ASA/PIX: Configurar Failover ativo/à espera no modo transparente

Índice

Introdução

A configuração de failover exige dois mecanismos de segurança conectados entre si através de um link de failover dedicado e, opcionalmente, de um link de failover stateful. A integridade das interfaces ativas e das unidades é monitorada para determinar se as condições específicas do failover são atendidas. Se essas condições são atendidas, o failover ocorre.

A ferramenta de segurança apoia duas configurações de failover:

- Failover Ativo/Ativo
- Failover ativo/à espera

Cada configuração de failover tem seu próprio método para determinar e executar o Failover. Com Failover ativo/ativo, ambas as unidades podem passar o tráfego de rede. Isto deixa-o configurar o Balanceamento de carga em sua rede. Failover ativo/ativo está somente disponível nas unidades que são executado no modo de contexto múltiplo. Com Failover ativo/à espera, somente uma unidade passa o tráfego quando a outra unidade esperar em um estado à espera. Failover ativo/à espera está disponível nas unidades em que seja executado escolhem ou modo de contexto múltiplo. Ambas as configurações de failover apoiam o stateful ou o Failover (regular) apátrida.

Um Firewall transparente, é um Firewall da camada 2 que atue como um *Bump In The Wire*, ou um *firewall furtivo*, e não é visto como um salto do roteador aos dispositivos conectados. A ferramenta de segurança conecta a mesma rede em suas portas internas e externas. Como o firewall não é um salto na rota, você pode facilmente introduzir um firewall transparente em uma rede existente; é desnecessário especificar um novo endereço o IP. Você pode ajustar a ferramenta de segurança adaptável para ser executado no modo de firewall distribuído padrão ou no modo de firewall transparente. Quando você muda modos, a ferramenta de segurança adaptável cancela a configuração porque muitos comandos não são apoiados nos ambos os modos. Se você já tem uma configuração povoada, seja certo suportar esta configuração antes que você mude o modo; você pode usar esta configuração de backup para a referência quando você cria uma configuração nova. Refira o exemplo transparente da configuração de firewall para obter mais informações sobre da configuração do dispositivo do Firewall no modo transparente.

Este documento focaliza em como configurar Failover ativo/à espera no modo transparente na ferramenta de segurança ASA.

Nota: O Failover VPN não é apoiado nas unidades que são executado no modo de contexto múltiplo. O failover de VPN está disponível somente nas configurações de **Failover Ativo/Standby**.

A Cisco recomenda que você não use a interface de gerenciamento para o failover, especialmente o failover stateful no qual o Security Appliance envia constantemente informações de conexão de um Security Appliance para o outro. A interface do failover deverá ser pelo menos da mesma capacidade que as interfaces que transmitem tráfego normal e, enquanto as interfaces no ASA 5540 são gigabit, a interface de gerenciamento é somente FastEthernet. A interface de gerenciamento é projetada para o tráfego de gerenciamento somente e especificada como management0/0. Mas, você pode usar o comando do **Gerenciamento-somente** a fim configurar toda a relação para ser uma relação do Gerenciamento-somente. Além disso, para Management 0/0, é possível desabilitar o modo somente de gerenciamento para que a interface possa transmitir tráfego da mesma forma que qualquer outra. Refira a referência de comandos do dispositivo do Cisco Security, versão 8.0 para obter mais informações sobre do comando do **Gerenciamento-somente**.

Este manual de configuração fornece uma configuração de exemplo para incluir uma breve introdução ao PIX/ASA tecnologia ativa/à espera 7.x. Consulte a Referência de Comandos do ASA/PIX para obter mais detalhes sobre a teoria por trás desta tecnologia.

Pré-requisitos

Requisitos

Requisito de hardware

As duas unidades em uma configuração de failover devem ter a mesma configuração de hardware. Devem ser o mesmo modelo, têm o mesmos número e tipos de relações, e o mesmo valor de RAM.

Nota: As duas unidades não precisam de ter a memória Flash do mesmo tamanho. Se você usa unidades com tamanhos de memória flash diferentes em sua configuração de failover, certifique-se que a unidade com a memória Flash menor tem bastante espaço para acomodar os arquivos de imagem de software e os arquivos de configuração. Se não faz, a sincronização de configuração da unidade com a memória Flash maior à unidade com a memória Flash menor falha.

Requisito de software

As duas unidades em uma configuração de failover devem reagir dos modos operacionais (distribuídos ou transparentes, únicos ou contexto múltiplo). Devem ter a mesma (versão de software principal (primeiro número) e menor do segundo número), mas você pode usar versões diferentes do software dentro de um processo de upgrade; por exemplo, você pode promover uma unidade da versão 7.0(1) à versão 7.0(2) e mandar o Failover permanecer ativo. Cisco recomenda que você promove ambas as unidades à mesma versão para assegurar a compatibilidade a longo prazo.

Refira as elevações zero de execução do tempo ocioso da máquina para a seção dos pares de failover do *guia do comando line configuration do dispositivo do Cisco Security, versão 8.0* para obter mais informações sobre de como promover o software em um par de failover.

Licencie exigências

Na plataforma da ferramenta de segurança ASA, pelo menos uma das unidades deve ter uma **licença ilimitada (do UR)**.

Nota: Pode ser que seja necessário atualizar as licenças em um par de failover para se obter características e benefícios adicionais. Refira a elevação da chave de licença em um par de failover para mais informação.

Nota: Os recursos licenciado (tais como o SSL O VPN espreita ou contextos de segurança) em ambas as ferramentas de segurança que participam no Failover devem ser idênticos.

Componentes Utilizados

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

- Ferramenta de segurança ASA com versão 7.x e mais tarde

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração também pode ser utilizada com estas versões de hardware e software:

- Ferramenta de segurança PIX com versão 7.x e mais tarde

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Failover ativo/à espera

Esta seção descreve Failover ativo/à espera e inclui estes assuntos:

- Vista geral ativa/à espera do Failover
- Estado preliminar/secundário e status ativo/em standby
- Iniciação e sincronização de configuração do dispositivo
- Replicação do comando
- Disparadores do Failover
- Ações do Failover

Vista geral ativa/à espera do Failover

Failover ativo/à espera deixa-o usar uma ferramenta de segurança à espera para tomar sobre a funcionalidade de uma unidade falha. Quando a unidade ativa falha, mudar ao estado à espera quando as mudanças de unidade em standby ao estado ativo. A unidade que se torna ativa supõe os endereços IP de Um ou Mais Servidores Cisco ICM NT, ou, para um Firewall transparente, o endereço IP de gerenciamento, e endereços MAC da unidade falha e começa a passar o tráfego. A unidade que está agora no estado à espera toma sobre os endereços IP em standby e endereços MAC. Porque os dispositivos de rede não veem nenhuma mudança no MAC ao endereço IP de Um ou Mais Servidores Cisco ICM NT que se emparelha, nenhuma mudança das

entradas de ARP ou cronometra para fora em qualquer lugar na rede.

