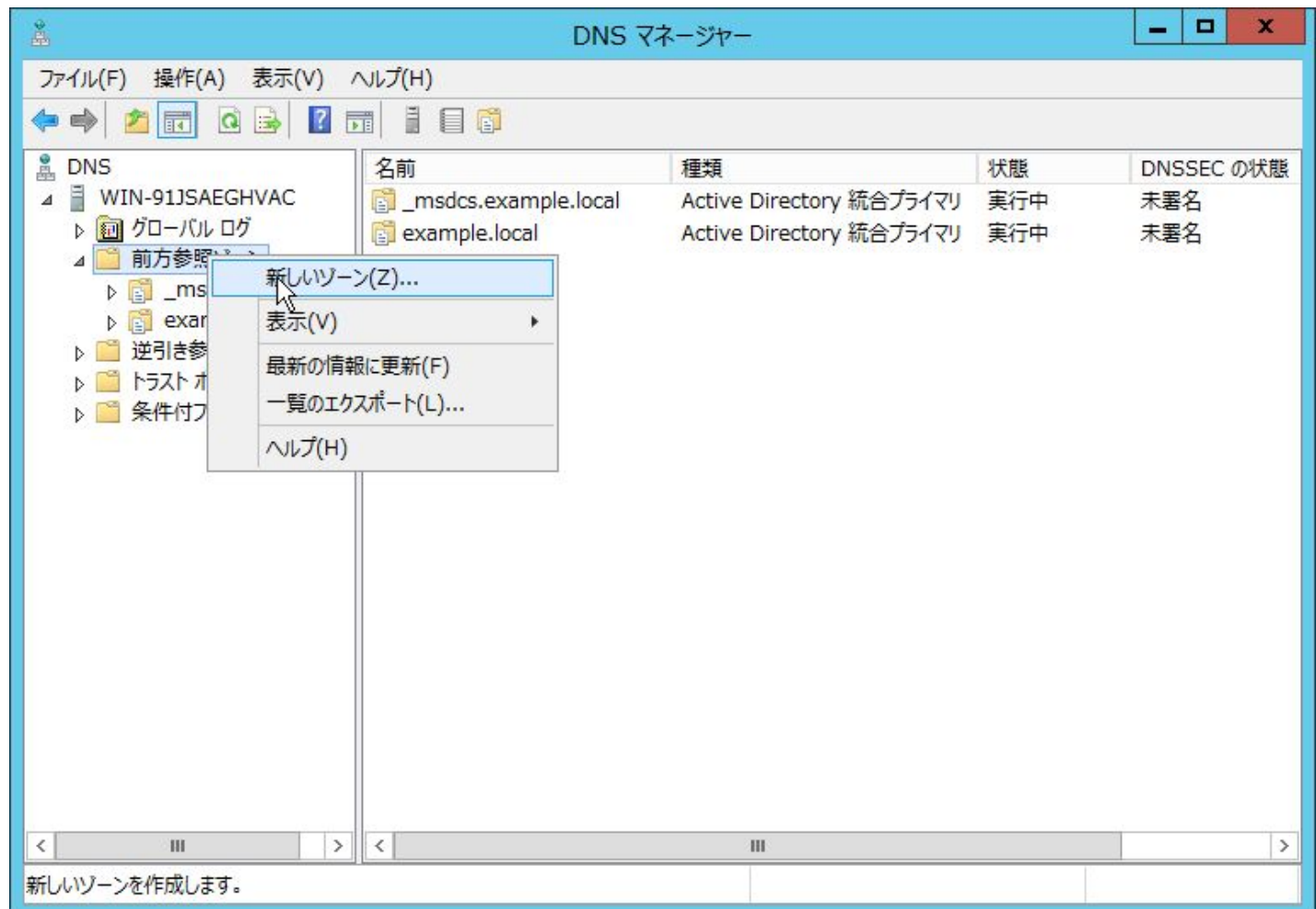
## 15. 付録2：DNS サーバーの設定

各 Windows クライアントから、OpenAM サーバーの名前解決ができるように、前方参照ゾーンに Host (A) レコードを、逆引き参照ゾーンに Pointer (PTR) レコードを追加します。

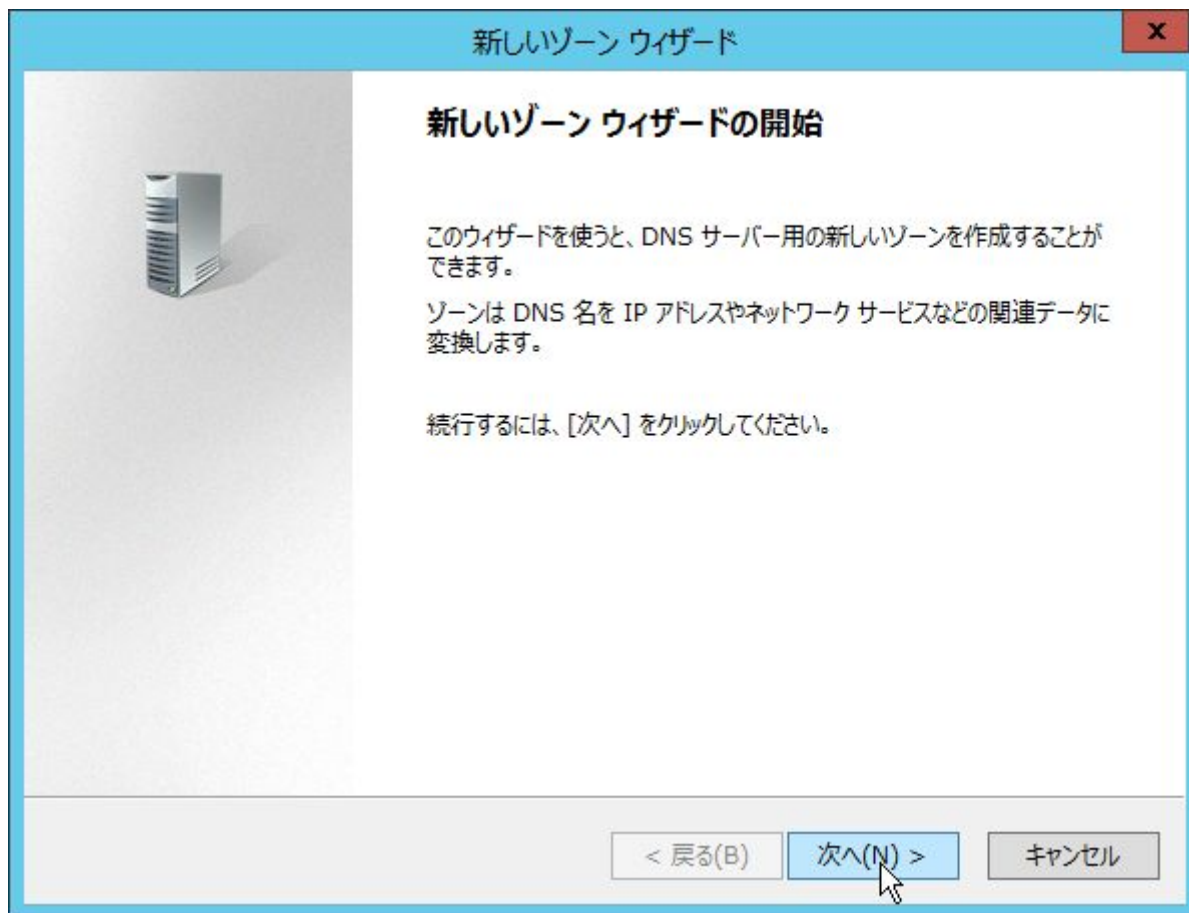
まずは、前方参照ゾーンに A レコードを追加します。「管理ツール」 > 「DNS」より、DNS マネージャーを起動して下さい。



