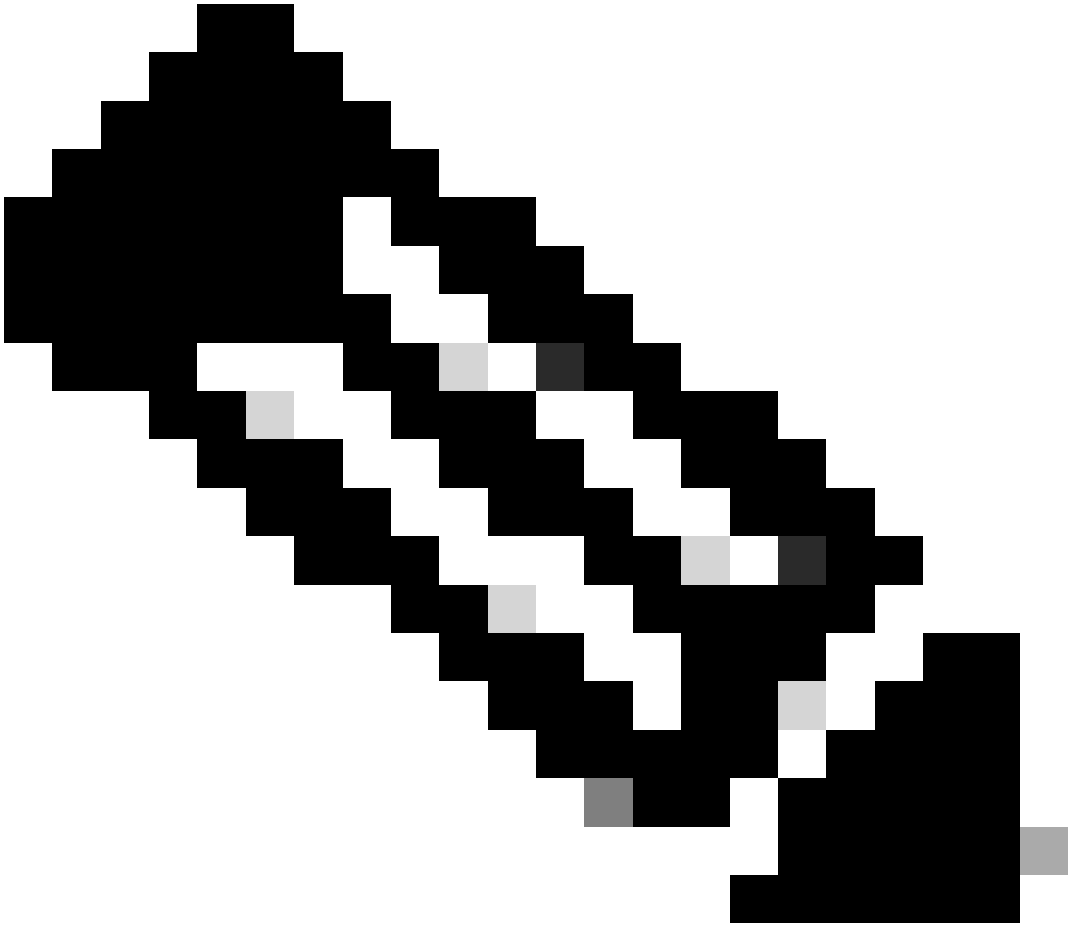
أستكشاف أخطاء EventID 4662 (في Windows 2008) وأ EventID 566 (في Windows 2003) وإصلاحها - النوع: تدقيق الفشل

المحتويات

المقدمة

يصف هذا المستند معرف حدث الأمان 566 ومعرف حدث الأمان 4662، وما هو الإجراء الذي يمكن إتخاذه عند العثور عليهما. يمكن توقع حدوث هذه الأحداث على وحدات التحكم بالمجال وأ خادم عضو يتم تشغيله كجزء من نشر Umbrella Insights.



ملاحظة: هذه الأحداث متوقعة وعادية. والإجراء المفضل والمدعوم هو عدم القيام بأي شيء وتجاهل هذه الأحداث.

```
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
```

أو تتلقى معرف أمان حدث Windows 2008 هذه 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}
```

السبب

صئاصخ نمضتت ةصاخ تامولعم ىمست ةديدج صئاصخ ةعومجم ميدقتب Windows 2008 ماق msPKI*. نمو لالخ التصميم، يتم تأمين هذه الخصائص بطريقة يمكن للكائن الذاتي فقط من الوصول إليها. يمكنك إستخدام الأمر DSACLS للتحقق من الأذونات على الكائن حسب الحاجة.

قد يؤدي التحقيق السريع إلى الاعتقاد بأن حدث التدقيق هذا ناجم عن حواله الكتابة إلى Microsoft تدقيق جهن نمض ثادحألا هذه ثودح ةقيقح نم حضاو اذهو .ةديقعملا صئاصخلا هذه تالواحم تدقيق موقي الو طقف (الكتابة) تاريغتلا تدقيق موقي يذلا يضارتفالا قراءة المعلومات من Active Directory.

ومع ذلك، فإن هذا ليس هو الحال، فحدث التدقيق يسرد بوضوح الإذن المطلوب للتحكم في الوصول (0x100). للأسف، لا يمكنك منح CA (Control Access) الإذن إلى مجموعة خصائص المعلومات الخاصة.

الحل

يمكنك تجاهل هذه الرسائل بأمان. هذا عن طريق التصميم.

إذا كانت خيارات الخيارات هذه تم تقديم، ومع ذلك، هذه الأحداث ظهور لمنع إجراء أي اتخاذ يوصى بأي لا تنفيذها. لا يوصى بأي من الحل البديل: استخدام مسؤول التكتيل الخاصة.

الحلول

الطريقة 1

تعطيل كافة عمليات التدقيق في Active Directory عن طريق تعطيل إعداد تدقيق خدمة Active Directory في وجهة التحكم بالمجال الافتراضي.

الطريقة 2

تستخدم العملية الأساسية التي تريد إذن التحكم بالوصول سمة searchFlags التي يتم تعيينها لكل خاصية (على سبيل المثال: msPKIRoamingTimeStamp). SearchFlags هو قناع بت. وهو يستخدم البت 8 (مع إحتساب من 0 إلى 7 في قناع) ووصول ثنائي = 100000 ووصول 10 = 128 رقما عشريا) لتنفيذ مفهوم الوصول السري. يمكنك تعديل هذه السمة يدويا في AD وتعطيل الوصول السري لهذه الخصائص. وهذا يؤدي بعد ذلك إلى منع إنشاء مخطط سجلات تدقيق الفشل.

لتعطيل الوصول السري لأي خاصية في AD، أستخدم محرر ADSI لإرفاقه بسياق تسمية المخطط في DC الذي يحتفظ بالدور الرئيسي للمخطط. اعثر على الخصائص المناسبة

لتعديلها، قد يكون اسمها مختلفا قليلا عما هو موضح في معرف الحدث 566 أو 4662.

لتحديد القيمة الصحيحة لإدخال طرح 128 من قيمة SearchFlags الحالية، وأدخل النتيجة كقيمة جديدة لـ searchFlags، وبالتالي 640-128 = 512. إذا كانت القيمة الحالية لـ searchFlags < 128 ال تفعل شيئا، فقد يكون لديك الخاصية الخطأ وأ أن الوصول السري ال يتسبب في حدث التدقيق.

قم بذلك لكل خاصية مدرجة في وصف معرف الحدث 566 أو 4662.

فرض النسخ المتماثل لـ "المخطط الرئيسي" على وحدات التحكم بالمجال الأخرى، ثم التحقق من وجود أحداث جديدة.

تعديل نهج تدقيق المجال لعدم تدقيق حالات الفشل على هذه الخصائص:

والجانب السلبي لهذه الطريقة هو أنه قد يتم تقليل الأداء نظرا لارتفاع عدد إدخالات التدقيق التي يلزم إضافتها.

مزيد من المعلومات:

إن ترجمة GUID إلى أسماء الكائنات هو أمر سهل باستخدام محرك البحث جوجل وأ أي محرك بحث آخر. هنا مثال على كيفية البحث باستخدام Google.

مثال: موقع:microsoft.com 91e647de-d96f-4b70-9557-d63ff4f3ccd8

{91e647de-d96f-4b70-9557-d63ff4f3ccd8} = مجموعة خصائص المعلومات الخاصة
{6617e4ac-a2f1-43ab-b60c-11fbd1facf05} = سمة ms-PKI-RoamingTimeStamp

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).