



# 動作検証結果報告書 ディレクトリサービスを使用したユーザー管理

---

Version.1

Last updated: 2024 年 6 月

Active Directory Lightweight Directory Services と連携  
した Enterprise Server セキュリティ



## 目次

1. はじめに .....	3
2. 稼働環境.....	3
1) OS エディション .....	3
2) OS バージョン .....	3
3) プロセッサ .....	3
4) Micro Focus 製品 バージョン .....	3
3. 外部 LDAP 互換セキュリティマネージャとの連携 .....	4
1) Enterprise Server Common Web Administration (以降 ESCWA と称す) との連携 .....	5
2) MFDS との連携 .....	6
4. AD LDS の構築 .....	8
1) Windows オプション機能の追加.....	8
2) Windows 機能の有効化 .....	8
3) AD LDS インスタンスの作成.....	9
5. LDAP スキーマの定義.....	11
1) セットアップスクリプトの実行.....	11
2) AD LDS 構築内容の確認.....	13
6. ESCWA への ESM 適用 .....	15
7. MFDS への ESM 適用 .....	20
8. Enterprise Server インスタンスへの ESM 適用 .....	21
9. Enterprise Server インスタンスの開始 .....	22
10. JCL の実行 .....	23
11. CICS PCT の実行 .....	24
12. Enterprise Server インスタンスの停止 .....	25
13. おわりに .....	26

## 1. はじめに

Enterprise Developer / Enterprise Server はメインフレームで稼働している COBOL, PL/I アプリケーションや IBM メインフレームの JCL, CICS, IMS をオープン環境で稼働させることができる製品です。

リホスト後は開発環境製品である Enterprise Developer でコンパイルした実行モジュールを、実行環境製品である Enterprise Server が提供するランタイム上で稼働させますが、オープン環境におけるユーザー管理やセキュリティをどのように設計するかは重要な課題の1つです。

一般的には課題解決のためにディレクトリサービスを導入することが多いことから、Enterprise Server はこの代表的なツールである OpenLDAP や Active Directory とユーザー管理情報の連携を図ることが可能な機能を備えています。

本書は Enterprise Server と Windows の Active Directory Lightweight Directory Services(以降 AD LDS と称す) 間におけるユーザー管理やセキュリティ情報の連携を検証するものです。

## 2. 稼働環境

本書は下記環境で検証されました。

### 1) OS エディション

Windows 11 Pro

### 2) OS バージョン

21H2

### 3) プロセッサ

Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz 2.11 GHz

### 4) Micro Focus 製品 バージョン

Micro Focus™ Enterprise Developer 9.0 Patch Update 1

補足) Micro Focus™ Enterprise Server 9.0 と同等の開発用実行環境が含まれています。

### 3. 外部 LDAP 互換セキュリティマネージャとの連携

基幹システムをオープン環境へ移行する際、ユーザーによるリソースのアクセス制限や、管理画面にログインできるユーザーの限定など、セキュリティ要件を求められることが多くあります。例えば下記のような IBM メインフレームのリソースアクセス管理機能である RACF と同等の要件は、製品が提供する機能と外部セキュリティマネージャ(以降 ESM と称す)を連携させ、リソースと権限を定義することで満たすことができます。

#### RACF CICS FCT の定義例)

```
RDEFINE FCICSFCT (file1, file2, ..., fileN)
  UACC(NONE)
  NOTIFY(sys_admin_userid)
  PERMIT file1 CLASS(FCICSFCT) ID(group1, group2) ACCESS(UPDATE)
  PERMIT file2 CLASS(FCICSFCT) ID(group1, group2) ACCESS(READ)
Default CICS CLASS used: FCICSFCT
Parameters passed to ESM:
  Entity: File ID
  Facility: Terminal
  Transaction active
```

#### LDIF 形式 CICS FCT:ACCTFIL の定義例)

```
dn: CN=ACCTFIL,CN=FCICSFCT,CN=Enterprise Server Resources,CN=Micro
Focus,CN=Program Data,DC=X
changetype: add
objectClass: microfocus-MFDS-Resource
microfocus-MFDS-Resource-Class: FCICSFCT
microfocus-MFDS-Resource-ACE: allow:ALLUSER group:update
microfocus-MFDS-Resource-ACE: deny:*:execute
microfocus-MFDS-UID: mfuid
description: ACCT Demo file
```

製品と連携可能なセキュリティマネージャについては、製品マニュアルの [ディプロイ>構成および管理 >Enterprise Server セキュリティ>Enterprise Server のインストールの保護>アーキテクチャ および概要>セキュリティ アーキテクチャ>セキュリティ マネージャーについて] をご参照ください。

製品機能と ESM の連携は2段階の設定が可能となり、まずはこれら2つの違いについて説明します。

## 1) Enterprise Server Common Web Administration (以降 ESCWA と称す) との連携

JCL や CICS などの処理は Enterprise Server インスタンスが実行と管理を行い、これらの Enterprise Server インスタンスは OS のプロセスで稼働している Micro Focus Directory Server (以降 MFDS と称す) が管理しています。

ESCWA は、異なるマシン、異なる OS 上で稼働している複数の MFDS と接続して、すべての Enterprise Server インスタンスを管理できる Web ベースのインターフェイスです。

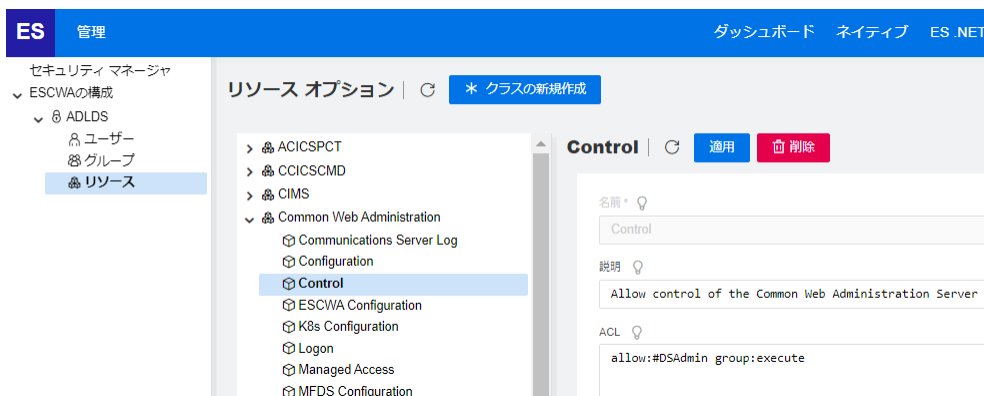
### ESCWA のインターフェイス



上記画像の ESCWA の [Directory Server] では、Windows と Red Hat Linux 環境で稼働している MFDS と接続し、各環境の IP アドレスを名前解決したホスト名である [WIN11-SVR]、[RHEL9] を用いて管理しています。

