Acesso de administrador TACACS ao exemplo de configuração convirgido dos controladores do Wireless LAN do acesso

Índice

Introdução

Este documento fornece um exemplo de configuração do protocolo tacacs+ (TACACS+) em Cisco convirgiu o controlador do Wireless LAN do acesso (WLC) 5760/3850/3650 para o CLI e o GUI. Este documento igualmente fornece algumas pontas básicas para pesquisar defeitos a configuração.

O TACACS+ é um protocolo cliente/servidor que forneça a Segurança centralizada para os usuários que tentam ganhar o acesso de gerenciamento a um roteador ou a um servidor do acesso de rede. O TACACS+ proporciona estes serviços do Authentication, Authorization, and Accounting (AAA):

- Autenticação dos usuários que tentam entrar ao equipamento de rede
- Autorização determinar que nível de usuários do acesso deve ter
- Explicar para manter-se a par de todas as mudanças o usuário faz

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como configurar WLC e Lightweight Access Points (regaços) para a operação básica
- Métodos de pouco peso do protocolo (LWAPP) e da segurança Wireless do Access point
- Conhecimento básico do RAIO e do TACACS+
- Conhecimento básico da configuração ACS de Cisco

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WLC 5760 que executa a liberação 3.3.3 do ® XE do Cisco IOS
- Access Control Server (ACS) 5.2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Configurações

Este é um processo em duas etapas:

- Configuração no WLC
- Configuração no server RADIUS/TACACS

Configuração no WLC

1. Defina o servidor de TACACS no WLC. Assegure-se de que você configure o exato o mesmo segredo compartilhado no TACACS.
```
tacacs-server host 10.106.73.71 key Cisco123
tacacs server ACS
 address ipv4 10.106.102.50
 key Cisco123
 timeout 10
```
2. Configurar os grupos de servidor e trace o server configurado na etapa precedente.
```
aaa group server tacacs+ ACS
 server name ACS
!
```
3. Configurar a autenticação e as políticas da autorização para o acesso de administrador. Nisto, você reserva o grupo TACACS seguido pelo local que é a reserva.
```
aaa authentication login Admin_Access group ACS local
```

```
aaa authorization exec Admin_Access group ACS local
```

4. Aplique a política à linha vty e ao HTTP.

```
line vty 0 4
 authorization exec Admin_Access
 login authentication Admin_Access
line vty 5 15
 exec-timeout 0 0
 authorization exec Admin_Access
 login authentication Admin_Access
```

5. Aplique o mesmos ao HTTP.

```
ip http server
ip http authentication aaa login-authentication Admin_Access
ip http authentication aaa exec-authorization Admin_Access
```

Configuração no ACS

1. Escolha **recursos de rede > dispositivos de rede e clientes de AAA** a fim adicionar o WLC como o cliente de AAA para o TACACS no ACS. Assegure-se de que o segredo compartilhado configurado aqui combine esse configurado no WLC.
2. Escolha **usuários e a identidade armazena > identidade interna armazena > usuários** a fim definir o usuário para o acesso de administrador.
3. Escolha **elementos da política > autorização e permissões > de administração > de shell do dispositivo perfis** a fim ajustar os níveis de privilégio a 15.
4. Escolha o **dispositivo Admin das políticas de acesso > dos serviços > do padrão do acesso** a fim permitir os protocolos exigidos.
5. Escolha o **dispositivo das políticas de acesso > dos serviços > do padrão do acesso Admin > identidade** a fim criar uma identidade para o administrador do dispositivo que permite usuários internos com opções de autenticação.
6. Escolha o **dispositivo das políticas de acesso > dos serviços > do padrão do acesso Admin > autorização** a fim permitir o perfil da autorização Priv15 criado em etapa 3. O cliente com a identidade passada (usuários internos) é posto aqui sobre o perfil Priv15.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Abra um navegador e incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do interruptor. Os indicadores exigidos autenticação da alerta. Incorpore as credenciais do usuário do grupo a fim entrar ao dispositivo.

A fim verificar o acesso do telnet/SSH, o telnet/SSH ao endereço IP de Um ou Mais Servidores Cisco ICM NT do interruptor e incorporar as credenciais.

Isto é indicado para o registro ACS.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Note: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Inscreva o **comando debug tacacs** a fim pesquisar defeitos sua configuração.

```
debug tacacs

*May 14 23:11:06.396: TPLUS: Queuing AAA Authentication request 4775 for processing
*May 14 23:11:06.396: TPLUS(000012A7) login timer started 1020 sec timeout
*May 14 23:11:06.396: TPLUS: processing authentication continue request id 4775
*May 14 23:11:06.396: TPLUS: Authentication continue packet generated for 4775
*May 14 23:11:06.396: TPLUS(000012A7)/0/WRITE/962571D4: Started 10 sec timeout
*May 14 23:11:06.396: TPLUS(000012A7)/0/WRITE: wrote entire 25 bytes request
*May 14 23:11:06.398: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:06.398: TPLUS(000012A7)/0/READ: read entire 12 header bytes (expect
16 bytes data)
*May 14 23:11:06.398: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:06.398: TPLUS(000012A7)/0/READ: read entire 28 bytes response
*May 14 23:11:06.398: TPLUS(000012A7)/0/962571D4: Processing the reply packet
*May 14 23:11:06.398: TPLUS: Received authen response status GET_PASSWORD (8)
*May 14 23:11:08.680: TPLUS: Queuing AAA Authentication request 4775 for processing
*May 14 23:11:08.680: TPLUS(000012A7) login timer started 1020 sec timeout
*May 14 23:11:08.680: TPLUS: processing authentication continue request id 4775
*May 14 23:11:08.680: TPLUS: Authentication continue packet generated for 4775
*May 14 23:11:08.680: TPLUS(000012A7)/0/WRITE/962571D4: Started 10 sec timeout
*May 14 23:11:08.680: TPLUS(000012A7)/0/WRITE: wrote entire 25 bytes request
*May 14 23:11:08.687: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.687: TPLUS(000012A7)/0/READ: read entire 12 header bytes (expect
6 bytes data)
*May 14 23:11:08.687: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.687: TPLUS(000012A7)/0/READ: read entire 18 bytes response
*May 14 23:11:08.687: TPLUS(000012A7)/0/962571D4: Processing the reply packet
*May 14 23:11:08.687: TPLUS: Received authen response status PASS (2)
*May 14 23:11:08.687: TPLUS: Queuing AAA Authorization request 4775 for processing
*May 14 23:11:08.687: TPLUS(000012A7) login timer started 1020 sec timeout
*May 14 23:11:08.687: TPLUS: processing authorization request id 4775
*May 14 23:11:08.687: TPLUS: Protocol set to None .....Skipping
*May 14 23:11:08.687: TPLUS: Sending AV service=shell
*May 14 23:11:08.687: TPLUS: Sending AV cmd*
*May 14 23:11:08.687: TPLUS: Authorization request created for 4775(surbg123)
*May 14 23:11:08.687: TPLUS: using previously set server 10.106.102.50 from
group SURBG_ACS
*May 14 23:11:08.688: TPLUS(000012A7)/0/NB_WAIT/93C63F04: Started 10 sec timeout
*May 14 23:11:08.690: TPLUS(000012A7)/0/NB_WAIT: socket event 2
*May 14 23:11:08.690: TPLUS(000012A7)/0/NB_WAIT: wrote entire 61 bytes request
*May 14 23:11:08.690: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.690: TPLUS(000012A7)/0/READ: Would block while reading
*May 14 23:11:08.696: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.696: TPLUS(000012A7)/0/READ: read entire 12 header bytes (expect
18 bytes data)
*May 14 23:11:08.696: TPLUS(000012A7)/0/READ: socket event 1
*May 14 23:11:08.696: TPLUS(000012A7)/0/READ: read entire 30 bytes response
*May 14 23:11:08.696: TPLUS(000012A7)/0/93C63F04: Processing the reply packet
*May 14 23:11:08.696: TPLUS: Processed AV priv-lvl=15
*May 14 23:11:08.696: TPLUS: received authorization response for 4775: PASS
```