起動したら、「前方参照ゾーン」を右クリックして、新しいゾーンを追加します。



「次へ」ボタンをクリックします。





「プライマリゾーン」を選択して、「次へ」ボタンをクリックします。

新しいゾーン ウィザード

**ゾーンの種類**  
DNS サーバーは各種のゾーンと記憶域をサポートします。

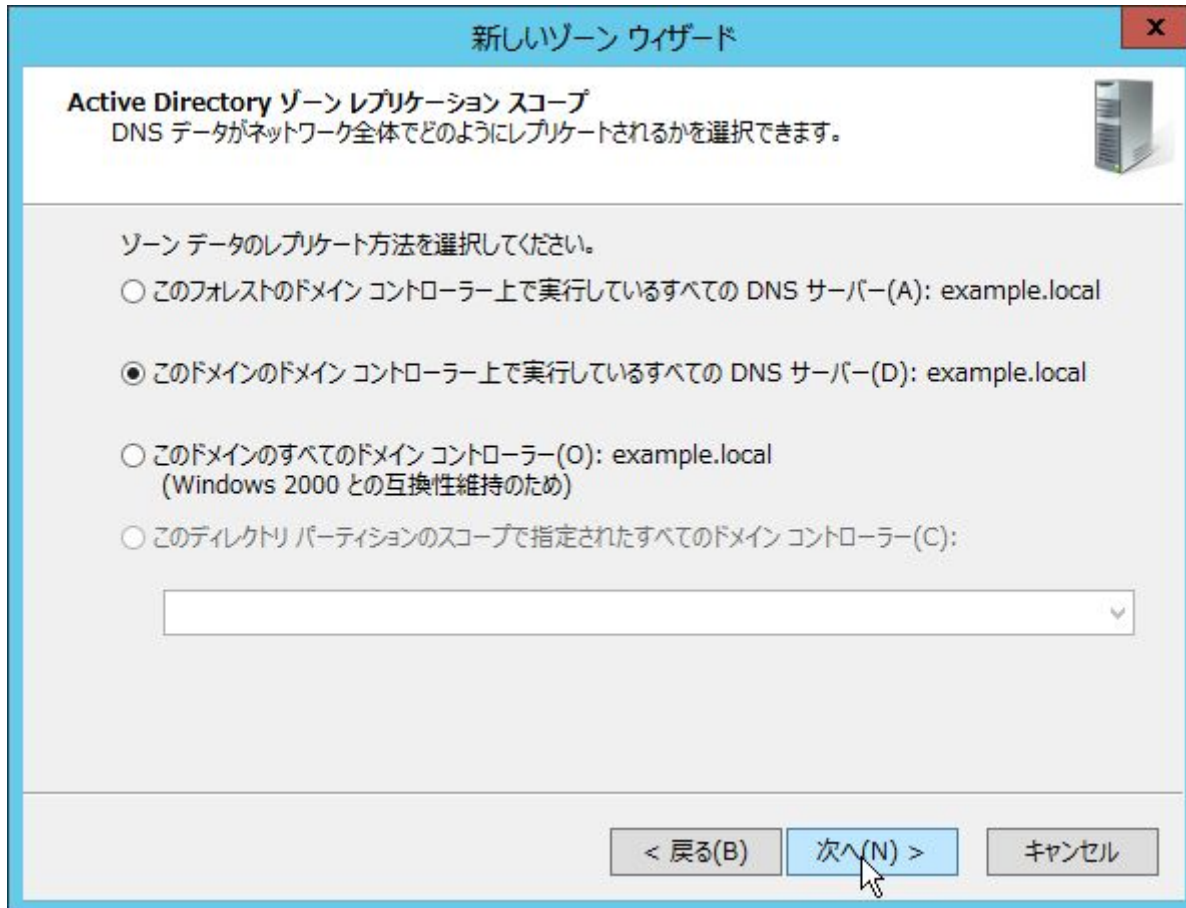
作成するゾーンの種類を指定してください:

- ☒ **プライマリ ゾーン(P)**  
このサーバーで直接更新ができるゾーンのコピーを作成します。
- ☐ **セカンダリ ゾーン(S)**  
ほかのサーバーに存在するゾーンのコピーを作成します。このオプションは、プライマリ サーバーの処理  
負荷の均衡化を助け、フォールト トレランスを提供します。
- ☐ **スタブ ゾーン(U)**  
ネーム サーバー (NS) 及び、SOA (Start of Authority) のみを含むゾーンのコピーを作成しま  
す (グルー ホスト (A) レコードも含めることが可能です)。スタブ ゾーンを含むサーバーは、そのゾーン  
に対して権威を持っていません。

☒ **Active Directory にゾーンを格納する(A)**  
(DNS サーバーが書き込み可能ドメイン コントローラーの場合のみ利用可能です)

< 戻る(B)    次へ(N) >    キャンセル

「このドメインのドメインコントローラー上で実行しているすべての DNS サーバー: example.local」を選択して、「次へ」ボタンをクリックします。



新しいゾーン ウィザード

**Active Directory ゾーン レプリケーション スコープ**  
DNS データがネットワーク全体でどのようにレプリケートされるかを選択できます。

ゾーン データのレプリケート方法を選択してください。

☐ このフォレストのドメイン コントローラー上で実行しているすべての DNS サーバー(A): example.local

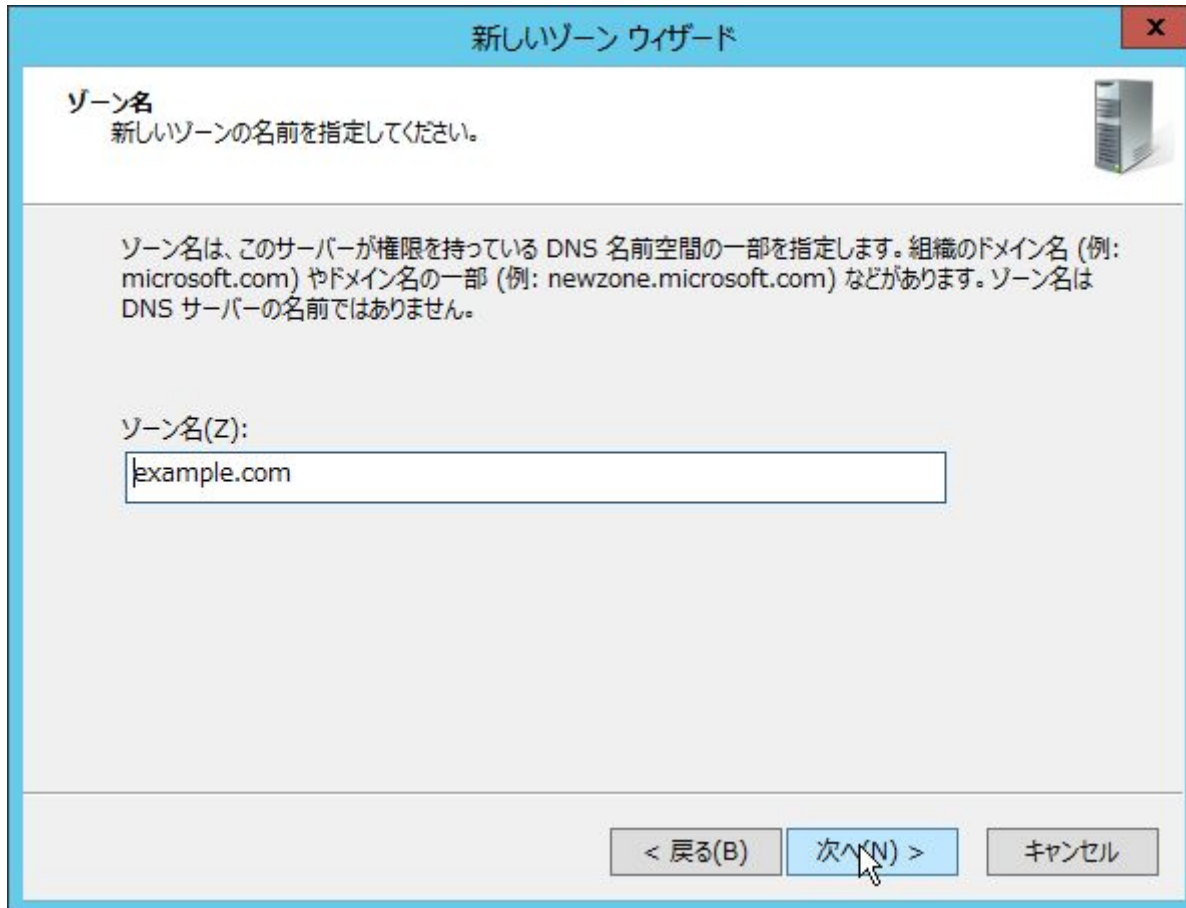
☒ このドメインのドメイン コントローラー上で実行しているすべての DNS サーバー(D): example.local

☐ このドメインのすべてのドメイン コントローラー(O): example.local  
(Windows 2000 との互換性維持のため)

☐ このディレクトリ パーティションの範囲で指定されたすべてのドメイン コントローラー(C):

< 戻る(B)    次へ(N) >    キャンセル

「ゾーン名」に OpenAM の Cookie ドメインから先頭の「.」を除いた値を入力して、「次へ」ボタンをクリックします。



新しいゾーン ウィザード

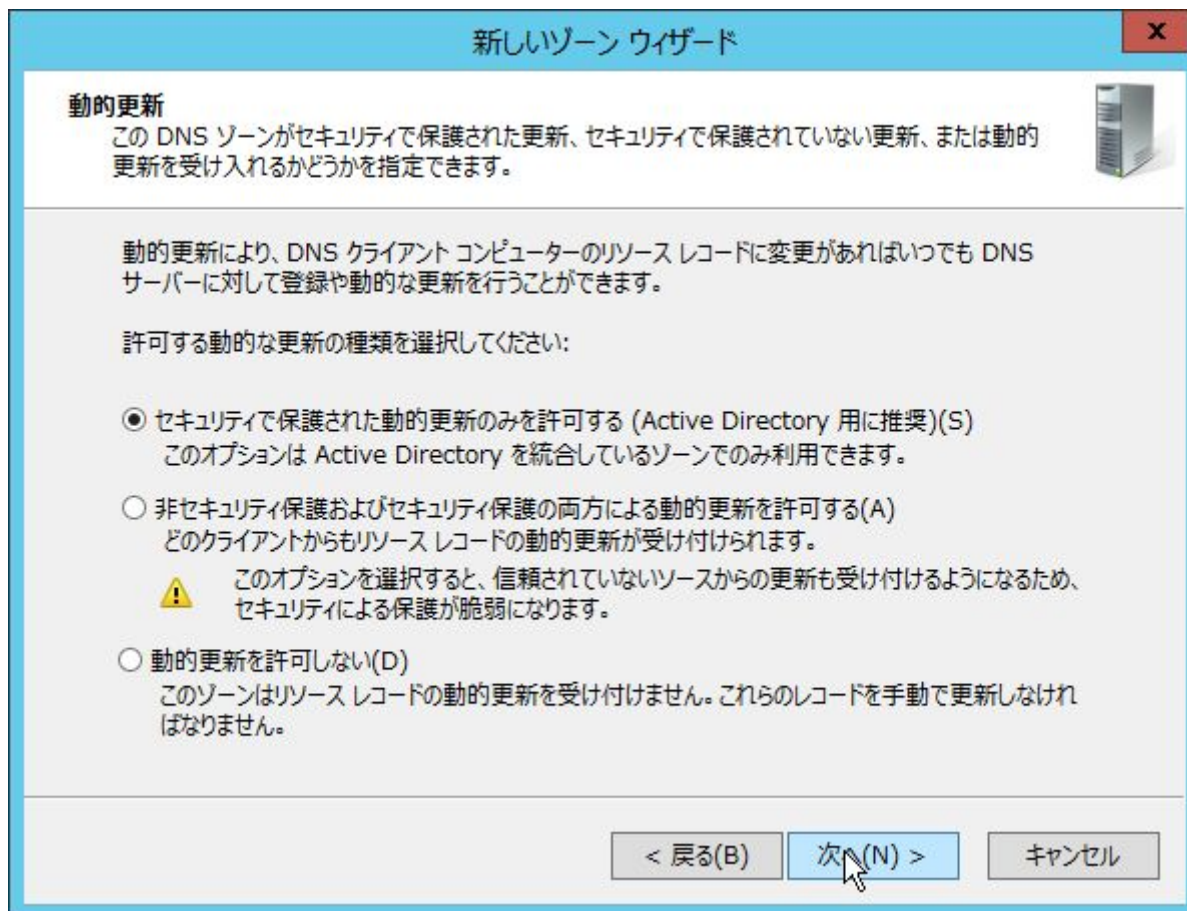
**ゾーン名**  
新しいゾーンの名前を指定してください。

ゾーン名は、このサーバーが権限を持っている DNS 名前空間の一部を指定します。組織のドメイン名 (例: microsoft.com) やドメイン名の一部 (例: newzone.microsoft.com) があります。ゾーン名は DNS サーバーの名前ではありません。

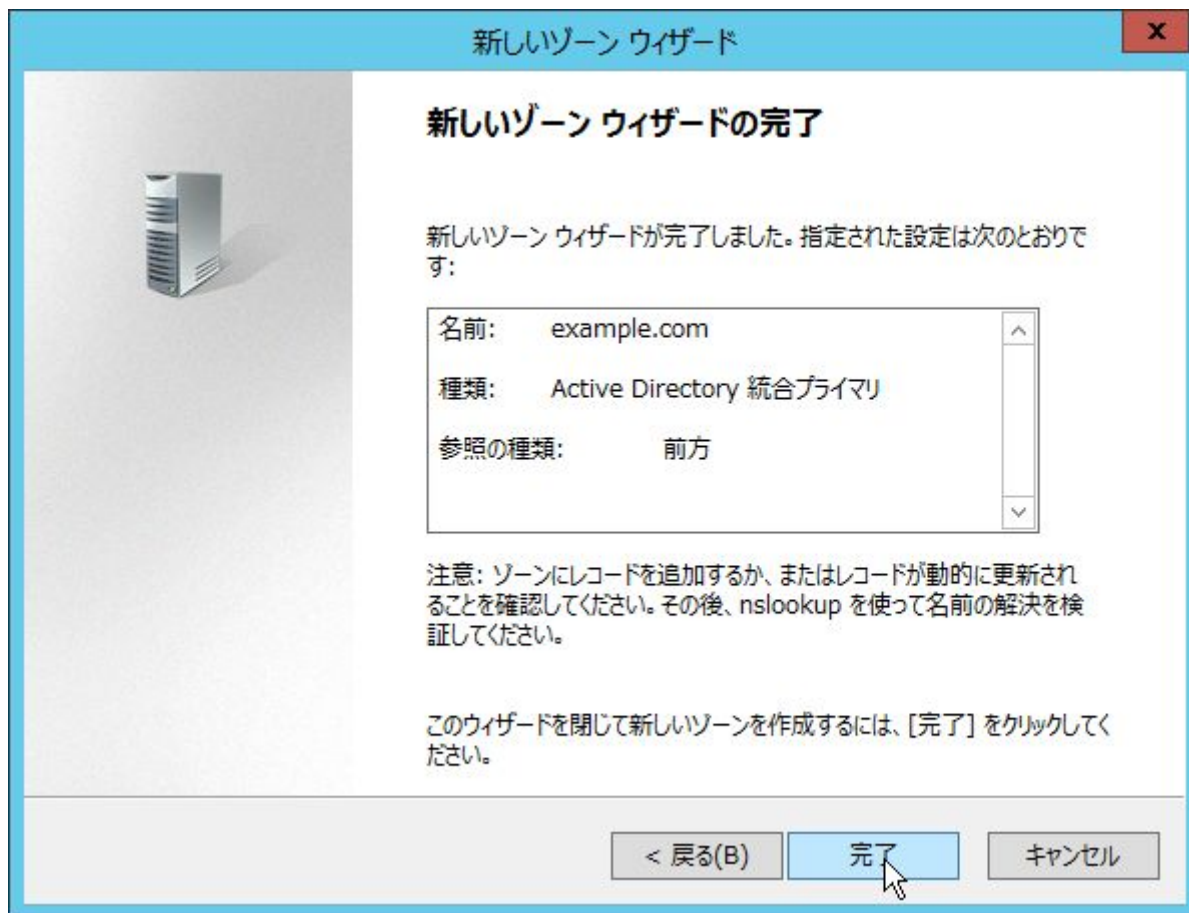
ゾーン名(Z):  
example.com

< 戻る(B)    次へ(N) >    キャンセル

「セキュリティで保護された動的更新のみを許可する」を選択して、「次へ」ボタンをクリックします。

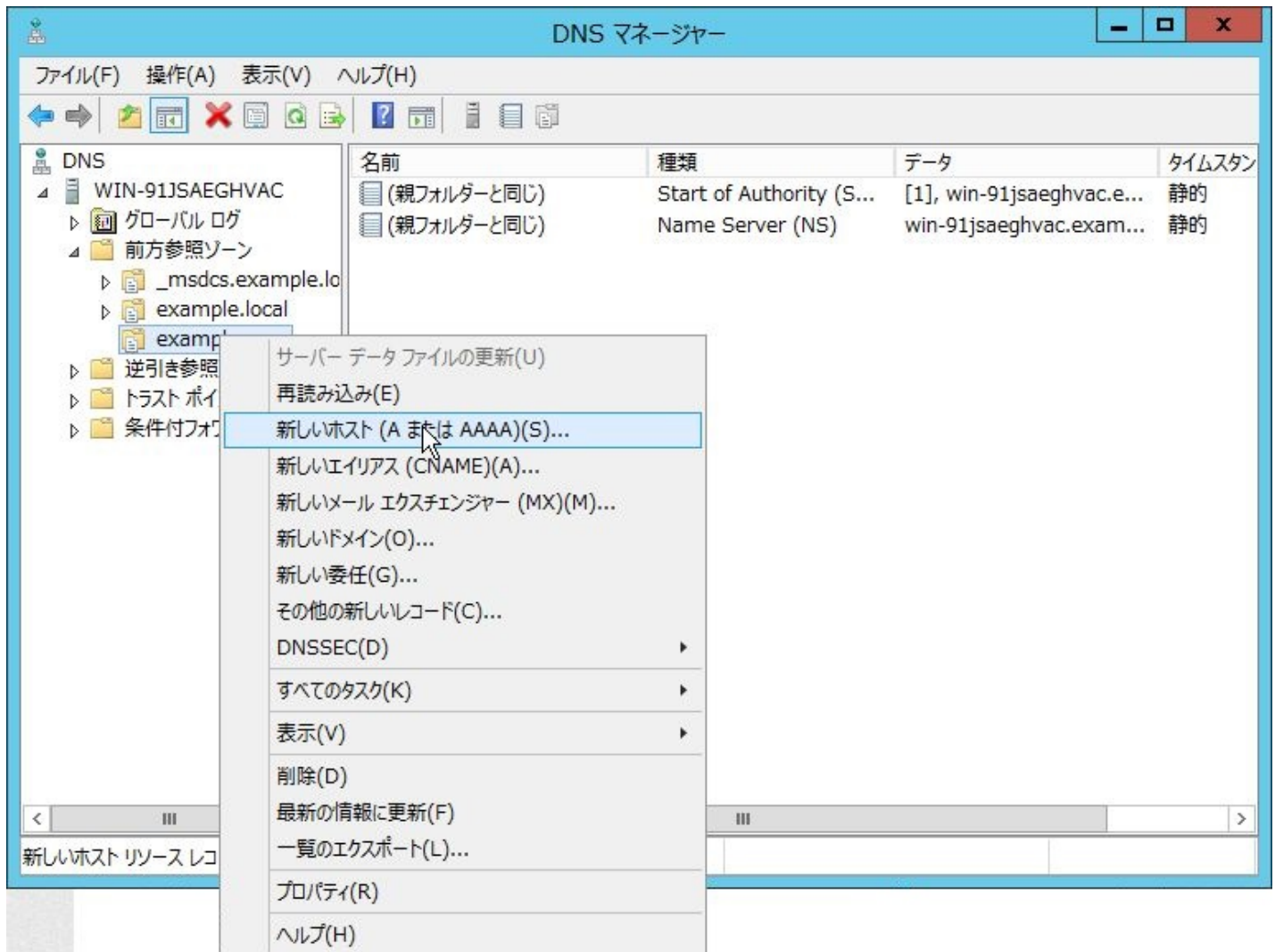


内容を確認して、「完了」ボタンをクリックします。





次に、作成された「example.com」を右クリックして、新しいホストを作成します。



OpenAM サーバーのホスト名と IP アドレスを入力して、「ホストの追加」ボタンをクリックします。



新しいホスト

名前 (空欄の場合は親ドメインを使用)(N):  
sso1

完全修飾ドメイン名 (FQDN):  
sso1.example.com.

IP アドレス(P):  
192.168.0.2

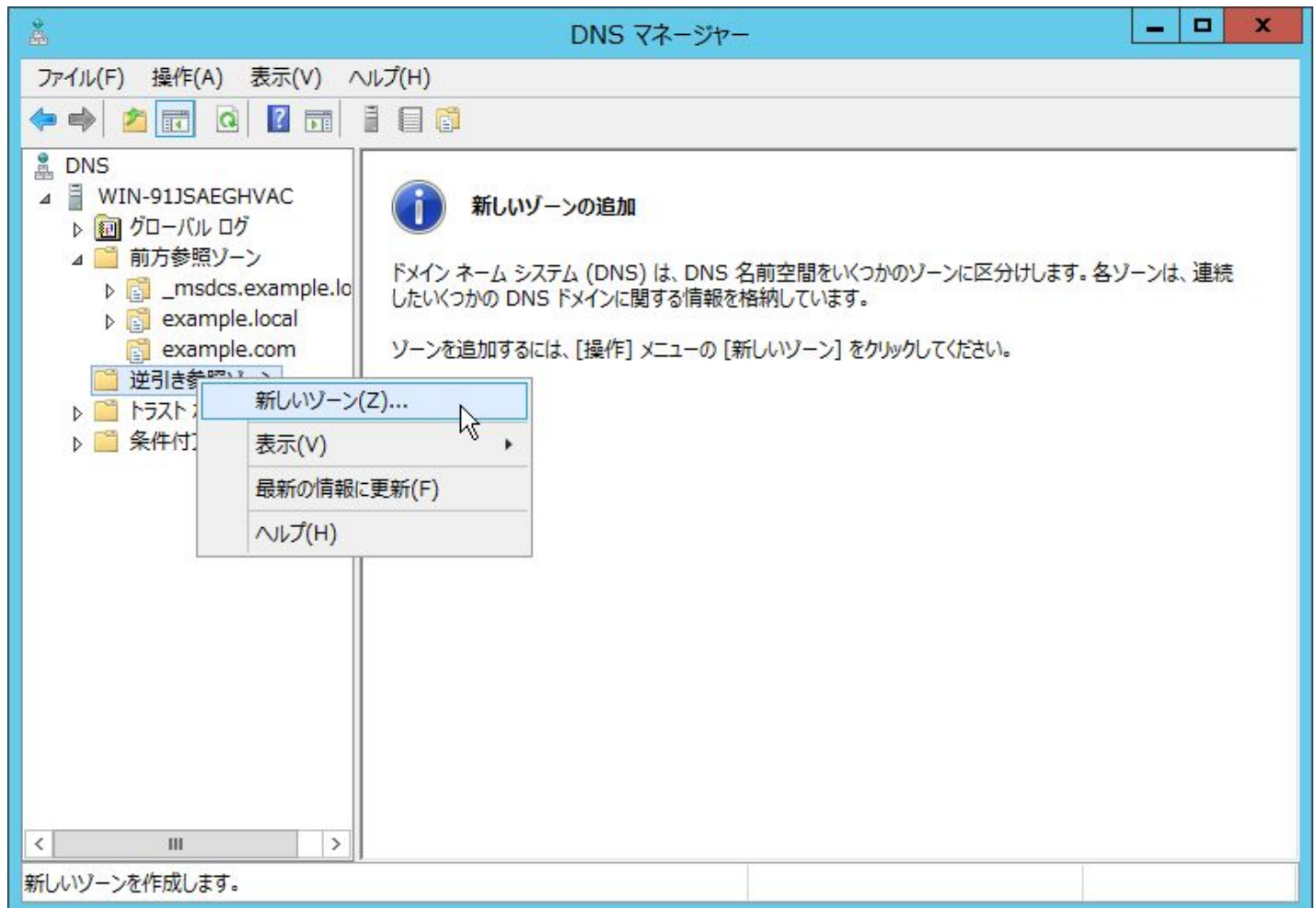
☐ 関連付けられたポインター (PTR) レコードを作成する(C)

☐ 同じ所有者名の DNS レコードの更新を認証されたユーザーに許可する(O)

ホストの追加(H) キャンセル

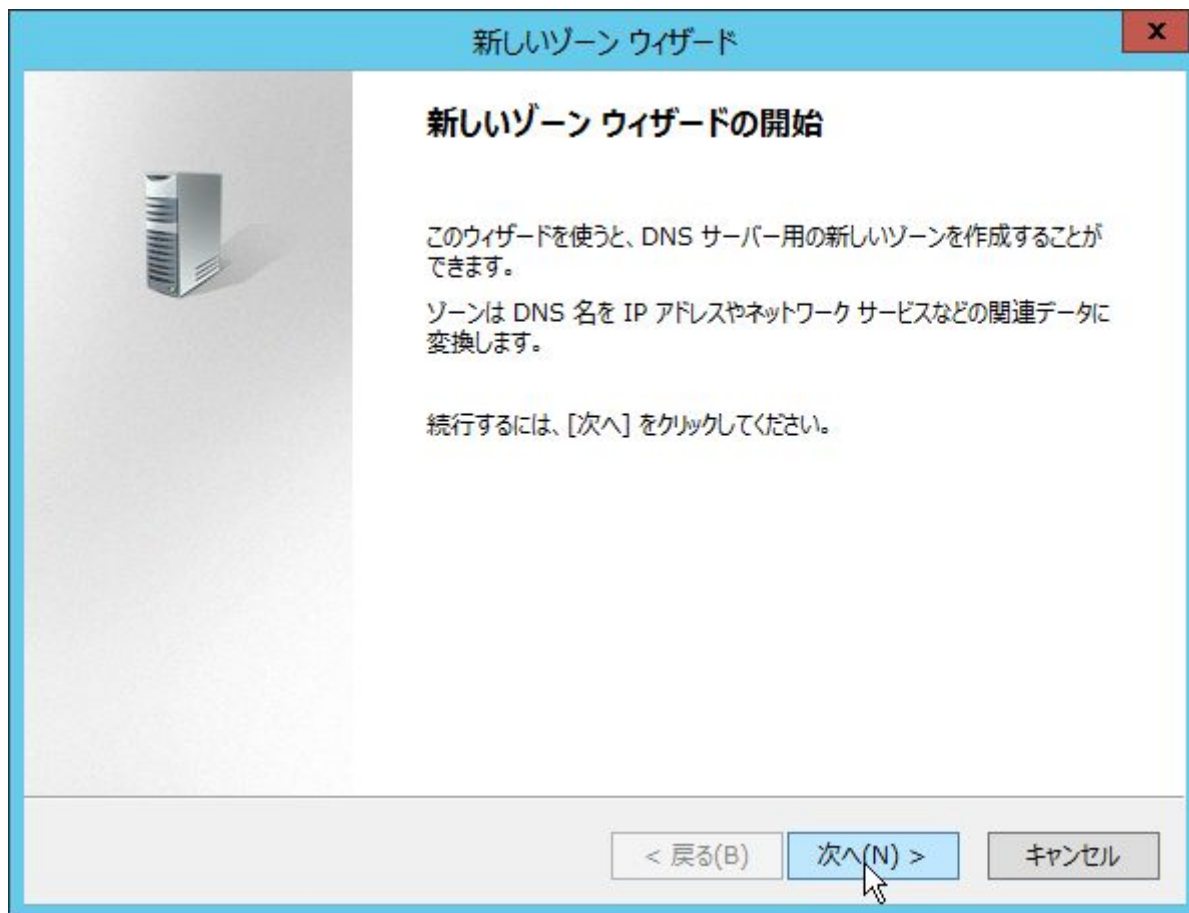
最後に、逆引き参照ゾーンに PTR レコードを追加します。

「逆引き参照ゾーン」を右クリックして、新規ゾーンを追加して下さい。

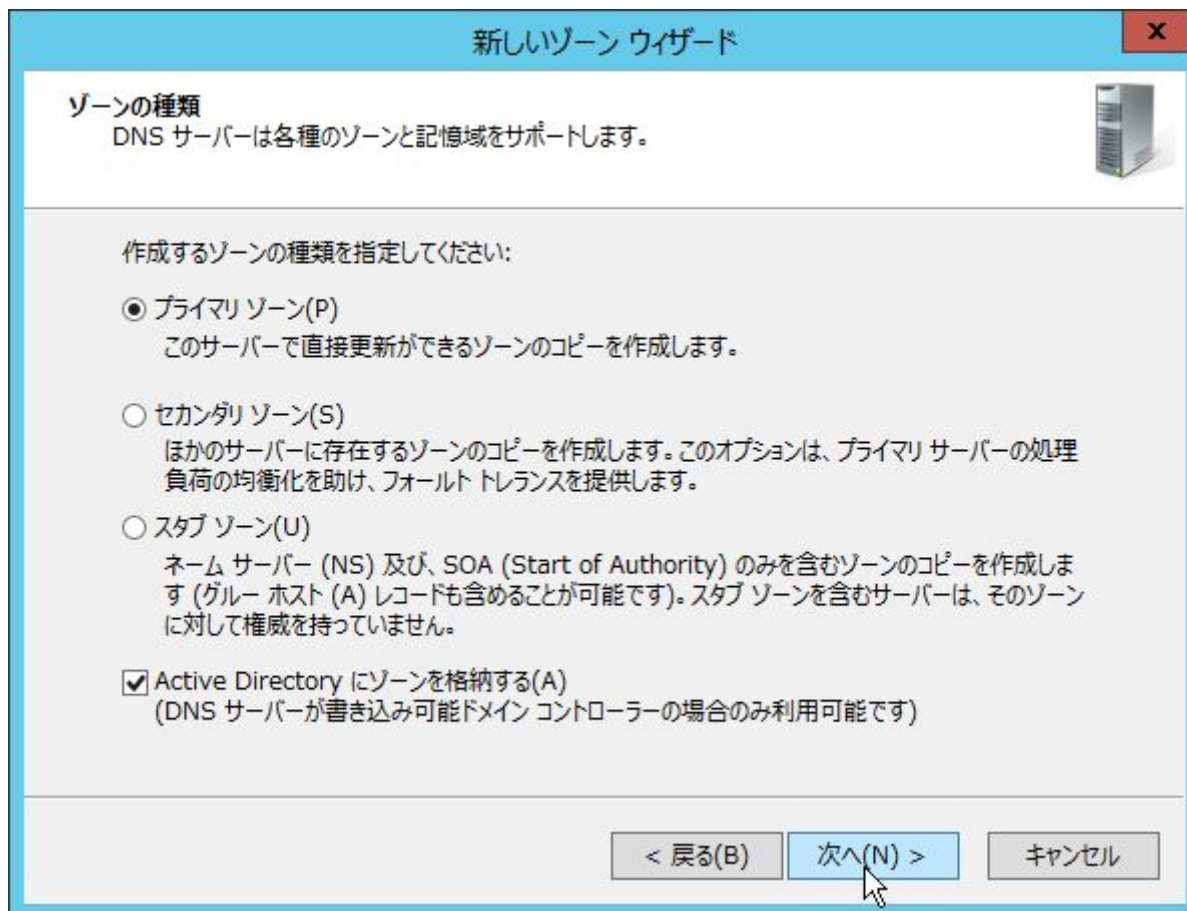




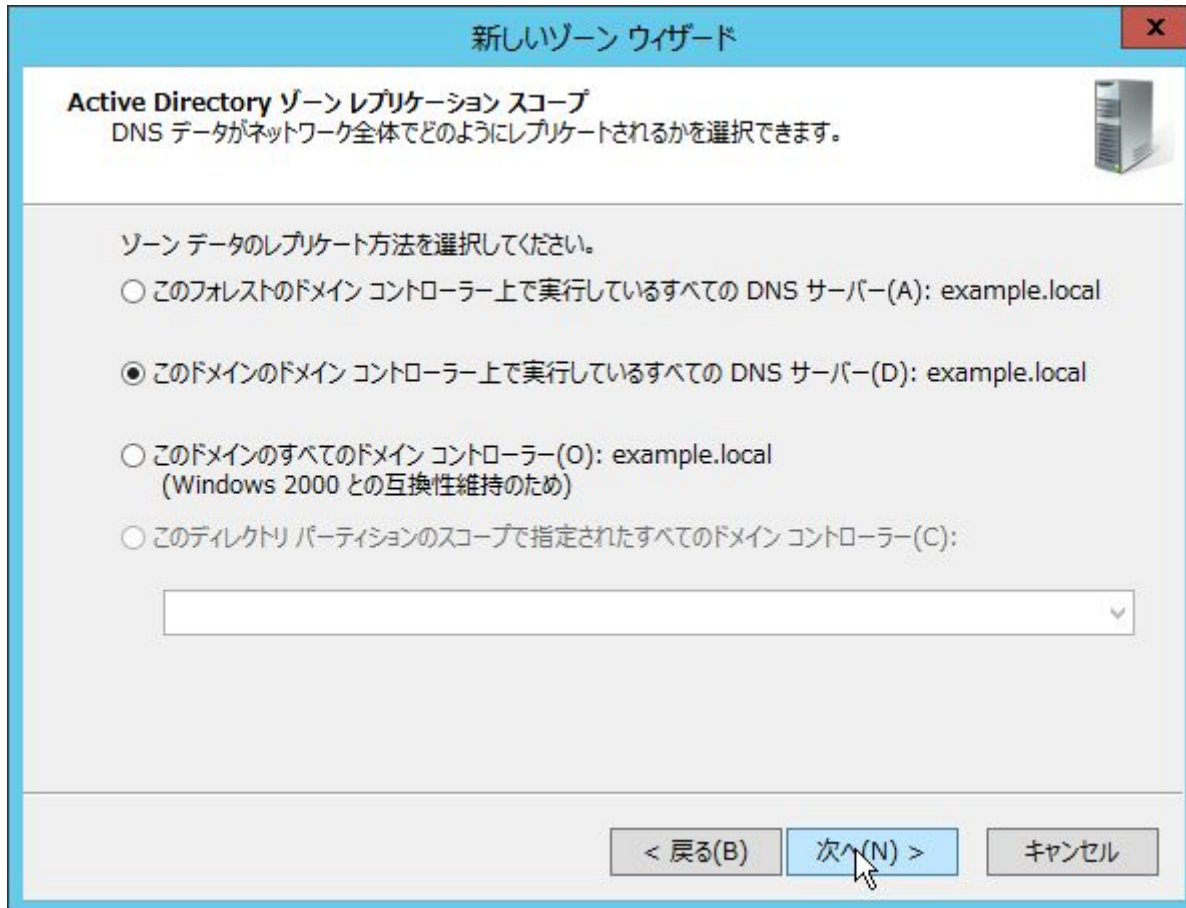
「次へ」ボタンをクリックします。



「プライマリゾーン」を選択して、「次へ」ボタンをクリックします。



「このドメインのドメインコントローラー上で実行しているすべての DNS サーバー: example.local」を選択して、「次へ」ボタンをクリックします。