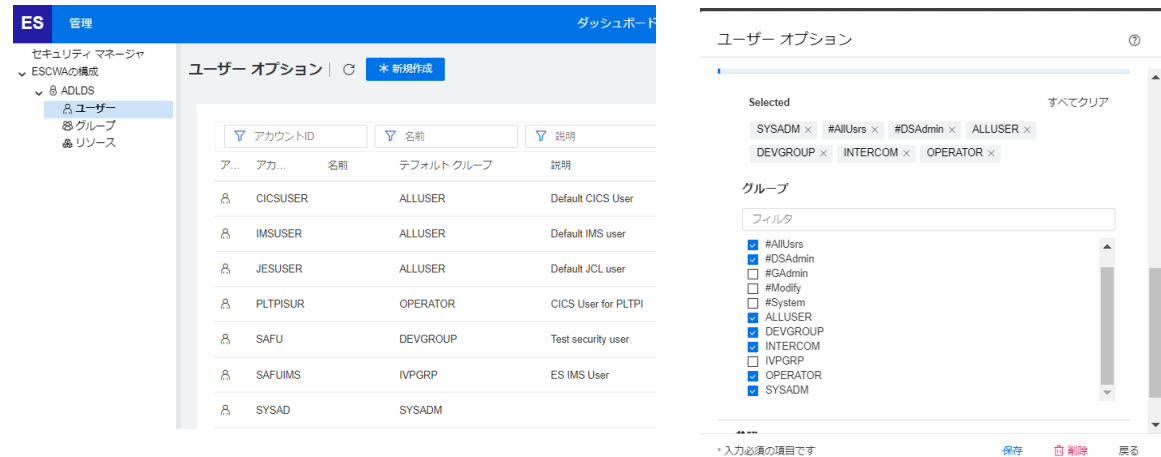
ESCWA へのログオン制限や PAC などの ESCWA で管理しているリソースのアクセス制限を行う要件がある場合は ESM と ESCWA を連携させます。

### ESCWA との連携例)



また、リソースのメンテナンスは ESM 側から実施することが基本ですが、ESM レポジトリの更新権限を持ったユーザーを使用して連携すれば、ESM に構築されたリソースのメンテナンスを ESCWA 上から行うこともできます。

### ESCWA のリソース表示例)



The screenshot shows the 'ユーザー オプション' (User Options) interface. On the left, there is a navigation menu with 'ユーザー' (Users) selected. The main area displays a table of users with columns for 'アカウントID' (Account ID), '名前' (Name), and '説明' (Description).

アカウントID	名前	説明
CICUSER	ALLUSER	Default CICS User
IMSUSER	ALLUSER	Default IMS user
JESUSER	ALLUSER	Default JCL user
PLTPISUR	OPERATOR	CICS User for PLTPI
SAFU	DEVGROU	Test security user
SAFUIMS	IVPGRP	ES IMS User
SYSAD	SYSADM	

On the right, the 'ユーザー オプション' dialog box is open, showing a list of selected users and groups. The 'Selected' section includes SYSADM, #AllUsrs, #DSAdmin, ALLUSER, DEVGROUP, INTERCOM, and OPERATOR. The 'グループ' (Groups) section has a search filter and a list of groups with checkboxes, including #AllUsrs, #DSAdmin, #GAdmin, #Modify, #System, ALLUSER, DEVGROUP, INTERCOM, IVPGRP, OPERATOR, and SYSADM.

## 2) MFDS との連携

各環境で稼働している MFDS や Enterprise Server インスタンスで実行するアプリケーションに関連したリソースのアクセス管理を行う場合は、ESM と MFDS を連携させます。

下記の画像は [WIN11-SVR] で稼働している MFDS に AD LDS を連携させたものです。

### Windows 環境の MFDS と連携した例)



The screenshot shows the '定義済みの外部のセキュリティ マネージャ' (Defined External Security Managers) interface. On the left, there is a tree view of Directory Servers, with 'WIN11-SVR' selected. The main area displays a table of security managers with columns for '名前' (Name), 'モジュール' (Module), '有効' (Enabled), '説明' (Description), and 'アクション' (Action).

名前	モジュール	有効	説明	アクション
AD LDS	mldap_esm	✓		

この連携により MFDS が管理する Enterprise Server インスタンスに細やかなセキュリティ設定ができるようになります。

## Enterprise Server インスタンスにセキュリティを設定した例)

- ▶ 企業
- ▶ PAC
- ▼ Directory Server
  - ▼ WIN11-SVR
    - 目 APAC1
    - 目 APAC2
    - 目 CICSDEMO
    - 目 CICSLSI
    - 目 DBDEMO
    - 目 DBDEMOEB
    - 目 ECIDEMO
    - 目 ESDEMO
    - 目 ESDEMO64
    - 目 IMSDEMO
    - 目 JCLDEMO
    - 目 JESSPL
    - 目 MFDBFH
    - 目 PAC2
    - 目 PLIIMS
    - 目 PLIIMS64
    - 目 PLIJCL
    - 目 PLIJCL64
    - 目 STAFF

### リージョンのセキュリティ機能の構成 | 適用

\* 入力必須の項目です

デフォルトのセキュリティ機能の構成を使用 ?

すべてのセキュリティ マネージャ ?  不明なリソースを検証

キャッシュTTL\*  秒

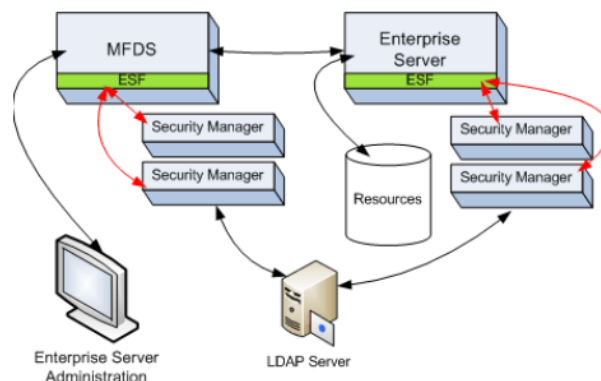
構成情報 ?

セキュリティ マネージャ リスト

+ 追加

1 ✓ AD LDS

Enterprise Server インスタンスに含まれている External Security Facility (以降 ESF と称す)は、ESM へセキュリティクエリを送信し、その結果で要求を許可することが適切であるかを判定しています。下記の図は製品に含まれるコンポーネントと各コンポーネント間の通信を示しています。詳しくは製品マニュアルをご参照ください。



ESM の構築や環境に関しては、以下の点についても注意が必要になります。

### 注意点1:

システムの堅牢性を確保して矛盾を回避するために、ESCWA、MFDS、Enterprise Server インスタンスには同じ ESM を使用することを強く推奨します。

### 注意点2:

製品が提供するリソースはすべてのクラスを網羅していますが、セキュリティエリのオーバーヘッド減少やメンテナンス性の観点から、必要なリソースだけを構築して簡素化することを推奨します。

まずはすべてのリソースを展開後、不要なものを削除する手順をお勧めします。

### 注意点3:

本書では 1 つの Windows 環境に Enterprise Server インスタンスと ESM を構築し、ローカル接続でセキュリティエリの通信を行っていますが、本番環境においてはそれぞれを異なる環境に構築し、ESM ヘリモート接続を行うことも考えられます。リモート接続を採用時、セキュリティエリの通信によるパフォーマンスの劣化が見られる場合は、通信環境の見直しなどの対策を講じてください。

パフォーマンスを最大限に引き出すためには、Enterprise Server インスタンスと ESM を同じ環境に構築することを推奨します。

## 4. AD LDS の構築

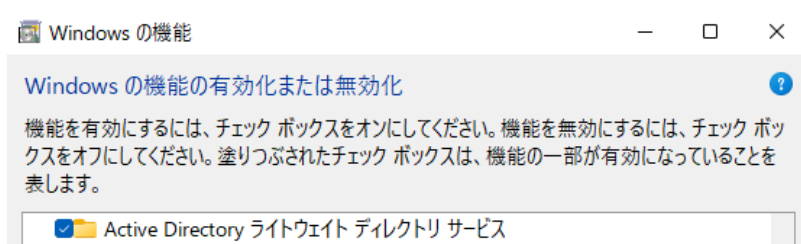
Windows11 はデフォルトで AD LDS がインストールされていないため、まずはこれをインストールすることから始めます。

