

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
ź	2) OS バージョン	3
~ `	3)プロセッサ	3
2	1) 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	2) MFDS との連携	6
4.	AD LDS の構築	8
) Windows オプション機能の追加	8
ź	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
) セットアップスクリプトの実行	11
ź	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 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)

ES ^{管理}		ダッシュボード ネイティブ ES.NET メインフレーム セキュリティ
 ↓ 「 づ ブ ループ ▶ 論理 	Directory Server C +追加	
✓ PAC	▲ 台 少なくとも1個のDirectory ServerホストはTLSが有効では	ありません
品 DEMOPAC		
 ✓ I Directory Server > ⊕	▼ 名前 ▼ 説明	状態 ~ ホスト ~ ボート ~ バージョン ~ TLS有効 ~ TLSボート
✓ ⊕ 🔓 RHEL9	ア 名前 ホスト	ポート 説明 パージョン 合 TL TL
E ESDEMO	III WIN11-SVR WIN11-SVR	86 1.29.15
E ESDEMO64	RHEL9 RHEL9	86 1.29.15
E SOLDEMO		

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。

LOCIA COLE	53751797	
ES 管理		ダッシュボード ネイティブ ES.NET
セキュリティ マネージャ VESCWAの構成 V ③ ADLDS	リソース オプション C <mark>* クラス</mark>	の新規作成
品 ユーザー 略 グループ	> & ACICSPCT	Control C 適用 位 削除
ي−رىل ھ	A CIMS A Common Web Administration O Communications Server Log O Configuration Control ESCWA Configuration C K8s Configuration O Logon O Managed Access O MFDS Configuration	名用・ Q Control 説明 Q Allow control of the Common Web Administration Server ACL Q allow:#DSAdmin group:execute

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。

S 管理					ダッシュボード	ユーザー オプション	0			
セキュリティ マネージャ ESCWAの構成 v ⑥ ADLDS	-د	ーザー	オプション C	* 新規作成		エージー・パンション Selected すべてクリ	7			
品 ユー ヮ ー 怒 グループ 島 リソース		▽	アカウントID アカ 名前	▼ 名前 テフォルトクループ	▼ 説明 説明	$\label{eq:sysadm} \begin{array}{l} \text{SYSADM} \times \ \text{\#AllUsrs} \times \ \text{\#DSAdmin} \times \ \text{ALLUSER} \times \\ \\ \text{DEVGROUP} \times \ \text{INTERCOM} \times \ \text{OPERATOR} \times \end{array}$				
		ക	CICSUSER	ALLUSER	Default CICS User	グループ				
					8	IMSUSER	ALLUSER	Default IMS user	フィルタ マ #AllUsrs	
		ക	JESUSER	ALLUSER	Default JCL user	 ✓ #DSAdmin ☐ #GAdmin 				
		8	PLTPISUR	OPERATOR	CICS User for PLTPI	#Modify #System ALLISED				
		8	SAFU	DEVGROUP	Test security user	 ☑ DEVGROUP ☑ INTERCOM 				
		8	SAFUIMS	IVPGRP	ES IMS User	VPGRP OPERATOR				
		8	SYSAD	SYSADM			*			

2) MFDS との連携

Windows 環境の MFDS と連携した例)

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。

✓ I Directory Server **定義済みの外部のセキュリティ マネージャ** | C 十追加 ↓ ⊕ ⊕ WIN11-SVR APAC1 APAC2 CICSDEMO ▼ 名前 ▼ 説明 モジュール~ 有 CICSLSI DBDEMO ア... 説明 アクション 名前 モジ.. 有効 DBDEMOEB ð AD LDS mldap_esm \checkmark ECIDEMO

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。



> am/±	リージョンのセキュリティ機能の構成 С 適用
✓ I Directory Server	
🗸 🌐 🔂 WIN11-SVR	
E APAC1	* 入力必須の項目です
APAC2 CICSDEMO	▼ デフォルトのセキュリティ機能の構成を使用 💡
CICSLSI	□ すべてのセキュリティ マネージャ ♀ □ 不明なリソースを を検証
ECIDEMO	
E ESDEMO	キャッシュTTL* Q 0 🇘 秒
ESDEMO64	供引注起 〇
IMSDEMO	and and an A
JCLDEMO	
JESSPL	
MFDBFH	
PAC2	
PLIIMS	
PLIIMS64	2+1971 ** -97 9XF
PLIJCL	十追加
PLIJCL64	
STAFF	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 ヘ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:

