NAC: Integração LDAP com ACS 5.x e exemplo de configuração mais atrasado

Índice

Introdução

Este documento fornece uma configuração de exemplo a fim configurar a baliza e o Cisco Secure Access Control System (ACS) 5.x e permitir mais tarde os dispositivos Cisco configurados para o desvio da autenticação de MAC (MAB) de forma eficaz e eficiente para autenticar dispositivos capazes non-802.1X na rede autenticada.

Cisco executou uma característica chamada MAB em seu Switches, assim como o apoio necessário no ACS, a fim acomodar valores-limite nas redes 802.1X-enabled que não podem autenticar com o 802.1X. Esta funcionalidade assegura-se de que os valores-limite que tentam conectar à rede 802.1X-enabled que não são equipados com a funcionalidade do 802.1X, por exemplo, não têm um suplicante funcional do 802.1X, podem ser autenticados antes da admissão, assim como têm a política de utilização da rede básica reforçada durante todo sua conexão.

O MAB permite a rede de ser configurado para admitir dispositivos identificados com o uso de seu MAC address como as credenciais preliminares quando o dispositivo não participa no protocolo do 802.1X. Para que o MAB seja distribuído e utilizado eficazmente, o ambiente deve ter meios identificar os dispositivos no ambiente que não são capazes da autenticação do 802.1X, e manter ao longo do tempo um base de dados atualizado destes dispositivos como move-se, adiciona e as

mudanças ocorrem. Esta lista precisa de ser povoada manualmente e mantido no Authentication Server (ACS), ou com alguns meios alternativos a fim assegurar-se de que os dispositivos que autenticam no MAC sejam terminados e válidos em qualquer momento a tempo.

O perfilador do valor-limite da baliza pode automatizar o processo da identificação de NON-autenticar valores-limite, aqueles sem suplicantes do 802.1X, e a manutenção da validez destes valores-limite nas redes da escala de variação na funcionalidade de monitoramento do perfilamento e do comportamento do valor-limite. Através de uma interface ldap padrão, o sistema da baliza pode servir como um base de dados externo ou um diretório dos valores-limite a ser autenticados com o MAB. Quando um pedido MAB é recebido da infraestrutura da borda, o ACS pode perguntar o sistema da baliza a fim determinar mesmo se um valor-limite dado deve ser admitido ao baseado na rede na maioria de informação atual sobre o valor-limite conhecido pela baliza. Isto impede a necessidade para a configuração manual.

Para uma configuração similar usando versões mais cedo do que ACS 5.x, refira o NAC: Integração LDAP com exemplo da configuração ACS.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco 3750 Switch que executa o Software Release 12.2(25)SEE2 de Cisco IOS®
- Cisco Secure ACS 5.x e mais tarde

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.

Informações de Apoio

O MAB é uma funcionalidade essencial para o apoio dinâmico dos dispositivos tais como impressoras, Telefones IP, máquinas de fax e outros dispositivos capazes non-802.1X no desenvolvimento do ambiente post-802.1X. Sem uma capacidade MAB, as portas do acesso de rede que fornecem Conectividade aos valores-limite capazes non-802.1X devem ser fornecida estaticamente a fim não tentar a autenticação do 802.1X ou com o uso dos outros recursos que fornecem opções muito limitadas da política. Por razões óbvias, isto não é inerentemente escalável em grandes ambientes de empreendimento. Com o MAB permitido conjuntamente com o 802.1X em todas as portas de acesso, os valores-limite capazes conhecidos non-802.1X podem

ser movidos em qualquer lugar no ambiente e ainda confiantemente (e firmemente) conecte à rede. Porque os dispositivos admitidos à rede estão sendo autenticados, as políticas diferentes podem ser aplicadas aos dispositivos diferentes.

Além, os valores-limite capazes non-802.1X que não são conhecidos no ambiente, tal como os portáteis que pertencem aos visitantes ou aos contratantes, podem ser acesso restrito fornecido à rede com o MAB se desejados.

