

ISE の外部 TACACSサーバを設定し、解決して下さい

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[ISE の設定](#)

[ACS の設定](#)

[確認](#)

[トラブルシューティング](#)

概要

この資料はプロキシとして識別 サービス Engine (ISE) を使用して配備の外部 TACACS+ サーバを利用するために機能を説明していたものです。

前提条件

要件

- ISE のデバイス 管理の基本的な知識。
- この文書は識別 サービス エンジン verison のあらゆるバージョンで適当な識別 サービス エンジン バージョン 2.0 に高くより 2.0 基づいています。

使用するコンポーネント

注: この資料の ACS へのどの参照でもあらゆる外部 TACACS+ サーバへの参照であるために interpreted できます。ただし、ACS の設定および他のどの TACACSサーバのも設定は変わるかもしれません。

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

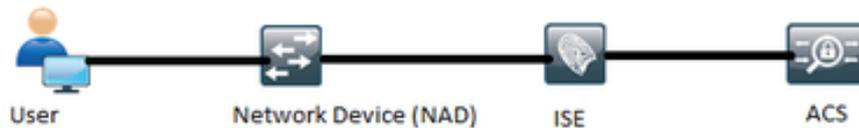
- 識別 サービス エンジン 2.0
- アクセスコントロールシステム (ACS) 5.7

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。ネットワークがライブである場合、あらゆるコンフィギュレーション変更の潜在的影響を理解することを確かめて下さい。

設定

このセクションは ACS にプロキシ TACACS+ 要求に ISE の設定を助けます。

ネットワーク図



ISE の設定

1. 複数の外部 TACACSサーバは ISE で設定し、ユーザを認証するのに使用することができます。ISE の外部 TACACS+ サーバを、ナビゲート作業センター > デバイス Administration > ネットワークリソース > TACACS 外部サーバに設定するため。外部サーバ 詳細の詳細を『Add』をクリックし、記入して下さい。

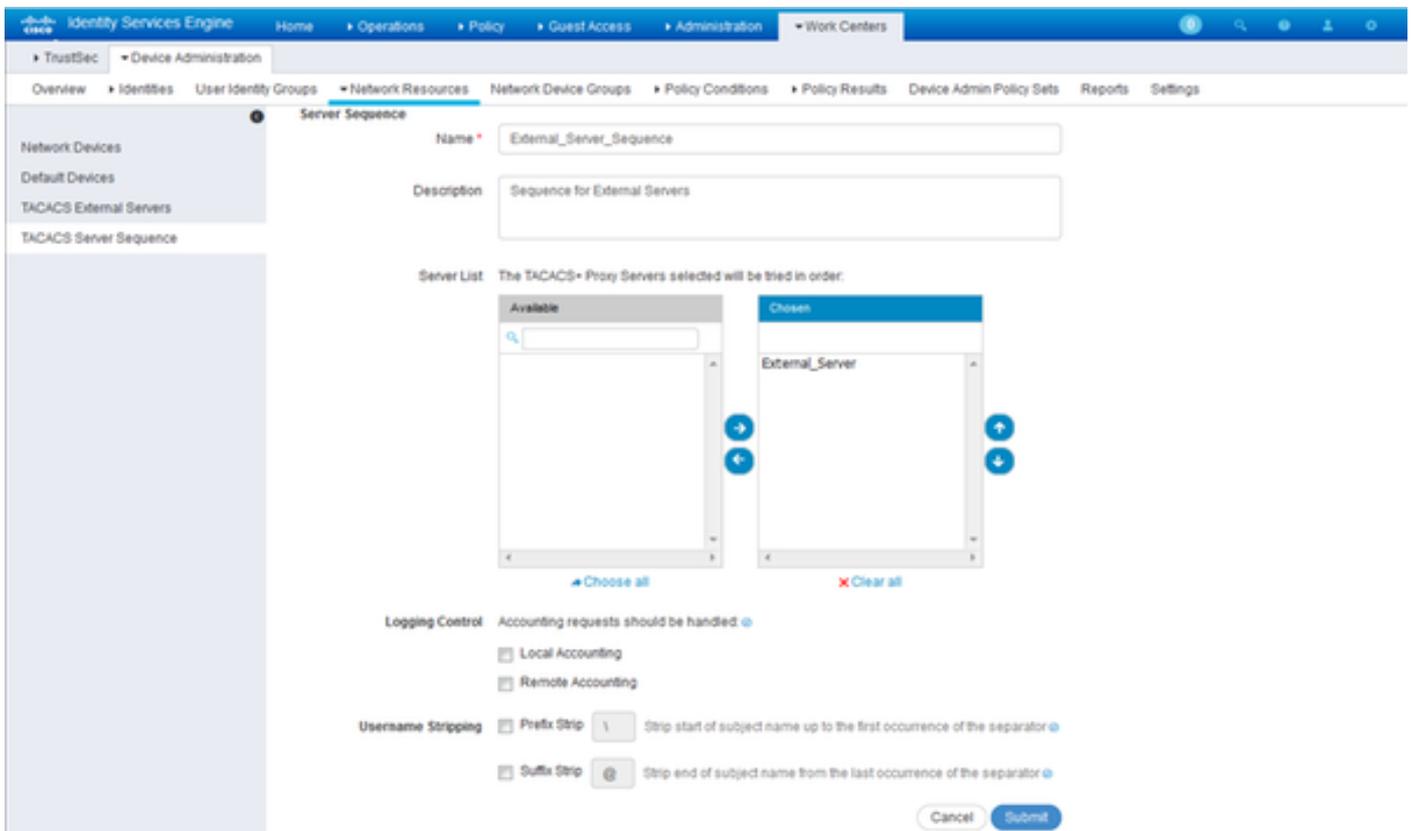
The screenshot shows the ISE Administration console with the following configuration details for an External TACACS Server:

- Name: External_Server
- Description: External TACACS Server
- Host IP: 10.127.196.237
- Connection Port: 49 (1-65,535)
- Timeout: 20 Seconds (1-999)
- Shared Secret: ***** (with Show Secret button)
- Use Single Connect:

Buttons: Cancel, Save

このセクションで提供される共有秘密は ACS で使用される同じシークレットである必要があります。

2. 設定される外部 TACACSサーバを利用するためにそれはポリシー セットで使用されるべき TACACSサーバ シーケンスに追加する必要があります。作業センター > デバイス Administration > ネットワークリソース > TACACSサーバ シーケンスに TACACSサーバ シーケンスを、ナビゲート設定するために命令します。『Add』をクリックし、詳細を記入し、必要そのシーケンスで使用するためにであるサーバを選択して下さい。

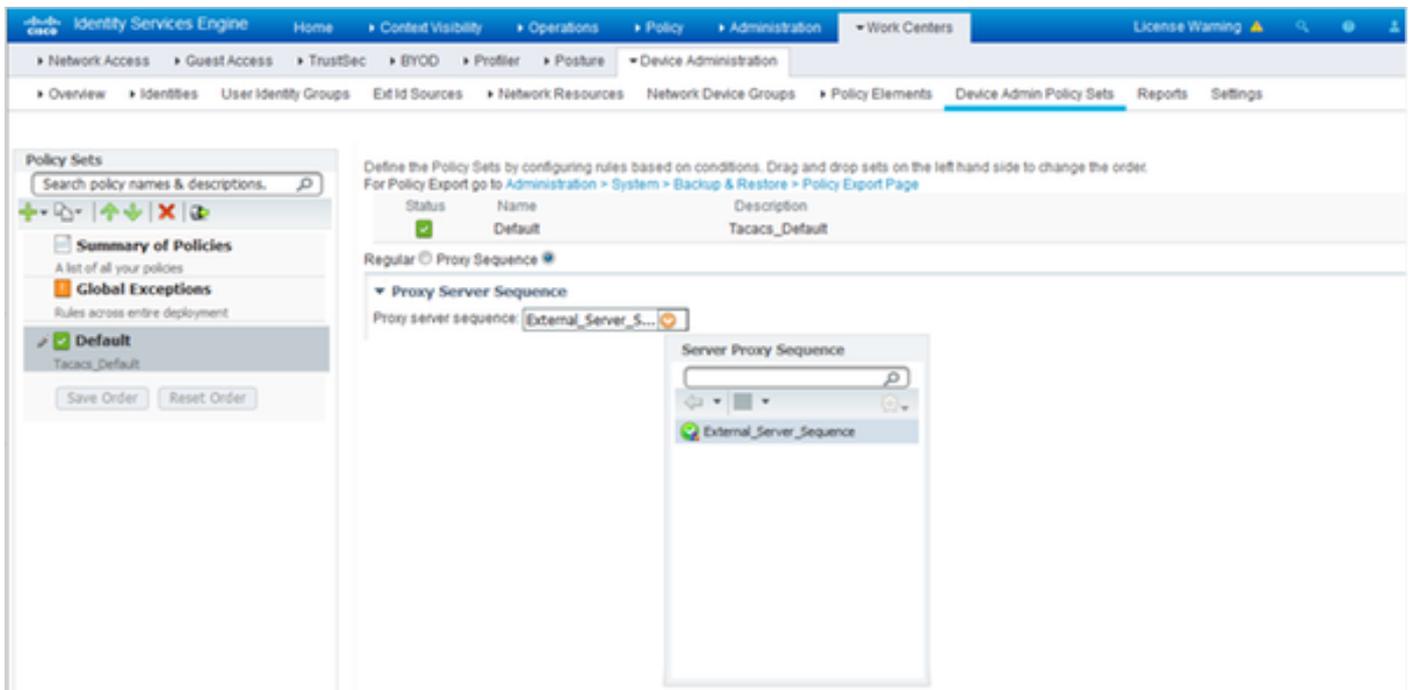


サーバシーケンスに加えて、2つのその他のオプションは提供されました。記録制御およびユーザ名除去。

記録制御は ISE でログにオプションにアカウントिंग要求をローカルで与えるか、または認証を同様に処理する外部サーバにアカウントिंग要求を記録します。

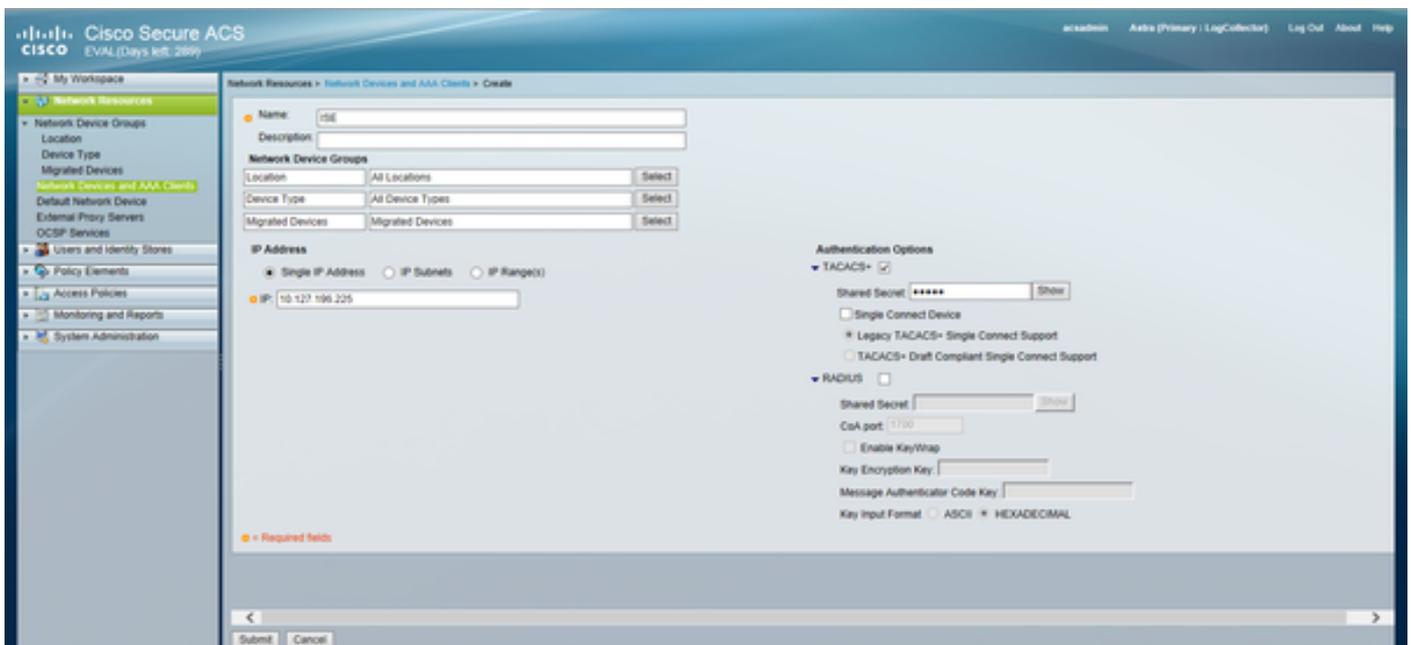
デリミタを specifying によってユーザ名除去が外部 TACACSサーバへ要求を転送する前にプレフィックスかサフィックスを除去するのに使用されています。

