動作検証結果報告書
Enterprise Server

ディレクトリ・サービスを使用したユーザー管理

OpenLDAP と連携した Enterprise Server セキュリティ

openldap 2.6.3-1 版

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ることになりますが、その際、オープン環境でユーザー管理情報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 Linux 版の OpenLDAP と Enterprise Server 間のユーザー管理やセキュリティ情報の連携が可能であることを検証するものです。

動作検証結果報告書
Enterprise Server

目次

1. 稼働環境

本書は下記環境で検証されました。

1）ディストリビューション

Red Hat Enterprise Linux release 9.3 (Plow)

2）Linux カーネルバージョン

Linux version 5.14.0-362.13.1.el9_3.x86_64

3）OpenLDAP バージョン

openldap-clients-2.6.3-1.el9.x86_64
openldap-servers-2.6.3-1.el9.x86_64

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 と同等の開発用実行環境が含まれています。

2. 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、管理画面にログオ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ツールである LDAP 互換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=FCICSFCT,cn=Enterprise Server Resources,cn=Micro Focus,dc=secldap,dc=com
objectClass: top
objectClass: container
structuralObjectClass: container
cn: FCICSFCT

dn: cn=ACCTFIL,cn=FCICSFCT,cn=Enterprise Server Resources,cn=Micro
Focus,dc=secldap,dc=com
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
structuralObjectClass: microfocus-MFDS-Resource
cn: ACCTFIL
```

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。

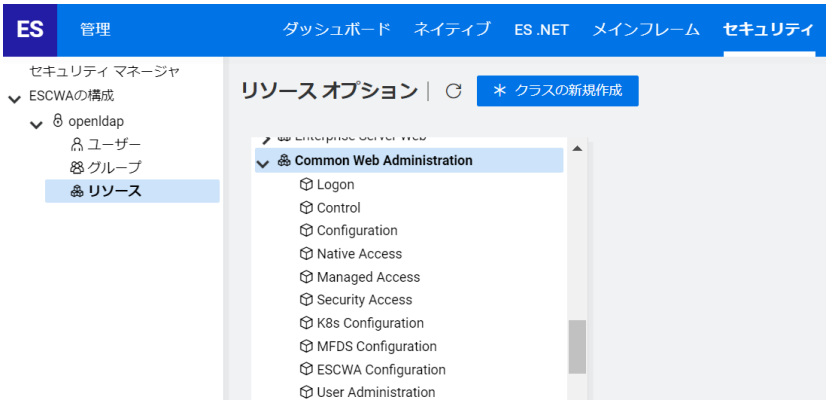
1）Enterprise Server Common Web Administration（以降 ESCWA と称す）との連携

ESCWA は異なるマシン、異なる OS で稼働している Micro Focus Directory Server（以降 MFDS と称す）と接続して 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）

上記画像の ESCWA と接続している2つの環境は、[WIN11-SVR]、[RHEL9] をホスト名として IP アドレスを名前解決しています。また、ESCWA に表示されている Directory Server は MFDS を指し、[WIN11-SVR] と [RHEL9] で稼働している MFDS のデフォルトポートである 86 を指定して、ホスト名と同じ名称を指定して管理しています。

ESCWA へのログオン制限、PAC などの ESCWA に関連するリソースのアクセス制限を行う要件がある場合は ESCWA と連携させます。



また、ESCWA と連携することで、権限を持ったユーザーが ESM に構築されたリソースのメンテナンスを ESCWA 上で行うこともできるようになります。

2）MFDS との連携

MFDS が管理する Enterprise Server インスタンス上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制限を行う目的で ESM と連携します。

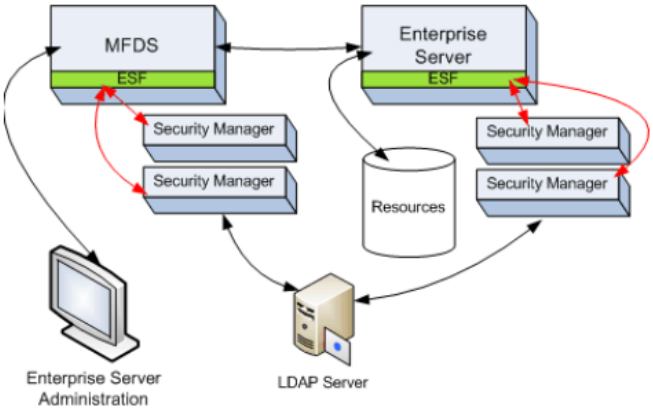
下記の画像は Linux9 環境で稼働している MFDS の［RHEL9］のみに OpenLDAP を連携させたものです。

Windows11 環境の MFDS）

Linux9 環境の MFDS）

MFDS と連携させることで、MFDS が管理する Enterprise Server インスタンスにセキュリティ設定を行うことができます。

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、そのクエリ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 の使用を強く推奨します。

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、セキュリティク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:

セキュリティクエリによるパフォーマンスの観点から、Enterprise Server インスタンスと ESM は同じマシンに設置することを推奨します。

3. OpenLDAP の構築

Red Hat Enterprise Linux 8 以降では標準レポジトリに openldap-servers パッケージが含まれないため、本書では EPEL の追加リポジトリを使用して OpenLDAP を構築します。別途入手した OpenLDAP インストールして使用することも可能です。実行はすべてルートユーザーで行います。

1）EPEL リポジトリの有効化

コマンド例）

subscription-manager repos --enable codeready-builder-for-rhel-9-$(arch)-rpms

2）

