

ASA: VPN de acesso remoto (AnyConnect) de modo multicontexto

Introduction

Este documento descreve como configurar a Rede Virtual Privada (VPN - Virtual Private Network) de Acesso Remoto (RA) no firewall Cisco Adaptive Security Appliance (ASA) no modo de Contexto Múltiplo (MC - Multiple Context) usando a CLI. Ele mostra o Cisco ASA em modo de contexto múltiplo com recursos suportados/não suportados e requisitos de licenciamento em relação à VPN RA.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração SSL do ASA AnyConnect
- Configuração de contexto múltiplo do ASA

Componentes Utilizados

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

- AnyConnect Secure Mobility Client versão 4.4.00243
- Dois ASA5525 com software ASA versão 9.6(2)

Note: Baixe o pacote AnyConnect VPN Client do [Download de Software](#) da Cisco (somente clientes [registrados](#)).

Note: The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

O multicontexto é uma forma de virtualização que permite que várias cópias independentes de um aplicativo sejam executadas simultaneamente no mesmo hardware, com cada cópia (ou dispositivo virtual) aparecendo como um dispositivo físico separado para o usuário. Isso permite que um único ASA apareça como vários ASAs para vários usuários independentes. A família ASA oferece suporte a firewalls virtuais desde o lançamento inicial; no entanto, não havia suporte de virtualização para acesso remoto no ASA. O suporte de LAN2LAN (L2L) de VPN para multicontexto foi adicionado para a versão 9.0.

Note: De 9.5.2, suporte de virtualização baseado em vários contextos para conexões VPN Remote Access (RA) para o ASA.

A partir de 9.6.2 temos suporte para virtualização de Flash, o que significa que podemos ter imagem do Anyconnect por contexto.

Histórico de recursos para multicontexto

Novos recursos adicionados ao ASA 9.6(2)

| Recurso | Descrição |
|---|---|
| Recurso de pré-preenchimento/nome de usuário do certificado para modo de contexto múltiplo | O suporte SSL do AnyConnect é estendido, permitindo que CLIs de recursos de pré-preenchimento/nome de usuário do certificado, anteriormente disponíveis apenas em modo único, também sejam ativados em modo de contexto múltiplo. |
| Virtualização em Flash para VPN de acesso remoto | O acesso remoto VPN no modo de contexto múltiplo agora suporta a virtualização flash. Cada contexto pode ter um espaço de armazenamento privado e um local de armazenamento compartilhado com base na memória flash total disponível. |
| Perfis de cliente AnyConnect suportados em dispositivos multicontexto | Os perfis de cliente do AnyConnect são suportados em dispositivos multicontexto. Para adicionar um novo perfil usando o ASDM, você deve usar o AnyConnect Secure Mobility Client versão 4.2.00748 ou 4.3.03013 e posterior. |
| Failover stateful para conexões do AnyConnect em modo de contexto múltiplo | O failover stateful agora é compatível com conexões AnyConnect em modo de contexto múltiplo. |
| A DAP (Remote Access VPN Dynamic Access Policy, Política de acesso dinâmico de VPN de acesso remoto) é suportada em modo de contexto múltiplo | Agora você pode configurar o DAP por contexto no modo de contexto múltiplo. |
| A CoA da VPN de acesso remoto (alteração de autorização) é suportada em modo de contexto múltiplo | Agora você pode configurar CoA por contexto no modo de contexto múltiplo. |
| A localização da VPN de acesso remoto é suportada no modo de contexto múltiplo | A localização é suportada globalmente. Há apenas um conjunto de arquivos de localização que são compartilhados em contextos diferentes. |
| O armazenamento de captura de pacotes por contexto é suportado. | A finalidade deste recurso é permitir que o usuário copie uma captura diretamente de um contexto para o armazenamento externo ou para o armazenamento privado de contexto na memória flash. Esse recurso também permite copiar a captura bruta para as ferramentas externas de captura de pacotes, como o wire-shark, de dentro de um contexto. |

Recursos do ASA 9.5(2)

| Recurso | Descrição |
|--|---|
| AnyConnect 4.x e posterior (somente VPN SSL; sem suporte a | Suporte de virtualização baseado em vários contextos para conexões VPN Remote Access (RA) para o ASA. |

IKEv2)

Configuração de imagem do AnyConnect centralizada

Atualização de imagem do AnyConnect

Gerenciamento de recursos de contexto para conexões do AnyConnect

- O armazenamento em Flash não é virtualizado.
- A imagem do AnyConnect é configurada globalmente no contexto do administrador e a configuração se aplica a todos os contextos

Os perfis de cliente do AnyConnect são suportados em dispositivos multiconto. Para adicionar um novo perfil usando o ASDM, você deve ter o AnyConnect Secure Mobility Client versão 4.2.00748 ou 4.3.03013 e posterior.

