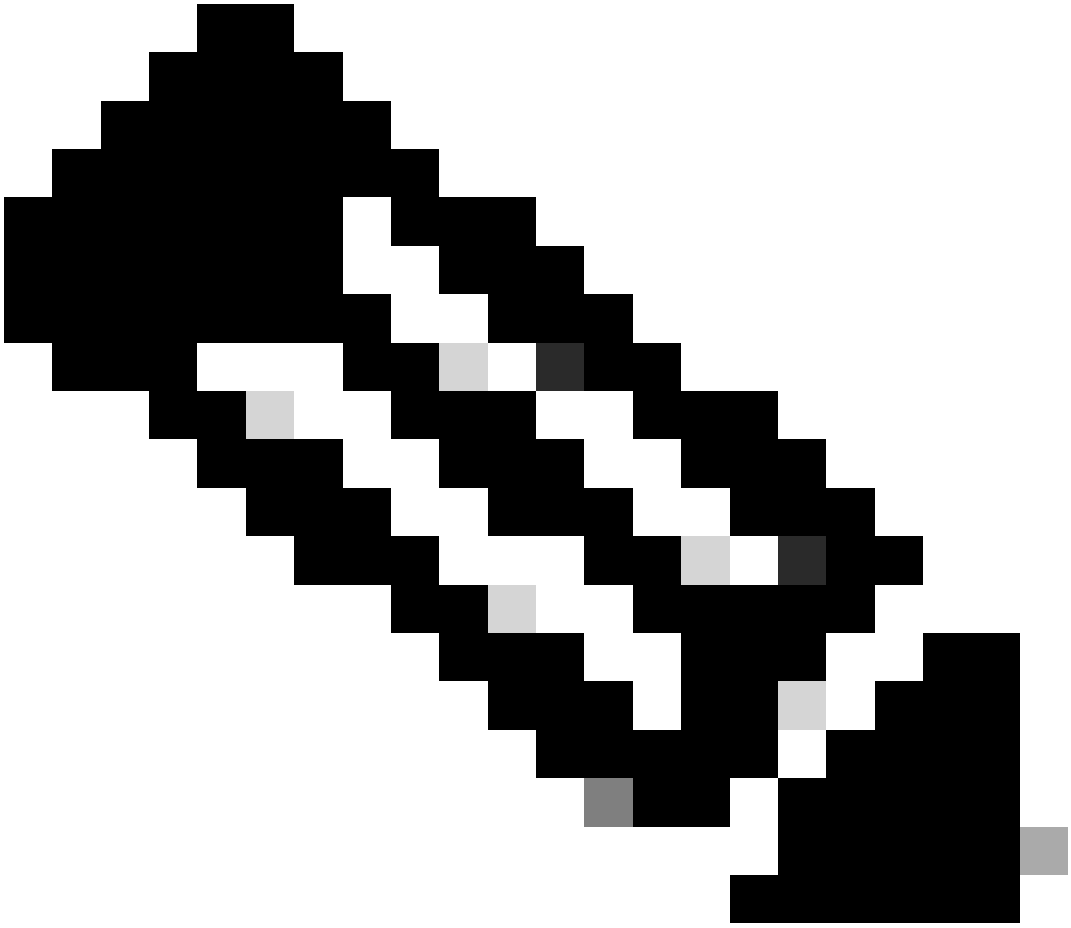
Dépannez EventID 4662 (Windows 2008) ou EventID 566 (Windows 2003) - Type : Audit des échecs

Table des matières

Introduction

Ce document décrit l'ID d'événement de sécurité 566 et l'ID d'événement de sécurité 4662, ainsi que l'action à entreprendre lorsqu'ils se produisent. Ces événements sont susceptibles de se produire sur des contrôleurs de domaine ou un serveur membre s'exécutant dans le cadre du déploiement d'Umbrella Insights.



