Camada 3 OOB de Cisco NAC com ACL

Índice

Introdução

O Cisco Network Admission Control (NAC) reforça as políticas de segurança de rede de uma organização em todos os dispositivos que buscam acesso à rede. Cisco NAC permite somente dispositivos de ponto final complacentes e confiados, tais como PC, server, e PDA, na rede. O acesso é restrito para dispositivos NON-complacentes, que limita o dano potencial das ameaças de segurança e dos riscos emergentes. Cisco NAC dá a organizações um método poderoso, papel-baseado a impedir o acesso não autorizado e melhora a elasticidade de rede.

A solução de Cisco NAC fornece os seguintes benefícios para os negócios:

- **Conformidade da política de segurança**: Assegura-se de que os valores-limite se conformem à política de segurança; protege a infraestrutura e a produtividade do funcionário; fixa ativos controlados e unmanaged; ambientes internos dos apoios e acesso do convidado; costura políticas a seu nível de risco.
- **Protege investimentos existentes**: É compatível com aplicativos de gerenciamento de terceira parte; as opções de distribuição flexíveis minimizam a necessidade para elevações da infraestrutura.
- **Abranda riscos dos vírus, dos worms, e do acesso não autorizado**: Os controles e reduzem rompimentos em grande escala da infraestrutura; reduz despesas de funcionamento fazendo movimentos, adiciona, e muda dinâmico e automatizado, que permite uma eficiência mais alta TI; integra com outros componentes da rede de auto-definição de Cisco para entregar a proteção de segurança detalhada.

Vista geral da solução

Esta seção introduz momentaneamente a camada 3 fora da banda (OOB) usando métodos do Access Control List (ACL) para executar uma arquitetura do Cisco Network Admission Control (NAC).

Descrição da solução

Cisco NAC é usado na infraestrutura de rede para reforçar a conformidade da política de segurança em todos os dispositivos que procuram o acesso aos recursos de rede. Cisco NAC permite que os administradores de rede autentiquem e autorizem usuários e avaliem-nos e remediate suas máquinas associadas antes que estejam concedidos o acesso de rede. Há diversos métodos de configuração que você pode se usar para realizar esta tarefa, mas mergulha 3 fora da banda (OOB) tem rapidamente tornado das metodologias as mais populares do desenvolvimento para o NAC. Esta SHIFT na popularidade é baseada em diversa dinâmica, incluindo a melhor utilização dos recursos do hardware.

Distribuindo Cisco NAC em uma metodologia da camada 3 OOB, uma única ferramenta NAC de Cisco (gerente de Cisco NAC ou server de Cisco NAC) pode escalar para acomodar mais usuários. Igualmente permite que as ferramentas NAC sejam ficadas situadas centralmente um pouco do que distribuída através do terreno ou da organização. Assim, as disposições da camada 3 OOB são muito mais eficazes na redução de custos ambos de um ponto de vista do capital e das despesas operacionais.

Este guia descreve uma aplicação ACL-baseada de Cisco NAC em um desenvolvimento da

camada 3 OOB.

Arquitetura da solução

A arquitetura da solução (veja figura 1) identifica os componentes de solução e os pontos chaves da integração.

Figura 1: Colocação da ferramenta NAC de Cisco em um ambiente de campus típico

As seguintes seções descrevem a camada de acesso, a camada de distribuição, a camada central, e os pontos da integração dos serviços do centro de dados que compõem uma arquitetura típica do terreno.

Camada de acesso

Cisco mergulha a solução 3 OOB NAC é aplicável a um projeto de campus roteado do acesso. No modo de acesso roteado, as interfaces virtuais comutadas da camada 3 (SVI) são configuradas no switch de acesso, e lá são um link da camada 3 entre o acesso e os switch de distribuição.

Nota: O termo “switch de acesso” e “switch de ponta” é usado permutavelmente neste documento.

Como visto em figura 2, o acesso VLAN da camada 3 (por exemplo, VLAN14) é configurado no switch de ponta, mergulha 3 que o roteamento é apoiado do interruptor ao switch de distribuição ou ao roteador ascendente, e o gerente de Cisco NAC controla as portas no switch de acesso.

Figura 2: Switch de acesso com camada 3 à borda

Camada de distribuição

A camada de distribuição é responsável para o roteamento da camada 3. Ao contrário de uma solução da camada 2, o server de Cisco NAC não precisa de ser ficado situado na camada de distribuição. Em lugar de, é colocado centralmente no bloco do serviço do centro de dados.

Camada central

A camada central usa roteadores baseado em IOS de Cisco. A camada central é reservada para o roteamento de alta velocidade, sem nenhuns serviços. Os serviços podem ser colocados em um interruptor do serviço no centro de dados.

O centro de dados presta serviços de manutenção à camada

O centro de dados presta serviços de manutenção a roteadores baseado em IOS e a Switches de Cisco dos usos da camada. O gerente de Cisco NAC e o server de Cisco NAC são ficados situado centralmente no bloco do serviço do centro de dados.

Componentes de solução

Esta seção descreve os componentes da solução da ferramenta NAC de Cisco.

Gerente de Cisco NAC

O gerente de Cisco NAC é o servidor de administração e o base de dados que centraliza a configuração e a monitoração de todos os server, usuários, e políticas de Cisco NAC em um desenvolvimento da ferramenta NAC de Cisco. Para um desenvolvimento OOB NAC, o gerente fornece o Gerenciamento OOB para adicionar e o Switches de controle no domínio do gerente e para configurar portas de switch.

Server de Cisco NAC

O server de Cisco NAC é o ponto da aplicação entre a rede (controlada) não confiável e a rede (interna) confiada. O server reforça policia definido no gerente de Cisco NAC, e os valores-limite comunicam-se com o server durante a autenticação. Neste projeto, o server não é colocado logicamente ou fisicamente “inline” para separar o não-confiável e a rede confiável. Este conceito é endereçado com maiores detalhes mais tarde “na seção do modo (OOB) fora da banda”.

Agente de Cisco NAC

O agente de Cisco NAC é um componente opcional da solução de Cisco NAC. Quando o agente é permitido para seu desenvolvimento de Cisco NAC, o agente assegura-se de que os computadores que alcançam sua reunião da rede as exigências da postura do sistema você especifiquem. O agente de Cisco NAC é um de leitura apenas, fácil de usar, o programa da pequeno-pegada que reside em máquinas do usuário. Quando um usuário tenta alcançar a rede, o agente verifica o sistema de cliente para ver se há o software que você exige, e os usuários das ajudas adquirem todas as atualizações ou software faltante.

Modo (OOB) fora da banda

No desenvolvimento da ferramenta NAC OOB de Cisco, o server de Cisco NAC comunica-se com o host final somente durante o processo de autenticação, posture a avaliação, e a remediação. Depois que se certifica, o host final não se comunica com o server. No modo OOB, o gerente de Cisco NAC usa o Simple Network Management Protocol (SNMP) ao Switches de controle e às atribuições de VLAN do grupo para portas. Quando o Cisco NAC Manager and Server se estabelece para OOB, o gerente pode controlar as portas de switch do Switches apoiado. Para uma lista de Switches apoiado, vá a:

http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/switch_spt.html#wp40017.

