# RDP を使用したリモート デスクトップへのログインによる IP アドレスに関連付けられているユーザの変更

## 内容



## 概要

Remote Desktop Protocol ( RDP ) を使用してリモート ホストにログインした場合で、リモート ユーザ名がユーザと異なるときは、FireSIGHT システムが、FireSIGHT Management Center の IP アドレスに関連付けられているユーザの IP アドレスを変更します。これにより、アクセス制御ルールに関するユーザの権限が変更されます。君は気づくだろう正しくないユーザがワークステーションに関連付けられている。このドキュメントでは、この問題のソリューションについて説明しています。

## 前提条件

FireSIGHT システムとユーザ エージェントに関する知識があることが推奨されます。

> **注**：このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 根本原因

この問題は、Microsoft Active Directory ( AD ) によるドメイン コントローラの Windows セキュリティ ログに対する RDP 認証試行の記録方法によって発生します。AD では、接続している RDP エンドポイントではなく、発信元ホストの IP アドレスと照合して RDP セッションの認証試

行を記録します。別のユーザ アカウントを使用してリモート ホストにログインすると、元のワークステーション IP アドレスと関連付けられたユーザが変更されます。

# 確認

何が発生しているかを確認するには、元のワークステーションからのログオン イベントの IP アドレスと RDP リモート ホストに同じ IP アドレスがあることを確認します。

これらのイベントを検出するには、次のステップに従う必要があります。

ステップ1：ホストが認証を行うドメインコントローラを決定します。

次のコマンドを実行します。

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

出力例：

```
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
```

「DC:」で始まる行がドメインコントローラの名前になり、「Address:」で始まる行がIPアドレスになります。

ステップ2：ステップ1で特定したドメインコントローラへのRDPログの使用

ステップ3:[Start] > [Administrative Tools] > [Event Viewer] に移動します。

ステップ4:[Windows Logs] > [Security] にドリルダウンします。

ステップ5:[Filter Current Log（現在のログをフィルタ）]をクリックし、[XML]タブをクリックし、[edit query（クエリの編集）]をクリックして、ワークステーションのIPアドレスをフィルタリングします。

ステップ6：次のXMLクエリーを入力し、<ip address>をIPアドレスに置き換えます

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

ステップ7:[Logon Event] をクリックし、[Details] タブをクリックします。

出力例：

```
- <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>
```

RDP でのログイン後に上述のステップを実行すると、元のログオンのログオン イベント XML データの次の行で示されているものと同じ IP アドレスを持つ別のログオン イベント（イベント ID 4624）を受信することがわかります。

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

# 解決方法

この問題を軽減するには、User Agent 2.1 以上をご使用であれば、
User Agent の設定で RDP に主に使用するアカウントを除外します。

ステップ1：ユーザエージェントホストにログインします。

ステップ2:User Agentユーザインターフェイスを起動します。

ステップ3:[Excluded Usernames] タブをクリックします。

ステップ4：除外するすべてのユーザ名を入力します。

ステップ5:[Save] をクリックします。

このリストに入力したユーザは、FireSIGHT Management Center でログイン イベントを生成せず、
IP アドレスに関連付けられません。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。