ISE との ASA バージョン 9.2.1 VPN ポスチャの 設定例

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 背景説明 設定 <u>ネットワーク図とトラフィック フロー</u> 設定 平均応答時間 ISE 定期的再評価 確認 トラブルシュート ISE でのデバッグ ASA でのデバッグ エージェントのデバッグ NAC エージェント ポスチャの障害 関連情報

概要

このドキュメントでは、インライン ポスチャ ノード(IPN)を使用せずに Cisco Identity Services Engine(ISE)に対して VPN ユーザをポスチャするように Cisco 適応型セキュリティ アプライアンス(ASA)バージョン 9.2.1 を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA CLI 設定およびセキュア ソケット レイヤ(SSL)VPN 設定に関する基本的な知識
- ASA でのリモート アクセス VPN 設定に関する基本的な知識
- ISE サービスとポスチャ サービスに関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco ASA ソフトウェア バージョン 9.2.1 以降
- Cisco AnyConnect セキュア モビリティ クライアント バージョン 3.1 を備えた Microsoft Windows Version 7
- パッチ 5 以降が適用された Cisco ISE バージョン 1.2

背景説明

Cisco ASA バージョン 9.2.1 は、RADIUS 認可変更(CoA)(RFC 5176)をサポートしています 。これにより、IPN を使用せずに Cisco ISE に対して VPN ユーザをポスチャすることが可能にな ります。VPN ユーザがログインした後、ASA は Web トラフィックを ISE にリダイレクトします 。そこでユーザは、ネットワーク アドミッション コントロール(NAC)エージェントまたは Web エージェントでプロビジョニングされます。エージェントは、オペレーティング システム (OS)、パッチ、ウイルス対策、サービス、アプリケーション、またはレジストリ ルールなど の一連の設定済みポスチャ ルールと照らしてコンプライアンスを確認するために、ユーザ マシン で特定のチェックを実行します。

その後、ポスチャ検証の結果が ISE に送信されます。マシンが準拠していると見なされた場合、 ISE は認証ポリシーの新しいセットを使用して ASA に RADIUS CoA を送信することができます 。ポスチャ検証と CoA に成功すると、ユーザは内部リソースへのアクセスが許可されます。

設定

ネットワーク図とトラフィック フロー



次のネットワーク図にトラフィック フローを示します。

- 1. リモート ユーザが Cisco AnyConnect を使用して ASA に VPN アクセスします。
- 2. ASA はそのユーザの RADIUS アクセス要求を ISE に送信します。
- 3. この要求に対しては、ISE で ASA92-posture という名前のポリシーがヒットします。その結果、ASA92-posture 認証プロファイルが返されます。ISE は、次の 2 つの Cisco Attribute-Value ペアを使用して、RADIUS Access-Accept を送信します。

url-redirect-acl=redirect 。これは、ASA でローカルに定義されたアクセス コントロール リ スト(ACL)の名前であり、リダイレクトするトラフィックを決定します。

url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=xx&action=cpp 。これは、リモート ユーザのリダイレクト先となる URL です。ヒント:VPNクライアントに 割り当てられたドメインネームシステム(DNS)サーバは、リダイレクトURLで返される完全 修飾ドメイン名(FQDN)を解決できる必要があります。VPN フィルタがトンネル グループ レベルでアクセスを制限するように設定されている場合は、クライアント プールが設定済 みポート(この例では TCP 8443)上で ISE サーバにアクセスできることを確認します。 4. ASA は RADIUS Accounting-Request 開始パケットを送信し、応答を受信します。これは、

4. ASA は RADIOS Accounting-Request 開始パアンドを返信し、応告を受信しより。これは、 ISE へのセッションに関するすべての詳細を送信するために必要です。詳細には、 session_id、VPN クライアントの外部 IP アドレス、および ASA の IP アドレスが含まれま す。ISE は session_id を使用してセッションを識別します。ASA はさらに、定期中間アカ ウント情報を送信します。この情報で最も重要な属性は、ASA によってクライアントに割 り当てられている IP を持つ Framed-IP-Address です(この例では 10.10.10.10)。

- 5. VPN ユーザからのトラフィックが、ローカルに定義された ACL(リダイレクト)と一致す る場合は、https://ise2.test-cisco.com:8443 にリダイレクトされます。設定によっては、ISE は NAC Agent または Web エージェントをプロビジョニングします。
- エージェントは、クライアント マシンにインストールされると、自動的に特定のチェック を実行します。この例では、c:\test.txt ファイルを探します。エージェントはまた、ISE にポ スチャ レポートを送信します。このレポートには、ISE にアクセスできるようにするために 、SWISS プロトコルおよびポート TCP/UDP 8905 を使用した複数の交換を含めることがで きます。
- 7. ISE がエージェントからポスチャ レポートを受信すると、認証ルールをもう一度処理します 。今回は、ポスチャの結果は既知であるため、別のルールがヒットします。これにより、次 のように RADIUS CoA のパケットが送信されます。

ユーザが準拠している場合は、フル アクセスを許可するダウンロード可能 ACL(DACL)名 が送信されます(AuthZ ルール ASA92 準拠)。

ユーザが準拠していない場合は、制限付きアクセスを許可する DACL 名が送信されます (AuthZ ルール ASA92 非準拠)。**注**:RADIUS CoAは常に確認されます。つまり、ASAは確 認のためにISEに応答を送信します。

- 8. ASA がリダイレクションを削除します。DACL がキャッシュされていない場合は、ISE から ダウンロードするために Access-Request を送信する必要があります。特定の DACL が VPN セッションに付加されます。
- 9. VPN ユーザがもう一度 Web ページにアクセスしようとすると、ASA にインストールされて いる DACL によって許可されたすべてのリソースにアクセスできます。 ユーザが準拠していない場合は、制限付きアクセスのみが付与されます。
 注:このフローモデルは、RADIUS CoAを使用するほとんどのシナリオとは異なります。有 線/無線 802.1x 認証の場合は、RADIUS CoA には属性は含まれていません。これにより、す べての属性(DACL など)が付加される 2 番目の認証のみがトリガーされます。ASA VPN ポスチャの場合は、2 番目の認証は行われません。すべての属性が RADIUS CoA で返され ます。VPN セッションがアクティブであるため、ほとんどの VPN ユーザ設定が変更不可に なっています。

