ASA/PIX: Configurar Failover ativo/ativo 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/ativo 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 ASA/PIX 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/Ativo

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

Visão Geral do Failover Ativo/Ativo

O Failover Ativo/Ativo está disponível somente em Security Appliances em execução no modo de contexto múltiplo. Em uma configuração de Failover Ativo/Ativo, ambos os Security Appliances podem transmitir tráfego de rede.

No Failover Ativo/Ativo, os contextos de segurança no Security Appliance são divididos em grupos de failover. Um grupo de failover nada mais é do que um grupo lógico de um ou mais contextos de segurança. É possível criar no máximo dois grupos de failover no Security Appliance. O contexto admin é sempre um membro do grupo1 do Failover. Todos os contextos de segurança unassigned são igualmente membros do grupo1 do Failover à revelia.

Os grupos de failover formam a unidade base do Failover Ativo/Ativo. Monitoração de falhas de interface, failover e os status ativo/standby são todos atributos de um grupo de failover, e não da unidade. Quando um grupo de failover ativo falha, ele entra no estado de standby. Ao mesmo tempo, o grupo de failover de standby se torna ativo. As interfaces no grupo de failover que se torna ativo assumem os endereços MAC e IP das interfaces do grupo de failover que falhou. As

interfaces no grupo de failover que agora está no estado de standby assumem os endereços MAC e IP de standby.

Nota: Um grupo do Failover que falha em uma unidade não significa que a unidade falhou. A unidade pode ainda ter um outro grupo do Failover que passe o tráfego nela.

Estado preliminar/secundário e status ativo/em standby

Assim como no Failover Ativo/Standby, uma unidade em um par de Failover Ativo/Ativo é designada como a unidade primária e a outra como unidade secundária. Ao contrário do Failover Ativo/Standby, essa designação não indica que unidade se torna ativa quando ambas as unidades são iniciadas simultaneamente. Em vez disso, a designação primária/secundária faz duas coisas:

- Determina qual unidade fornece a configuração em execução para o par quando eles tentam inicializar simultaneamente.
- Determina em qual unidade cada grupo de failover entra no estado ativo quando as unidades inicializam ao mesmo tempo. Cada grupo de failover na configuração é configurado com uma preferência de unidade primária ou secundária. Você pode configurar ambos os grupos do Failover esteja no estado ativo em uma única unidade nos pares, com a outra unidade que contém os grupos do Failover no estado à espera. Mas, mais configuração típica é atribuir a cada grupo do Failover uma preferência diferente do papel para fazer cada um ativo em uma unidade diferente, e distribui o tráfego através dos dispositivos.**Nota:** A ferramenta de segurança não proporciona serviços do Balanceamento de carga. O balanceamento de carga deve ser gerenciado por um roteador que envia tráfego para o Security Appliance.

A unidade em que cada grupo de failover se torna ativo é determinada conforme mostrado.

- Quando uma unidade inicializa sem que a unidade peer esteja disponível, ambos os grupos de failover se tornam ativos na unidade.
- Quando as botas de uma unidade quando a unidade do par for ativa (com ambos os grupos do Failover no estado ativo), os grupos do Failover permanecerem no estado ativo na unidade ativa apesar da preferência preliminar ou secundária do grupo do Failover até uma destas ocorrências:Um failover ocorra.Você force manualmente o grupo de failover para a outra unidade com o comando **no failover active**.Você configure o grupo de failover com o comando **preempt**, o que fará com que o grupo de failover se torne ativo automaticamente na unidade preferida quando a unidade se tornar disponível.
- Quando ambas as unidades inicializarem ao mesmo tempo, cada grupo de failover se tornará ativo em sua unidade preferencial após as configurações terem sido sincronizadas.

Iniciação e sincronização de configuração do dispositivo

A sincronização da configuração ocorre quando uma ou ambas as unidades em um par de failover inicializam. As configurações são sincronizadas da seguinte forma:

- Quando uma unidade inicializa quando a unidade peer está ativa (com ambos os grupos de failover ativos), a unidade que está inicializando se comunica com a unidade ativa para obter a configuração em execução, independentemente da designação de primária ou secundária da primeira unidade.
- Quando ambas as unidades inicializam ao mesmo tempo, a unidade secundária obtém a

configuração em execução da unidade primária.

Quando a replicação começa, o console da ferramenta de segurança na unidade que envia a configuração indica `replicação de configuração começo da` mensagem do `": Enviando para acoplar-se,"` e quando está completa, a ferramenta de segurança indica a mensagem `"replicação do fim de configuração para acoplar-se."` Durante a replicação, os comandos entered na unidade que envia a configuração não podem replicate corretamente à unidade do par, e os comandos entered na unidade que recebem a configuração podem ser overwritten pela configuração que?a. Não feito os comandos em uma ou outra unidade no par de failover durante o processo da replicação de configuração. A replicação, que depende em cima do tamanho da configuração, pode tomar de alguns segundos a diversos minutos.

Na unidade que recebe a configuração, a configuração existe somente em memória running. A fim salvar a configuração à memória Flash após a sincronização, inscreva o **comando all da memória da escrita no** espaço da execução do sistema na unidade que tem o grupo1 do Failover no estado ativo. O comando é replicado para a unidade peer, a qual escreve sua configuração na memória Flash. O uso de **toda a** palavra-chave com este comando causa sistema e todas as configurações do contexto a ser salvar.

Nota: As configurações de inicialização salvar em servidores internos são acessíveis de uma ou outra unidade sobre a rede e não precisam de ser salvar separadamente para cada unidade. Você também pode copiar os contextos dos arquivos de configuração do disco na unidade primária para um servidor externo, e então copiá-los para o disco da unidade secundária, onde eles se tornarão disponíveis quando a unidade recarregar.

Replicação do comando

Após ambas as unidades começarem a executar, os comandos serão replicados de uma unidade para a outra:

- Os comandos inseridos com um contexto de segurança são replicados da unidade na qual o contexto de segurança está no estado ativo para a unidade peer.**Nota:** O contexto é considerado no estado ativo de uma unidade quando o grupo de failover ao qual ele pertence está no estado ativo dessa unidade.
- Os comandos inseridos no espaço de execução do sistema são replicados da unidade na qual o grupo de failover 1 está no estado ativo para a unidade na qual o grupo de failover 1 está no estado de standby.
- Os comandos inseridos no contexto de administrador são replicados da unidade na qual o grupo de failover 1 está no estado ativo para a unidade na qual o grupo de failover 1 está no estado de standby.

Toda a configuração e comandos file (a **cópia, rebatiza, suprime, mkdir, rmdir,** e assim por diante) replicated, com estas exceções. os comandos **show, debug, mode, firewall, failover lan unit** não são replicados.

Falhar ao executar os comandos na unidade apropriada para que a replicação de comandos ocorra fará com que as configurações fiquem fora de sincronia. Aquelas mudanças são perdidas possivelmente a próxima vez que a sincronização da configuração inicial ocorre.

Você pode usar o comando **write standby** para ressincronizar as configurações dessincronizadas. Para o Active/**escreva o** Failover **standbyActive**, o **comando write standby** comporta-se como mostrado:

- Se você executar o comando **write standby** no espaço de execução do sistema, a configuração do sistema e as configurações para todos os outros contextos de segurança no Security Appliance serão escritas na unidade peer. Isso inclui informações de configuração para contextos de segurança no estado de standby. Você deve executar o comando no espaço de execução do sistema na unidade que possui o grupo de failover 1 no estado ativo.**Nota:** Se há uns contextos de segurança no estado ativo na unidade do par, o **comando write standby** faz com que as conexões ativa com aqueles contextos estejam terminadas. Use o **comando failover ative na** unidade que fornece a configuração para se certificar que todos os contextos são ativos nessa unidade antes de inscrever o **comando write standby**.
- Se você inserir o comando **write standby** em um contexto de segurança, somente a configuração do contexto de segurança será escrita na unidade peer. Você deve inserir o comando no contexto de segurança da unidade em que o contexto está no estado ativo.

Os comandos replicados não são salvos na memória Flash ao serem replicados para a unidade peer. Eles são adicionados à configuração em execução. Para salvar os comandos replicados na memória Flash de ambas as unidades, execute o comando **write memory** ou **copy running-config startup-config** na unidade na qual você fez as alterações. O comando é replicado para a unidade peer e faz com que a configuração seja salva na memória Flash da unidade peer.

