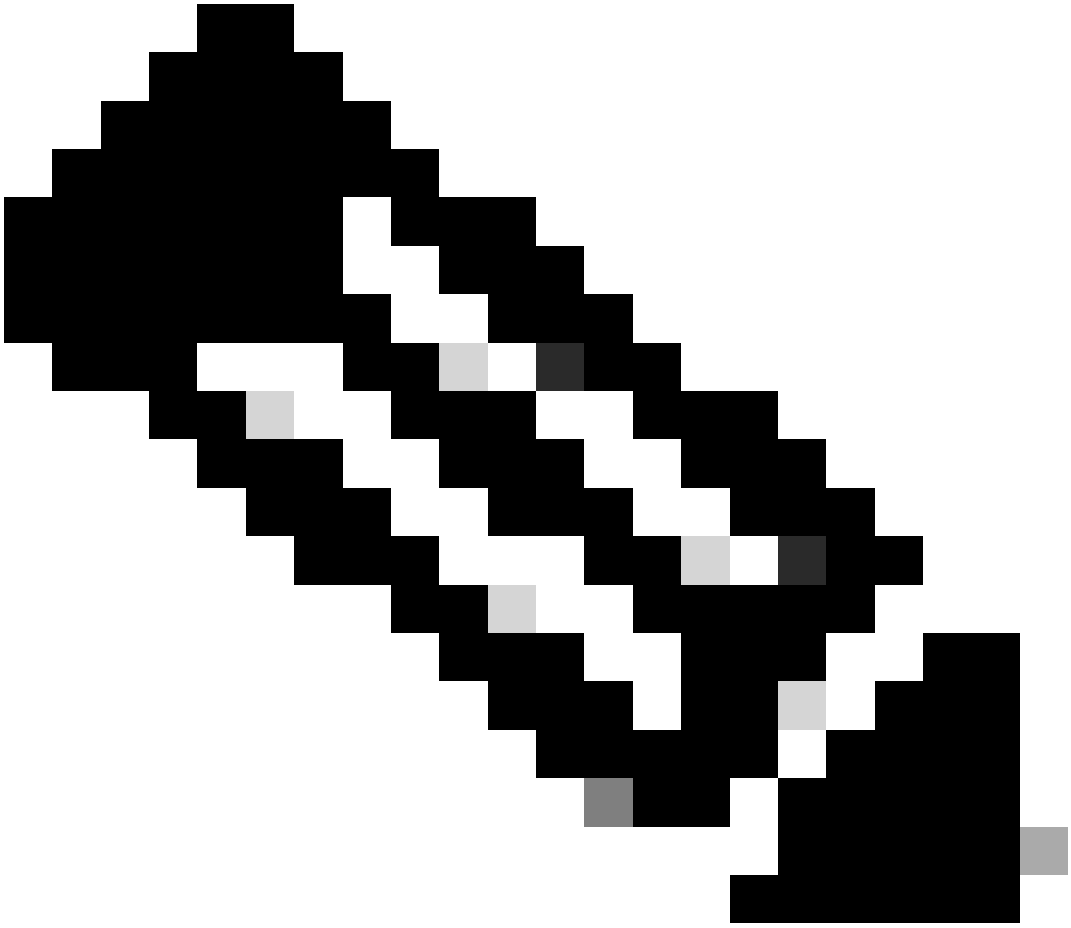
EventID 4662(Windows 2008)またはEventID 566(Windows 2003)のトラブルシューティング – タイプ：失敗の監査

内容

はじめに

このドキュメントでは、セキュリティイベントID 566とセキュリティイベントID 4662について、およびこれらのイベントが発生した場合に実行可能なアクションについて説明します。これらのイベントは、ドメインコントローラーまたはUmbrella Insights展開の一部として実行されているメンバーサーバーで発生する可能性があります。



注：これらのイベントは予期されるものであり、通常のものです。推奨およびサポートされるアクションは、何も行わず、これらのイベントを無視することです。

```
Event ID: 566
Source: Security
Category: Directory Service Access
Type: Failure Audit
Description:
Object Operation:
Object Server:  DS
Operation Type: Object Access
Object Type:    user
Object Name:   CN=USER1,OU=MyOU,DC=domain,DC=net
Handle ID:        -
Primary User Name:     DC1$
Primary Domain:           DOMAIN1
Primary Logon ID:        (0x0,0x3E7)
Client User Name:        COMPUTER1$
Client Domain:  DOMAIN1
Client Logon ID:           (0x0,0x19540114)
```

```
Accesses:         Control Access
Properties:

Private Information

msPKIRoamingTimeStamp
msPKIDPAPIMasterKeys
msPKIAccountCredentials
msPKI-CredentialRoamingTokens
Default property set
unixUserPassword

user
Additional Info:
Additional Info2:
Access Mask:   0x100
```