### 1) Windows オプション機能の追加

Windows メニューから [設定]>[アプリ]>[オプション機能] を表示して [オプション機能を追加する] の [機能の表示] ボタンをクリックします。表示された画面から [RSAT:Active Directory Domain Services およびライトウェイトディレクトリサービスツール] を選択してインストールします。

### 2) Windows 機能の有効化

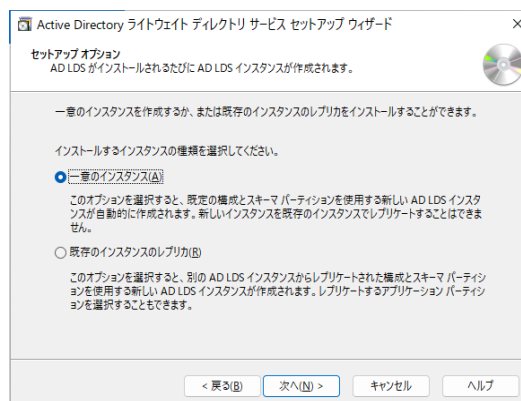
Windows コントロールパネルの [プログラムと機能]>[Windows の機能の有効化または無効化アプリ] を選択し、[Active Directory Domain Services およびライトウェイトディレクトリサービスツール] にチェックを入れて有効化します。



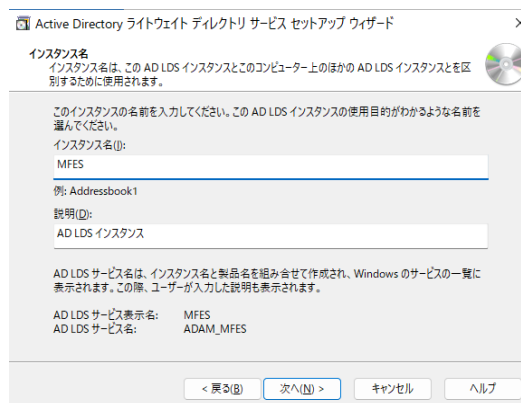


### 3) AD LDS インスタンスの作成

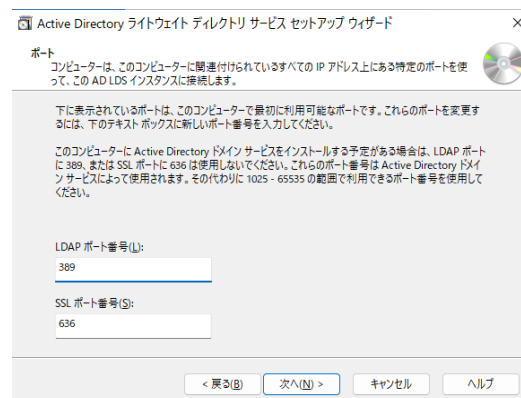
Windows メニューの [スタート]>  
[Windows ツール]>  
[AD LDS セットアップウィザード] を起動し、  
[セットアップオプション] に  
[一意のインスタンス] を選択後、  
[次へ] ボタンをクリックします。



[インスタンス名] には MFES を、  
[説明] には AD LDS インスタンス  
を入力して [次へ] ボタンをクリックします。  
この入力値は任意です。



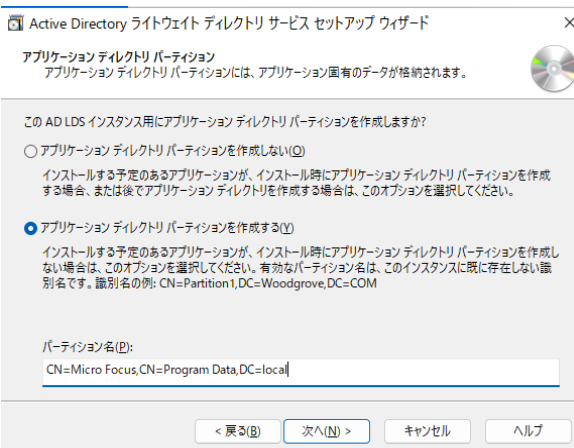
[ポート] は本書ではデフォルトのまま  
[次へ] ボタンをクリックします。  
独自のポートを指定する場合は  
ここで使用するポート番号を指定します。



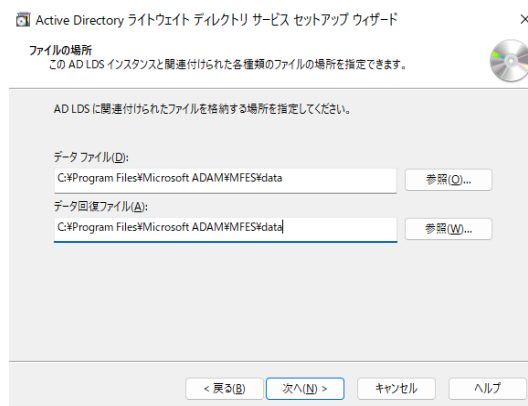
[アプリケーション ディレクトリ パーティション] では  
[アプリケーション ディレクトリ パーティションを作成する] を選択し、[パーティション名] に以下  
を入力後、[次へ] ボタンをクリックします。  
[パーティション名] の各 [=] 以降の値は  
任意です。

#### パーティション名例)

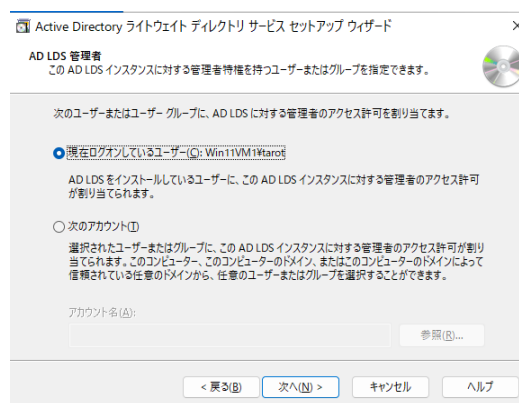
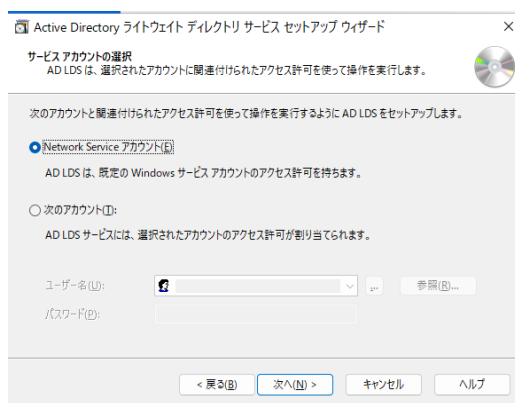
CN=Micro Focus,CN=Program Data,DC=local



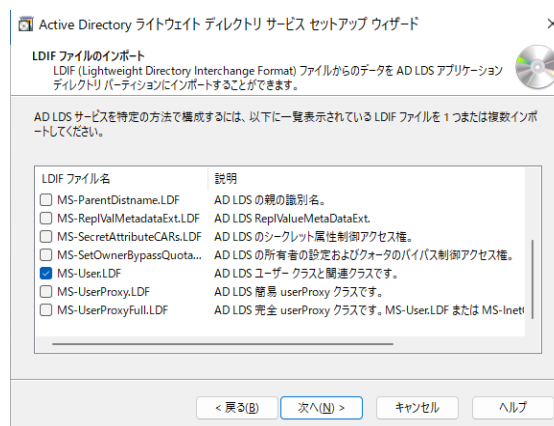
AD LDS に関連する [ファイルの場所] は任意ですが、本書ではデフォルトのまま [次へ] ボタンをクリックします。