A próxima mostra dos diagramas como o gerente de Cisco NAC usa OOB para controlar como um usuário obtém o acesso à rede. A sequência é como segue:

1. Um PC é conectado fisicamente a um interruptor na rede (veja figura 3).
2. O interruptor envia o MAC address usando o SNMP ao gerente de Cisco NAC (veja figura 3).
3. O gerente de Cisco NAC verifica mesmo se o PC “está certificado.”Se o PC não é certificado, o gerente de Cisco NAC instrui o interruptor para atribuir a porta de switch do PC a uma autenticação VLAN (veja figura 4). Continue com etapa 4 com a etapa 6.Se o PC é certificado, vá pisar 5.
4. O PC comunica-se com o server de Cisco NAC e atravessa-se a autenticação, a avaliação da postura, e a remediação (veja figura 4).

5. O server de Cisco NAC informa o gerente de Cisco NAC que o PC “está certificado” (veja a figura 5).
6. O PC é conectado à rede como um dispositivo confiável.

Figura 3: Uma comunicação OOB SNMP (1 de 3) Figura 4: Uma comunicação OOB SNMP (2 de 3) Figura 5: Uma comunicação OOB SNMP (3 de 3)

Considerações do projeto

Quando você considera um desenvolvimento da camada 3 OOB NAC, você deve rever diversas considerações de projeto. Estas considerações estão listadas discutidas nas seguintes subseções, e uma breve discussão de sua importância é incluída.

Classificação do valor-limite

Diversos fatores contribuem à classificação do valor-limite, incluindo tipos de dispositivo e papéis de usuário. O tipo de dispositivo e o papel de usuário impactam o papel do valor-limite.

Tipos de dispositivo possíveis

- Dispositivos corporativos
- dispositivos NON-corporativos
- Dispositivos NON-PC

Papéis de usuário possíveis

- Empregado
- Contratante
- Convidados

Inicialmente, todos os valores-limite são atribuídos ao VLAN não-autenticado. O acesso aos outros papéis é permitido depois que o processo da identidade e da postura está completo.

Papéis do valor-limite

O papel de cada tipo de valor-limite deve inicialmente ser determinado. Um desenvolvimento típico do terreno inclui diversos papéis, tais como empregados, convidados, e contratantes, e outros valores-limite, tais como impressoras, pontos de acesso Wireless, e câmeras IP. Os papéis são traçados ao switch de ponta VLAN.

Nota: O papel não autenticado traça inicialmente todos os usuários a um VLAN não-autenticado para a autenticação principiante.

Isolamento do papel

Évital isolar os papéis do valor-limite quando você executa a solução de Cisco NAC. Selecione um mecanismo de aplicação apropriado para fornecer o tráfego e o isolamento do trajeto para todo o tráfego que origina dos computadores centrais não-autenticados e de host não autorizado. Em um ambiente da camada 3 OOB, o switch de ponta da camada 3 (que usa ACL) atua como o ponto da aplicação que assegura a segregação entre “limpa” e redes “não-autenticados”.

Fluxo de tráfego

O processo NAC começa quando um valor-limite conecta a um interruptor NAC-controlado. O tráfego classificado como “não-autenticado” é restringido pelos ACL aplicados no VLAN não-autenticado. O valor-limite é permitido comunicar-se à relação “não confiável” do server de Cisco NAC para continuar com o processo da avaliação e da remediação da postura (há diversos métodos para executar a avaliação e a remediação da postura que são discutidos mais tarde da “nas políticas atualização do cisco.com no gerente de Cisco NAC.” seção). Após a autenticação, o valor-limite é movido para o VLAN confiado.

Modo de servidor de Cisco NAC

Um server de Cisco NAC pode ser distribuído no modo virtual do gateway (ponte) ou no modo (roteado) do gateway real-IP.

Modo virtual do gateway (ponte)

O modo virtual do gateway (ponte) é usado tipicamente quando o server de Cisco NAC é a camada 2 junto aos valores-limite. Neste modo, o server atua como uma ponte e não é envolvido na decisão de roteamento do tráfego de rede.

Nota: O modo virtual do gateway (ponte) não é aplicável para o projeto da camada 3 OOB ACL.

Modo (roteado) do gateway Real-IP

O modo (roteado) do gateway real-IP é aplicável quando o server de Cisco NAC é saltos múltiplos longe do valor-limite. Quando você usa o server como um gateway real-IP, especifique os endereços IP de Um ou Mais Servidores Cisco ICM NT de suas duas relações: um endereço IP de Um ou Mais Servidores Cisco ICM NT para o lado confiado (para prever o Gerenciamento do gerente de Cisco NAC) e um endereço IP de Um ou Mais Servidores Cisco ICM NT para o lado não confiável. Os dois endereços devem estar em sub-redes diferentes. O endereço IP de Um ou Mais Servidores Cisco ICM NT da interface não confiável é usado comunicando-se com o valor-limite na sub-rede não confiável. Um desenvolvimento da camada 3 OOB que usa ACL exige o valor-limite comunicar-se com a interface não confiável para finalidades da authentication e autorização. Porque o modo real-IP usa um endereço IP válido para a interface não confiável, o server de Cisco NAC deve ser configurado para funcionar no modo do gateway real-IP.

Escalabilidade

Um server padrão de Cisco NAC pode controlar até 5000 utilizadores finais simultâneos. O projeto da camada 3 OOB ACL é serido para um local que serve não mais de 5000 usuários. Se você tem sites múltiplo, você pode ter server adicionais pelo local. Se você tem um único local que precise de servir mais de 5000 usuários, você pode usar técnicas externos do Balanceamento de carga (por exemplo, equilibrador da carga do motor do controle de aplicativo (ACE)) para escalar mais de 5000 usuários para o único local.

Nota: A discussão do equilibrador da carga ACE é além do alcance deste documento.

Host da descoberta

O host da descoberta é o endereço IP de Um ou Mais Servidores Cisco ICM NT do nome de domínio totalmente qualificado (FQDN) ou da interface não confiável usado pelo agente de Cisco

NAC para descobrir os saltos múltiplos encontrados server de Cisco NAC afastado na rede. O agente inicia o processo de descoberta enviando pacotes de UDP ao endereço de host conhecido da descoberta. Os pacotes de descoberta devem alcançar a interface não confiável do server NAC para receber uma resposta. No caso de um desenvolvimento da camada 3 OOB, o server não está no trajeto do tráfego de dados na autenticação VLAN. Consequentemente, a configuração de host da descoberta deve ser configurada para ser o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface não confiável do server de Cisco NAC de modo que o agente possa enviar os pacotes de descoberta diretamente ao server.

Experiência do usuário (com o agente de Cisco NAC)

Tipicamente, os administradores de rede corporativa instalam o agente de Cisco NAC em máquinas cliente antes de emitir aquelas máquinas aos usuários. O endereço IP de Um ou Mais Servidores Cisco ICM NT do host da descoberta ou o nome do pode ser resolvido no agente de Cisco NAC provocam os pacotes de descoberta a ser enviados à interface não confiável do server NAC, que guia automaticamente a máquina cliente com o processo NAC.

