動作検証報告書

Micro Focus 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 2.4.44 版

Micro Focus の Enterprise Developer / Enterprise Server はメインフレームで稼働している COBOL, PL/I アプリケーションを Linux/UNIX や Windows OS へリホストして、メインフレームの開発コストや運用コストの削減を実現可能にする製品です。また、JES や CICS, IMS などのミドルウェアをエミュレートしており、リホスト時の負担を軽減することもできます。

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１つの重要な課題です。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。

MICRO FOCUS

動作検証報告書

Micro Focus 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 Server release 7.2

2) Linux カーネルバージョン

Linux version 3.10.0-327.el7.x86_64

3) OpenLDAP バージョン

openldap-servers-2.4.44-15.el7_5.x86_64

openldap-clients-2.4.44-15.el7_5.x86_64

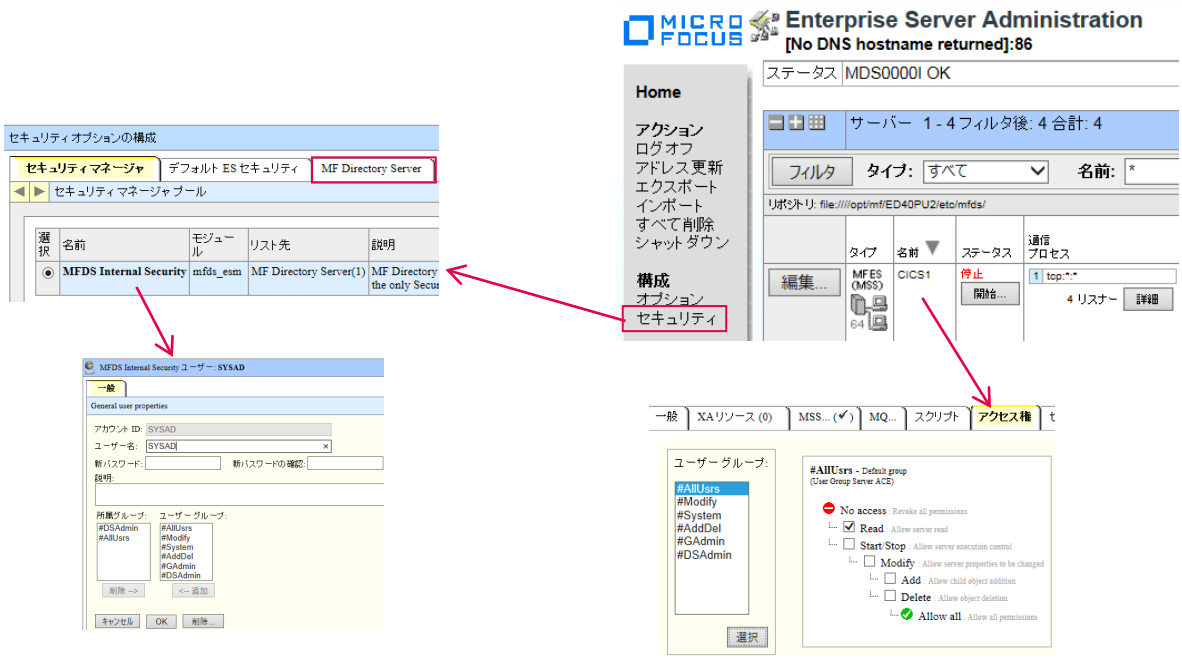
4) Micro Focus 製品 バージョン

Micro Focus Enterprise Developer 4.0 Patch Update 2

補足）Micro Focus Enterprise Server と同等の開発用実行環境を含んでいます。

2. Enterprise Server インスタンスのセキュリティオプション

製品にはデフォルトでセキュリティ機能が搭載されており、これを各インスタンスへ設定するとオペレーティングシステムのアクセスレベルとは関係なく、実行ユーザーID 単位にアプリケーションやリソースへのアクセス制御が可能になります。デフォルト設定の内容は複数の Enterprise Server インスタンスを管理する Administration 画面で確認することができます。



セキュリティ要件に合わせた詳細なアクセス制御が必要な場合は外部セキュリティマネージャ（以下 ESM と称する）を構築後、セキュリティマネージャに追加し、連携させて各インスタンスへ反映させることになります。

この Administration 画面は Windows では Micro Focus Directory Server（以下 MFDS と称する）サービスとして、 Linux/UNIX では目的に沿った環境変数を指定後に MFDS コマンド実行により ESM と連携して起動させます。

注意）

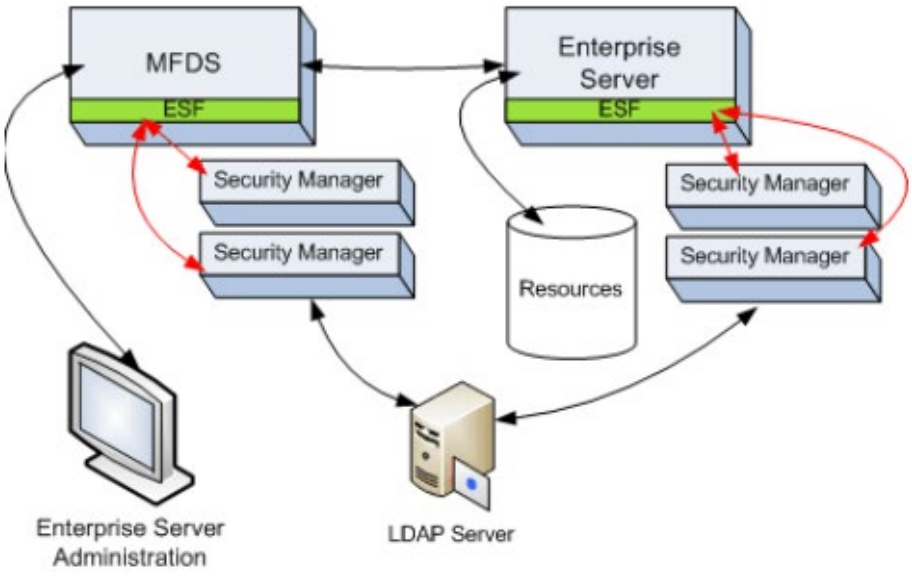
システムの堅牢性を確保するには矛盾が生じないよう MFDS と Enterprise Server インスタンスの両方に同じセキュリティマネージャを設定してください。

3. Enterprise Server のセキュリティ アーキテクチャ

1) 関連するシステムコンポーネントとプロセスフロー

ユーザーが Enterprise Server インスタンスの機能やアプリケーションへのアクセス、またはアプリケーションからリソースにアクセスする際、Enterprise Server インスタンスの External Security Facility（以下 ESF と称する）は、そのアクションを認証または許可することが適切であるかチェックするために ESM へセキュリティクエリを送信し、そのクエリ結果で判定を行っています。