設定

ここでは、ASA および ISE を設定します。

平均応答時間

Cisco AnyConnect アクセスの基本的な ASA 設定は次のとおりです。

ip local pool **POOL 10.10.10.10.10.10.100** mask 255.255.255.0

interface GigabitEthernet0/0
nameif outside
security-level 0

```
ip address xxxx 255.255.255.0
1
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.111.10 255.255.255.0
aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.48.66.74
key cisco
webvpn
enable outside
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
anyconnect enable
tunnel-group-list enable
group-policy GP-SSL internal
group-policy GP-SSL attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless
tunnel-group RA type remote-access
tunnel-group RA general-attributes
address-pool POOL
authentication-server-group ISE
default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
group-alias RA enable
```

ISE ポスチャと ASA を統合する場合は、必ず次の操作を実行します。

- CoA を受け入れるため、認証、認可、およびアカウンティング(AAA)サーバを動的認証に 設定します。
- VPN セッションの詳細情報を ISE へ送信できるように、アカウンティングをトンネル グル ープとして設定します。
- ユーザに割り当てられた IP アドレスを送信する中間アカウンティングを設定し、定期的に ISE でのセッション ステータスを更新します。

DNS と ISE トラフィックを許可するかどうかを決定するリダイレクト ACL を設定します。
 他の HTTP トラフィックはすべて、ポスチャのため ISE にリダイレクトされます。
 次に設定の例を示します。

```
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.48.66.74
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
aaa-server ISE protocol radius
```

```
authorize-only
interim-accounting-update periodic 1
dynamic-authorization
aaa-server ISE (inside) host 10.48.66.74
key cisco
```

tunnel-group RA general-attributes address-pool POOL authentication-server-group ISE accounting-server-group ISE default-group-policy GP-SSL

ISE

ISE を設定するには、次の手順を実行します。

1. [Administration] > [Network Resources] > [Network Devices] に移動し、ASA をネットワーク デバイスとして追加します。

alaha ang ang ang ang ang ang ang ang ang an	
cisco Identity Services Engine	
🔆 System 🦉 Identity Management 📷 N	letwork Resources 🛛 🛃 Web Portal Management 🛛 🖓 Feed Service
Network Devices Network Device Groups Ext	ernal RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers
Network Devices	Network Devices List > New Network Device Network Devices * Name ASA Description * IP Address: 192.168.111.10 / 32 Model Name * Software Version * * Network Device Group Location All Locations © Set To Default Device Type All Device Types © Set To Default Set To Default
	Enable Authentication Settings
	* Shared Secret Show

2. [Policy] > [Results] > [Authorization] > [Downloadable ACL] に移動し、フル アクセスを許可 するように DACL を設定します。ACL のデフォルト設定では、ISE 上のすべての IP トラフ ィックを許可します。

cisco Identity Services Engine	▲ Home Operations ▼ Policy ▼ Administration ▼
Authentication 👩 Authorization 🔀 Dictionaries Conditions Results	Profiling 👩 Posture 🔂 Client Provisioning 📄 Security Group Access
Results Image: Security Group Access	Downloadable ACL List > PERMIT_ALL_TRAFFIC Downloadable ACL * Name PERMIT_ALL_TRAFFIC Description Allow all Traffic * DACL Content 1 permit ip any any 2 3 4 5 6 7 9 10

- 3. 制限付きアクセスを提供する同様の ACL を設定します(非準拠ユーザ向け)。
- 4. [Policy] > [Results] > [Authorization] > [Authorization Profiles] に移動し、ASA92-posture と いう許可プロファイルを設定します。これが、ポスチャのためにユーザをリダイレクトしま す。[Web Redirection] チェック ボックスをオンにし、ドロップダウン リストから [Client Provisioning] を選択し、[ACL] フィールドに redirect と表示されることを確認します。

cisco Identity Services Engine	Administration ▼ Policy ▼
Authentication Authorization Conditions Results Dictionaries Conditions Results Results	Home Operations Policy Administration Profiling Posture Client Provisioning Security Group Access Authorization Profiles > ASA92-posture Authorization Profile *Name ASA92:posture Description *Access Type ACCESS_ACCEPT Service Template * Common Tasks
Security Group Access	 Voice Domain Permission Web Redirection (CWA, DRW, MDM, NSP, CPP) Client Provisioning (Posture) ACL redirect Static IP/Host name

5. ASA92-compliant という名前の認証プロファイルを設定します。このプロファイルが、 PERMIT_ALL_TRAFFIC という DACL だけを返すようにします。これにより、準拠するユ ーザにはフル アクセスが提供されます。

cisco Identity Services Engine	Administration ▼
Authentication Authorization I Dictionaries Conditions Results	Profiling 👩 Posture 🔊 Client Provisioning 🚊 Security Group Access
Results	Authorization Profiles > ASA92-compliant Authorization Profile * Name ASA92-compliant Description * Access Type ACCESS_ACCEPT v Service Template
Posture Client Provisioning	▼ Common Tasks
 Security Group Access 	DACL Name PERMIT_ALL_TRAFFIC -

- 6. ASA92-noncompliant という名前の同様の認証プロファイルを設定します。このプロファイ ルは、制限付きアクセスを提供する DACL を返すようにします(非準拠ユーザ向け)。
- 7. [Policy] > [Authorization] に移動し、認証ルールを設定します。

ポスチャの結果が準拠する場合にフル アクセスを許可するルールを作成します。この結果が ASA92-compliant という認証ポリシーです。

ポスチャの結果が準拠しない場合に制限付きアクセスを許可するルールを作成します。この 結果が ASA92-noncompliant という認証ポリシーです。

上記の2つのルールのどちらにも該当しなかった場合にデフォルト ルールが ASA92posture を返すようにします。これにより ASA でリダイレクションが強制的に実行されます

0						
1	2	ASA92 complaint	if	Session:PostureStatus EQUALS Compliant	then	ASA92-compliant
1	×	ASA92 non complaint	if	Session:PostureStatus EQUALS NonCompliant	then	ASA92-noncompliant
1	×	ASA92 redirect	if	Radius:NAS-IP-Address EQUALS 192.168.111.10	then	ASA92-posture

8. デフォルトの認証ルールは、内部 ID ストア内でユーザ名を確認します。この動作(たとえ ば、Active Directory(AD)での確認など)を変更する必要がある場合は、[Policy] > [Authentication] に移動し、変更を行います。

aliali cisco	Identity Services Engine		🏠 Home	Operations 🔻	Policy 🔻	Administration	•	
AL	uthentication 🧕 🧕 Authorizati	on 🔀 Profiling) 💽 Post	ure 👩 Clien	t Provisioning	📑 Security	Group Access	🐥 Pol
Auther	ntication Policy							
Define the Policy Typ	e Authentication Policy by selecti pe O Simple	ng the protocols that d	ISE should us	e to communicate	with the netwo	ork devices, and th	e identity sources	that it sh
	MAB	: If Wired_MAB Wireless_M/	DR AB			Allow Protocols :	Default Network	Access
	Default	:use Interna	al Endpoints					
	Dot1X	: If Wired_802.1 Wireless_80	X OR 2.1X			Allow Protocols :	Default Network	Access
	🗹 Default	:use Interna	al Users					
6	Default Rule (If no match)	: Allow Protocols	Default Netwo	ork Access	а	nd use : Internal U	Jsers	

9. [Policy] > [Client Provisioning] に移動し、プロビジョニング ルールを設定します。これらは 、プロビジョニングされるエージェントのタイプを決定するルールです。この例では、単純 なルールが 1 つだけ存在し、ISE がすべての Microsoft Windows システムで NAC Agent を 選択します。

cisco Identity S	ervices Engine	🟠 Hon	ne Operations • Policy	▼ Administration ▼		
🛓 Authentication	 Authorization 	🛃 Profiling 🛛 🕅 P	osture 🔄 Client Provisio	ning 🔄 Security Group Access	🐥 Policy Elements	
Client Provisioning Policy Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation: For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package. For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.						
• Rule !	lame .	Identity Groups	Operating Systems	Other Conditions	Results	
🖌 🖌 ASA92-;	oosture	If Any	and Windows All	and Condition(s)	then NACAgent 4.9.0.1013	

エージェントが ISE 上にない場合はダウンロードできます。

ACAgent 4.9 🗢		Done
Agent Configuration		
Agent:	NACAgent 4.9.0.1013	📀 🗹 Is Upgrade Mandatory
Profile:	Choose a Profile	Agents
Compliance Module:	Choose a Compliance Module	
Agent Customization Package:	Choose a Customization Package	(. •] .
Native Supplicant Co Config Wizard: Choose a Wizard Profile: Choose a	nfiguration Config Wizard O Wizard Profile O	 Clei Download Resource NACAgent 4.9.0.52 NACAgent 4.9.0.1009 NACAgent 4.9.0.1013 WebAgent 4.9.0.24 WebAgent 4.9.0.28 WebAgent 4.9.0.31 WebAgent 4.9.0.1005 WebAgent 4.9.0.1007

- 10. 必要に応じて、[Administration] > [System] > [Settings] > [Proxy] に移動し、ISE のプロキシ を設定できます(インターネット アクセスのための設定)。
- 11. クライアント設定を検証するポスチャ ルールを設定します。以下を確認するルールを設定 できます。

ファイル - 存在、バージョン、日付

レジストリ - キー、値、存在

- アプリケーション プロセス名、実行中、非実行中
- サービス-サービス名、実行中、非実行中
- ウイルス対策 100 を超えるベンダーをサポート、バージョン、定義更新のタイミング

スパイウェア対策 - 100 を超えるベンダーをサポート、バージョン、定義更新のタイミン グ

複合条件 - すべての組み合わせ

カスタム ディクショナリ条件 - ほとんどの ISE ディクショナリの使用状況

12. この例では、単純なファイルの存在チェックを実行します。**c:\test.txt ファイルがクライア ント マシンに存在する場合は、準拠しているため、フル アクセスが許可されます。** [Policy] > [Conditions] > [File Conditions] に移動し、ファイル条件を設定します。

cisco Identity Services Engine	Administration ▼	
Authentication o Authorization	Profiling 👩 Posture 👸 Client Provisioning 📑 Security Group Access	🔒 Policy Elements
Posture	File Conditions List > file_condition * Name file_condition Description * File Path ABSOLUTE_PATH * * File Type FileExistence * * File Operator Exists * * Operating System Windows All \$ Save Reset	Ø

13. [Policy] > [Results] > [Posture] > [Requirements] に移動し、要件を作成します。この要件は 、直前の条件を満たした場合に満たす必要があります。条件を満たさない場合は、修復ア クションが実行されます。多くの種類の修復アクションを使用できますが、この例では最 も単純な方法である特定のメッセージが表示されます。

cisco Identity Services Engine		Administration +		
🛃 Authentication 💿 Authorization 🔀 Profili Dictionaries Conditions Results	ng 🛛 Posture 👦 Client Provision in	ng 📃 Security Group Access	🐥 Policy Elements	
Results	lequirements Name	Operating Systems	Conditions	Remediation Actions
Qu ▼ E ▼ Qu ▼	file_requirement	for Windows All m	et if file_condition	else Message Text Only
Automation Profiling Posture	Any_AV_Installation_Win	for Windows All m	etif ANY_av_win_inst	else Message Text Only
Clevet Provision Actions Clevet Provisionica	Any_AS_Installation_Win	for Windows All m	etif ANY_as_win_inst	n else Message Text Only
 Security Group Access 	Any_AS_Definition_Win	for Windows All m	etif ANY_as_win_def	else AnyASDefRemediationWi n
	Any_AV_Installation_Mac	for Mac OSX m	et if ANY_av_mac_inst	else Message Text Only
	Any_AS_Installation_Mac	for Mac OSX m	etif ANY_as_mac_inst	else Message Text Only
	Any_AS_Definition_Mac	for Mac OSX m	etif ANY_as_mac_def	else Message Text Only