Remarque : Ces événements sont à prévoir et sont normaux. L'action préférée et prise en charge est de ne rien faire et d'ignorer ces événements.

```
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
```

Vous pouvez également recevoir cet ID de sécurité des événements Windows 2008 4662.

```
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}
```

Motif

Windows 2008 a introduit un nouvel ensemble de propriétés appelé Informations privées qui inclut les propriétés msPKI*. Ces propriétés sont sécurisées de manière à ce que seul l'objet SELF puisse y accéder. Vous pouvez utiliser la commande DSACLS pour vérifier les autorisations sur l'objet, le cas échéant.

Une enquête sommaire peut vous laisser croire que cet événement d'audit est provoqué par une tentative d'écriture dans ces propriétés restreintes. Cela est évident par le fait que ces événements se produisent sous la stratégie d'audit par défaut de Microsoft qui audite uniquement les modifications (écritures) et n'audite pas les tentatives de lecture d'informations à partir d'Active Directory.

Cependant, ce n'est pas le cas, l'événement d'audit indique clairement que l'autorisation demandée est Accès au contrôle (0x100). Malheureusement, vous ne pouvez pas accorder l'autorisation CA (Accès au contrôle) au jeu de propriétés Informations privées.

Solution

Vous pouvez ignorer ces messages en toute sécurité. C'est intentionnel.

Il n'est pas recommandé de prendre des mesures pour empêcher l'apparition de ces événements. Toutefois, ces options sont présentées sous forme d'options si vous choisissez de les implémenter. Aucune solution de contournement n'est recommandée : utilisation à vos propres risques.

Solution De Contournement

Méthode 1

Désactivez tous les audits dans Active Directory en désactivant le paramètre d'audit Directory Service dans la stratégie de contrôleur de domaine par défaut.

Méthode 2

Le processus sous-jacent qui gère l'autorisation Accès au contrôle utilise l'attribut searchFlags qui est affecté à chaque propriété (c'est-à-dire : msPKIRoamingTimeStamp). searchFlags est un masque d'accès de 10 bits. Il utilise le bit 8 (en comptant de 0 à 7 dans un masque d'accès binaire = 10000000 = 128 décimal) pour implémenter le concept d'accès confidentiel. Vous pouvez modifier manuellement cet attribut dans le schéma Active Directory et désactiver l'accès confidentiel de ces propriétés. Cela empêche ensuite la génération des journaux d'audit des

échecs.

Pour désactiver l'accès confidentiel pour une propriété dans AD, utilisez Édition ADSI pour attacher au contexte d'attribution de noms de schéma sur le contrôleur de domaine qui détient le rôle de maître de schéma. Recherchez les propriétés à modifier. Leur nom peut être légèrement différent de celui indiqué dans l'ID d'événement 566 ou 4662.

Pour déterminer la valeur correcte à entrer, soustrayez 128 de la valeur searchFlags actuelle et entrez le résultat comme nouvelle valeur de searchFlags, ainsi 640-128 = 512. Si la valeur actuelle de searchFlags est < 128 ne faites rien, vous pouvez avoir la mauvaise propriété ou l'accès confidentiel n'est pas à l'origine de l'événement d'audit.

Effectuez cette opération pour chaque propriété répertoriée dans la description Event ID 566 ou 4662.

Forcez la réplication du contrôleur de schéma vers les autres contrôleurs de domaine, puis recherchez de nouveaux événements.

Modifiez la stratégie d'audit de domaine pour ne pas auditer les échecs sur ces propriétés :

L'inconvénient de cette méthode est que les performances peuvent être dégradées en raison du nombre élevé d'entrées d'audit qui doivent être ajoutées.

Plus d'informations:

La traduction du GUID en noms d'objets est facile à utiliser avec Google ou un autre moteur de recherche. Voici un exemple de recherche à l'aide de Google.

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

{91e647de-d96f-4b70-9557-d63ff4f3ccd8} = Jeu de propriétés Informations privées {617e4ac-a2f1-43ab-b60c-11fbd1facf05} = Attribut ms-PKI-RoamingTimeStamp

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.