NAC 4.5: Exemplo de configuração da Importação-exportação da política

Índice

Introdução

Este documento fornece um guia passo a passo em como configurar a característica da Importação-exportação da política (TORTA) na liberação 4.5 de Cisco NAC. A finalidade desta característica é sincronizar os filtros do dispositivo, as regras do tráfego e da remediação, e os perfis da porta entre gerentes NAC (gerentes limpos do acesso). Quando esta característica é discutida, o gerente NAC onde as políticas são definidas está chamado o **mestre**, que pode empurrar ou sincroniza as políticas do tanto como como dez gerentes NAC (gerentes limpos do acesso), chamado **Receptor**. As políticas podem ser sincronizadas automaticamente com um temporizador do pré-ajuste ou com uma sincronização manual.

Pré-requisitos

Cisco recomenda que você têm a familiaridade com a interface da WEB do gerente de Cisco NAC (Access Manager limpo) e as políticas que são configurados tipicamente. Refira os Release Note para a liberação 4.5 de Cisco NAC para obter informações sobre do que é apoiado e não apoiado com TORTA.

Requisitos

Estabelecer os gerentes e server NAC de acordo com o Guia de Instalação e Configuração de Cisco NAC. Refira recomendações da melhor prática configurando a Importação-exportação da política do gerente NAC a fim identificar que gerente deve ser usado como o mestre e qual como o receptor. Este documento supõe que os gerentes do mestre e do receptor NAC estão identificados e as recomendações da melhor prática estão usadas.

Componentes Utilizados

A informação neste documento é baseada no software 4.5.0 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.

Note: Antes que você comece, confirme que o mestre e os receptores executam o exato as mesmas versões. Também, assegure-se de que os ajustes da atualização de Ruleset sob o **Gerenciamento de dispositivos > acesso limpo > atualizem >** fósforo da **atualização em** mestre e em todos os receptores.

O NAC configura

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

Termine estas etapas a fim configurar a importação/exportação da política entre gerentes NAC.

1. **Permita a sincronização da política no gerente mestre NAC:**No gerente do mestre NAC, navegue à administração > ao gerente CCA > à sincronização da política > permitem.Verifique a caixa da **sincronização da política da possibilidade**. Escolha **(permita a exportação da política) a** opção **mestra**, e clique a **atualização**.
2. **Identifique as políticas a ser empurradas:**Nesta etapa, você identifica as políticas que devem ser sincronizadas entre o CAM mestre e os receptores. Para este exemplo, o objetivo é sincronizar as políticas de controle do tráfego global entre os gerentes. Neste caso, a política global do tráfego baseado em ip deve ser escolhida sob papéis de usuário > controle de tráfego > IP (o papel provisório seleto, não-confiável > confiou na gota para baixo, como mostrado. Clique seleto. Esta regra não existe no receptor ainda.Consulte para adicionar políticas globais do tráfego baseado em ip para obter informações sobre de como configurar políticas do tráfego IP.Escolha a administração > Access Manager limpo > sincronização da política > configuram o mestre e verificam a caixa de verificação da possibilidade como mostrado e clicam a atualização.**Note**: Sincronizar o tráfego policia igualmente exige a sincronização de regras, de exigências, de exigências do papel, de filtros do dispositivo (tipos do PAPEL, da VERIFICAÇÃO) e de papéis.
3. **Adicionar/identifique os receptores:**Você pode adicionar acima a dez receptores apoiados a seu mestre. Neste exemplo, você adiciona um receptor ao gerente do mestre NAC.Escolha a administração > Access Manager limpo > sincronização da política > configuram o mestre. Sob o host Name/IP do receptor, adicionar o hostname (gerente do mestre o NAC deve poder resolver o DNS para o nome de host) ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do receptor. Adicionar uma descrição opcional e o clique adiciona.Uma vez que adicionado, o receptor novo aparece. Você pode adicionar os receptores múltiplos (até

dez apoiados) esta maneira. Na Alta disponibilidade (HA) das encenações, você precisa de adicionar nome de host virtual/compartilhado ou endereço IP de Um ou Mais Servidores Cisco ICM NT virtual/compartilhado dos pares HA à lista.

