

CA Client Automation

encUtilCmd コマンド リファレンス

12.9



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。本ドキュメントは、CA が知的財産権を有する機密情報であり、CA の事前の書面による承諾を受けずに本書の全部または一部を複写、譲渡、変更、開示、修正、複製することはできません。

本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし、CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負います。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本書の制作者は CA および CA Inc. です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2014 CA. All rights reserved. 本書に記載されたすべての商標、商号、サービス・マークおよびロゴは、それぞれの各社に帰属します。

CA Technologies 製品リファレンス

このマニュアルセットで参照されている CA 製品は、以下のとおりです。

- CA Advantage® Data Transport® (CA Data Transport)
- CA Asset Intelligence
- CA APM (CA Asset Portfolio Management)
- CA Business Intelligence
- CA Common Services™
- CA DMM (CA Desktop Migration Manager)
- CA Embedded Entitlements Manager (CA EEM)
- CA MDM (CA Mobile Device Management)
- CA NSM (CA Network and Systems Management)
- CA Patch Manager
- CA Process Automation
- CA Service Desk Manager
- CA WorldView™

CA への連絡先

テクニカルサポートの詳細については、弊社テクニカルサポートの Web サイト (<http://www.ca.com/jp/support/>) をご覧ください。

目次

第 1 章 : encUtilCmd の使用法	7
auditapi : ENC ローカル監査設定を確認します	8
certimport - ローカル マシンの証明書ストアに証明書をインポートします	13
certverify - 必要な証明書が提供されていることを確認します	15
create - 認証ルール セットを作成します	17
export - 設定ストアから認証ルールのセットをエクスポートします	19
import - 認証ルールのセットを設定ストアにインポートします。	21
importdb - 認証ルールのセットをデータベースにインポートします	24
クライアント - ENC クライアントを設定します	28
netdiag : 一連の ENC 特有の診断を提供します	31
updateConfig—ENC 設定を更新します	33
verify - 認証ルールのセットをロードおよび検証します。	34
スクリプト コマンド	39
イベント タイプ	41
ルール ファイル形式	44
server : ENC ゲートウェイ サーバのステータスを表示します	52

第 1 章： encUtilCmd の使用法

encUtilCmd は ENC インフラストラクチャ用のコマンドライン ユーティリティです。 この ユーティリティには以下の機能があります。

監査

監査 [コマンド： auditapi]

ENC 監査設定データベースへのアクセスを許可します。

権限

ルール セットの作成 [コマンド： create]

認証ルールの基本セットを作成します。

エクスポート [コマンド： export]

共通保存内容から現在の認証ルールを読み取り、構造化テキストファイルに書き込みます。

インポート [コマンド： import]

構造化テキスト ファイルから認証ルールを読み取り、CMS 共通保存内容に書き込みます。

インポート データベース [コマンド： importdb]

構造化テキスト ファイルから認証ルールを読み取り、CMS CCNF データベースに書き込みます。

検証 [コマンド： verify]

認証ルール ファイルの内容とお客様の入力に基づいて認証ルールをテストします。

認証

証明書インポート [コマンド : certimport]

ENC が使用できるように Microsoft 証明書ストアに、証明書と PKCS#12 形式のキーをインポートします。

検証 [コマンド : certverify]

インストールされた証明書をテストおよび列挙します: 使用可能か、有効かです。

Miscellaneous

クライアント [コマンド : client]

ENC ゲートウェイ クライアントを有効または無効にします。

ネットワーク診断 [コマンド : netdiag]

一連の ENC 特有の診断を提供します。

サーバステータス [コマンド : server]

ENC ゲートウェイ サーバのステータスを表示します。

設定更新 [コマンド : updateconfig]

ポリシーまたは共通保存内容からポリシーを ENC コンポーネントに自動的にコピーします。

auditapi : ENC ローカル監査設定を確認します

短縮形 'au'

このコマンドは、ローカル マシン上の ENC 監査設定データベースへのアクセスを提供します。 監査の設定にはグラフィカル ユーザ インタフェースの使用をお勧めしますが、このコマンドを使用すると、GUI からはアクセスできない監査の要素のいくつかを制御できます。

auditapi の使用法

encUtilCmd auditapi 引数 [オプション]

オプション

-c カテゴリ

すべての監査カテゴリを表示します。

-cd カテゴリの無効化

1 つ以上のカテゴリを無効にし、パターン照合のための正規表現を許可します。

-ce カテゴリの有効化

1 つ以上のカテゴリを有効にし、パターン照合のための正規表現を許可します。

-da すべてをダンプ

すべての監査レコードをダンプします。

-dc カテゴリをダンプ

指定したカテゴリ内の監査レコードをダンプします。

-e 有効

メッセージが有効かどうかを指定します。

-f フィルタ

正規表現を使用してフィルタを適用します。

-ggs グローバル状態を取得

現在のグローバルな監査状態を表示します。

-mdメッセージの無効化

1つ以上のメッセージを無効にし、パターン照合のための正規表現を許可します。

-meメッセージの有効化

1つ以上のメッセージを有効化し、パターン照合のための正規表現を許可します。

-mgr マネージャ

マネージャ アクセスによって強制的に上書きします。

-sgsグローバル状態を設定

グローバルな監査状態を指定します。

-test 一致のテスト

パターン照合中に照合したカテゴリまたはメッセージのみを、設定データベースに変更をコミットすることなく表示します。

各項目は以下のとおりです。

-c カテゴリ [引数なし]

すべての監査カテゴリを表示します。これにより、最上位のカテゴリおよびそれに関連する状態が一覧表示されます。

-cd カテゴリの無効化 [パターン]

1つ以上のカテゴリを無効にします。引数は、照合対象のカテゴリ名のサブ文字列を指定します。たとえば、'-cd er'では、エラーおよびサーバが照合されます。エラーのみを照合するには、式を'-cd "^error\$"'というように完全修飾することができます。

注：'^'という記号は、Windows コマンドプロセッサ用の特殊文字で、ユーティリティ コマンドに渡すには、かっこで囲む必要があります。

-ce カテゴリの有効化 [パターン]

1 つ以上のカテゴリを有効にします。引数は、カテゴリの無効化オプションと同様に、サブ文字列を指定します。

-da すべてをダンプ

すべての監査レコードをコンソールにダンプします。このオプションは、すべての監査レコード ID およびそれに関連するカテゴリと個別のレコードの状態（有効または無効）を一覧表示します。監査レコードのサブセットのみが必要な場合は、このオプションと **-f** および **-dc** オプションを組み合わせます。

-dc カテゴリをダンプ [カテゴリ]

指定したカテゴリ内の監査レコードのみをダンプします。

注：このオプションは、**-da** スイッチと組み合わせて使用します。

例：

```
encutilcmd au -da -dc
```

-e 有効 [メッセージ ID]

メッセージが有効かどうかを指定します。このオプションの引数は、「IDS_CLI_NO_CERTS」のように、完全な監査レコード ID です。ユーティリティは、監査レコードの有効状態、そのカテゴリ、およびレコードの状態の理由を表示します。

-f フィルタ [パターン]