注:通常のシナリオでは、ファイル修復アクションを使用できます(ISEはダウンロード可能なファイルを提供します)。

14. [Policy] > [Posture] に移動し、前の手順で作成した要件(file_requirement)をポスチャ ルールに使用します。唯一のポスチャ ルールは、すべての Microsoft Windows システムが file_requirement を満たすことです。この要件が満たされている場合、ステーションは準拠 しています。要件が満たされていない場合、ステーションは非準拠です。

cisco Identity Serv	vices Engine	🟠 Home Ope	rations • Policy • Administra	tion 🕶	
🛓 Authentication	🧕 Authorization 🛛 🔀	Profiling 🛛 Posture	🛃 Client Provisioning 📑 Ser	curity Group Access 🛛 🐥 Policy	Elements
Posture Policy Define the Posture Policy by	/ configuring rules based	on operating system and/or of	her conditions.		
Status Rule Nar	ne	Identity Groups	Operating Systems	Other Conditions	Requirements
posture		If Any	and Windows All		then file_requirement

定期的再評価

デフォルトでは、ポスチャはワンタイム イベントです。ただし、定期的にユーザの準拠性を確認 し、その結果に基づいてリソースへのアクセスを調整しなければならない場合もあります。この 情報は、SWISS プロトコル(NAC Agent)を介してプッシュされるか、アプリケーション(Web Agent)内にエンコードされています。

次の手順を実行して、ユーザの準拠性を確認します。

1. [Administration] > [Settings] > [Posture] > [Reassessments] に移動し、再評価をグローバル に有効にします(ID グループ設定ごと)。



2. すべての再評価に一致するポスチャ条件を作成します。

cisco Identity Services Engine	A Home Operations	▼ Policy ▼ Administration	V
🛓 Authentication 🛛 🧕 Authorization	🔀 Profiling 👩 Posture 词	Client Provisioning 📃 Security	y Group Access
Dictionaries Conditions Results			
Posture	Dictionary Conditions List > New Dictionary Simple Con * Name reassesment Description * Attribute Session:Agent-Request-Typ Submit Cancel	Pictionary Condition dition * Operator e ♥ Equals	* Value * Value Periodic Reassessment *

3. 最初の評価のみと一致する同様の条件を作成します。

cisco Identity Services Engine	🟠 Home Opera	tions • Policy • Administration •
💄 Authentication 🛛 👩 Authorization	🔀 Profiling 🛛 🧭 Posture	🙀 Client Provisioning 🔄 Security Group Access 🤹 Policy Elements
Dictionaries Conditions Results		
Posture	P Dictionary Conditions List>	New Dictionary Condition Condition
↓ ■ .	Description	
File Condition		
Registry Condition		
Application Condition	* Attribute	* Operator * Value
Service Condition	Session:Agent-Reques	it-Type 📀 🛛 Equals 🔹 🔹 Initial 🔹
E Compound Condition	Submit Cancel	
12 AV Compound Condition		·
AS Compound Condition		
📄 Dictionary Simple Condition		
E Dictionary Compound Condition		

ポスチャ ルールではこの両方の条件を使用できます。最初のルールは最初の評価のみと一致し、 2 番目のルールは後続のすべての評価と一致します。

CISCO Identity Services Engine	🟠 Home Operatio	ns • Policy • Administration •	
💫 Authentication 🛛 🧔 Authorization	Refiling Posture	Client Provisioning 📃 Security Group Access	4 Policy Elements
Posture Policy Define the Posture Policy by configuring rules ba	ised on operating system and/or other	conditions.	
Status Rule Name	Identity Groups	Operating Systems Other Conditions	Requirements
gosture_initial	lí Any	and Windows All initial	then file_requirement
posture_reassessment	if Any	and Windows All reassessment	then file_requirement

確認

次の手順に従って、設定が正しく機能するかどうかを確認します。

- 1. VPN ユーザが ASA に接続します。
- 2. ASA が RADIUS-Request を送信し、url-redirect 属性と url-redirect-acl 属性が含まれた応答 を受信します。

• • 🖌 🔳 🔬 🕒	🗎 🗶 😂 🔍 🔶 🍁	🗢 🗿 🔮	🔲 🖪 🔍 Q. Q. 🔍 🖻 👹 🕅 🕵 😹 😫
Filter:		▼ Expressi	on Clear Apply Save
No. Source	Destination	Protocol L	ength Info
1 192.168.111.10	10.48.66.74	RADIUS	312 Access-Request(1) (id=46, l=270)
2 10.48.66.74	192.168.111.10	RADIUS	311 Access-Accept(2) (idm46, 1x269)
4			
Frame 2: 311 bytes of	on wire (2488 bits), 3	11 bytes ca	ptured (2488 bits)
Ethernet II, Src: W	ware_c0:00:03 (00:50:	56:c0:00:03	I), Dst: Ymware_e8:ef:25 (00:0c:29:e8:ef:25)
Internet Protocol Ve	ersion 4, Src: 10.48.6	6.74 (10.48	1.66.74), Dst: 192.168.111.10 (192.168.111.10)
> User Datagram Protoc	ol, Src Port: sightli	ne (1645),	Dst Port: 54459 (54459)
Radius Protocol			
Code: Access-Accep	t (2)		
Packet identifier:	0x2e (46)		
Length: 269			
Authenticator: bef	22fb479a10c1e2dea5093	7882e0d4	
This is a respons	e to a request in fra	ne 11	
[Time from request	: 0.059399000 seconds	1	
	irs		
▷ AVP: l=7 t=User	-Name(1): cisco		
▷ AVP: l=40 t=Sta	te(24): 52656175746853	657373696f	ie3a63396138373830613830
▷ AVP: l=50 t=Clar	ss(25): 434143533a6330	61383730306	513030303064303030353262
✓ AVP: l=33 t=Ven	dor-Specific(26) v=cis	coSystems(
▷ VSA: l=27 t=Cis	<pre>ico-AVPair(1): url-red</pre>	irect-acl=r	edirect
✓ AVP: l=119 t=Ver	ndor-Specific(26) v=ci	iscoSystems	(9)
▶ VSA: l=113 t=Ci	<pre>sco-AVPair(1): url-re</pre>	direct=http	s://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=c0a8700a0000000052b1b1bc&action=cpp

3. ISE ログには、認証がポスチャ プロファイルと一致したことが示されています(最初のログ エントリ)。

×	0	#ACSACL#-IP-P	ASA9-2		Compliant ise2
×	à	192.168.10.6	7 ASA9-2	ASA92-compliant	Compliant ise2
0	à	0 cisco 192.168.10.6	7		Compliant ise2
×	à	cisco 192.168.10.6	7 ASA9-2	ASA92-posture User lo	dentity Gro Pending ise2

4. ASA が VPN セッションにリダイレクトを追加します。

aaa_url_redirect: Added url redirect:https://ise2.test-cisco.com:8443/
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
acl:redirect for 10.10.10.10

5. ASA での VPN セッションのステータスにポスチャが必要であることが示され、HTTP トラ フィックをリダイレクトします。

ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

:	cisco	Inde	x	:	9			
:	10.10.10.10	Publ	ic IP	:	10	.147.24.	.61	
:	AnyConnect-Parent SSL-7	lunne	l DTLS-Tu	ını	nel	_		
:	AnyConnect Essentials							
:	AnyConnect-Parent: (1)	ione	SSL-Tunr	ie.	1:	(1)RC4	DTLS-Tunnel:	(1)AES128
:	AnyConnect-Parent: (1)	ione	SSL-Tunr	ie.	1:	(1)SHA1	DTLS-Tunnel:	(1)SHA1
:	16077	Bytes	s Rx	:	19	9497		
:	43	Pkts	Rx	:	22	25		
:	0	Pkts	Rx Drop	:	0			
:	GP-SSL	Tunne	el Group	:	RA	A		
:	14:55:50 CET Mon Dec 23	8 2013	3					
:	0h:01m:34s							
:	0h:00m:00s							
:	N/A	VLAN		:	nc	one		
:	c0a8700a000900052b840e	e6						
:	0							
		: cisco : 10.10.10.10 : AnyConnect-Parent SSL-7 : AnyConnect-Parent: (1)r : AnyConnect-Parent: (1)r : AnyConnect-Parent: (1)r : 16077 : 43 : 0 : GP-SSL : 14:55:50 CET Mon Dec 23 : 0h:01m:34s : 0h:00m:00s : N/A : c0a8700a000900052b840e : 0	: cisco Index : 10.10.10.10 Publ: : AnyConnect-Parent SSL-Tunnel : AnyConnect-Parent: (1)none : AnyConnect-Parent: (1)none : AnyConnect-Parent: (1)none : 16077 Bytes : 43 Pkts : 0 Pkts : GP-SSL Tunnel : 14:55:50 CET Mon Dec 23 2012 : 0h:01m:34s : 0h:00m:00s : N/A VLAN : c0a8700a0000900052b840e6 : 0	: cisco Index : 10.10.10.10 Public IP : AnyConnect-Parent SSL-Tunnel DTLS-Tu : AnyConnect-Parent: (1)none SSL-Tunn : AnyConnect-Parent: (1)none SSL-Tunn : AnyConnect-Parent: (1)none SSL-Tunn : 16077 Bytes Rx : 43 Pkts Rx : 0 Pkts Rx Drop : GP-SSL Tunnel Group : 14:55:50 CET Mon Dec 23 2013 : 0h:01m:34s : 0h:00m:00s : N/A VLAN : c0a8700a0000900052b840e6 : 0	: cisco Index : : 10.10.10.10 Public IP : : AnyConnect-Parent SSL-Tunnel DTLS-Tune : AnyConnect-Parent: (1)none SSL-Tunne : AnyConnect-Parent: (1)none SSL-Tunne : AnyConnect-Parent: (1)none SSL-Tunne : 16077 Bytes Rx : : 43 Pkts Rx : : 43 Pkts Rx : : 0 Pkts Rx Drop : : GP-SSL Tunnel Group : : 14:55:50 CET Mon Dec 23 2013 : 0h:01m:34s : 0h:00m:00s : N/A VLAN : : c0a8700a0000900052b840e6 : 0	: cisco Index : 9 : 10.10.10.10 Public IP : 10 : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel : AnyConnect Essentials : AnyConnect-Parent: (1)none SSL-Tunnel: : AnyConnect-Parent: (1)none SSL-Tunnel: : 16077 Bytes Rx : 19 : 43 Pkts Rx : 22 : 0 Pkts Rx Drop : 0 : GP-SSL Tunnel Group : RA : 14:55:50 CET Mon Dec 23 2013 : 0h:01m:34s : 0h:00m:00s : N/A VLAN : no	<pre>: cisco Index : 9 : 10.10.10.10 Public IP : 10.147.24. : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel : AnyConnect Essentials : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 : 16077 Bytes Rx : 19497 : 43 Pkts Rx : 225 : 0 Pkts Rx Drop : 0 : GP-SSL Tunnel Group : RA : 14:55:50 CET Mon Dec 23 2013 : 0h:01m:34s : 0h:00m:00s : N/A VLAN : none : c0a8700a0000900052b840e6 : 0</pre>	<pre>: cisco Index : 9 : 10.10.10.10 Public IP : 10.147.24.61 : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel : AnyConnect Essentials : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: : 16077 Bytes Rx : 19497 : 43 Pkts Rx : 225 : 0 Pkts Rx Drop : 0 : GP-SSL Tunnel Group : RA : 14:55:50 CET Mon Dec 23 2013 : 0h:01m:34s : 0h:00m:00s : N/A VLAN : none : c0a8700a0000900052b840e6 : 0</pre>

AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 9.1 Public IP : 10.147.24.61 Hashing : none Encryption : none TCP Src Port : 50025 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : win Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5204 Bytes Rx : 779 Pkts Tx : 4 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 9.2 Assigned IP : 10.10.10.10 Public IP : 10.147.24.61 Encryption : RC4 Hashing : SHA1 Encapsulation: TLSv1.0 TCP Src Port : 50044 TCP Dst Port : 443 Auth Mode : userPassword Idle TO Left : 28 Minutes Idle Time Out: 30 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5204 Bytes Rx : 172 Pkts Tx : 4 Pkts Rx : 2 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 9.3 Assigned IP : 10.10.10.10 Public IP : 10.147.24.61 Hashing : SHA1 Encryption : AES128 UDP Src Port : 63296 Encapsulation: DTLSv1.0 UDP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040 Bytes Tx : 5669 Bytes Rx : 18546 : 35 : 222 Pkts Tx Pkts Rx Pkts Tx Drop : 0 Pkts Rx Drop : 0

ISE Posture:

Redirect URL : https://ise2.test-cisco.com:8443/guestportal/gateway?
 sessionId=c0a8700a0000900052b840e6&action=cpp
Redirect ACL : redirect

6. リダイレクト ACL と一致する HTTP トラフィックを開始するクライアントは、ISE にリダ イレクトされます。

aaa_url_redirect: Created proxy for 10.10.10.10
aaa_url_redirect: Sending url redirect:https://ise2.test-cisco.com:8443/
guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
for 10.10.10.10

7. クライアントはポスチャのために ISE にリダイレクトされます。

A https://ive2terf	Client Provi	opSetup.action7session=cl sioning Portal	0:0700:00000600	052b0366c8tes=Window	a⊺(A) ☆ ♥ C	📲 - AVG Secure 1	Search A	•	^	2 -
Cisco Id Engine I Notice	entity Serv Network	vices anty Warning to you want to Com he connection to this we web the contect is not this application will b contain the Permisson	tinue? bisite is untrus sites https://is valid and cannot e blocked in a fut ins attribute. Ple	Determining prior sted. e2.test-cisco.com:8443 be used to verify the kient ture Java security update b ase context the Publisher fr	ty of this website. Execuse the JAR file or more information.	manfest does not More Enformation	levice28 sec	ond(s).		

8. NAC Agent がインストールされます。NAC Agent がインストールされると、SWISS プロト コルを介してポスチャ ルールをダウンロードし、コンプライアンスを確認するためのチェ ックを実行します。ポスチャ レポートが ISE に送信されます。

🚱 Cisco NAC Agent	
cisco NAC Agent	About
Full Network Access	
Your device conforms with all the security policies for this protected network	

9. ISE はポスチャ レポートを受信し、認証ルールを再評価し、(必要に応じて)認証ステータ スを変更して CoA を送信します。これは ise-psc.log で確認できます。

```
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a8700a0000900052b840e6

:::- Decrypting report

cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a000900052b840e6

:::- User cisco belongs to groups NAC Group:NAC:IdentityGroups:User Identity

Groups:Employee,NAC Group:NAC:IdentityGroups:An

cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6

:::- Posture report token for endpoint mac 08-00-27-CD-E8-A2 is Healthy

cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6

:::- Posture state is compliant for endpoint with mac 08-00-27-CD-E8-A2

cisco.cpm.posture.runtime.PostureCoA -:cisco:c0a8700a0000900052b840e6

:::- Posture CoA is triggered for endpoint [null] with session

[c0a8700a0000900052b840e6]

10. ISE は、session_id を含む RADIUS CoA と、フル アクセスを許可する DACL 名を送信し
```

ます。

No.	Source	Destination	Protocol	Length	Info						
	7 10.48.66.74	192.168.111.10	RADIUS	231	CoA-Request(43) (i	d=11, l=189)					
1	3 192.168.111.10	10.48.66.74	RADIUS	62	CoA-ACK(44) (id=11	, l=2θ)					
*											
▶ Fi	Frame 7: 231 bytes on wire (1848 bits), 231 bytes captured (1848 bits)										
▶ E1	Ethernet II, Src: Vmware_c0:00:03 (00:50:56:c0:00:03), Dst: Vmware_e8:ef:25 (00:0c:29:e8:ef:25)										
⊳ Ir	nternet Protocol Versi	ion 4, Src: 10.48.66	.74 (10.	48.66.7	4), Dst: 192.168.1	11.10 (192.168.111.10)					
▶ Us	er Datagram Protocol,	Src Port: 44354 (4	4354), D	st Port	: mps-raft (1700)						
▼ Ra	Radius Protocol										
	Code: CoA-Request (43)										
	Packet identifier: 0x	b (11)									
	Length: 189										
	Authenticator: d20817	c6ca828ce7db4ee54f15	5177b8d								
	[The response to this	request is in frame	2 81								
~	Attribute Value Pairs										
	> AVP: l=6 t=NAS-IP-/	Address(4): 10.147.2	4.61								
	AVP: l=15 t=Calling	g-Station-Id(31): 19	2.168.10	.67							
	▶ AVP: l=6 t=Event-T:	imestamp(55): Dec 18	, 2013 1	5:32:10	.000000000 CET						
	▷ AVP: l=18 t=Message	e-Authenticator(80):	1ee29f1	d83e5f3	aa4934d60aa617ebeb						
	▼ AVP: l=75 t=Vendor	-Specific(26) v=cisc	oSystems	(9)							
	♦ VSA: l=69 t=Cisco-	AVPair(1): ACS:Cisco	oSecure-I	Defined	- ACL=#ACSACL#-IP-P	ERMIT_ALL_TRAFFIC-51ef7db1					
	▼ AVP: l=49 t=Vendor	-Specific(26) v=cisc	oSystems	(9)							
	▹ VSA: l=43 t=Cisco-	AVPair(1): audit-se	ssion-id:	=c0a870	0a0000d00052b1b1bc						

