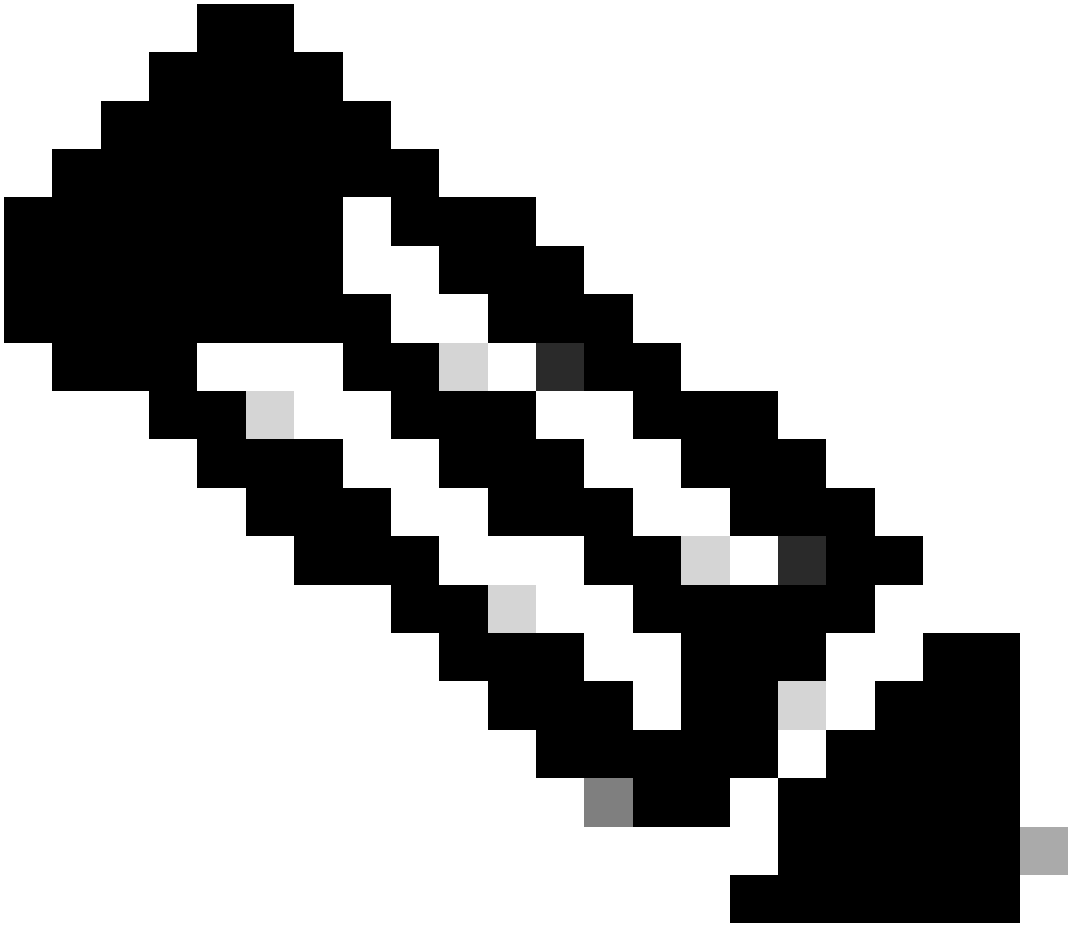
Problembehandlung bei EventID 4662 (Windows 2008) oder EventID 566 (Windows 2003) - Typ: Fehlerüberwachung

Inhalt

Einleitung

In diesem Dokument werden die Sicherheitsereignis-ID 566 und die Sicherheitsereignis-ID 4662 beschrieben. Außerdem wird erläutert, welche Maßnahmen ergriffen werden können, wenn diese erkannt werden. Diese Ereignisse könnten auf Domänencontrollern oder auf einem Mitgliedsserver auftreten, der als Teil der Umbrella Insights-Bereitstellung ausgeführt wird.