Disparadores do Failover

Failover ativo/ativo, o Failover pode ser provocado a nível da unidade se um destes eventos ocorre:

- A unidade sofre uma falha de hardware.
- A unidade sofre uma falha de alimentação de energia.
- A unidade tem uma falha de software.
- O comando **no failover active** ou **failover active** é inserido no espaço de execução do sistema.

O Failover está provocado a nível do grupo do Failover quando um destes eventos ocorre:

- Um número excessivo de interfaces monitoradas no grupo falha.
- O comando **no failover active group group_id** ou **failover active group group_id** é inserido.

Ações do Failover

Na configuração de Failover Ativo/Ativo, o failover ocorre com base em grupos de failover, e não em sistema. Por exemplo, se você designar ambos os grupos de failover como ativos na unidade primária e o grupo 1 falhar, o grupo 2 permanecerá ativo na unidade primária e o grupo 1 se tornará ativo na unidade secundária.

Nota: Quando você configura Failover ativo/ativo, certifique-se de que o tráfego combinado para ambas as unidades está dentro da capacidade de cada unidade.

Esta tabela mostra a ação do Failover para cada evento de falha. Para cada evento de falha, a política, mesmo se o Failover ocorrem, as ações para o grupo ativo do Failover, e as ações para o grupo à espera do Failover são dadas.

Evento de falha	Política	Ação do grupo	Ação do grupo	Notas

		o ativo	de standby	
A unidade sofre uma falha de alimentação de energia ou software	Failover	Tornar standby. Marcar como falha.	Tornar standby. Marque o active como falhado	Quando uma unidade em um par de failover falha, todos os grupos de failover ativos nessa unidade são marcados como com falha e se tornam ativos na unidade peer.
Falha de interface no grupo de failover ativo acima do limite	Failover	Marcar grupo ativo como falha.	Torne-se ativo	Nenhum
Falha de interface no grupo de failover standby acima do limite	Sem falha	Nenhuma ação	Marcar grupo de standby como falha.	Quando o grupo de failover de standby é marcado como falha, o grupo de failover ativo não tenta executar o failover, mesmo quando o limite de falha da interface é ultrapassado.
O grupo de failover ativo anterior se recupera	Sem falha	Nenhuma ação	Nenhuma ação	A menos que configurado com o comando **preempt**, o grupo de failover permanece ativo em sua unidade atual.
Link failover falhado na partida	Sem falha	Torne-se ativo	Torne-se ativo	Se o link de failover estiver inativo na inicialização, ambos os grupos de failover em ambas as unidades se tornarão ativos.
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 do link de	Sem	n/a	n/a	Cada unidade marca a interface do failover como

failover durante a operação	falha			falha. Você deve restaurar o link de failover o mais rápido possível porque a unidade não pode executar o failover para a unidade de standby quando o link está inoperante.

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 restabelecer as conexões quando a nova unidade ativa assume.

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 (quando 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 gerenciador de chamada. 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 gerenciador de chamada dentro de um determinado período de tempo, considera o gerenciador de chamada inacessível e não registrados própria.

Limitações da Configuração do Failover

Você não pode configurar o Failover com estes tipos de endereços IP de Um ou Mais Servidores Cisco ICM NT:

- Endereços IP obtidos por DHCP
- Endereços IP obtidos por PPPoE
- Endereços IPv6

Adicionalmente, estas limitações aplicam-se:

- Não há suporte ao failover stateful no ASA 5505 Adaptive Security Appliance.
- Não há suporte ao Failover Ativo/Ativo no ASA 5505 Adaptive Security Appliance.
- Não é possível configurar o failover quando o Easy VPN Remote está habilitado no ASA 5505 Adaptive Security Appliance.
- Não há suporte ao failover de VPN no modo de contexto múltiplo.

Recursos não suportados

O modo de contexto múltiplo não apoia estas características:

- Protocolos de roteamento dinâmicoOs contextos de segurança aceitam somente rotas estáticas. Você não pode permitir o OSPF ou o RASGO no modo de contexto múltiplo.
- VPN
- Transmissão múltipla

Configuração de Failover Ativo/Ativo Baseado em LAN

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Esta seção descreve como configurar Failover ativo/ativo 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: Em vez de um cabo de Ethernet de cruzamento para ligar diretamente as unidades, Cisco recomenda que você usa um switch dedicado entre as unidades principais e secundárias.

Esta seção inclui estes tópicos:

- Configuração da unidade secundária

Configuração da unidade primária

Termine estas etapas a fim configurar a unidade primária configuração de failover ativa/ativa:

1. Caso ainda não tenha feito, configure os endereços IP ativo e de standby para cada interface de dados (modo roteado), para o endereço IP de gerenciamento (modo transparente) ou para a interface somente de gerenciamento. 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.Você deve configurar os endereços da interface em cada contexto de segurança. Use o **comando context do changeto** comutar entre contextos. O comando prompt muda ao hostname/contexto (config-if) #, onde o contexto é o nome do contexto atual. No modo de firewall transparente, você deve inserir um endereço IP de gerenciamento para cada contexto.**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** a fim configurar uma relação dedicada da comutação classificada em uma etapa mais atrasada.`hostname/context(config-if)#` **`ip address`** *`active_addr`* **`netmask standby`** *`standby_addr`* No exemplo, a interface externa para context1 do ASA preliminar é configurada esta maneira:`ASA/context1(config)#` **`ip address 172.16.1.1 255.255.255.0 standby 172.16.1.2`** Para Context2:`ASA/context2(config)#` **`ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2`** No modo de firewall roteado e para a interface somente de gerenciamento, este comando é inserido no modo de configuração de cada interface. No modo de firewall transparente, o comando é inserido no modo de configuração global.
2. Configurar os parâmetros básicos do Failover no espaço da execução do sistema.(Somente PIX Security Appliance) Habilite o failover baseado em LAN:`hostname(config)#` **`failover lan enable`** Defina a unidade como a unidade primária:`hostname(config)#` **`failover lan unit primary`** Especifique o link de failover:`hostname(config)#` **`failover lan interface`** *`if_name phy_if`*Neste exemplo, usamos a interface ethernet3 como a interface de failover baseado em LAN.`ASA(config)#` **`failover lan interface LANFailover ethernet3`** 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. No ASA 5505 Adaptive Security Appliance, phy_if especifica uma VLAN. Essa interface não deve ser usada para nenhum outro fim (exceto, opcionalmente, para o link de failover stateful).Especifique os endereços IP ativo e de standby do link de failover:`hostname(config)#` **`failover interface ip`** *`if_name ip_addr`* **`mask standby`** *`ip_addr`* Neste exemplo, usamos 10.1.0.1 e 10.1.0.2 como endereços IP ativo e de standby para a interface de failover.`ASA(config)#` **`failover interface ip LANFailover 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 IP 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 fica sempre com a unidade primária, quando o endereço IP em standby ficar com a unidade secundária.

Configuração da unidade secundária

Quando você configura Failover ativo/ativo LAN-baseado, você precisa de amarrar a unidade secundária a fim reconhecer o link failover. Isso permite que a unidade secundária se comunique com e receba a configuração em execução da unidade primária.

Termine estas etapas a fim amarrar a unidade secundária configuração de failover ativa/ativa:

1. (Ferramenta de segurança PIX somente) Enable LAN-baseou o Failover.`hostname(config)#`**`failover lan enable`**
2. Defina a relação do Failover. Use as mesmas configurações aplicadas à unidade primária:Especifique a relação a ser usada como a relação do Failover.`hostname(config)#`**`failover lan interface`** *`if_name phy_if`* `ASA(config)#failover lan interface LANFailover ethernet3`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. No ASA 5505 Adaptive Security Appliance, phy_if especifica uma VLAN.Atribua o endereço IP ativo e de standby ao link de failover:`hostname(config)#`**`failover interface ip`** *`if_name ip_addr`* **`mask standby`** *`ip_addr`* `ASA(config)#`**`failover interface ip LANFailover 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.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.Permita a relação.`hostname(config)#`**`interface`** *`phy_if`* `hostname(config-if)#`**`no shutdown`**
3. Defina esta unidade como a unidade secundária:`hostname(config)#`**`failover lan unit secondary`** **Nota:** Esta etapa é opcional porque as unidades são designadas à revelia como secundário a menos que configuradas previamente de outra maneira.
4. Permita o Failover.`hostname(config)#`**`failover`** 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.**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.
5. Depois que a configuração running terminou a replicação, incorpore este comando salvar a configuração à memória Flash:`hostname(config)#`**`copy running-config startup-config`**
6. Se necessário, force qualquer grupo de failover ativo na unidade primária a entrar no estado ativo na unidade secundária. Para forçar um grupo do Failover a tornar-se ativo na unidade secundária, incorpore este comando ao espaço da execução do sistema na unidade primária:`hostname#`**`no failover active group group_id`** O argumento group_id especifica o grupo que você deseja que se torne ativo na unidade secundária.

Configurações

Este documento utiliza as seguintes configurações:

ASA preliminar - Configuração Context1

```
ASA/context1(config)#show running-config : Saved : ASA
Version 7.2(3) <context> ! hostname context1 enable
password 8Ry2YjIyt7RRXU24 encrypted names ! interface
inside_context1 nameif inside security-level 100 !---
Configure the active and standby IP's for the logical
inside !--- interface of the context1. ip address
192.168.1.1 255.255.255.0 standby 192.168.1.2 !
interface outside_context1 nameif outside security-level
0 !--- Configure the active and standby IP's for the
logical outside !--- interface of the context1. ip
address 172.16.1.1 255.255.255.0 standby 172.16.1.2 !
passwd 2KFQnbNIdI.2KYOU encrypted access-list 100
extended permit tcp any host 172.16.1.1 eq www pager
lines 24 mtu inside 1500 mtu outside 1500 monitor-
interface inside monitor-interface outside icmp
unreachable rate-limit 1 burst-size 1 asdm image
flash:/asdm-522.bin no asdm history enable arp timeout
14400 static (inside,outside) 172.16.1.1 192.168.1.5
netmask 255.255.255.255 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 telnet
timeout 5 ssh timeout 5 ! 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
Cryptochecksum:00000000000000000000000000000000 : end
```

ASA preliminar - Configuração Context2

```
ASA/context2(config)#show running-config : Saved : ASA
Version 7.2(3) <context> ! hostname context2 enable
password 8Ry2YjIyt7RRXU24 encrypted names ! interface
inside_context2 nameif inside security-level 100 !---
Configure the active and standby IP's for the logical
inside !--- interface of the context2. ip address
192.168.2.1 255.255.255.0 standby 192.168.2.2 !
interface outside_context2 nameif outside security-level
0 !--- Configure the active and standby IP's for the
logical outside !--- interface of the context2. ip
address 172.16.2.1 255.255.255.0 standby 172.16.2.2 !
passwd 2KFQnbNIdI.2KYOU encrypted access-list 100
extended permit tcp any host 172.16.2.1 eq www pager
lines 24 mtu inside 1500 mtu outside 1500 monitor-
interface inside monitor-interface outside icmp
unreachable rate-limit 1 burst-size 1 asdm image
flash:/asdm-522.bin no asdm history enable arp timeout
14400 static (inside,outside) 172.16.2.1 192.168.2.5
netmask 255.255.255.255 access-group 100 in interface
outside route outside 0.0.0.0 0.0.0.0 172.16.2.3 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 telnet
timeout 5 ssh timeout 5 ! 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
Cryptochecksum:00000000000000000000000000000000 : end
```

ASA preliminar

```
ASA(config)#show running-config : Saved : ASA Version
7.2(3) <system> ! !--- Use the firewall transparent
command !--- in global configuration mode in order to !-
-- set the firewall mode to transparent mode. firewall
transparent hostname ASA enable password
8Ry2YjIyt7RRXU24 encrypted no mac-address auto !
interface Ethernet0 ! interface Ethernet0.1 vlan 2 !
interface Ethernet0.2 vlan 4 ! interface Ethernet1 !
interface Ethernet1.1 vlan 3 ! interface Ethernet1.2
vlan 5 ! !--- Configure "no shutdown" in the stateful
failover interface as well as !--- LAN Failover
interface of both Primary and secondary ASA/PIX.
interface Ethernet2 description STATE Failover Interface
! interface Ethernet3 description LAN Failover Interface
! interface Ethernet4 shutdown ! interface Ethernet5
shutdown ! class default limit-resource All 0 limit-
resource ASDM 5 limit-resource SSH 5 limit-resource
Telnet 5 ! ftp mode passive pager lines 24 failover
failover lan unit primary !--- Command to assign the
interface for LAN based failover failover lan interface
LANFailover Ethernet3 !--- Configure the
Authentication/Encryption key failover key *****
failover link stateful Ethernet2 !--- Configure the
active and standby IP's for the LAN based failover
failover interface ip LANFailover 10.1.0.1 255.255.255.0
standby 10.1.0.2 failover interface ip stateful 10.0.0.1
255.255.255.0 standby 10.0.0.2 failover group 1 failover
group 2 secondary no asdm history enable arp timeout
14400 console timeout 0 admin-context admin context
admin config-url flash:/admin.cfg ! context context1
allocate-interface Ethernet0.1 inside_context1 allocate-
interface Ethernet1.1 outside_context1 config-url
flash:/context1.cfg join-failover-group 1 ! context
context2 allocate-interface Ethernet0.2 inside_context2
allocate-interface Ethernet1.2 outside_context2 config-
url flash:/context2.cfg join-failover-group 2 ! prompt
hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

ASA secundário

```
ASA#show running-config failover failover lan unit
secondary failover lan interface LANFailover Ethernet3
failover key ***** failover interface ip LANFailover
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(config-subif)#show failover Failover On Cable status: N/A - LAN-based failover enabled
Failover unit Primary Failover LAN Interface: LANFailover Ethernet3 (up) Unit Poll frequency 15
seconds, holdtime 45 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface
Policy 1 Monitored Interfaces 4 of 250 maximum Version: Ours 7.2(3), Mate 7.2(3) Group 1 last
failover at: 06:12:45 UTC Jan 17 2009 Group 2 last failover at: 06:12:43 UTC Jan 17 2009 This
host: Primary Group 1 State: Active Active time: 359610 (sec) Group 2 State: Standby Ready
Active time: 3165 (sec) context1 Interface inside (192.168.1.1): Normal context1 Interface
outside (172.16.1.1): Normal context2 Interface inside (192.168.2.2): Normal context2 Interface
outside (172.16.2.2): Normal Other host: Secondary Group 1 State: Standby Ready Active time: 0
(sec) Group 2 State: Active Active time: 3900 (sec) context1 Interface inside (192.168.1.2):
Normal context1 Interface outside (172.16.1.2): Normal context2 Interface inside (192.168.2.1):
Normal context2 Interface outside (172.16.2.1): Normal Stateful Failover Logical Update
Statistics Link : stateful Ethernet2 (up) Stateful Obj xmit xerr rcv rerr General 48044 0 48040
1 sys cmd 48042 0 48040 1 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 2 0 0 0 Xlate_Timeout 0 0 0 0 Logical Update Queue Information Cur Max Total Recv Q: 0 1
72081 Xmit Q: 0 1 48044
```

ASA secundário

```
ASA(config)#show failover Failover On Cable status: N/A - LAN-based failover enabled Failover
unit Secondary Failover LAN Interface: LANFailover Ethernet3 (up) Unit Poll frequency 15
seconds, holdtime 45 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface
Policy 1 Monitored Interfaces 4 of 250 maximum Version: Ours 7.2(3), Mate 7.2(3) Group 1 last
failover at: 06:12:46 UTC Jan 17 2009 Group 2 last failover at: 06:12:41 UTC Jan 17 2009 This
host: Secondary Group 1 State: Standby Ready Active time: 0 (sec) Group 2 State: Active Active
time: 3975 (sec) context1 Interface inside (192.168.1.2): Normal context1 Interface outside
(172.16.1.2): Normal context2 Interface inside (192.168.2.1): Normal context2 Interface outside
(172.16.2.1): Normal Other host: Primary Group 1 State: Active Active time: 359685 (sec) Group 2
State: Standby Ready Active time: 3165 (sec) context1 Interface inside (192.168.1.1): Normal
context1 Interface outside (172.16.1.1): Normal context2 Interface inside (192.168.2.2): Normal
context2 Interface outside (172.16.2.2): Normal Stateful Failover Logical Update Statistics Link
: stateful Ethernet2 (up) Stateful Obj xmit xerr rcv rerr General 940 0 942 2 sys cmd 940 0 940
2 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 2 0
Xlate_Timeout 0 0 0 0 Logical Update Queue Information Cur Max Total Recv Q: 0 1 1419 Xmit Q: 0
1 940
```

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

ASA preliminar

```
ASA(config)#show failover state State Last Failure Reason Date/Time This host - Primary Group 1
Active None Group 2 Standby Ready None Other host - Secondary Group 1 Standby Ready None Group 2
Active None ====Configuration State=== Sync Done ====Communication State=== Mac set
```

Unidade secundária

```
ASA(config)#show failover state State Last Failure Reason Date/Time This host - Secondary Group
1 Standby Ready None Group 2 Active None Other host - Primary Group 1 Active None Group 2
Standby Ready None ====Configuration State=== Sync Done - STANDBY ====Communication State=== Mac
set
```

Para verificar os endereços IP da unidade de failover, use o comando **show failover interface**.

Unidade primária

```
ASA(config)#show failover interface interface stateful Ethernet2 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 interface LANFailover
Ethernet3 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
```

Unidade secundária

```
ASA(config)#show failover interface interface LANFailover Ethernet3 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 stateful Ethernet2
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.

Nota: A fim permitir o monitoramento de funcionamento em uma relação específica, use o comando da monitor-relação no modo de configuração global:

monitor-interface <*if_name***>**

ASA preliminar

```
ASA/context1(config)#show monitor-interface This host: Secondary - Active Interface inside
(192.168.1.1): Normal Interface outside (172.16.1.1): Normal Other host: Secondary - Standby
Ready Interface inside (192.168.1.2): Normal Interface outside (172.16.1.2): Normal
```

ASA secundário

```
ASA/context1(config)#show monitor-interface This host: Secondary - Standby Ready Interface
inside (192.168.1.2): Normal Interface outside (172.16.1.2): Normal Other host: Secondary -
Active Interface inside (192.168.1.1): 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 das relações permanece em um `estado de espera`. Você deve ajustar um endereço IP de Um ou Mais Servidores Cisco ICM NT do Failover para que o Failover trabalhe. Refira o Failover da mostra para obter mais informações sobre dos estados diferentes para o 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** 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 a fim 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/ativo, incorpore este comando na unidade onde o grupo do Failover, que contém a relação que conecta seus anfitriões é ativo:`hostname(config)#`**no failover active group** *group_id*

3. Use o FTP a fim 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/ativo, incorpore este comando na unidade onde o grupo do Failover, que contém a relação que conecta seus anfitriões é ativo:`hostname(config)#`**`failover active group`** *`group_id`*

Failover forçado

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

Incorpore este comando ao espaço da execução do sistema da unidade onde o grupo do Failover está no estado à espera:

`hostname#`**`failover active group`** *`group_id`*
Ou, incorpore este comando ao espaço da execução do sistema da unidade onde o grupo do Failover está no estado ativo:

`hostname#`**`no failover active group`** *`group_id`*
Quando você incorpora este comando ao sistema, o espaço da execução faz com que todos os grupos do Failover tornem-se ativos:

`hostname#`**`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 forçada 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 grupo ativo/ativo falhado do Failover a um estado unfailed, incorpore este comando:

`hostname(config)#`**`failover reset group`** *`group_id`*
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:

1. Mensagens de sistema de failover
2. Debugar mensagens
3. SNMP:

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.

Comunicações de failover perdidas preliminares com o companheiro no interface_name da relação

Este mensagem de failover é indicado se uma unidade do par de failover pode já não se comunicar com a outra unidade dos pares. Preliminar pode igualmente ser alistado como secundário para a unidade secundária.

(Preliminar) perdeu comunicações de failover com o companheiro no interface_name da relação

Verifique que a rede que é conectada à interface especificada funciona corretamente.

Debugar mensagens

A fim ver para debugar mensagens, incorpore o comando do **fover debugar**. Consulte a Referência de Comandos do Cisco Security Appliance Versão 7.2 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 Versão 7.2 para obter mais informações.

Tempo de Poll do Failover

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

O comando failover polltime unit msec [time] representa o intervalo de tempo da verificação da existência da unidade de standby com o uso de mensagens de hello de polling.

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.

Consulte failover polltime para obter mais informações.

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.

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