または、Windows 2008イベントセキュリティID 4662を受け取ります。

```
Event ID: 4662
Type: Audit Failure
Category: Directory Service Access

Description:

An operation was performed on an object.

Subject :

Security ID:     DOMAIN1\COMPUTER1$
Account Name:     COMPUTER1$
Account Domain:     DOMAIN1

Logon ID:     0x3a26176b

Object:

Object Server:     DS
Object Type:     user
Object Name:     CN=USER1,OU=MyOU,DC=domain,DC=net

Handle ID:     0x0

Operation:

Operation Type:     Object Access
Accesses:     Control Access
Access Mask:     0x100

Properties:     ---

{91e647de-d96f-4b70-9557-d63ff4f3ccd8}
{6617e4ac-a2f1-43ab-b60c-11fbd1facf05}
{b3f93023-9239-4f7c-b99c-6745d87adbc2}
{b8dfa744-31dc-4ef1-ac7c-84baf7ef9da7}
{b7ff5a38-0818-42b0-8110-d3d154c97f24}
{bf967aba-0de6-11d0-a285-00aa003049e2}
```

原因

Windows 2008では、msPKI*プロパティを含むPrivate Informationという新しいプロパティセットが導入されました。設計上、これらのプロパティは、SELFオブジェクトだけがアクセスできるように保護されています。 必要に応じて、DSACLSコマンドを使用してオブジェクトの権限を確認できます。

調査が簡単な場合は、これらの制限されたプロパティへの書き込みが原因でこの監査イベントが発生していると思われる可能性があります。これは、変更（書き込み）のみを監査し、Active Directoryからの情報の読み取り試行を監査しないデフォルトのMicrosoft監査ポリシーでこれらのイベントが発生するという事実から明らかです。

ただし、そうではない場合、監査イベントには要求されているアクセス許可が制御アクセス(0x100)として明確に一覧表示されます。申し訳ございませんが、プライベート情報プロパティセットにCA (制御アクセス)アクセス許可を付与することはできません。

解決方法

これらのメッセージを無視しても安全です。これは仕様です。

これらのイベントが表示されないようにするための措置を取ることは推奨されません。ただし、これらを実装することを選択した場合は、オプションとして提示されます。 どちらの回避策も推奨されません。ご自身の責任で使用してください。

回避策

方式 1

デフォルトのドメインコントローラポリシーでディレクトリサービス監査設定を無効にして、Active Directoryのすべての監査を無効にします。

方式 2

コントロールアクセス権限を管理する基本プロセスは、各プロパティ（例：msPKIRoamingTimeStamp）に割り当てられたsearchFlags属性を利用します。searchFlagsは10ビットアクセスマスクです。ビット8(2進数のアクセスマスクで0から7まで数える= 10000000 = 128 10進数)を使用して、機密アクセスの概念を実装します。 ADスキーマでこの属性を手動で変更し、これらのプロパティの機密アクセスを無効にすることができます。これにより、失敗の監査ログが生成されなくなります。

ADの任意のプロパティの機密アクセスを無効にするには、ADSI Editを使用して、スキーママス

ターロールを保持するDCのスキーマ名前付けコンテキストにアタッチします。変更する適切なプロパティを検索します。プロパティ名は、イベントID 566または4662に表示されるプロパティとは少し異なる場合があります。

入力する正しい値を判別するには、現在のsearchFlagsの値から128を引き、その結果をsearchFlagsの新しい値、つまり640-128 = 512として入力します。searchFlagsの現在の値が128未満で、何も行わない場合、プロパティが正しくないか、Confidential Accessによって監査イベントが発生していない可能性があります。

イベントID 566または4662の説明に記載されている各プロパティに対して、この操作を実行します。

スキーママスターのレプリケーションを他のドメインコントローラーに強制し、新しいイベントを確認します。

ドメイン監査ポリシーを変更して、次のプロパティの失敗を監査しないようにします。

この方法の欠点は、追加が必要な監査エントリの数が多いためにパフォーマンスが低下する可能性があることです。

詳細情報:

Googleやその他の検索エンジンを使用すると、GUIDをオブジェクト名に簡単に変換できます。
ここでは、googleを使用して検索する方法の例を示します。

例： site:microsoft.com 91e647de-d96f-4b70-9557-d63ff4f3ccd8

{91e647de-d96f-4b70-9557-d63ff4f3ccd8} = プライベート情報プロパティセット
{6617e4ac-a2f1-43ab-b60c-11fbd1facf05} = ms-PKI-RoamingTimeStamp属性

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。