正規表現を使用してフィルタを適用します（監査レコード）。このオプションを **-da** オプションと組み合わせることで、指定した正規表現に一致するレコードのみを表示できます。

-sgs グローバル状態を取得

現在のグローバルな監査設定の状態を表示します。表示される状態は、すべて、なし、またはカテゴリのいずれかです。

グローバルな状態を設定するには、**-sgs** オプションを使用します。

-md メッセージの無効化 [パターン]

1 つ以上のメッセージを無効にし、パターン照合のための正規表現を許可します。このオプションは、個別レコードを無効化します。

-me メッセージの有効化

1 つ以上のメッセージを有効化し、パターン照合のための正規表現を許可します。このオプションは、個別レコードの有効状態が親カテゴリによって無効化されている可能性がある場合でも、その個別レコードを有効化します。

個別レコードの有効状態を表示するには、**-e** オプションを使用します。

-mgr マネージャ

マネージャ アクセスによって強制的に上書きするようにし、設定が DSM セキュリティ ポリシーによって一元管理されている場合でも、ローカルの監査設定を変更できるようにします。

注：このオプションには、管理者権限が必要です。

-sgs グローバル状態を設定

グローバルな監査状態を指定します。

状態は以下のとおりです。

- なし : すべての監査が無効です。
- すべて : すべての監査が有効です。
- カテゴリ - カテゴリおよび個々の状態の制御メッセージ。

注：ステータスが [カテゴリ] に設定されている場合は、**-e** オプションを使用してメッセージが有効または無効になっている理由を示します。

-test 一致のテスト

パターン照合中に照合したカテゴリまたはメッセージのみを、設定データベースに変更をコミットすることなく表示します。

このオプションを使用すると、実際は変更をコミットすることなく何が変更されるのかを評価できます。

certimport - ローカル マシンの証明書ストアに証明書をインポートします

短縮形 'certi'

この証明書インポート コマンドは、ENC が使用できるように Microsoft ローカル マシン証明書ストアに証明書をインポートします。ルート証明書は “Trusted Root Certification Authorities” フォルダに配置され、PKCS#12 証明書キーペアは “Personal” フォルダに追加されます。

使用法の出力

certimport - 必要な証明書が現在のマシンで利用できることを確認します。

certimport の使用法

encUtilCmd certimport 引数 [オプション]

オプション

-a 管理者をスキップ

管理者確認をスキップします。

-i PKCS#12

インポートする PKCS#12 形式の証明書とキーを指定します。複数の -i オプションを指定できますが、それぞれに対応する -p エントリが必要です。

-p パスワード

PKCS#12 ファイルの入力パスワードを指定します。

-r ルート

インポートするルート証明書を指定します。複数の **-r** オプションを指定できます。

-v 詳細

最大限の出力でコマンドを実行します。

各項目は以下のとおりです。

-a 管理者をスキップ

デフォルトでは、ユーザが管理者グループのアクティブなメンバであることを確認してから、インポート コマンドを実行します。このオプションを指定すると、ユーザが管理者グループのメンバでなくてもインポートを実行できる権限がある場合、確認をスキップできます。

-i PKCS#12

入力 PKCS#12 ファイルのパスを指定します。複数の **-i** オプションを指定できますが、それぞれに対応する **-p** オプションが必要です。PKCS#12 ファイルは、エクスポート不可能とマークされたプライベート キーとともにインポートされます。

-p パスワード

PKCS#12 形式ファイルの復号化に使用するパスワードを指定します。.

-r ルート証明書

Microsoft システム ストアにインポートされるルート証明書を指定します。

-v 詳細

詳細オプションを指定すると、インポート処理が発生したときに、処理に関して出力される情報が多くなります。

certverify - 必要な証明書が提供されていることを確認します

短縮形 'certv'

証明書確認コマンド **certverify** を使用して、必要な証明書が現在のマシンに提供されていることを確認します。

使用法の出力

certimport の使用法

encUtilCmd certverify 引数 [オプション]

オプション

-a 管理者をスキップ

管理者確認をスキップします。

-l ループバック

ローカルループバック接続を試行し、使用した ID について報告します。

-t ターゲット

ループバックで使用されるよう完全には設定されていないマシンに関して、ローカルな **FQDN** を指定します。

-v 詳細

最大限の出力でコマンドを実行します。

各項目は以下のとおりです。

-a 管理者をスキップ

デフォルトでは、ユーザが管理者グループのアクティブなメンバーであることを確認してから、インポート コマンドを実行します。このオプションを指定すると、ユーザが管理者グループのメンバーでなくてもインポートを実行できる権限がある場合、確認をスキップできます。

-l ループバック

これが指定されている場合、ユーティリティによってクライアントおよびサーバのセキュリティ コンテキストが作成され、証明書が有効であることを確認するためのループバック認証が実行されます。使用された証明書 ID が表示されます。インストールされた証明書で、クライアントおよびサーバの認証での使用が意図されている場合のみ、このオプションを使用できます。

-t ターゲット

ループバック オプションを使用するとき、ユーティリティがローカル マシンの完全修飾ドメイン名を自動的に決定できない場合、このオプションを使用して DNS 名を指定する必要がある場合があります。

-v 詳細

詳細オプションを指定すると、インポート処理が発生したときに、処理に関して出力される情報が多くなります。

create - 認証ルール セットを作成します

短縮形 'cr'

このコマンドにより、ENC インフラストラクチャ領域、DSM 管理領域、および指定された DSM メンバ領域（オプション）などの認証ルールの基本セットが作成されます。コマンドの出力は、認証テスト、共有の保存内容へのインポートまたは設定データベースへのインポートで使用できます。

構文

encUtilCmd create 引数 [オプション]

オプション

-ex XML のエクスポート

ルールの XML バージョンを指定ファイルに書き込みます。

-o 出力

指定されたファイルに出力を書き込みます。デフォルトでは、コンソールに書き込みます。

-r 領域

領域の名前を指定します。このオプションは複数回指定できます。

-tb テスト用バッチ ファイル

-ts によって作成されたスクリプトを呼び出してテストする指定のバッチ ファイルを作成します。

-ts テスト スクリプト

指定のテスト スクリプトを作成します。-o オプションの設定が必要です。

-v 詳細

最大限の出力でコマンドを実行します。

各項目は以下のとおりです。

-ex XML のエクスポート

XML 形式でルール セットを出力します。これは、`ccnfregdb` コマンドへの直接入力として使用できます。

-o 出力

テキスト形式のルール セットを格納するために使用する出力ファイルを指定します。デフォルトでは、ルールはコンソールに書き込まれます。

-r 領域

ルール セットに含める指定の領域を指定します。複数の領域を指定するには、「`-r`」オプションで複数のインスタンスを指定します。

-tb テスト用バッチ ファイル

テスト用バッチ ファイルを作成して、`-ts` オプションを使用して作成されたテスト スクリプトを呼び出すようユーティリティに指示します。

-ts テスト用スクリプト

このオプションにより、新しく作成されたルール セットを実行するためのテスト スクリプトが作成されます。

-v 詳細

詳細オプションを指定すると、ルール セット処理が発生したときに、処理に関して出力される情報が多くなります。

export - 設定ストアから認証ルールセットをエクスポートします

短縮形 'e'