Nota: Para o modo de contexto múltiplo, a ferramenta de segurança pode falhar sobre a unidade inteira, que inclui todos os contextos, mas não pode falhar sobre contextos individuais separadamente.

Estado preliminar/secundário e status ativo/em standby

Os principais diferença entre as duas unidades em um par de failover são relacionados a que a unidade é ativa e a que a unidade é à espera, a saber que os endereços IP de Um ou Mais Servidores Cisco ICM NT a se usar e que a unidade é preliminar e passam ativamente o tráfego.

Algumas diferenças existem entre as unidades baseadas em que unidade é preliminar, como especificado na configuração, e que unidade é secundária:

- A unidade primária transforma-se sempre a unidade ativa se ambas as unidades começam acima ao mesmo tempo (e seja da saúde operacional igual).
- O MAC address da unidade primária é acoplado sempre com os endereços IP de Um ou Mais Servidores Cisco ICM NT ativos. A exceção a esta regra ocorre quando a unidade secundária é ativa e não pode obter o endereço MAC principal sobre o link failover. Neste caso, o MAC address secundário é usado.

Iniciação e sincronização de configuração do dispositivo

A sincronização de configuração ocorrer quando um ou ambo o dispositivo na bota do par de failover. As configurações são sincronizadas sempre da unidade ativa à unidade em standby. Quando a unidade em standby termina sua partida inicial, cancela sua configuração running, à exceção dos comandos failover que são precisados de se comunicar com a unidade ativa, e a unidade ativa envia sua configuração completa à unidade em standby.

A unidade ativa é determinada por estes:

- Se uma unidade carreg e detecta um par já operativo como o active, transforma-se a unidade em standby.
- Se as botas de uma unidade e não detectam um par, ele transformam-se a unidade ativa.
- Se ambas as unidades carreg simultaneamente, a unidade primária transforma-se a unidade ativa, e a unidade secundária transforma-se a unidade em standby.

Nota: Se as botas da unidade secundária e não detectam a unidade primária, ele transformam-se a unidade ativa. Usa seus próprios endereços MAC para os endereços IP de Um ou Mais Servidores Cisco ICM NT ativos. Quando a unidade primária se tornar disponível, as mudanças que de unidade secundária o MAC endereça àqueles da unidade primária, que pode causar uma interrupção em seu tráfego de rede. A fim evitar isto, configurar o par de failover com endereços MAC virtuais. Consulte a seção Configuração do Failover Ativo/Standby deste documento para obter mais informações.

Quando a replicação começar, o console da ferramenta de segurança nos indicadores de unidade ativa a `replicação de configuração do começo da` mensagem`: Enviando para acoplar-se`, e, quando está completa, a ferramenta de segurança indica a `replicação do fim de configuração da` mensagem `para acoplar-se.` Dentro da replicação, os comandos entered na unidade ativa não podem replicate corretamente à unidade em standby, e os comandos entered na unidade em standby podem ser overwritten pela configuração que replicated da unidade ativa. Não incorpore

comandos em uma ou outra unidade ao par de failover dentro do processo da replicação de configuração. O dependente em cima do tamanho da configuração, replicação pode tomar de alguns segundos a diversos minutos.

Da unidade secundária, você pode observar que a mensagem da replicação como ela sincroniza da unidade primária:

```
ASA> .

        Detected an Active mate
Beginning configuration replication from mate.
End configuration replication from mate.

ASA>
```

Na unidade em standby, a configuração existe somente em memória running. A fim salvar a configuração à memória Flash após a sincronização, incorpore estes comandos:

- Para o único modo do contexto, inscreva o **comando copy running-config startup-config na** unidade ativa. O comando replicated à unidade em standby, que continua escrever sua configuração à memória Flash.
- Para o modo de contexto múltiplo, inscreva o **comando copy running-config startup-config na** unidade ativa do espaço da execução do sistema e de dentro de cada contexto no disco. O comando replicated à unidade em standby, que continua escrever sua configuração à memória Flash. Os contextos com configurações de inicialização em servidores internos são acessíveis de uma ou outra unidade sobre a rede e não precisam de ser salvar separadamente para cada unidade. Alternativamente, você pode copiar os contextos no disco da unidade ativa a um servidor interno, e copia-os então ao disco na unidade em standby, onde se tornam disponíveis quando os reloads da unidade.

Replicação do comando

A replicação do comando flui sempre da unidade ativa à unidade em standby. Enquanto os comandos são incorporados na unidade ativa, estão enviados através do link failover à unidade em standby. Você não tem que salvar a configuração ativa à memória Flash para replicate os comandos.

Nota: As mudanças feitas na unidade em standby não replicated à unidade ativa. Se você executar um comando na unidade de standby, o Security Appliance exibirá a mensagem **** WARNING **** Configuration Replication is NOT performed from Standby unit to Active unit. As configurações são sincronizadas já não. Esta mensagem é indicada mesmo se você incorpora os comandos que não afetam a configuração.

Se você inscreve o **comando write standby na** unidade ativa, a unidade em standby cancela sua configuração running, à exceção dos comandos failover usados para comunicar-se com a unidade ativa, e a unidade ativa envia sua configuração completa à unidade em standby.

Para o modo de contexto múltiplo, quando você inscreve o **comando write standby no** espaço da execução do sistema, todos os contextos replicated. Se você inscreve o comando write standby dentro de um contexto, o comando replicates somente a configuração do contexto.

Os comandos replicados são armazenados na configuração running. A fim salvar os comandos replicados à memória Flash na unidade em standby, incorpore estes comandos:

- Para o único modo do contexto, inscreva o **comando copy running-config startup-config na** unidade ativa. O comando replicated à unidade em standby, que continua escrever sua configuração à memória Flash.
- Para o modo de contexto múltiplo, inscreva o **comando copy running-config startup-config na** unidade ativa do espaço da execução do sistema e dentro de cada contexto no disco. O comando replicated à unidade em standby, que continua escrever sua configuração à memória Flash. Os contextos com configurações de inicialização em servidores internos são acessíveis de uma ou outra unidade sobre a rede e não precisam de ser salvar separadamente para cada unidade. Alternativamente, você pode copiar os contextos no disco da unidade ativa a um servidor interno, e copia-os então ao disco na unidade em standby.

Disparadores do Failover

A unidade pode falhar se um destes eventos ocorre:

- A unidade tem uma falha do hardware ou uma falha de energia.
- A unidade tem uma falha de software.
- Falha monitorada demais das relações.
- **O comando no failover ative** é inscrito na unidade ativa, ou o **comando failover ative** é inscrito na unidade em standby.

Ações do Failover

Failover ativo/à espera, o Failover ocorre em uma base da unidade. Mesmo nos sistemas que são executado no modo de contexto múltiplo, você não pode individual ou em grupo do Failover dos contextos.

Esta tabela mostra a ação do Failover para cada evento de falha. Para cada evento de falha, a tabela mostra a política do Failover (Failover ou sem falha), a ação tomada pela unidade ativa, a ação tomada pela unidade em standby, e todas as notas especiais sobre a condição e as ações do Failover. A tabela mostra o comportamento do Failover.