Enquanto o nome sugere, o desvio da autenticação de MAC utiliza o MAC address do valor-limite como as credenciais preliminares. Com o MAB permitido em uma porta de acesso, se um valor-limite conecta e não responde ao desafio de autenticação do 802.1X, a porta reverte ao modo MAB. O interruptor que tenta o MAB de um valor-limite faz uma requisição RADIUS padrão ao ACS com o MAC da estação. Tenta conectar à rede e pede a autenticação do valor-limite do ACS antes da admissão do valor-limite à rede.

Configuração

Diagrama do fluxograma

Este fluxograma ilustra como o MAB está utilizado conjuntamente com a autenticação do 802.1X na infraestrutura da borda de Cisco enquanto os valores-limite novos tentam conectar à rede.

Este documento usa estes trabalhos do fluxograma:

Figura 1: Fluxo da autenticação

O ACS pode ser configurado para utilizar seu próprio base de dados interno ou um servidor ldap externo a fim autenticar requisições de usuário do MAC address. O sistema do perfilador do valor-limite da baliza LDAP-é permitido inteiramente à revelia e pode ser utilizado pelo ACS a fim autenticar requisições de usuário do MAC address com a funcionalidade do padrão LDAP. Porque a baliza automatiza a descoberta assim como o perfilamento de todos os valores-limite na rede, o ACS pode perguntar a baliza com o LDAP a fim determinar se o MAC for admitido à rede, e que agrupam o valor-limite devem ser traçados. Isto significativamente automatiza e aumenta a característica MAB, particularmente em grandes ambientes de empreendimento.

Com a funcionalidade de monitoramento comportável fornecida pela baliza, os dispositivos que são observados para se comportar incompativelmente com os perfis permitidos para o MAB são concluiu a transição fora de 4 perfis LDAP-permitidos e para falhar subseqüentemente a tentativa regular seguinte da reautenticação.

Configuração de sistema do perfilador do valor-limite da baliza para o MAB

A configuração do sistema da baliza para a integração com o ACS para fins do apoio MAB é direta porque a funcionalidade LDAP é permitida à revelia. As tarefas de configuração preliminares são identificar os perfis que contêm os valores-limite que são desejados ser autenticados com o MAB no ambiente, e para permitir então aqueles perfis para o LDAP. Tipicamente, os perfis da baliza, que contêm dispositivos possuíram pela organização, devem ser acesso de rede fornecido quando considerados em uma porta contudo são sabidos para ser incapazes de autenticar com o 802.1X. Tipicamente, estes são os perfis que contêm impressoras, Telefones IP ou UPSs manejável como exemplos comuns.

Se as impressoras perfiladas pela baliza foram colocadas em um perfil nomeado *Impressora*, e os

Telefones IP em um perfil nomearam *Telefones IP*, por exemplo, a seguir necessidade destes perfis ser permitido para o LDAP tais que os valores-limite colocados naqueles perfis conduzem à autenticação bem sucedida como o telefone IP e impressoras conhecidos no ambiente com o MAB. Se você permite um perfil para o LDAP, este exige a escolha do botão de rádio LDAP na configuração de perfil do valor-limite, segundo as indicações deste exemplo:

Figura 2: Permita um perfil para o LDAP

Quando a autenticação de MAC dos proxys ACS a iluminar com o LDAP, a pergunta consistir em duas perguntas secundárias. Ambos devem retornar um resultado válido, NON-nulo. A primeira pergunta a iluminar é mesmo se o MAC está sabido para iluminar, por exemplo, se se descobriu e foi adicionado ao base de dados da baliza. Se o valor-limite tem ser descoberto ainda pela baliza, o valor-limite está considerado ser desconhecido.

A segunda pergunta não é necessária no caso dos valores-limite que a baliza não descobriu e não está em seu base de dados. Se o valor-limite foi descoberto e está no base de dados da baliza, a pergunta seguinte é determinar o perfil atual do valor-limite. Se um valor-limite tem ser perfilado ainda ou está atualmente em um perfil não 5 permitido para o LDAP, o resultado desconhecido está retornado ao ACS, e a autenticação do valor-limite pela baliza falha. Depende de como o ACS é configurado que este pode conduzir ao dispositivo com a recusa do acesso à rede completamente, ou dado uma política que seja apropriada para o desconhecido ou os dispositivos do convidado.