- Configuração para controlar o uso máximo de licenças por contexto
- Configuração para permitir a intermitência de licença por contexto

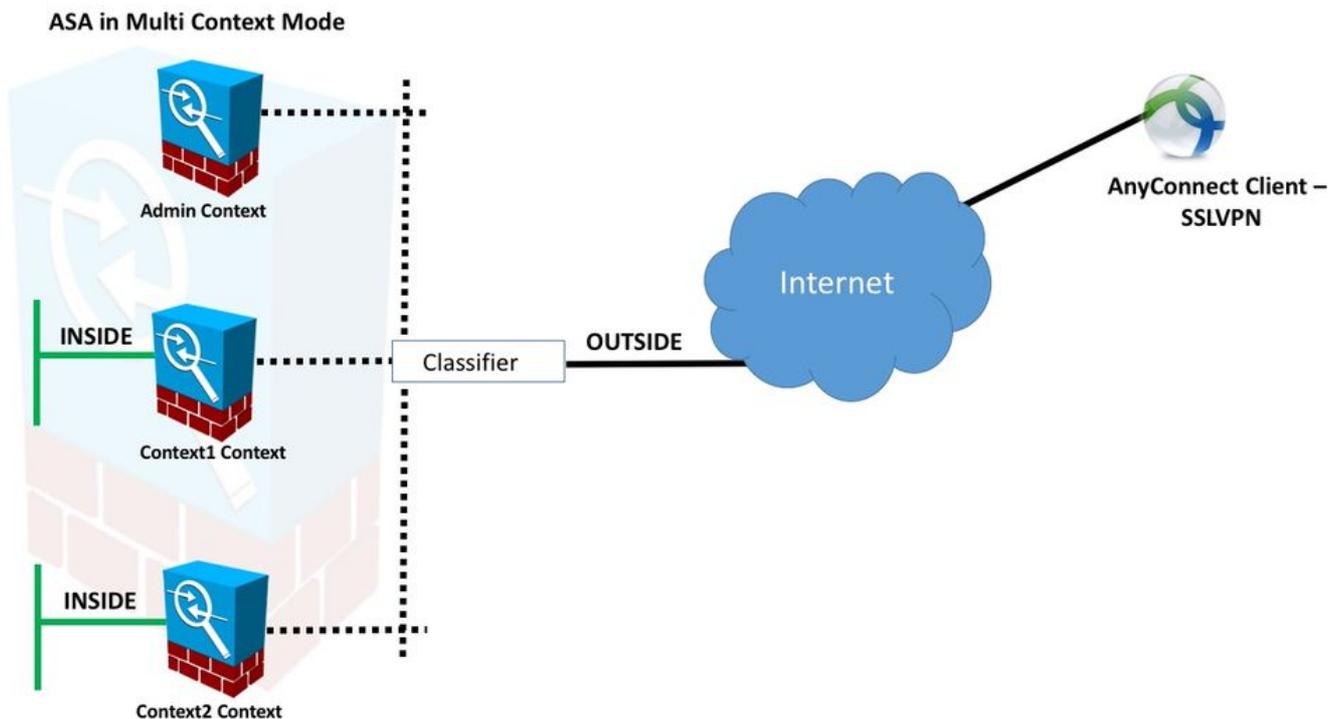
Licenciamento

- Licença Apex do AnyConnect necessária
- Licenças essenciais ignoradas/não permitidas
- Configuração para controlar o uso máximo de licenças por contexto
- Configuração para permitir a intermitência de licença por contexto

Configurar

Note: Use a [Command Lookup Tool \(somente clientes registrados\)](#) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede



Note: Vários contextos neste exemplo compartilham uma interface (FORA DO LADO) e o classificador usa os endereços MAC exclusivos (automáticos ou manuais) da interface para

encaminhar pacotes. Para obter mais detalhes sobre como o Security Appliance classifica pacotes em vários contextos, consulte [Como o ASA Classifica Pacotes](#)

O procedimento de configuração a seguir é com a versão ASA 9.6.2 e posterior, o que ilustra alguns dos novos recursos disponíveis. As diferenças no procedimento de configuração para as versões ASA anteriores à 9.6.2 (e superiores à 9.5.2) estão documentadas no [Apêndice A](#) do documento.