Experiência do usuário (sem o agente de Cisco NAC)

Os valores-limite sem um agente de Cisco NAC (convidados mais provável, contratantes, e ativos NON-corporativos) não podem automaticamente continuar com o processo NAC. Os métodos manuais e guiados existem para ajudar aos valores-limite que não têm o agente. Para mais detalhe, veja “valor-limite a seção a uma comunicação do server de Cisco NAC”.

Nota: Para a melhor experiência de usuário final possível, Certificados do uso que são confiados pelo navegador do utilizador final. Usar Certificados auto-gerados no server de Cisco NAC não é recomendada para um ambiente de produção.

Fluxos de processo de Cisco NAC

Esta seção explica o fluxo de processo básico para uma solução NAC OOB. As encenações são ambos descritos com e sem um agente de Cisco NAC instalado na máquina cliente. Esta seção mostra como o gerente de Cisco NAC controla as portas de switch usando o SNMP como o media do controle. Estes fluxos de processo são macroanalíticos na natureza e contêm somente etapas funcionais da decisão. Os fluxos de processo não incluem cada opção nem pisam que ocorre e não incluem as decisões de autorização que são baseadas em critérios de avaliação do valor-limite.

Refira o diagrama de fluxo de processo mostrado na figura 7 para as etapas circundadas mostradas na figura 6.

Figura 6: Fluxo de processo NAC para a solução fora da banda da camada 3 NAC Figura 7: Diagrama de fluxo de processo

Implementação de solução de Cisco NAC

Em um projeto da camada 3 OOB NAC que use ACL, a autenticação dos guias de servidor de Cisco NAC funciona, mas o server não é o ponto do reforço de política na rede. O switch de ponta atua como um ponto da aplicação durante a autenticação, a quarentena, e as fases do acesso. Baseado nesta SHIFT, algumas mudanças adicionais são exigidas no switch de ponta.

Isolamento do papel

Para um desenvolvimento bem sucedido NAC, o isolamento dos valores-limite é crítico. Depois que o projeto da classificação do valor-limite é determinado, as permissões entre classes devem ser determinadas. Um abordagem recomendada segue, com base em figura 8.

Figura 8: Aproximação do isolamento do papel na solução de Cisco NAC OOB

Nota: A relação do gerente de Cisco NAC e a relação confiada do server de Cisco NAC são ilustradas acima em VLAN diferentes. Contudo, estas duas relações podem ser no mesmo VLAN se o server é distribuído no modo do gateway real-IP.

O VLAN não-autenticado exige o acesso a estes recursos:

- Serviços da infraestrutura tais como o DHCP e o DNS
- Authentication Server, tipicamente o controlador de domínio para o início de uma sessão do domínio do Windows antes da validação NAC
- A interface não confiável do server NAC
- Server da remediação (opcionais)

O empregado VLAN tem tipicamente o acesso irrestrito a todos os recursos, o contratante VLAN tipicamente limitou o acesso a um subconjunto dos recursos, e o convidado VLAN tem tipicamente somente o acesso ao Internet.

Técnica da lista de acessos

Uma lista de acesso (ACL) é usada para especificar o tráfego de rede. Depois que você especifica o tráfego com um ACL, você pode fazer uma variedade de coisas com o tráfego. Por exemplo, você pode permiti-lo, negá-lo, limitá-lo, ou usá-lo para restringir atualizações de roteamento.

Na técnica ACL, um grupo de ACL é aplicado a cada interface de VLAN que nova você cria baseado em suas exigências. Os comandos CLI dados nas seguintes subseções mostram os comandos required configurar isolamento confiada e de rede não confiável do trajeto usando VLAN ACL. Siga o procedimento abaixo para executar ACL.

Nota: A adição de VLAN para o isolamento do papel e de ACL configurar naqueles VLAN deve ser executada em cada switch de ponta. Este trabalho deve ser parte de prontidão do desenvolvimento NAC.

1. Antes de executar o NAC, examine a configuração do VLAN existente.Os comandos CLI mostrados no seguinte texto mostram como os empregados VLAN são configurados tipicamente antes que o NAC esteja executado.!
```
int vlan
200description EMPLOYEES_Vlan
ip address 10.100.1.1 255.255.255.0
!
```
2. Configurar VLAN adicionais.O planeamento do PRE-desenvolvimento NAC exige configurar os VLAN adicionais e os ACL relevantes aplicados às interfaces de VLAN. Como um exemplo, o seguinte texto CLI mostra como adicionar uma camada nova 3 VLAN para cada um do não-autenticado, dos empregados, dos contratantes, e dos papéis de convidado.!
```
int vlan
100description UNAUTHENTICATED_Vlan
ip address 172.16.1.1 255.255.255.0
```

```
!
int vlan
200description EMPLOYEES_Vlan
ip address 10.100.1.1 255.255.255.0
!
int VLAN
210description CONTRACTORS_Vlan
ip address 10.120.1.1 255.255.255.0
!
int vlan
300description GUESTS_Vlan
ip address 192.168.1.1 255.255.255.0
!
```

3. Limitações do implementar no papel não autenticado.Os dispositivos não-autenticados no papel não autenticado exigem tipicamente o acesso aos recursos na rede limpa, tal como o DNS, o DHCP, o diretório ativo, e os server da remediação. Igualmente exigem o acesso à interface não confiável do server de Cisco NAC, na configuração de exemplo abaixo, o papel não autenticado têm o acesso aos recursos em 10.10.10.0/24 redes e a interface não confiável do server de Cisco NAC.!

```
! this access-list permits traffic destined to devices on 10.10.10.x
! this should be a consistent ACL that can be applied across all L3
switches
!
ip host NAC_SERVER_UNTRUSTED_INTERFACE <IP_Address>
access-list 100 permit ip any host NAC_SERVER_UNTRUSTED_INTERFACE
access-list 100 permit ip any 10.10.10.0 255.255.255.0
!
!
! then apply this access-list to the UNAUTHENTICATED_Vlan
!
int vlan100
description UNAUTHENTICATED_Vlan
ip address 172.16.1.1 255.255.255.0
ip access-group 100 in
!
int vlan200
description EMPLOYEES_Vlan
ip address 10.100.1.1 255.255.255.0
!
int vlan300
description GUESTS_Vlan
ip address 192.168.1.1 255.255.255.0
!
```

4. Limitações do implementar nos convidados VLAN.Tipicamente, o papel de convidado tem o acesso ao Internet somente. Todo o acesso aos recursos unneeded, tais como todas as redes internas, deve explicitamente ser negado. A única exceção pode ser um servidor interno de DNS.!

```
! ACL 100 permits traffic destined to devices on 10.10.10.0 / 24
! this should be a consistent ACL that can be applied across all L3
switches
!
access-list 100 permit ip any 10.10.10.0 255.255.255.0
!
!
! ACL 101 for Guests should deny access to all internal networks
! while DNS is permitted
!
access-list 101 permit udp any host GUEST_DNS_SERVER eq 53
access-list 101 deny ip any 10.0.0.0 255.0.0.0
access-list 101 deny ip any 192.168.0.0 255.255.0.0
```

```
access-list 101 deny ip any 172.16.0.0 255.240.0.0
access-list 101 permit ip any any
!
int VLAN100
description UNAUTHENTICATED_VLAN
ip address 172.16.1.1 255.255.255.0
ip access-group 100 in
!
int VLAN200
description EMPLOYEES_VLAN
ip address 10.100.1.1 255.255.255.0
!
!
int VLAN300
description GUESTS_VLAN
ip address 192.168.1.1 255.255.255.0
ip access-group 101 in
!
```

Valor-limite a uma comunicação do server de Cisco NAC

O server de Cisco NAC obtém a informações MAC do agente de Cisco NAC ou de uma página de login da Web permitido para ActiveX ou o Java applet de determinar o MAC address do dispositivo e de relatá-lo de volta ao gerente de Cisco NAC.