4. **Autorize os receptores:**Depois que você adiciona os receptores, é importante fixar a comunicação entre o mestre e os receptores. Somente um mestre autorizado pode empurrar políticas para um receptor. Similarmente, o mestre deve poder comunicar-se somente com os receptores autorizados. Também, uma confiança precisa de ser estabelecida para certificar-se que o mestre e os receptores são quem reivindica ser. O SSL é usado por esse motivo. Não somente o mestre e o receptor têm que identificar-se com a informação DN no certificado, mas igualmente precisa de ter seu certificado de identidade de uma autoridade confiada (CA). Na necessidade curto, mestra e do receptor de confiar Certificados de cada um.Desde que este documento é gerado de uma instalação de laboratório, os certificados auto-assinados são usados neste exemplo. Contudo, note que você precisa de usar um certificado assinado de CA em seu ambiente de produção. Refira recomendações da melhor prática configurando a Importação-exportação da política do gerente NAC para mais informação.No receptor, escolha a administração > o gerente CCA > o certificado SSL > X509.Identifique o certificado do gerente CCA e clique sobre o ícone sob a vista. No indicador que aparece, selecione e copie (clicar com o botão direito e cópia) a informação DN.O retorno ao gerente do mestre NAC sob a administração > o gerente CCA > a sincronização da política > configuram o mestre. Na parte inferior, sob a lista de receptores autorizados pelo nome destacado do certificado, pasta que a informação DN do certificado que você copiou do receptor na etapa e no clique precedentes adiciona.
5. **Permita a sincronização da política no gerente do receptor NAC:**No gerente do receptor NAC, navegue à administração > ao gerente CCA > à sincronização da política > permitem.Verifique a caixa da **sincronização da política da possibilidade**. Escolha a opção do **receptor (permita a importação da política)**, e clique a **atualização**.**Note**: Observe que a bandeira na parte superior gerencie o vermelho, que indica que este gerente NAC é permitido de ser um receptor.
6. **Autorize o mestre:**No mestre, escolha a administração > o gerente CCA > o certificado SSL > X509.Identifique o certificado do gerente CCA e clique sobre o ícone sob a vista. No indicador que aparece, selecione e copie (clicar com o botão direito e cópia) a informação DN.O retorno ao gerente do receptor NAC sob a administração > o gerente CCA > a sincronização da política > configuram o receptor. Ao lado do mestre autorizado, cole a informação DN do certificado que você copiou do mestre na etapa e na atualização precedentes do clique.
7. **Configurar a auto sincronização (opcional):**A sincronização da política pode ser manual ou automatizou. Uma sincronização manual pode ser executada em uma base como necessário, quando um auto temporizador da sincronização puder ser setup para executar automaticamente uma vez uma sincronização da política entre os gerentes NAC cada número *x de* dias (o mínimo é um dia) em um horário pré-determinado. Cisco recomenda-o fortemente executa uma sincronização manual e verifica que a sincronização trabalha com sucesso antes que você permita a auto sincronização entre seus gerentes NAC. Veja para pesquisar defeitos a fim compreender como você pode usar a sincronização manual para pesquisar defeitos as edições relativas à TORTA.A fim permitir a auto sincronização, navegue à administração > ao gerente CCA > à sincronização da política > auto sincronização no gerente do mestre NAC.Verifique **automaticamente a sincronização que parte do _(HH: milímetro: ss) cada** caixa de verificação dos **dias do _**.Incorpore a época da sincronização (1:00 AM neste exemplo) e como frequentemente (cada 15 dias neste

exemplo) esse você quer executar a auto sincronização.Verifique a caixa sob o **automóvel** a fim selecionar os receptores que recebem automaticamente políticas em uma base periódica, e clique a **atualização**.