As configurações necessárias no contexto do sistema e nos contextos personalizados para configurar a VPN de acesso remoto são descritas abaixo:

Configurações iniciais no contexto do sistema

Para começar, no Contexto do sistema, configure failover, alocação de recursos VPN, contextos personalizados e verificação de licença Apex. O procedimento e as configurações são descritos nesta seção e na próxima seção

Etapa 1. Configuração de failover.

```
!! Active Firewall

failover
failover lan unit primary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2

!! Secondary Firewall

failover
failover lan unit secondary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2
```

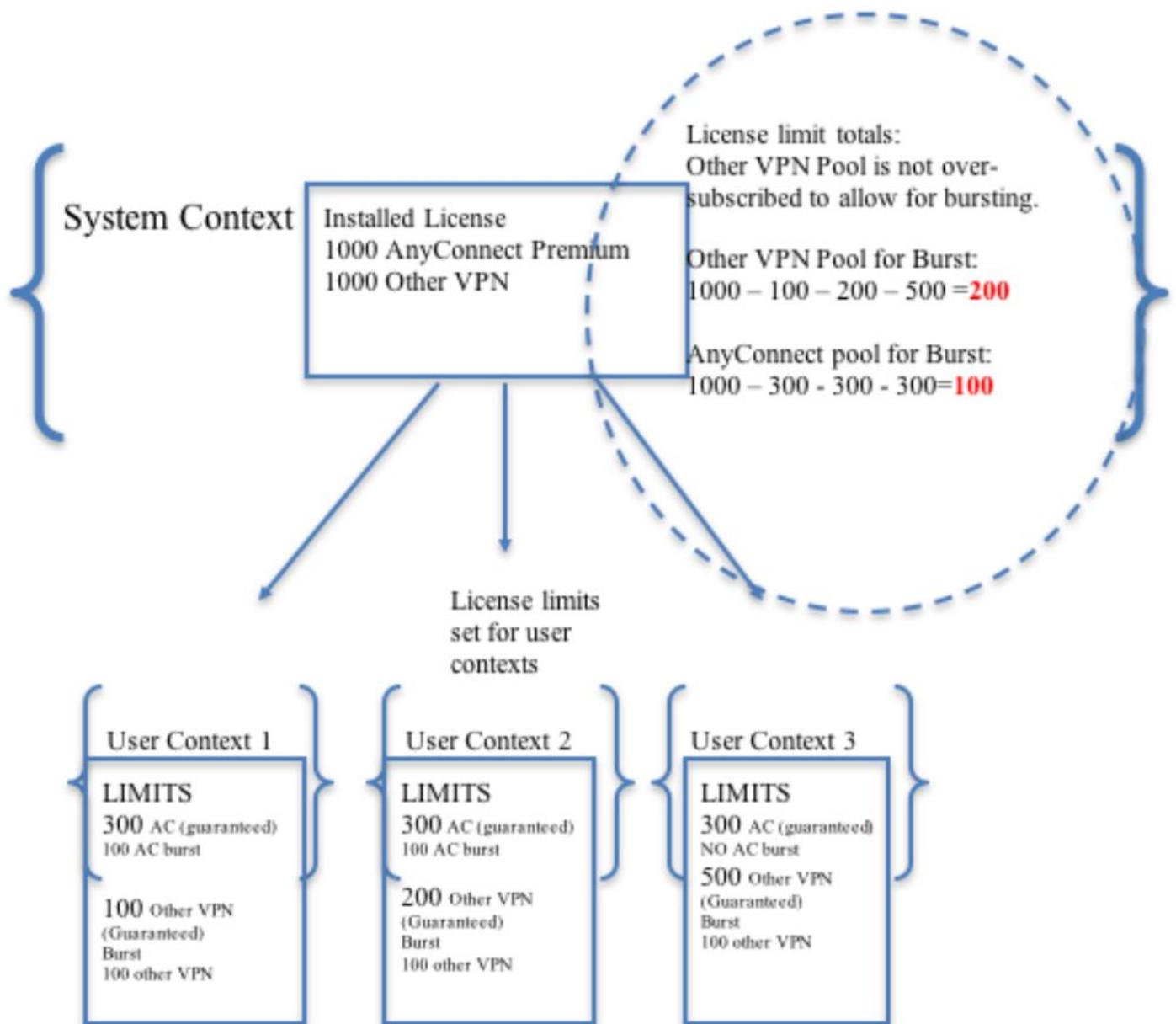
Etapa 2. Alocar recurso de VPN.