新しいゾーン ウィザード

**Active Directory ゾーン レプリケーション スコープ**  
DNS データがネットワーク全体でどのようにレプリケートされるかを選択できます。

ゾーン データのレプリケート方法を選択してください。

☐ このフォレストのドメイン コントローラー上で実行しているすべての DNS サーバー(A): example.local

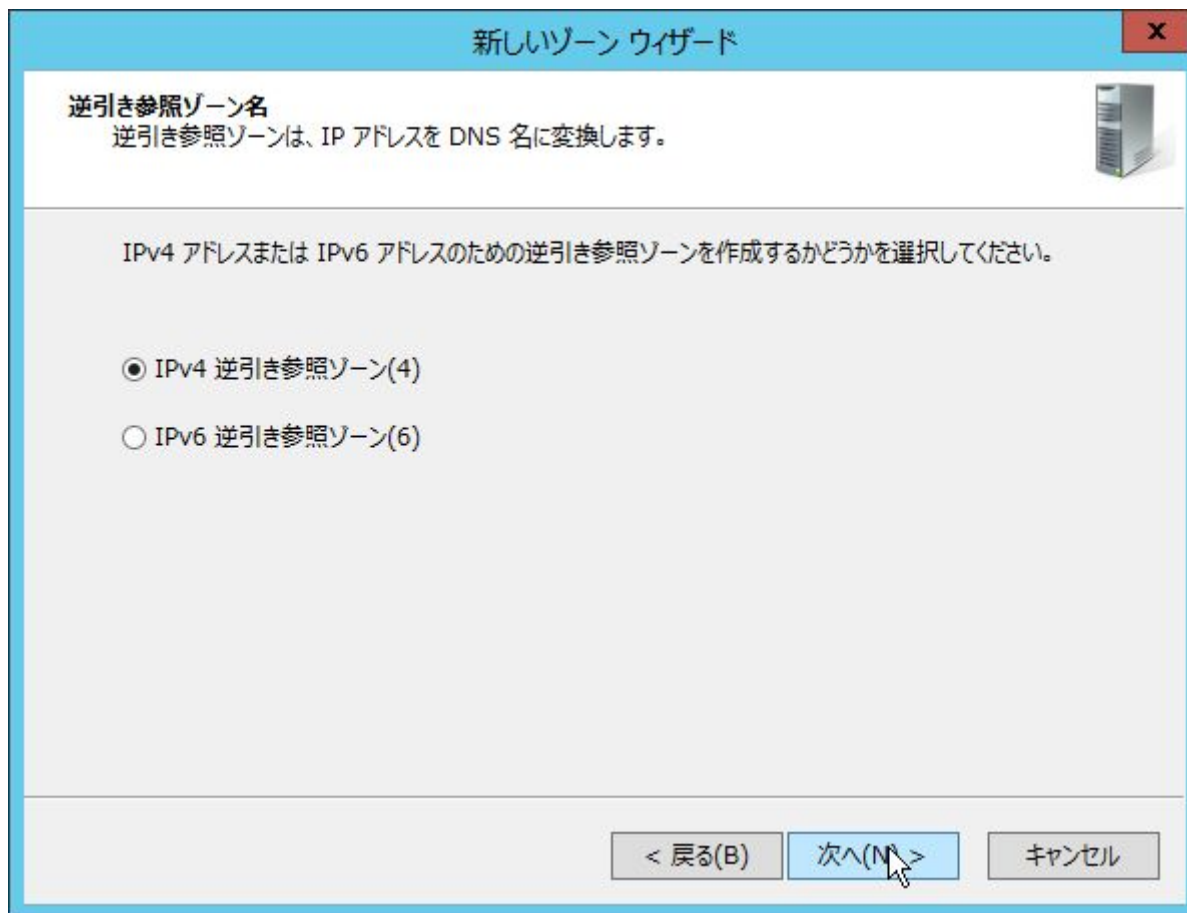
☒ このドメインのドメイン コントローラー上で実行しているすべての DNS サーバー(D): example.local

☐ このドメインのすべてのドメイン コントローラー(O): example.local  
(Windows 2000 との互換性維持のため)