3. 設定される外部 TACACSサーバシーケンスを利用するためにポリシーセットは作成されるシーケンスを使用するために設定する必要があります。ポリシーセットを作業センター > デバイス Administration > デバイス Admin ポリシーセットに外部サーバシーケンスを、ナビゲート使用するために設定するため > [ポリシーセットを選択して下さい]。プロキシシーケンスを言う Toggleオプション・ボタン。作成される外部サーバシーケンスを選択して下さい。

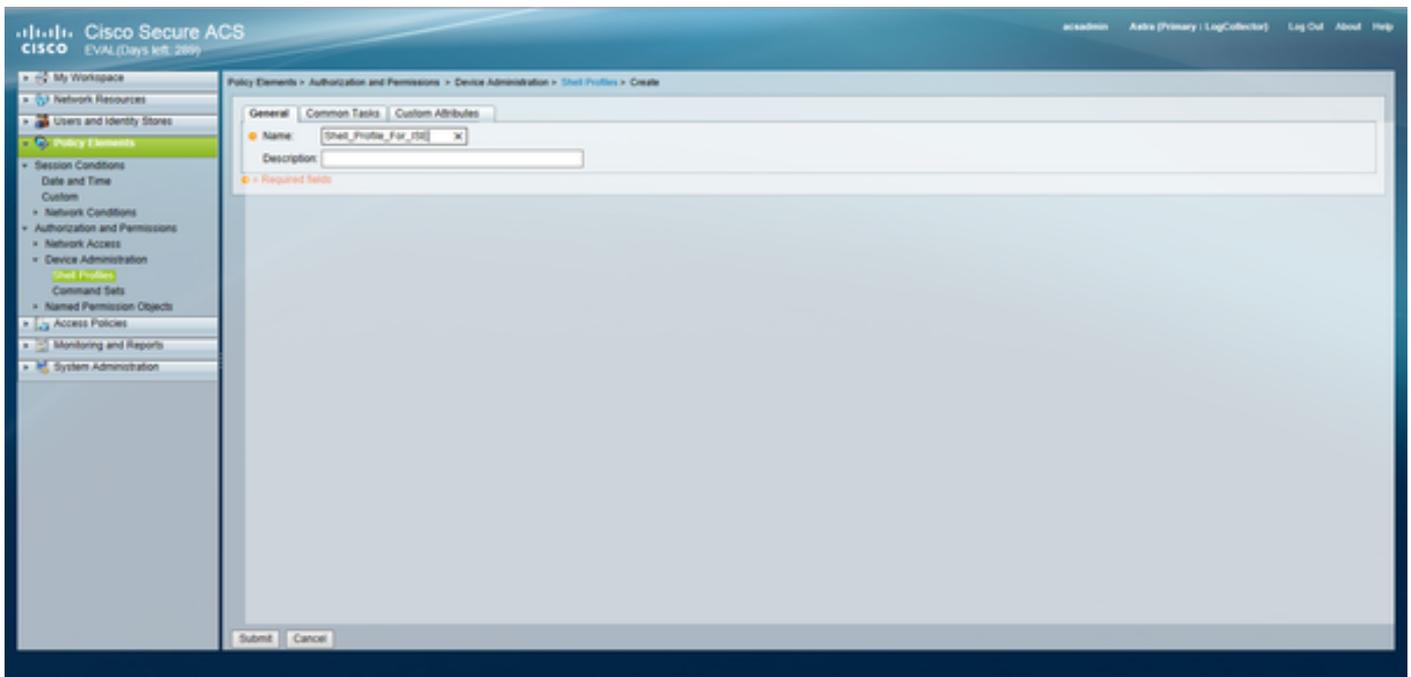


ACS の設定

ACS に関しては、ISE は TACACS 要求を送信するありふれたネットワークデバイスです。ISE をネットワークリソース > ネットワークデバイスおよび AAA クライアントに ACS のネットワークデバイス、ナビゲートで設定するため。ISE で設定されると同じ共有秘密を使用して ISE サーバの詳細を『Create』をクリックし、記入して下さい。



ある ACS、シェル プロファイルおよびコマンド セットのデバイス 管理パラメータを設定して下さい。シェル プロファイルを設定するために、ポリシー要素 > 許可および権限 > デバイス Administration > シェルにプロファイル ナビゲートして下さい。要件によって名前、一般的なタスクおよびカスタム属性を『Create』をクリックし、設定して下さい。



conofigure コマンド セットはポリシー要素 > 許可に、ナビゲートし、権限 > デバイス Administration > コマンドは設定します。要件によって詳細を『Create』をクリックし、記入して下さい。

General
Name: Status: 

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions
 Protocol:

Results
Service:

要件によってサービス セレクション ルールで選択されるアクセス サービスを設定して下さい。アクセスを設定するために識別ストアが認証に選択することができる使用する必要があるアクセスポリシー > アクセス サービス > Default デバイス Admin > 識別にルールを、ナビゲート保守して下さい。承認規則はアクセスポリシー > アクセス サービス > Default デバイス Admin > 許可へのナビゲートによって設定することができます。

注: 特定のデバイスのための承認ポリシーおよびシエル profiles の設定は変わるかもしれ、それはこの資料の範囲外にあります。

検証

設定がきちんと機能することを確認するのにこのセクションを使用して下さい。

確認は ISE および ACS 両方ですることができます。ISE の設定のどの誤りでもか ACS は認証失敗という結果に終わります。ACS は ACS サーバに出入して認証および認証要求を処理するプライマリ サーバ、ISE 耐えます要求に対する責任におよびプロキシとして機能するためにです。パケットが両方のサーバを通過して通過するので、認証または認証要求の確認は両方のサーバですること

とができます。

ネットワークデバイスは TACACSサーバおよび ACS で ISE で設定されます。それ故に要求は ISE に最初に達し、要求が外部サーバに転送される必要があるかどうか設定されるルールに基づいて ISE は決定します。これはライブ TACACS でログオンします ISE を確認することができます。

ライブを表示するためにログオンします **オペレーション > TACACS** に ISE を、ナビゲート > **ライブ ログ**。ライブ レポートはこのページで見られ、特定の要求の詳細は対象であるその特定の要求に関して拡大鏡アイコンをクリックしてチェックすることができます。

Steps

- 13020 Get TACACS+ default network device setting
- 13013 Received TACACS+ Authentication START Request
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Network Access.Protocol
- 15006 Matched Default Rule
- 13064 TACACS proxy received incoming request for forwarding.
- 13065 TACACS proxy received valid incoming authentication request.
- 13063 Start forwarding request to remote TACACS server.
- 13074 Finished to process TACACS Proxy request.
- 13020 Get TACACS+ default network device setting
- 13014 Received TACACS+ Authentication CONTINUE Request
- 13064 TACACS proxy received incoming request for forwarding.
- 13065 TACACS proxy received valid incoming authentication request.
- 13071 Continue flow (seq_no > 1).
- 13063 Start forwarding request to remote TACACS server.
- 13074 Finished to process TACACS Proxy request.

ACS の認証レポートを表示するために、**モニタリングおよびレポート > 起動モニタリング**にナビゲートし、**ビューア > モニタリング**を報告し、**> レポート > AAAプロトコル > TACACS認証**を報告します。ISE のように、特定の要求の詳細は対象であるその特定の要求に関して拡大鏡アイコンをクリックしてチェックすることができます

Steps
Received TACACS+ Authentication START Request
Evaluating Service Selection Policy
Matched rule
Selected Access Service - Default Device Admin
Evaluating Identity Policy
Matched Default Rule
Selected Identity Store - Internal Users
Looking up User in Internal Users IDStore - external
Found User in Internal Users IDStore
TACACS+ will use the password prompt from global TACACS+ configuration.
Returned TACACS+ Authentication Reply
Received TACACS+ Authentication CONTINUE Request
Using previously selected Access Service
Evaluating Identity Policy
Matched Default Rule
Selected Identity Store - Internal Users
Looking up User in Internal Users IDStore - external
Found User in Internal Users IDStore
Authentication Passed
Evaluating Group Mapping Policy
Evaluating Exception Authorization Policy
No rule was matched
Evaluating Authorization Policy
Matched Default Rule
Returned TACACS+ Authentication Reply

