コンピュータのマシン名または NULL ユーザ名がアクセス ログに記録されるのはなぜですか。

内容

質問

- コンピュータのマシン名または NULL ユーザ名がアクセス ログに記録されるのはなぜですか。
- 以降の認証で除外対象となるように、ワークステーションまたは NULL クレデンシャルを使用して要求を識別するには、どうすればよいですか。

環境

- Cisco Web Security Appliance（WSA）（すべてのバージョン）
- IP サロゲートを使用した認証スキーム NTLMSSP
- Windows Vista 以降のデスクトップおよびモバイル Microsoft オペレーティング システム

症状

WSA が一部のユーザからの要求をブロックする、または予期しない動作を見せる。
アクセス ログに、ユーザ ID ではなくコンピュータのマシン名または NULL ユーザ名とドメインが記録される。

この問題は、次のイベントの後に自動的に解決します。

- サロゲート タイムアウト（サロゲート タイムアウトのデフォルト値は 60 分 です）
- プロキシ プロセスの再起動（CLI コマンド > *diagnostic* > *proxy* > *kick*）
- 認証キャッシュのクリア（CLI コマンド > *authcache* > *flushall*）

背景説明

Microsoft オペレーティング システムの最近のバージョンでは、ユーザが実際にアプリケーションにログインしなくても、要求をインターネットに送信できるようなっています。これらの要求を WSA が受信して、認証が必要になった場合、クライアント ワークステーションで認証に使用するユーザ クレデンシャルがないため、代わりにコンピュータのマシン名が使用されます。

WSA は提供されたマシン名を取り、Active Directory（AD）に転送して検証させます。

認証が有効であれば、WSA は IP サロゲートを作成してマシンのワークステーション名をワークステーションの IP アドレスにバインドします。同じ IP から送信される以降の要求は、このサロゲートを使用します。つまり、ワークステーション名を使用することになります。

ワークステーション名がどの AD グループのメンバーにもなっていない場合、期待されるアクセス ポリシーはトリガーされないため、要求がブロックされます。この問題は、サロゲートのタイムアウトが発生して、認証の更新が必要になるまで続きます。その時点で、実際のユーザがログインして、有効なクレデンシャルが使用可能になると、その情報を利用して新しい IP サロゲートが作成されるため、以降の要求は期待されるアクセス ポリシーと一致することになります。

もう 1 つのシナリオは、アプリケーションが有効なマシン クレデンシャルではなく、無効なクレデンシャル（NULL ユーザ名および NULL ドメイン）を送信した場合です。これは認証失敗と見なされ、要求がブロックされます。または、ゲスト ポリシーが有効になっている場合は、失敗した認証が「ゲスト」と見なされます。

ワークステーション名は、**$ に続く @DOMAIN で終わるので、アクセス ログで CLI コマンド grep を使用して $@** を検索することで簡単にワークステーション名をトレースできます。詳細については、次の例を参照してください。

```
> grep $@ accesslogs

1332164800.0000 9 10.20.30.40 TCP_DENIED/403 5608 GET http://www.someURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_WEBCAT_11-DefaultGroup-Internet-NONE-NONE-
NONE-NONE <-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

上記の行は、IP アドレス 10.20.30.40 を対象に作成された IP サロゲートと、マシン名 **gb0000d01$**

マシン名を送信した要求を見つけるには、この特定の IP アドレスに対応するワークステーション名の最初のオカレンスを特定する必要があります。それには、次の CLI コマンドを使用します。

```
> grep 10.20.30.40 -p accesslogs
```

ワークステーション名の最初の出現の結果を検索します。3つの最初の要求は、一般に、次に示すように、NTLMシングルサインオン(NTLMSSP/NTLMSSP)ハンドシェイクとして認識されます。

```
1335248044.836 0 10.20.30.40 TCP_DENIED/407 1733 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.839 0 10.20.30.40 TCP_DENIED/407 483 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.845 10 10.20.30.40 TCP_DENIED/403 2357 GET http://SomeOtherURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_ADMIN_PROTOCOL_11-DefaultGroup-DefaultGroup-
DefaultGroup-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

トラブルシューティングを行う際は、これら 3 つの要求が同じ URL を対象としていること、お

よび自動 NTLMSSP ハンドシェイクであることを示す非常に短い間隔でログに記録されていることを確認します。

上記の例では、前述の要求は、明示的な要求である場合は HTTP 応答コード 407（プロキシ認証が必要）で記録され、透過的な要求である場合は HTTP 応答コード 401（未認証）で記録されます。

AsyncOS 7.5.0 以降には、マシン クレデンシャルに異なるサロゲート タイムアウトを定義できる新しい機能が用意されています。これは、次のコマンドを使用して設定できます。

```
> advancedproxyconfigChoose a parameter group:- AUTHENTICATION - Authentication
related parameters- CACHING - Proxy Caching related parameters- DNS - DNS related
parameters- EUN - EUN related parameters- NATIVEFTP - Native FTP related parameters-
FTPOVERHTTP - FTP Over HTTP related parameters- HTTPS - HTTPS related parameters-
SCANNING - Scanning related parameters- WCCP - WCCPv2 related parameters-
MISCELLANEOUS - Miscellaneous proxy relatedparameters[]> AUTHENTICATION...Enter the
surrogate timeout.[3600]>Enter the surrogate timeout for machine credentials.[10]>.
```

送信された NULL クレデンシャルを受け取る要求を検出し、無効なクレデンシャルを送信している URL またはユーザ エージェントを見つけて、それらを認証から除外する場合と同じ手順を使用できます。

認証から URL を除外する

この要求が偽のサロゲートを作成することを防ぐために、URLを認証から除外する必要があります。または、URLを認証から除外する代わりに、要求自体を送信するアプリケーションを認証から除外し、アプリケーションの認証を免除します。それには、WAS のアクセス ログ サブスクリプションでオプションの [Custom Fields] **にパラメータ %u を追加して、アクセス ログに記録するユーザ エージェントを追加します。**ユーザ エージェントを特定した後、そのエージェントを認証から除外する必要があります。