Atribuição do VLAN dinâmico com servidor Radius ACS 5.2 e exemplo de configuração WLC

Índice

Introdução

Este documento introduz o conceito da atribuição da VLAN dinâmica. Ele também descreve como configurar o Controller de LAN Wireless (WLC) e um servidor RADIUS, Access Control Server (ACS) que executa a versão 5.2, para atribuir clientes de LAN Wireless (WLAN) a uma VLAN específica de forma dinâmica.

Pré-requisitos

Requisitos

Certifique-se de que você cumpre estas exigências antes que você tente esta configuração:

- Tenha um conhecimento básico do WLC e do Lightweight Access Points (os regaços)
- Tenha um conhecimento funcional do servidor AAA
- Tenha um conhecimento completo das redes Wireless e das edições de segurança Wireless

Componentes Utilizados

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

- Cisco 5508 WLC que executa a versão de firmware 7.0.220.0
- REGAÇO do Cisco 3502 Series
- Suplicante nativo de Microsoft Windows 7 com versão do driver 14.3 de Intel 6300-N
- Cisco Secure ACS que executa a versão 5.2
- Cisco 3560 Series Switch

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.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Atribuição do VLAN dinâmico com um servidor Radius

Na maioria de sistemas de WLAN, cada WLAN tem uma política estática que se aplica a todos os clientes associados com um Service Set Identifier (SSID), ou o WLAN na terminologia do controlador. Embora poderoso, este método tem limitações porque exige que os clientes se associem com os diferentes SSID para herdar diferentes QoS e políticas de segurança.

Mas a solução de Cisco WLAN suporta identidades na rede. Isto permite a rede anuncie um único SSID, mas permite que os usuários específicos herdem QoS diferente, atributos VLAN, e/ou políticas de segurança baseadas nas credenciais do usuário.

A atribuição da VLAN dinâmica é um recurso que coloca um usuário wireless em uma VLAN específica baseado nas credenciais fornecidas pelo usuário. Esta tarefa de atribuir usuários a um VLAN específico é segurada por um servidor de autenticação RADIUS, tal como o Cisco Secure ACS. Isto pode ser usado, por exemplo, para permitir que o host wireless permaneça na mesma VLAN enquanto ele se desloca em uma rede no campus.

Em consequência, quando um cliente tenta associar a um REGAÇO registrado com um controlador, o REGAÇO passa as credenciais do usuário ao servidor Radius para a validação. Quando a autenticação é bem sucedida, o servidor Radius passa determinados atributos da

Internet Engineering Task Force (IETF) ao usuário. Estes atributos RADIUS decidem a ID da VLAN que deve ser atribuído ao cliente wireless. A SSID (WLAN, em termos do WLC) do cliente não importa porque o usuário sempre recebe esta identificação predeterminada da VLAN.

Os atributos do usuário do RADIUS usados para a atribuição de ID da VLAN são:

- IETF 64 (tipo de túnel) - Ajuste isto ao **VLAN**.
- IETF 65 (tipo médio do túnel) - ajuste isto a **802**.
- IETF 81 (grupo privado ID do túnel) - ajuste isto ao ID de VLAN.

A ID da VLAN tem 12 bits, e um valor entre 1 e 4094, inclusive. Como a ID de Grupo Privado do Túnel é do tipo string, como definido na RFC2868 para uso com a IEEE 802.1X, o valor de número inteiro da ID de VLAN é codificado como uma string. Quando estes atributos de túnel são enviados, é necessário preencher o campo Tag.

Como é explicado na RFC2868 , seção 3.1: **O campo Tag tem um octeto de comprimento e permite agrupar no mesmo pacote atributos que se referem ao mesmo túnel.** Os valores válidos para este campo são de 0x01 a 0x1F, inclusive. Se o campo Tag não for utilizado, ele deve ser zero (0x00). Consulte na RFC 2868 mais informações sobre todos os atributos de RADIUS.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

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

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Estes são os detalhes de configuração dos componentes usados neste diagrama:

- O endereço IP de Um ou Mais Servidores Cisco ICM NT do server ACS (RAIO) é 192.168.150.24.
- O Gerenciamento e o endereço da relação do gerenciador AP do WLC são 192.168.75.44.
- Os servidores DHCP endereçam 192.168.150.25.
- O VLAN 253 e o VLAN 257 são usados durante todo esta configuração. Student-1 é configurado para a colocação em VLAN 253 e Teacher-1 está configurado para a colocação em VLAN 257 pelo servidor Radius quando ambos os usuários conectam ao mesmo SSID “goa”.VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.1VLAN 257: 192.168.157.x/24. Gateway: 192.168.157.1VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1
- Este documento usa o 802.1x com o PEAP como o mecanismo de segurança.**Note**: A Cisco recomenda que você use métodos de autenticação avançados, tais como o EAP-FAST e a autenticação EAP-TLS, para proteger a WLAN.

Hipóteses

- O Switches é configurado para toda a camada 3 VLAN.

- O servidor DHCP é atribuído um escopo de DHCP.
- A Conectividade da camada 3 existe entre todos os dispositivos na rede.
- O REGAÇO é juntado já ao WLC.
- Cada VLAN tem a máscara de /24.
- O ACS 5.2 tem um certificado auto-assinado instalado.

Passos de configuração

Esta configuração é separada em três etapas de nível elevado:

1. Configurar o servidor Radius.
2. Configurar o WLC.
3. Configurar a utilidade do cliente Wireless.

Configurar o servidor Radius

A configuração do servidor Radius é dividida em quatro etapas:

1. Configurar recursos de rede.
2. Configurar usuários.
3. Defina elementos da política.
4. Aplique políticas de acesso.

O ACS 5.x é um sistema de controle de acesso com base em política. Isto é, o ACS 5.x usa um modelo baseado em regras da política em vez do modelo grupo-baseado usado nas versões 4.x.

O modelo baseado em regras da política ACS 5.x fornece um controle de acesso mais poderoso e mais flexível comparado à aproximação grupo-baseada mais velha.

No modelo grupo-baseado mais velho, um grupo define a política porque contém e amarra junto três tipos de informação:

- Informação de identidade - Esta informação pode ser baseada na sociedade em grupos AD ou LDAP ou em uma atribuição estática para usuários internos ACS.
- Outras limitações ou circunstâncias - Restrições de tempo, limitações do dispositivo, e assim por diante.
- Permissões - Níveis de privilégio do ® VLAN ou de Cisco IOS.

O modelo da política ACS 5.x é baseado em regras do formulário:

- Se a circunstância resulta então

Por exemplo, nós usamos a informação descrita para o modelo grupo-baseado:

- Se identidade-condição, autorização-perfil da limitação-condição então.

Em consequência, isto dá-nos a flexibilidade limitar sob que circunstâncias é permitido ao usuário alcançar a rede assim como que nível da autorização é permitido quando as circunstâncias específicas são estadas conformes.

Configurar recursos de rede

Este procedimento explica como adicionar o WLC como um cliente de AAA no servidor RADIUS para que o WLC possa passar as credenciais do usuário ao servidor RADIUS.

Conclua estes passos:

1. Do ACS GUI, vá aos **recursos de rede** > aos **grupos de dispositivo de rede** > ao **lugar**, e o clique **cria** (na parte inferior).
2. Adicionar os campos requerido, e o clique **submete-se**.Você verá agora esta tela:
3. **O tipo de dispositivo do** clique > **cria**.
4. Clique em Submit. Você verá agora esta tela:
5. Vá aos **recursos de rede** > aos **dispositivos de rede e aos clientes de AAA**.
6. O clique **cria**, e preenche os detalhes como mostrado aqui:
7. Clique em Submit. Você verá agora esta tela:

Configurar usuários

Nesta seção, você criará usuários locais no ACS (Student-1 e Teacher-1). Student-1 é atribuído ao grupo dos “estudantes” e Teacher-1 é atribuído ao grupo dos “professores”.

1. Vá aos **usuários e a identidade armazena > grupos da identidade > cria**.
2. Uma vez que você clique **se submete**, a página olhará como esta:
3. Crie e atribua a usuários Student-1 e Teacher-1 a seus grupos respectivos.
4. Clique **usuários e a identidade armazena > identidade agrupa > usuários > cria**.
5. Similarmente, crie Teacher-1.A tela olhará como esta:

Defina elementos da política

Termine estas etapas a fim definir atributos IETF para os usuários:

1. Vá aos **elementos** > à **autorização da política e as permissões** > os **perfis do acesso de rede** > da **autorização > criam**.
2. Da aba comum das tarefas:
3. Adicionar estes atributos IETF:Tipo de túnel = 64 = VLANTúnel-Media-tipo = 802Túnel-Privado-Grupo-ID = 253 (Student-1) e 257 (Teacher-1)Para estudantes do grupo:Para professores do grupo:
4. Uma vez que ambos os atributos são adicionados, a tela olhará como esta:

Aplique políticas de acesso

Termine estas etapas a fim selecionar que métodos de autenticação devem ser usada e como as regras devem ser configuradas (baseado nas etapas precedentes):

1. Vai às **políticas de acesso** > ao **acesso presta serviços de manutenção** > o **acesso de rede padrão > edita: De “acesso rede padrão”**.
2. Selecione que o método de EAP você como os clientes Wireless autenticaria. Neste exemplo, nós usamos **PEAP- MSCHAP-V2**.
3. Clique em Submit.
4. Verifique o grupo que da identidade você selecionou. Neste exemplo, nós usamos os

usuários internos, que nós criamos no ACS. Salve as alterações.

5. A fim verificar o perfil da autorização, vá às **políticas de acesso** > ao **acesso presta serviços de manutenção > acesso > autorização de rede padrão**.Você pode personalizar sob que circunstâncias você permitirá a acesso de usuário à rede e que perfil da autorização (atributos) você passará autenticado uma vez. Esta granularidade está somente disponível em ACS5.x. Neste exemplo, nós selecionamos o **lugar**, o **tipo de dispositivo**, o **protocolo**, o **grupo da identidade**, e o **método de autenticação de EAP**.
6. **APROVAÇÃO do** clique, e **mudanças da salvaguarda**.
7. A próxima etapa é criar uma regra. Se nenhuma regra é definida, o acesso está permitido ao cliente sem nenhumas circunstâncias.O clique **cria > Rule-1**. Esta regra é para Student-1.
8. Similarmente, crie uma regra para Teacher-1. Clique **mudanças da salvaguarda**.A tela olhará como esta:
9. Nós definiremos agora regras de seleção do serviço. Use esta página a fim configurar uma política simples ou baseado em regras determinar que serviço a se aplicar às requisições recebidas. Neste exemplo, uma política baseado em regras é usada.

Configurar o WLC

Essa configuração requer estes passos:

1. Configurar o WLC com os detalhes do Authentication Server.
2. Configurar as interfaces dinâmica (VLAN).
3. Configurar os WLAN (SSID).

Configurar o WLC com os detalhes do Servidor de Autenticação

Énecessário configurar o WLC assim que pode comunicar-se com o servidor Radius a fim autenticar os clientes, e igualmente para todas as outras transações.

Conclua estes passos:

1. Na interface gráfica do usuário, clique em **Security**.
2. Digite o endereço IP do servidor RADIUS e a chave secreta compartilhada usados entre o servidor RADIUS e o WLC.Esta chave secreta compartilhada deve ser a mesma que essa configurada no servidor Radius.

Configurar as interfaces dinâmicas (VLANs)

Este procedimento descreve como configurar interfaces dinâmica no WLC. Como explicado antes neste documento, a ID de VLAN especificada sob o atributo Tunnel-Private-Group ID do servidor RADIUS deve igualmente existir no WLC.

No exemplo, Student-1 é especificado com o Túnel-Privado-**grupo ID de 253 (VLAN =253) no** servidor Radius. Similarmente, Teacher-1 é especificado com o Túnel-Privado-**grupo ID de 257 (VLAN =257) no** servidor Radius. Veja a seção dos atributos de raio de IETF do indicador da instalação de usuário.

Conclua estes passos:

1. A interface dinâmica é configurada do controlador GUI, no indicador do **controlador > das relações**.
2. Clique em Apply.Isto toma-o ao indicador da edição desta interface dinâmica (VLAN 253 aqui).
3. Digite o endereço IP e o gateway padrão desta interface dinâmica.
4. Clique em Apply.
5. Similarmente, nós criaremos uma interface dinâmica para VLAN 257 para Teacher-1.
6. As interfaces configuradas configuradas olharão como esta:

Configurar as WLANs (SSID)

Termine estas etapas a fim configurar os WLAN no WLC:

1. Do controlador GUI, vão aos **WLAN > criam novo** a fim criar um WLAN novo. A janela New WLANs é exibida.
2. Digite a ID da WLAN e a SSID da WLAN.Você pode dar entrada com todo o nome como o WLAN SSID. Este exemplo usa o **goa** como o WLAN SSID.
3. O clique **aplica-se** a fim ir ao indicador da edição do goa WLAN.
4. Permita a opção da **ultrapassagem reservar AAA no** controlador para cada WLAN (SSID) configurado. A opção da ultrapassagem reservar AAA de um WLAN permite que você configure o WLAN para trabalhos em rede da identidade. Permite que você aplique a colocação de etiquetas, o QoS, e os ACL VLAN aos clientes individuais baseados nos atributos RADIUS retornados do servidor AAA. Neste exemplo, é usada a fim atribuir um VLAN aos clientes.A maioria da configuração para permitir a ultrapassagem AAA é feita no servidor Radius. Permitir este parâmetro permite que o controlador aceite os atributos retornados pelo servidor Radius. O controlador aplica então estes atributos a seus clientes.**Note**: Quando o grupo de interface é traçado a um WLAN e aos clientes conecta ao WLAN, o cliente não obtém o endereço IP de Um ou Mais Servidores Cisco ICM NT em uma forma redonda de Robin. A ultrapassagem AAA com grupo de interface não é apoiada.

Configurar a utilidade do cliente Wireless

Em nosso cliente de teste, nós estamos usando o suplicante nativo de Windows 7 com um cartão de Intel 6300-N que executa a versão do driver 14.3. Recomenda-se testar usando os direcionadores os mais atrasados dos vendedores.

Termine estas etapas a fim criar um perfil em Windows zero configurações (WZC):

1. Vá ao **Control Panel** > à **rede e o Internet > controla redes Wireless**.
2. Clique a aba **adicionar**.
3. O clique **cria manualmente um perfil da rede**.
4. Adicionar os detalhes como configurados no WLC.**Note**: O SSID é diferenciando maiúsculas e minúsculas.
5. Clique em Next.
6. **Configurações de conexão da mudança do** clique a fim verificar novamente os ajustes.
7. Neste exemplo, nós não estamos validando o certificado de servidor. Se você verifica esta caixa e não pode conectar, tente desabilitar a característica e o teste outra vez.
8. Alternativamente, você pode usar suas credenciais de Windows a fim entrar. Contudo, neste

exemplo nós não estamos indo usar aquele. Click **OK**.

9. **Ajustes avançados do** clique a fim configurar o nome de usuário e senha.
10. Uma vez que você terminou testar Student-1, teste Teacher-1. Click **OK**.

Seu utilitário de cliente está agora pronto para conectar.

Verificar

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

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Verifique Student-1

Do WLC GUI, vá ao **monitor >** aos **clientes**, e selecione o MAC address.

Stats do RAIO WLC:

```
(Cisco Controller) >show radius auth statistics
Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.150.24
Msg Round Trip Time.............................. 1 (msec)
First Requests................................... 8
Retry Requests................................... 0
Accept Responses................................. 1
Reject Responses................................. 0
Challenge Responses.............................. 7
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Logs ACS:

1. Termine estas etapas a fim ver as contagens da batida:Se você verifica os logs dentro de 15 minutos da autenticação, certifique-se de você refrescar a contagem da batida.Você tem uma aba para a **contagem da batida na** parte inferior da mesma página.
2. **A monitoração do** clique **e os relatórios** e uma janela pop-up nova aparecem. Vá às **autenticações – Raio – Hoje**. Você pode igualmente clicar **detalhes** a fim verificar que regra de seleção do serviço era aplicada.

Verifique Teacher-1

Do WLC GUI, vá ao **monitor >** aos **clientes**, e selecione o MAC address.

O ACS registra:

1. Termine estas etapas a fim ver as contagens da batida:Se você verifica os logs dentro de 15 minutos da autenticação, certifique-se de você refrescar a contagem da BATIDA.Você tem

uma aba para a **contagem da batida na** parte inferior da mesma página.
2. **A monitoração do** clique **e os relatórios** e uma janela pop-up nova aparecem. Vá às **autenticações – Raio – Hoje**. Você pode igualmente clicar **detalhes** a fim verificar que regra de seleção do serviço era aplicada.

Troubleshooting

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

Comandos para Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

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

1. Se você experimenta quaisquer problemas, emita estes comandos no WLC:**debugar o cliente que o *<mac adiciona do client>*debug aaa all enablemostre o *addr> do <mac do* detalhe do cliente** - Verifique o estado do gerente da política.**mostre estatísticas do AUTH do raio** - Verifique a razão da falha.**debugar o desabilitação-todo** - Gire debuga fora.**cancele** estatísticas do raio do **fim de alerta do AUTH do raio stats no** WLC.
2. Verifique que entra o ACS e note a razão da falha.

Informações Relacionadas

- Atribuição do VLAN dinâmico com servidor Radius ACS 4.1 e exemplo da configuração de controle do Wireless LAN
- Suporte Técnico e Documentação - Cisco Systems