Ferramenta NAC: Postura do Mac OSX AV no exemplo de configuração da liberação 4.5 de Cisco NAC

Índice

Introdução

Este documento descreve como configurar a avaliação limpa da postura do agente do acesso de Mac OS X através do console de web do gerente do Network Admission Control (NAC) para a liberação 4.5.

A avaliação da postura do Mac nesta liberação é limitada ao apoio AV/AS somente. Refira os Release Note do Dispositivo Cisco NAC (Clean Access) para a lista de AV/AS que são apoiados no Mac OSX.

Pré-requisitos

Requisitos

Termine estas etapas antes que você tente esta configuração:

Este documento supõe que você está executando a liberação 4.5 da ferramenta NAC de Cisco e

isso você terminou as seguintes etapas de acordo com as diretrizes na ferramenta NAC de Cisco – Guia de Instalação e Configuração limpo do Access Manager, a liberação 4.5:

1. Instale ou promova seu gerente NAC e server NAC com liberação 4.5 da ferramenta NAC de Cisco como descrito no guia de início rápido da instalação de hardware da ferramenta NAC de Cisco, a liberação 4.5.
2. Assegure-se de que o agente o mais atrasado de Mac OS X (versão 4.5) e os pacotes de apoio AV/AS estejam disponíveis em seu gerente NAC como descrito em configurem e se transfira atualizações.
3. Crie uma página de login do usuário padrão como descrito na página do login de usuário.
4. Exija o uso do Mac OS X que o agente limpo 4.5 do acesso como descrito em exige o uso do agente.
5. Crie uns ou vários papéis de usuário para usuários de Macintosh como descrito em criam papéis de usuário.

Nota: Refira por favor a seção das limitações do agente de MAC OS X para versões do OS X e Produtos AV/AS e tipos da exigência que são apoiados para a avaliação da postura do Mac.

Componentes Utilizados

A informação neste documento é baseada na liberação 4.5 de Cisco NAC.

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.

Avaliação da postura do Mac com AntiVirus dos moluscos (ClamAV)

O objetivo deste procedimento é verificar que ClamAV 1.1.0 está instalado e atualizado com as definições de vírus as mais atrasadas na máquina cliente.

Se ClamAV 1.1.0 não é instalado na máquina cliente, você deve fornecer o usuário um link ao Web site de ClamAV a fim transferir e instalar o software. Em seguida, você deve verificar que ClamAV está atualizado com as definições as mais atrasadas. Se não, o agente limpo do acesso pode comunicar-se com os moluscos AV com um atendimento API (com o tipo da exigência da *atualização AV*) e pedir ClamAV para atualizar-se.

Nota: Até à data da liberação de Cisco NAC 4.5, o tipo da exigência da atualização AV é apoiado somente com ClamWin AV. Para todo AV/AS restante, uma *distribuição do link* ou um tipo *local da verificação de* exigência podem ser configurados aos usuários do remediate se suas definições de vírus não são atualizadas.

Etapa 1. Configurar uma regra para verificar se ClamAV é instalado

1. Vai ao **Gerenciamento de dispositivos > o acesso limpo > agente limpo > regras do acesso > regra nova AV**.
2. Datilografe um nome para a regra. Este exemplo usa *Is_Clamwin_Installed_OSX*.**Nota:** Seja descritivo de modo que você possa facilmente identificar a finalidade da regra. Você pode não usar dígitos e relevos no nome, mas nenhum espaço.
3. Escolha **ClamWin da** lista de drop-down do vendedor do Antivirus.
4. Escolha a **instalação do** tipo gota-para baixo.
5. Escolha o **Mac OSX da** lista de drop-down do sistema operacional.A tabela na parte inferior da página é povoada com estes valores.
6. Verifique a caixa de verificação da **instalação** para ver se há 1.x.
7. Datilografe uma descrição no campo de texto da descrição da regra, e clique a **regra da salvaguarda**.

A regra nova AV é adicionada à parte inferior da lista da regra.

Etapa 2. Configurar uma exigência aos usuários de Remediate se ClamAV não é instalado

Se o agente limpo do acesso detecta que ClamAV 1.1.0 não está instalado na máquina cliente, quarantines o usuário. Neste momento, você pode configurar um tipo da exigência da *distribuição do link* a fim fornecer o usuário um link para transferir ClamAV 1.1.0.

1. Clique a aba **limpa do agente do acesso**, e clique então **exigências**.
2. Clique a **exigência nova**.
3. Escolha a **distribuição do link do** tipo lista de drop-down da exigência.
4. Escolha **imperativo do** tipo lista de drop-down do reforço.Neste exemplo, o utilizador final está informado desta exigência e não pode continuar ou ter o acesso de rede a menos que o sistema de cliente cumprir a exigência.Refira configurar uma exigência opcional/auditoria para obter informações sobre de outros tipos da aplicação.
5. Escolha o nível da prioridade da execução para esta exigência na máquina cliente.Uma alta prioridade (por exemplo, 1) significa que esta exigência está verificada no sistema antes de todas exigências restantes (e aparece nos diálogos limpos do agente do acesso nessa ordem). Este exemplo supõe que a verificação da instalação de ClamWin é a primeira exigência da postura e ajusta a prioridade a um (1).**Nota:** O agente de Mac OS X não apoia a remediação automática. Consequentemente, o tipo da remediação é ajustado ao manual. Também, as funções que aparecem na página de configuração nova da exigência (tipo, intervalo, e contagem de novas tentativas da remediação) não servem nenhuma finalidade quando você cria tipos da exigência para a remediação do cliente macintosh.
6. No campo de texto do link de arquivo URL, datilografe a URL a que os utilizadores finais devem ser dirigidos a fim transferir ClamAV 1.1.0.
7. No nome da exigência o texto arquivou, datilografa um nome exclusivo que transportasse a ação ao utilizador final.Este nome é visível aos usuários nos diálogos limpos do agente do acesso. Este exemplo usa a *transferência ClamAV*.
8. No campo de texto da descrição, datilografe uma descrição da exigência e das instruções guiar os usuários que não cumprem a exigência.
9. Clique a caixa de verificação do **Mac OS** alistada na seção do sistema operacional.
10. O clique **adiciona a exigência** a fim adicionar a exigência à lista da exigência.

A exigência nova é adicionada à lista da exigência.

Etapa 3. Trace a exigência da distribuição do link com a regra da instalação AV

1. Clique a aba **limpa do agente do acesso**, e clique então **exigências**.
2. Clique Exigência-**regras**.
3. Da lista de drop-down do nome da exigência, escolha a exigência que você criou em etapa 2.
4. Escolha o **Mac OSX da** lista de drop-down do sistema operacional.As regras criadas para o sistema operacional escolhido são indicadas na parte inferior da página.
5. Clique a caixa de verificação para a regra que você criou em etapa 1, e clique então a **atualização**.

Etapa 4. Configurar uma regra para verificar se ClamAV é atualizado

1. Vai ao **Gerenciamento de dispositivos > o acesso limpo > agente limpo > regras do acesso > regra nova AV**.
2. Datilografe um nome para a regra. Este exemplo usa *Is_ClamAV_Updated_OSX*.**Nota:** Seja descritivo de modo que você possa facilmente identificar a finalidade da regra. Você pode não usar dígitos e relevos no nome, mas nenhum espaço.
3. Escolha **ClamWin da** lista de drop-down do vendedor do Antivirus.
4. Escolha a **definição de vírus do** tipo lista de drop-down.
5. Escolha o **Mac OSX da** lista de drop-down do sistema operacional.As verificações da definição de vírus para a tabela do Mac OSX na parte inferior da página são povoadas.
6. Verifique a caixa de verificação da **instalação** para ver se há 1.x.
7. Datilografe uma descrição no campo de texto da descrição da regra, e clique a **regra da salvaguarda**.

A regra nova AV é adicionada à parte inferior da lista da regra.

Etapa 5. Configurar uma exigência aos usuários de Remediate se ClamAV não é atualizado

Se o agente limpo do acesso detecta que ClamAV 1.1.0 não está atualizado na máquina cliente, quarantines o usuário. Neste momento, o usuário é fornecido com um remediate do botão Update Button.

Uma vez que o usuário clica o botão Update Button, o agente limpo do acesso comunica-se com o software subjacente de ClamAV e pede-se ClamAV para atualizar-se.

Você pode configurar um tipo da exigência da atualização da definição AV a fim executar esta funcionalidade.

1. Clique a aba **limpa do agente do acesso**, e clique então **exigências**.
2. Clique a **exigência nova**.
3. Escolha a **atualização da definição AV do** tipo lista de drop-down da exigência.
4. Escolha **imperativo** o do tipo lista de drop-down do reforço.Neste exemplo, o utilizador final está informado desta exigência e não pode continuar ou ter o acesso de rede a menos que o sistema de cliente cumprir a exigência.Refira configurar uma exigência opcional/auditoria para obter informações sobre de outros tipos da aplicação.
5. Escolha o nível da prioridade da execução para esta exigência na máquina cliente.Uma alta

prioridade (por exemplo, 1) significa que esta exigência está verificada no sistema antes de todas exigências restantes (e aparece nos diálogos limpos do agente do acesso nessa ordem). Este exemplo supõe que a verificação da atualização de ClamWin é a segunda exigência da postura e ajusta a prioridade a dois (2).**Nota:** O agente de Mac OS X não apoia a remediação automática. Consequentemente, o tipo da remediação é ajustado ao manual. Também, note que as opções do tipo, do intervalo, e do contagem de novas tentativas da remediação que aparecem na página de configuração nova da exigência não servem nenhuma finalidade quando você cria tipos da exigência para a remediação do cliente macintosh.

6. Escolha **ClamWin – (Mac OS) da** lista de drop-down do nome de fornecedor do Antivirus.**Cuidado:** Certifique-se de você escolher o *ClamWin – opção (do Mac OS)*, não a opção de ClamWin.**Nota:** Até à data da liberação de Cisco NAC 4.5, o tipo da exigência da atualização AV é apoiado somente com Mac OSX de ClamAVon. Para todo AV/AS restante no Mac OSX, uma distribuição do link ou um tipo local da exigência da verificação podem ser configurados aos usuários do remediate se suas definições de vírus não são atualizadas.
7. No campo de texto do nome da exigência, datilografe um nome exclusivo que transporte a ação ao utilizador final.Este nome é visível aos usuários nos diálogos limpos do agente do acesso. Este exemplo usa a *atualização ClamAV*.
8. No campo de texto da descrição, datilografe uma descrição da exigência e das instruções guiar os usuários que não cumprem a exigência.
9. Clique a caixa de verificação do **Mac OS** alistada na seção do sistema operacional.
10. O clique **adiciona a exigência** a fim adicionar a exigência à lista da exigência.

A exigência nova é adicionada à lista da exigência.

Etapa 6. Trace a exigência da atualização da definição AV com a regra da definição de vírus

1. Clique a aba **limpa do agente do acesso**, e clique então **exigências**.
2. Clique Exigência-**regras**.
3. Da lista de drop-down do nome da exigência, escolha a exigência que você criou na etapa 5.
4. Escolha o **Mac OSX da** lista de drop-down do sistema operacional.As regras criadas para o sistema operacional escolhido são indicadas na parte inferior da página.
5. Clique a caixa de verificação para a regra que você criou em etapa 4, e clique então a **atualização**.

Etapa 7. Trace as exigências aos papéis

Neste momento, você pode ligar as exigências da postura (que foram traçadas às regras) ao papel em que o utilizador final é colocado.