[サービスアカウントの選択] では [Network Service アカウント] を選択後 [次へ] ボタンをクリックし、[AD LDS 管理者] には [現在ログオンしているユーザー] を指定して [次へ] ボタンをクリックします。



[LDIF ファイルのインポート] では [MS-User.LDF] を選択し、 [次へ] ボタンをクリックします。



[インストール準備完了] 画面で設定内容を確認後、[次へ] ボタンをクリックしてインストールします。

インストール終了後、インスタンス名に指定した MFES が Windows のサービスとして実行されていることを確認します。ログオンユーザーの変更が必要な場合は、変更後にサービスを再起動します。

名前	説明	状態	スタートアップの種類	ログオン
McpManagementService	<説明を読み取れませんでした。エラー...		手動	Local S...
MessagingService_46f98	テキストメッセージと関連する機能を...		手動 (トリガー開始)	Local S...
MFES	AD LDS インスタンス	実行中	自動	Local S...

## 5. LDAP スキーマの定義

ESCWA, MFDS, Enterprise Server インスタンスに関連するセキュリティデータを格納する LDAP オブジェクトクラスおよびコンテナを定義します。

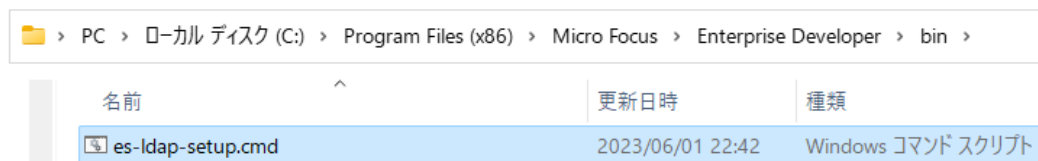
### 1) セットアップスクリプトの実行

製品をインストールしたパスの bin フォルダに含まれている セットアップスクリプトである es-ldap-setup.cmd ファイルを実行します。

このスクリプトでは Microsoft Ldifde コマンドを使用しています。注意点については、製品マニュアルの [デプロイ>構成および管理>Enterprise Server セキュリティ>Enterprise Server のインストールの保護>Active Directory を使用したセキュリティの構成>AD LDS を使用したセキュリティの設定>Ldifde の注意事項] をご参照ください。

#### セットアップスクリプトのパス例)

```
%ProgramFiles(x86)%¥Micro Focus¥Enterprise Developer¥bin¥es-ldap-setup.cmd
```



Enterprise Developer コマンドプロンプトを管理者権限で起動します。



スクリプトが存在するパスへ移動して `es-ldap-setup.cmd` を実行すると、いくつかの項目で入力を求められますが、デフォルト設定の場合はそのまま Enter を押下して進みます。

```
C:\Program Files (x86)\Micro Focus\Enterprise Developer\bin>es-ldap-setup
es-ldap-setup: Initial LDAP security setup for Enterprise Server
Version 1.3.1
Copyright 2006-2014 Micro Focus. All rights reserved.
Run "es-ldap-setup /?" for usage information.
続行するには何かキーを押してください . . .

Enter the information for the AD/LDS administrative user.
This user account will be automatically created if necessary.
Enter "-" to use your current logon credentials.
Enter LDAP user name:
Enter LDAP password [password]:
Enter LDAP partition DN [CN=Micro Focus,CN=Program Data,DC=local]:
Enter LDAP host:port [localhost:389]:
*** Checking password operations state...
```

- **[LDAP user name]:**

LDAP サーバーの管理ユーザー名を指定します。デフォルトでは実行しているユーザーが設定されます。本書ではデフォルト値を使用します。

- **[LDAP password]:**

LDAP 管理ユーザーの初期パスワードを指定します。デフォルトでは [password] が設定されます。

本書ではデフォルト値を使用します。

- **[LDAP partition]:**

前項で構築した LDAP パーティション名を指定します。

本書ではデフォルト値である [CN=Micro Focus,CN=Program Data,DC=local] を使用します。

- **[LDAP host:port]:**

前項で構築した LDAP のポート番号を指定します。

本書ではデフォルト値である [389] を使用します。

スクリプトの詳細は、製品マニュアルの [ディプロイ>構成および管理>Enterprise Server セキュリティ>Enterprise Server のインストールの保護>Active Directory を使用したセキュリティの構成>AD LDS を使用したセキュリティの設定>セットアップ スクリプトの実行] をご参照ください。

実行の途中で “RDO ファイルがオープンできない” というエラーが表示されますが、これは AD LDS を構築する前に Enterprise Server インスタンスで使用していたユーザー情報を取り込む場合のみに必要となるもので、ここでは無視して構いません。

```
*** Importing users from CAS RDO file...
続行するには何かキーを押してください . . .

Fatal error: RDO file (dfhdrdat) open failed: (5) file not found
```

RDO ファイルを利用する場合は、製品マニュアルの [ディプロイ>構成および管理>Enterprise Server セキュリティ>Enterprise Server のインストールの保護>Active Directory を使用したセキュリティの構成>AD LDS を使用したセキュリティの設定>AD LDS リポジトリの構成>LDAP リポジトリへの MSS ユーザーの追加] をご参照ください。

実行が終了すると、カレントパスに ldif.log と ldif.err ファイルが作成され、実行結果を確認することができます。

### ldif.log の例)

```

"localhost:389" に接続しています
ドメイン "Win11VM1" に SSPI を使って "tarot" としてログインしています
ファイル "es_default_ldap.ldf" からディレクトリをインポートしています
エントリーを読み込んでいます
1: cn=SYSADM,CN=Enterprise Server User Groups,CN=Micro Focus,CN=Program Data,DC=local
Entry DN: cn=SYSADM,CN=Enterprise Server User Groups,CN=Micro Focus,CN=Program Data,DC=local
changetype: add
Attribute 0) adminDisplayName:System administrators group
Attribute 1) objectClass:microfocus-MFDS-Group
Attribute 2) microfocus-MFDS-UID:mfluid
Attribute 3) description:ES System administrators group
Attribute 4) microfocus-MFDS-Group-Member:SYSAD

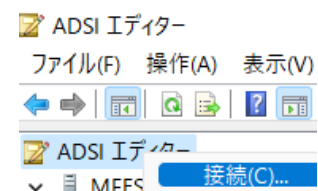
```

## 2) AD LDS 構築内容の確認

構築した LDAP オブジェクトクラスおよびコンテナを ADSI エディターから確認します。

Windows の検索ボックスに ADSI と入力すると [ADSI エディター] が表示されますので、これをクリックして起動します。

起動後、ADSI エディターを右クリックし、[接続] を選択します。



[接続の設定] では前項で構築した AD LDS の内容を指定して [OK] ボタンをクリックします。

#### [名前]:

LDAP インスタンス名として MFES を入力します。

#### [接続ポイント]:

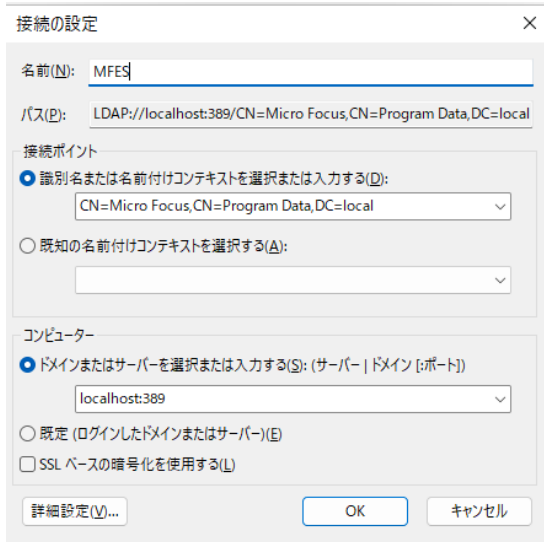
LDAP パーティション名として

CN=Micro Focus,CN=Program Data,DC=local

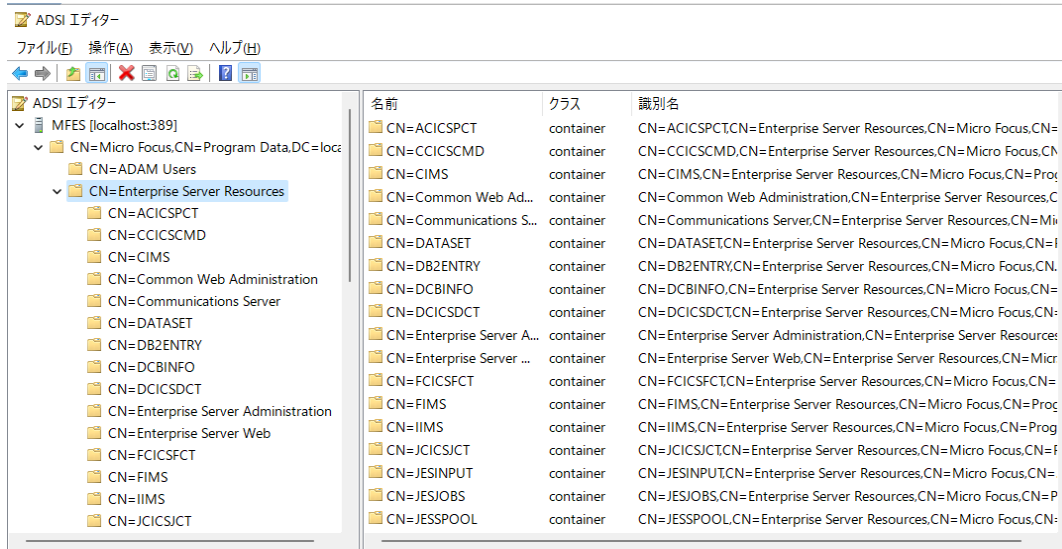
を入力します。

#### [コンピューター]:

LDAP を構築したマシンとポート番号として localhost:389 を入力します。



接続すると、セットアップスクリプトによって取り込まれた内容を確認することができます。

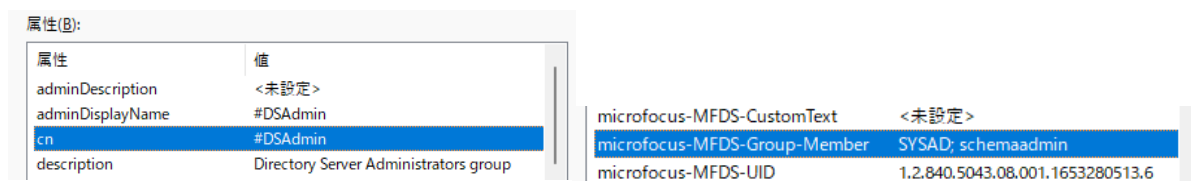


CN=ADAM Users にはデフォルトで設定される MFReader ユーザーとセットアップスクリプトを実行した tarot ユーザーが登録されています。



Enterprise Server User Groups と Enterprise Server Users の内容を表示して、どのユーザーがどのグループに含まれているかを確認します。

### SYSAD ユーザーの例

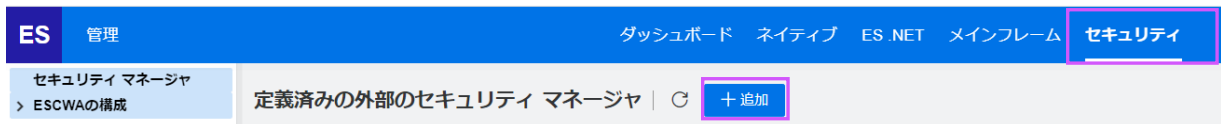


## 6. ESCWA への ESM 適用

本書では前項で確認したデフォルトの MFReader ユーザーを使用して ESCWA と連携します。MFReader ユーザーは読み取り権限のみを持つユーザーで、本来であれば ESCWA から AD LDS レポジトリを更新することはできませんが、本書では ESCWA からの変更を確認するために MFReader ユーザーに更新権限を付与しています。

AD LDS レポジトリの更新権限をユーザーに付与する必要がある場合は、製品マニュアルの [ディプロイ>構成および管理>Enterprise Server セキュリティ>Enterprise Server のインストールの保護>Active Directory を使用したセキュリティの構成>AD LDS を使用したセキュリティの設定>AD LDS レポジトリの構成>LDAP およびユーザー パスワードの変更に対する MFDS 管理の有効化] をご参照ください。

ESCWA の [セキュリティ] メニューをクリックし、[追加] ボタンをクリックします。



[外部のセキュリティマネージャ構成] 画面では以下の値を入力し、[保存] ボタンをクリックします。

外部のセキュリティ マネージャ構成

有効

名前\*  モジュール\*

接続パス

認証ID

パスワード

説明

構成情報

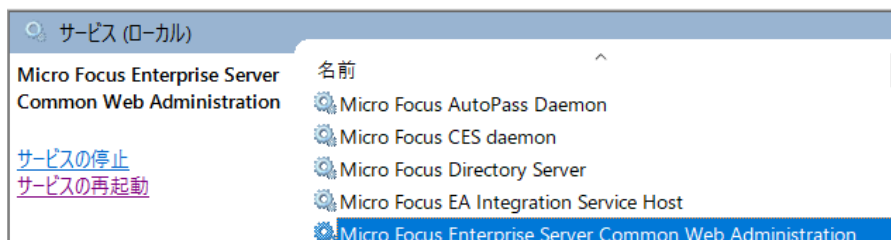
\* 入力必須の項目です 保存 戻る

- **[有効]:**  
チェックして有効に指定します。



- **[名前]:**  
任意で指定します。本書では ADLDS とします。
- **[モジュール]:**  
mldap.esm を指定します。
- **[接続パス]:**  
LDAP が構築されているマシンの IP アドレスもしくはホスト名を指定し、使用するポート番号を指定します。本書では名前解決されている WIN11-SVR:389 を指定します。
- **[認証 ID]:**  
前項で確認した MFReader ユーザーを使用して認証します。本書では CN=MFReader,CN=ADAM Users,CN=Micro Focus,CN=Program Data,DC=local を指定します。
- **[パスワード]:**  
セットアップスクリプトで指定した値を指定します。  
本書では password が該当します。
- **[説明]:**  
任意で入力します。
- **[構成情報]:**  
次の値を指定します。  
base=CN=Micro Focus,CN=Program Data,DC=local  
user class=microfocus-MFDS-User  
user container=cn=Enterprise Server Users  
group container=cn=Enterprise Server User Groups  
resource container=cn=Enterprise Server Resources

保存後は、ESCWA のセキュリティ設定の変更を有効にするために、Windows サービスで実行中の ESCWA を再起動します。





再起動後、ESCWA のセキュリティ画面へ移動し、左側メニューの [ESCWA の構成] を選択します。  
[セキュリティマネージャリスト] の [追加] ボタンをクリックします。



[定義済みの外部のセキュリティマネージャ] 画面では、  
連携済の [ADLDS] をチェック後 [選択] ボタンを  
クリックすると、[ESCWA セキュリティ機能の構成] 画面  
に戻ります。



変更を反映するために [適用] ボタンをクリックします。



変更権限をチェックする画面が表示されます。

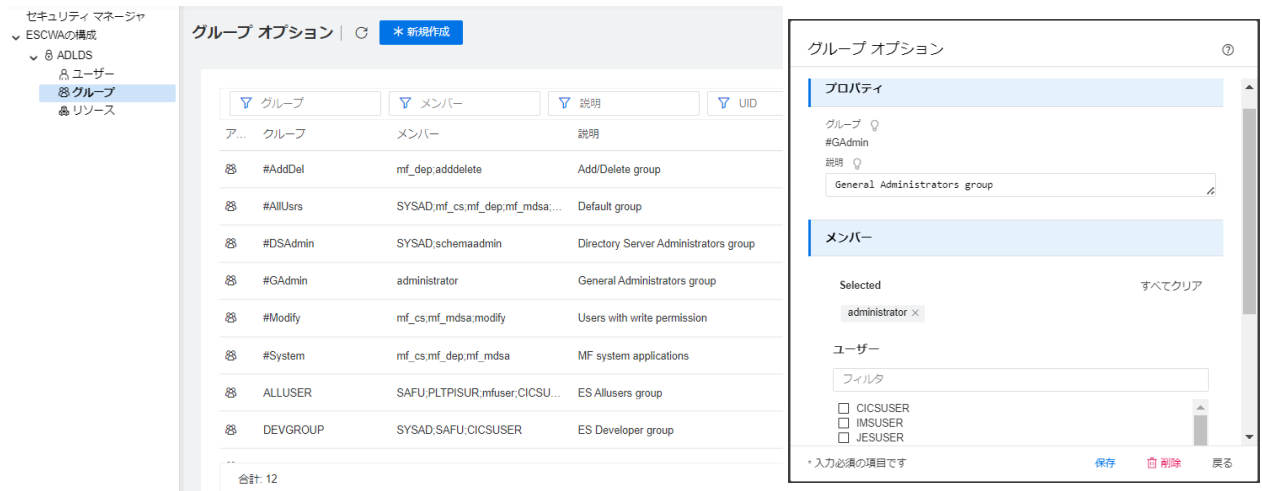
ユーザー名とパスワードに SYSAD を入力して [ログオン] をクリックします。



[セキュリティマネージャリスト] に [ADLDS] が追加され、左側メニューにも [ADLDS] が表示されます。



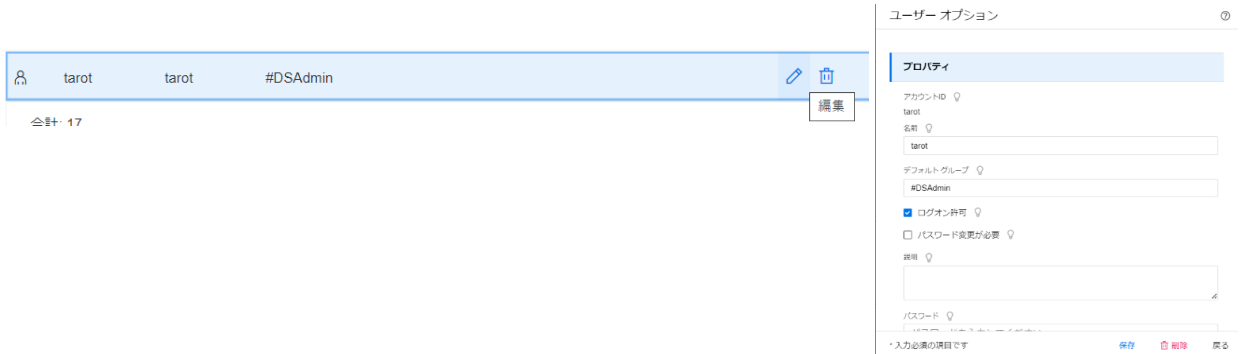
左側メニューの [ADLDS] をクリックすると、構築した AD LDS のリソース類が表示されます。AD LDS レポジトリに更新権限を持つユーザーを使用して接続している場合は、ESCWA 上でのメンテナンスが可能になります。



例えばユーザーを追加する場合は、左側メニューで [ユーザー] を選択し、右側の [新規作成] ボタンをクリック後にユーザー情報を入力して [保存] ボタンをクリックします。



既に存在している項目はダブルクリックまたは [編集] アイコンをクリックして、メンバーを修正または削除することができます。



製品に関連するリソースについての詳細は、製品マニュアルの

- ・ [ディプロイ>構成および管理>Enterprise Server セキュリティ>Enterprise Server のインストールの保護>MLDAP ESM モジュール>Micro Focus LDAP スキーマ]
- ・ [ディプロイ>構成および管理>Enterprise Server セキュリティ>Enterprise Server のインストールの保護>セキュリティのリファレンス情報>Enterprise Server が使用するリソース クラス]

をご参照ください。

製品マニュアルの抜粋)

JESJOBS

JES 関連	エンティティ	アクセスレベル
ジョブ名によるジョブのサブミットおよびキャンセルの制御。	<b>CANCEL</b> <i>localnodeid.userid.jobname</i> (ジョブのキャンセル権限の場合) <b>SUBMIT</b> <i>localnodeid.jobname.userid</i> (ジョブのサブミットの場合) <i>localnodeid</i> は、エンタープライズサーバーの名前です。 これらのルールは、一般的には使用されませんが、特殊な要件を持つ環境に対して細かな制御を提供します。	<b>NONE</b> アクセスは許可されません。 <b>READ</b> ユーザーはジョブをサブミットできます。 <b>UPDATE</b> READ と同等です。 <b>CONTROL</b> UPDATE と同等です。 <b>ALTER</b> ジョブをキャンセルできます。

ESCWA のセキュリティが有効になるとセッションタイムアウトが発生します。この場合はユーザー名とパスワードに SYSAD を入力して再度ログオンします。



## 7. MFDS への ESM 適用

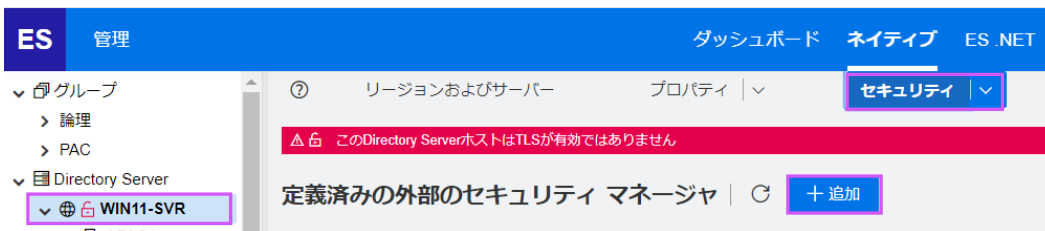
構築した AD LDS を ESCWA に表示された [WIN11-SVR] で稼働している MFDS と連携します。

ESCWA の [ネイティブ] を選択します。



左側メニューの [WIN11-SVR] を選択して [セキュリティ] メニューを選択します。

MFDS に対する [定義済みの外部のセキュリティマネージャ] が表示されますので、[追加] ボタンをクリックします。



ESCWA と同様の [定義済みの外部のセキュリティマネージャ] 画面には、ESCWA と同じ値を入力して保存すると、その内容が一覧に反映されます。

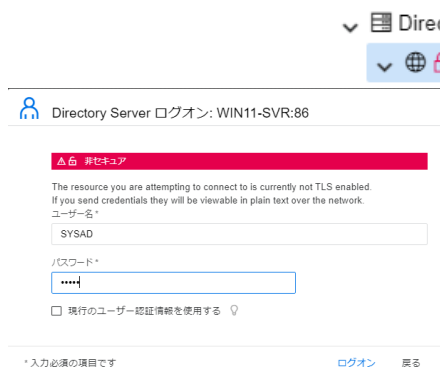


MFDS の [セキュリティ] メニューから [デフォルトのES構成] を選択し、[追加] ボタンをクリックします。ESCWA と同様に [AD LDS] にチェックして [選択] ボタンをクリックするとリストに表示されます。画面上部の [適用] ボタンで変更を保存します。



MFDS に関連するリソース操作にもユーザー権限を設定する場合は、MFDS の [セキュリティ] メニューから [Directory Server のセキュリティ機能の構成] を選択し、[ES デフォルトセキュリティマネージャを使用] にチェックをすると、[デフォルトの ES 構成] で設定した AD LDS が適用されます。

また、[Directory Server アクセスを制限する] にチェックをすると、MFDS へのアクセスに制限を設けることができます。

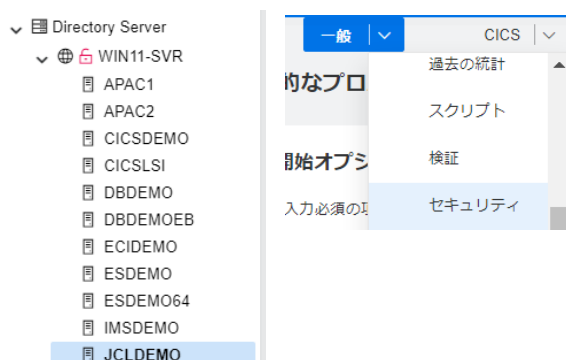


[適用] ボタンによる設定変更時は、ESCWA と同様に SYSAD を指定して更新します。

## 8. Enterprise Server インスタンスへの ESM 適用

[WIN11-SVR] にある作成済の JCLDEMO インスタンスに MFDS と連携させた AD LDS を適用します。

左側メニューの [WIN11-SVR] から JCLDEMO を選択し、JCLDEMO インスタンスの [一般] メニューから [セキュリティ] を選択します。



[リージョンのセキュリティ機能の構成] 画面の [デフォルトのセキュリティ機能の構成を使用] にチェックを入れると [セキュリティマネージャリスト] に [AD LDS] が表示されます。

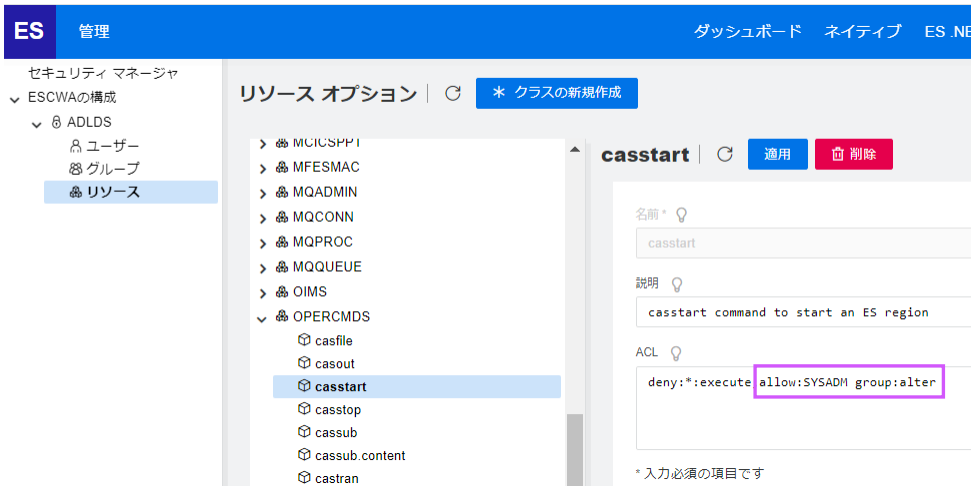


画面上部の [適用] ボタンをクリックして設定を保存します。

## 9. Enterprise Server インスタンスの開始

AD LDS を適用した JCLDEMO インスタンスを起動します。

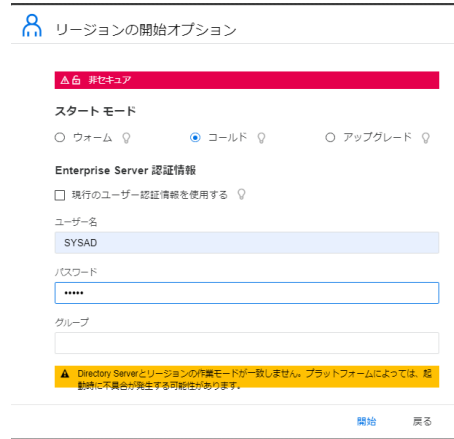
ESCWA の [セキュリティ] から AD LDS の [OPERCMD5] リソースを確認すると、Enterprise Server インスタンスの開始コマンドである casstart の実行権限を持つのは [SYSADM group] に所属するユーザーであることが確認できます。



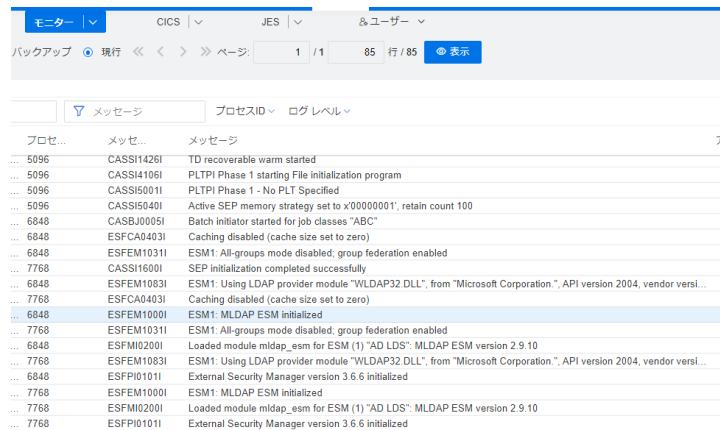
現在、このグループに所属しているユーザーは  
SYSAD ユーザーです。



権限のある SYSAD ユーザーで  
JCLDEMO インスタンスを ESCWA から開始します。



ESCWA からコンソールログを表示し、  
正常に開始されたことを確認します。



## 10. JCL の実行

JCLDEMO インスタンスに向けて JCL を実行します。

ESCWA の [セキュリティ] から AD LDS の [OPERCMDS] リソースを確認すると、JCL 実行コマンドである `cassub` の実行権限を持つのは [ALLUSER group] に所属するユーザーであることが確認できます。



このグループに属していない JESUSER ユーザーで JCL を実行すると、権限がない旨のメッセージが出力され、JCL は実行されません。

```
>cassub /sWIN11-SVR:57911 /jC:%work%\JCLDEMO%copy1.jcl /uJESUSER /pJESUSER
CASBJ0047S JES Submit: User ID "JESUSER" not authorized 15:23:45
Processed "C:%work%\JCLDEMO%copy1.jcl"
```

コンソールログにも同じ内容が記録されます。

```
CASBJ0047S JES Submit: User ID "JESUSER" not authorized
```

権限のある SYSAD ユーザーで同じ JCL を実行すると正常に終了し、結果をコンソールログやスプールで確認することができます。

```
>cassub /sWIN11-SVR:58366 /jC:¥work¥JCLDEMO¥copy1.jcl /uSYSAD /pSYSAD
JCLCM0187I J0001436 COPY1 JOB SUBMITTED (JOBNAME=COPY1,JOBNUM=0001436) 15:29:08
JCLCM0180I J0001436 COPY1 Job ready for execution. 15:29:08
Processed "C:¥work¥JCLDEMO¥copy1.jcl"
```

### コンソールログ内容)

JCLCM0187I	J0001436 COPY1 JOB SUBMITTED (JOBNAME=COPY1,JOBNUM=0001436)
JCLCM0180I	J0001436 COPY1 Job ready for execution.
JES000004I	J0001436 COPY1 JOB DISPATCHED
JCLCM0188I	J0001436 COPY1 JOB STARTED
JCLCM0182I	J0001436 COPY1 JOB ENDED - COND CODE 0000

### スプール内容)

ジョブ: **J0001436** | 適用 保留 削除

一般 メッセージ DDエントリ ジョブステップ

**メッセージ**

```
JCLCM0188I J0001436 COPY1 JOB STARTED 15:29:08
JCLCM0182I J0001436 COPY1 JOB ENDED - COND CODE 0000 15:29:08
```

## 11. CICS PCT の実行

JCLDEMO インスタンスを使用して CICS の PCT である CINQ を実行します。

ESCWA の [セキュリティ] から AD LDS の [TCICSTRAN] リソースである [CINQ] を確認すると、この PCT の実行権限を持つのは [SYSADM group] と [OPERATOR group] に所属するユーザーであることが確認できます。

CENV  
 CFCP  
 CFCR  
 CFLE  
 CFLI  
 CFLS  
 CFMT  
 **CINQ**  
 CINS  
 CLOG  
 CMAP  
 CMAX

**CINQ** | 適用 削除

名前\*

説明

ACL

権限のあるグループに属さない CICSUSER ユーザーで 3270 エミュレータからログインし、



[CINQ] を実行すると、セキュリティ違反のメッセージが表示され、結果は確認できません。

**プロパティ**

アカウントID

名前

デフォルトグループ

ログオン許可

パスワード変更が必要

**所属するグループ**

Selected すべてクリア

ALLUSER x DEVGROUP x

グループ

フィルタ

- #AddDel
- #AllUsrs
- #DSAdmin
- #GAdmin
- #Modify
- #System
- ALLUSER
- DEVGROUP
- INTERCOM
- IVPGRP
- OPERATOR

### CICSUSER ユーザーでの実行結果

```
CINQ
```

```
CASSE0001E Security violation. Terminal B000, transaction CINQ, user CICSUSER.
```

権限のある SYSAD ユーザーで実行すると、正常に実行され、結果が表示されます。

```
Invalid-request(ivrq...) ABCODE(____) ABDUMP(.) ABPROGRAM(____)
ALTSRNHT(024) ALTSRNWD(080) APLKYBD(.) APLTEXT(.) APPLID(JCLDEMO)
ASRAINTRPT(LowValue) ASRAPSW(LowValue) ASRAREGS(LowValue) BTRANS(.) CMDSEC(.)
COLOR(y) CWALENG(00512) DEFSCRNHT(024) DEFSCRNWD(080) DELIMITER(x'00')
DESTCOUNT(ivrq...) DESTID(ivrq...) DESTIDLENG(ivrq...) DS3270(.) DSSCS(.)
EWASUPP(.) EXTDS(y) FACILITY(C000) FCI(x'01') GCHARS(00000) GCODES(00000)
GMMI(.) HIGHLIGHT(y) INITPARM(LowValue) INITPARMLEN(00) INPARTN(____) KATAKANA(.)
LDCMNEM(ivrq...) LDCNUM(.) MAPCOLUMN(ivr) MAPHEIGHT(ivr) MAPLINE(ivr)
MAPWIDTH(ivr) MSRCONTROL(.) NATLANGINUSE(E) NETNAME(NETC000) NEXTTRANSID(...)
NUMTAB(.) OPCLASS(x'303030') OPERKEYS(x'0000000000000000') OPID(x'202020')
OPSECURITY(x'000000') ORGABCODE(____) OUTLINE(.) PAGENUM(ivr) PARTNPAGE(ivr)
PARTNS(.) PARTNSET(____) PRINSYSID(ivrq) PROGRAM(DFHZCINQ) PS(.) QNAME(ivrq)
RESSEC(.) RESTART(.) SCRNHT(024) SCRNWD(080) SIGDATA(00000) SOSI(.)
STARTCODE(TD) STATIONID(.) SYSID($IVP) TASKPRIORITY(000) TCTUALENG(000)
TELLERID(.) TERMCODE(x'9132') TERMPRIORITY(000) TEXTKYBD(.) TEXTPRINT(.)
TRANPRIORITY(000) TWALENG(00000) UNATTEND(y) USERID(SYSAD____)
USERNAME(____) USERPRIORITY(000) VALIDATION(.)
```

## 12. Enterprise Server インスタンスの停止

JCLDEMO インスタンスを停止します。

ESCWA の [セキュリティ] から AD LDS の [OPERCMDS] リソースを確認し、Enterprise Server インスタンスの停止コマンドである `casstop` の実行権限を持つ SYSAD ユーザーで停止します。

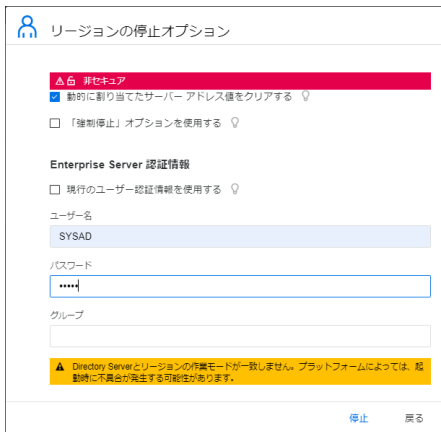
- > JICICSJCT
- > JESINPUT
- > JESSPOOL
- > MCICSPPT
- ▼ OPERCMDS
  - DIAGS
  - casout
  - casub
  - casfile
  - casstop
  - castran

説明

ACL

\* 入力必須の項目です

## ESCWA からの停止例)



## 13. おわりに

製品と ESM の1つである AD LDS を連携することにより、ESCWA や MFDS へのアクセスや Enterprise Server インスタンスに関連するリソースへの細やかなユーザー権限設定が可能であることを検証しました。

セキュリティ要件の実現には、ユーザーの職務に適した権限やグループの事前設計、ESM 全般について精通していることも重要になります。

ESM との連携において本書をお役立ていただければ幸いです。

Enterprise Server のセキュリティ全般に関しては、製品マニュアルの [ディプロイ>構成および管理 >Enterprise Server セキュリティ>Enterprise Server のインストールの保護] をご参照ください。