ASA/PIX: Como usar o CLI para promover a imagem do software em um par de failover

Índice

Introdução

Este documento descreve como usar o CLI a fim promover a imagem do software em um par de failover do Dispositivos de segurança adaptáveis Cisco ASA série 5500.

Nota: O Security Device Manager adaptável (ASDM) não trabalha se você promove (ou downgrade) o software da ferramenta de segurança de 7.0 a 7.2 diretamente ou promove (ou downgrade) o software ASDM de 5.0 a 5.2 diretamente. Você deve promover (ou downgrade) na ordem incremental.

Para obter mais informações sobre de como promover o ASDM e a imagem do software no ASA, refira o PIX/ASA: Promova uma imagem do software usando o ASDM ou o exemplo da configuração de CLI

Nota: No modo do multicontext, você não pode usar o **comando copy tftp flash** promover ou degradar a imagem PIX/ASA em todos os contextos; é apoiada somente no modo exec do sistema.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Ferramenta de segurança adaptável de Cisco (ASA) com versão 7.0 e mais recente
- Versão ASDM Cisco 5.0 e mais atrasado

Nota: Refira permitir o acesso HTTPS para o ASDM para obter informações sobre de como permitir que o ASA seja configurado pelo ASDM.

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.

Produtos Relacionados

Esta configuração pode igualmente ser usada com versão de software 7.0 da ferramenta de segurança da série do Cisco PIX 500 e mais atrasado.

Convenções

Refira as convenções dos dicas técnicas da Cisco para obter informações sobre das convenções de documento.

Configuração

Execute elevações do Zero-tempo ocioso da máquina para pares de failover

As duas unidades em uma configuração de failover devem ter a mesma (versão de software principal (primeiro número) e menor do segundo número). Contudo, você não precisa de manter a paridade da versão nas unidades durante o processo de upgrade; você pode ter versões diferentes no software que é executado em cada unidade e ainda manter o apoio do Failover. A fim assegurar a compatibilidade e a estabilidade a longo prazo, Cisco recomenda que você promove ambas as unidades à mesma versão o mais cedo possível.

Há 3 tipos de elevações disponíveis. São os seguintes:

1. **Versão de manutenção** — Você pode promover de toda a versão de manutenção a qualquer outra versão de manutenção dentro de uma versão menor. Por exemplo, você pode promover 7.0(1) a 7.0(4) sem primeiramente instalar as versões de manutenção in-between.
2. **Versão menor** — Você pode promover de uma versão menor à versão menor seguinte. Você não pode saltar uma versão menor. Por exemplo, você pode promover 7.0 a 7.1. Promover de 7.0 diretamente a 7.2 não é apoiado para elevações do zero-tempo ocioso da máquina; você deve primeiramente promover a 7.1
3. **Versão principal** — Você pode promover da última versão menor da versão anterior à versão principal seguinte. Por exemplo, você pode promover 7.9 a 8.0, supondo que 7.9 são a última versão menor na liberação 7.x.

Promova configuração de failover ativa/à espera

Termine estas etapas a fim promover duas unidades *configuração de failover ativa/à espera*:

1. Transfira o software novo a ambas as unidades, e especifique a imagem nova para carregar com o comando boot system.Consulte para promover uma imagem do software e uma imagem ASDM usando o CLI para mais informação.
2. Recarregue a unidade em standby para carreg a imagem nova incorporando o comando reload-à espera do Failover na unidade ativa como mostrado abaixo:`active#failover reload-standby`
3. Quando a unidade em standby terminou o recarregamento e está no estado pronto à espera, force a unidade ativa para falhar sobre à unidade em standby inscrevendo o comando no failover ative na unidade ativa.`active#no failover active` **Nota:** Use o comando show failover a fim verificar que a unidade em standby está no estado pronto à espera.
4. Recarregue a unidade ativa anterior (agora a unidade em standby nova) inscrevendo o comando reload:`newstandby#reload`
5. Quando a unidade em standby nova terminou o recarregamento e está no estado pronto à espera, retorne a unidade ativa original ao status ativo inscrevendo o comando failover ative:`newstandby#failover active`

Isto termina o processo de promover par de failover ativo/à espera.

Promova configuração de failover ativa/ativa

Termine estas etapas a fim promover duas unidades *configuração de failover ativa/ativa*:

1. Transfira o software novo a ambas as unidades, e especifique a imagem nova para carregar com o comando boot system.Consulte para promover uma imagem do software e uma imagem ASDM usando o CLI para mais informação.
2. Faça a ambos os grupos do Failover o active na unidade primária inscrevendo o comando failover ative no espaço da execução do sistema da unidade primária:`primary#failover active`
3. Recarregue a unidade secundária para carreg a imagem nova incorporando o comando reload-à espera do Failover ao espaço da execução do sistema da unidade primária:`primary#failover reload-standby`
4. Quando a unidade secundária terminou o recarregamento, e ambos os grupos do Failover estão no estado pronto à espera nessa unidade, fazem a ambos os grupos do Failover o active na unidade secundária usando o comando no failover ative no espaço da execução do sistema da unidade primária:`primary#no failover active` **Nota:** Use o comando show failover a fim verificar que ambos os grupos do Failover estão no estado pronto à espera na unidade secundária.
5. Certifique-se que ambos os grupos do Failover estão no estado pronto à espera na unidade primária, e recarregam então a unidade primária usando o comando reload:`primary#reload`
6. Se os grupos do Failover são configurados com o comando cancelar, tornar-se-ão automaticamente ativos em sua unidade designada depois que o atraso cancelar passou. Se os grupos do Failover não são configurados com o comando cancelar, você pode retorná-los ao status ativo em suas unidades designadas usando o comando group do active do Failover.

Troubleshooting

%ASA-5-720012: ((VPN-Secundário) Falha na atualização do tempo de execução do IPSec na unidade em espera (ou) %ASA-6-720012: ((VPN-unidade) Falha na atualização do tempo de execução de dados na unidade em espera

Problema

Uma destas Mensagens de Erro aparecem quando você tenta atualizar a Ferramenta de Segurança Adaptável da Cistos (ASA):

```
%ASA-5-720012: (VPN-Secundário) Falha na atualização do tempo de execução do failover do IPSec
na unidade em espera.

%ASA-6-720012: (VPN-unidade) Falha na atualização do tempo de execução do failover do IPsec na
unidade em espera.
```

Solução

Estes Mensagens de Erro são erros informativos. As mensagens não impactam a funcionalidade do ASA ou do VPN.

Estas mensagens aparecem quando o subsistema do failover VPN não pode atualizar os dados do tempo de execução do IPSEC relacionados ao túnel de IPsec correspondente que foi apagado da unidade em pespera. A fim resolver estes, execute o **comando standby do wr na** unidade ativa.

Dois erros foram arquivados para endereçar este comportamento; você pode promover a uma versão de software do ASA onde estes erros são fixos. Refira ao Cisco bug IDs CSCtj58420 (somente clientes registrados) e CSCtn56517 (somente clientes registrados) para mais informação.

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Adaptive Security Device Manager
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems