Windowsでのセキュアエンドポイントのインストールに必要なルート証明書のリストのトラブルシューティング

内容

はじめに

このドキュメントでは、証明書エラーが原因で高度なマルウェア防御(AMP)のインストールが失敗した場合に、インストールされているすべての認証局(CA)を確認する方法について説明します。

使用するコンポーネント

- Security Connector（旧称AMP for Endpoints）6.3.1以降
- Windows 7以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

Windows用エンドポイントコネクタのAMPで問題が発生した場合は、この場所のログを確認してください。

<#root>

C:\ProgramData\Cisco\AMP\immpro_install.log

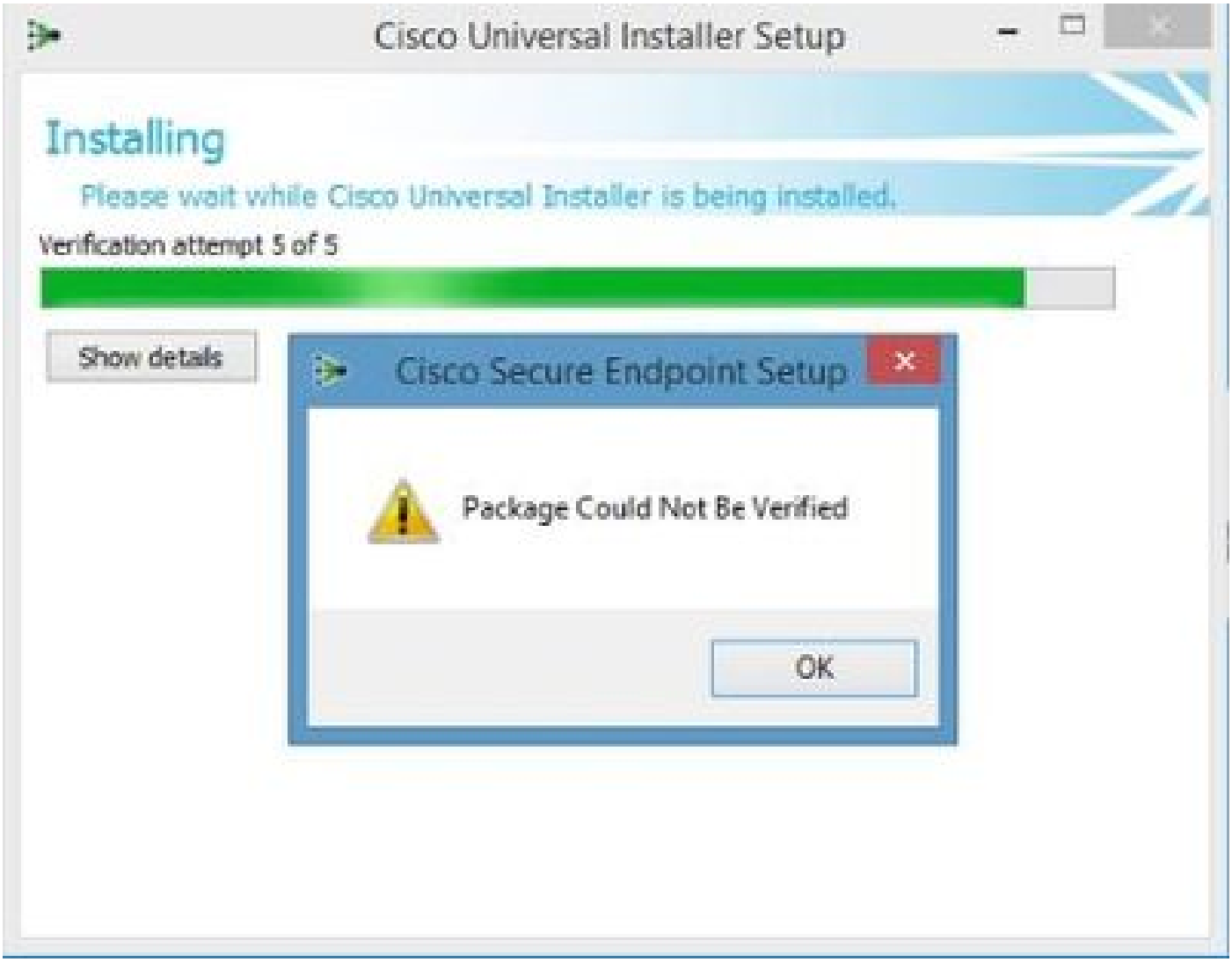
このメッセージまたは類似のメッセージが表示された場合。

<#root>

```
ERROR: Util::VerifyAll: signature verification failed : -2146762487 : A certificate chain processed, but
```

<#root>

```
Package could not be verified
```



必要なすべてのRootCA証明書がインストールされていることを確認します。

解決方法

ステップ 1：管理者権限でPowerShellを開き、コマンドを実行します。

<#root>

```
Get-ChildItem -Path Cert:LocalMachine\Root
```

結果は、マシンに格納されているインストール済みRootCA証明書のリストを示します。

ステップ 2：手順1で取得した拇印を、次の表1に示す拇印と比較します。

拇印	サブジェクト名/属性
3B1EFD3A66EA28B16697394703A72CA340A05BD5	CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
D69B561148F01C77C54578C10926DF5B856976AD	CN=GlobalSign, O=GlobalSign, OU=GlobalSignルートCA - R3
D4DE20D05E66FC53FE1A50882C78DB2852CAE474	CN=Baltimore CyberTrust Root、OU=CyberTrust、O=Baltimore、C=IE
D1EB23A46D17D68FD92564C2F1F1601764D8E349	CN=AAA証明書サービス、O=Comodo CA Limited、L=Salford、S=Greater Manchester、C=GB
B1BC968BD4F49D622AA89A81F2150152A41D829C	CN=GlobalSignルートCA、OU=ルートCA、O=GlobalSign nv-sa、C=BE
AD7E1C28B064EF8F6003402014C3D0E3370EB58A	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US
A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
742C3192E607E424EB4549542BE1BBC53E6174E2	OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
5FB7EE0633E259DBAD0C4C9AE6D38F1A61C7DC25	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
2796BAE63F1801E277261BA0D77770028F20EEE4	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US
0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43	CN=DigiCert Assured ID Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
DDFB16CD4931C973A2037D3FC83A4D7D775D05E4	CN=DigiCert Trusted Root G4, OU=www.digicert.com, O=DigiCert Inc, C=US

CA3AFBCF1240364B44B216208880483919937CF7	CN=QuoVadis Root CA 2、O=QuoVadis Limited、C=BM
2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E	CN=USERTrust RSA Certification Authority, O=USERTRUSTネットワーク、L=ジャージーシティ、S=ニュージャージー、C=米国
F40042E2E5F7E8EF8189FED15519AECE42C3BFA2	CN=Microsoft Identity Verification Root Certificate Authority 2020, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
DF717EAA4AD94EC9558499602D48DE5FBCF03A25	CN=US、O=Identrust、CN=Identrust商用ルートCA 1

表 1.Cisco Secure Connectorに必要な証明書のリスト

ステップ 3：マシンストアに存在しない証明書をPEM形式の発行者からダウンロードします。

ヒント：証明書はインターネット上の拇印で検索できます。証明書を一意に定義する。

ステップ 4：スタートメニューからmmcコンソールを開きます。

ステップ 5：File > Add/Remove Snap-in... > Certificates > Add > Computer Account > Next > Finish > OKの順に移動します。

手順 6：Trusted Root Certification Authoritiesの下のCertificatesを開きます。Certificatesフォルダを右クリックして、All Tasks > Import...の順に選択し、ウィザードに従ってCertificatesフォルダに表示されるまで証明書をインポートします。

手順 7：インポートする証明書が他にある場合は、手順6を繰り返します。

ステップ 8：すべての証明書をインポートした後、AMP for Endpoints Connectorのインストールが正常に行われたかどうかを確認します。そうでない場合は、immpro_install.logファイルのログを再び確認します。

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。