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。

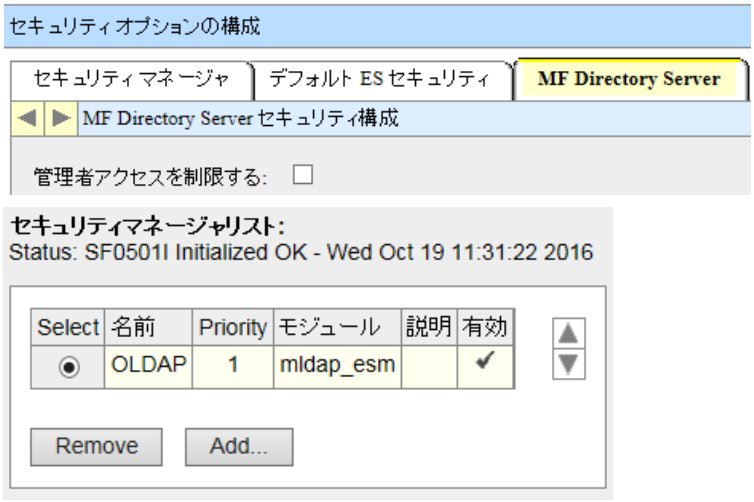


2) External Security Facility (ESF)

ESF は、Enterprise Server インスタンスおよび MFDS 両方へのアクセスを管理し、セキュリティマネージャへアプリケーションやリソースのアクセス許可要求クエリを送信します。

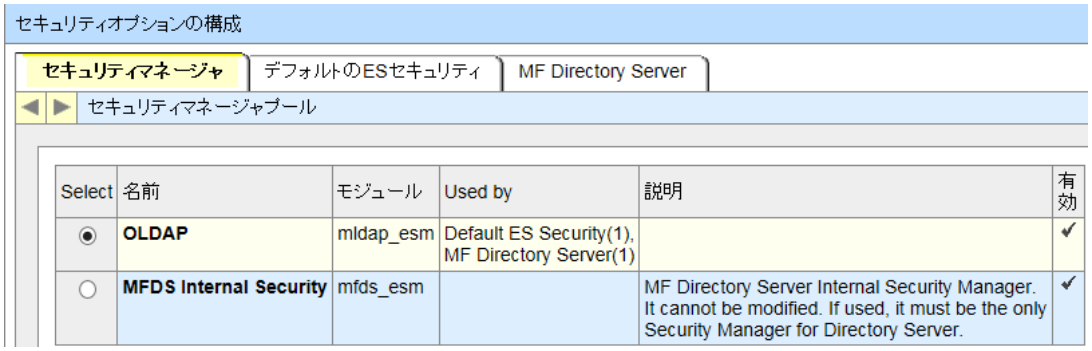
下記機能を担当します。

1. 関連するセキュリティマネージャの読み込みと呼び出し
2. セキュリティマネージャへセキュリティ要求クエリを送信
3. クエリ結果の管理
4. セキュリティマネージャと自身の構成情報メンテナンス



3) セキュリティマネージャ

セキュリティマネージャは ESF によって生成されたセキュリティ要求クエリを処理して、許可、拒否または不明のいずれかのステータスを返却します。セキュリティマネージャプールへ複数のセキュリティマネージャを設定して利用することも可能です。



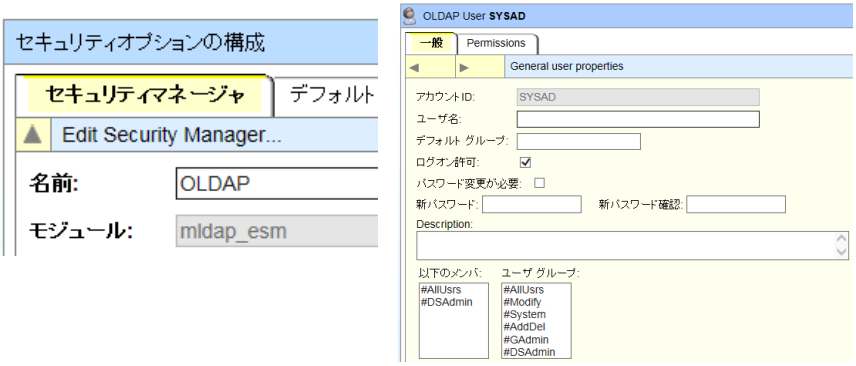
MFDS には下記セキュリティマネージャモジュールが含まれており、定義することにより使用できます。

1. osesm：Windows のみ

   Windows OS のユーザー構成へのアクセスを提供します。これにより Windows ユーザーを認証後にアクセスレベルに応じた許可を適用することができます。

2. mldap_esm：

   この利用により Enterprise Server のセキュリティを LDAP と統合することができます。OpenLDAP と Microsoft Active Directory の両方で使用することができ、ユーザーアクセス管理やアプリケーションが使用するファイルのアクセス管理が可能となります。



3. MFDS Internal Security：
   他のセキュリティマネージャが存在しない場合に使用されます。ユーザーとグループを定義し、Administration 画面機能へのアクセスを制限できます。
4. CASESM：
   CAS ESM モジュール（casesm）は Enterprise Server の CICS リソース定義に格納されているレガシーセキュリティ定義を使用します。これは旧製品で使用されていたモデルとなります。

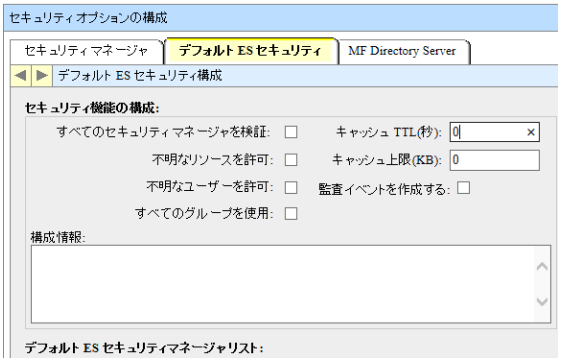
4) セキュリティポリシーの設計

セキュリティポリシーの設計と導入には慎重な計画が必要です。設計に関する考慮事項は本書の範疇を超えるため、セキュリティ機能を使用したユーザーの認証、およびリソースのアクセス制御を管理する手順について簡単に説明します。

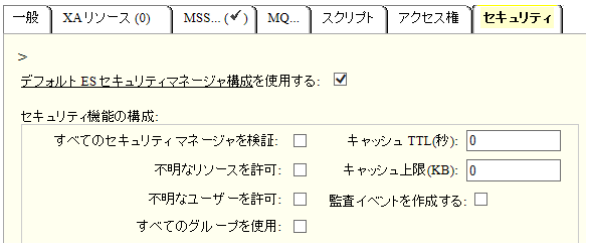
1. 使用する外部セキュリティマネージャを決定します。一般的には 1 つの外部セキュリティマネージャが使用されますが、複数使用する際には各外部セキュリティマネージャ間の責任を決定する必要があります。
2. 使用する外部セキュリティマネージャが管理するリポジトリ内に、必要なユーザー、リソース、およびルールを定義する必要があります。この定義にはデフォルトの MFDS セキュリティ定義からのユーザーやリソースの移行と、MLDAP ESM モジュールを使用する LDAP リポジトリの場合はセキュリティ情報をサポートするためのスキーマ変更が含まれます。
3. 次に、外部セキュリティマネージャに接続するために使用される ESM モジュールと、これに関連する設定情報を MFDS へ設定します。これによりセキュリティマネージャプールへ追加されます。

4. この時点でセキュリティ構成オプションの定義を行うことができます。各 Enterprise Server インスタンスに異なる構成オプションを指定することも可能ですし、全インスタンスにデフォルトの構成を指定することも可能です。

【 MFDS 】



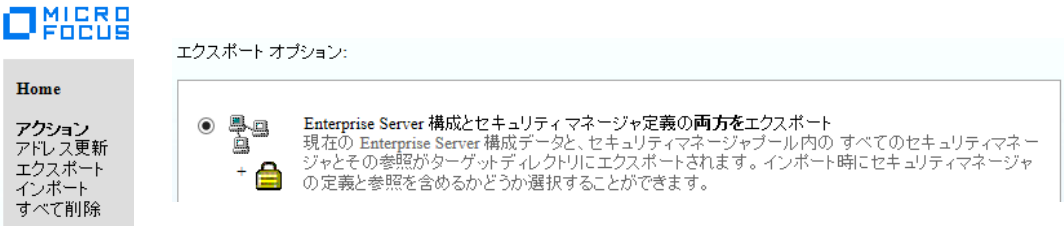
【各インスタンス】



5. 構成オプションには使用するセキュリティマネージャの参照順序付きリストが含まれています。他オプションと同様に、Enterprise Server インスタンス毎に異なるリストを指定することも可能ですし、全インスタンスにデフォルトのリストを指定することも可能です。リストの順序は要求を処理する際の順序となります。

4. OpenLDAP の構成設定

事前に Enterprise Server Administration 画面の左側メニューから [エクスポート] をクリックし、構成とセキュリティマネージャの両方をエクスポートしてバックアップすることをお勧めします。



1) OpenLDAP 構築の事前準備

root 権限を持つユーザーで下記作業を行います。

1. Server と Client 両方がインストールされており、正常稼働の実績があること。
   インストール例）yum -y install openldap openldap-clients openldap-servers

2. Enterprise Server インスタンスの稼働ビット数と OpenLDAP Client の対応ビット数が一致していること。
   例）32 ビットで稼働させる場合は OpenLDAP Client 32 ビットを使用します。
   本書では 64 ビットを使用しています。

3. firewall を使用している場合は、OpenLDAP がデフォルトで使用する 389 ポートを LDAP プロトコルが使用することを許可します。

4. OpenLDAP のデータを管理するために使用する Berkeley DB の設定ファイルをサンプルからコピーします。
   例）cp -a /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG

5. slapd サービスは ldap ユーザーとして実行されるためディレクトリ所有者を変更します。
   例）chown -R ldap:ldap /var/lib/ldap

2) slapd サービス の開始

slapd サービスは /etc/openldap/slapd.d/ ディレクトリに存在する設定値を使用して起動されます。

1. slapd サービス自動起動
   サーバ起動時に slapd サービスを自動起動するよう設定します。
   コマンド）systemctl enable slapd

2. slapd サービス起動
   slapd サービスを開始します。
   コマンド）systemctl start slapd

3. slapd サービスのステータス確認
   slapd サービスのステータスが Active であることを確認します。
   コマンド）systemctl status slapd

```
● slapd.service - OpenLDAP Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)
   Active: active (running) since 木 2018-11-01 10:05:22 JST; 1h 13min ago
     Docs: man:slapd
           man:slapd-config
           man:slapd-hdb
           man:slapd-mdb
           file:///usr/share/doc/openldap-servers/guide.html
 Main PID: 624 (slapd)
   CGroup: /system.slice/slapd.service
           └─624 /usr/sbin/slapd -u ldap -h ldapi:/// ldap:///
```

4. ポートの使用確認

slapd サービスが 389 ポートで LISTEN 状態であることを確認します。

コマンド）lsof -i:389

```
COMMAND PID USER   FD   TYPE  DEVICE SIZE/OFF NODE NAME
slapd   624 ldap    8u  IPv4 2428165      0t0  TCP *:ldap (LISTEN)
slapd   624 ldap    9u  IPv6 2428166      0t0  TCP *:ldap (LISTEN)
```

3) OpenLDAP 構成設定

root 権限を持つユーザーで下記設定を行います。

1. 作業用ディレクトリの作成

構成時に使用する ldif ファイルを置く作業用ディレクトリを作成します。このディレクトリパスは任意ですので、作業者の書き込み権限があるディレクトリへ作成してください。

例）mkdir /etc/openldap/work

2. パスワードの暗号化生成

OpenLDAP に使用する管理者パスワードを暗号化します。

【実行コマンド】

slappasswd -s password

【実行結果】

{SSHA}TOml4t9wEyeqmFyCQlEFsOhcvey2tSvG

3. パスワードの変更と登録

管理者パスワードを変更するために change-password.ldif ファイルを作業用ディレクトリへ作成して登録します。olcRootPW の値は前項で暗号化した値を指定します。

【 ldif ファイル内容】

```
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}TOml4t9wEyeqmFyCQlEFsOhcvey2tSvG
```

【 登録コマンド】

ldapadd -Y EXTERNAL -H ldapi:// -f /etc/openldap/work/change-password.ldif

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

4. ベースエントリの変更

ベース DN の dc=my-domain,dc=com を dc=mfldap,dc=com へ変更するため change-domain.ldif ファイルを作業用ディレクトリへ作成して登録します。

【 ldif ファイル内容】

```
dn: olcDatabase={1}monitor,cn=config
                changetype: modify
                replace: olcAccess
                olcAccess: {0}to * by
dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
 read by dn.base="cn=Manager,dc=mfldap,dc=com" read by * none

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=mfldap,dc=com

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=Manager,dc=mfldap,dc=com

dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}TOml4t9wEyeqmFyCQlEFsOhcvey2tSvG
```

【 登録コマンド】

ldapmodify -x -D cn=config -w password -f /etc/openldap/work/change-domain.ldif

```
#ldapmodify -x -D cn=config -w password -f /etc/openldap/work/change-domain.ldif
modifying entry "olcDatabase={1}monitor,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"
```

5. ベースエントリの登録

ベースエントリを作成するため base.ldif ファイルを作業用ディレクトリへ作成して登録します。

【 ldif ファイル内容】

```
dn: dc=mfldap,dc=com
objectClass: dcObject
objectClass: organization
dc: mfldap
o: Micro Focus
```

【 登録コマンド】

ldapadd -x -D "cn=Manager,dc=mfldap,dc=com" -w password -f /etc/openldap/work/base.ldif

```
#ldapadd -x -D "cn=Manager,dc=mfldap,dc=com" -w password -f /etc/openldap/work/base.ldif
adding new entry "dc=mfldap,dc=com"
```

4) Enterprise Server スキーマ定義のエクスポート

Enterprise Developer または Enterprise Server の環境変数を設定後、スキーマをエクスポートします。

例 1）. /opt/mf/ED40PU2/bin/cobsetenv

例 2）export COBMODE=64

1. Enterprise Server スキーマ定義のエクスポート

MFDS スキーマを下記コマンドでエクスポートすると mfds.schema ファイルがカレントディレクトリに生成されます。

【実行コマンド】

mfds -l "dc=mfldap,dc=com" 2 mfds.schema

2. コンテナスキーマ定義の作成

コンテナスキーマを作成するため container.schema ファイルを作業用ディレクトリへ作成します。

【 schema ファイル内容】

```
objectclass (
        1.2.840.113556.1.3.23
        NAME 'container'
        SUP top
        STRUCTURAL
            MUST ( cn ) )
```

3. スキーマファイル拡張子の変換

/etc/openldap/schema ディレクトリを作業用ディレクトリへコピーします。次に拡張子を変換する対象スキーマファイルを指定した schema_convert.conf ファイルをコピー先の schema ディレクトリへ作成します。また前項でエクスポートした mfds.schema ファイルと container.schema ファイルもこのディレクトリへコピーして、コマンドを実行します。

【 conf ファイル内容】

```
include corba.schema
include core.schema
include cosine.schema
include duaconf.schema
include dyngroup.schema
include inetorgperson.schema
include java.schema
include misc.schema
include nis.schema
include openldap.schema
include ppolicy.schema
include collective.schema
include container.schema
include mfds.schema
```

【実行コマンド】

```
slaptest -f /etc/openldap/work/schema/schema_convert.conf -F .
```

注意）最後の “.” はコマンドに含まれます。

```
#slaptest -f /etc/openldap/work/schema/schema_convert.conf -F .
config file testing succeeded
```

4. 生成されたファイルのコピーと権限設定

前項のコマンドにより /etc/openldap/work/schema/cn=config/cn=schema へ生成された全ファイルを /etc/openldap/slapd.d/cn=config/cn=schema ディレクトリへコピーして所有者を変更します。

【所有者変更コマンド】

```
chown -R ldap:ldap /etc/openldap/slapd.d/cn=config/cn=schema
```

5. slapd サービスの再起動

変更を有効にするためサービスを再起動し、正常に起動されたことを確認します。

コマンド）systemctl restart slapd

6. コンテナ定義の作成

コンテナスキーマを作成するため mf-containers.ldif ファイルを作業用ディレクトリへ作成して登録します。

【 ldif ファイル内容】

dn: cn=Micro Focus,dc=mfldap,dc=com

cn: Micro Focus

objectClass: container

dn: cn=Enterprise Server Users,cn=Micro Focus,dc=mfldap,dc=com

cn: Enterprise Server Users

objectClass: container

dn: cn=Enterprise Server User Groups,cn=Micro Focus,dc=mfldap,dc=com

cn: Enterprise Server User Groups

objectClass: container

dn: cn=Enterprise Server Resources,cn=Micro Focus,dc=mfldap,dc=com

cn: Enterprise Server Resources

objectClass: container

【 登録コマンド】

ldapadd -v -D "cn=Manager,dc=mfldap,dc=com" -w password -f /etc/openldap/work/mf-containers.ldif

7. MFDS デフォルト定義のインポート

MFDS デフォルトユーザー、ユーザーグループとリソース定義が含まれる mfldap.ldif ファイルを 作業用ディレクトリへ置き、OpenLDAP へインポートします。

【対象ファイル】

mfldap.ldif ファイルは本報告書に添付されています。

【インポート実行コマンド】

ldapadd -v -D "cn=Manager,dc=mfldap,dc=com" -w password -f /etc/openldap/work/mfldap.ldif

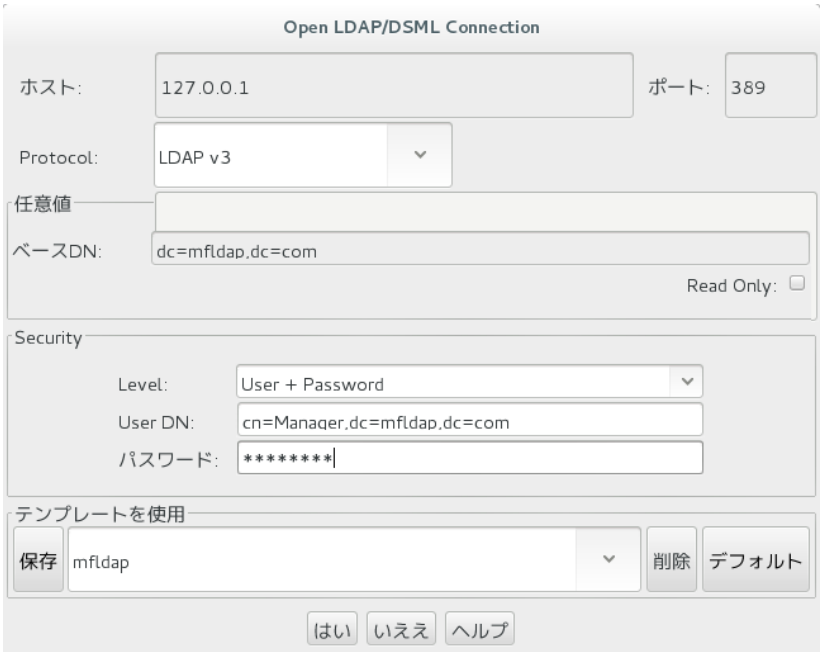
```
add objectClass:
        microfocus-MFDS-Group
add cn:
        #GAdmin
add description:
        General Administrators group
add microfocus-MFDS-Group-Member:
        administrator
add microfocus-MFDS-UID:
        1.2.840.5043.08.001.1523844490.5
adding new entry "cn=\#GAdmin,cn=Enterprise Server User Groups,cn=Micro Focus,dc=mfldap,dc=com"
modify complete
```

8. OpenLDAP の内容確認

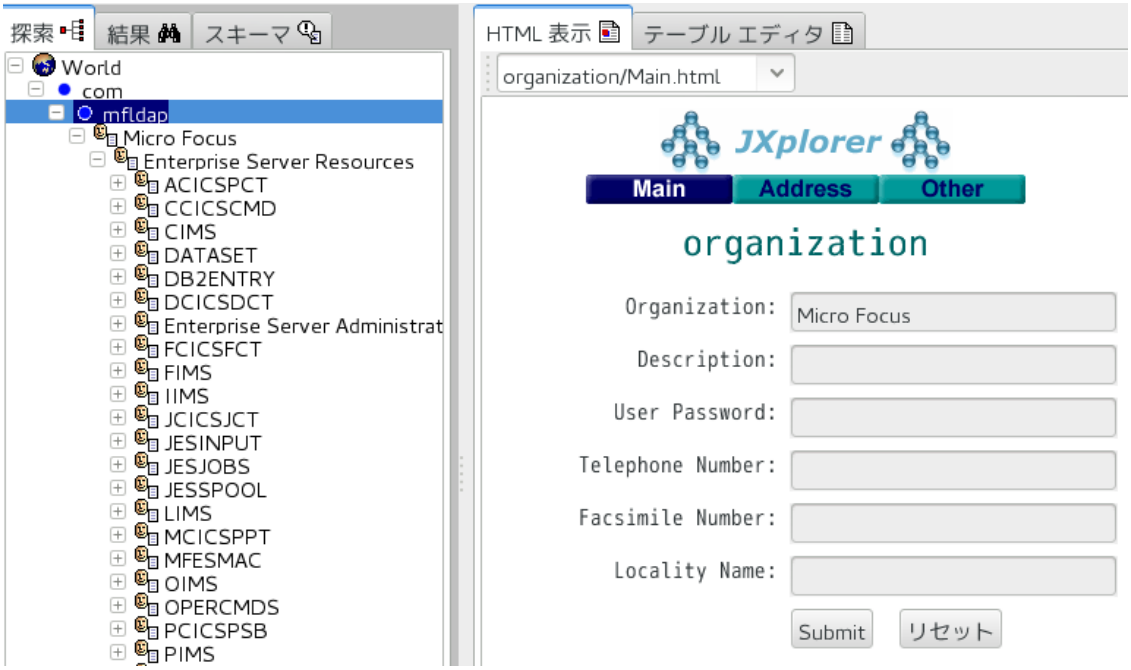
構成した OpenLDAP の内容を確認します。本書では LDAP GUI ブラウザとして JXplorer を使用して OpenLDAP へ接続後、内容を確認しています。

1) OpenLDAP への接続

構成時に指定した内容で
接続を行います。

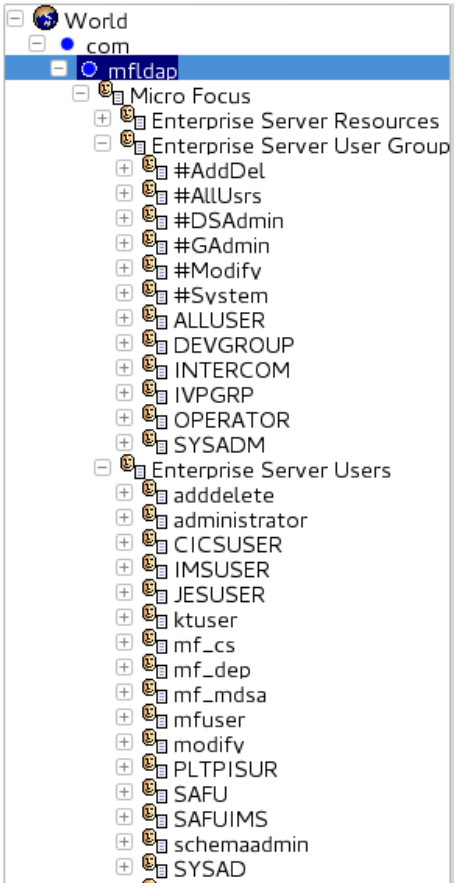


正常に接続され、構成指示した通り表示されています。



2) 接続先内容の確認

[Micro Focus] 配下を展開すると構成で指定した MFDS デフォルトユーザー、ユーザーグループとリソースが追加されています。



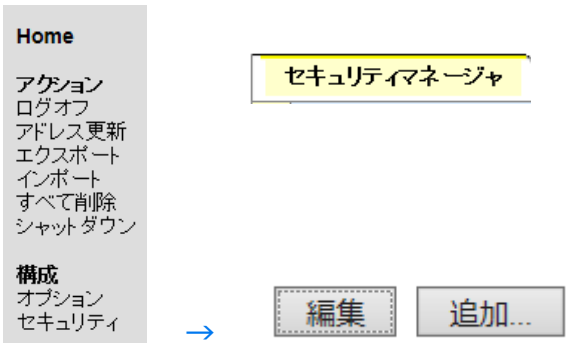
9. Micro Focus External Security Facility の設定

OpenLDAP 定義との連携を行うため、MFDS を起動して Enterprise Server 管理画面から設定を行います。

1) セキュリティマネージャの新規作成

OpenLDAP 連携のために新しいセキュリティマネージャを作成します。

1. 画面左側メニューの [セキュリティ] をクリックし [セキュリティマネージャ] タブで [追加] ボタンをクリックします。



2. 各項目を設定して [追加] ボタンをクリックします。
   - 名前： 任意です。本書では OLDAP とします。
   - モジュール： mldap_esm を指定します。
   - 接続パス： ldap://127.0.0.1:389 を指定します。
     （同一マシンに OpenLDAP が存在しており、ポート番号が 389 である場合）
   - 許可された ID： cn=Manager,dc=mfldap,dc=com を指定します。
     （前項の OpenLDAP 構成と同一）
   - パスワード： password を指定します。
   - 有効： チェックオンします。
   - キャッシュ上限： デフォルト値です。
   - キャッシュ TTL： デフォルト値です。

- 構成情報：下記のように指定します。

  [LDAP]

  provider=/usr/lib64/libldap-2.4.so.2

  Base=cn=Micro Focus,dc=mfldap,dc=com

  user container=cn=Enterprise Server Users

  group container=cn=Enterprise Server User Groups

  resource container=cn=Enterprise Server Resources

2) デフォルトの ES セキュリティ

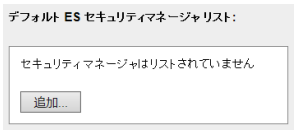
1. [デフォルトの ES セキュリティ] タブの [デフォルトの ES セキュリティマネージャリスト] へ、新規作成した OLDAP セキュリティマネージャを追加します。

【Add ボタンをクリック】　【OLDAP を選択して追加ボタンをクリック】

3) MF Directory Server

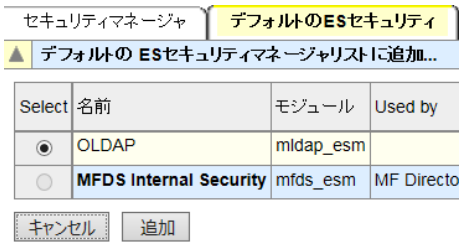
1. [MF Directory Server] タブの [セキュリティマネージャリスト] へ、新規作成した OLDAP セキュリティマネージャを設定します。