Evento de falha	Política	Ação ativa	Ação à espera	Notas
Unidade ativa falhada (potência ou hardware)	Failover	n/a	Torne-se ativo; marque o active como falhado	Nenhum mensagem Hello Messages é recebido em toda a relação monitorada ou no link failover.
Anteriormente a unidade ativa recupera	Sem falha	Torne-se à espera	Nenhuma ação	Nenhum

Unidade em standby falhada (potência ou hardware)	Sem falha	Marque o apoio como falhado	n/a	Quando a unidade em standby é marcada como falhado, a unidade ativa não tenta ao Failover, mesmo se o ponto inicial da falha da relação é ultrapassado.
Link failover falhado dentro da operação	Sem falha	Marque a relação do Failover como falhada	Marque a relação do Failover como falhada	Você deve restaurar o link failover o mais cedo possível porque a unidade não pode Failover à unidade em standby quando o link failover estiver para baixo.
Link failover falhado na partida	Sem falha	Marque a relação do Failover como falhada	Torne-se ativo	Se o link failover está para baixo na partida, ambas as unidades tornam-se ativas.
Link da comutação classificada falhado	Sem falha	Nenhuma ação	Nenhuma ação	A informação de estado torna-se expirado, e as sessões são terminadas se um Failover ocorre.
Falha da relação na unidade ativa acima do ponto inicial	Failover	Marque o active como falhado	Torne-se ativo	Nenhum
Falha da relação na unidade em standby acima do ponto inicial	Sem falha	Nenhuma ação	Marque o apoio como falhado	Quando a unidade em standby é marcada como falhado, a unidade ativa não tenta falhar sobre mesmo se o ponto inicial da falha da relação é ultrapassado.

Regular e comutação classificada

A ferramenta de segurança apoia dois tipos de Failover, de regular e de stateful. Esta seção inclui estes assuntos:

- Failover regular
- Failover stateful

Failover regular

Quando um Failover ocorre, todas as conexões ativa estão deixadas cair. Os clientes precisam de restabelecer conexões quando a unidade ativa nova toma sobre.

Failover stateful

Quando a comutação classificada é permitida, a unidade ativa passa continuamente a informação de estado da conexão per. à unidade em standby. Depois que um Failover ocorre, a mesma informação de conexão está disponível na unidade ativa nova. Os aplicativos de usuário finais apoiados não são exigidos para reconectar para manter a mesma sessão de comunicação.

A informação de estado passada à unidade em standby inclui estes:

- A tabela de tradução NAT
- Os estados da conexão de TCP
- Os estados da conexão de UDP
- A tabela ARP
- A tabela de Bridge da camada 2 (somente quando o Firewall for executado no **modo de firewall transparente**)
- Os estados da conexão de HTTP (se a replicação HTTP é permitida)
- A tabela ISAKMP e IPsec SA
- A base de dados de conexão GTP PDP

A informação que não está passada à unidade em standby quando a comutação classificada é permitida inclui estes:

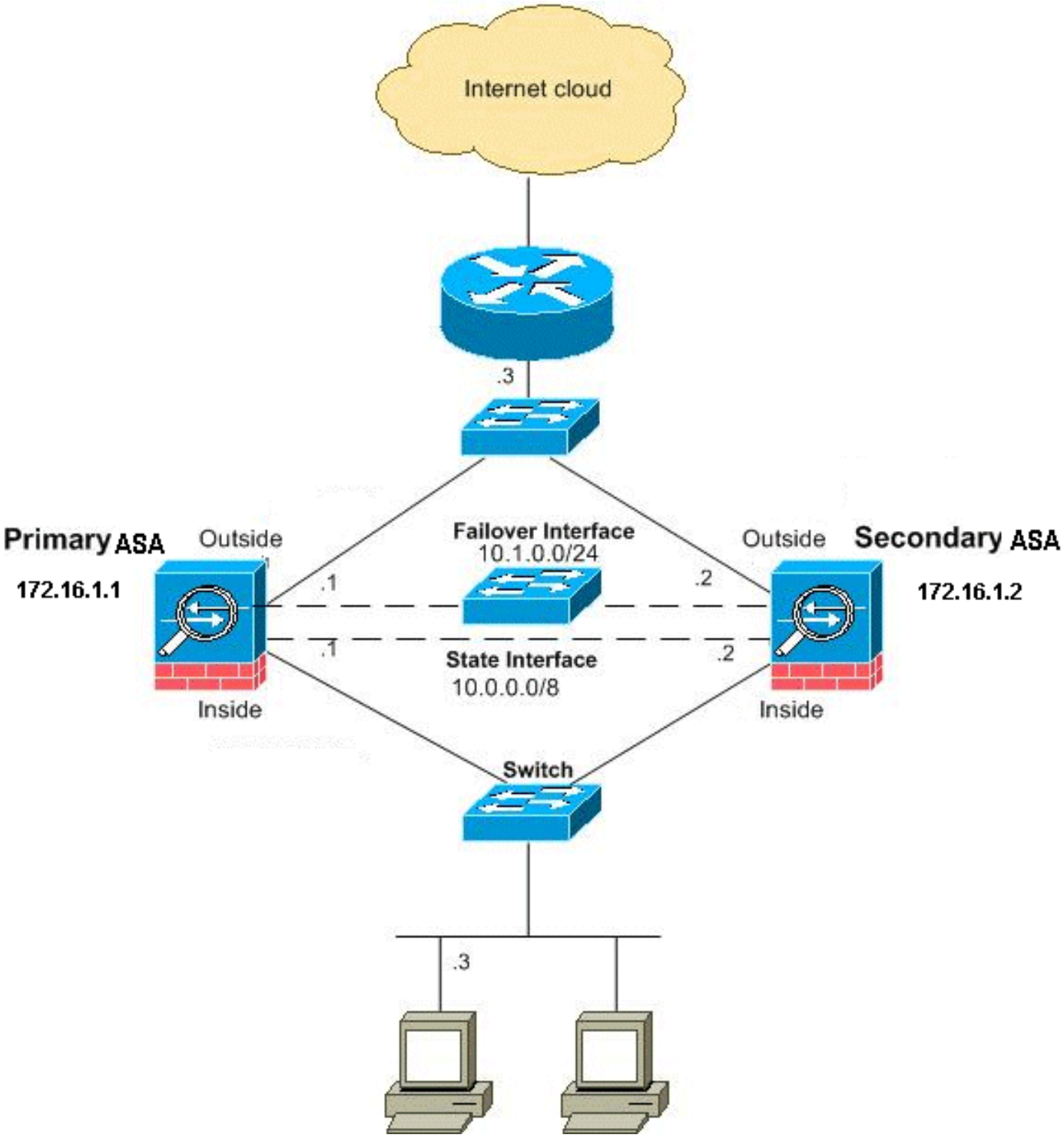
- A tabela da conexão de HTTP (a menos que a replicação HTTP é permitida)
- A tabela da autenticação de usuário (uauth)
- As tabelas de roteamento
- Informação de estado para os módulos de serviço de segurança

Nota: Se o failover ocorrer em uma sessão ativa do Cisco IP SoftPhone, a chamada permanecerá ativa porque as informações de estado da sessão da chamada são replicadas para a unidade de standby. Quando o atendimento é terminado, o cliente do IP SoftPhone perde a conexão com o CallManager da Cisco. Isto ocorre porque não há nenhuma informação de sessão para a mensagem do complexo CTIQBE na unidade em standby. Quando o cliente do IP SoftPhone não recebe uma resposta para trás do CallManager da Cisco dentro de um determinado período de tempo, considera o CallManager da Cisco inacessível e não registrados próprio.

Configuração de failover ativa/à espera LAN-baseada

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Esta seção descreve como configurar Failover ativo/à espera no modo transparente com um link failover dos Ethernet. Quando você configura o Failover LAN-baseado, você deve amarrar o dispositivo secundário para reconhecer o link failover antes que o dispositivo secundário possa obter a configuração running do dispositivo principal.

Nota: Se você muda do Failover cabo-baseado ao Failover LAN-baseado, você pode saltar muitas etapas, tais como a atribuição do active e dos endereços IP em standby para cada relação, que você terminou para a configuração de failover cabo-baseada.

Configuração da unidade primária

Termine estas etapas a fim configurar a unidade primária configuração de failover LAN-baseada, ativa/à espera. Estas etapas fornecem a configuração mínima necessária permitir o Failover na unidade primária. Para o modo de contexto múltiplo, todas as etapas são executadas no espaço da execução do sistema salvo disposição em contrário.

A fim configurar a unidade primária par de failover ativo/à espera, termine estas etapas:

1. Se você não tem feito tão já, configurar o active e os endereços IP em standby para a interface de gerenciamento (modo transparente). O endereço IP em standby é usado na ferramenta de segurança que é atualmente a unidade em standby. Deve estar na mesma sub-rede como o endereço IP de Um ou Mais Servidores Cisco ICM NT ativo.**Nota:** Não configurar um endereço IP de Um ou Mais Servidores Cisco ICM NT para o link da comutação classificada se você usa uma relação dedicada da comutação classificada. Você usa o **comando ip da relação do Failover** configurar uma relação dedicada da comutação classificada em uma etapa mais atrasada.`hostname(config-if)#` **`ip address active_addr netmask standby standby_addr`** Ao contrário do modo roteado, que exige um endereço IP de Um ou Mais Servidores Cisco ICM NT para cada relação, um Firewall transparente tem um endereço IP de Um ou Mais Servidores Cisco ICM NT atribuído ao dispositivo inteiro. A ferramenta de segurança usa este endereço IP de Um ou Mais Servidores Cisco ICM NT como o endereço de origem para os pacotes que originam na ferramenta de segurança, tal como mensagens de sistema ou comunicações AAA. No exemplo, o endereço IP de Um ou Mais Servidores Cisco ICM NT para o ASA preliminar é configurado como mostrado abaixo:`hostname(config)#` **`ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2`** Aqui, 172.16.1.1 é usado para a unidade primária, e 172.16.1.2 atribui à unidade (à espera) secundária.**Nota:** No modo de contexto múltiplo, você deve configurar os endereços da relação de dentro de cada contexto. Use o **comando context do changeto** a fim comutar entre contextos. O comando prompt muda ao `hostname/contexto (config-if) #`, onde o contexto é o nome do contexto atual.
2. (Plataforma da ferramenta de segurança PIX somente) permita o Failover LAN-baseado.`hostname(config)#` **`failover lan enable`**
3. Designe a unidade como a unidade primária.`hostname(config)#` **`failover lan unit primary`**
4. Defina a relação do Failover.Especifique a relação a ser usada como a relação do Failover.`hostname(config)#` **`failover lan interface`** *`if_name phy_if`* Nesta documentação, o “Failover” (nome da relação para o ethernet0) é usado para uma relação do Failover.`hostname(config)#` **`failover lan interface failover`** *`Ethernet3`* O argumento *if_name* atribui um nome à interface especificada pelo argumento *phy_if* . O argumento do *phy_if* pode ser o nome de porta física, tal como Ethernet1, ou uma subinterface previamente criada, tal como Ethernet0/2.3.Atribua o active e o endereço IP em standby ao link failover`hostname(config)#` **`failover interface ip`** *`if_name ip_addr`* **`mask standby`** *`ip_addr`* Nesta documentação, para configurar o link failover, 10.1.0.1 é usado para o active, 10.1.0.2 para a unidade em standby, e o “Failover” é um nome da relação do ethernet0.`hostname(config)#` **`failover interface ip failover 10.1.0.1 255.255.255.0 standby 10.1.0.2`** O endereço IP em standby deve estar na mesma sub-rede como o endereço IP de Um ou Mais Servidores Cisco ICM NT ativo. Você não precisa de identificar a máscara de sub-rede do endereço em standby.O endereço IP de Um ou Mais Servidores Cisco ICM NT e o MAC address do link failover não mudam no Failover. O endereço IP de Um ou Mais Servidores Cisco ICM NT ativo para o link failover fica sempre com a unidade primária, quando o endereço IP em standby ficar com a unidade secundária.Permita a

relação`hostname(config)#`**`interface`** *`phy_if`* `hostname(config-if)#`**`no shutdown`** No exemplo, Ethernet3 é usado para o Failover:`hostname(config)#`**`interface ethernet3`** `hostname(config-if)#`**`no shutdown`**

5. (Opcional) a fim permitir a comutação classificada, configurar o link da comutação classificada.Especifique a relação a ser usada como o link da comutação classificada.`hostname(config)#`**`failover link`** *`if_name phy_if`* Este exemplo usou o “estado” como um nome da relação para que Ethernet2 troque a informação de estado do link failover:`hostname(config)#`**`failover link state Ethernet2`** **Nota:** Se o link da comutação classificada usa o link failover ou uma interface de dados, você precisa somente de fornecer o argumento do *if_name*.O argumento do *if_name* atribui um nome lógico à relação especificada pelo argumento do *phy_if*. O argumento do *phy_if* pode ser o nome de porta física, tal como Ethernet1, ou uma subinterface previamente criada, tal como Ethernet0/2.3. Esta relação não deve ser usada para nenhuma outra finalidade, exceto, opcionalmente, como o link failover.Atribua um active e um endereço IP em standby ao link da comutação classificada.**Nota:** Se o link da comutação classificada usa o link failover ou a interface de dados, salte esta etapa. Você tem definido já o active e os endereços IP em standby para a relação.`hostname(config)#`**`failover interface`** *`ip if_name ip_addr`* **`mask standby`** *`ip_addr`* 10.0.0.1 é usado como um active e 10.0.0.2 como um endereço IP em standby para o link da comutação classificada neste exemplo.`hostname(config)#`**`failover interface ip state 10.0.0.1 255.0.0.0 standby 10.0.0.2`** O endereço IP em standby deve estar na mesma sub-rede como o endereço IP de Um ou Mais Servidores Cisco ICM NT ativo. Você não precisa de identificar a máscara de sub-rede do endereço em standby.O endereço IP de Um ou Mais Servidores Cisco ICM NT e o MAC address do link da comutação classificada não mudam no Failover a menos que usar uma interface de dados. O endereço IP de Um ou Mais Servidores Cisco ICM NT ativo fica sempre com a unidade primária, quando o endereço IP em standby ficar com a unidade secundária.Permita a relação.**Nota:** Se o link da comutação classificada usa o link failover ou a interface de dados, salte esta etapa. Você tem permitido já a relação.`hostname(config)#`**`interface phy_if`** `hostname(config-if)#`**`no shutdown`** **Nota:** Por exemplo, nesta encenação, Ethernet2 é usado para o link da comutação classificada:`hostname(config)#`**`interface ethernet2`** `hostname(config-if)#`**`no shutdown`**
6. Permita o Failover.`hostname(config)#`**`failover`** **Nota:** Emita o **comando failover no** dispositivo principal primeiramente, e emita-o então no dispositivo secundário. Após você executar o comando **failover** no dispositivo secundário, ele começará imediatamente a obter a configuração do dispositivo primário e definirá a si mesmo como *standby*. O ASA primário permanece em operação, transmite tráfego normalmente e marca a si mesmo como o dispositivo *ativo*. Desse ponto em diante, sempre que houver uma falha no dispositivo ativo, o dispositivo de standby se tornará o ativo.
7. Salvar a configuração de sistema à memória Flash.`hostname(config)#`**`copy running-config startup-config`**

Configuração da unidade secundária

A única configuração exigida na unidade secundária é para a relação do Failover. A unidade secundária exige estes comandos comunicar-se inicialmente com a unidade primária. Depois que a unidade primária envia sua configuração à unidade secundária, a única diferença permanente entre as duas configurações é o comando da **unidade lan do Failover**, que identifica cada unidade como preliminar ou secundária.

Para o modo de contexto múltiplo, todas as etapas são executadas no espaço da execução do

sistema salvo disposição em contrário.

A fim configurar a unidade secundária, termine estas etapas:

1. (Plataforma da ferramenta de segurança PIX somente) Enable LAN-baseou o Failover.`hostname(config)#`**`failover lan enable`**
2. Defina a relação do Failover. Use os mesmos ajustes que você usou para a unidade primária.Especifique a relação a ser usada como a relação do Failover.`hostname(config)#`**`failover lan interface`** *`if_name phy_if`* Nesta documentação, o ethernet0 é usado para uma relação do failover de LAN.`hostname(config)#`**`failover lan interface failover`** *`Ethernet3`* O argumento *if_name* atribui um nome à interface especificada pelo argumento *phy_if* .Atribua o active e o endereço IP em standby ao link failover.`hostname(config)#`**`failover interface ip`** *`if_name ip_addr`* **`mask standby`** *`ip_addr`* Nesta documentação, para configurar o link failover, 10.1.0.1 é usado para o active, 10.1.0.2 para a unidade em standby, e o “Failover” é um nome da relação do ethernet0.`hostname(config)#`**`failover interface ip failover 10.1.0.1 255.255.255.0 standby 10.1.0.2`** **Nota:** Incorpore este comando exatamente como você o incorporou na unidade primária quando você configurou a relação do Failover na unidade primária.Permita a relação.`hostname(config)#`**`interface`** *`phy_if`* `hostname(config-if)#`**`no shutdown`** Por exemplo, nesta encenação, o ethernet0 é usado para o Failover.`hostname(config)#`**`interface ethernet3`** `hostname(config-if)#`**`no shutdown`**
3. (Opcional) designe esta unidade como a unidade secundária.`hostname(config)#`**`failover lan unit secondary`** **Nota:** Esta etapa é opcional porque, à revelia, as unidades são designadas como secundário a menos que configuradas previamente.
4. Permita o Failover.`hostname(config)#`**`failover`** **Nota:** Após o failover ser habilitado, a unidade ativa envia a configuração na memória de execução para a unidade de standby. Como os sincronizars da configuração, as mensagens que *começam a replicação de configuração: A emissão a acoplar-se* e a *replicação do fim de configuração a acoplar-se* aparecem no console da unidade ativa.
5. Depois que a configuração running terminou a replicação, salvar a configuração à memória Flash.`hostname(config)#`**`copy running-config startup-config`**

Configurações

Este documento utiliza as seguintes configurações:

ASA preliminar

```
ASA#show running-config ASA Version 7.2(3) ! !--- To set
the firewall mode to transparent mode, !--- use the
firewall transparent command !--- in global
configuration mode. firewall transparent hostname ASA
domain-name default.domain.invalid enable password
2KFQnbNIdI.2KYOU encrypted names ! interface Ethernet0
nameif failover description LAN Failover Interface !
interface Ethernet1 nameif inside security-level 100 !
interface Ethernet2 nameif outside security-level 0 !---
Configure no shutdown in the stateful failover interface
!--- of both Primary and secondary ASA. interface
Ethernet3 nameif state description STATE Failover
Interface ! interface Ethernet4 shutdown no nameif no
security-level no ip address ! interface Ethernet5
shutdown no nameif no security-level no ip address !
```

```
passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns
server-group DefaultDNS domain-name
default.domain.invalid access-list 100 extended permit
ip any any pager lines 24 mtu outside 1500 mtu inside
1500 !--- Assign the IP address to the Primary and !---
Seconday ASA Security Appliance. ip address 172.16.1.1
255.255.255.0 standby 172.16.1.2 failover failover lan
unit primary failover lan interface failover Ethernet0
failover lan enable failover key ****** failover link
state Ethernet3 failover interface ip failover 10.1.0.1
255.255.255.0 standby 10.1.0.2 failover interface ip
state 10.0.0.1 255.0.0.0 standby 10.0.0.2 asdm image
flash:/asdm-522.bin no asdm history enable arp timeout
14400 access-group 100 in interface outside route
outside 0.0.0.0 0.0.0.0 172.16.1.3 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

ASA secundário

```
ASA#show running-config ASA Version 7.2(3) ! hostname
ASA domain-name default.domain.invalid enable password
2KFQnbNIdI.2KYOU encrypted names ! failover failover lan
unit secondary failover lan interface failover Ethernet0
failover lan enable failover key ****** failover
interface ip failover 10.1.0.1 255.255.255.0 standby
10.1.0.2
```

Verificar

Uso do comando show failover

Esta seção descreve a saída do comando **show failover**. Em cada unidade, você pode verificar o status do failover com o comando **show failover**.

ASA preliminar

```
ASA#show failover Failover On Cable status: N/A - LAN-based failover enabled Failover unit
Primary Failover LAN Interface: failover Ethernet0 (up) Unit Poll frequency 200 milliseconds,
holdtime 800 milliseconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface
Policy 1 Monitored Interfaces 2 of 250 maximum Version: Ours 7.2(3), Mate 7.2(3) Last Failover
at: 00:08:03 UTC Jan 1 1993 This host: Primary - Active Active time: 1820 (sec) Interface inside
(172.16.1.1): Normal Interface outside (172.16.1.1): Normal Other host: Secondary - Standby
Ready Active time: 0 (sec) Interface inside (172.16.1.2): Normal Interface outside (172.16.1.2):
Normal Stateful Failover Logical Update Statistics Link : state Ethernet3 (up) Stateful Obj xmit
```

```
xerr rcv rerr General 185 0 183 0 sys cmd 183 0 183 0 up time 0 0 0 0 RPC services 0 0 0 0 TCP
conn 0 0 0 0 UDP conn 0 0 0 0 ARP tbl 0 0 0 0 L2BRIDGE Tbl 2 0 0 0 Xlate_Timeout 0 0 0 0 Logical
Update Queue Information Cur Max Total Recv Q: 0 1 7012 Xmit Q: 0 1 185
```

ASA secundário

```
ASA(config)#show failover Failover On Cable status: N/A - LAN-based failover enabled Failover
unit Secondary Failover LAN Interface: failover Ethernet0 (up) Unit Poll frequency 200
milliseconds, holdtime 800 milliseconds Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1 Monitored Interfaces 2 of 250 maximum Version: Ours 7.2(3), Mate 7.2(3) Last
Failover at: 16:39:12 UTC Aug 9 2009 This host: Secondary - Standby Ready Active time: 0 (sec)
Interface inside (172.16.1.2): Normal Interface outside (172.16.1.2): Normal Other host: Primary
- Active Active time: 1871 (sec) Interface inside (172.16.1.1): Normal Interface outside
(172.16.1.1): Normal Stateful Failover Logical Update Statistics Link : state Ethernet3 (up)
Stateful Obj xmit xerr rcv rerr General 183 0 183 0 sys cmd 183 0 183 0 up time 0 0 0 0 RPC
services 0 0 0 0 TCP conn 0 0 0 0 UDP conn 0 0 0 0 ARP tbl 0 0 0 0 L2BRIDGE Tbl 0 0 0 0
Xlate_Timeout 0 0 0 0 Logical Update Queue Information Cur Max Total Recv Q: 0 1 7043 Xmit Q: 0
1 183
```

Use o comando do **estado do Failover da mostra** verificar o estado.

ASA preliminar

```
ASA#show failover state State Last Failure Reason Date/Time This host - Primary Active None
Other host - Secondary Standby Ready Comm Failure 00:02:36 UTC Jan 1 1993 ====Configuration
State=== Sync Done ====Communication State=== Mac set
```

Unidade secundária

```
ASA#show failover state State Last Failure Reason Date/Time This host - Secondary Standby Ready
None Other host - Primary Active None ====Configuration State=== Sync Done - STANDBY
====Communication State=== Mac set
```

A fim verificar os endereços IP de Um ou Mais Servidores Cisco ICM NT da unidade de failover, use o **comando interface do Failover da mostra**.

Unidade primária

```
ASA#show failover interface interface failover Ethernet0 System IP Address: 10.1.0.1
255.255.255.0 My IP Address : 10.1.0.1 Other IP Address : 10.1.0.2 interface state Ethernet3
System IP Address: 10.0.0.1 255.255.255.0 My IP Address : 10.0.0.1 Other IP Address : 10.0.0.2
```

Unidade secundária

```
ASA#show failover interface interface failover Ethernet0 System IP Address: 10.1.0.1
255.255.255.0 My IP Address : 10.1.0.2 Other IP Address : 10.1.0.1 interface state Ethernet3
System IP Address: 10.0.0.1 255.255.255.0 My IP Address : 10.0.0.2 Other IP Address : 10.0.0.1
```

Ideia de relações monitoradas

A fim ver o estado de relações monitoradas: No único modo do contexto, incorpore o comando da monitor-relação da mostra ao modo de configuração global. No modo de contexto múltiplo, insira o comando **show monitor-interface** em um contexto.

ASA preliminar

```
ASA(config)#show monitor-interface This host: Primary - Active Interface inside (172.16.1.1):
Normal Interface outside (172.16.1.1): Normal Other host: Secondary - Standby Ready Interface
inside (172.16.1.2): Normal Interface outside (172.16.1.2): Normal
```

ASA secundário

```
ASA(config)#show monitor-interface This host: Secondary - Standby Ready Interface inside
(172.16.1.2): Normal Interface outside (172.16.1.2): Normal Other host: Primary - Active
```

```
Interface inside (172.16.1.1): Normal Interface outside (172.16.1.1): Normal
```

Nota: Se você não incorpora um endereço IP de Um ou Mais Servidores Cisco ICM NT do Failover, o **comando show failover** indica 0.0.0.0 para o endereço IP de Um ou Mais Servidores Cisco ICM NT e a monitoração da relação permanece em um *estado de espera*. Refira a seção do Failover da mostra da *referência de comandos do dispositivo do Cisco Security, versão 7.2* para obter mais informações sobre dos estados diferentes do Failover.

Indicador dos comandos failover na configuração running

A fim ver os comandos failover na configuração running, incorpore este comando:

```
hostname(config)#show running-config failover
```

Todos os comandos failover são indicados. Nas unidades em execução no modo de contexto múltiplo, execute o comando **show running-config failover** no espaço de execução do sistema. Incorpore a executar-**configuração da mostra todo o comando failover** a fim indicar os comandos failover na configuração running e comandos include para que você não mudou o valor padrão.

Testes da funcionalidade do Failover

Termine estas etapas na ordem de ordem para testar a funcionalidade do Failover:

1. Teste que seu grupo da unidade ativa ou do Failover passa o tráfego como esperado com FTP (por exemplo) para enviar um arquivo entre anfitriões em relações diferentes.
2. Force um Failover à unidade em standby com este comando:Para Failover ativo/à espera, incorpore este comando na unidade ativa:`hostname(config)#no failover active`
3. Use o FTP para enviar um outro arquivo entre os mesmos dois anfitriões.
4. Se o teste não era bem sucedido, inscreva o **comando show failover** a fim verificar o status de comutação.
5. Quando você é terminado, você pode restaurar o grupo da unidade ou do Failover ao status ativo com este comando:Para Failover ativo/à espera, incorpore este comando na unidade ativa:`hostname(config)#failover active`

Failover forçado

A fim forçar a unidade em standby para tornar-se ativa, incorpore um destes comandos:

Incorpore este comando na unidade em standby:

```
hostname#failover active
```

Incorpore este comando na unidade ativa:

```
hostname#no failover active
```

Failover deficiente

A fim desabilitar o Failover, incorpore este comando:

```
hostname(config)#no failover
```

Se você desabilita o Failover par ativo/à espera, causa o estado ativo e à espera de cada unidade a ser mantida até que você reinicie. Por exemplo, a unidade em standby permanece no modo standby de modo que ambas as unidades não comecem passar o tráfego. A fim fazer o active da

unidade em standby (mesmo com o Failover desabilitado), veja a seção de forçamento do Failover.

Se você desabilita o Failover par ativo/ativo, faz com que os grupos do Failover permaneçam no estado ativo em qualquer unidade são atualmente ativos sobre, nenhuma matéria que a unidade ela é configurada para preferir. O comando **no failover** pode ser executado no espaço de execução do sistema.

Restauração de uma unidade falha

A fim restaurar uma unidade falha a um estado unfailed, incorpore este comando:

```
hostname(config)#failover reset
```

Se você restaura uma unidade falha a um estado unfailed, não lhe faz automaticamente o active; as unidades ou os grupos restaurados permanecem no estado à espera até o active feito pelo Failover (forçado ou natural). Uma exceção é um grupo do Failover configurado com o comando cancelar. Se previamente ativo, um grupo do Failover torna-se ativo se está configurado com o comando cancelar e se a unidade em que falhou é sua unidade preferida.

Troubleshooting

Quando um Failover ocorre, ambas as ferramentas de segurança mandam mensagens de sistema. Esta seção inclui estes assuntos

- Monitoramento de failover
- Falha de unidade
- %ASA-3-210005: O LU atribui a conexão falhada
- Mensagens de sistema de failover
- Debugar mensagens
- SNMP:
- Problemas conhecidos

Monitoramento de failover

Este exemplo demonstra o que acontece quando o failover não começou a monitorar as interfaces de rede. O Failover não começa monitorar as interfaces de rede até que ouça o segundo `pacote Hello da` outra unidade nessa relação. Isto toma aproximadamente 30 segundos. Se a unidade é anexada a um switch de rede que execute o Spanning Tree Protocol (STP), este toma duas vezes o `tempo de retardo de encaminhamento` configurado no interruptor, que é configurado tipicamente como 15 segundos, mais este segundo atraso 30. Isto é porque na inicialização ASA e imediatamente depois de um evento do Failover, o switch de rede detecta um Loop de Bridge temporário. Após detecção deste laço, para para enviar pacotes nestas relações pelo `tempo de retardo de encaminhamento`. Então entra no modo da `escuta` por um `tempo de retardo de encaminhamento` adicional, dentro que da hora o interruptor escuta loop de bridge mas não envia o tráfego ou `pacotes Hello` dianteiros do Failover. Após o dobro do tempo de atraso de encaminhamento (30 segundos), o tráfego volta a fluir. Cada ASA permanece em um modo de `espera` até que ouça um valor de 30 segundos dos `pacotes Hello da` outra unidade. Dentro do tempo que o ASA passa a tráfego, não falha a outra unidade baseada em não ouvir os `pacotes Hello`. Todo monitoramento de failover restante ainda ocorre, isto é, potência, perda de interface de enlace, e cabo de comutação `olá!`.

Para o Failover, Cisco recomenda fortemente que os clientes permitem o portfast em todas as portas de switch que conectam às relações ASA. Além disso, o trunking e a canalização devem ser desabilitados nessas portas. Se a relação do ASA vai para baixo dentro do Failover, o interruptor não tiver que esperar 30 segundos quando as transições de porta de um estado de escuta a aprendizagem à transmissão.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Active
Active time: 6930 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
Other host: Secondary - Standby
Active time: 15 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Normal (Waiting)
```

Em resumo, verifique estas etapas a fim reduzir para baixo os problemas do Failover:

- Verifique os cabos de rede conectados à interface no estado de espera/falha e, se possível, substitua-os.
- Se houver um switch conectado entre as duas unidades, verifique se as redes conectadas à interface no estado de espera/falha estão funcionando corretamente.
- Verifique a porta do switch conectada à interface no estado de espera/falha e, se possível, use outra porta de FE no switch.
- Verifique se você habilitou o port fast e desabilitou o trunking e a canalização nas portas do switch conectadas à interface.

Falha de unidade

Nesse exemplo, o failover detectou uma falha. Observe que a Interface 1 na unidade principal é a origem da falha. As unidades estão para trás no modo de `espera` devido à falha. A unidade falha removeu-se da rede (as relações estão para baixo) e já não envia `pacotes Hello na` rede. A unidade ativa permanece em um `estado de espera` até que a unidade falha estejam substituídos e os começos das comunicações de failover outra vez.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Standby (Failed)
Active time: 7140 (sec)
Interface inside (172.16.1.2): Normal (Waiting)
Interface outside (172.16.1.2): Failed (Waiting)
Other host: Secondary - Active
Active time: 30 (sec)
Interface inside (172.16.1.1): Normal (Waiting)
Interface outside (172.16.1.1): Normal (Waiting)
```

O LU atribui a conexão falhada

Um problema de memória pôde existir se você recebe este Mensagem de Erro:

```
O LU atribui a conexão falhada
```

Esta edição é documentada na identificação de bug Cisco CSCte80027 (clientes registrados

somente). A fim resolver esta edição, promova seu Firewall a uma versão de software em que este erro é fixo. Algumas das versões de software ASA sob que este erro obteve fixo são 8.2(4), 8.3(2), 8.4(2).

Mensagens de sistema de failover

A ferramenta de segurança emite um número de mensagens de sistema relativos ao Failover a nível da prioridade 2, que indica uma condição crítica. Para exibir estas mensagens, consulte Configuração de Log e Mensagens do Log do Sistema do Cisco Security Appliance para habilitar o log e ver descrições das mensagens de sistema.

Nota: Dentro do switchover, o Failover logicamente fechou e trouxe então acima relações, que gerencie mensagens do Syslog **411001** e **411002**. Esta é atividade normal.

Debugar mensagens

A fim ver para debugar mensagens, incorpore o comando do **fover debugar**. Consulte a Referência de Comandos do Cisco Security Appliance para obter mais informações.

Nota: Porque o resultado do debug é atribuído a alta prioridade no processo de CPU, pode drasticamente afetar o desempenho de sistema. Por isso, use o comando **debug fover** somente para fazer o troubleshooting de problemas específicos ou em sessões de troubleshooting acompanhadas pela equipe de suporte técnico da Cisco.

SNMP:

A fim receber armadilhas de SYSLOG SNMP para o Failover, configurar o agente SNMP para enviar o SNMP traps às estações do gerenciamento de SNMP, defina um syslog host, e compile o Syslog MIB de Cisco em sua estação do gerenciamento de SNMP. Consulte os comandos **snmp-server** e **logging** na Referência de Comandos do Cisco Security Appliance para obter mais informações.

Tempo de Poll do Failover

Para especificar os tempos de poll e espera da unidade de failover, use o comando **failover polltime** no modo de configuração global.

`O [time] milissegundo da unidade do período de eleição de failover` vota mensagens Hello Messages a fim representar o intervalo de tempo a fim verificar a existência da unidade em standby.

De forma semelhante, failover holdtime unit msec [time] representa o período de tempo durante o qual uma unidade deve receber uma mensagem de hello no link de failover. Decorrido esse tempo, a unidade peer é declarada como tendo sofrido uma falha.

Para especificar os tempos de poll e espera da interface de dados em uma configuração de failover Ativo/Standby, use o comando **failover polltime interface** no modo de configuração global. Para restaurar os tempos de poll e espera padrão, use a forma **no** deste comando.

failover polltime interface [msec] *time* **[holdtime** *time***]**

Use o comando **failover polltime interface** para alterar a freqüência na qual cada pacote de hello é enviado pelas interfaces de dados. Esse comando está disponível somente no failover Ativo/Standby. No failover Ativo/Ativo, use o comando **polltime interface** no modo de configuração de grupo do failover em vez do comando **failover polltime interface**.

Não é possível inserir um valor de **holdtime** inferior a 5 vezes o tempo de poll da interface. Quando um tempo de poll menor é usado, o Security Appliance pode detectar uma falha e acionar o failover mais rápido. No entanto, uma detecção muito rápida pode causar trocas desnecessárias quando a rede está congestionada temporariamente. O teste da interface começa quando um pacote de hello não é ouvido na interface por metade do tempo de espera.

Você pode incluir o comando failover polltime unit e o comando failover polltime interface na configuração.

Este exemplo define a freqüência do tempo de poll da interface como 500 milissegundos e o tempo de espera como 5 segundos:

```
hostname(config)#failover polltime interface msec 500 holdtime 5
```

Consulte a seção failover polltime da *Referência de Comandos do Cisco Security Appliance, Versão 7.2* para obter mais informações.

Configuração da Exportação do Certificado/Chave Privada no Failover

O dispositivo primário replica automaticamente o certificado/chave privada para a unidade secundária. Emita o **comando write memory na** unidade ativa a fim replicate a configuração, que inclui o certificado/chave privada, à unidade em standby. Todos os certificados/chaves na unidade de standby são apagados e preenchidos novamente com a configuração da unidade ativa.

Nota: Você não deve manualmente importar os Certificados, as chaves, e os pontos da confiança do dispositivo ativo e então exportá-los para o dispositivo à espera.

AVISO: Falha da descriptografia do mensagem de failover.

Mensagem de Erro:

```
Failover message decryption failure. Please make sure both units have the
same failover shared key and crypto license or system is not out of memory
```

Este problema ocorre devido à configuração da chave do Failover. A fim resolver esta edição, remova a chave do Failover, e configurar a chave compartilhada nova.

Problema: O Failover está batendo sempre após ter configurado Failover ativo/à espera transparente do modo múltiplo

O Failover é constante quando as interfaces internas de ambos os ASA são conectadas diretamente e as interfaces externas dos ambos ASA estão conectadas diretamente. Mas o Failover está batendo quando um interruptor é usado in-between.

Solução: Desabilite o BPDU nas relações ASA a fim resolver esta edição.

Failover de Módulos ASA

Se o Advanced Inspection and Prevention Security Services Module (AIP-SSM) ou o Content Security and Control Security Services Module (CSC-SSM) forem usados nas unidades ativa e de standby, eles funcionarão de forma independente do ASA em termos de failover. **Os módulos devem ser configurados manualmente nas unidades ativa e em standby, o Failover não replicate a configuração de módulo.**

Em termos de failover, ambas as unidades ASA que possuem os módulos AIP-SSM ou CSC-SSM devem ser do mesmo tipo de hardware. Por exemplo, se a unidade primária possuir o módulo ASA-SSM-10, a unidade secundária deverá possuir o módulo ASA-SSM-10.

Alloc do bloco do mensagem de failover falhado

Mensagem de Erro `%PIX|ASA-3-105010: Alloc (preliminar) do bloco do mensagem de failover falhado`

Explicação: A memória do bloco foi esgotada. Esta é uma mensagem transiente, e a ferramenta de segurança deve recuperar. *Preliminar* pode igualmente ser alistado como *secundário* para a unidade secundária.

Ação recomendada: Use o **comando show blocks** a fim monitorar a memória do bloco atual.

Problema do Failover do módulo de AIP

Se você tem dois ASA em uma configuração de failover e cada um tem um AIP-SSM, você deve manualmente replicate a configuração dos AIP-SS. Somente a configuração do ASA replicated pelo mecanismo do Failover. O AIP-SSM não é incluído no Failover.

Primeiramente, o AIP-SSM opera-se independentemente do ASA em termos do Failover. Para o Failover, tudo que é precisado de uma perspectiva ASA é que os módulos de AIP sejam do mesmo tipo de hardware. Além disso, como com qualquer outra parcela de Failover, a configuração do ASA entre o ativo e à espera deve estar na sincronização.

Como para estabelecido dos AIP, são eficazmente sensores independentes. Há sem falha entre os dois, e não têm nenhuma conscientização de se. Podem executar versões de código independentes. Isto é, não têm que combinar, e o ASA não se importa com a versão de código no AIP no que diz respeito ao Failover.

O ASDM inicia uma conexão ao AIP através do IP da interface de gerenciamento que você configurou no AIP. Ou seja conecta ao sensor tipicamente com o HTTPS, que depende de como você estabelece o sensor.

Você poderia ter um Failover do independente ASA dos módulos IPS (AIP). Você é conectado ainda ao mesmo porque você conecta a seu IP de gerenciamento. A fim conectar ao outro AIP, você deve reconectar a seu IP do manangement para configurar-lo e alcançá-lo.

Refira o ASA: Envie o tráfego de rede do ASA ao exemplo de configuração AIP SS para mais configurações da informação e de amostra em como enviar o tráfego de rede que passa através da ferramenta de segurança adaptável do 5500 Series de Cisco ASA (ASA) ao módulo de Serviços de segurança avançado da inspeção e da prevenção (AIP-SSM) (os IPS)

Problemas conhecidos

Quando você tenta alcançar o ASDM no ASA secundário com software da versão 8.x e versão 6.x ASDM para a configuração de failover, este erro está recebido:

```
Erro: O nome no Security Certificate é inválido ou não combina o nome do local
```

No certificado, o expedidor e o nome do sujeito são o endereço IP de Um ou Mais Servidores Cisco ICM NT da *unidade ativa*, não o endereço IP de Um ou Mais Servidores Cisco ICM NT da *unidade em standby*.

Na versão ASA 8.x, o certificado (ASDM) interno replicated da unidade ativa à unidade em standby, que causa o Mensagem de Erro. Mas, se o mesmo Firewall é executado no código da versão 7.x com 5.x ASDM e você tenta alcançar o ASDM, você recebe este aviso regular da Segurança:

```
O Security Certificate tem um nome válido que combina o nome da página que você está tentando
ver
```

Quando você verifica o certificado, o expedidor e o nome do sujeito são o endereço IP de Um ou Mais Servidores Cisco ICM NT da unidade em standby.

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco PIX Firewall Software
- Configuração de failover do módulo de serviços de firewall (FWSM)
- Troubleshooting do Failover FWSM
- Como o Failover trabalha no firewall PIX segura Cisco
- Suporte Técnico e Documentação - Cisco Systems