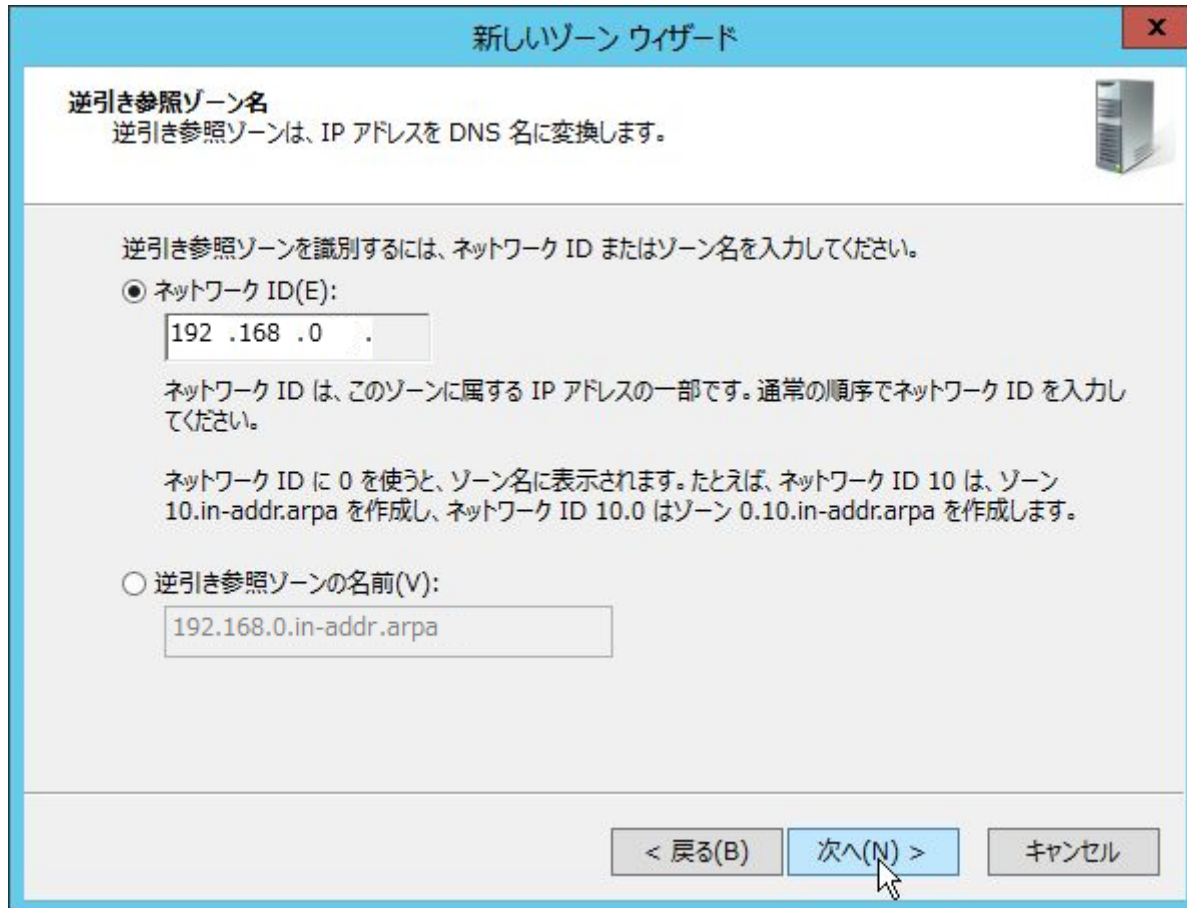
☐ このディレクトリ パーティションの範囲で指定されたすべてのドメイン コントローラー(C):

< 戻る(B)    次へ(N) >    キャンセル

「IPv4 逆引き参照ゾーン」を選択して、「次へ」ボタンをクリックします。



「ネットワーク ID」に IP アドレス範囲のネットワーク ID を入力します。例えば、OpenAM サーバーの IP アドレスが「192.168.0.11」の場合は「192.168.0」を入力して、「次へ」ボタンをクリックします。



新しいゾーン ウィザード

**逆引き参照ゾーン名**  
逆引き参照ゾーンは、IP アドレスを DNS 名に変換します。

逆引き参照ゾーンを識別するには、ネットワーク ID またはゾーン名を入力してください。

● ネットワーク ID(E):  
192 .168 .0 .

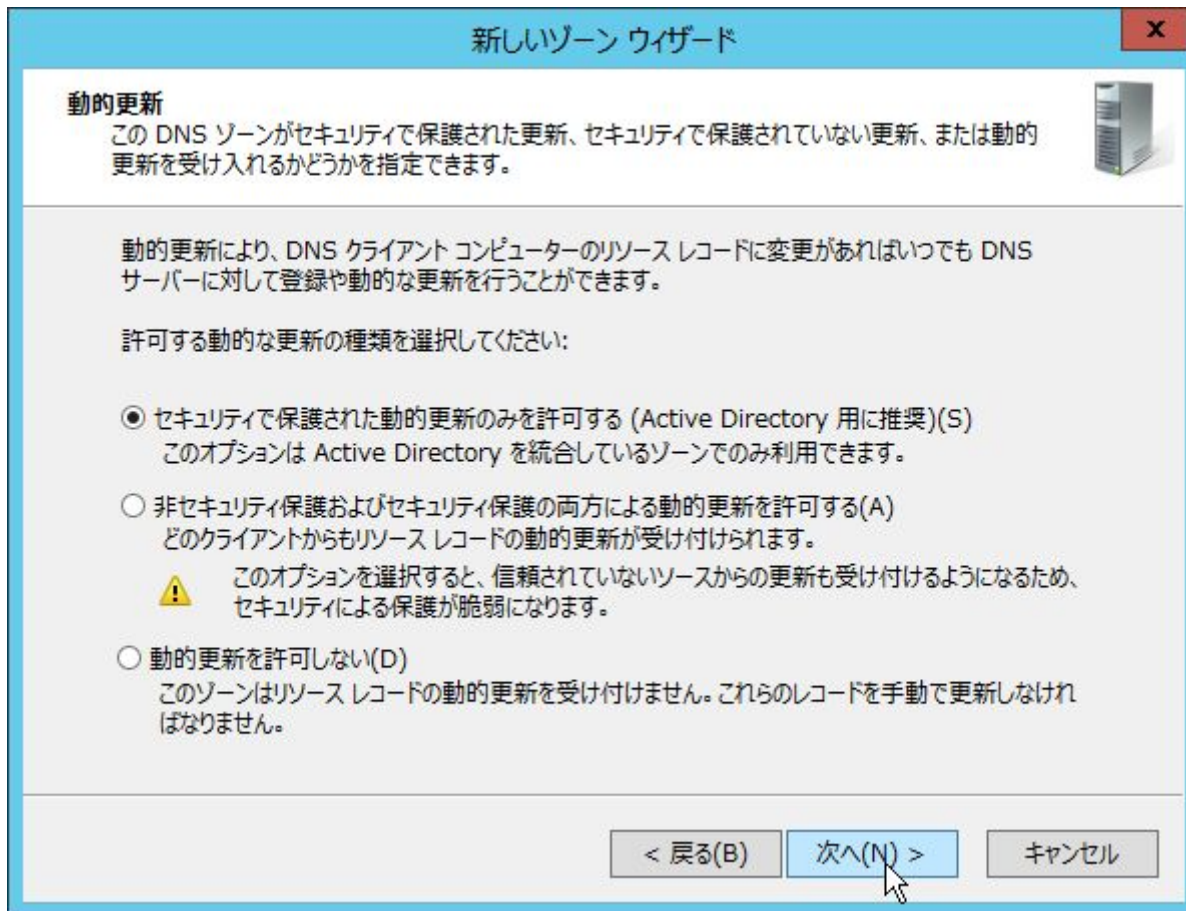
ネットワーク ID は、このゾーンに属する IP アドレスの一部です。通常の順序でネットワーク ID を入力してください。

ネットワーク ID に 0 を使うと、ゾーン名に表示されます。たとえば、ネットワーク ID 10 は、ゾーン 10.in-addr.arpa を作成し、ネットワーク ID 10.0 はゾーン 0.10.in-addr.arpa を作成します。

○ 逆引き参照ゾーンの名前(V):  
192.168.0.in-addr.arpa

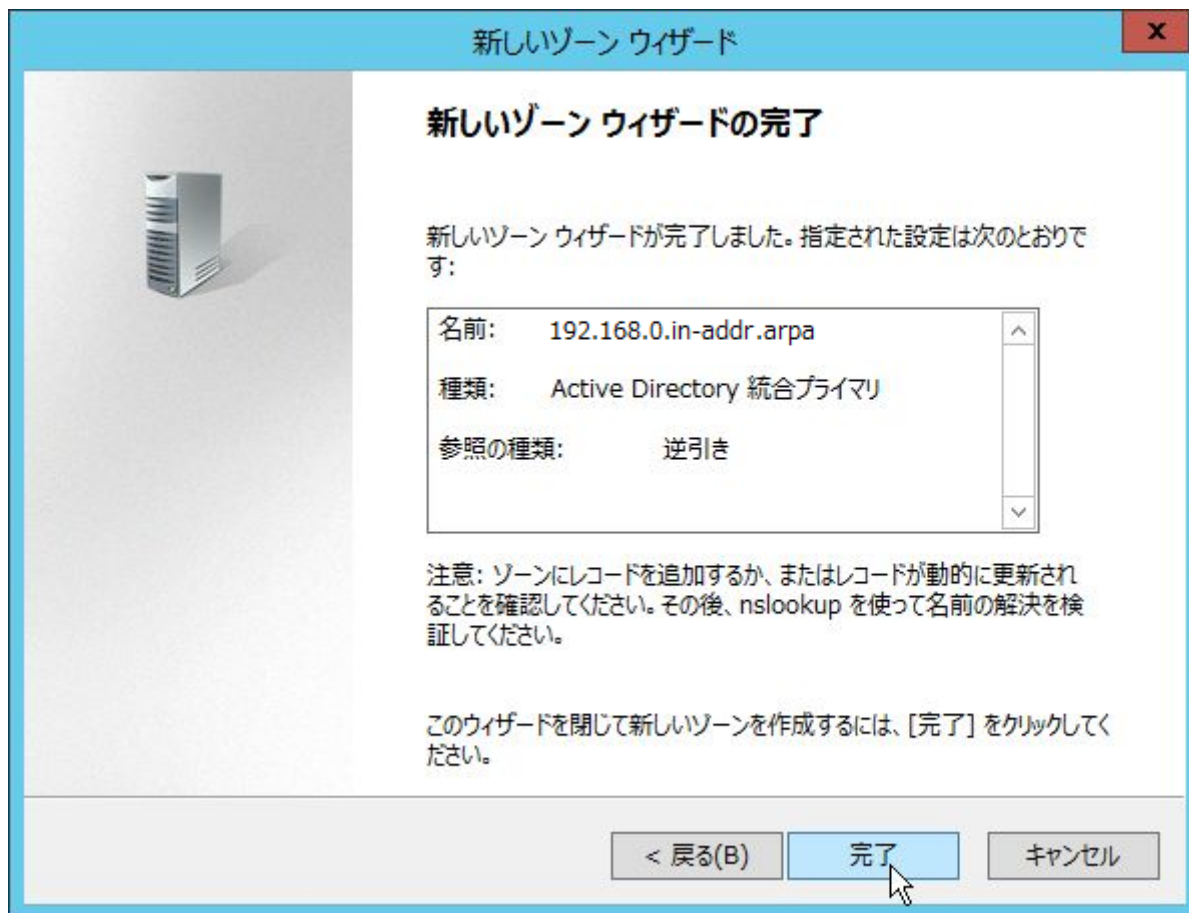
< 戻る(B)    次へ(N) >    キャンセル

「セキュリティで保護された動的更新のみを許可する」を選択して、「次へ」ボタンをクリックします。





最後に、「完了」ボタンをクリックします。



以上で、DNS サーバーの設定は完了です。



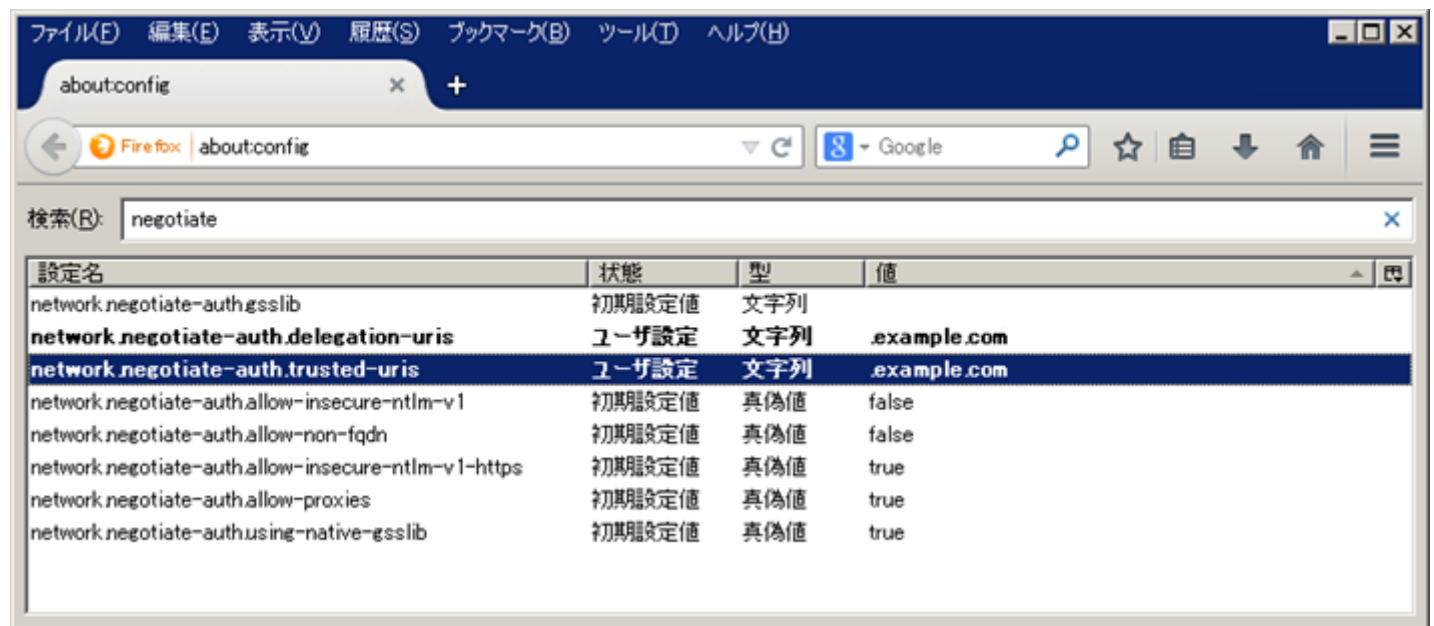
## 16. 付録3: Firefox と Chrome の設定

Firefox を使用して、Windows デスクトップ SSO 行う場合は以下の設定が必要です。

Firefox を起動して、アドレスバーに“about:config”を入力します。次に、フィルタに “ negotiate” と入力して絞り込みを行い、次の2つの属性に OpenAM の Cookie ドメインを設定します。

network.negotiate-auth.delegation-uris 属性: .example.com

network.negotiate-auth.trusted-uris 属性: .example.com



Chrome を使用して Windows デスクトップ SSO 行う場合は、「11. クライアント PC (Windows) の設定」で説明した Internet Explorer の設定があれば十分です。

## 17. 参考資料

OpenAM Release Notes

<http://OpenAM.forgerock.org/OpenAM-documentation/OpenAM-doc-source/doc/release-notes/index/index.html>

OpenAM Wiki – How does OpenAM work with Windows Desktop SSO

<https://wikis.forgerock.org/confluence/display/OpenAM/How+does+OpenAM+work+with+Windows+Desktop+SSO>

OpenAM 12.0.0 Administration Guide – Hints for the Windows Desktop SSO Authentication Module

<http://docs.forgerock.org/en/openam/12.0.0/admin-guide/index/chap-auth-services.html#desktop-module-conf-hints>

OpenAM Nightly Builds

<http://forgerock.org/downloads/OpenAM-builds/>

OpenAM コンソーシアム OpenAM インストール手順

<http://www.OpenAM.jp/category/member/techtips>