La connexion à un bureau distant à l'aide du protocole RDP modifie l'utilisateur associé à une adresse IP

Table des matières

Introduction

Si vous vous connectez à un hôte distant à l'aide du protocole RDP (Remote Desktop Protocol), et que le nom d'utilisateur distant est différent de votre utilisateur, FireSIGHT System modifie l'adresse IP de l'utilisateur qui est associé à votre adresse IP sur FireSIGHT Management Center. Elle entraîne une modification des autorisations de l'utilisateur par rapport aux règles de contrôle d'accès. Vous le remarquerezun utilisateur incorrect est associé à la station de travail. Ce document fournit une solution à ce problème.

Conditions préalables

Cisco vous recommande d'avoir des connaissances sur FireSIGHT System et User Agent.

> Remarque : les informations de ce document ont été créées à partir des périphériques d'un environnement de travaux pratiques spécifique. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Cause première

Ce problème se produit en raison de la manière dont Microsoft Active Directory(AD) enregistre les tentatives d'authentification RDP dans les journaux de sécurité Windows sur le contrôleur de

domaine. AD consigne la tentative d'authentification pour la session RDP sur l'adresse IP de l'hôte d'origine plutôt que sur le point d'extrémité RDP auquel vous vous connectez. Si vous vous connectez à l'hôte distant avec un autre compte d'utilisateur, l'utilisateur associé à l'adresse IP d'origine de votre station de travail sera modifié.

Vérification

Pour vérifier que c'est bien ce qui se passe, vous pouvez vérifier que l'adresse IP de l'événement de connexion de votre station de travail d'origine et de l'hôte distant RDP ont la même adresse IP.

Pour trouver ces événements, vous devez suivre les étapes ci-dessous :

Étape 1 : déterminez le contrôleur de domaine sur lequel votre hôte s'authentifie :

Exécutez la commande suivante :

```
nltest /dsgetdc:<windows.domain.name>
```

Exemple de rapport :

```
C:\Users\WinXP.LAB>nltest /dsgetdc:support.lab
           DC: \\Win2k8.support.lab
      Address: \\192.X.X.X
     Dom Guid: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
     Dom Name: support.lab
  Forest Name: support.lab
 Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
        Flags: PDC GC DS LDAP KDC TIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST
 CLOSE_SITE FULL_SECRET WS 0x4000
The command completed successfully
```

La ligne qui commence par « DC: » sera le nom du contrôleur de domaine et la ligne qui commence par « Address: » sera l'adresse IP.

Étape 2 : Utilisation de la connexion RDP au contrôleur de domaine identifié à l'étape 1

Étape 3 : Accédez à Démarrer > Outils d'administration > Observateur d'événements.

Étape 4 : Explorez vers le bas jusqu'à Windows Logs > Security.

Étape 5 : Filtrez l'adresse IP de votre station de travail en cliquant sur Filtrer le journal actuel, en cliquant sur l'onglet XML, puis sur Modifier la requête.

Étape 6 : Entrez la requête XML suivante, en remplaçant votre adresse IP par **<ip address>**

```
<QueryList>
<Query Id="0" Path="Security">
<Select Path="Security">
*[EventData[Data[@Name='IpAddress'] and(Data='<IP address>')]]
</Select>
</Query>
</QueryList>
```

Étape 7 : Cliquez sur l'événement de connexion et cliquez sur l'onglet Détails.

Exemple de résultat :

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
<Provider Name="Microsoft-Windows-Security-Auditing"
Guid="{XXXXXXXX-XXX-XXXX-XXX-XXXXXXXXXXXX}"/>
<EventID>4624</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2014-07-22T20:35:12.750Z" />
<EventRecordID>4130857</EventRecordID>
<Correlation />
<Execution ProcessID="576" ThreadID="704" />
<Channel>Security</Channel>
<Computer>WIN2k8.Support.lab</Computer>
<Security />
</System>
- <EventData>
<Data Name="SubjectUserSid">S-1-0-0</Data>
<Data Name="SubjectUserName">-</Data>
<Data Name="SubjectDomainName">-</Data>
<Data Name="SubjectLogonId">0x0</Data>
<Data Name="TargetUserSid">S-X-X-XX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXX-XXXX</Data>
<Data Name="TargetUserName">WINXP-SUPLAB$</Data>
<Data Name="TargetDomainName">SUPPORT</Data>
<Data Name="TargetLogonId">0x13c4101f</Data>
<Data Name="LogonType">3</Data>
<Data Name="LogonProcessName">Kerberos</Data>
<Data Name="AuthenticationPackageName">Kerberos</Data>
<Data Name="WorkstationName" />
<Data Name="LogonGuid">{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">-</Data>
<Data Name="KeyLength">0</Data>
```

```
<Data Name="ProcessId">0x0</Data>
<Data Name="ProcessName">-</Data>
<Data Name="IpAddress">192.0.2.10</Data>
<Data Name="IpPort">2401</Data>
</EventData>
```

Effectuez ces mêmes étapes après vous être connecté via RDP et vous remarquerez que vous recevrez un autre événement d'ouverture de session (ID d'événement 4624) avec la même adresse IP que celle indiquée par la ligne suivante à partir des données XML de l'événement d'ouverture de session de l'ouverture de session d'origine :

```
<Data Name="IpAddress">192.x.x.x</Data>
```

Solution

Pour limiter ce problème, si vous utilisez User Agent 2.1 ou version ultérieure, vous pouvez exclure tous les comptes que vous souhaitez
à utiliser principalement pour le protocole RDP dans la configuration de l'agent utilisateur.

Étape 1 : Connectez-vous à l'hôte User Agent.

Étape 2 : Lancez l'interface utilisateur de l'agent utilisateur.

Étape 3 : Cliquez sur l'onglet Noms d'utilisateur exclus.

Étape 4 : Entrez tous les noms d'utilisateur que vous souhaitez exclure.

Étape 5 : Cliquez sur Save.

Les utilisateurs entrés dans cette liste ne génèrent pas d'événements de connexion sur FireSIGHT Management Center et ne sont pas
associés aux adresses IP.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.