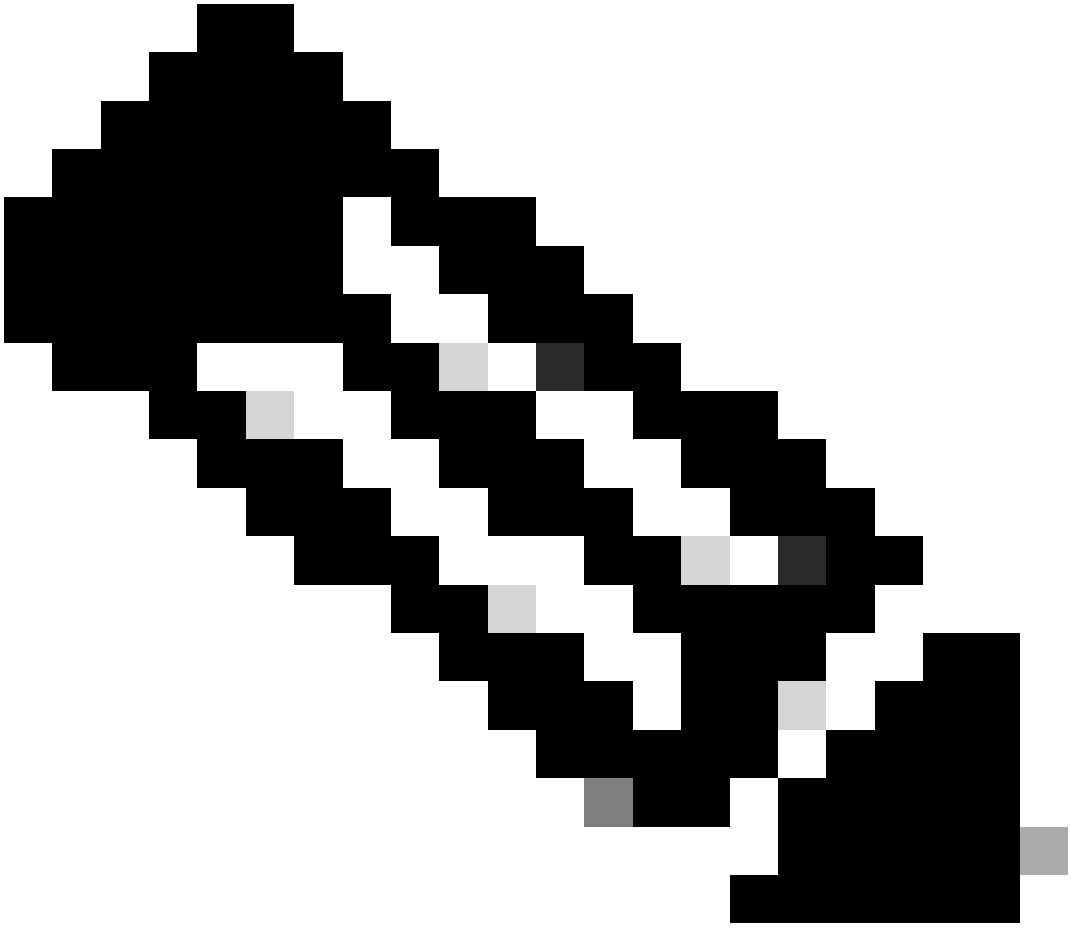
對EventID 4662(Windows 2008)或EventID 566(Windows 2003)進行故障排除 — 型別：失敗稽核

目錄

簡介

本文描述安全事件ID 566和安全事件ID 4662，以及遇到它們時可以採取什麼操作。這些事件可能會在作為Umbrella Insights部署的一部分運行的域控制器或成員伺服器上發生。



附註：這些事件在意料之中，並且是正常的。首選且受支援的操作是不執行任何操作並忽略這些事件。

```
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
```

或者您收到此Windows 2008事件安全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}
```

原因

Windows 2008引入了一個名為Private Information的新屬性集，其中包括msPKI*屬性。按照設計，這些屬性的安全保護方式使得只有SELF對象可以訪問它們。您可以根據需要使用DSACLS命令來驗證對象上的許可權。

粗略調查可能會使您相信此稽核事件是由試圖寫入這些受限制屬性造成的。一個事實證明了這一點：這些事件發生在預設的Microsoft審計策略下，該策略僅審計更改（寫入），而不審計從Active Directory讀取資訊的嘗試。

但是，實際情況並非如此，稽核事件將明確列出請求的許可權作為控制訪問(0x100)。很遺憾，您不能將CA(控制訪問)許可權授予Private Information屬性集。

解決方案

您可以放心地忽略這些消息。這是有計畫的。

建議不要採取任何操作來阻止這些事件的出現。但是，如果您選擇實施它們，則這些選項將作為選項顯示。建議不要使用任何替代方法：自擔風險。

因應措施

方法1

通過禁用預設域控制器策略中的目錄服務稽核設定，禁用Active Directory中的所有稽核。

方法2

管理控制訪問權限的基礎進程使用分配給每個屬性的searchFlags屬性(即：msPKIRoamingTimeStamp)。searchFlags是10位元的存取遮罩。它使用第8位(二進位制訪問掩碼= 10000000 = 128十進位制數從0到7計數)實現機密訪問的概念。您可以在AD方案中手動修改此屬性並禁用這些屬性的機密訪問。這樣將防止生成故障稽核日誌。

要為AD中的任何屬性禁用機密訪問，請使用ADSI Edit附加到擁有架構主角色的DC上的架構命名上下文。找到要修改的相應屬性，其名稱可能與事件ID 566或4662中所示略有不同。

若要確定正確的值，以從當前searchFlags值中減去128，然後將結果輸入為searchFlags的新值，因此640-128 = 512。如果searchFlags的當前值是< 128，則可能具有錯誤的屬性或Confidential Access不會導致稽核事件。

對事件ID 566或4662說明中列出的每個屬性執行此操作。

強制將架構主機複製到其他域控制器，然後檢查是否有新事件。

修改域稽核策略以不稽核這些屬性上的失敗：

這種方法的缺點是效能可能會因需要新增的審計條目數量過多而降低。

更多資訊：

使用google或其他搜尋引擎可以輕鬆將GUID轉換為對象名稱。以下是如何使用google進行搜尋的示例。

範例：站點：microsoft.com 91e647de-d96f-4b70-9557-d63ff4f3ccd8

{91e647de-d96f-4b70-9557-d63ff4f3ccd8} = 專用資訊屬性集
{6617e4ac-a2f1-43ab-b60c-11fbd1facf05} = ms-PKI-RoamingTimeStamp屬性

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。