Anmerkung: Diese Ereignisse sind zu erwarten und normal. Die bevorzugte und unterstützte Aktion besteht darin, nichts zu tun und diese Ereignisse zu ignorieren.

```
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
```

Alternativ erhalten Sie diese 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}
```

Ursache

In Windows 2008 wurde ein neuer Eigenschaftensatz mit dem Namen Private Information eingeführt, der die msPKI*-Eigenschaften enthält. Diese Eigenschaften sind so gesichert, dass nur das SELF-Objekt auf sie zugreifen kann. Sie können den DSACLS-Befehl verwenden, um die Berechtigungen für das Objekt bei Bedarf zu überprüfen.

Eine Cursoruntersuchung könnte Sie zu der Annahme verleiten, dass dieses Überwachungsereignis durch einen Schreibversuch in diese eingeschränkten Eigenschaften verursacht wird. Dies wird dadurch deutlich, dass diese Ereignisse unter der standardmäßigen Microsoft-Überwachungsrichtlinie auftreten, die nur Änderungen überwacht (Schreibvorgänge) und nicht versucht, Informationen aus Active Directory zu lesen.

Dies ist jedoch nicht der Fall, das Überwachungsereignis listet die angeforderte Berechtigung eindeutig als Steuerungszugriff (0x100) auf. Leider können Sie dem Eigenschaftensatz Private Information die CA-Berechtigung (Steuerungszugriff) nicht gewähren.

Lösung

Sie können diese Meldungen ignorieren. Das ist Absicht.

Es wird nicht empfohlen, Maßnahmen zu ergreifen, um das Auftreten dieser Ereignisse zu verhindern. Diese werden jedoch als Optionen angezeigt, wenn Sie sie implementieren möchten. Es wird keine Problemumgehung empfohlen: auf eigene Gefahr verwenden.

Problemumgehungen

Methode 1

Deaktivieren Sie die gesamte Überwachung in Active Directory, indem Sie die Überwachungseinstellung des Verzeichnisdiensts in der Standardrichtlinie für den Domänencontroller deaktivieren.

Methode 2

Der zugrunde liegende Prozess, der die Zugriffssteuerungsberechtigung verwaltet, verwendet das searchFlags-Attribut, das jeder Eigenschaft zugewiesen ist (d. h.: msPKIRoamingTimeStamp). searchFlags ist eine Zugriffsmaske mit 10 Bit. Es verwendet Bit 8 (von 0 bis 7 in einer binären Zugriffsmaske = 10000000 = 128 dezimal), um das Konzept des vertraulichen Zugriffs zu implementieren. Sie können dieses Attribut im AD-Schema manuell ändern und den vertraulichen Zugriff dieser Eigenschaften deaktivieren. Dadurch wird verhindert, dass

Fehlerüberwachungsprotokolle generiert werden.

Um den vertraulichen Zugriff für eine beliebige Eigenschaft in AD zu deaktivieren, verwenden Sie ADSI Edit, um das Anfügen an den Schemanamenkontext auf dem Domänencontroller mit der Schemamaster-Rolle vorzunehmen. Suchen Sie nach den entsprechenden zu ändernden Eigenschaften. Ihr Name kann sich geringfügig von dem in Ereignis-ID 566 oder 4662 angezeigten Namen unterscheiden.

Um den richtigen Wert zu ermitteln, um 128 vom aktuellen searchFlags-Wert zu subtrahieren und das Ergebnis als neuen Wert von searchFlags einzugeben, also 640-128 = 512. Wenn der aktuelle Wert von searchFlags < 128 ist, haben Sie möglicherweise die falsche Eigenschaft oder Vertraulicher Zugriff verursacht kein Überwachungsereignis.

Führen Sie dies für jede Eigenschaft aus, die in der Ereignis-ID 566 oder 4662 aufgeführt ist.

Erzwingen Sie die Replikation des Schemamasters auf die anderen Domänencontroller, und überprüfen Sie dann, ob neue Ereignisse vorliegen.

Ändern Sie die Domänenüberwachungsrichtlinie, um Fehler bei diesen Eigenschaften nicht zu überwachen:

Der Nachteil dieser Methode ist, dass die Leistung aufgrund der hohen Anzahl von hinzuzufügenden Prüfungseinträgen beeinträchtigt werden kann.

Weitere Informationen:

Die Übersetzung von GUID in Objektnamen ist einfach mit Google oder einer anderen Suchmaschine. Hier ist ein Beispiel, wie Sie mit Google suchen.

Beispiel: Website: microsoft.com 91e647de-d96f-4b70-9557-d63ff4f3ccd8

{91e647de-d96f-4b70-9557-d63ff4f3ccd8} = Eigenschaftsset für private Informationen
{6617e4ac-a2f1-43ab-b60c-11fbd1facf05} = ms-PKI-RoamingTimeStamp-Attribut

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.