Fazer login em um desktop remoto usando RDP altera o usuário associado a um endereço IP

Contents

Introduction

Se você fizer login em um host remoto usando o Remote Desktop Protocol (RDP) e o nome de usuário remoto for diferente do seu usuário, o FireSIGHT System alterará o endereço IP do usuário associado ao seu endereço IP no FireSIGHT Management Center. Causa uma alteração nas permissões do usuário em relação às regras de Controle de Acesso. Você perceberáO usuário incorreto está associado à estação de trabalho. Este documento fornece uma solução para esse problema.

Prerequisites

A Cisco recomenda que você tenha conhecimento sobre o sistema FireSIGHT e o agente de usuário.

> **Observação**: as informações neste documento foram criadas a partir dos dispositivos em um ambiente de laboratório específico. 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.

Causa raiz

Esse problema ocorre devido ao modo como o Microsoft Ative Diretory(AD) registra as tentativas de autenticação RDP nos Logs de Segurança do Windows no Controlador de Domínio. O AD registra a tentativa de autenticação para a sessão RDP com base no endereço IP do host de origem em vez do ponto de extremidade RDP ao qual você está se conectando. Se você estiver

efetuando login no host remoto com uma conta de usuário diferente, isso alterará o usuário associado ao endereço IP da sua estação de trabalho original.

Verificação

Para verificar se isso é o que está ocorrendo, você pode verificar se o endereço IP do evento de logon de sua estação de trabalho original e o host remoto RDP têm o mesmo endereço IP.

Para localizar esses eventos, você precisará seguir as etapas abaixo:

Etapa 1: Determine o controlador de domínio no qual o host está autenticando:

Execute o seguinte comando:

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

Saída de exemplo:

```
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
```

A linha que inicia o "DC:" será o nome do controlador de domínio e a linha que inicia o "Endereço:" será o endereço IP.

Etapa 2: Usando o registro RDP no controlador de domínio identificado na Etapa 1

Etapa 3: vá para **Iniciar > Ferramentas Administrativas > Visualizador de Eventos**.

Etapa 4: Vá até **Logs do Windows > Segurança**.

Etapa 5: filtre o endereço IP de sua estação de trabalho clicando em Filtrar log atual, clicando na guia XML e clicando em editar consulta.

Etapa 6: digite a seguinte consulta XML, substituindo **<endereço IP>** pelo seu endereço IP

```
<QueryList>
```

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

Etapa 7: clique no **Evento de logon** e clique na guia **Detalhes**.

Um exemplo de saída:

```
- <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>
```

Conclua estas mesmas etapas depois de fazer logon via RDP e você perceberá que receberá outro evento de logon (ID de Evento 4624) com o mesmo endereço IP mostrado pela seguinte linha dos dados XML do evento de logon do logon original:

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

Solução

Para atenuar esse problema, se estiver usando o Agente de usuário 2.1 ou superior, você poderá excluir qualquer conta que
estar usando principalmente para RDP na Configuração do agente do usuário.

Etapa 1: Efetue login no Host do agente do usuário.

Etapa 2: Inicie a interface do usuário do agente do usuário.

Etapa 3: clique na guia **Nomes de usuário excluídos**.

Etapa 4: digite todos os nomes de usuário que deseja excluir.

Etapa 5: Clique em **Salvar**.

Os usuários inseridos nessa lista não geram eventos de logon no FireSIGHT Management Center e não podem
associados aos endereços IP.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.