DSM 共通保存内容から現在の認証ルールセットを抽出し、フラット ファイル構造に変換します。

`encUtilCmd export` 引数 [オプション]

オプション

-ab 省略

省略されたイベントを使用してエクスポート ルールセットを指定します。

-al 代替

代替ルール セットを指定します。

-ex XML のエクスポート

ルールの XML バージョンを指定ファイルに書き込みます。

-o 出力

指定されたファイルに出力を書き込みます。

デフォルトでは、コンソールに書き込みます。

-v 詳細

最大限の出力でコマンドを実行します。

各項目は以下のとおりです。

-ab 省略

イベント名を省略されたバージョンでエクスポートします。

例：ServerRegisterAgent は、SRA としてエクスポートされます。

注：verify -pe コマンドとオプションの組み合わせは、イベントの完全な名前、およびそれらの省略名がカッコに囲まれた形式で表示されます。

-al 代替

デフォルトでは、export コマンドは、共通保存内容の場所 “itrm/common/enc/authz” から認証ルールセットを読み取ります。マシンの処理に影響を及ぼさずにマシンでルールを評価できるように、別の場所（たとえば、“test1”）にルールを配置するよう指定できます。

-ex XML のエクスポート

ccnfredb ツールで使用するのに適した XML バージョンを作成および保存します。

-o 出力

フラット ファイルルール用の出力ファイルを指定します。デフォルトでは、ユーティリティはコンソールに出力します。

-v 詳細

export コマンドを詳細モードで実行します。'-v' オプションの使用は累積的です。コマンドラインで 1 回または複数回指定して、詳細さのレベルをインクリメントできます。

import - 認証ルールセットを設定ストアにインポートします。

短縮形 'import'

指定のフラット ファイルから入力を読み込み、ある程度入力を確認してから、共通保存内容の指定領域に書き込みます。

`encUtilCmd import` 引数 [オプション]

必須引数 :

-i 入力ファイル

入力ファイルを指定します。

オプション

-al 代替

代替ルール セットを指定します。

-ex XML のエクスポート

ルールの XML バージョンを指定ファイルに書き込みます。

-fl 保存内容の消去

新規ルール セットを書き込む前に、現在のルール セットを共通保存内容から消去します。

-lr 領域のリスト

入力ファイルから領域名を出力します。

-mgr マネージャ

マネージャがアクセスして上書きするようにします。

管理者権限が必要です。

-notify 通知

設定が変更されたことを通知するために、ENC プロセスにシグナルを送ります。

-nw 書き込みなし

ルールをコミットせず、入力ファイルの解析だけを行います。

-v 詳細

最大限の出力でコマンドを実行します。

各項目は以下のとおりです。

-i 入力ファイル

入力フラット ファイルの名前を指定します。

-al 代替

デフォルトでは、import コマンドは、認証ルールセットを共通保存内容の場所 “itrm/common/enc/authz” に書き込みます。 マシンの処理に影響を及ぼさずにマシンでルールを評価できるように、別の場所（たとえば、“test1”）にルールを配置するよう指定できます。

-ex XML のエクスポート

ccnfregdb ツールで使用するのに適した XML バージョンを作成および保存します。

-fl 保存内容の消去

共通保存内容にルールセットがすでに存在する場合、ユーティリティは、破損や競合を防止するために、現在のセットを上書きしません。 ‘-fl’ 消去コマンドを使用して既存のルールセットをクリアしてから、新しいルールセットをコミットします。

-lr 領域のリスト

入力ファイルから読み取った領域をリストします。

-mgr マネージャ

現在のルールセットが集中管理されたポリシーとして適用され、しかもルール定義が正しくないためにポリシーセットによってマシンの通信が妨げられる場合は、**'-mgr'** スイッチを使用してルールを適用し、集中管理されたポリシー オプションを上書きします。マシンが次にポリシー更新を受信したとき、これらのルールは集中管理され定義されたルールによって上書きされます。

-notify 通知

ENC ゲートウェイが新しい設定データをただちに読み取るようにするには、このオプションを使用します。認証設定が更新されたすべてのリスンプロセスに、ユーティリティがシグナルを送ります。

-nw 書き込みなし

ユーティリティは新しいルールセットを共通保存内容にコミットしません。ユーティリティは、共通保存内容にコミットせずに、新しいルールセットをロード、解析、および評価できます。

注： このオプションは、**flush** コマンドの処理を停止しません。**'-fl'** と **'-nw'** を組み合わせて使用すると、新しいルールセットを書き込まずに、既存の共通保存内容を消去できます。これは空の設定セットをテストし、古いテストセットをクリアするのに便利ことがあります。

-v 詳細

import コマンドを詳細モードで実行します。**'-v'** オプションの使用は累積的です。コマンドラインで **1** 回または複数回指定して、詳細さのレベルをインクリメントできます。

importdb - 認証ルールをデータベースにインポートします

短縮形 'importd'

importdb コマンドは、指定のフラット ファイルから入力を読み込み、入力を確認してから、**ccnfredb** ツールを使用してルールセットを **CCNF** データベースに書き込みます。認証設定は **ENC** ゲートウェイ ノードにのみ配信される必要があるため、**ENC** ノードの **DSM** グループとの次の関連付けのための新しいポリシーがこのコマンドによって作成されます。この動作は、既存のデフォルトのコンピュータ ポリシーに書き込むようデフォルトのオプションを指定することにより修正できます。

`encUtilCmd importdb` 引数 [オプション]

必須引数 :

-i 入力ファイル

入力ファイルを指定します。

-n ポリシー名

インポートするポリシー名を指定します。

オプション

-def デフォルト

デフォルトのコンピュータ ポリシーに書き込みます。

-desc 説明

ポリシーの説明を定義します。

-ex XML のエクスポート

ルールの XML バージョンを指定ファイルに書き込みます。

-lr 領域のリスト

入力ファイルから領域名を出力します。

-m マネージャ

CCNFREGDB：ターゲット マネージャ名を指定します。

デフォルトは localhost です。

-nw 書き込みなし

ルールをコミットせず、入力ファイルの解析だけを行います。

-o 上書き

CCNFREGDB。既存の設定データベース値を上書きするかどうかを指定します。

デフォルトでは、上書きしません。

-s 自動更新をスキップ

CCNFREGDB。影響を受けるコンピュータについて自動設定更新をスキップするかどうかを指定します。

デフォルトでは、すぐに更新を行います。

-v 詳細

最大限の出力でコマンドを実行します。

各項目は以下のとおりです。

-def デフォルト

新しい名前付きポリシーではなく、デフォルトのコンピュータ ポリシーに認証データがインポートされるように指定します。これにより、現在の **DSM** ドメインに関連付けられたすべての **DSM** ノードに認証データが配信されます。

-desc 説明 [テキスト文字列]

インポートされたポリシーに演算子が指定された記述文字列を適用します。これは、ポリシーの目的に関するコメントを追加するのに使用されます。

-ex XML のエクスポート

ccnfregdb ツールで使用するのに適した **XML** バージョンを作成および保存します。

-i 入力ファイル

入力フラット ファイルの名前を指定します。

-lr 領域のリスト

入力ファイルから読み取った領域をリストします。

-m マネージャ

このオプションは、登録コマンドのターゲット マネージャとして **ccnfregdb** ツールに渡されます。デフォルトでは、コマンドはドメイン マネージャ ホストで実行されると予測されるので、ターゲットは 'localhost' です。

-n ポリシー名 [テキスト文字列]

新しくインポートされたポリシーに名前を付けます。

例：ENC-RuleSet-Main

-nw 書き込みなし

ユーティリティは新しいルールセットをデータベースにコミットしません。ユーティリティは、新しいルールセットをコミットせずに、ロード、解析、および評価できます。

-o 上書き

このオプションは **ccnfregdb** ツールに渡されます。設定データベース内の既存のルールを上書きするかどうかを指定します。**ccnfregdb** ツールのデフォルトのオプションでは、既存データに上書きしません。

-s 自動更新をスキップ

このオプションは **ccnfregdb** ツールに渡されます。影響を受けるコンピュータについて自動設定更新をスキップするかどうかを指定します。デフォルトでは、影響を受けるすべてのコンピュータにすぐにポリシーが配信されます。

-v 詳細

importdb コマンドを詳細モードで実行します。'-v' オプションの使用は累積的です。コマンドラインで 1 回または複数回指定して、詳細さのレベルをインクリメントできます。

クライアント - ENC クライアントを設定します

短い形式「cl」

ENC ゲートウェイ クライアントを有効または無効にし、そのクライアントに関連する他の設定項目を設定します。

このコマンドを使用すると、ターゲット **ENC** ゲートウェイ サーバおよびその設定ポートを設定したり、プロキシ設定情報を設定したりできます。

ENC クライアントはポリシーによって設定されます。これには、インターネット プロキシ サーバへの接続に必要なユーザ名とパスワードが含まれることがあります。違うパスワードがポリシーによって間違えて送信された場合、ターゲット マシンは、プロキシと認証できなくなるため、**ENC** から切断されることがあります。

ファイアウォールによってドメイン マネージャから分離されている場合、マシンは問題を訂正するためのポリシー更新を受信できません。これに対応するには、通常は **ccnfcmda** を使用して正しいクレデンシャルを **comstore** に手動で入力する必要がありますが、パスワードが暗号化されているので、これだけでは不十分です。**Encutilcmd** には、暗号化されたパスワードを入力する手段があります。

構文

Encutilcmd client [オプション]

必須オプション：

-proxy_http

HTTP プロキシのクレデンシャルを設定します -

-proxy_socks

SOCKS5 プロキシのクレデンシャルを設定します

-state

ENC クライアントの状態を設定します。

状態のオプション :

-port_http

ENC ゲートウェイ サーバのターゲット HTTP ポートを指定します。

-port_tcp

ENC ゲートウェイ サーバのターゲット TCP ポートを指定します。

-server

ターゲット ENC ゲートウェイ サーバの完全修飾ドメイン名を指定します。

プロキシのオプション :

-password [パスワード]

プロキシのパスワードを指定します。この引数が省略されていたり、'*'文字列として指定されている場合、入力した文字のエコーなしで、それがコマンドによって要求されます。

-proxy_clear

1 つ以上の格納済みプロキシ設定のエントリを削除する必要があることを指定します。

-proxy_host

プロキシサーバのホスト名を指定します。

-proxy_port

プロキシサーバのポート番号を指定します。

-proxy_view

現在の格納済みプロキシ設定のエントリを表示するには、このオプションを使用します。

-user [ユーザ名]

プロキシのユーザ名を指定します。

その他のオプション :

-mgr

マシンの設定が集中管理されている場合、設定を強制的に変更するオプションを使用します。このオプションには、管理者権限が必要です。次回集中的なポリシーが配信されたときには、変更が失われる場合があります。

-restart

SSA および CAM が最初に ENC を使用するよう設定されている場合、SSA および CAM を再起動する必要があります。このオプションを使用すると、ステータス コマンドの完了時に再起動します。

-start

現在のコマンドの完了時に ENC クライアントを起動するには、このオプションを使用します。-stop と組み合わせて、ENC クライアントを循環させることができます。

-stop

現在のコマンドの完了後に ENC クライアントを停止するには、このオプションを使用します。上記の -start と組み合わせることができます。

例 :

```
Encutilcmd client -state show
```

ENC クライアントの現在の設定の状態が表示されます。

```
Encutilcmd client -state enabled -server example.forwardinc.ca -start
```

これによりクライアントの状態が有効に設定され、example.forwardinc.ca の ENC ゲートウェイ サーバに接続するようクライアントが設定され、ENC クライアントが起動します。

```
Encutilcmd client -proxy_http -proxy_host <proxy server name> -proxy_port <proxy server port> -user <username> -password <password>
```

このコマンドにより、HTTP プロキシ接続の詳細がクライアント用に設定されます。

netdiag : 一連の ENC 特有の診断を提供します

短縮形 'ne'

一連の ENC 特有の診断を得るには、netdiag コマンドを使用します。

netdiag の使用法 :

encUtilCmd netdiag 引数 [オプション]

オプション

-r 解決

指定された名前を ENC アドレスに解決しようとします。

-Summary サマリ

ローカル ENC コンポーネントの設定およびステータスのサマリの出力を表示します。

-track トラッキング

指定されたセキュリティ サブ文字列を現在のマシン上のトラッキング リストに追加します。これらの文字列を含むすべての認可リクエストは、高レベルでトレースされます。

-trclear トラッキングをクリア

現在のトラッキング値をクリアします。

-trshow トラッキングを表示

現在のトラッキング値を表示します。

-v 詳細

最大限の出力でコマンドを実行します。

各項目は以下のとおりです。

-r 解決 [ホスト名]

指定された名前を ENC アドレスに解決しようとします。

-summary Summary [no arguments]

ローカル ENC コンポーネントの設定およびステータスのサマリの出力を表示します。

-track トラッキング [テキスト文字列]

指定されたセキュリティ サブ文字列を現在のマシン上の追跡リストに追加します。これらの文字列を含むすべての認可リクエストは、高レベルでトレースされます。

注：# を区切り文字として使用して、複数の文字列を指定できます。

これにより、一般的なトレース レベルを増やしてすべてのマシンを含める代わりに、ターゲットであるマシンを選択的にトレースできるようになります。

例：

```
-track dc=forwardinc#cn=someone#cn=someone-else
```

クライアントの認証済み ID が「dc=forwardinc」、「cn=someone」、または「cn=someone-else」のサブ文字列のいずれかを含む認可リクエストのトレース レベルが増加します。

-trclear トラッキングをクリア

現在のトラッキング値をクリアします。

-trshow トラッキングを表示

現在のトラッキング値を表示します。

-v 詳細

netdiag の処理が行われる際に、その詳細を表示します。

updateConfig—ENC 設定を更新します

サーバ、ソケットアダプタ、Tomcat のように、ポリシーまたは共通保存内容から直接設定されないいくつかの **ENC** コンポーネントがあります。直接設定される代わりに、これらのコンポーネントには専用のプライベートデータファイルがあります。通例、ポリシーはこれらのファイルに自動的にコピーされます。しかし、パラメータをローカルに設定する必要がある場合は、**updateConfig** コマンドでコピー操作を実行します。代表的な例を挙げると、マシンが誤設定されており、ファイアウォールによってドメインマネージャから切り離されようとしている場合です。このようなマシンは、問題を修正する新しいポリシーを受信できません。問題は手動で解決する必要があります。必要な変更は **ccnfcmda** コマンドを使用して **comstore** に対して行い、“**encutilcmd updateconfig**” を使用して転送できます。

updateConfig コマンドは、すべての設定データが更新されたことをすべてのプロセスに通知します。単一の領域のみ更新するほうが望ましい場合もあります。

オプション

-audit 監査

監査設定の更新の変更を通知します。

-authz 認証

認証の更新の変更を通知します。

-server サーバ

ENC サーバプロセスの更新の変更を通知します。

-ssaSSA

SSA の更新の変更を通知します。

verify - 認証ルールセットをロードおよび検証します。

短縮形 'v'

認証ルールセットで定義された基準に対して、1つまたは複数のイベントを評価できます。評価パラメータは、1つのイベントを評価するためにコマンドラインに直接渡すこともできますし、1つまたは複数のイベントをシリアルに評価するためにスクリプトファイルとして提供することもできます。

encUtilCmd verify 引数 [オプション]

必須引数：

-e イベント

評価するイベントを指定します（すべての場合は **-pe** を使用）。イベントごとにオプションを設定する必要があります。 **-f** を設定した場合、このオプションは無視されます。

-f テスト ファイル

指定されたテスト ファイルをロードおよび処理します。

-i 入力ファイル

入力ファイルを指定します。指定しないと、共通保存内容が直接使用されます。指定する場合は、**-al** も指定する必要があります。

オプション

-al 代替

代替ルールセットを指定します。

-date 日付

テストで評価する日付を [形式 YYYYMMDD] という形式で指定します。

デフォルト – 現在の日付。

-error エラー

ルールが失敗した場合、キー入力があるまで一時停止します。

-fl 保存内容の消去

新規ルールセットを書き込む前に、現在のルールセットを共通保存内容から消去します。

-nt ノードタイプ

テスト用のノードタイプを指定します（MRS/SRS/ROUTER）。

-p プリンシパル

テスト用のセキュリティプリンシパルを指定します（URI）。

-pause 一時停止

各イベントの後、キー入力用に一時停止します。

-pe イベントの出力

イベントタイプの一覧を出力します。

-q クワイエット

ルール的一致を表示せず、イベント完了サマリだけを表示します。

-s ソース IP

テスト用のソース IP アドレスを指定します。

-t ターゲット

テスト用のターゲットを指定します。

-time 時刻

テストで評価する時刻を [形式 HHMMSS] という形式で指定します。

デフォルト – 現在の時刻。

-tz タイムゾーン

ターゲットのタイムゾーンを指定します [UTC+HHMM 形式]。

-v 詳細

最大限の出力でコマンドを実行します。

注: 'e'、'f'、'i' の各オプションはすべて必須引数としてリストされますが、指定する必要があるのは 'e' または 'f' のみです。

-al 代替

評価に使用する代替ルールセットを指定します。こうすると、('i' スイッチを使用する場合) テスト用に別の場所に新規ルールセットを書き込めますし、すでにインポート済みの場合は既存の代替セットを使用できます。

-date 日付

評価の間に使用するシミュレーションされる日付を指定します。デフォルトでは、現在の日付が使用されます。このオプションの形式は YYYYMMDD です。YYYY は 4 桁の年、MM は 2 桁の月 (01 ~ 12)、DD は 2 桁の日 (01 ~ 31) です。日付は部分的に YYYY または YYYYMM と指定することもできます。この場合、月と日はそれぞれ "01" と仮定されます。

-e イベント

評価するイベントタイプを指定します。'-e' オプションを指定し、必要なパラメータのセットを指定せずに検証コマンドを実行すると、エラーが記録されます。

-error エラー

一連のルールを評価するとき、ルールが失敗しても検証ユーティリティは停止しませんが、残りのルールの評価を続行します。ルールエントリでエラーが発生したときにルールの評価を一時停止する場合に、このオプションを指定できます。

-f テスト ファイル

評価するイベントを含むテスト スクリプト ファイルを指定します。スクリプトに関して使用できるコマンドについては “Script Commands” のセクションを参照してください。

-fl 保存内容の消去

‘-l’ オプションを指定する場合は、共通保存内容から既存のルールを消去してから新規セットを書き込む必要がある場合があります。このオプションを使用して、既存のルールを削除します。

-i 入力ファイル

入力ルール ファイルセットを指定します。指定しないと、共通保存内容内の現在のルールが明示的に使用されます。

-nt ノード タイプ

イベント評価の間に使用するノードタイプを指定します。デフォルトは設定で決まりますが、このオプションを使用すると、動作を異なるノードタイプとしてエミュレートできます。使用できる値は、MRS、SRS および Router の組み合わせです。複数のオプションを指定する場合は、-nt “SRS Router” のように引用符に囲んでください。

-p プリンシパル

イベント評価の間に使用するセキュリティ プリンシパルを指定します。

-pe イベントの出力

認識されたイベント タイプのリストをコンソールに出力するようユーティリティに指定します。

-q クワイエット

イベントの評価中にマッチング ルールの名前を表示せず、サマリ ステータスのみ表示します。

-s ソース IP

「ipconnection」 イベントのソース IP アドレスを指定します。

-t ターゲット

イベント評価の間に使用するターゲットを指定します。これはイベントのコンテキストに特有です。関連するターゲットについては“Event Types”のセクションを参照してください。.

-time 時刻

イベント評価の間に使用される、シミュレーションされた時刻を指定します。デフォルトでは、現在の時刻が使用されます。このオプションの形式は HHMMSS です。HH は時間 (0 ~ 23)、MM は分 (00 ~ 59)、SS は秒 (0 ~ 59) です。日付は部分的に HH または HHMM と指定することもできます。この場合、分と秒はそれぞれ “00” と仮定されます。

-tz タイム ゾーン [時間文字列]

ルール検証時に、操作のターゲットのタイム ゾーンを指定します。このオプションの形式は、UTC+HHMM です。

例 : -tz UTC+02:00 ;

-tz UTC-05:00

各 ENC オブジェクトは、ENC インフラストラクチャへの登録時に、設定されたタイム ゾーンを転送します。特定のターゲットに対するすべてのアクセス制御エントリが、そのタイム ゾーンで評価されます。検証コマンドは、このオプションを使用してタイム ゾーンをシミュレートすることができます。使用しない場合は、UTC+0 のタイム ゾーンに想定されます。

-v 詳細

検証コマンドを詳細モードで実行します。'-v' オプションの使用は累積的です。コマンドラインで 1 回または複数回指定して、詳細さのレベルをインクリメントできます。

スクリプト コマンド

このセクションでは、検証コマンドのスクリプト処理セクションで使用できる全コマンドをリストします。

検証コマンドは、直接のコマンドラインまたはスクリプト ファイルで指定できます。スクリプト ファイルは以下のもののよう、単純な形式があります。

キーワード 値 <EOL>

先頭が ';' または '#' の行はコメント行と見なされ、無視されます。

使用できるキーワードと可能な値は次のとおりです。

principal [変数]

認証チェックで実行されるセキュリティ プリンシパル URI を指定します。値の形式は自由です。キーワードから行末までのすべてがプリンシパル名としてロードされます。このキーワードは正しいかどうか検証されません。

sourceip [変数]

アドレス認証チェックに使用される IP アドレスを指定します。値の形式は自由です。キーワードから行末までのすべてがアドレスにロードされます。このキーワードは正しいかどうか検証されません。

nodetype [変数]

認証チェック用にノード タイプを指定します。以下の 1 つ以上を指定できます。

- MRS – マスタ ノード (マネージャ)
- SRS – スレーブ ノード (サーバ)
- Router – ルータ ノード (ルータ)

エージェント タイプは常に黙示的です。

target [変数]

処理のターゲットを指定します (保護対象オブジェクト)。

date [変数]

テスト用にシミュレーションされる日付を指定します。形式は検証コマンドの “-date” オプションと同じです。

time [変数]

テスト用にシミュレーションされる時刻を指定します。形式は検証コマンドの “-time” オプションと同じです。

クリア

すべての変数または 1 つの指定変数をクリアします。[変数] としてマークされたキーワードはすべてクリアできます。

event [変数]

テストするイベント タイプを設定し、テスト評価も開始します。

テスト スクリプトの例 :

テスト スクリプトの例は次のとおりです。

```
1      #
2      # すべての目的 ENC ノードへの IP 接続をエミュレート
3      # 2008 年 12 月 25 日 12:34:04
4      #
5      nodetype mrs srs router
6      sourceip 192.168.0.1
7      date 20081225
8      time 123404
9      event ipconnection
```

このスクリプトは、“nodetype”、“sourceip”、“date”、および“time”変数を設定してから、“ipconnection”アクセスを確認します。

テスト出力の例 :

```
イベント <ipconnection> をライン <9> から処理
日付 <20081225> 時刻 <123404> ノードタイプ <mrs srs router>。
処理は次の理由で許可されました。
'Item found in allowed list by pattern match'
パターン:
'.'
イベント <ipconnection> は <allowed> でした。
```

イベント タイプ

このセクションでは、検証コマンドに適用できるイベント キーワードをリストします。

いずれの場合でも、該当するパラメータが認証 API に渡され、API はアクセスが許可されるか拒否されるかを決定します。 イベントが許可または拒否される理由が表示され、理由および関連アクセス制御エントリが示されます。

イベント : NetworkConnection

パラメータ : sourceip、nodetype

該当するコンテキスト : すべてのノード

このイベントは、ENC ノードへの初期 TCP/IP 接続の間に呼び出されます。アドレスの認証ホワイトリストにより、ターゲット ノードへのアクセスが決定されます。

イベント : AuthenticatedConnection

パラメータ : principal、nodetype、target

該当するコンテキスト : すべてのノード

このイベントは、クライアント接続が認証シーケンスを完了した後で呼び出されます。認証 ID (プリンシパル) とターゲット (領域) が認証 API に渡されます。

イベント : ManagerRegisterServer

パラメータ : principal、nodetype、target

関連するコンテキスト : ゲートウェイ マネージャ

SRS ノードが MRS に登録コマンドを送信するとき、このイベントが呼び出されます。

イベント : ServerRegisterRouter

パラメータ : principal、nodetype、target

関連するコンテキスト : ゲートウェイ サーバ

Router ノードが SRS に登録コマンドを送信するとき、このイベントが呼び出されます。

イベント : ManagerRegisterRouter

パラメータ : principal、nodetype、target

関連するコンテキスト : ゲートウェイ マネージャ

SRS が MRS にルータ登録コマンドを転送するとき、このイベントが呼び出されます。

イベント : ServerRegisterAgent

パラメータ : principal、nodetype、target

関連するコンテキスト : ゲートウェイ サーバ、ルータ

エンドクライアントが SRS ノードまたは Router ノードに登録しようとしたときに、このイベントが呼び出されます。

イベント : ManagerRegisterAgent

パラメータ : principal、nodetype、target

関連するコンテキスト : ゲートウェイ マネージャ

SRS がクライアント登録イベントを MRS に転送したときに、このイベントが呼び出されます。

イベント : ManagerNameLookup

パラメータ : principal、nodetype、target

該当するコンテキスト : すべてのノード

このイベントは、エンド ノードが名前のルックアップ リクエストを実行するときに呼び出されます。

イベント : AgentConnect

パラメータ : principal、nodetype、target

関連するコンテキスト : ゲートウェイ マネージャ、サーバ

このイベントは、エンド ノードがターゲット ノードへのアクティブな発信接続を試みるときに呼び出されます。.

イベント : RouterAgentConnect

パラメータ : principal、nodetype、target

関連するコンテキスト : ゲートウェイ ルータ

このイベントは、エンド ノードがルータに接続してピア ノードへの仮想接続を設定しようとするときに呼び出されます。

イベント : ManagementAccess

パラメータ : principal、nodetype、target

関連するコンテキスト : ゲートウェイ マネージャ

エンド ノードが ENC ゲートウェイ マネージャからの管理情報を要求したときに、このイベントが呼び出されます。

ルール ファイル形式

このセクションでは、認証ルール ファイルの形式を定義します。次に抽出したものは、ファイルの基本レイアウトを示します。

[authz] セクション タイトルとバージョン キーをファイルの最初のエントリにする必要があります。

個別のセクション（ [timeRange] 、 [timeacl] 、 [URIMapping] 、 [dnsmapping] および [IPAddWhiteList] ）は、すべては存在する必要がありませんし、事前決定された順序である必要也没有。しかし、存在する場合は、すべて “end” キーワードで終了する必要があります。

何行かの最後に `+` 記号がある場合は、1 つのセクション内に複数のエントリがある可能性が示されますが、記号を実際のファイルには入力してはなりません。

```
[authz]
RulesVersion=n
```

```
realm
{ name xxx notes yyy}+*
end
```

```
timeRange
{name xxx enabled x hours hhh type ttt weekdays www year yyyy month mmm day ddd}+*
end
```

```
timeacl
{name xxx enabled x SecPrincType xxx events xxx RuleType xxx TimeRange xxx SecPrinc
xxx SecObj xxx SecObjType xxx }+*
end
```

```
URIMapping
{URI xxx enabled x type xxx realm xxx}+*
end
```

```
IPAddWhiteList
{IPAddress enabled x xxx type xxx}+*
end
```

各セクションとエントリの詳細な分析は次のとおりです。

すべてのレコードタイプについて、スペースを含む値は二重引用符で囲んで、値の開始と終了を示す必要があります。たとえば、次のとおりです。

名前 “this is the record name”

さらに、各レコードの最初と終了は開いた中括弧と閉じた中括弧にする必要があります。‘{’ と ‘}’ です。

共通属性：

2 つ以上のセクションで使用される属性がいくつかあります。ここで詳細に説明します。

属性：‘enabled’

個別のレコードを有効にするには **1** に設定し、無効にするには **0** に設定します。

無効にされたレコードも処理、検証、および格納されますが、認証コンポーネントの作用を受けることはありません。

属性：‘name’

timeRange エントリまたは **timeacl** エントリを記述する読み取り可能な名前。この名前は直接の認証のためには使用されません。診断のため、および時間帯でアクセス制御エントリを相互参照するために使用されます。たとえば、7 月 4 日の **timeRange** エントリは “Independence Day” と呼ばれます。

セクション： 領域

このセクションは、次のセクションの領域名を定義します。

属性：‘name’

これは、後で使用するために領域の名前を定義します。通常領域名には、メンバシップリスト用にわかりやすい名前を付ける必要があります。

属性：‘notes’

この属性は、この領域エントリに注意事項を追加するための機能を提供します。注意事項は解釈はされませんが、認証設定のグラフィカルユーザインターフェースに表示されます。

セクション： timeRange

このセクションでは、timeacl セクションがその後使用するように時間帯を定義します。

時間帯は、一般的な曜日の範囲、または休日やスケジュールされたメンテナンスなどの重要な日付を記述できます。

timeRange の各エントリの最初の属性と値ペアは名前属性にする必要があります。

属性： 'name'

共通属性で説明したとおりです。

属性： 'enabled'

共通属性で説明したとおりです。

属性： 'hours'

この属性は、時間帯が有効な時間を記述します。'hours' エントリの最小単位は 30 分です。'hours' の値は、1 つのエントリ、開始と終了のある 1 つの範囲、または複数の範囲で指定できます。

- 'hours' 値「7:00」は、ローカル時間の午前 7 時から午前 7 時 29 分 59 秒までを意味します。
- 'hours' 値「9:00 – 17:00」は、ローカル時間の午前 9 時から 17 時 00 分 00 秒までを意味します。
- 'hours' 値「9:00 – 11:30 13:00 – 17:00」は、ローカル時間の午前 9 時から午前 11 時 30 分 00 秒まで、および午後 1 時から午後 5 時 00 分 00 秒までを意味します。

属性： 'type'

'type' 属性によって、この時間帯レコードの種類が決まります。指定できる値は 'normal' または 'special' です。

- 'normal' 値は、アクティブである時点を決定するために 'weekdays' 値を使用する通常のレコードを定義します。タイプが 'normal' の場合は、'weekdays' 属性と値のペアが存在する必要があります。
- 'special' 値は特定の日付にのみ適用できるレコードを定義します。タイプが 'special' の場合は、年、月、日の属性と値のペアが存在する必要があります。

属性：‘weekdays’

‘weekdays’ 属性は、通常（normal）時間帯がアクティブな期間を定義します。値は、1 つの日、複数の個別の日、1 つの日の範囲、または複数の日の範囲にできます。.

- ‘weekdays’ エントリ “Sunday” は、日曜にのみ有効になる時間帯を定義します。
- ‘weekdays’ エントリ “Monday Friday” は、月曜と金曜にのみ有効になる時間帯を定義します。
- ‘weekdays’ エントリ “Sunday-Tuesday” は、日曜から火曜日に有効になる時間帯を定義します。
- ‘weekdays’ エントリ “Sunday-Monday Wednesday-Thursday Saturday” は、日曜から月曜、水曜から木曜、および土曜に有効になる時間帯を定義します（つまり、火曜と金曜は除きます）。

属性：‘year’、‘month’、‘day’

これらの属性はすべて ‘specialdaytype’ について存在する必要があるなので、一緒にまとめます。

- ‘year’ の値は、年を 4 桁の数値で表したものです。
- ‘month’ の値は、月の値を表す数値です。有効な値は “1” ～ “12” で、それぞれ 1 月から 12 月です。
- ‘day’ の値は、“1” ～ “31” を表す数値です（1 と 31 を含みます）。

特別な日付の値のいずれかがゼロ（0）である場合、これはワイルドカードの一致として使用され、0 が年、月または日付のそれぞれに一致します。

セクション： timeacl

このセクションは、Time ACL（時刻アクセス制御リスト）を形成する個別の TACE（時刻アクセス制御エントリ）を定義します。

timeacl の各エントリの、最初の属性と値のペアは名前属性にする必要があります。

属性：‘name’

共通属性で説明したとおりです。

属性：‘enabled’

共通属性で説明したとおりです。

属性：‘SecPrincType’

この属性値は、この TACE を使用するときに行われる一致のタイプを定義します。値は ‘normal’、‘pattern’、または ‘realm’ のいずれかを指定できます。

- ‘normal’ に設定されているとき、TACE は、‘SecPrinc’ 属性値に正確に一致する ID についてアクティブです。
- ‘pattern’ に設定されているとき、TACE は、‘SecPrinc’ 属性値の正規表現に一致するすべての ID についてアクティブです。
- ‘realm’ に設定されているとき、TACE は、‘SecPrinc’ 属性値の正規表現に一致するすべての ID についてアクティブです。

属性：‘Events’

この属性は、TACE が適用できるイベント（1 つまたは複数）を定義します。イベント名はセクション “Event Types” に定義されているとおりです。

属性：‘RuleType’

この属性は TACE のタイプを定義します。値は ‘allow’ または ‘deny’ のどちらかです。

属性：‘TimeRange’

これは時間帯エントリの相互参照です。いつ TACE がアクティブかを制御します。属性値は時間帯名と正確に一致する必要があります。インポートユーティリティは、各 TACE が有効な時間帯を参照することを検証します（ただし、時間帯について ‘enabled’ フラグを立てることは強制されません）。

属性：‘SecPrinc’

これは、1 つのセキュリティ プリンシパルの明示的な名前、複数のセキュリティ プリンシパルに一致させるのに使用する正規表現、または領域名、これらのいずれかです。

属性：‘SecObj’

これは、保護対象オブジェクト（処理のターゲット）の明示的な名前、または複数の保護対象オブジェクトとの一致に使用される正規表現です。

属性：‘SecObjType’

これは、‘SecObj’ 属性内の文字列を定義します。

定義されている現在のタイプは、

- ‘normal’
- ‘pattern’
- ‘realm’

セクション： URIMapping

このセクションでは、セキュリティプリンシパル名がどのように領域にマップされるかを定義します。各エントリの最初の属性と値のペアは‘URI’ キーワードでなければなりません。

属性：‘URI’

この文字列は、領域メンバシップを決定するために、セキュリティプリンシパル ID との比較に使用されます。

属性：‘enabled’

共通属性で説明したとおりです。

属性 : 'type'

エントリのタイプを定義します。値は 'normal' または 'pattern' に設定できます。

- 'normal' に設定すると、URI の値が領域メンバシップと完全一致として使用されます。
- 'pattern' に設定すると、URI の値がパターン一致の正規表現として使用されます。

属性 : 'realm'

この属性は、セキュリティプリンシパルのマップ先領域（1 つまたは複数）の名前を定義します。

各領域名を '#' 記号で区切ると、複数の領域を指定できます。

"*" という特殊な領域名があり、これはすべての領域と一致します。'*' 領域関連付けがあるプリンシパルはすべての領域にアクセスできます。'*' 領域メンバシップを使用するのは、セキュリティ上の意味合いが完全に分かっている場合のみにしてください。こういうことはまれにしかありません。

セクション : IPAddWhitelist

このセクションは、ターゲット ノードへの接続が許可されている IP アドレスのリストを定義します。

各エントリの最初の属性と値のペアは、キーワード 'ipaddress' でなければなりません。

属性 : 'ipaddress'

この文字列は、明示的な IP アドレス、または着信 IP アドレスに対してパターン照合を行う正規表現を定義します。

属性 : 'enabled'

共通属性で説明したとおりです。

属性 : 'type'

このホワイトリスト エントリのタイプを定義します。値は 'normal' または 'pattern' を指定できます。

- 'normal' に設定した場合、継続が許可されるためには、IP アドレスが完全に一致する必要があります。
- 'pattern' に設定する場合、継続を許可されるためには、IP アドレスはパターン一致の必要があります。

server : ENC ゲートウェイ サーバのステータスを表示します

このコマンドは、ENC ゲートウェイ サーバのステータスを表示します。以下を表示するのにも使用されます。

- ゲートウェイ マネージャに登録してあるクライアントとサーバのリスト。
- ゲートウェイ ルータが現在処理している接続のリスト。
- ENC トポロジおよびその他のオプション。

このコマンドは、出力をフィルタする、またはファイルへ送信するためのオプションも提供します。

構文

`Encutilcmd server` [クエリ オプション] [引数] [-host <ホスト名>] [-port <n>] [-v] [-dump <ファイル>]

クエリ オプション

`-client` [[-fqdn <ホスト名>] [-pattern]]

サーバに登録済みのクライアントのリストをクエリします。

`-connection`

ルータにアクティブな ENC 接続のリストをクエリします。

`-general`

サーバにステータスをクエリします。

`-router`

サーバに登録済みのゲートウェイ ルータのリストをクエリします。

`-server`

ENC ゲートウェイ マネージャに登録済みのサーバのリストをクエリします。

`-topology`

ENC ゲートウェイ マネージャに ENC ネットワーク トポロジをクエリします。

引数

-dump <ファイル名>

コマンド出力を XML ファイルに書き込みます。これは、Web ブラウザまたはテキスト エディタに表示したり、他のプログラムで処理したりできます。

-fqdn <ホスト名>

-client からの出力をフィルタするためのホスト名またはパターンを指定します。

注： -pattern を指定すると、-fqdn の値はパターンかホスト名になります。

-host <ホスト名>

クエリ対象のゲートウェイ サーバの完全修飾ドメイン名を指定します。

デフォルト： ローカル ホスト

-pattern

-fqdn に続く文字列を、クライアントのリストと照合される正規表現として指定します。

デフォルト： fqdn は、単一のコンピュータと一致します。

注： 正規表現の構文は、Perl 標準に従います。

-port <n>

ターゲット マシン上のサーバのポート番号を指定します。

デフォルト： 443

-v

可能であれば詳細な出力を指定します。

各項目は以下のとおりです。

-client

このオプションは、指定したサーバに登録してある ENC クライアント (encClient.exe) のリストを取得します。

ターゲットサーバが ENC マネージャの場合は、すべてのクライアントが返され、ターゲットサーバが ENC サーバの場合は、そのサーバに登録されているクライアントのみが返されます。

注：ルータは何も返しません。

-dump 引数を使用してファイルへ出力を送信するか、パターン照合を使用して出力をフィルタできます。

クライアントごとに、出力リストには以下の情報が一覧表示されます。

- 完全修飾ドメイン名
- ホスト UUID
- ENC 仮想アドレス
- Time zone

例：クライアントをすべて一覧表示

- ローカルホストで動作中の ENC サーバ上のすべてのクライアントが一覧表示されます。

```
encutilcmd server -client
```

- mymgr マシンで動作中の ENC サーバ上のすべてのクライアントが一覧表示されます。

```
encutilcmd server -client -host mymgr
```

- fred.com ドメインに存在する mymgr マシンで動作中の ENC サーバ上のすべてのクライアントが一覧表示されます。

```
encutilcmd server -client -host mymgr -fqdn .*%.fred%.com -pattern
```

- host1.fred.com で動作中の ENC クライアントに関する情報が表示されます。

```
encutilcmd server -client -host mymgr -fqdn host1.fred.com
```

-connection

ゲートウェイ ルータにアクティブな接続のリストをクエリします。
接続ごとに、以下が表示されます。

- 接続を行ったホスト。
- 接続を承認したホスト。

ルータは、これらのホスト間でデータを送信するので、ホストごとに以下が表示されます。

- 本当の IP アドレス。
- そのサーバが認証に使用する証明書。ホストの完全修飾ドメイン名を示す証明書の説明。

-general

このオプションは、サーバの一般情報を表示します。クエリが指定されていない場合は、このオプションがデフォルトのクエリになります。

一般情報には、以下のものが含まれます。

- サーバタイプ (マネージャ、サーバ、ルータ、またはすべて)
- バージョン ID
- サーバが実行されている期間。
- ENC 接続用に開かれているポート番号。
- それが登録されている ENC サーバの完全修飾ドメイン名。
(ENC サーバまたはマネージャ)
- それに登録されているサーバの数。
- 指定されたホストが ENC ゲートウェイの場合、仮想 ENC アドレスを割り当てるのに使用するアドレス範囲。 マネージャ。

例 : サーバの一般情報の表示

- ローカル ホスト上のサーバの一般情報が表示されます。

```
encutilcmd server
```

- myhost.xyz.com というホスト上のサーバの一般情報が表示されます。

```
encutilcmd server -general -host myhost.xyz.com
```

-router

ターゲット サーバに登録されているゲートウェイ ルータのリストを表示します。

ルータごとに、以下が表示されます。

- ルータがマネージャに対して自分自身を認証するために使用する証明書の URL。
- サーバタイプ (サーバ、ルータ、または両方)
- クライアント接続用に開かれているポート番号。
- バージョン ID

以下の例は、mymgr.xyz.com に登録されたルータを示します。

```
Encutilcmd server -router -host mymgr.xyz.com
```

-server

ターゲット サーバに登録されているゲートウェイ サーバのリストを表示します。このオプションがゲートウェイ マネージャに使用されると、すべてのサーバが表示されます。ゲートウェイ サーバに使用されると、そのサーバに登録されているすべてのルータが表示されます。表示される情報は、**-router** オプションのものと同じです。

以下の例は、**mymgr.xyz.com** に登録されたサーバを示します。

```
Encutilcmd server -server -host mymgr.xyz.com
```

-topology

このオプションは、**ENC** ネットワークのトポロジを示します。これには、ゲートウェイ マネージャに続いて、サーバおよびルータのインデントされたリストが表示されます。

サーバごとに、登録対象のサーバが以下のように表示されます。

マネージャ

Server1 (このサーバはマネージャに登録されます)

Server2 (このサーバもマネージャに登録されます)

Router1 (このルータは **Server2** に登録されます)

Router2

Server3

Router3

Router4 (このルータはマネージャに登録されます)

以下の例は、**ENC** ゲートウェイ マネージャ **mymgr.xyz.com** のトポロジを示します。

```
Encutilcmd server -topology -host mymgr.xyz.com
```