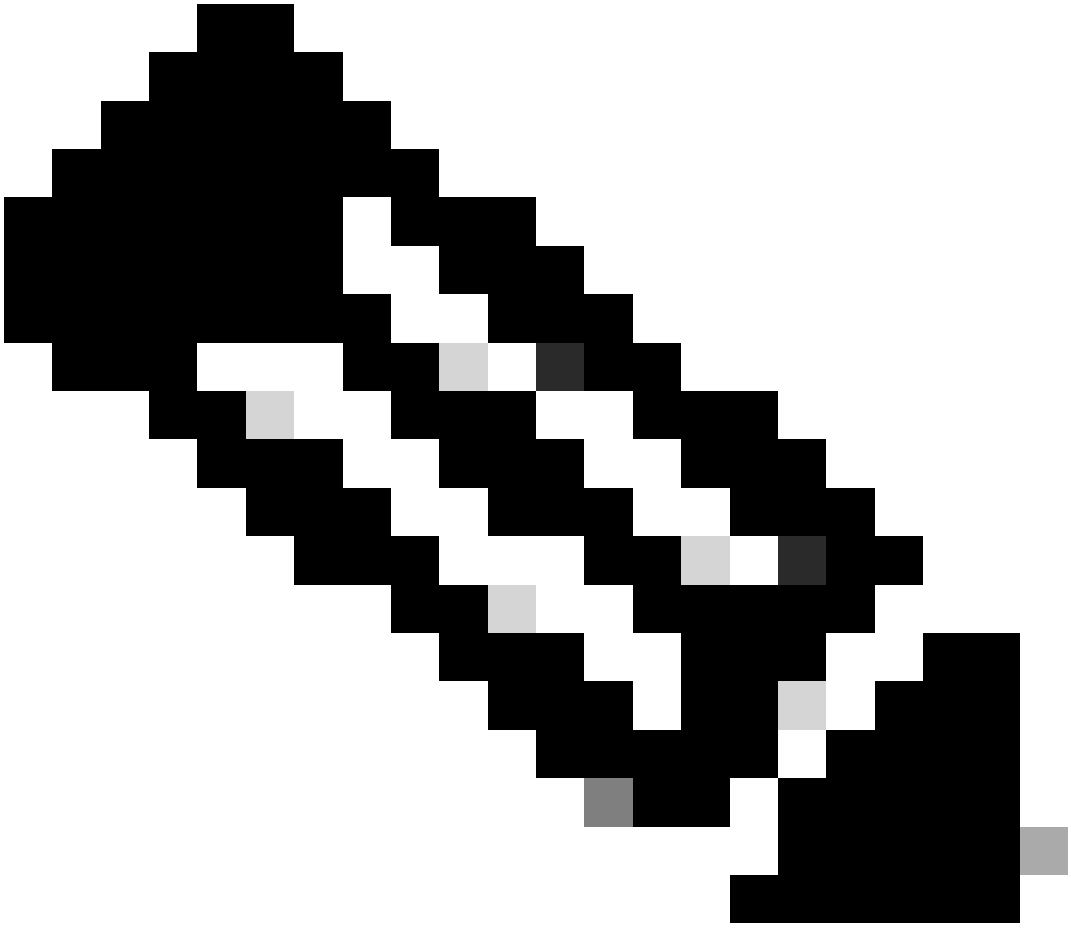
Risoluzione dei problemi relativi a EventID 4662 (Windows 2008) o EventID 566 (Windows 2003) - Tipo: Controllo operazioni non riuscite

Sommario

Introduzione

In questo documento vengono descritti l'ID 566 e l'ID 4662 dell'evento di protezione e viene descritto come procedere quando si incontrano questi elementi. È possibile che questi eventi si verifichino nei controller di dominio o in un server membro in esecuzione nell'ambito della distribuzione di Umbrella Insights.



Nota: Si tratta di eventi normali e prevedibili. L'azione preferita e supportata consiste nel non eseguire alcuna operazione e ignorare questi eventi.

```
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
```

In alternativa, viene visualizzato l'ID di protezione evento 4662 di Windows 2008.

```
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}
```

Causa

In Windows 2008 è stato introdotto un nuovo insieme di proprietà denominato Private Information che include le proprietà msPKI*. In base alla progettazione, queste proprietà sono protette in modo che solo l'oggetto SELF possa accedervi. È possibile utilizzare il comando DSACLS per verificare le autorizzazioni sull'oggetto in base alle esigenze.

L'analisi della cronologia può indurre a ritenere che questo evento di controllo sia stato causato da un tentativo di scrivere in queste proprietà limitate. Ciò è evidente dal fatto che questi eventi si verificano in base ai criteri di controllo predefiniti di Microsoft che controllano solo le modifiche (scritture) e non i tentativi di lettura delle informazioni da Active Directory.

In caso contrario, l'evento di controllo elenca chiaramente l'autorizzazione richiesta come Accesso di controllo (0x100). Non è tuttavia possibile concedere l'autorizzazione CA (Accesso di controllo) all'insieme di proprietà Informazioni private.

Soluzione

È possibile ignorare questi messaggi. Questo è il risultato del progetto.

Non è consigliabile intraprendere alcuna azione per impedire la visualizzazione di questi eventi. Tuttavia, se si sceglie di implementarle, queste opzioni vengono presentate come alternative. Non è consigliabile adottare una delle due soluzioni: utilizzare a proprio rischio.

Soluzioni

Metodo 1

Disabilitare il controllo in Active Directory disabilitando l'impostazione di controllo del servizio di directory nel criterio controller di dominio predefinito.

Metodo 2

Il processo sottostante che gestisce l'autorizzazione Control Access utilizza l'attributo searchFlags assegnato a ciascuna proprietà, ad esempio: msPKIRoamingTimeStamp). searchFlags è una maschera di accesso a 10 bit. Il bit 8 (contando da 0 a 7 in una maschera di accesso binaria = 10000000 = 128 decimali) viene utilizzato per implementare il concetto di accesso riservato. È possibile modificare manualmente questo attributo nello schema AD e disabilitare l'accesso riservato di queste proprietà. In questo modo si evita che vengano generati i log di controllo degli errori.

Per disabilitare l'accesso riservato per qualsiasi proprietà in AD, utilizzare Modifica ADSI per collegarsi al contesto di denominazione dello schema nel controller di dominio con il ruolo di master schema. Trovare le proprietà appropriate da modificare. Il nome potrebbe essere leggermente diverso da quello visualizzato nell'ID evento 566 o 4662.

Per determinare il valore corretto, sottrarre 128 dal valore searchFlags corrente e immettere il risultato come nuovo valore di searchFlags, quindi 640-128 = 512. Se il valore corrente di searchFlags è < 128, non eseguire alcuna operazione, è possibile che la proprietà sia errata o che Accesso riservato non stia causando l'evento di controllo.

Eseguire questa operazione per ogni proprietà elencata nella descrizione dell'evento con ID 566 o 4662.

Imporre la replica del master schema negli altri controller di dominio, quindi verificare la presenza di nuovi eventi.

Modificare i criteri di controllo del dominio in modo che non eseguano il controllo degli errori nelle proprietà seguenti:

Il problema di questo metodo è che le prestazioni potrebbero peggiorare a causa dell'elevato numero di voci di controllo da aggiungere.

Ulteriori informazioni:

Tradurre GUID in nomi di oggetti è facile con google o con un altro motore di ricerca. Di seguito è riportato un esempio di come eseguire una ricerca con google.

Esempio: sito:microsoft.com 91e647de-d96f-4b70-9557-d63ff4f3ccd8

{91e647de-d96f-4b70-9557-d63ff4f3ccd8} = Set di proprietà Private Information
{6617e4ac-a2f1-43ab-b60c-11fbd1facf05} = Attributo ms-PKI-RoamingTimeStamp

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).