1. Clique a aba **limpa do agente do acesso**, e clique então Papel-**exigências**.
2. Clique Papel-**exigências**.
3. Escolha o **papel normal do início de uma sessão do** tipo lista de drop-down do papel.
4. Do papel de usuário da lista de drop-down, escolha o papel onde você quer as exigências da postura ser aplicado. Este exemplo aplica as exigências da postura ao papel do *empregado.*As exigências criadas mais cedo neste exemplo são indicadas na parte inferior da página.
5. Verifique as caixas de seleção para ver se há as exigências que você quer aplicar a este

papel, e clique a **atualização**.

Etapa 8. Permita o acesso ao local da remediação no papel provisório

Uma vez que os usuários são encontrados para ser NON-complacentes, quarantined e estão colocados no papel provisório. Neste momento, os usuários devem poder alcançar os recursos da remediação (server AV, Web site, server da correção de programa, etc.) de modo que possam remediate eles mesmos.

Por esse motivo, você deve abrir o acesso apropriado no papel provisório. Neste exemplo, os usuários devem poder alcançar http://www.clamxav.com para ambas as exigências (atualização da instalação e da definição de vírus).

1. Escolha o **gerenciamento de usuário > os papéis de usuário**, e clique então a aba do **controle de tráfego**.
2. Clique o **host**.
3. Escolha o **papel provisório da** lista de drop-down, e enrole-o para baixo a parte inferior da lista.
4. Adicionar **clamxav.com à** lista permitida do host, e o clique **adiciona**.Esta etapa assegura-se de que o tráfego dos clientes a http://www.clamxav.com esteja permitido através dos server NAC.**Nota:** Estas duas circunstâncias são importantes:O server NAC usa a resposta de DNS do servidor DNS para abrir dinamicamente o acesso. Daqui, o tráfego de retorno do servidor DNS (resposta de DNS) deve atravessar o server NAC.Você deve ter um servidor DNS confiado definido. Para melhores prática, Cisco recomenda que você adiciona entradas específicas do servidor DNS aqui ao contrário de confiar todos os servidores DNS (*). Este exemplo adiciona o IP do servidor DNS (192.168.2.44) como um servidor DNS confiado. Você pode adicionar servidores DNS confiados múltiplos. Se você não tem um servidor DNS confiado definido, o gerente NAC recomenda-o em conformidade através de uma mensagem segundo as indicações desta imagem:

Verifique a experiência de usuário final

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

Esta encenação da verificação da postura do Mac supõe que sua instalação inicial NAC (gerente e server NAC) está completa e que o server NAC é alcançável das máquinas cliente. O Cisco Clean Access Agent 4.5.0.0 deve ser instalado no Mac que executa OSX 10.4 ou mais alto. Esta encenação supõe que o Mac não tem ClamAV instalado antes deste teste.

1. Início de uma sessão a seu agente limpo do acesso (versão 4.5.0.0).Quarantined e é-lhe convidado ao remediate.**Nota:** As caixas de seleção da CORRIDA são verificadas, mas não editável, porque as exigências são imperativas. Se uma exigência foi configurada como *opcional*, a caixa de verificação da CORRIDA seria editável, e você pode escolher saltar essa exigência.
2. Clique **Remediate**.Você é reorientado ao Web site de ClamAV.
3. Transfira e instale ClamAV.Você pôde ser alertado executar o motor do Antivirus dos moluscos antes que você possa usar ClamAV segundo as indicações desta imagem:
4. Siga as instruções na tela a fim terminar a instalação.O agente limpo do acesso indica o

estado da exigência de *ClamAV da transferência* como bem sucedido e move-se sobre para a segunda exigência (*atualização ClamAV*).Uma vez que ClamAV é atualizado, o estado da exigência de *ClamAV da atualização* indica bem sucedido.

5. Clique **completo** para entrar à rede.Uma vez que você entra com sucesso à rede, esta as mensagens aparecem.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Sustentação do produto do Dispositivo Cisco NAC (Clean Access)
- Suporte Técnico e Documentação - Cisco Systems