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ク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、セキュリティクエリの通信によ 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。	17.75774 17.75774は、この AD LDS イソスタソスと20コンピューター上のほかの AD LDS イソスタソスとを区 別するために使用されます。 このイソスタソスの使用目的がわかるような名前を 重んでください、 パンスタソス名(10): MFES 例: Addressbook1 説明(D): AD LDS インスタンスス AD LDS インスタンスス AD LDS サービス名は、インスタンススを知為名を組み会せて作成され、Windows のサービスの一覧に 表示されます。この解、ユーザーガン入した説明も表示されます。 AD LDS サービス名:: ADAM_MFES
「ポート」は木書ではデフォルトのまま	Call Active Directory フイトウェイト アイレクトリ リーと人 ゼットアウノ ウイリート ボート コンビューターは、このコンビューターに関連付けられているすべての P アドレス上にある特定のボートを使 って、この AD LDS インスタンスに接続します。 マトニューンサン アレンボールト マのコンピューター マーヨンド 利田 可当た ボートマオ マルこの ボートネマオ ヨオ
[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	「たちんさいていが、「たちしひ」と、プレランパーガーがあい、「くちょう」であらが、「とまた」 このコンビューターにActive Directory ドメイン サービスをインストールする予定がある場合は、LDAP ポート に 389、まだは SSL ポートに 636 ほゆ用しないでください、これらのポート番号は Active Directory ドメイ ンサービスによって使用されます。その代わりに 1025 - 65535 の範囲で利用できるポート番号を使用して ください。
ここで使用するポート番号を指定します。	LDAP ボート출号(山: 389 SSL ボート番号(S): 636

🛐 Active 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

🛐 Active 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

一意のインスタンスを作成するか、または既存のインスタンスのレプリカをインストールすることができます。

このオプションを選択すると、既定の構成とスキーマパーティションを使用する新しい AD LDS インスタ ンスが自動的に作成されます。新しいインスタンスを既存のインスタンスでレプリケートすることはできま せん。

このオプションを選択すると、別の AD LDS インスタンスからレプリケートされた構成とスキーマ パーティシ ョンを使用する新しい AD LDS インスタンスが作成されます。レプリケートするアプリケーション パーティシ ョンを選択することもできます。

< 戻る(<u>B</u>) 次へ(<u>N</u>) > キャンセル

セットアップ オプション AD LDS がインストールされるたびに AD LDS インスタンスが作成されます。

インストールするインスタンスの種類を選択してください。

一意のインスタンス(A)

×

2

ヘルプ

< 戻る(B) 次へ(N) > キャンセル ヘルプ



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。

🔄 Active 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	×			
ファイルの場所 この AD LDS インスタンスと関連付けられた各種類のファイルの場所を指定できます。	0			
AD LDS に関連付けられたファイルを格納する場所を指定してください。				
データ ファイリレ(<u>D</u>):				
C:¥Program Files¥Microsoft ADAM¥MFES¥data 参照(Q)				
データ回復ファイル(<u>A</u>):				
C:¥Program Files¥Microsoft ADAM¥MFES¥data 参照(<u>W</u>)				
	·			
<戻3(B) 次へ(M) > キャンセル ヘルノ				

[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。

□ Active 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 ×	□ Active 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 ×
サービス アカウントの選択 AD LDS は、選択されたアカウンドに関連付けられたアクセス許可を使って操作を実行します。	AD LDS 管理者 この AD LDS インスタンスに対する管理者特権を持つユーザーまたはグループを指定できます。
次のアカウンドと関連付けられたアクセス許可を使って操作を実行するように AD LDS をセットアップします。 ● <u>Network Service アカウンド(F)</u> AD LDS は、既定の Windows サービス アカウントのアクセス許可を持ちます。 ● 次のアカウントロ: AD LDS サービスには、選択されたアカウントのアクセス許可が割り当てられます。 ユーザーぶ(L): 「スワード(P): ● マンビル ヘルブ	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制り当てます。
.DIF ファイルのインポート] では AS-User.LDF] を選択し、 Rへ] ボタンをクリックします。	Active 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 LDIF ファイルのインボート LDIF にはiphtweight Directory Interchange Format) ファイルからのデータを AD LDS アブリケーション ディレクトリインボートすることができます。 AD LDS サービスを物定の方法で構成す るには、以下に一覧表示されている LDIF ファイルを 1 つまたは複数インボートしてください。 LDIF ファイル名 ED5 サービスを物定の方法で構成す るには、以下に一覧表示されている LDIF ファイルを 1 つまたは複数インボートしてください。 LDIF ファイル名 MS-SeptValMetadataExt.LDF AD LDS のサーブリット電気も別であった。 MS-SeretAttributeCARE.LDF AD LDS のドオークロシテムと観念ワクスです。 MS-UserLDF AD LDS オーゲークスと観念ワクスです。 MS-UserLDF AD LDS オーゲークスです。 MS-UserLDF AD LDS アボーターンの「スとしい」の「パース制造のアウセス権。 MS-UserLDF AD LDS アボーターンのです。 MS-UserLDF AD LDS アボーク・クラスです。 AD LDS アボーク・クラム LDS アボーク・クラム LDS アボークラムです。 AD LDS アボーク・クラム LDS アボークラム LDF アボーク・クラム LDS アボーク・ク

[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。

♀ サービス (ローカル)					
MFES	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	. .	手動	Local S
<u>サービスの停止</u>	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
<u>サービスの冉起動</u>	🖓 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ーを定義します。

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> 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-Idap-setup es-Idap-setup: Initial LDAP security setup for Enterprise Server Version 1.3.1 Copyright 2006-2014 Micro Focus. All rights reserved. Run "es-Idap-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)



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ーを 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。

2 ADSI 1719-							
ファイル(E) 操作(A) 表示(V) ヘルブ(H)							
☑ ADSI Iディター	名前	クラス	識別名				
✓	CN=ACICSPCT	container	CN=ACICSPCT,CN=Enterprise Server Resources,CN=Micro Focus,CN=				
✓	CN=CCICSCMD	container	CN=CCICSCMD,CN=Enterprise Server Resources,CN=Micro Focus,CN				
CN=ADAM Users	CN=CIMS	container	CN=CIMS,CN=Enterprise Server Resources,CN=Micro Focus,CN=Proc				
✓	CN=Common Web Ad	container	CN=Common Web Administration,CN=Enterprise Server Resources,C				
CN=ACICSPCT	CN=Communications S	container	CN=Communications Server,CN=Enterprise Server Resources,CN=Mi				
CN=CCICSCMD	CN=DATASET	container	CN=DATASET,CN=Enterprise Server Resources,CN=Micro Focus,CN=1				
CN=CIMS	CN=DB2ENTRY	container	CN=DB2ENTRY.CN=Enterprise Server Resources.CN=Micro Focus.CN.				
CN=Common Web Administration	CN=DCBINFO	container	CN=DCBINEQ.CN=Enterprise Server Resources.CN=Micro Focus.CN=				
CN=Communications Server	CN=DCICSDCT	container	CN=DCICSDCTCN=Enterprise Server Resources.CN=Micro Focus.CN:				
CN=DATASET	CN=Enterprise Server A	container	CN=Enterprise Server Administration.CN=Enterprise Server Resources				
CN=DB2ENTRY	CN=Enterprise Server	container	CN=Enterprise Server Web CN=Enterprise Server Resources CN=Micr				
CN=DCBINFO	CN=ECICSECT	container	CN=ECICSECTCN=Enterprise Server Resources CN=Micro Focus CN=				
CN=DCICSDCT		container	CN-EIMS CN-Enterprise Server Resources CN-Micro Focus CN-Proc				
CN=Enterprise Server Administration		container	CN-IIMS CN-Enterprise Server Resources CN-Micro Focus CN-Prog				
CN=Enterprise Server Web		container	CN-ICICSICTCN-Enterprise Server Resources CN-Micro Focus CN-E				
CN=FCICSFCT		container	CN=JCIC32CI, CN=Enterprise Server Resources, CN=Micro Focus, CN=				
CN=FIMS		container	CN=JESINPO I, CN=Enterprise Server Resources, CN=Micro Focus, CN=				
CN=IIMS		container	CIN=JESJOBS, CIN=Enterprise Server Resources, CIN=Micro Focus, CIN=P				
CN=JCICSJCT	CIN=JESSPOOL	container	CIN=JESSPOOL, CIN=Enterprise Server Resources, CIN=Micro Focus, CIN=				

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。

📝 ADSI エディター

~	-	MFES [localhost:389]
	~	CN=Micro Focus,CN=Program Data,DC=
		CN-ADAM LISOR

占前	クラス
CN=MFReader	user
CN=tarot	user

識別名

CN=MFReader,CN=ADAM Users,CN=Micro Focus,CN=Program Data,DC=local CN=tarot,CN=ADAM Users,CN=Micro Focus,CN=Program Data,DC=local

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)

属性(<u>B</u>):				
属性	値			
adminDescription	<未設定>			
adminDisplayName	#DSAdmin		microfocus-MFDS-CustomText	<未設定>
cn	#DSAdmin		microfocus-MFDS-Group-Member	SYSAD; schemaadmin
description	Directory Server Administrators group		microfocus-MFDS-UID	1.2.840.5043.08.001.1653280513.6

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 リポジトリの構成>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。

ES	管理	ダッシュポード ネイティブ ES.NET メインフレーム セキュリティ	
セキ: > ESC	ュリティ マネージャ WAの構成	定義済みの外部のセキュリティ マネージャ C + 追加	

[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* 💡	
ADLDS	mldap_esm	
接続パス 💡		
WIN11-SVR:389		
認証ID 💡		
CN=MFReader, CN=ADAM Users, CN=Micro Focus, CN=F	Program Data,DC=local	
パスワード		
説明 ♀		
構成情報 ♀		
LUMF T base=CN=Micro Focus,CN=Program Data,DC=local user class=microfocus-MFDS-User user container=cn=Enterprise Server User group container=cn=Enterprise Server User Grou resource container=cn=Enterprise Server Resour	ips ices	* *
* 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。

ES	管理	ダッシュボード ネイティブ ES.NET メインフレーム セキュリティ							
セキュリティ マネージャ		ESCWA セキュリティ機能の構成 C 適用 再初期化							
		● これらの設定は、ESCWAのセキュリティを構成します。Directory Server には適用されません。							
		* 入力必須の項目です							
		 □ すべてのセキュリティ マ ○ □ 不明なリソースを許可 ○ □ 不明なユーザーを許可 ○ □ 監査イベントを作成・ ネージャを検証 							
		キャッシュTTL* 🖗 0 🛟 秒 キャッシュ上限* 🖗 0 🛟 kB							
		構成情報 🖓							
		セキュリティ マネージャ リスト							
		十追加							

[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。

定義済みの外部のセキュリティ マネージャ						
Selected ADLDS ×	すべてクリア					
定義済みの外部のセキュリティ	マネージャ					
ADLDS	•					
	選択 戻る					

変更を反映するために [適用] ボタンをクリックします。

ESCWA セキュリティ機能の構成 | C 適用 再初期化

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。

ക	管理者ユーザーの認証情報の更新
	セキュリティ構成が更新され、アクセスが制限されています。ESCWAリソース クラス の「ユーザー管理」リソースの権限のある既存のIDとパスワードを指定する必要があり ます。 ユーザー名 *
	バスワード・
* 2,7	ロ必須の項目です ログオン 戻る

[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。

ゼキュリティ マネーンヤ		
✓ ESCWAの構成 C	ESCWAセキュリティ機能の構成	
> @ ADLDS		
	 これらの設定は、ESCWAのセキュリティを構成します 	「。 Directory Server には適用されません
	* 入力必須の項目です	
	□ 9へてのセキュリティ マネーシャ ∨ を検証	□ 不明なリソースを許可 ♀
	キャッシュTTL* 8 0	秒 キャッ
	構成情報 🛇	
	セキュリティ マネージャ リスト	
	十追加	
	1 VADLDS	

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。

セキュリティ マネージャ V ESCWAの構成 V O ADLDS	グル	/ーブ	゚ <i>オプション</i> │ C	* 新規作成		グループ オプション			0
品 ユーザー									
8 グループ		V	グループ	X X X/-	/ 説明	JUNFA			-
鼻 リソース		P	クループ	メンバー	說明	ブループ 〇 #GAdmin			
		88	#AddDol	mf den adddelete	Add/Delete group	説明 😡			
			in toolor		, da Boleto group	General Administrators group			
		88	#AllUsrs	SYSAD;mf_cs;mf_dep;mf_mdsa;	Default group				~
		8	#DSAdmin	SYSAD;schemaadmin	Directory Server Administrators group	-71.5%			- 1
		88	#GAdmin	administrator	General Administrators group	Selected		すべてクリア	
		88	#Modify	mf_cs;mf_mdsa;modify	Users with write permission	administrator $ imes$			
		88	#System	mf_cs;mf_dep;mf_mdsa	MF system applications	ユーザー			
		88	ALLUSER	SAFU;PLTPISUR;mfuser;CICSU	ES Allusers group				
		88	DEVGROUP	SYSAD;SAFU;CICSUSER	ES Developer group	☐ IMSUSER ☐ JESUSER		ĺ	•
		 合	i†: 12			* 入力必須の項目です	保存	茴 削除	戻る

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。

ヤキュリティ マネージャ		ユーザー オブション	0
✓ ESCWAの構成	ユーザー オプション С * 新規作成	プロバティ	
🗸 🖯 ADLDS		アカウントロ・ 🛇	
ನಿ ユーザー		TESTUSER	
88 グループ ぬ リソース	▼ アカウントID ▼ 名前	名利 🛇 TESTUSER	
		デフォルト グループ Q ALLUSER	
		2 ログオン許可 🛇	
		□ バスワード変更が必要 🛇	
		a)(2)	
			h
		9 H-EXX	
		パスワードを入力してください	
		* 入力必須の項目です	保存 戻る

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。

						ユーザー	オプション			0
0				~	, A ,	プロパラ	• - 1			
스타· 17	tarot	#DSAdmin		0	編集	アカウント tarot 名称 Q tarot デフォルト	0 0 Ju-J 0			
						#DSAd 2 ログ: 1 パス・ 説明 0	min t>許可 0 7一ド波更が必要 0			
						バスワート ・ 、 入力必須の	Q 月日です	保有	10 刑除	<i>4</i> 戻る

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。

表面マニュアルの扱件/			
	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 コーザーはジョブをサブミ ットできます。 UPDATE READと同等です。 UPDATEと同等です。 ALTER 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。

✓								
	🗸 🌐 🔓 WIN11-SVR	たお	5A010	JJ7FaPUJ	641972	x1 .		
	APAC1							
	APAC2							
	CICSDEMO		Y	名前		▼ 説明		モジュール・
	CICSLSI		-	-103		P P/0-/3		
	DBDEMO		ア	名前	モジ	有効	使用元	説明
	DBDEMOEB							
	ECIDEMO		ð	AD LDS	mldap_esm	\checkmark	デフォルト	·
	ESDEMO							

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。

ネイティブ ES NET メインフレーム セ		
セキュリティ 〜 ジャーナル	Directory Server G MIN11-SVR APAC1	デフォルトの ES セキュリティ機能の構成 C 🎽
 ✓ セキュリティ マネージャ 追加 デフォルトの ES 構成 	APAC2 CICSDEMO CICSLSI DRDEMO	・入力必須の項目です コーオへてのセキュリティマ ② ロー不明なリソースを許可 ③ ロー不明なユーザーを許可 ◎ ロー 監査イベントを作成する ◎ ローオべてのグループを使用 ◎ ネージャを検証
	DBDEMOEB DBDEMOEB ECIDEMO ESDEMO ESDEMO ESDEMO64 IMSDEMO JCLDEMO	キャッシュエル: ② 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	JESSPL MFDBFH PALS PLIMAS PLIMAS PLIJALB4 PLIJALB4 STAEE	を セキュリティマネージャリスト ・ 近回 1 、 AD LDS