```
# subscription-manager repos --enable codeready-builder-for-rhel-9-$(arch)-rpms
リポジトリー 'codeready-builder-for-rhel-9-x86_64-rpms' は、このシステムに対して有効になりました。
```

コマンド例）

dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm

```
# dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
サブスクリプション管理リポジトリーを更新しています。
Red Hat CodeReady Linux Builder for RHEL 9 x86_64 (RPMs)          7.2 MB/s | 6.4 MB     00:00
epel-release-latest-9.noarch.rpm                                   18 kB/s |  19 kB     00:01
依存関係が解決しました。
================================================================================
 パッケージ              アーキテクチャー      バージョン              リポジトリー          サイズ
================================================================================
インストール:
 epel-release            noarch                9-7.el9                 @commandline          19 k

トランザクションの概要
================================================================================
インストール  1 パッケージ
```

3）OpenLDAP サーバーのインストール

コマンド例）yum install openldap-servers

```
================================================================================
 パッケージ              アーキテクチャー      バージョン              リポジトリー          サイズ
================================================================================
インストール:
 openldap-servers        x86_64                2.6.3-1.el9             epel          2.3 M

トランザクションの概要
================================================================================
インストール  1 パッケージ
```

4）OpenLDAP クライアントのインストール

コマンド例）yum install openldap-clients

```
================================================================================
 パッケージ              Arch          バージョン              リポジトリー          サイズ
================================================================================
インストール:
 openldap-clients        x86_64        2.6.3-1.el9             rhel-9-for-x86_64-baseos-rpms  182 k

トランザクションの概要
================================================================================
インストール  1 パッケージ
```

5）OpenLDAP スキーマの拡張とロード

OpenLDAP の初期構築と Enterprise Server で使用するスキーマの拡張を実行するサンプルファイル類を任意のディレクトリへ展開後、シェルを実行します。このサンプルは、Web ページの本動作検証結果報告書の下にあるリンクからダウンロードしてください。実行前に内容をご確認のうえ、環境に合わせて利用者の責任において自由に変更してご使用いただけます。

サンプルファイル名）rhel_9_openldap_2.6.3.tgz

① サンプルファイルの解凍

サンプルファイルを解凍すると配下にディレクトリが作成され、OpenLDAP 構築に必要なファイルが展開されます。

コマンド例)tar zxvf rhel_9_openldap_2.6.3.tgz

```
# tar zxvf rhel_9_openldap_2.6.3.tgz
rhel_9_openldap_2.6.3/
rhel_9_openldap_2.6.3/openldap-setup/
rhel_9_openldap_2.6.3/openldap-setup/chrootpwd.ldif
rhel_9_openldap_2.6.3/openldap-setup/ppolicy.ldif
rhel_9_openldap_2.6.3/openldap-setup/backend.ldif
rhel_9_openldap_2.6.3/openldap-setup/configure-openldap.sh
rhel_9_openldap_2.6.3/openldap-setup/schema/
rhel_9_openldap_2.6.3/openldap-setup/schema/container.schema
rhel_9_openldap_2.6.3/openldap-setup/schema/mf-containers.ldif
rhel_9_openldap_2.6.3/openldap-setup/schema/ppolicy.schema
rhel_9_openldap_2.6.3/openldap-setup/schema/schema_convert.conf
rhel_9_openldap_2.6.3/openldap-setup/schema/top.ldif
```

② 環境変数の設定

製品が稼働するために必要な環境変数を指定します。

1行目： LANG で指定する ja_JP.sjis がマシンにインストールされていないと ESCWA、MFDS は正常に起動できません。localectl list-locales コマンドなどでこの存在を確認してください。

2行目： 製品をインストールしたディレクトリ配下の /bin/cobsetenv を指定します。

3行目： 64 ビット稼働モードを指定しています。

コマンド例)

```
export LANG=ja_JP.sjis
. /opt/mf/ED90PU1/bin/cobsetenv
export COBMODE=64
```

③ configure-openldap.sh の編集

サンプルに含まれる configure-openldap.sh を環境に合わせて変更します。

- パスワードの変更

  必要であれば指定された2つのパスワードを変更します。

  本書では変更せずにこのまま password を使用します。

```
echo 'INFO: Please create a password for your LDAP directory configuration.'