Agente de Cisco NAC

O agente de Cisco NAC precisa de comunicar-se com a interface não confiável do server NAC para iniciar o processo de login. As tentativas do agente para descobrir o server baseado no valor conhecido do host da descoberta. Segundo as indicações da figura 9, o valor do host da descoberta no Cisco agent (nacs.nac.local) aponta à interface não confiável (172.23.117.57) no server NAC. A figura 9 mostra uma combinação de três telas.

Veja do “o início de uma sessão agente.” secione para mais detalhes na abertura através do agente de Cisco NAC.

Figura 9: Host da descoberta que aponta à interface não confiável do server NAC

Nota: O agente de Cisco NAC não aparece se o agente não pode receber nenhuma parte traseira da resposta do server de Cisco NAC.

Início de uma sessão da Web

O início de uma sessão da Web é exigido tipicamente para sessões de login do convidado. Quando a técnica do isolamento ACL é usada, a interface não confiável do server NAC não está diretamente no trajeto do tráfego de dados. Consequentemente, o usuário não está reorientado automaticamente à página de login quando o navegador é aberto primeiramente. Duas opções podem permitir o host final de obter a página de login.

Opção 1

- Crie um início de uma sessão URL do convidado conhecido aos usuários (por exemplo, guest.cisco.com).
- O convidado deve então abrir um navegador e incorporar essa URL, que causa uma reorientação à página de login.

Opção 2

- Crie um servidor DNS do manequim para a sub-rede de usuário não-autenticado.
- Este servidor DNS do manequim resolve cada URL à interface não confiável do server de Cisco NAC.
- Quando o convidado abre um navegador, apesar que da URL está tentando alcançar, é reorientado à página de login.
- Quando o usuário é movido então para o VLAN apropriado para seu papel, obtém uma atribuição de endereço DNS nova ao executar a liberação IP ou renova-a em um login bem-sucedido.

Em um projeto da camada 3 OOB, usuários que entram usando uma transferência do página da web e executam um controle activex (para navegadores do internet Explorer) ou um Java applet (para os navegadores NON-IE). O controle activex (ou as Javas) devem ser executado para executar o seguinte:

- Recolha o MAC address do host, que é relatado ao server de Cisco NAC e ao gerente de Cisco NAC para fornecer o mapeamento do endereço IP de Um ou Mais Servidores Cisco ICM NT e do MAC address.
- Execute a liberação IP e renove-a do cliente do valor-limite.

Nota: A decisão para permitir que os convidados usem o DNS interno ou externo é uma decisão de política que cada organização deve fazer. Usar um serviço público-baseado DNS levanta menos risco potencial nesta aproximação.

Veja o início de uma sessão da Web, para mais detalhes na abertura através de um página da web.

O NAC mergulha o exemplo da configuração ACL 3 OOB

Para distribuir com sucesso uma solução NAC OOB, os componentes NAC precisam de ser configurados para combinar a arquitetura desejada. A figura 10 mostra um diagrama de rede lógica da camada 3 NAC OOB que seja usado nesta seção para ilustrar a configuração relevante do gerente de Cisco NAC, do server de Cisco NAC, e de um switch de ponta para o desenvolvimento da camada 3 OOB NAC usando ACL.

Figura 10: Diagrama da topologia lógica da camada 3 OOB NAC

Para configurar um desenvolvimento real-IP OOB NAC da camada 3, siga estas etapas:

1. Configurar o switch de ponta para a aplicação.Primeiramente, crie três VLAN adicionais (NÃO-AUTENTICADOS, CONTRATANTES, e CONVIDADOS) no switch de ponta. A produção existente VLAN será usada para os empregados.Configurar e aplique ACL em cada VLAN para restringir o acesso ao baseado na rede no papel atribuído.Papel não autenticado: Nome VLAN 17 e ACL: UNAUTH_ACL`! Create SVI for Un-auth VLAN`

```
Edge Switch(config)#interface vlan 17
Edge Switch (config)#ip address 192.168.7.1 255.255.255.0
Edge Switch (config)#ip helper-address 192.168.3.10
! 192.168.3.10 is the dhcp server (see Figure 10)

! Configure ACL for Un-auth Role
Edge Switch(conf)#ip access-list extended UNAUTH_ACL
   remark Allow Discovery packets from Agent to NAC Server
```

```
   permit udp any host 192.168.8.10 eq 8906
   remark Allow Discovery packets from Agent to NAC Server for ADSSO
   permit udp any host 192.168.8.10 eq 8910
   remark Allow Web traffic from PC to NAC Server
   permit tcp any host 192.168.8.10 eq www
   remark Allow SSL traffic from PC to NAC Server
   permit tcp any host 192.168.8.10 eq 443
   remark Allow DHCP permit udp any any eq bootpc
   permit udp any any eq bootps
   remark Allow DNS
   permit udp any any eq domain
   remark Allow Web traffic to the Remediation Server
   permit tcp any host 192.168.3.10 eq www

! Apply ACL for Un-auth VLAN Interface

Edge Switch(config)#interface vlan 17
Edge Switch(config)# ip access-group UNAUTH_ACL in
```

Papel do contratante: Nome VLAN 77 e ACL: CONTRACTOR_ACL

```
! Create SVI for Contractor VLAN

Edge Switch(config)#interface vlan 77
Edge Switch (config)#ip address 192.168.77.1 255.255.255.0
Edge Switch (config)#ip helper-address 192.168.3.10

! Configure ACL for Contractor Role

Edge Switch(conf)#ip access-list extended CONTRACTOR_ACL
   remark Allow DHCP permit udp any any eq bootpc
   permit udp any any eq bootps
   remark Allow DNS
   permit udp any any eq domain
   remark Allow traffic to DMZ Subnet
   permit ip any 192.168.3.0 0.0.0.255
   remark deny rest of the internal resources
   deny ip any 10.0.0.0 255.0.0.0
   deny ip any 192.168.0.0 255.255.0.0
   deny ip any 172.16.0.0 255.240.0.0
   remark permit internet
   permit ip any any

! Apply ACL for Contractor VLAN Interface

Edge Switch(config)#interface vlan 77
Edge Switch(config)# ip access-group CONTRACTOR_ACL in
```

Papel de convidado: Nome VLAN 78 e ACL: GUEST_ACL

```
! Create SVI for GUEST VLAN

Edge Switch(config)#interface vlan 78
Edge Switch (config)#ip address 192.168.78.1 255.255.255.0
Edge Switch (config)#ip helper-address 192.168.3.10

! Configure ACL for Guest Role

Edge Switch(conf)#ip access-list extended GUEST_ACL
   remark Allow DHCP
   permit udp any any eq bootpc
   permit udp any any eq bootps
   remark Allow DNS
   permit udp any any eq domain
   remark deny access to the internal resources
   deny ip any 10.0.0.0 255.0.0.0
   deny ip any 192.168.0.0 255.255.0.0
   deny ip any 172.16.0.0 255.240.0.0
```

```
   remark permit internet
   permit ip any any

! Apply ACL for GUEST VLAN Interface

Edge Switch(config)#interface vlan 78
Edge Switch(config)# ip access-group GUEST_ACL in
```

Papel do empregado: VLAN14 e ACL: Production_ACLA produção existente VLAN pode ser usada para mover o empregado do VLAN não-autenticado para o empregado VLAN. Depois que o cliente da extremidade é movido para este VLAN, o agente de Cisco NAC ainda tenta descobrir o server de Cisco NAC. O agente é projetado comportar-se esta maneira. Se o agente pode alcançar o server, o agente estala acima e tenta executar outra vez o processo de login, mesmo que a máquina já conceda o acesso. Obviamente, este é um comportamento indesejável e os administradores devem assegurar-se de que os pacotes de descoberta UDP 8906 que originam do agente estejam deixados cair. Employee_ACL é configurado para deixar cair estes pacotes de descoberta.

```
! Use Existing Production Layer 3 VLAN for Employees

Edge Switch(config)#interface vlan 14
Edge Switch (config)#ip helper-address 192.168.3.10

! Configure ACL to prevent discovery packets from reaching the
untrusted interface on the NAC Server

Edge Switch(conf)#ip access-list extended Employee_ACL
   remark Deny Discovery packets from Agent to NAC Server
   deny udp any host 192.168.8.10 eq 8906
   permit ip any any

! Apply ACL for Employee VLAN Interface

Edge Switch(config)#interface vlan 14
Edge Switch(config)# ip access-group Employee_ACL in
```

2. Execute a instalação inicial do Cisco NAC Manager and Server.A instalação do Cisco NAC Manager and Server é executada com o acesso de console. A instalação de serviço público guia-o com a configuração inicial para o gerente e o server. Para executar a instalação inicial, vá a:http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_instal.html
3. Aplique a licença ao gerente de Cisco NAC.Depois que você executa a instalação inicial através do console, alcance o GUI de gerenciador de Cisco NAC para continuar a configurar o Cisco NAC Manager and Server. Transfira arquivos pela rede primeiramente o gerente e as licenças de servidor que vieram com os dispositivos. Para mais detalhe em transferir arquivos pela rede as licenças, vá a:http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_instal.html#wp1113597**Nota:** Todas as licenças do Cisco NAC Manager and Server são baseadas no MAC address do eth0 do gerente. Em uma instalação do Failover, as licenças são baseadas no MAC address do eth0 de gerentes preliminares e secundários de Cisco NAC.
4. Atualize políticas do cisco.com no gerente de Cisco NAC.O gerente de Cisco NAC deve ser configurado para recuperar atualizações periódicas do server central da atualização situado em Cisco. A lista apoiada ferramenta NAC do produto de Cisco AV/AS é um arquivo versioned XML distribuído de um server centralizado da atualização que forneça a matriz a mais atual de vendedores apoiados do antivirus e do antispyware e as versões do produto

usadas para configurar regras do antivirus ou do antispyware e exigências da atualização da definição do antivirus ou do antispyware para a avaliação e a remediação da postura. Esta lista é atualizada regularmente para o antivirus e o Produtos e as versões do antispyware apoiados em cada agente de Cisco NAC liberam e incluem novos produtos para versões de agente novas. Note que a lista fornece a informação de versão somente. Quando o gerente de Cisco NAC transfere a lista apoiada do produto do antivirus e do antispyware, está transferindo a informação sobre o que as versões as mais atrasadas são para o Produtos do antivirus e do antispyware; não está transferindo arquivos de correção ou arquivos de definição de vírus reais. Baseado nesta informação, o agente pode então provocar o aplicativo nativo do antivirus ou do antispyware executar atualizações. Para obter mais informações sobre de como as atualizações são recuperadas, vá a:http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_agntd.html#wp1351880

5. Instale Certificados de um Certificate Authority (CA) da terceira.Durante a instalação, o script do utilitário de configuração para o gerente de Cisco NAC e o server de Cisco NAC exige-o gerar um certificado provisório SSL. Para o ambiente de laboratório, você pode continuar a usar os certificados auto-assinados; contudo, não são recomendados para uma rede de produção.Para obter mais informações sobre de instalar Certificados no gerente de Cisco NAC de CA da terceira, vá a:http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_admin.html#wp1078189Para obter mais informações sobre de instalar Certificados no server de Cisco NAC de CA da terceira, vá a:http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cas/s_admin.html#wp1040111**Nota:** Se você está usando os Certificados do auto-sinal no ambiente de laboratório, no gerente de Cisco NAC e no server de Cisco NAC cada necessidade de confiar o certificado do outro, que o exige transferir arquivos pela rede os Certificados para ambos como um Certificate Authority confiado sob SSL > autoridades do certificado confiável.
6. Adicionar o server de Cisco NAC ao gerente de Cisco NAC.Para adicionar o server NAC ao gerente NAC, siga estas etapas:Clique **server CCA** sob a placa do Gerenciamento de dispositivos (veja figura 11).Clique a aba **nova do server**.Use a caixa do *endereço IP do servidor* para adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação confiada do server NAC.Na caixa da *localização do servidor*, entre no **server OOB NAC** como a localização do servidor.Escolha o Real-IP-**gateway fora da banda da** lista suspensa do *tipo de servidor*.O clique **adiciona o servidor de acesso limpo**.**Figura 11: Adicionando o server de Cisco NAC ao gerente de Cisco NAC** Depois que você adiciona o server de Cisco NAC, aparece na lista sob a lista de aba dos server (veja figura 12).**Nota:** O gerente de Cisco NAC e o server de Cisco NAC têm que confiar o Certificate Authority (CA) de cada um para que o gerente adicione com sucesso o server.
7. Configurar o server de Cisco NAC.Segundo as indicações de figura 12, clique a **lista de** aba dos **server**.Clique o ícone do **controlo** (circundado) para que o server de Cisco NAC continue a configuração.**Figura 12: Server de Cisco NAC controlado pelo gerente de Cisco NAC** Depois que você clica o ícone do controlo, a tela mostrada em figura 13 aparece.
8. Permita o apoio da camada 3.Clique a aba da **rede** (figura 13).Verifique a caixa de seleção do **apoio da possibilidade L3**.Verifique o **modo restrito da possibilidade L3 para obstruir dispositivos NAT com a** caixa de seleção **limpa do agente do acesso**.Clique em **Update**.Recarregue o server de Cisco NAC como instruído.**Figura 13: Detalhes da rede de servidor de Cisco NAC Nota:** Gerencia sempre o certificado para o server de Cisco NAC

com o endereço IP de Um ou Mais Servidores Cisco ICM NT de sua interface não confiável. Para o certificado nome-baseado, o nome deve resolver ao endereço IP de Um ou Mais Servidores Cisco ICM NT da interface não confiável. Quando o valor-limite se comunica com a interface não confiável do server para começar o processo NAC, o server reorientará o usuário ao hostname do certificado ou ao IP. Se o certificado aponta à relação confiada, o processo de login não funcionará corretamente.Em figura 13 acima, você vê que os dois gateways padrão estam presente. Somente o gateway padrão configurado na relação confiada é aplicável. O valor na interface não confiável não é usado enviando o tráfego. O tráfego que é enviado da interface não confiável é dependente da rota estática coberta na próxima etapa.

9. Configurar rotas estáticas.Depois que as repartições do server de Cisco NAC, retornam ao server e continuam com a configuração.O server deve usar a interface não confiável para comunicar-se com os valores-limite no VLAN não-autenticado.Vão a **avançado > as rotas estáticas** (veja figura 14) para adicionar rotas ao VLAN não-autenticado.Preencha as sub-redes apropriadas para os VLAN não-autenticados.O clique **adiciona a rota**.Selecione a **interface não confiável [eth1]** para estas rotas.**Figura 14: Adicionando a rota estática para alcançar a sub-rede de usuário não-autenticado**
10. Perfis estabelecidos para o Switches no gerente de Cisco NAC.**O Gerenciamento** seleto **OOB > perfila > dispositivo > edita** (veja figura 15).Preencha a informação de perfil de dispositivo, usando o exemplo como guia.Cada interruptor será associado com um perfil. Adicionar um perfil para cada tipo de switch de ponta que o gerente de Cisco NAC controlará. O gerente apoia o SNMPv1, o SNMPv2C, e o SNMPv3. Este exemplo cobre o SNMPv1 somente. Você pode querer configurar SNMPv2 ou SNMPv3c para uma comunicação mais segura SNMP entre o gerente e o interruptor.**Figura 15: Perfil SNMP usado para controlar o interruptor**Estabelecer a configuração de switch para o SNMP.O switch de ponta deve ser configurado para os mesmos string de comunidade de leitura/gravação SNMP que aqueles configurados no gerente de Cisco NAC. Veja os comandos CLI abaixo.`3560-remote(config)#snmp-server community cisco123 RO`
`3560-remote(config)#snmp-server community cisco321 RW`**O Gerenciamento** seleto **OOB > perfila > porta > novo** (veja figura 16).Para o controle da porta individual, configurar um perfil da porta sob o **Gerenciamento > os perfis > a porta OOB** que inclui o padrão o acesso não-autenticado VLAN VLAN e de padrão. Na seção do acesso VLAN, especifique o papel de usuário VLAN usando o **acesso VLAN** dropdown. O gerente de Cisco NAC muda o VLAN não-autenticado ao acesso VLAN baseado no VLAN definido no papel onde o usuário pertence.Defina o perfil da porta para controlar o VLAN da porta baseado nos papéis de usuário e nos VLAN executados.O AUTH VLAN é o VLAN NÃO-AUTENTICADO (VLAN 17) a que os dispositivos não-autenticados são atribuídos inicialmente.O acesso VLAN do padrão é os EMPREGADOS VLAN (VLAN14). Este VLAN é usado se o usuário autenticado não tem um VLAN papel-baseado definido.O acesso VLAN pode cancelar o VLAN padrão a um papel de usuário VLAN, que é definido sob o papel de usuário (para obter mais informações sobre dos papéis de usuário da fundação, veja “para configurar papéis de usuário.” seção). Os mapeamentos LDAP podem ser usados para traçar papéis de usuário no NAC aos grupos LDAP. Para mais informação, vá a:http://www.cisco.com/en/US/products/ps6128/products_tech_note09186a0080846d7a.shtml**Figura 16: Perfil da porta para controlar a porta de switch Nota:** Você pode igualmente definir nomes VLAN em vez dos ID. Se você define nomes VLAN, você pode ter VLAN diferente ID no Switches diferente através do terreno, mas o mesmo nome VLAN anexado a um papel particular.As opções adicionais estão disponíveis sob o perfil da porta para a

liberação IP e renovam opções. Enrole para baixo a página mostrada em figura 16 para ver estas opções.Se o usuário é atrás de um telefone IP, desmarcar o salto a porta depois que o VLAN é a caixa de seleção mudada (veja figura 17), que, se verificado, pôde recarregar o telefone IP quando a porta é saltada.**Figura 17: Perfil inferior disponível da porta das várias opções**

11. Configurar ajustes do receptor SNMP.Além do que estabelecer a série de comunidade snmp para lido ou escreva, você deve igualmente configurar o gerente de Cisco NAC para receber o SNMP traps do interruptor. Estas armadilhas são enviadas quando o usuário conecta e disconexões da porta. Quando o server de Cisco NAC envia a informação do endereço IP de Um ou Mais Servidores Cisco ICM NT MAC/de um ponto final particular ao gerente, o gerente constrói uma tabela de mapeamento internamente para o MAC/IP e a porta de switch.**Nota:** Você deve configurar todo o Switches para enviar armadilhas ou informa a Cisco NAC o gerente que usa os string de comunidade definidos em figura 18.**O Gerenciamento** seleto **OOB > perfila > receptor SNMP** (veja figura 18).Configurar os ajustes da armadilha de SNMP usando a tela em figura 18 como guia.**Figura 18: O ajuste do receptor do gerente SNMP NAC para recolher o SNMP traps e informa**Para configurar as configurações de switch para o SNMP traps, aumente o temporizador limpo do resplendor do Access Manager do switch padrão (CAM) a 1 hora (3600 na caixa CLI abaixo) por recomendações da melhor prática de Cisco para NAC OOB. A amostra CLI mostra o conjunto de parâmetro do tempo de envelhecimento do mac-address-table a 3600.Ajustar o temporizador a 1 hora reduz a frequência das notificações MAC enviadas fora já dos dispositivos conectados ao gerente de Cisco NAC. Use o comando trap da fonte especificar o endereço de origem que é usado para mandar as armadilhas.`snmp-server enable traps mac-notification`
`snmp-server host 192.168.2.33 informs NacTraps`
`snmp-server trap-source Vlan 2`
`mac-address-table aging-time 3600`Opcionalmente, configurar a associação e as armadilhas de linkdown para enviar a Cisco NAC o gerente (não mostrado na amostra CLI). Estas armadilhas são usadas somente em um cenário de distribuição onde os host finais não sejam conectados atrás de um telefone IP.**Nota:** O SNMP informa é recomendado porque são mais seguros do que o SNMP traps. Também, considere QoS para o SNMP em um ambiente de rede do tráfego elevado.
12. Adicionar o Switches como dispositivos no gerente de Cisco NAC.**Gerenciamento** seleto **> dispositivos > dispositivos OOB > novo** (veja figura 19).O perfil do interruptor criado na etapa 10 será usado para adicionar o interruptor.Sob o perfil de dispositivo, use o perfil que você criou, mas não mude o valor do perfil da porta padrão quando você adiciona o interruptor.**Nota:** Para o perfil da porta padrão, selecione sempre “descontrolado,” porque você nunca controla todas as portas do switch de acesso. Um mínimo de uma porta de uplink deve ser descontrolado. Consequentemente, você deve adicionar o interruptor com um perfil descontrolado da porta e então selecionar as portas que precise de ser controlado.**Figura 19: Adicionando um switch de ponta no gerente de Cisco NAC para controlar usando o SNMP**Depois que o interruptor é adicionado ao gerente de Cisco NAC, selecione as portas que você quer controlar.
13. Configurar portas de switch para que os dispositivos sejam controlados pelo NAC.**O Gerenciamento** seleto **OOB > o [IP address] do interruptor de dispositivos > movem > lista** para considerar as portas de switch que disponíveis você pode controlar (veja figura 20).**Figura 20: Seleção do controle da porta disponível para um interruptor controladoO Gerenciamento** seleto **OOB > o [IP address] > as portas do interruptor de dispositivos >**

controlam controlar imediatamente diversas portas (veja figura 21).**Figura 21: Controlar portas múltiplas com juntam-se à opção**

14. Configurar papéis de usuário.Neste exemplo, três papéis adicionais são criados. Os VLAN já criados na borda que cada um corresponde a um papel.**O gerenciamento de usuário > os papéis de usuário** seletos **> editam o papel** e criam um papel do empregado usando figura 22 como guia.**Figura 22: Criando o papel do empregado e traço à produção VLAN14O gerenciamento de usuário > os papéis de usuário** seletos **> editam o papel** e criam um papel do contratante usando figura 23 como guia.**Figura 23: Criando o papel e o traço do contratante dele ao acesso limitado VLAN 77O gerenciamento de usuário > os papéis de usuário** seletos **> editam o papel** e criam um papel de convidado usando figura 24 como guia.**Figura 24: Criando o papel de convidado e traçando o ao Internet somente VLAN** No total, você deve ver seis papéis criados nesta seção (três papéis do padrão e três papéis novos), segundo as indicações de figura 25.**Figura 25: Adicionando papéis no gerente NAC**
15. Adicionar usuários e atribua-os para apropriar o papel de usuário.Em um ambiente de campus, você integrará com um servidor de autenticação externa e traçará o usuário a um papel particular por meio do atributo LDAP. Este exemplo usa um usuário local e associados esse usuário local com um papel.
16. Personalize a página do login de usuário para o início de uma sessão da Web.Uma página de login do padrão é criada já no gerente de Cisco NAC. Você pode opcionalmente personalizar a página de login para mudar a aparência do portal da web. Para uma solução da camada 3 OOB NAC, o componente de ActiveX ou de Javas deve ser transferido ao cliente da extremidade para executar as seguintes tarefas:Busque o MAC address da máquina cliente.Execute a liberação do endereço IP de Um ou Mais Servidores Cisco ICM NT e renove-a.**A administração > páginas de usuário** seletas (veja figura 26).Edite a página para fazer para permitir as opções mostradas em figura 26.**Figura 26: Composição do usuário para o início de uma sessão da Web**
17. Personalize o agente de Cisco NAC para os papéis de usuário.**Gerenciamento de dispositivos** seleto **> acesso limpo > instalação > início de uma sessão gerais do agente** (veja figura 27).O gerente de Cisco NAC pode ser configurado para fazer o agente imperativo para todo o papel de usuário. Neste exemplo, o agente é imperativo para o papel do empregado. O contratante e os papéis de convidado devem usar o início de uma sessão da Web.Verifique o **uso da exigência da** caixa de seleção do **agente**.**Figura 27: Início de uma sessão do agente exigido para o papel do empregado**
18. Distribua o host da descoberta para o agente de Cisco NAC.A distribuição de agente de software de Cisco NAC, a instalação, e a configuração são cobertas no apêndice “que configura a ferramenta NAC de Cisco para na seção do início de uma sessão do agente e da avaliação da postura do cliente”. Este exemplo configura o host da descoberta no gerente de Cisco NAC.**Gerenciamento de dispositivos** seleto **> acesso limpo > agente > a instalação limpos do acesso** (veja figura 28).**Figura 28: Host da descoberta para o agente de Cisco NAC** O campo do host da descoberta PRE-está povoado segundo as indicações de figura 28 se o agente de Cisco NAC é transferido do server de Cisco NAC.
19. Início de uma sessão da Web.Conecte a máquina cliente que usa uma das portas de ponta controladas pelo gerente de Cisco NAC.A máquina cliente é colocada no VLAN não-autenticado. A máquina deve obter um endereço IP de Um ou Mais Servidores Cisco ICM NT da sub-rede não-autenticado VLAN.Abra o navegador para executar o início de uma sessão.A suposição é que esta máquina cliente não tem um agente de Cisco NAC instalado já. Se todas as entradas de DNS estão sendo reorientadas à interface não

confiável do server de Cisco NAC, o navegador deve ser reorientado a uma página de login automaticamente. Se não, vá a uma URL específica (por exemplo, guest.nac.local) executar o início de uma sessão (figura 29).**Figura 29: Página de login da Web**

20. Início de uma sessão do agente.O agente de Cisco NAC pode ser distribuído apenas como todo o aplicativo de outro software aos utilizadores finais ou pode ser forçado usando o server de Cisco NAC.**Nota:** Mais informação detalhada na distribuição de agente e na instalação está disponível na *ferramenta NAC de Cisco - manual de configuração limpo do Access Manager*.Quando o agente é ativado, a tela mostrada em figura 30 aparece.**Figura 30: Início de uma sessão do agente** Selecione o server da lista suspensa do **server**.Incorpore o **username**.Incorpore a **senha**.Clique em login.A tela em figura 31 aparece, seguido logo por figura 32.**Figura 31: O agente de Cisco NAC que executa a liberação IP e renova Figura 32: O agente de Cisco NAC que indica o acesso de rede completo após o IP refresca**Clique em **OK**.

Verifique a atribuição de VLAN

A porta controlada para este exemplo é 0/7. Depois que você termina com sucesso o processo de login, o VLAN está mudado do VLAN14 não-autenticado ao empregado VLAN 17. Você pode confirmar que porta está executando a configuração emitindo o comando seguinte:

```
3560-remote#show run interface fast 0/7
Building configuration…

Current configuration : 153 bytes
!
interface FastEthernet0/7
 switchport access VLAN 14
 switchport mode access
 snmp trap mac-notification change added
 spanning-tree portfast
end
```

Solução da camada 3 OOB ACL NAC para o Sem fio

A solução Wireless existente NAC OOB é limitada atualmente a uma solução da camada 2 OOB com o server de Cisco NAC no modo de gateway virtual. A limitação dessa solução é que o controlador do Wireless LAN (WLC) deve ser a camada 2 adjacente com o server de Cisco NAC. Para obter mais informações sobre do desenvolvimento wireless da camada 2 OOB, vá a:

http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a138cc.shtml

Nota: Atualmente, Cisco está trabalhando em uma solução da camada 3 OOB ACL NAC para disposições wireless.

Apêndice

Alta Disponibilidade

Cada um dos gerentes de Cisco NAC e dos server individuais de Cisco NAC na solução pode ser configurado na Alta disponibilidade do modo, significando que há dois dispositivos que atuam em

uma configuração ativo-à espera.