【追加ボタンをクリック】



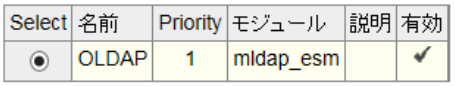
→

【OLDAP を選択して追加ボタンをクリック】



【OK ボタンをクリック】

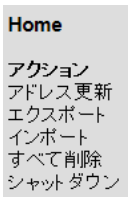
→



→

【リストが変更されたことを確認】

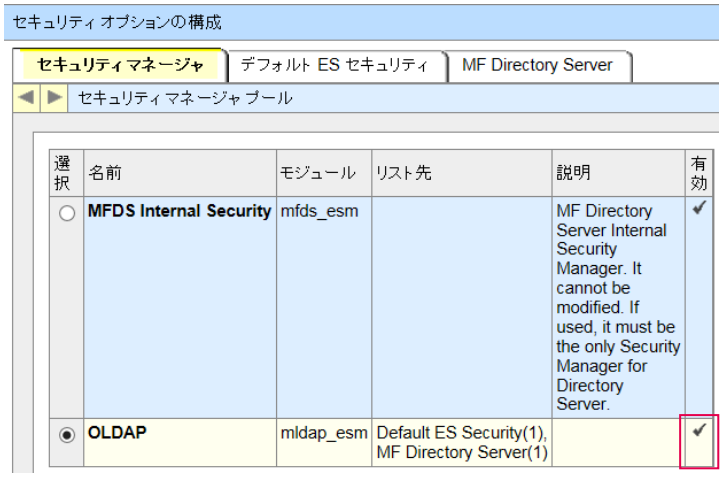
2. 管理画面の左側メニューから [シャットダウン] をクリックします。



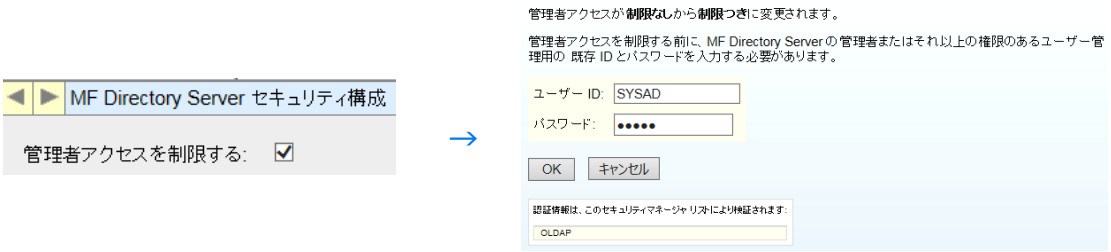
3. 64 ビットの MFDS を再起動します。

コマンド）mfds64 &

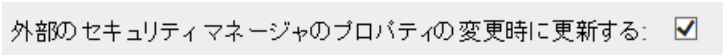
4. OLDAP が正常にロードされたことを [セキュリティ マネージャ] タブで確認します。エラーの場合はここへエラーが表示されます。



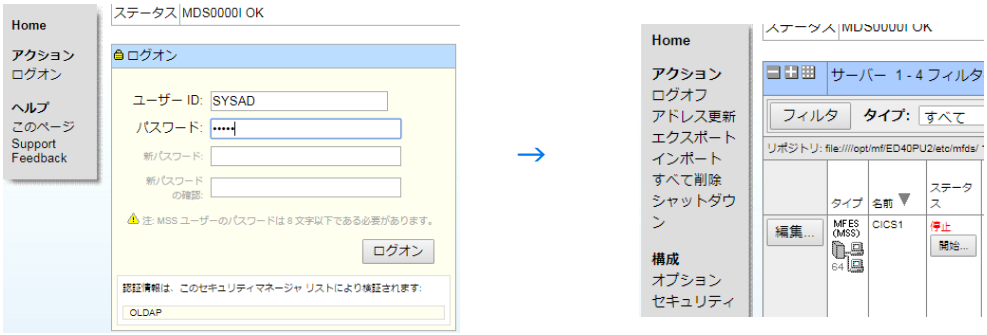
5. [MF Directory Server] タブへ戻り、画面上部にある [管理者アクセスを制限する] のチェックをオンにして [適用] ボタンをクリックすると、ユーザー確認画面が表示されますので [ユーザーID] と [パスワード] へ SYSAD を指定します。これにより管理画面へのアクセスが制限されます。



6. LDAP 側の変更を反映させるために [外部のセキュリティ マネージャのプロパティの変更時に更新する] のチェックをオンにして [適用] ボタンをクリックします。



7. 最後に [OK] ボタンをクリックしてブラウザを閉じ、再度ブラウザから管理画面へアクセスするとユーザー ID とパスワードの入力画面が表示されます。前項で設定した SYSAD を入力して [ログオン] ボタンをクリックすると、Enterprise Server インスタンス一覧が表示されます。



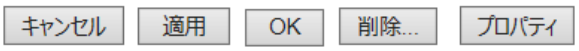
10. LDAP リソース定義とアクセス権の確認

OpenLDAP から設定した内容を Enterprise Server 管理画面から確認します。

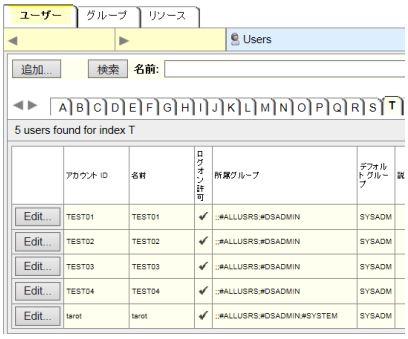
1) OLDAP のユーザー確認

1. Enterprise Server 管理画面、画面左側メニューの [セキュリティ] をクリックし [セキュリティマネージャ] タブの [OLDAP] が選択された状態で [編集] ボタンをクリックします。

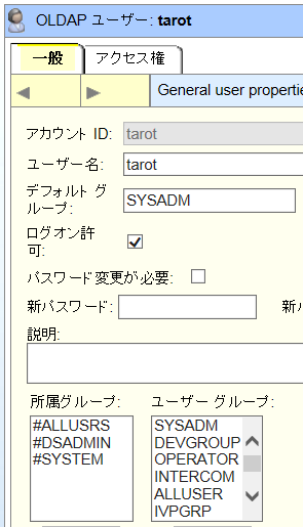
2. セキュリティオプションの構成画面が表示されますので [プロパティ] ボタンをクリックします。



3. 次画面では [T] をクリックしてユーザー一覧を表示し、OpenLDAP サイドから登録した tarot ユーザーの [Edit] ボタンをクリックします。

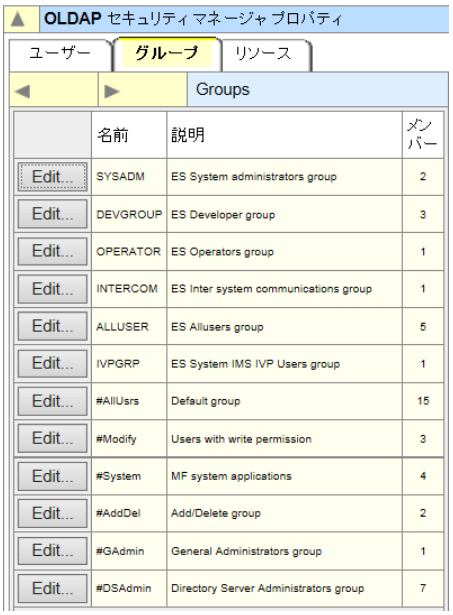


4. tarot ユーザーの設定内容が表示されます。デフォルトグループは SYSAD ユーザーと同様の SYSADM を指定しています。



2) OpenLDAP のユーザーグループ確認

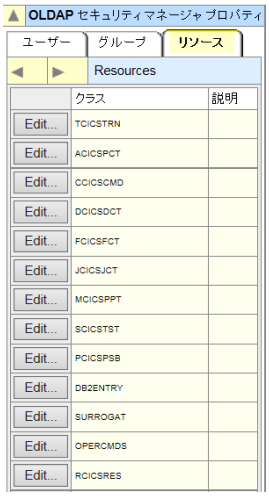
1. 既に OpenLDAP サイドから登録済みのグループは前項と同様に OLDAP のプロパティを選択後、[グループ] タブで確認することができます。

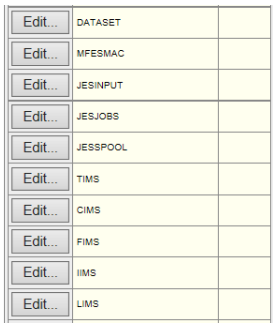


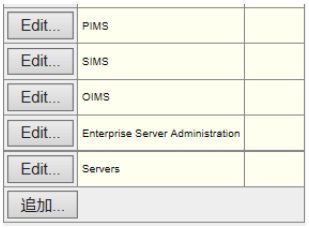
2. [Edit] ボタンをクリックするとグループに属するメンバーとアクセス権を確認できます。

3) OpenLDAP のリソース確認

1. 既に OpenLDAP サイドから登録済みのリソースは、前項と同様に OLDAP のプロパティを選択後、[リソース] タブで確認することができます。



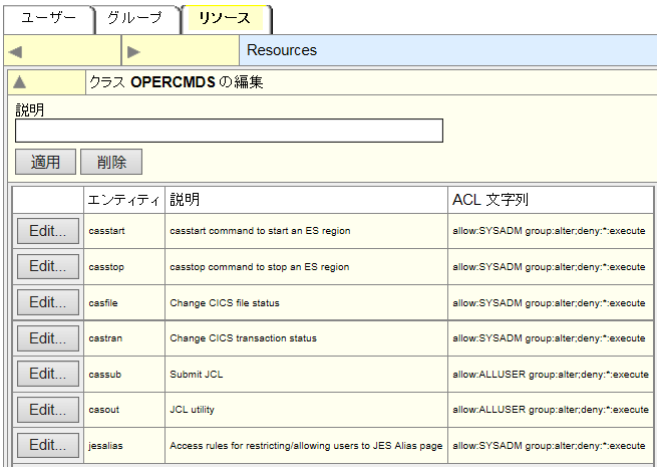




リソースクラスに関しては下記 URL をご参照ください。

https://www.microfocus.co.jp/manuals/ED40/Eclipse/HHSACHESSA30.html

2. [Edit] ボタンをクリックするとリソースのアクセス権設定が確認できます。



11. 設定内容の検証

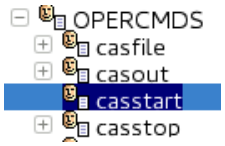
前項までに設定したユーザーもしくはユーザーグループ権限が有効であるか検証を行います。検証する Enterprise Server インスタンスは製品マニュアルの JCL チュートリアルに記述されている [JCLDEMO] を使用しています。必要であれば、下記 URL に書かれている環境を Windows から Linux に読み替えて内容をご確認ください。

https://www.microfocus.co.jp/manuals/ED40/Eclipse/MFEDEL04_400_05_JCL01.pdf

1) Enterprise Server インスタンスの開始

casstart 命令を使用したインスタンスの開始権限を検証するため、OpenLDAP の設定を確認します。

1. Enterprise Server Resources – OPERCMDS – casstart 命令の権限を確認します。
   SYSADM グループに所属するユーザーが実行を許可されています。



microfocus-MFDS-Resource-ACE	allow:SYSADM group:alter
microfocus-MFDS-Resource-ACE	deny:*:execute

2. Enterprise Server Resources – Servers – ＊ の権限を確認します。
   インスタンスに対する各権限は下記の各グループに属するユーザーに付与されています。

microfocus-MFDS-Resource-ACE	allow:#AddDel group:Execute,Read,Update,A...
microfocus-MFDS-Resource-ACE	allow:#AllUsrs group:Read
microfocus-MFDS-Resource-ACE	allow:#DSAdmin group:Execute,Read,Update,...
microfocus-MFDS-Resource-ACE	allow:#GAdmin group:Execute,Read,Update,A...
microfocus-MFDS-Resource-ACE	allow:#Modify group:Execute,Read,Update
microfocus-MFDS-Resource-ACE	allow:#System group:Execute,Read,Update,A...

3. 実行するユーザーの所属グループを確認します。
   tarot ユーザーは SYSADM グループに属しており、かつ #DSAdmin グループにも属しているため casstart 命令とインスタンス更新権限を保有しておりインスタンスの開始権限があります。既存の TEST04 ユーザーは casstart 命令の実行権限をなくすために、デフォルトグループを ALLUSER に変更します。

	アカウント ID	名前	ログオン許可	所属グループ	デフォルトグループ
Edit...	tarot	tarot	✓	;;#ALLUSRS;#DSADMIN;#SYSTEM	SYSADM
Edit...	TEST04	TEST04	✓	;;#ALLUSRS;#DSADMIN	ALLUSER

4. TEST04 ユーザーで casstart 命令を実行します。

   【 casstart 】ユーザー ID とパスワードは必須です。

   コマンド）casstart /rJCLDEMO /uTEST04 /ppassword

```
#casstart /rJCLDEMO /uTEST04 /ppassword
..
CASCD0167I ES Daemon successfully auto-started
CASCD0050I ES "JCLDEMO" initiation is starting
```

   開始命令は正常に受け入れられましたがインスタンスは正常に開始されませんでした。コンソールログを見ると権限設定により拒否されていることがわかります。

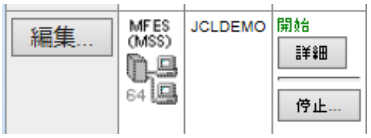
   【コンソールログ】

   CASSE0033E User TEST04 not authorized to start ES "JCLDEMO", region terminating

5. 次に tarot ユーザーで casstart 命令を実行します。

   tarot ユーザーは開始権限を保有しているため、コンソールログにエラーはなく、インスタンスが正常に起動されることが確認できます。

```
#casstart /rJCLDEMO /utarot /ppassword
..
CASCD0167I ES Daemon successfully auto-started
CASCD0050I ES "JCLDEMO" initiation is starting
```



2) ESMAC 機能の表示

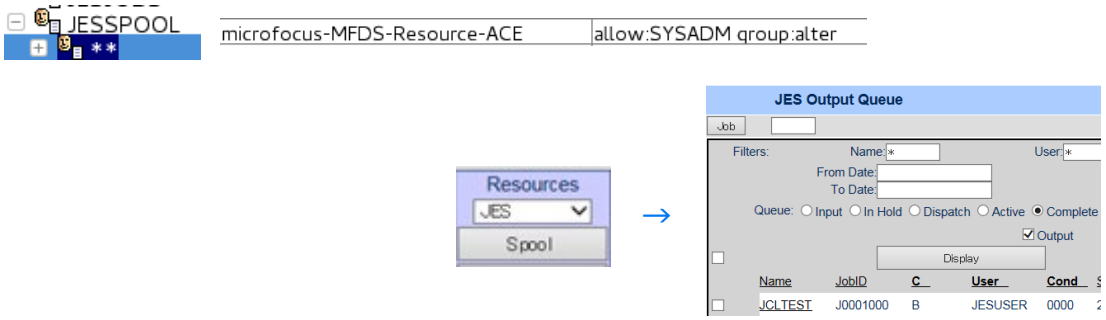
ESMAC 画面にある JES メニューからのスプール参照権限を検証するために、OpenLDAP の設定を確認します。

1. Enterprise Server Resources – MFESMAC – TABLE* の権限を確認します。これは ESMAC 画面の左側に表示される [Resources] を含むメニューの操作権限となり、複数グループのユーザーが許可されています。

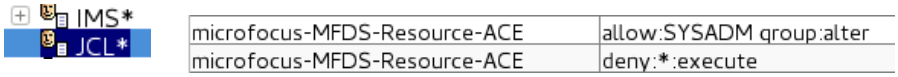
   前述の tarot, TEST04 ユーザーは共に操作権限を持つことになります。

microfocus-MFDS-Resource-ACE	allow:ALLUSER group:alter
microfocus-MFDS-Resource-ACE	allow:DEVGROUP group:alter
microfocus-MFDS-Resource-ACE	allow:OPERATOR group:alter
microfocus-MFDS-Resource-ACE	allow:SYSADM group:alter
microfocus-MFDS-Resource-ACE	deny:*:execute

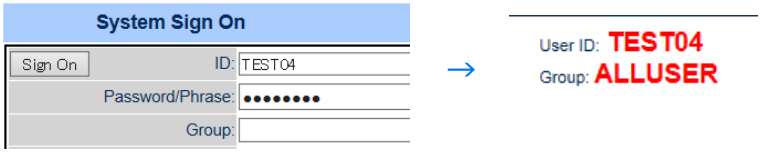
2. Enterprise Server Resources – JESSPOOL – ** の権限を確認します。これは [Resources] メニューから [JES] を選択後に現れる [Spool] ボタンをクリック後のスプール利用権限となり、SYSADM グループのみが許可されているため tarot ユーザーが操作可能となります。



3. Enterprise Server Resources – MFESMAC – JCL* の権限を確認します。これは [Resources] メニューから [JES] を選択後に現れる JES 関連ボタンの利用権限となり、SYSADM グループのみが許可されているため tarot ユーザーが操作可能となります。

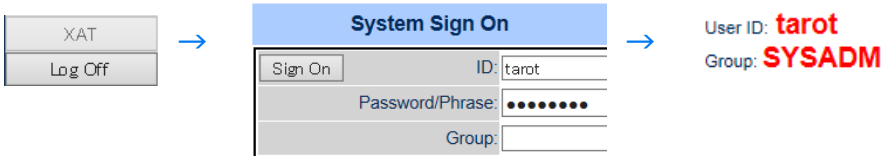


6. まずは ESMAC 画面へ TEST04 ユーザーでサインオンします。画面右上にサインオンユーザーとグループが表示されます。

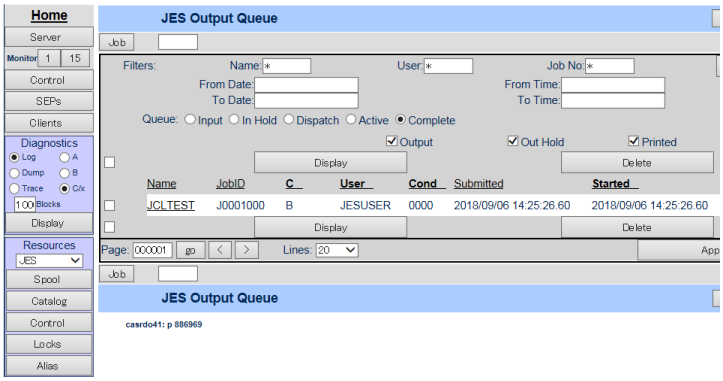


7. TEST04 ユーザーは左側メニューが表示される権限を持っているため [Resources] メニューの選択は可能ですが、JES 配下の権限を持っていないためボタンがグレーアウトされて使用できません。

8. ログオフ後、ESMAC 画面へ tarot ユーザーで再度サインオンします。



9. tarot ユーザーは左側メニューが表示される権限、スプールの更新権限、JES 配下の機能権限を持っているため、JES 配下のボタンが使用できスプールも表示されます。



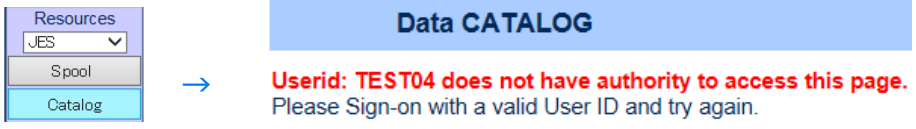
10. Enterprise Server Resources – MFESMAC – JCL* へ TEST04 ユーザーを許可するよう権限を付与します。

microfocus-MFDS-Resource-ACE	allow:SYSADM group:alter
microfocus-MFDS-Resource-ACE	allow:TEST04:alter

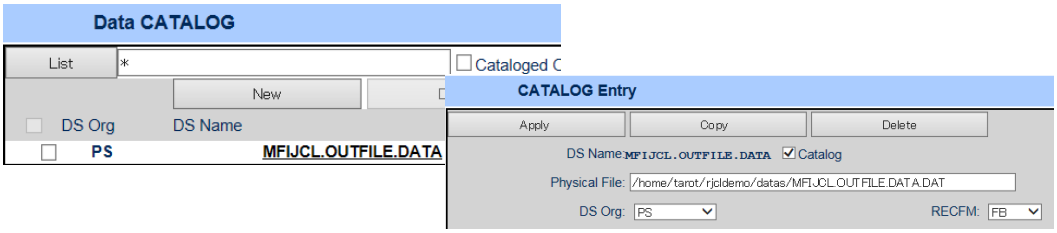
11. カタログ情報の操作権限を Enterprise Server Resources – DATASET – ** で確認します。SYSADM グループに権限が付与されているため tarot ユーザーが操作権限を持つことになります。

microfocus-MFDS-Resource-ACE	allow:SYSADM group:alter

12. ESMAC 画面へ TEST04 ユーザーでサインオンします。権限を付与したため JES 配下のボタンが有効になり、[Catalog] ボタンはクリックできますが、スプールへのアクセス権限がないため [List] ボタンをクリックすると TEST04 ユーザーはメッセージと共にアクセスが拒否されます。



13. 次に ESMAC 画面へ tarot ユーザーでログオンします。権限を保持しているため [Catalog] ボタンをクリック後 [List] ボタンをクリックするとカタログ一覧が表示され、内容を参照や更新が可能です。



12.おわりに

ESF と外部ディレクトリ・サービスの連携を図ることにより、Enterprise Server インスタンスの機能やリソースへの細やかな権限設定が可能であることを検証しました。
しかしながら細かい設定が可能であるがゆえ事前のユーザー権限やグループ設計が重要であり、かつ外部ディレクトリ・サービスの機能全般について精通している必要があると考えます。

Enterprise Server に関するセキュリティ全般に関しては下記 URL をご参照ください。
参考 URL）
https://www.microfocus.co.jp/manuals/ED40/Eclipse/GUID-96DE94E5-C4FF-4AFC-91CF-6075936B60AB.html