#confirm_password
password="configpw"
```

```
echo 'INFO: Please create a password for administrator connection.'

#confirm_password
password="password"
```

・ 製品インストールパスの指定

製品をインストールしたパスに変更します。

変更前）

```
echo 'INFO: Modify /opt/ed92/etc/es_default_ldap_openldap.ldf.'↓
rm $currentdir/schema/es_default_ldap_openldap.ldif↓
sed 's/DC=X/CN=Micro Focus,dc=secldap,dc=com/' /opt/ed92/etc/es_default_ldap_openldap.ldf > $currentdir/schema/es_default_ldap_openldap.ldif
```

変更後）

```
echo 'INFO: Modify /opt/mf/ED90PU1/etc/es_default_ldap_openldap.ldf.'↓
rm $currentdir/schema/es_default_ldap_openldap.ldif↓
sed 's/DC=X/CN=Micro Focus,dc=secldap,dc=com/' /opt/mf/ED90PU1/etc/es_default_ldap_openldap.ldf > $currentdir/schema/es_default_ldap_openldap.ldif
```

④ configure-openldap.sh の実行

configure-openldap.sh が存在するパスに移動し、実行権限があることを確認します。

コマンド例）

cd /home/tarot/ldap/rhel_9_openldap_2.6.3/openldap-setup

ll

```
# ll
合計 28
-rwxrwxrwx 1 tarot tarot  588 12月 25 19:32 backend.ldif
-rwxrwxrwx 1 tarot tarot  123 12月 25 19:32 chrootpwd.ldif
-rwxrwxrwx 1 tarot tarot 7017 11月 10 01:52 configure-openldap.sh
-rwxrwxrwx 1 tarot tarot 4570 11月  8 04:31 ppolicy.ldif
drwxrwxrwx 4 tarot tarot 4096 12月 25 19:32 schema
```

configure-openldap.sh を実行します。

コマンド例）./configure-openldap.sh

```
INFO: Modify /opt/mf/ED90PU1/etc/es_default_ldap_openldap.ldf.
INFO: ldapadd es_default_ldap_openldap.ldf. Log written to log/es_default_ldap_openldap.log.
ldap_initialize( ldap://localhost:389 )
ldap_add: Invalid DN syntax (34)
        additional info: invalid DN
INFO: Output written to ./schema/es_default_ldap_openldap.txt.
```

⑤ リソース定義の確認

シェルの実行により OpenLDAP に Enterprise Server インスタンスで使用するリソース定義がロードされていることを確認します。

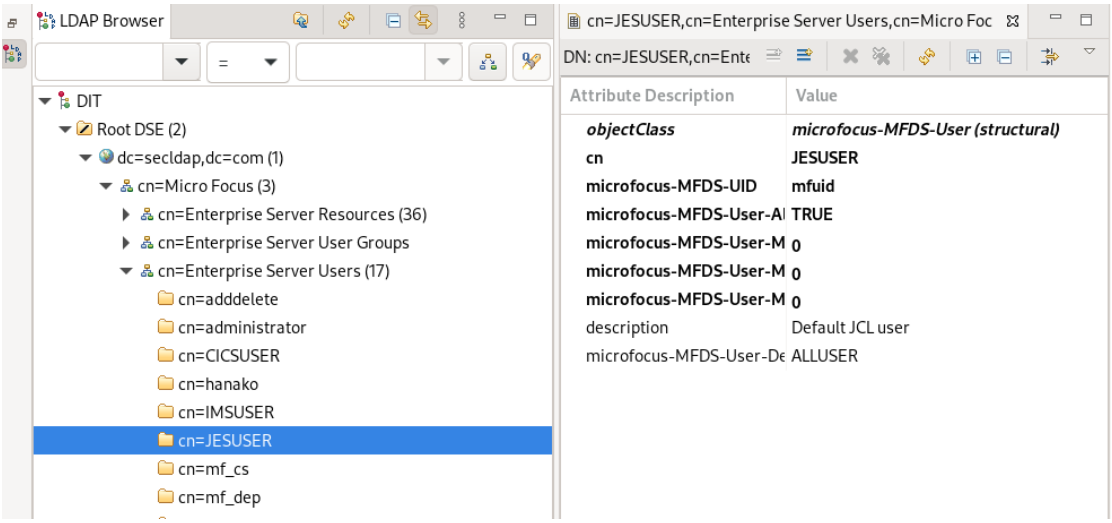
コマンド例）改行は含まれません。

ldapsearch -H ldap://localhost:389 -b ”cn=Enterprise Server Users,cn=Micro Focus,dc=secldap,dc=com” -x -D ”cn=Manager,dc=secldap,dc=com” -w password