Gerente NAC

O gerente de Cisco NAC pode ser configurado na Alta disponibilidade do modo onde há dois gerentes NAC que atuam em uma configuração ativo-à espera. A configuração completa em um gerente é armazenada em um base de dados. O gerente do apoio sincroniza seu base de dados com o base de dados no gerente ativo. Todas as alterações de configuração feitas ao gerente ativo são empurradas imediatamente para o gerente à espera. Os seguintes pontos chaves fornecem um sumário de nível elevado da Alta disponibilidade da operação do gerente:

- A Alta disponibilidade do modo do gerente de Cisco NAC é uma configuração de dois-server ativa ou passiva em que um gerente à espera atua como um backup a um gerente ativo.
- O gerente ativo de Cisco NAC executa todas as tarefas para o sistema. O gerente do apoio monitora o gerente ativo e mantém seu base de dados sincronizado com o base de dados do gerente ativo.
- Ambos os gerentes de Cisco NAC compartilham de um IP virtual do serviço para a relação confiada eth0. O IP do serviço deve ser usado para o certificado SSL.
- Os gerentes preliminares e secundários de Cisco NAC trocam pacotes de heartbeat UDP cada 2 segundos. Se o temporizador ritmado expira, a comutação classificada ocorre.
- Para assegurar um gerente ativo de Cisco NAC está sempre disponível, sua relação confiada (eth0) deve estar acima. A situação deve ser evitada onde um gerente é ativo mas não é direta acessível sua relação confiada. Esta circunstância ocorre se o gerente à espera recebe pacotes de heartbeat do gerente ativo, mas a relação do eth0 do gerente ativo falha). O mecanismo da link-detecção permite que o gerente à espera saiba quando a relação do eth0 do gerente ativo se torna não disponível.
- Você pode escolher “configura automaticamente” a relação Eth1 na página da administração > do gerente > do Failover CCA. Contudo, você deve manualmente configurar a outra (Eth2 ou Eth3) Alta disponibilidade das relações com um endereço IP de Um ou Mais Servidores Cisco ICM NT e um netmask antes que você configure a Alta disponibilidade no gerente de Cisco NAC.
- O eth0, as relações Eth1, e Eth2/Eth3 podem ser usados para pacotes de heartbeat e sincronização de base de dados. Além, toda a relação (COM) de série disponível pode igualmente ser usada para pacotes de heartbeat. Se você se está usando mais de uma destas relações, o Failover ocorre somente se todas as relações da pulsação do coração falham.

Nota: A Alta disponibilidade dos pares do gerente de Cisco NAC não pode ser separada por um link da camada 3.

Para mais detalhes, refira a documentação do gerente de Cisco NAC em:

http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_ha.html

Server de Cisco NAC

Para fornecer a proteção contra um ponto de falha único, o server de Cisco NAC pode ser configurado na Alta disponibilidade do modo. A Alta disponibilidade do modo para o server de Cisco NAC é similar àquela do gerente de Cisco NAC e igualmente usa uma configuração ativo-à

espera. Os server de Cisco NAC ainda compartilham de um endereço IP de Um ou Mais Servidores Cisco ICM NT virtual (chamado um IP do serviço), mas não compartilham de endereços MAC virtuais.

Os seguintes pontos chaves fornecem uma visão geral de alto nível da Alta disponibilidade da operação de servidor de Cisco NAC:

- A Alta disponibilidade do modo do server de Cisco NAC é uma configuração de dois-server ativo-passiva em que uma máquina do servidor à espera de Cisco NAC atua como um backup a um server ativo de Cisco NAC.
- O server ativo de Cisco NAC executa todas as tarefas para o sistema. Porque a maioria da configuração do servidor está armazenada no gerente de Cisco NAC, quando o Failover do server ocorre, o gerente empurra a configuração para o server novo-ativo.
- O server à espera de Cisco NAC não envia nenhuns pacotes entre suas relações.
- O server à espera de Cisco NAC monitora a saúde do servidor ativo através de uma relação da pulsação do coração (série e umas ou várias relações UDP). Os pacotes de heartbeat podem ser enviados na interface serial, na relação Eth2 dedicada, na relação Eth3 dedicada, ou na relação Eth0/Eth1 (se nenhuma relação Eth2 ou Eth3 está disponível).
- Os server preliminares e secundários de Cisco NAC trocam pacotes de heartbeat UDP cada dois segundos. Se o temporizador ritmado expira, a comutação classificada ocorre.
- Além do que o Failover pulsação do coração-baseado, o server de Cisco NAC igualmente fornece o Failover link-baseado baseado no eth0 ou na falha do link Eth1. O server envia pacotes do ping ICMP a um endereço IP externo através do eth0 e/ou da relação Eth1. O Failover ocorre somente se um server de Cisco NAC pode sibilar os endereços externos.

Para mais detalhes, refira a documentação de servidor de Cisco NAC em:

http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/47/hi_ha.html

Diretório ativo SingleSignOn (diretório ativo SSO)

O diretório ativo SSO de Windows é a capacidade para uma ferramenta NAC de Cisco automaticamente aos usuários de login já autenticada a um controlador de domínio backend do Kerberos (servidor ative directory). Esta capacidade elimina a necessidade de registrar em Cisco NAC o server depois que você é registrado já no domínio. Para mais detalhes sobre configurar o diretório ativo SSO em uma ferramenta NAC de Cisco, vá a:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cas/s_adsso.html

Considerações do ambiente do domínio do Windows

Àvista de um desenvolvimento NAC, as mudanças à política do script do início de uma sessão podem ser exigidas. Os scripts do início de uma sessão de Windows podem ser classificados como scripts da partida ou da parada programada e do fazer logon ou do fazer logoff. Windows executa a partida e a parada programada passa pelo processo de script da “em um contexto máquina.” Executar os scripts funciona somente se a ferramenta NAC de Cisco abre os recursos de rede apropriados exigidos pelo script para o papel particular quando estes scripts estão executados na bota PC acima ou na parada programada, que são tipicamente o papel não autenticado. Os scripts do fazer logon e do fazer logoff são executados do “em um contexto usuário,” que significa que o script de logon executa depois que o usuário entrou com Windows

GINA. O script de logon pode não executa se a autenticação ou a avaliação da postura da máquina cliente não terminam e o acesso de rede não está concedido a tempo. Estes scripts podem igualmente ser interrompidos pelo endereço IP de Um ou Mais Servidores Cisco ICM NT refrescam iniciado pelo agente de Cisco NAC depois que um evento do fazer logon OOB. Para obter mais informações sobre das alterações necessárias aos scripts do início de uma sessão, vá a:

http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a70c18.shtml

Configurando a ferramenta NAC de Cisco para o início de uma sessão do agente e a avaliação da postura do cliente

O agente de Cisco NAC e o agente da Web de Cisco NAC fornecem a avaliação e a remediação locais da postura para máquinas cliente. Os usuários transferem e instalam o agente de Cisco NAC ou o agente da Web de Cisco NAC (software do cliente de leitura apenas), que podem verificar o registro, os processos, os aplicativos, e os serviços do host. Para mais detalhes sobre o agente e a avaliação e a remediação da postura, vá a:

http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/47/cam/m_agntd.html

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems