# Por que os nomes das máquinas de computador ou os nomes de usuário NULL estão registrados nos registros de acesso?

## Contents



## Pergunta

- Por que os nomes das máquinas de computador ou os nomes de usuário NULL estão registrados nos registros de acesso?
- Como você identifica as solicitações usando a estação de trabalho ou credenciais NULL para isenção de autenticação posterior?

## Ambiente

- Cisco Web Security Appliance (WSA) - todas as versões
- Esquema de autenticação NTLMSSP com substitutos de IP
- Windows Vista e sistemas operacionais Microsoft para desktops e portáteis mais recentes

## Sintomas

O WSA bloqueia solicitações de alguns usuários ou se comporta inesperadamente.
Os registros de acesso mostram nomes de computadores ou nome de usuário e domínio NULL em vez de IDs de usuário.

O problema se resolve após:

- Substitui o tempo limite (o valor padrão para o tempo limite de substituição é 60 minutos)
- Reiniciando o processo de proxy (comando CLI > *diagnóstico* > *proxy* > *chute*)
- Limpando cache de autenticação (comando CLI > *authcache* > *flat*)

## Informações de Apoio

Em versões recentes do Sistema Operacional Microsoft, não é necessário que um usuário real esteja mais conectado para que os aplicativos enviem solicitações à Internet. Quando essas

solicitações são recebidas pelo WSA e solicitadas para autenticação, nenhuma credencial de usuário está disponível para uso na autenticação pela estação de trabalho do cliente, que pode tomar o nome da máquina do computador como substituto.

O WSA pegará o nome da máquina fornecido e o encaminhará para o Ative Diretory (AD) que o valida.

Com uma autenticação válida, o WSA cria um substituto IP que vincula o nome da estação de trabalho da máquina ao endereço IP da estação de trabalho. Outras solicitações provenientes do mesmo IP usarão o substituto e, portanto, o nome da estação de trabalho.

Com o nome da estação de trabalho não sendo membro de nenhum grupo do AD, as solicitações podem não disparar a Diretiva de Acesso esperada e, portanto, ser bloqueadas. O problema persiste até que o substituto tenha expirado e a autenticação tenha que ser renovada. Desta vez, com um usuário conectado e credenciais de usuário válidas disponíveis, um novo substituto de IP será criado com essas informações e outras solicitações corresponderão à política de acesso esperada.

Outro cenário observado é quando os aplicativos enviam credenciais inválidas (nome de usuário NULL e domínio NULL) e NÃO credenciais de máquina válidas. Isso é considerado uma falha de autenticação e será bloqueado ou, se as políticas de convidado estiverem ativadas, o áudio com falha será considerado como um "convidado".

O nome da estação de trabalho termina com um **$** seguido por **@DOMAIN**, o que facilita o rastreamento de nomes de estações de trabalho usando o comando CLI **grep** nos registros de acesso para **$@**. Consulte o exemplo abaixo para obter esclarecimentos.

```
> 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,-,"-","-"> -
```

A linha acima mostra um exemplo de um substituto de IP já criado para o endereço IP 10.20.30.40 e o nome da máquina **gb0000d01$.**

Para localizar a solicitação que enviou o nome da máquina, a primeira ocorrência do nome da estação de trabalho para o endereço IP específico deve ser identificada. O seguinte comando CLI realiza isso:

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

Pesquise o resultado da primeira ocorrência do nome da estação de trabalho. As três primeiras solicitações são geralmente reconhecidas como handshake NTLM Single-Sin-On (NTLMSSP/NTLMSSP), conforme descrito aqui e mostrado no exemplo abaixo:

```
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,-,"-","-"> -
```

Ao solucionar problemas, certifique-se de que essas solicitações sejam para o mesmo URL e estejam registradas em um intervalo de tempo muito curto indicando que é um handshake NTLMSSP automatizado.

No exemplo acima, as solicitações anteriores são registradas com o código de resposta HTTP 407 (Autenticação de proxy necessária) para solicitações explícitas, enquanto as solicitações transparentes seriam registradas com o código de resposta HTTP 401 (Não autenticado).

Há um novo recurso disponível no AsyncOS 7.5.0 e posterior, no qual você pode definir um intervalo substituto diferente para credenciais da máquina. Ele pode ser configurado usando o seguinte comando:

```
> 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]>.
```

Você pode usar as mesmas etapas para detectar quais solicitações obtêm as credenciais NULL enviadas e descobrir qual URL ou Agente de usuário está enviando as credenciais inválidas e as isenta da autenticação.

### Isentando a URL da autenticação

Para evitar que essa solicitação faça com que o substituto falso seja criado, o URL deve ser isento de autenticação.Ou, em vez de isentar o URL da autenticação, você pode decidir isentar o aplicativo que envia a própria solicitação da autenticação, certificando-se de obter quaisquer solicitações para que o aplicativo seja isento de autenticação. Isso é possível adicionando o Agente de usuário a ser registrado nos registros de acesso adicionando o parâmetro adicional **%u** nos **Campos personalizados** opcionais na assinatura do log de acesso do WSA. Depois de identificar o Agente de usuário, ele deve ser isento de autenticação.