トラブルシューティング

このセクションは設定をトラブルシューティングするのに使用できる情報を提供します

1. ISE のレポートの詳細が図で表示されるエラーメッセージを表示する場合 ISE か Netowrk デバイス (NAD) で設定される無効な共有秘密を示します。

Message Text

TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets

2. ISE の要求のための認証レポートがなければが、ネットワークデバイスへのエンドユーザへのアクセスが拒否されれば、これは通常複数の事柄を示します。

- 要求自体は範囲を ISE サーバしませんでした。
- デバイス管理外的人格が ISE でディセーブルにされる場合、ISE へのどの TACACS+ 要求でも無言で廃棄されます。同じを示すログはレポートかライブ ログで示されません。これを、ナビゲート **Administration > システム > 配備**に確認するため > [ノードを選択して下さい]。図に示すように一般の **Settings** タブの下で「**イネーブル デバイス Admin サービス**」チェックボックスを『Edit』をクリックし、注意して下さい。チェックボックスは ISE で動作するためにデバイス 管理があるように確認される必要があること。

Personas

Administration Role **PRIMARY**

Monitoring Role PRIMARY Other Monitoring Node

Policy Service

Enable Session Services Include Node in Node Group None

Enable Profiling Service

Enable Threat Centric NAC Service

Enable SXP Service Use Interface GigabitEthernet 0

Enable Device Admin Service

Enable Passive Identity Service

pxGrid

- デバイス管理ライセンスが期限切れのない場合、すべての TACACS+ 要求は無言で廃棄されます。ログは同じのための GUI で示されていません。Administration > システムに > ナビゲートして デバイス 管理ライセンスをチェックするために認可します。

Licenses How do I register, modify or lookup my licenses?

License File	Quantity	Term	Expiration Date
EVALUATION.lic			
Base	100	90 days	22-Jan-2017 (43 days remaining)
Plus	100	90 days	22-Jan-2017 (43 days remaining)
Apex	100	90 days	22-Jan-2017 (43 days remaining)
Wired	100	90 days	22-Jan-2017 (43 days remaining)
Device Admin	Uncounted	90 days	22-Jan-2017 (43 days remaining)

- ネットワークデバイスが設定されないか、または間違ったネットワークデバイス IP が ISE で設定されれば、ISE は無言でパケットを廃棄します。無応答はクライアントに送られ、ログは GUI で示されていません。これは要求は unknown ネットワークデバイスか AAA クライアントから入ったこと知らせる ACS のそれと比較されたとき TACACS+ のための ISE の動作の変更です。
- 要求は ACS に達しましたが、応答は ISE に戻りませんでした。このシナリオは図に示すように ACS のレポートからチェックすることができます。これは ISE のために設定される ACS または ACS のために設定される ISE の無効な共有秘密が理由で通常そうなったものです。

Steps

Message

Received TACACS+ Authentication START Request
Invalid TACACS+ request packet - possibly mismatched Shared Secrets

- 応答は ISE が設定されなくてか、もまたは ISE のマネージメントインターフェイスの IP アドレスがネットワーク デバイスの設定の ACS で設定されない返されません。そのような scenario では、図のメッセージは ACS で監視することができます。

Steps

Message

Received TACACS+ packet from unknown Network Device or AAA Client

- ISE の No レポートが見られれば、ユーザが拒否されれば見られ、認証の成功レポートが

ACS で、とてもよくネットワークの問題である可能性があります。これは必要なフィルターとの ISE のパケットキャプチャによって確認することができます。ISE のパケットキャプチャを、ナビゲートはオペレーションに集めるために >> 診察道具 > 汎用ツール > TCP ダンプ 解決します。

TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status  Stopped

Host Name

Network Interface

Promiscuous Mode On Off

Filter

Example: 'ip host helios and not iceburg'

Format

Dump File Last created on Fri Dec 09 20:51:18 IST 2016
File size: 9,606 bytes
Format: Raw Packet Data
Host Name: tornado
Network Interface: GigabitEthernet 0
Promiscuous Mode: On

3. レポートが ISE でない ACS で見られる場合があるが、場合要求が ISE のまたは ACS のパケットキャプチャによって識別することができるネットワーク上の問題が理由で Detailed レポートに基づいていた解決することができる ISE のポリシー セットのミスコンフィギュレーションが理由で ACS に達しなかったことをどちらか意味しますできました。

4. レポートが ISE および ACS 両方で見られればが、ユーザがそれでもアクセスを拒否されれば、それはより頻繁に ACS の Detailed レポートに基づいていた解決することができる ACS のアクセスポリシー設定の問題です。また、ISE からの Network デバイスへのリターントラフィックは許可する必要があります。