これは、ISE ログに反映されます。

最初のログ エントリは、ポスチャ プロファイルを返す(リダイレクションを伴う)最初の 認証です。

2番目のログエントリは、準拠している SWISS レポートを受信した後に入力されます。

3 番目のログ エントリは、CoA が送信される(確認を伴う)ときに入力されます(「動的 認証の成功」の説明を参照)。

最後のログエントリは、ASA が DACL をダウンロードするときに作成されます。

<u>~</u>		#ACSACL#-IP-P		ASA9-2			Compliant	ise2
×	ò		192.168.10.67	ASA9-2	ASA92-compliant		Compliant	ise2
0	à 0	cisco	192.168.10.67				Compliant	ise2
×		cisco	192.168.10.67	ASA9-2	ASA92-posture	User Identity Gro	Pending	ise2

11. ASA でのデバッグに、CoA を受信したこと、およびリダイレクトが削除されたことが示さ れています。ASA は必要に応じて DACL をダウンロードします。

ASA# Received RAD_COA_REQUEST

RADIUS packet decode (CoA-Request)

 Radius: Value (String) =

 41 43 53 3a 43 69 73 63 6f 53 65 63 75 72 65 2d
 | ACS:CiscoSecure

 44 65 66 69 6e 65 64 2d 41 43 4c 3d 23 41 43 53
 | Defined-ACL=#ACS

 41 43 4c 23 2d 49 50 2d 50 45 52 4d 49 54 5f 41
 | ACL#-IP-PERMIT_A

 4c 4c 5f 54 52 41 46 46 49 43 2d 35 31 65 66 37
 | LL_TRAFFIC-51ef7

 64 62 31
 | db1

Got AV-Pair with value audit-session-id=c0a8700a000900052b840e6
Got AV-Pair with value ACS:CiscoSecure-Defined-ACL=
#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1