Configurado por meio da configuração de classe existente. As licenças são permitidas pelo número de licenças ou % do total por contexto

Novos tipos de recursos introduzidos para o MC RAVPN:

- VPN AnyConnect: Garantido a um contexto e não pode ter excesso de assinaturas
- VPN Burst AnyConnect: Permitir licenças adicionais de contexto além do limite garantido. O pool de burst consiste em quaisquer licenças não garantidas a um contexto e são permitidas para um contexto de burst em uma base de primeiro a chegar primeiro a usar

Modelo de provisionamento de licença VPN:



Note: O ASA5585 oferece no máximo 10.000 sessões de usuário do Cisco AnyConnect e, neste exemplo, 4.000 sessões de usuário do Cisco AnyConnect são alocadas por contexto.

```
class resource02
  limit-resource VPN AnyConnect 4000
  limit-resource VPN Burst AnyConnect 2000
```

```
class resource01
  limit-resource VPN AnyConnect 4000
  limit-resource VPN Burst AnyConnect 2000
```

Etapa 3. Configure contextos e atribua recursos.

Observação: neste exemplo, a GigabitEthernet0/0 é compartilhada entre todos os contextos.

```
admin-context admin
```

```
context admin
  allocate-interface GigabitEthernet0/0
  config-url disk0:/admin

context context1
  member resource01
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/1
  config-url disk0:/context1
  join-failover-group 1

context context2
  member resource02
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/2
  config-url disk0:/context2
  join-failover-group 2
```

Etapa 4. Verifique se a licença Apex está instalada no ASA, consulte o link abaixo para obter mais detalhes.

[Ativando ou desativando chaves de ativação](#)

Etapa 5. Configure um pacote de imagem do Anyconnect. Dependendo da versão do ASA que está sendo usada, há duas maneiras de carregar a imagem do Anyconnect e configurar a VPN do RA. Se a versão for 9.6.2 e superior, a virtualização Flash pode ser usada. Para versões anteriores à 9.6.2 consulte o [Apêndice A](#)

Note: Na versão 9.6.2 e superior, temos suporte para virtualização Flash, o que significa que podemos ter imagem do Anyconnect por contexto.

Virtualização em Flash

A VPN de acesso remoto requer armazenamento em flash para várias configurações e imagens, como pacotes do AnyConnect, pacotes de hostscan, configuração de DAP, plug-ins, personalização e localização, etc. No modo multicontexto antes de 9.6.2, os contextos do usuário não podem acessar nenhuma parte da flash e a memória flash é gerenciada e acessível ao administrador do sistema somente através do contexto do sistema.

Para resolver essa limitação, mantendo a segurança e a privacidade dos arquivos na memória flash, bem como a capacidade de compartilhar a memória flash de forma justa entre contextos, um sistema de arquivos virtual é criado para a memória flash no modo multicontexto. A finalidade deste recurso é permitir que as imagens do AnyConnect sejam configuradas por contexto, em vez de serem configuradas globalmente. Isso permite que diferentes usuários tenham diferentes imagens do AnyConnect instaladas. Além disso, ao permitir que as imagens do AnyConnect sejam compartilhadas, a quantidade de memória consumida por essas imagens pode ser reduzida. O armazenamento compartilhado é usado para armazenar arquivos e pacotes comuns a todos os contextos.

Note: O administrador de contexto do sistema continuará a ter acesso total de leitura e gravação a toda a memória flash e a sistemas de arquivos de armazenamento privados e compartilhados. O administrador do sistema precisará criar uma estrutura de diretório e organizar todos os arquivos privados e compartilhados em diferentes diretórios para que

esses diretórios possam ser configurados para contextos que possam ser acessados como armazenamento compartilhado e armazenamento privado, respectivamente.

Cada contexto terá permissão de leitura/gravação/exclusão em seu próprio armazenamento privado e terá acesso somente de leitura a seu armazenamento compartilhado. Somente o contexto do sistema terá acesso de gravação ao armazenamento compartilhado.

Nas configurações abaixo, o Contexto personalizado 1 será configurado para ilustrar o armazenamento privado e o Contexto personalizado 2 será configurado para ilustrar o armazenamento compartilhado.

Armazenamento privado

Você pode especificar um espaço de armazenamento privado por contexto. Você pode ler/gravar/excluir desse diretório no contexto (assim como no espaço de execução do sistema). No caminho especificado, o ASA cria um subdiretório nomeado após o contexto.

Por exemplo, para o contexto1, se você especificar `disk0:/private-storage` para o caminho, o ASA criará um subdiretório para esse contexto em `disk0:/private-storage/context1/`.

Armazenamento compartilhado

Um espaço de armazenamento compartilhado somente leitura pode ser especificado por contexto. Para reduzir a duplicação de arquivos grandes comuns que podem ser compartilhados entre todos os contextos (como pacotes do AnyConnect), o espaço de armazenamento compartilhado pode ser usado.

Configurações para usar o espaço de armazenamento privado

```
!! Create a directory in the system context.
ciscoasa(config)# mkdir private_context1

!! Define the directory as private storage url in the respective context.

ciscoasa(config)# context context1 ciscoasa(config-ctx)# storage-url private
disk0:/private_context1 context1

!! Transfer the anyconnect image in the sub directory.
ciscoasa(config)# copy flash:/anyconnect-win-4.2.01035-k9.pkg flash:/private_context1/context1
```

Configurações para usar o espaço de armazenamento compartilhado

```
!! Create a directory in the system context.

ciscoasa(config)# mkdir shared

!! Define the directory as shared storage url in the respective contexts.

ciscoasa(config)# context context2 ciscoasa(config-ctx)# storage-url shared disk0:/shared shared

!! Transfer the anyconnect image in the shared directory.
ciscoasa(config)# copy disk0:/anyconnect-win-4.3.05019-k9.pkg disk0:/shared
```

Verificar a imagem sob os respectivos contextos

!! Custom Context 1 configured for private storage.

```
ciscoasa(config)#changeto context context1
ciscoasa/context1(config)# show context1:
213 19183882 Jun 12 2017 13:29:51 context1:/anyconnect-win-4.2.01035-k9.pkg
```

!! Custom Context 2 configured for shared storage.

```
ciscoasa(config)#changeto context context2
ciscoasa/context2(config)# show shared:
195 25356342 May 24 2017 08:07:02 shared:/anyconnect-win-4.3.05017-k9.pkg
```

Etapa 6. Abaixo está o resumo das configurações no Contexto do sistema que inclui as configurações de virtualização flash descritas acima:

Contexto do sistema

```
context context1
member resource01
allocate-interface GigabitEthernet0/0
  storage-url private disk0:/private_context1 context1
config-url disk0:/context1.cfg
join-failover-group 1
!
context context2
member resource02
allocate-interface GigabitEthernet0/1
storage-url shared disk0:/shared shared
config-url disk0:/context2.cfg
join-failover-group 2
```

Passo 7: Configure os dois contextos personalizados conforme mostrado abaixo

Contexto personalizado 1

!! Enable WebVPN on respective interfaces

```
webvpn
enable outside
anyconnect image context1:/anyconnect-win-4.2.01035-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

!! IP pool and username configuration

```
ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0
username cisco password cisco
```

!! Configure the required connection profile for SSL VPN

```
access-list split standard permit 192.168.1.0 255.255.255.0
```

```
group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
banner value "Welcome to Context1 SSLVPN"
wins-server none
dns-server value 192.168.20.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
```

```
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
group-alias MC_RAVPN_1 enable
```

Contexto personalizado 2

```
!! Enable WebVPN on respective interfaces
```

```
webvpn
enable outside
anyconnect image shared:/anyconnect-win-4.3.05017-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

```
!! IP pool and username configuration
```

```
ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0
username cisco password cisco
```

```
!! Configure the required connection profile for SSL VPN
```

```
access-list split standard permit 192.168.1.0 255.255.255.0
```

```
group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
banner value "Welcome to Context2 SSLVPN"
wins-server none
dns-server value 192.168.60.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com
!
!
tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
group-alias MC_RAVPN_2 enable
```

Verificar

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

Verifique se a licença Apex está instalada

O ASA não reconhece especificamente uma licença Apex do AnyConnect, mas aplica as características de licença de uma licença Apex que incluem:

- AnyConnect Premium licenciado até o limite da plataforma
- AnyConnect para dispositivos móveis
- AnyConnect para telefone Cisco VPN

- Avaliação avançada de endpoint

Um syslog será gerado quando uma conexão for bloqueada porque uma licença Apex do AnyConnect não está instalada.

Verifique se o pacote do AnyConnect está disponível em contextos personalizados (9.6.2 e superiores)

```
! AnyConnect package is available in context1

ciscoasa/context1(config)# show context1:

213 19183882 Jun 12 2017 13:29:51 context1:/anyconnect-win-4.2.01035-k9.pkg

ciscoasa/pri/context1/act# show run webvpn
webvpn
enable outside
anyconnect image context1:/anyconnect-win-4.2.01035-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

Caso a imagem não esteja presente no contexto personalizado, consulte a [configuração da imagem do Anyconnect \(9.6.2 e superior\)](#).

Verifique se os usuários podem se conectar via AnyConnect em contextos personalizados

Dica: para melhor exibição, veja os vídeos abaixo em tela inteira.

```
!! One Active Connection on Context1

ciscoasa/pri/context1/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : cisco Index : 5
Assigned IP : 192.168.1.1 Public IP : 10.142.168.102
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Mobile
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 3186 Bytes Rx : 426
Group Policy : GroupPolicy_MC_RAVPN_1 Tunnel Group : MC_RAVPN_1
Login Time : 15:33:25 UTC Thu Dec 3 2015
Duration : 0h:00m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a2c2600005000566060c5
Security Grp : none

!! Changing Context to Context2

ciscoasa/pri/context1/act# changeto context context2

!! One Active Connection on Context2
```

```
ciscoasa/pri/context2/act# show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username : cisco Index : 1
Assigned IP : 192.168.51.1 Public IP : 10.142.168.94
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 10550 Bytes Rx : 1836
Group Policy : GroupPolicy_MC_RAVPN_2 Tunnel Group : MC_RAVPN_2
Login Time : 15:34:16 UTC Thu Dec 3 2015
Duration : 0h:00m:17s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a2c2400001000566060f8
Security Grp : none
```

```
!! Changing Context to System
```

```
ciscoasa/pri/context2/act# changeto system
```

```
!! Notice total number of connections are two (for the device)
```

```
ciscoasa/pri/act# show vpn-sessiondb license-summary
```

```
-----
VPN Licenses and Configured Limits Summary
-----
```

```
Status : Capacity : Installed : Limit
-----
```

```
AnyConnect Premium : ENABLED : 10000 : 10000 : NONE
Other VPN (Available by Default) : ENABLED : 10000 : 10000 : NONE
AnyConnect for Mobile : ENABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment : ENABLED(Requires Premium)
AnyConnect for Cisco VPN Phone : ENABLED
VPN-3DES-AES : ENABLED
VPN-DES : ENABLED
-----
```

```
-----
VPN Licenses Usage Summary
-----
```

```
Local : Shared : All : Peak : Eff. :
In Use : In Use : In Use : In Use : Limit : Usage
-----
AnyConnect Premium : 2 : 0 : 2 : 2 : 10000 : 0%
AnyConnect Client : : 2 : 2 : 0%
AnyConnect Mobile : : 2 : 2 : 0%
Other VPN : : 0 : 0 : 10000 : 0%
Site-to-Site VPN : : 0 : 0 : 0%
-----
```

```
!! Notice the resource usage per Context
```

```
ciscoasa/pri/act# show resource usage all resource VPN AnyConnect
```

```
Resource Current Peak Limit Denied Context
```

```
AnyConnect 1 1 4000 0 context1
```

```
AnyConnect 1 1 4000 0 context2
```

Troubleshoot

Esta seção fornece as informações que você pode usar para solucionar problemas de sua configuração.

[Solução de problemas do AnyConnect](#)

Tip: Caso o ASA não tenha a licença Apex instalada, a sessão do AnyConnect seria encerrada com o syslog abaixo:

