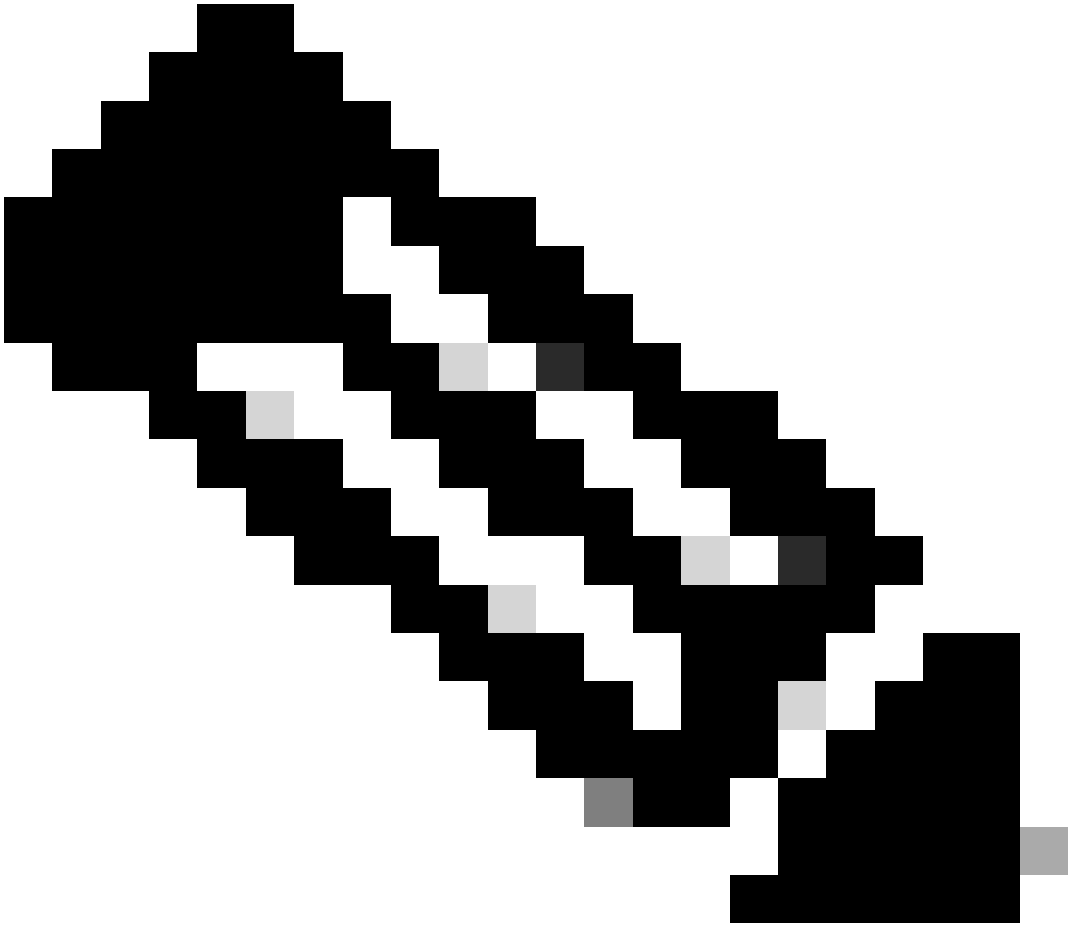
Problemen oplossen met EventID 4662 (Windows 2008) of EventID 566 (Windows 2003) - Type: foutcontrole

Inhoud

Inleiding

In dit document worden Security Event ID 566 en Security Event ID 4662 beschreven en wordt beschreven welke actie kan worden ondernomen wanneer u ze tegenkomt. Deze gebeurtenissen kunnen zich naar verwachting voordoen op domeincontrollers of een lidserver die wordt uitgevoerd als onderdeel van de Umbrella Insights-implementatie.