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	Directory Serverのセキュリティ機能の構成 C 適用
ことができます。	・入力必須の項目です
	✓ Directory Server アクセス を制限する
✓ ⊕ 🔂 🕀 WIN11-SVR	□ すべてのセキュリティマ ♀ □ 不明なリソースを許可 ♀ □ 不明 ネージャを検証
A Directory Server ログオン: WIN11-SVR:86	
▲ ⑥ 彩セキュア	キャッシュTTL* 🖗 0 🔷 秒 キャッシュ上限* 🖗 0
The resource you are attempting to connect to is currently not TLS enabled. If you send credentials they will be viewable in plain text over the network. $\Box = - f - \Xi^*$ SYSAD	機成情報 📿
/はスワード・ 	セキュリティ マネージャ リスト
*入力必須の項目です ログオン 戻る	✓ ES デフォルト セキュリティ マネージャを使用 ○

[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。



?	一般 ~	CICS V	· · · ·	JES ~	&ユーザー	~
<u>י</u> ע-	ージョンのセキ	ュリティ機能の	の構成 (う適用		
	* 入力必須の項目で	ġ				
	🔽 デフォルトのセ	キュリティ機能の構成	成を使用 💡			
	 すべてのセキュ ャを検証 	リティマネージ 🎖	□ 不明	なリソースを許	न 0	□ オ
	キャッシュTTL* 💡		^ ↓ 秒		キャッシュ上限* 💡	0
	構成情報					
	セキュリティ マス	ネージャ リスト				
	1 🗸 AD LDS					

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 [OPERCMDS] 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。

ES 管理		ダッシュボード ネイティブ ES.NE	
セキュリティ マネージ > ESCWAの構成 > & ADLDS 糸 ユーザー 巻 グループ 急 リソース	ヤ リソースオプション C * 25 > & MCICSPPT > & MFESMAC > & MQADMIN > & MQCONN	スの新規作成 ▲ casstart C 適用 団 削除 名前・Q	
	 > Im MOPROC > Im MOPROC > Im MOPROC > Im OPERCMDS OPERCMDS Operating Immodeling Im	cassian 説明 ② casstart command to start an ES region ACL ② deny:*:execute allow:SYSADM group:alter * 入力必須の項目です	
現在、このグ. SYSAD ユー	ループに所属しているユーザー -ザーです。	グループオブション プロパティ ジループ Q SYSADM 脚同 Q E5 System administrators group	2
		Selected SYSAD ×	すべてクリア

A リージョンの開始オプション 権限のある SYSAD ユーザーで ▲台 非 JCLDEMO インスタンスを ESCWA から開始します。 スタート モード ○ ウォーム ♀ コールド Ω ○ アップグレード ○ Enterprise Server 認証情報 □ 現行のユーザー認証情報を使用する 🛇 ユーザーダ SYSAD グループ A Dir 致しません 8854 厚る cics | ~ JES 🗸 🗸 &ユーザー ~ ESCWA からコンソールログを表示し、 バックアップ 💿 現行 ≪ < > ≫ ページ: 1 /1 85 行 / 85 💿 表示 正常に開始されたことを確認します。 ▼ メッセージ プロセスID > ログレベル フロセ メッセ.. メッセージ 5096 5096 5096 TD recoverable warm started PLTPI Phase 1 starting File initialization program PLTPI Phase 1 - No PLT Specified CASSI1426I CASSI4106I CASSI5001I PLIPI Phase 1 - No PLI Specified Active SEP memory strategy set to x'00000001', retain count 100 Batch initiator started for job classes "ABC" Caching disabled (cache size set to zero) 5096 CASSI50401 6848 CASBJ0005I 6848 ESFCA0403I Caching disabled (cache size set to zero) ESM1 - JAl groups mode disabled; group federation enabled SEP initialization completed successfully ESM1 - Using UDAP provider module "VLDAP32 DLL", from "Microsoft Corporation.", API version 2004, vendor versi. Caching disabled (cache size set to zero) ESM1 - MI-groups mode disabled; group federation enabled Loaded module midag, esm for ESM (1) "AD LDS". MLDAP ESM version 2.9.10 ESM1: SMI-provider module "VLDAP32 DLL", from "Microsoft Corporation.", API version 2004, vendor versi. EsM1: SMI-provider module "VLDAP32 DLL", from "Microsoft Corporation.", API version 2004, vendor versi. External Security Manager version 3.6 in initialized ESM1: MLDAP ESM initialized ESM1: MLDAP ESM initialized ESM2: MLDAP ESM initialized 6848 7768 6848 7768 6848 7768 6848 7768 6848 ESFEM1031 CASSI1600 CASSI1600I ESFEM1083I ESFCA0403I ESFEM1000I ESFEM1031I ESFMI0200I ESFEM1083I ESFPI0101I 7768 ESFEM1000I Loaded module midap esm for ESM (1) "AD LDS": MLDAP ESM version 2.9.10 7768 ESFMI02001 7768 ESFPI0101I External Security Manager version 3.6.6 initialized

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。

A OPERCMDS	aaaaub	
© DIAGS		プロパティ
✿ casout	説明 ♀	グループ 🖓
☆ cassub	Submit JCL	ALLUSER
😚 casfile		ES Allusers group
	ACL 🖓	*
😚 castran	allow:ALLUSER group:alter;deny:*:execute	メンバー
𝗘 casstart		
🏵 jesalias		Selected すべてクリア
		${\rm SYSAD} \times {\rm CICSUSER} \times {\rm mfuser} \times {\rm PLTPISUR} \times {\rm SAFU} \times \\$
		tarot \times

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.jc| /uJESUSER /pJESUSER XSBJ0047S JES Submit: User ID "JESUSER" not authorized 15:23:45 Processed "C:¥work¥JCLDEMO¥copy1.jc|" 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.icl"

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	ョ ブ: J0001436 C	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 JCLCM0182I J0001436 COPY1	JOB JOB	STARTED ENDED	15:29:08 - 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	▲ CINQ I C 適用 回 削除
♥ CFCP	
O CFCR	
𝔅 CFLE	名前* 💡
♥ CFLI	CINQ
✿ CFLS	
✿ CFMT	説明 💡
© CINQ	Terminal Environment Inquiry
O CINS	
✿ CLOG	ACL Q
✿ CMAP	<pre>deny:*:execute;allow:SYSADM group:read;allow:OPERATOR group:read</pre>
✿ CMAX	

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え、結果は確認できません。

プロバティ	所属するグループ	
アカウントID Q CICSUSER 名前 Q	Selected ALLUSER × DEVGROUP ×	すべてクリア
	グループ	
デフォルトグループ 💡		
ALLUSER	#AllUsrs	
🖌 ログオン許可 💡	#GAdmin #GAdmin	
□ パスワード変更が必要 🛇	I #System ✓ ALLUSER	
	DEVGROUP	
	UFERATOR	

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。



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 cassop の実行権限を持つ SYSAD ユーザーで停止し

ます。	
> & JCICSJCT	説明 ○
> & JESINPUT	casston command to ston an ES region
> & JESSPOOL	
> & MCICSPPT	ACL O
V & OPERCMDS	allow:SYSADM group:alter:denv:*:execute
Ø DIAGS	
🍄 casout	
🎯 cassub	
☺ casfile	* 入力必須の項目です
♡ casstop	
♀ castran	



ESCWA からの停止例)

A リージョンの停止オプション	
▲ ロ <u>#12+ユ</u> ア ■ 動的に割り当てたサーバー アドレス値をクリアする [♀]	
□ 「弾制停止」オプションを使用する 🛇	
Enterprise Server 認証情報	
□ 現行のユーザー認証情報を使用する 🛇	
ユーザー名	
SYSAD	
パスワード	_
グループ	
	•3
 Unectory Serverとワーンヨンリオキモモトが一致しません。ノラットノオームによっては、 動時に不具合が発生する可能性があります。 	8
停止 戻	5

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。



記載の会社名、製品名は各社の商標または登録商標です。 本動作検証結果報告書は 2024年 6月に作成したものです。 MFWPE5-2406-00MFA | © 2024 Rockrtsoftware,Inc All rights