aaa_url_redirect: Deleted url redirect for 10.10.10.10

ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

```
Username : cisco
                                  Index : 9
Assigned IP : 10.10.10.10
                                 Public IP : 10.147.24.61
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Essentials
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx
          : 94042
                                  Bytes Rx : 37079
Pkts Tx : 169
                                 Pkts Rx
                                             : 382
Pkts Tx Drop : 0
                                 Pkts Rx Drop : 0
Group Policy : GP-SSL
                                 Tunnel Group : RA
Login Time : 14:55:50 CET Mon Dec 23 2013
           : 0h:05m:30s
Duration
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                  VLAN : none
Audt Sess ID : c0a8700a0000900052b840e6
Security Grp : 0
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnvConnect-Parent:
Tunnel ID : 9.1
Public IP : 10.147.24.61
 Encryption : none
                                  Hashing
                                              : none
 TCP Src Port : 50025
                                  TCP Dst Port : 443
 Auth Mode : userPassword
 Idle Time Out: 30 Minutes
                                  Idle TO Left : 24 Minutes
 Client OS : win
 Client Type : AnyConnect
 Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040
Bytes Tx : 5204 Bytes Rx : 779
 Pkts Tx : 4
                                  Pkts Rx : 1
 Pkts Tx Drop : 0
                                   Pkts Rx Drop : 0
SSL-Tunnel:
 Tunnel ID : 9.2
 Assigned IP : 10.10.10.10 Public IP : 10.147.24.61
 Encryption : RC4
                                  Hashing
                                              : SHA1
 Encapsulation: TLSv1.0
                                  TCP Src Port : 50044
                                 Auth Mode : userPassword
 TCP Dst Port : 443
 Idle Time Out: 30 Minutes
                                  Idle TO Left : 24 Minutes
 Client OS : Windows
 Client Type : SSL VPN Client
 Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040
                                   Bytes Rx : 172
 Bytes Tx : 5204
 Pkts Tx : 4
                                   Pkts Rx
                                              : 2
 Pkts Tx Drop : 0
                                   Pkts Rx Drop : 0
 Filter Name : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
DTLS-Tunnel:
Tunnel ID : 9.3
 Assigned IP : 10.10.10.10 Public IP : 10.147.24.61
                                 Hashing : SHA1
UDP Src Port : 63296
Auth Mode : userPassword
Idle TO Left : 29 Minutes
 Encryption : AES128
 Encapsulation: DTLSv1.0
 UDP Dst Port : 443
 Idle Time Out: 30 Minutes
```

```
Client OS : Windows

Client Type : DTLS VPN Client

Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.02040

Bytes Tx : 83634 Bytes Rx : 36128

Pkts Tx : 161 Pkts Rx : 379

Pkts Tx Drop : 0 Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

注:CoAにDACLが接続されていない場合でも、ASAは常にリダイレクトルールを削除します。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ISE でのデバッグ

[Administration] > [Logging] > [Debug Log Configuration] に移動し、デバッグを有効にします。シ スコでは、以下の一時的なデバッグを有効にすることを推奨します。

- SWISS
- Nonstop Forwarding (NSF)
- NSF-Session
- [Provision]
- ポスチャ

CLI で次のコマンドを入力して、デバッグを表示します。

ise2/admin# show logging application ise-psc.log tail count 100

[Operations] > [Reports] > [ISE Reports] > [Endpoints and Users] > [Posture Details Assessment] に移動し、ポスチャ レポートを表示します。

alada									247 abor	Legent Feelbeck D
CISCO Identity Services Engine	Home Operations + Policy + Administration +								Setup As	
🙍 Authentications 📑 Reports 📷 Drok	point Protection Genice	Tott	foor field							
Report Selector	Posture Detail Asses	sment								🔶 Favorita 🛛 🚇 Export 🛛 💾
Favorites										Generated at 2013-02-5
ISE Reports	From 12232013 12:08:00	IAM10 12	152/58/12	03:56:58 PM						Page << 1 >> Page 167
 Auth Services Stelve 	Logged At	Status	Detail	PRA	Identity	Endpoint ID	P Address	Endpoint DS	Agent	Message
8 reports	2013-12-23 15:21:34.9			continue	cisco	08:08:27:CD:E8:A	10.147.24.92	Windows 7 Enterprise 64-bit	CISCO RAC A	Received a posture report from an endpoint
Deprogramment Status T1 reports	2013-12-23 15:08:58.3		.0	continue	cisco	08/08/27/CD/68/A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A	Received a posture report from an endpoint
+ Endpoints and Users	2013-12-23 14:59:34.3			continue	cisco	08:00:27:CD:68:A	10.147.24.92	Windows 7 Enterprise 64-bit	CISCO NAC A	Received a posture report from an endpoint
Client Provisioning	2013-12-23 14:55:28.6	•	.o	N/A	cisco	08-00-27-CD-E8-A	10.147.24.92	Windows 7 Enterprise 64-bit	Cisco NAC A	Received a posture report from an endpoint
Current Active Sessions	2013-12-23 14:44:45.0	٠		NA	cisco	08:08:27:CD/E8:A	10.147.24.92	Windows 7 Enterprise 64-bit	CISCO NAC A	Received a posture report from an endpoint
Count Arthute	2013-12-23 13:34:30.3	•	.0	NA	cisco	08/08/27/76/56/6	10.147.24.92	Windows 7 Utimate 64 bit	Cisco NAC A	Received a posture report from an endpoint
OTEX ACING	2013-12-23 13:27:10.3	•		NA	cisco	08:08:27:77:57:6	10.147.24.92	Windows 7 Utimate 64-bit	CISCO RAC A	Received a posture report from an endpoint
Guest Accounting										
Guest Sponsor Happing										
Guest Sponsor Summary										
Endpoint Protection Service Audit										
Mobile Device Hanagement										
Posture Det al Assessment Pitters • Time Range Today •										

[Posture More Detail Assessment] ページに、ポリシー名と要件名が表示され、さらにその結果が 表示されます。

Posture More Detail Assessment

Time Range: From 12/23/2013 12:00:00 AM to 12/23/2013 03:57:31 PM Generated At: 2013-12-23 15:57:31.248

Client Details									
Username:	cisco								
Mac Address:	08:00:2	:00:27:CD:E8:A2							
IP address:	10.147.	147.24.92							
Session ID:	c0a870	0a0000b00052b8	46c0						
Client Operating System	m: Window	s 7 Enterprise 64-	bit						
Client NAC Agent:	Cisc o N	AC Agent for Winde	ows 4.9.0	0.1013					
PRA Enforcement:	1								
CoA:	Receive	d a posture report	from an	endpoint					
PRA Grace Time:									
PRA Interval:	240								
PRA Action:	continue								
User Agreement Statu	Agreement Status: NotEnabled								
System Name:	MGARCA	MGARCARZ-W S01							
System Domain:	cisco.co	m							
System User:	mgarca	rz							
User Domain:	CISCO								
AV Installed:	McAfee	VirusScan Enterpr	ise;8.8.0.	975;7227;10/13/2	2013;McAfeeAV,Cisc	o Security Agent;6.0.2.130;;;CiscoAV			
AS Installed:	Window	s Defender;6.1.76	00.1638	5;1.95.191.0;11/1	9/2010;MicrosoftAS				
Posture Report									
Posture Status:	Complia	int							
Logged At:	2013-12	2-23 15:21:34.902	2						
Posture Policy Details									
Policy	Name	Enforcement	Statu	Passed	Failed	Skipped Conditions			
posture_initial	file_require	Mandatory		file_condition					

ASA でのデバッグ

ASA では以下のデバッグを有効にすることができます。

- debug aaa url-redirect
- debug aaa authorization
- · debug radius dynamic-authorization
- · debug radius decode
- debug radius user cisco

エージェントのデバッグ

NACエージェントの場合は、Cisco Log Packagerを使用してデバッグを収集できます。Cisco Log Packagerは、GUIまたはCLIで**CCAAgentLogPackager.app**を使用して開始します。

🛨 Cisco Log Pa	ckager v1.	7.0.11									
cisco.	Cisco	Cisco Log Packager									
	Cisco Log Packager collects information for product support requests. The information is stored in a ZIP archive that can be protected by a password.										
Protect dat	a with foll	owing password:									
Collect Da	ita	Show Log	Locate Report File	Cancel	Exit						

ヒント:結果をデコードするには、Technical Assistance Center(TAC)ツールを使用します。

Web エージェントのログを取得するには、次の場所に移動します。

- C: > Document and Settings > *<user> > Local Settings > Temp > webagent.log (TACツール* でデコード)
- C: > Document and Settings > <user> > Local Settings > Temp > webagentsetup.log

注: ログがこれらの場所にない場合は、TEMP Environment変数を確認します。

NAC エージェント ポスチャの障害

ポスチャが失敗した場合は、次のようにその原因が表示されます。



修復アクションが設定されている場合は、ユーザに修復アクションの実行が許可されます。

CISCO Client Provisioning Portal		
Information	Cisco NAC Agent	Cancel About
	Temporary Network Access There is at least one mandatory requirement failing. You are require before you can access the network. Repair Show Details Continue	00:03:58 left ed to update your system tue
	System Check Complete	

関連情報

- セキュリティ アプライアンスのユーザ認証に外部サーバを設定
- <u>Cisco ASA シリーズ VPN CLI 構成ガイド 9.1</u>
- 『Cisco Identity Services Engine User Guide, Release 1.2 (Cisco Identity Services Engine ユ ーザガイドリリース 1.2)』
- ・ テクニカル サポートとドキュメント – Cisco Systems

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。