Opmerking: Deze gebeurtenissen zijn te verwachten en zijn normaal. De voorkeur en de ondersteunde actie is om niets te doen en deze gebeurtenissen te negeren.

```
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
```

Of u ontvangt deze Windows 2008 Event Security ID 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}
```

Oorzaak

Windows 2008 introduceerde een nieuwe eigenschapsset met de naam Privé-informatie die de msPKI*-eigenschappen bevat. Door het ontwerp zijn deze eigenschappen zodanig beveiligd dat alleen het SELF-object er toegang toe heeft. U kunt de opdracht DSACLS gebruiken om de machtigingen voor het object te controleren.

Een vluchtig onderzoek kan ertoe leiden dat u denkt dat deze audit-gebeurtenis wordt veroorzaakt door een poging om naar deze beperkte eigenschappen te schrijven. Dit blijkt uit het feit dat deze gebeurtenissen plaatsvinden onder het standaard Microsoft-auditbeleid dat alleen wijzigingen controleert (schrijft) en geen pogingen controleert om informatie uit Active Directory te lezen.

Dit is echter niet het geval, de audit-gebeurtenis vermeldt duidelijk de toestemming die wordt gevraagd als Control Access (0x100). Helaas kunt u de CA (Control Access)-toestemming niet verlenen voor de eigenschapset Privé-informatie.

Oplossing

U kunt deze berichten veilig negeren. Dit is met opzet.

Het wordt niet aanbevolen dat u enige actie onderneemt om te voorkomen dat deze gebeurtenissen zich voordoen. Deze worden echter gepresenteerd als opties als u ervoor kiest om ze te implementeren. Geen van beide oplossingen wordt aanbevolen: gebruik op eigen risico.

tijdelijke oplossingen

Methode 1

Schakel alle controles in Active Directory uit door de instelling voor Directory Service-controle in het standaardbeleid voor domeincontrollers uit te schakelen.

Methode 2

Het onderliggende proces dat de machtiging Control Access beheert, maakt gebruik van het kenmerk searchFlags dat aan elke eigenschap is toegewezen (dat wil zeggen: msPKIRoamingTimeStamp). searchFlags is een 10-bits toegangsmasker. Het gebruikt bit 8 (tellen van 0 tot 7 in een binair toegangsmasker = 1000000 = 128 decimaal) om het concept Vertrouwelijke toegang te implementeren. U kunt dit kenmerk handmatig wijzigen in het AD-schema en de vertrouwelijke toegang van deze eigenschappen uitschakelen. Hierdoor wordt voorkomen dat de controlelogboeken voor fouten worden gegenereerd.

Als u Vertrouwelijke toegang voor een eigenschap in AD wilt uitschakelen, gebruikt u ADSI Bewerken om te koppelen aan de context Schema-naamgeving op de DC met de Schema-hoofdrol. Zoek de juiste eigenschappen om te wijzigen, hun naam kan enigszins verschillen van wat wordt weergegeven in Event ID 566 of 4662.

Om de juiste waarde in te voeren, trekt u 128 af van de huidige waarde searchFlags en voert u het resultaat in als de nieuwe waarde van searchFlags, dus 640-128 = 512. Als de huidige waarde van searchFlags < 128 is, hoeft u niets te doen, hebt u mogelijk de verkeerde eigenschap of veroorzaakt Confidential Access de audit-gebeurtenis niet.

Doe dit voor elke eigenschap die wordt vermeld in de beschrijving van Event ID 566 of 4662.

Forceer replicatie van de Schema Master naar de andere domeincontrollers en controleer vervolgens op nieuwe gebeurtenissen.

Wijzig het controlebeleid voor domeinen om fouten in deze eigenschappen niet te controleren:

Het nadeel van deze methode is dat de prestaties kunnen afnemen vanwege het grote aantal auditItems dat moet worden toegevoegd.

Meer informatie:

Het vertalen van GUID naar objectnamen is eenvoudig met behulp van google of een andere zoekmachine. Hier is een voorbeeld van hoe te zoeken met behulp van Google.

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

{91E647DE-D96F-4B70-9557-D63FF4F3CCD8} = Privé-informatie, eigenschappenset
{6617E4AC-A2F1-43AB-B60C-11FBD1FACF05} = ms-PKI-RoamingTimeStamp Attribuut

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.