Somente no caso onde o MAC é um valor-limite que a baliza descubra e colocado em um perfil LDAP-permitido, a resposta é que o valor-limite está conhecido e perfilado pela baliza esteja retornado ao ACS. Mais importante ainda, porque baliza destes valores-limite fornece o nome de perfil atual. Isto permite o ACS de traçar valores-limite conhecidos aos grupos de Cisco SecureAccess. Isto permite uma determinação granulada da política feita, tão granulado quanto uma política separada para cada perfil LDAP-permitido baliza, se desejado.

Configuração ACS para o MAB e utilização da baliza como uma base de dados de usuário externo

A configuração do ACS para o MAB e da utilização da baliza como uma base de dados de usuário externo exige três etapas distintas. A ordem ilustrada neste documento segue uns trabalhos que sejam eficientes quando executam a configuração MAB em sua totalidade, e possam variar para os sistemas que estiveram na operação com outros modos de autenticação já configurados.

Quando você tenta o MAB para um ponto final particular que tentem conectar à rede, o ACS pergunta a baliza no LDAP a fim determinar se a baliza descobriu o MAC, e o que baliza do perfil colocou atualmente o MAC address dentro como descrito mais cedo no documento.

Neste documento, dois perfis separados são criados:

- BeaconKnownDevices — para os valores-limite descobertos e perfilados pela baliza
- BeaconUnknownDevices — para os dispositivos que não são sabidos atualmente pela baliza

Uma ou outra baliza não descobriu o MAC, nem não o perfilou atualmente a um perfil LDAP-permitido. O perfil de BeaconKnownDevices porá os valores-limite no VLAN10 e o perfil de BeaconUnkownDevices porá os valores-limite em VLAN 7.

Mais tarde neste documento, uma conexão ldap ao perfilador do valor-limite da baliza do ACS é criada e grupos são escolhidos do perfilador do valor-limite da baliza baseado no que valores-

limite serão considerados como dispositivos de BeaconKnown, e serão atribuídos o perfil de BeaconKnownDevices (que os porá no VLAN10). Todos os dispositivos desconhecidos que uma ou outra baliza não descobriu o MAC, nem não o perfilou atualmente em um perfil LDAP-permitido serão atribuídos o perfil de BeaconUnkownDevices (que os porá em VLAN 7).

Crie um perfil da autorização

Termine estas etapas a fim criar um perfil da autorização:

1. Escolha **elementos > autorização da política e as permissões > o acesso de rede > os perfis** e o clique da **autorização criam** para criar um perfil novo da autorização.
2. Forneça o **nome do** perfil novo da autorização.
3. **Em tarefas da terra comum a** aba ajustou o **VLAN à estática** com o **valor** como o **10.** Depois, clique em **Submit**.
4. Escolha **elementos > autorização da política e as permissões > o acesso de rede > os perfis** e o clique da **autorização criam** para criar um perfil novo da autorização.
5. Forneça o **nome do** perfil novo da autorização.
6. **Em tarefas da terra comum a** aba ajustou o **VLAN à estática** com o **valor** como o **7.** Depois, clique em **Submit**.

Crie uma conexão de base de dados LDAP

Termine as etapas a fim criar uma conexão de base de dados LDAP:

1. Escolha **usuários e a identidade armazena > identidade externo armazena > LDAP** e clique **cria** para criar uma conexão de base de dados LDAP nova.
2. Forneça um **nome** para a **conexão de base de dados LDAP** nova e clique-o **em seguida**.
3. Na aba da **conexão de servidor** incorpore o **hostname/endereço IP de Um ou Mais Servidores Cisco ICM NT da BALIZA LDAP separam, movem, Admin DN, a senha** (GBSbeacon neste exemplo). Então, clique **em seguida**.
4. Na aba da **organização do diretório** incorpore a informação requerida. Então, **revestimento do** clique.
5. Clique a **conexão ldap** recém-criado (baliza neste exemplo).
6. Escolha a aba dos **grupos do diretório** e clique **seleto**. conexão.
7. Selecione todos os grupos na tela seguinte que você quer traçar a **BeaconKnownDevices**.
8. Neste exemplo estes grupos, a saber lab_laptop, 3com_gear e apple_users, são escolhidos. Depois, clique em **Submit**.

Configurar serviços do acesso

Termine estas etapas a fim configurar os serviços do acesso:

1. Escolha **políticas de acesso > serviços do acesso** e o clique **cria** para criar um serviço novo do acesso.
2. **No tab geral** forneça o **nome do** serviço novo, a seguir clique **seleto** ao lado do **baseado no molde do serviço**.
3. Escolha o **acesso de rede - Desvio da autenticação de MAC** e **APROVAÇÃO do** clique.
4. Clique em Next.

5. Clique em Finish.
6. Clique em Sim.
7. O clique **personaliza**.
8. Mova **UseCase da selecionada disponível** e clique a **APROVAÇÃO**.
9. O clique **cria** para criar uma **regra de seleção** nova do **serviço**.
10. Selecione o **protocolo** e use o **raio** como o valor. Similarmente, **UseCase** seleto e **consulta do host do** uso como o valor. Escolha o Baliza-**AUTH** como o serviço e clique a **APROVAÇÃO**.
11. Mova a regra recém-criado para a parte superior.
12. Clique **mudanças da salvaguarda**.
13. Escolha **políticas de acesso > acesso presta serviços de manutenção > Baliza-AUTH > identidade** e clicam **seleto** ao lado da **fonte da identidade**.
14. Escolha a **baliza** e clique a **APROVAÇÃO**.
15. Clique **mudanças da salvaguarda**.
16. Escolha **políticas de acesso > acesso presta serviços de manutenção > Baliza-AUTH > autorização** e o clique **personaliza**.
17. **Baliza do** movimento**: ExternalGroups de disponível selecionou** e da **APROVAÇÃO do** clique.
18. O clique **cria** para criar uma **regra** nova.
19. Escolha 3com_users, apple_users e lab_laptop como as circunstâncias e a autorização perfilam **BeaconKnownDevices** como o **resultado**. Então, **APROVAÇÃO do** clique.
20. **Padrão do** clique.
21. Escolha 3com_users, apple_users e lab_laptop como as circunstâncias e a autorização perfilam **BeaconUnKnownDevices** como o resultado. Então, **APROVAÇÃO do** clique.
22. **Mudanças da salvaguarda do** clique.Isto termina o procedimento.

Configuração de switch para o desvio da autenticação de MAC

Esta configuração de switch fornece um exemplo de configuração para a autenticação do 802.1X o MAB permitido, e o reafectação do VLAN dinâmico exigido a fim aplicar os atributos RADIUS retornados do ACS.

Switch

```
switch#show running-config ! version 12.2 no service pad
service timestamps debug uptime service timestamps log
datetime service password-encryption service sequence-
numbers ! ! aaa new-model aaa authentication login
default line aaa authentication enable default enable
aaa authentication dot1x default group radius aaa
authorization network default group radius aaa
accounting dot1x default start-stop group radius ! aaa
session-id common switch 1 provision ws-c3750g-24ts ip
subnet-zero ip routing no ip domain-lookup ! ! ! ! ! !
dot1x system-auth-control no file verify auto spanning-
tree mode pvst spanning-tree extend system-id ! vlan
internal allocation policy ascending ! ! interface Port-
channel1 switchport trunk encapsulation dot1q switchport
trunk allowed vlan 5,7,9,10 ! interface Port-channel2
description LAG/trunk to einstein switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk ! interface Port-channel3
description "LAG to Edison" switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
```

```
allowed vlan 5,9,11 switchport mode trunk ! interface
GigabitEthernet1/0/1 switchport trunk encapsulation
dot1q switchport trunk allowed vlan 5,7,9,10 channel-
group 1 mode passive ! interface GigabitEthernet1/0/2
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,7,9,10 channel-group 1 mode passive !
interface GigabitEthernet1/0/3 switchport trunk
encapsulation dot1q switchport trunk allowed vlan
5,7,9,10 channel-group 1 mode passive ! interface
GigabitEthernet1/0/4 switchport access vlan 7 switchport
mode access ! interface GigabitEthernet1/0/5 switchport
access vlan 5 switchport mode access spanning-tree
portfast ! interface GigabitEthernet1/0/6 switchport
trunk encapsulation dot1q switchport trunk allowed vlan
5,7,9 switchport mode trunk switchport nonegotiate !
interface GigabitEthernet1/0/7 switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk channel-group 2 mode active !
interface GigabitEthernet1/0/8 switchport trunk
encapsulation dot1q switchport trunk allowed vlan 5,9,10
switchport mode trunk channel-group 2 mode active !
interface GigabitEthernet1/0/9 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/10 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/11 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/12 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/13 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/14 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/15 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/16 switchport access vlan 5
switchport mode access spanning-tree portfast !
interface GigabitEthernet1/0/17 switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk channel-group
3 mode active spanning-tree portfast ! interface
GigabitEthernet1/0/18 switchport access vlan 5
switchport trunk encapsulation dot1q switchport trunk
allowed vlan 5,9,11 switchport mode trunk channel-group
3 mode active spanning-tree portfast ! interface
GigabitEthernet1/0/19 switchport mode access dot1x mac-
auth-bypass dot1x pae authenticator dot1x port-control
auto dot1x timeout quiet-period 10 dot1x timeout reauth-
period 60 dot1x timeout tx-period 10 dot1x timeout supp-
timeout 10 dot1x max-req 1 dot1x reauthentication dot1x
auth-fail max-attempts 1 spanning-tree portfast !
interface GigabitEthernet1/0/20 switchport mode access
dot1x mac-auth-bypass dot1x pae authenticator dot1x
port-control auto dot1x timeout quiet-period 10 dot1x
timeout reauth-period 60 dot1x timeout tx-period 10
dot1x timeout supp-timeout 10 dot1x max-req 1 dot1x
reauthentication dot1x auth-fail max-attempts 1
spanning-tree portfast ! interface GigabitEthernet1/0/21
switchport access vlan 10 switchport mode access
spanning-tree portfast ! interface GigabitEthernet1/0/22
switchport access vlan 10 switchport mode access
spanning-tree portfast ! interface GigabitEthernet1/0/23
switchport access vlan 10 spanning-tree portfast !
interface GigabitEthernet1/0/24 switchport access vlan
```

```
10 spanning-tree portfast ! interface
GigabitEthernet1/0/25 ! interface GigabitEthernet1/0/26
! interface GigabitEthernet1/0/27 ! interface
GigabitEthernet1/0/28 ! interface Vlan1 no ip address
shutdown ! interface Vlan5 ip address 10.1.1.10
255.255.255.0 ! interface Vlan9 ip address 10.9.0.1
255.255.0.0 ! interface Vlan10 ip address 10.10.0.1
255.255.0.0 ip helper-address 10.1.1.1 ip helper-address
10.10.0.204 ! interface Vlan11 ip address 10.11.0.1
255.255.0.0 ip helper-address 10.1.1.1 ip helper-address
10.10.0.204 ! ip default-gateway 10.1.1.1 ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1 ip route 10.30.0.0
255.255.0.0 10.10.0.2 ip route 10.40.0.0 255.255.0.0
10.10.0.2 ip http server ip http secure-server ! ! snmp-
server community public RW snmp-server host 10.1.1.191
public radius-server host 10.10.0.100 auth-port 1645
acct-port 1646 key 7 05090A1A245F5E1B0C0612 radius-
server source-ports 1645-1646 ! control-plane ! ! line
con 0 password 7 02020D550C240E351F1B line vty 0 4
password 7 00001A0803790A125C74 line vty 5 15 password 7
00001A0803790A125C74 ! end
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Informações Relacionadas

- Cisco NAC Appliance (Clean Access)
- Cisco Secure Access Control System
- Suporte Técnico e Documentação - Cisco Systems