Verificar

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

1. Navegue à administração > ao gerente CCA > à sincronização da política > sincronização manual no mestre.
2. Datilografe um nome (opcional) para a sincronização sob a descrição da sincronização
3. Selecione os receptores em que você quer executar a ação da sincronização. Verifique a caixa sob selecionado, e clique a **sincronização**. Neste exemplo, você tem somente um receptor, 172.23.117.10, assim que é escolhido.
4. Neste momento, o mestre executa uma verificação de sanidade PRE-sincronização contra o receptor. A verificação PRE-sincronização assegura-se de que os gerentes do mestre e do receptor NAC estejam configurados corretamente (para empurrar e receber políticas), e que a informação de autorização está correta, etc. Se há algum configuração ou erro da autorização, a verificação PRE-sincronização falha com Mensagens de Erro apropriados. Veja a seção da pesquisa de defeitos.
5. Se não há nenhuma edição da configuração ou da autorização, o mestre indica uma verificação PRE-sincronização bem sucedida.
6. A batida continua a terminar com sucesso a sincronização.
7. Vá ao gerente do receptor NAC e verifique que a regra de tráfego está sincronizada.

Troubleshooting

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

Registro

O sumário da sincronização é registrado sob o gerente CCA > a sincronização > a história da política no mestre e nos receptores.

No gerente do mestre NAC:

No gerente do receptor NAC:

Clique o ícone da lupa sob a ordem do início de uma sessão para ver log de transação detalhados:

```
*************** Master Log ***************

Starting policy import/export on Policy Sync Master.
Created dump file for policy: User Management -> User Roles -> List of Roles/Schedule
Created dump file for policy: Device Management > Clean Access > Clean Access Agent > Role-
Requirements
```

```
Created dump file for policy: Device Management > Filters > Devices
Created dump file for policy: User Management->Traffic Control->IP
Created dump file for policy: User Management->Traffic Control->Host
Created dump file for policy: User Management->Traffic Control->Ethernet
Dump file creation is complete.
Created policy import/export dump file.
Created  policy import/export header file.
Created policy import/export tar file.


*************** Receiver Log ***************

Starting policy import on Policy Sync Receiver.
Hash value is a match.
Policy Sync Master and Receiver CAM versions match.
All SQL statements successfully executed
All requirements are valid.
All rules are valid.
Role tables integrity check is successful.
```

Importação/exportação da política terminada com sucesso no receptor da sincronização da política.

Problemas

1. **Acesso negado receptor. Este CAM não é autorizado como o mestre da sincronização da política no receptor.**Este erro significa tipicamente que o receptor rejeita a sincronização da política porque a informação DN mestra é desconfigurada no gerente do receptor NAC. Escolha a administração > o gerente CCA > a sincronização da política > configuram o receptor no receptor e certificam-se de que a informação “mestra” autorizada está configurada corretamente.
2. **Este receptor não é autorizado**Esta mensagem significa tipicamente que o receptor não setup para a autorização ou os parâmetros de autorização (a informação DN do receptor) configurados no gerente do mestre NAC estão incorretos. Escolha a administração > o gerente CCA > a sincronização da política > configuram o mestre no mestre e certificam-se que a informação DN do certificado do receptor existe sob a lista de receptores autorizados pelo nome destacado do certificado e está configurada corretamente.
3. **Este host não é configurado como o receptor da sincronização da política.**Esta mensagem significa tipicamente que o mestre tenta à sincronização a um host que ou não seja permitido para a sincronização da política ou não é configurada para ser um receptor. Escolha a administração > o gerente CCA > a sincronização > os ajustes da política no gerente NAC que é escolhido ser o receptor e se assegurar de que a caixa permitida sincronização da política esteja verificada e que o botão de rádio está ajustado ao receptor (permita a política de importação).

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems