AD LDS 管理者アカウントの変更手順について

2016/8/10

EVE MA サポートセンター

1. はじめに

本資料では、EVE MA サーバーセットアップ時に使用した AD LDS 管理者アカウントを追加・変更・削除する手順について記載します。

EVE MA サーバーセットアップ時に Windows ログオンしているユーザーを AD LDS 管理 者に設定するようご案内しております。(EVE MA Rel.3.21 以前)

(8) 現在ログオ セス許可多	トンしているユーザーに AD LDS インスタンスに対する管理者のアク F割り当てます。
a Act	ive Directory ライトウェイト ディレクトリ サービス セットアップ ウィザード XI
	この AD LDS インスタンスに対する管理者特備を持つユーザーまたはグループを指定できます。 次のユーザーまたはユーザー グループに、AD LDS に対する管理者のアクセス許可を取り当てます。
	○ 現在ログオンしているユーザー(①): DDS¥Administratori AD LDS をインストールしているユーザーに、この AD LDS インスタンスに対する管理者のアクセスは すべかない ルイントールしているユーザーに、この AD LDS インスタンスに対する管理者のアクセスは
	■1の増かヨこくれます。 「次のアガントUD 満秋されまユーザーまたはグループに、この AD LDG インスタンスに対する管理者のアクセス将可が割 り当てられます。」のコージュースのロンレビューの時にメイン、または、コージェーンのドメインによって 信頼されていたら生産のドメインから、任意のユーザーまたはグループを選択すること形できます。
	7万分2十名(A) 参照(日)
	< 戻る(B) 次へ(N)> キャンセル ヘルブ
	図 22 AD LDS セットアップ ウィザード

図 1 AD LDSインスタンス作成手順(『EVE MAインストールマニュアル』より)

この AD LDS 管理者の権限が、後のメンテナンス作業で必要となるケースがございます。 そのため、あらかじめ、以下の手順にて、AD LDS 管理者の権限を Domain Admins など のグループに付与して頂くことをお勧めいたします。

2. AD LDS の管理者アカウントについて

EVE MA サーバーセットアップ後、セットアップ時の Windows ユーザーとは異なるユー ザーがメンテナンス作業を行う場合、AD LDS の管理者権限を付与されていないことが原 因で以下のようなエラーメッセージが出力されることがあります。

Windows 7 / Windows Server 2008 (maconfig --import-plugin-settings コマンド)
 Error: error have occurred while executingldifde.exe (code=5).
 To view the error log, find at "C:¥Users¥ユーザー名¥AppDate¥Local¥Temp".

C:¥evema¥R3.10¥x64¥tools>maconfig.exe --import-plugin-settings u17.mldf c:¥windows¥system32¥ldifde.exe -i -s 10.2.3.36 -t 43553 -c "CN=Schema,CN=Configuration.DC=X" "#schemaNamingContext" -f "C:¥Users¥■"■"■"¥AppData¥Local¥Temp¥mac 9D77.tmp" -j "C:¥Users¥II"■" *AppData¥Local¥Temp" "10.2.3.36" [E接続しています SSPI を使って現在のユーザーとしてログインしています ファイル "C:¥Users¥II"■" *AppData¥Local¥Temp¥mac9D77.tmp" からディレクトリをイ ンボートしています ていたりを読み込んでいます たいよりを読み込んでいます たいます。 たいよりを読み込んでいます たいます。 たいよりを読み込んでいます たいます。 たいよりを読み込んでいます たいます。 たいよりを正していまう。 の0000005: SecErr: DSID-031521D0, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0 0 個のエントリを正しく修正しました。 だいたいます。 たいたいます。 たいたいまうーが発生しました Error: error have occurred while executing Idifde.exe (code=5). To view the error log, find at "C:¥Users¥II"■" *AppData¥Local¥Temp".

図 2 import-plugin-settingsコマンドでエラー

上記エラーが発生した場合、以下の手順に従って AD LDS 管理者の権限を Domain Admins などのグループ、または、別のユーザーに付与してください。

3. AD LDS 管理者アカウントの変更手順

以下の手順にて、LDS の管理者アカウントを確認、および追加と削除をすることができます。

3.1. AD LDS インスタンスに接続する

- (1) AD LDS (EVEMAサーバー) に LDS の管理者権限(セットアップ時に使用したユーザー) でWindowsログオンします。
- (2) スタートメニューから [管理ツール] [ADSIエディター] を起動します。

【参考情報】 Title: ADSI エディターを使用して AD LDS インスタンスを管理する URL: <u>https://technet.microsoft.com/ja-jp/library/cc731156.aspx</u>

(3) ウィンドウの左側の [ADSIエディター] の上で右クリックし [接続…] を選択します。

📝 ADSI エディター					_ 🗆 ×
ファイル(F) 操作(A) 表示(V) ヘルブ(H)					
ADSI Iディカー 接待(C)	名前	クラス	識別名	操作	
	│	container		ADSI エディター	-
表示(V) ▶				他の操作	•
最新の情報に更新(F)					
<u>一覧のエクスボート(L)…</u>					
ヘルプ(H)					
	1			1	

図 3 ADSIエディター(AD LDSインスタンスに接続する)

(4) [接続の設定] 画面で以下を入力して [OK]ボタンをクリックします。

```
表 1 AD LDS インスタンス接続の設定
```

項目	説明
[名前]	任意の接続名(設定の例:構成)
[接続ポイント]	構成
[コンピュータ]	localhost:<ウィザードで設定したポート番号>

接続の設定
名前(N): 構成
パス(P): LDAP://localhost:43553/構成
接続ポイント
○ 既知の名前付けコンテキストを選択する(A):
構成
- コンピューター ◎ ドメインまたはサーバーを選択または入力する(S): (サーバー ドメイン [ポート])
localhost:43553
 ○ 既定 (ログインしたドメインまたはサーバー)(E) □ SSL ベースの暗号化を使用する(L)
詳細設定(V) OK キャンセル

図 4 AD LDSインスタンス接続の設定(Windows Server 2008 R2の場合)

CN=Configuration,CN={GUID} への接続が完了します。

📝 ADSI ፲፫ィター					_ 🗆 🗙
ファイル(E) 操作(A) 表示(V) ヘルプ(H)					
🗢 🔿 🖄 🔜 🗙 🖬 🍳 📄					
📝 ADSI エディター	名前	クラス	識別名	操作	
	このビューに表示する項目()	はありません。		CN=Administrators	A
 Generation (CN={944776C2-3139- 				他の操作	•
CN=DirectoryUpdates	1				

図 5 AD LDSインスタンス接続完了(Windows Server 2008 R2の場合)

3.2. AD LDS アカウントの追加を行う

本資料ではアカウント管理作業の容易さの点から、Domain Adminsなどのグループを追加する ことを推奨します。

 CN=Configuration, CN={GUID} の [CN=Roles] - [CN=Administrators] を右クリックし[プロ パティ]を選択します。



図 6 AD LDSインスタンス接続完了(Windows Server 2008 R2の場合)

(2) 属性エディターの中から、 [member] を選択し、[編集] をクリックします。

属性	值
managedBy	〈未設定〉
member	CN=S-1-5-21-3522015002-1199606823-250406275-
mS-DS-Consistency	〈未設定〉
mS-DS-Consistency	〈未設定〉
msDS-LastKnownR	〈未設定〉
msDS-NonMembers	
name	Administrators
objectCategory	CN=Group,CN=Schema,CN=Configuration,CN={944776
objectClass	top; group
objectGUID	432e69eb-3cat-482c-ate/-e551c1/9150d
objectSid	5-1-384685208-406783928-519
objectiversion	< 木設定>
otherwellKnownUbje	〈木設定〉
partialAttributeDelet	〈木設定〉

図 7 member 属性を編集する

(3) [Windows アカウントの追加] をクリックします。

雑数値のセキュリティ プリンシパル付益別名エディタ 腐性(A): nember 値(U):	- X
名前 コンテナー	識別名/SID
Kenshou_admin	CIN=2-1-9-51-3055019005-1188"
Windows アカウントの追加(W) DN の追加(D)	再(⑤秋(R)
	OK キャンセル

図8 管理者権限を持つグループ、ユーザーの名前が表示される

(4) [オブジェクトの種類] をクリックします。

ユーザー、コンピューター または グループ の選択	? ×
オブジェクトの種類の違訳(S): ユーザー、コンピューター、 グループ または ビルトイン セキュリティ プリンシパル	オブジェクトの種類(0)
場所の指定(F): Coal	場所(L)
選択するオブジェクト名を入力してください (例)(E):	
	名前の確認(C)
■¥純粗設定(A)OK	キャンセル

図 9 管理者として必要なアカウントを追加する

(5) 追加するオブジェクトの種類を選択し、[OK]をクリックします。(設定例:グループ)

オブジェクトの種類	? ×
検索するオブジェクトの種類を選択してください。	
オブジェクトの種業類(_):	
日本 「 「 「 「 「 」 「 」 「 」 「 」 「 」 「 」 「 」 「	
	Subari I
UK	

図 10 オブジェクトの種類を選択する

グループではなく、ユーザーを追加したい場合はここで [ユーザー] を選択してください。

(6) 追加するオブジェクト名を設定し、[OK]をクリックします。(設定例: Domain Admins)

ユーザー、コンピューター または グループ の選択	? ×
オブジェクトの種類の違択(<u>S)</u> : グループ	オブジェクトの種類(の)
場所の指定(<u>F</u>):	
選択するオブジェクト名を入力してください (例)(E): Domain Admins	名前の確認(<u>C</u>)
詳細設定(A)	OK ++>>セル

図 11 オブジェクト名を設定し、[OK]をクリックする

(7) [OK]をクリックし、アカウントの追加を行います。

78	敬値のセキュリティ ブリ	ンシバル付購別名エディター		×
	爾性(<u>A</u>): m/ 値(<u>U</u>):	ember		
	名前	コンテナー	識別名/SID	
	kenshou_admin	5 TERAN	CN=S-1-5-21-3522015002-1199	
	Domain Admins	1. SHEAT	<sid=010500000000005150000< td=""><td></td></sid=010500000000005150000<>	
	Windows アカウントのi DN のi自加(D)	<u>8708.90-</u>		育邸秋(B)
			OK	

図 12 設定したアカウントを追加する

新住(日):	
属性	値
isRecycled	〈未設定〉
lastKnownParent	〈未設定〉
managedBy	〈未設定〉
member	CN=S-1-5-21-3522015002-1199606823-250406275-!
mS-DS-Consistency	〈未設定〉
mS-DS-Consistency	〈未設定〉
msDS-LastKnownR	〈未設定〉 ―
msDS-NonMembers	〈未設定〉
name	Administrators
objectCategory	CN=Group,CN=Schema,CN=Configuration,CN={944776
objectClass	top; group
objectGUID	432e69eb-3caf-482c-afe7-e551c179150d
objectSid	S-1-384685208-406783928-519
objectVersion	〈未設定〉
↓ [► I
objectVersion ▲	〈未設定〉 ↓ ↓

(8) [適用] – [OK] をクリックし、[member] 属性に対して変更内容を反映させます。

図 13 変更内容を反映させる

3.3. AD LDS アカウントの削除を行う

以下の手順、(1)~(2)は、アカウント追加の手順と同じ手順です。

- CN=Configuration,CN={GUID}の[CN=Roles] [CN=Administrators]を右クリックし[プロ パティ]を選択します。
- (2) 属性エディターの中から、 [member] を選択し、[編集] をクリックします。
- (3) 削除したいアカウントを選択し、[削除] をクリックします。

E(A):	member		
(U):		sector anno	
5MI	1/77-	CN-S-1-E-21-2522015002-1100	_
comain Admins		CN=S=1=5=21=3522015002=1199	
ensnou_aumin		ON=3-1-9-21-9922019002-1199	
			1.002
Windows アカワント(55850(W)_	R153	(R)
DAL (D. Bho)	n) [
DN 0002000	0)		
			Local.

図 14 削除対象を選択し、[削除]をクリックする

(4) アカウントが消えていることを確認し、[OK] をクリックします。

il.	数 値のセキュリティ ブリ 寄性(A): me 直(U):	ンシパル付達別名エ mber	ディター				×
	名前	コンテナー		識別名/SID			-
	Domain Admins	1.18953		CN=S-1-5-21-3522015002-	-1199_		
	Windows アカウントの別 DN のiBtn(D)	Biblo(W)				育/序余(R)	
1					OK	キャンセル	

図 15 削除されていることを確認し[OK] をクリックする

(5) [適用] – [OK] をクリックし、[member] 属性に対して変更内容を反映させます。

属性	値			
isBecycled	(未設定)			
lastKnownParent	(未設定)			
managedBv				
member	CN=S-1-5-21-3522015002-1199606823-250406275-1			
mS-DS-Consistency	〈未設定〉			
mS-DS-Consistency	〈未設定〉			
msDS-LastKnownR	〈未設定〉			
msDS-NonMembers	〈未設定〉			
name	Administrators			
objectCategory	CN=Group,CN=Schema,CN=Configuration,CN={944776			
objectClass	top; group			
objectGUID	432e69eb-3caf-482c-afe7-e551c179150d			
objectSid	S-1-384685208-406783928-519			
objectVersion	〈未設定〉			
•				

図 16 変更内容を反映させる