```
# extended LDIF
#
# LDAPv3
# base <cn=Enterprise Server Users,cn=Micro Focus,dc=secldap,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# Enterprise Server Users, Micro Focus, secldap.com
dn: cn=Enterprise Server Users,cn=Micro Focus,dc=secldap,dc=com
cn: Enterprise Server Users
objectClass: container
```

```
# administrator, Enterprise Server Users, Micro Focus, secldap.com
dn: cn=administrator,cn=Enterprise Server Users,cn=Micro Focus,dc=secldap,dc=c
 om
cn: administrator
objectClass: microfocus-MFDS-User
microfocus-MFDS-UID: 1.2.840.5043.09.002.1703480864.4
microfocus-MFDS-User-MTO-Priority: 0
microfocus-MFDS-User-MTO-Timeout: 0
microfocus-MFDS-User-MTO-OperatorClass: 0
microfocus-MFDS-User-AllowLogon: TRUE
microfocus-MFDS-User-Pwd: MF-MD5:SMvAqpFw:dNTBrrSylrzCJPDUXCsR4+==

# search result
search: 2
result: 0 Success

# numResponses: 17
# numEntries: 16
```

外部の GUI ツールを使用すれば内容がよりわかりやすく確認できます。



⑥ OpenLDAP の確認

OpenLDAP が開始されていることを確認します。停止している場合は起動してください。

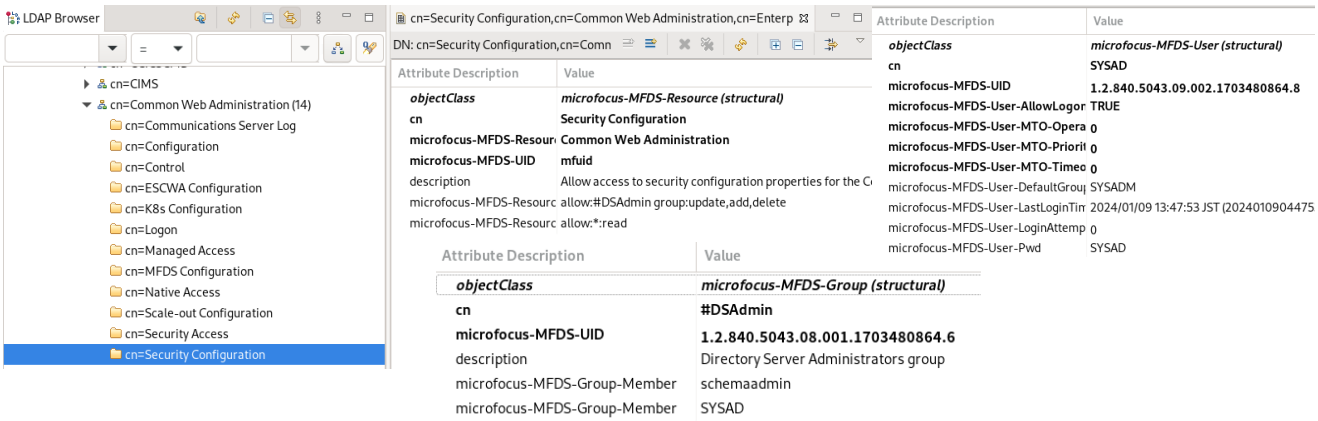
確認コマンド例)systemctl status slapd

```
# systemctl status slapd
* slapd.service - OpenLDAP Server Daemon
     Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; preset: disabled)
     Active: active (running) since Fri 2024-01-05 16:29:50 JST; 18h ago
```

4. ESCWA への適用

Linux9 環境に構築された OpenLDAP を ESCWA へ適用します。

ESCWA のセキュリティ設定に権限があるユーザーを使用して実施します。本書では #DSAdmin グループに所属する SYSAD ユーザーを使用します。



また、SYSAD ユーザーのパスワードはわかりやすいように SYSAD に変更しています。

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。

- 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 openldap とします。
- モジュール：mldap_esm を指定します。
- 接続パス：

  OpenLDAP が構築されているマシンの IP もしくは ホスト名を指定し、389 番ポートを指定します。

  本書では名前解決されている RHEL9:389 を指定します。
- 認証 ID：

  configure-openldap.sh で指定した値を指定します。

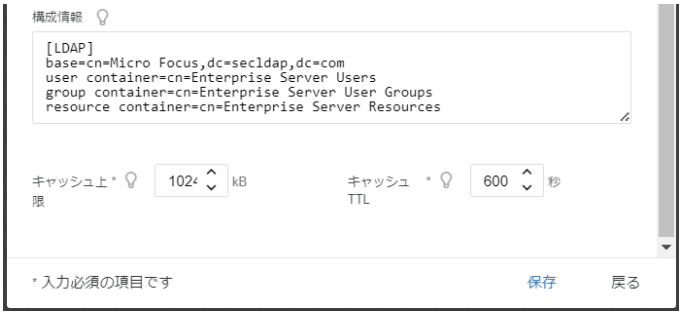
  本書では cn=Manager,dc=secldap,dc=com が該当します。
- パスワード：

  configure-openldap.sh 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。

  [LDAP]
  base=cn=Micro Focus,dc=secldap,dc=com
  user container=cn=Enterprise Server Users
  group container=cn=Enterprise Server User Groups
  resource container=cn=Enterprise Server Resources



連携が成功した時点で ESCWA のリソースに関連するユーザー権限が有効になり、セッションがタイムアウトすると ESCWA へのログオンを求められます。この場合は、再度 SYSAD ユーザーでログインします。

ESCWA のセキュリティ設定の変更を有効にするため、操作権限を持つユーザーで ESCWA を再起動します。本書では Windows 環境の ESCWA を使用しているため、Windows のサービスを再起動しますが、

Linux 環境の ESCWA を利用している場合は下記のコマンドを実行します。

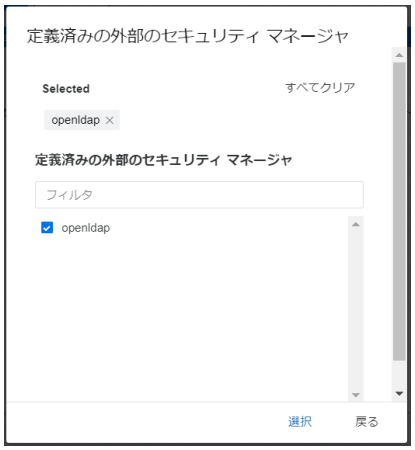
停止コマンド例)escwa --shutdown SYSAD SYSAD

開始コマンド例)改行は入りません。

nohup escwa --BasicConfig.MfRequestedEndpoint="tcp:*:10086" --write=true < /dev/null > escwa.out 2>&1 &

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［openldap］にチェックして［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。

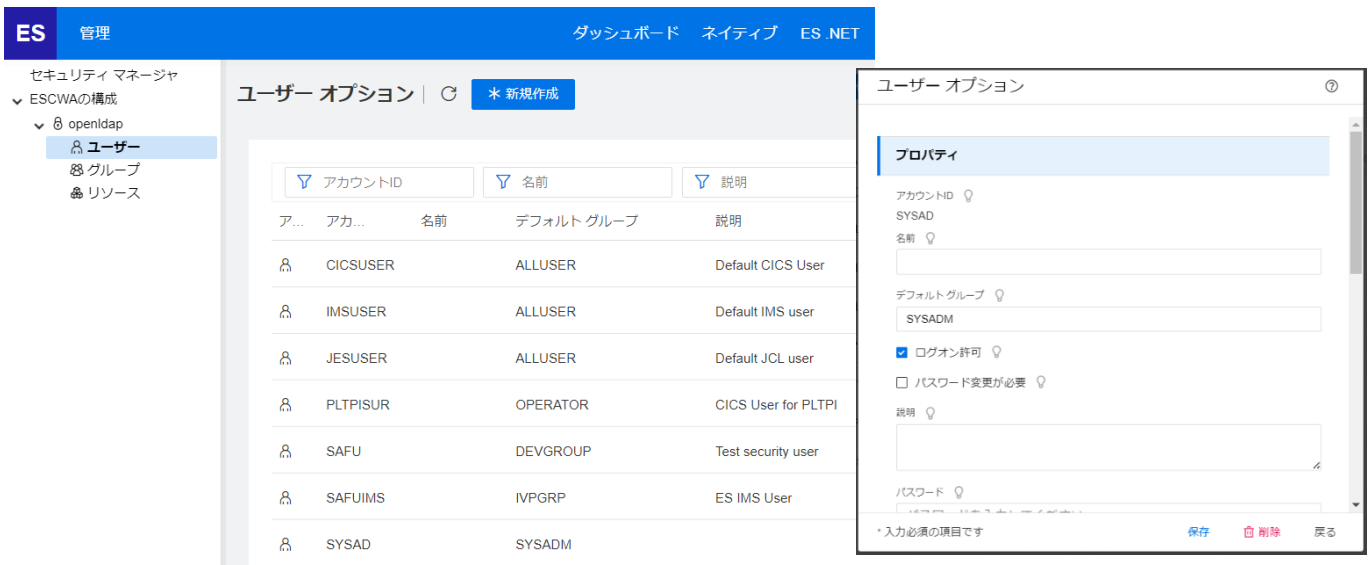


変更を反映するために［適用］ボタンをクリックします。

変更権限をチェックする画面が表示されます。
SYSAD を指定して［ログオン］をクリックします。

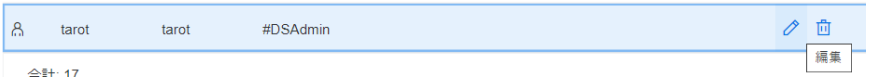
［セキュリティマネージャリスト］に［openldap］が追加され、左側メニューにも［openldap］が表示されます。

左側メニューの［openldap］をクリックすると、Linux9 環境で構築した OpenLDAP のリソースが表示されます。これにより ESCWA 上でリソース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］ボタンをクリックして値を入力後に［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。



もちろん Linux9 環境で LDAP クライアントコマンドを利用したメンテナンスも可能です。

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

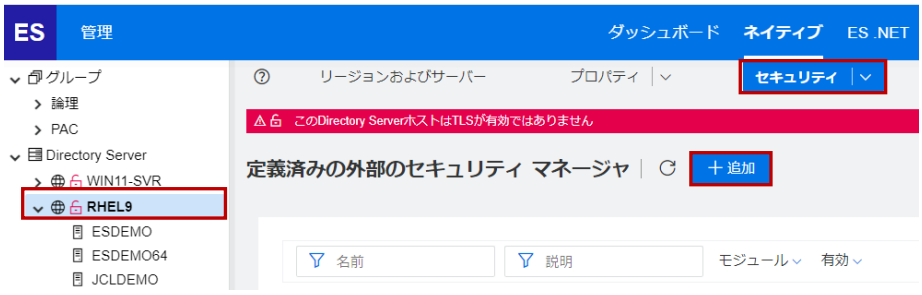
JES 関連	エンティティ	アクセス レベル
ジョブ名によるジョブのサブミットおよびキャンセルの制御。	CANCEL *localnodeid.userid.jobname* (ジョブのキャンセル権限の場合) SUBMIT *localnodeid.jobname.userid* (ジョブのサブミットの場合) *localnodeid* は、エンタープライズ サーバーの名前です。 これらのルールは、一般的には使用されませんが、特殊な要件を持つ環境に対して細かな制御を提供します。	NONE アクセスは許可されません。 READ ユーザーはジョブをサブミットできます。 UPDATE READ と同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

5. MFDS への適用

Linux9 環境に構築された OpenLDAP を ESCWA に表示された［RHEL9］で稼働している MFDS へ適用します。MFDS においても権限のある SYSAD ユーザーを使用します。

ESCWA の［ネイティブ］を選択します。

左側メニューの［RHEL9］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。



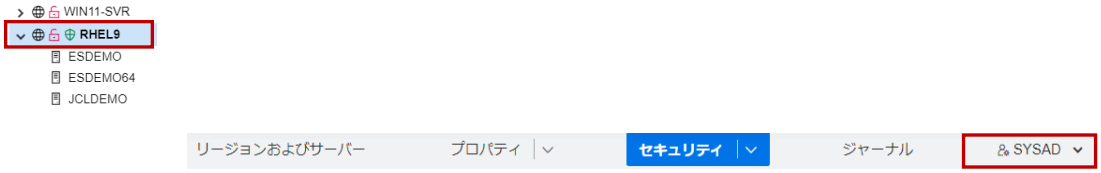
ESCWA と同様の［定義済みの外部のセキュリティマネージャ］画面が表示されますので、ESCWA と同じ値を入力して保存すると一覧に表示されます。

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［openldap］にチェックして［選択］ボタンをクリックすると、[openldap］がリストに表示されますので、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、上記デフォルトで設定した openldap 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 へのログイン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。



6. Enterprise Server インスタンスへの適用

［RHEL9］にある作成済の JCLDEMO インスタンスに MFDS と連携させた openldp を適用します。

左側メニューの［RHEL9＞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。

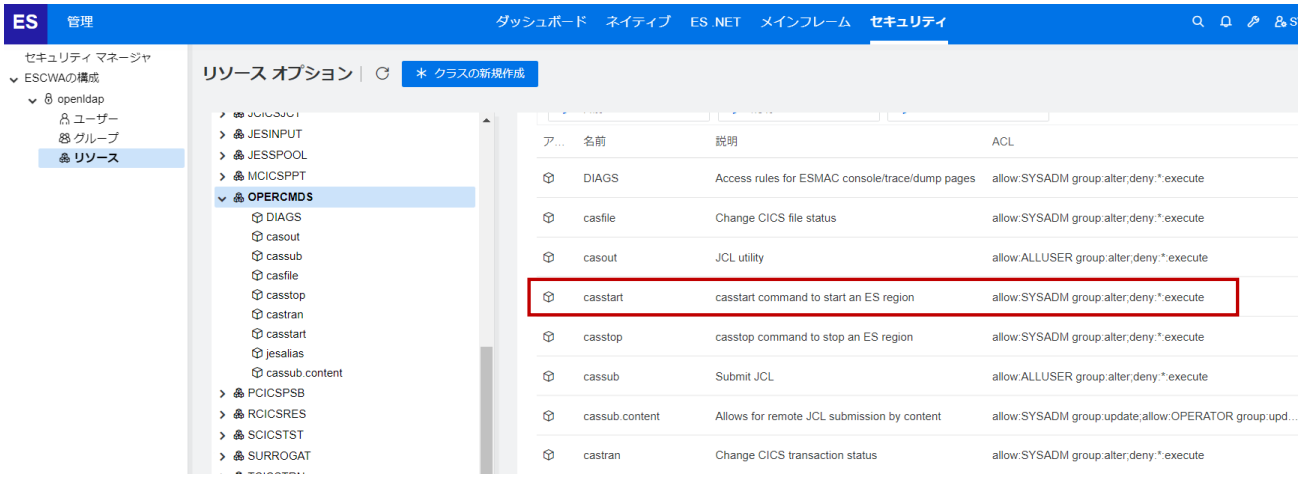
［リージョンのセキュリティ機能の構成］画面の［デフォルトのセキュリティ機能の構成を使用］にチェックを入れると［セキュリティマネージャリスト］に［openldap］が表示されます。

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。

7. Enterprise Server インスタンスの開始

openldap 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 openldap の［OPERCMDS］リソースを確認すると、起動コマンドである 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。

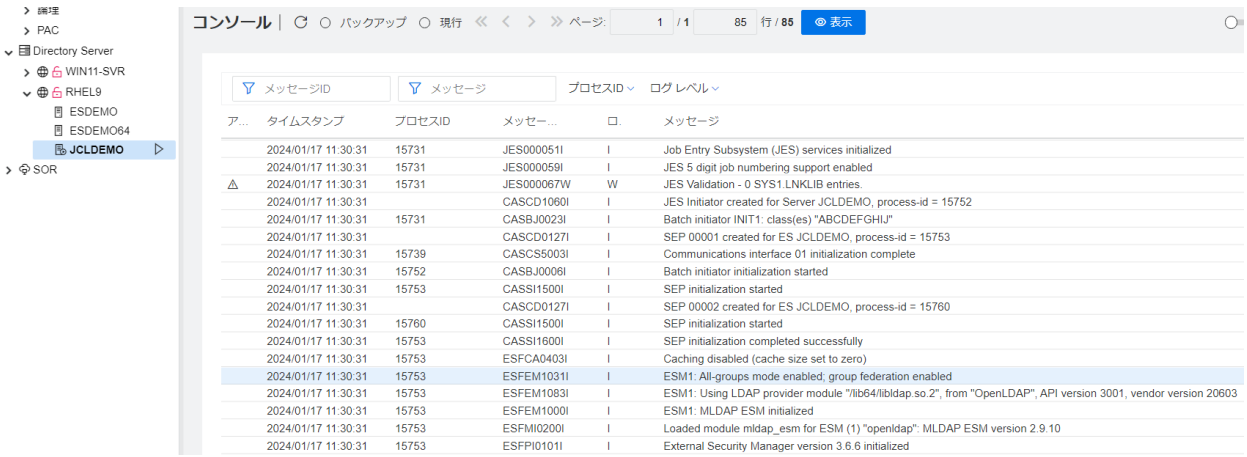


現在、このグループに所属しているユーザーは SYSAD と tarot ユーザーです。

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

```
# casstart /rJCLDEMO /uSYSAD /pSYSAD
..
CASCD0167I ES Daemon successfully auto-started 11:30:30
CASCD1005I /var/mfcobol/es/JCLDEMO/console.log 11:30:30
CASCD0050I ES "JCLDEMO" initiation is starting 11:30:30
```

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。



8. 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 openldap の［OPERCMDS］リソースを確認すると、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 /rJCLDEMO /j/home/tarot/rjcldemo/copy1.jcl /uJESUSER /ppassword
CASBJ0047S JES Submit: User ID "JESUSER" not authorized 11:52:39
Processed "/home/tarot/rjcldemo/copy1.jcl"
```

コンソールログにも同じ内容が記録されます。

CASBJ0047S	S	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 /rJCLDEMO /j/home/tarot/rjcldemo/copy1.jcl /uSYSAD /pSYSAD
JCLCM0187I J0001002 COPY1    JOB  SUBMITTED (JOBNAME=COPY1,JOBNUM=0001002) 13:19:56
JCLCM0180I J0001002 COPY1    Job ready for execution. 13:19:56
Processed "/home/tarot/rjcldemo/copy1.jcl"
```

コンソールログ）

JCLCM0187I	I	J0001002 COPY1 JOB SUBMITTED (JOBNAME=COPY1,JOBNUM=0001002)
JCLCM0180I	I	J0001002 COPY1 Job ready for execution.
JES0000004I	I	J0001002 COPY1 JOB DISPATCHED
JCLCM0188I	I	J0001002 COPY1 JOB STARTED
JCLCM0182I	I	J0001002 COPY1 JOB ENDED - COND CODE 0000

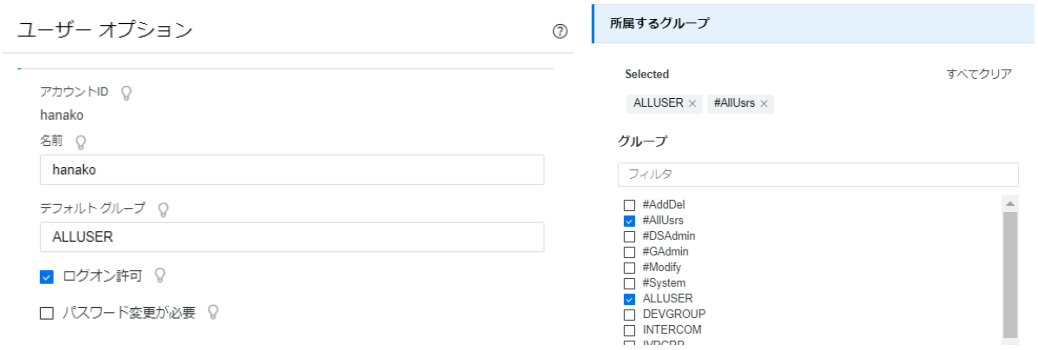
スプール）

9. CICS PCT の実行

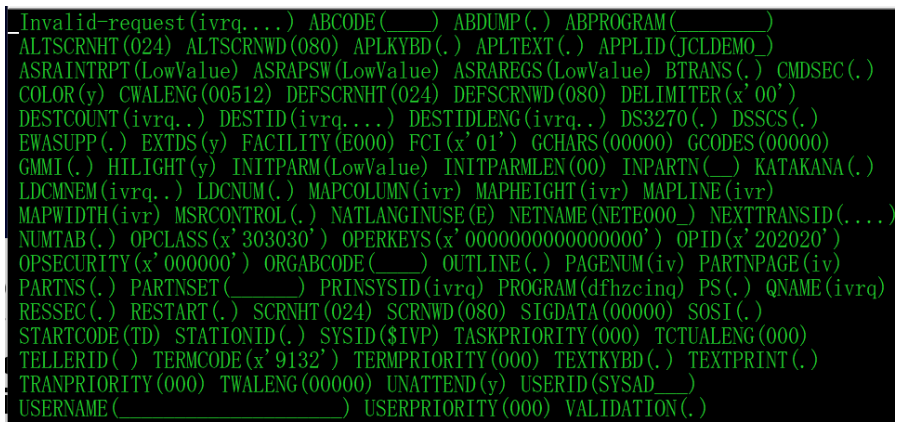
JCLDEMO インスタンスを使用して CICS の PCT である CINQ を実行します。

ESCWA の［セキュリティ］から openldap 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［OPERATOR group］と［SYSADM group］に所属するユーザーであることが確認できます。

権限のあるグループに属さない hanako 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え、結果は確認できません。



権限のある SYSAD ユーザーでは正常に実行され、結果が表示されます。



10. 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 openldap の［OPERCMDS］リソースを確認し、停止コマンドである cassop の実行権限を持つユーザーで停止します。


```
# casstop /rJCLDEMO /uSYSAD /pSYSAD
```

11. おわりに

製品と ESM の1つである OpenLDAP を連携することにより、ESCWA や MFDS へのログインや 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。

また、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の設定やグループ設計、ESM 全般について精通している、などの事柄も重要になります。

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 に関する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。