```
%ASA-6-725002: O dispositivo concluiu o handshake SSL com o cliente
OUTSIDE:10.142.168.86/51577 para 10.106.44.38/443 para a sessão TLSv1
%ASA-6-113012: Autenticação de usuário AAA bem-sucedida: banco de dados local:
usuário = cisco
%ASA-6-113009: AAA recuperou a política de grupo padrão (GroupPolicy_MC_RAVPN_1)
para usuário = cisco
%ASA-6-113008: ACEITO do status da transação AAA: usuário = cisco
%ASA-3-716057: IP do usuário do grupo <10.142.168.86> Sessão encerrada, sem licença
Apex do AnyConnect disponível
%ASA-4-113038: O IP do usuário do grupo <10.142.168.86> não pode criar a sessão pai do
AnyConnect.
```

Apêndice A - Configuração de imagem do Anyconnect para versões anteriores à 9.6.2

A imagem do AnyConnect é configurada globalmente no contexto de administrador para as versões do ASA antes de 9.6.2 (observe que o recurso está disponível na versão 9.5.2) porque o armazenamento flash não é virtualizado e está acessível somente no contexto do sistema.

Etapas 5.1. Copie o arquivo do pacote do AnyConnect para a memória flash no contexto do sistema.

Contexto do sistema:

```
ciscoasa(config)# show flash:
```

```
195 25356342 May 24 2017 08:07:02 anyconnect-win-4.3.05017-k9.pkg
```

Etapas 5.2. Configurar a imagem do Anyconnect no contexto Admin.

Contexto do administrador:

```
webvpn
anyconnect image disk0:/anyconnect-win-4.3.05017-k9.pkg 1
anyconnect enable
```

Note: A imagem do Anyconnect pode ser configurada somente no contexto do administrador. Todos os contextos referem-se automaticamente a esta configuração global de imagem do Anyconnect.

Contexto personalizado 1:

```
!! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
nameif OUTSIDE
security-level 0
ip address 10.106.44.38 255.255.255.0 standby 10.106.44.39

!! Enable WebVPN on respective interfaces

webvpn
enable OUTSIDE
anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
banner value "Welcome to Context1 SSLVPN"
wins-server none
dns-server value 192.168.20.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
group-alias MC_RAVPN_1 enable
group-url https://10.106.44.38/context1 enable
```

Contexto personalizado 2:

```
!! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
nameif OUTSIDE
security-level 0
ip address 10.106.44.36 255.255.255.0 standby 10.106.44.37

!! Enable WebVPN on respective interface

webvpn
enable OUTSIDE
anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_2 internal
```

```
group-policy GroupPolicy_MC_RAVPN_2 attributes
banner value "Welcome to Context2 SSLVPN"
wins-server none
dns-server value 192.168.60.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com
```

```
tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
group-alias MC_RAVPN_2 enable
group-url https://10.106.44.36/context2 enable
```

Verifique se o pacote do AnyConnect está instalado no contexto do administrador e está disponível em contextos personalizados (antes de 9.6.2)

!! AnyConnect package is installed in Admin Context

```
ciscoasa/pri/admin/act# show run webvpn
webvpn
anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
anyconnect enable
```

```
ciscoasa/pri/admin/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
CISCO STC win2k+
3,1,10010
Hostscan Version 3.1.10010
Wed 07/22/2015 12:06:07.65
```

1 AnyConnect Client(s) installed

!! AnyConnect package is available in context1

```
ciscoasa/pri/admin/act# changeto context context1
```

```
ciscoasa/pri/context1/act# show run webvpn
webvpn
enable OUTSIDE
anyconnect enable
tunnel-group-list enable
```

```
ciscoasa/pri/context1/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
CISCO STC win2k+
3,1,10010
Hostscan Version 3.1.10010
Wed 07/22/2015 12:06:07.65
```

1 AnyConnect Client(s) installed

Referências

[Notas de versão: 9.5\(2\)](#)

[Notas de versão: 9.6\(2\)](#)

Informações Relacionadas

- [Dispositivos de segurança adaptáveis Cisco ASA 5500 Series](#)
- [Guia de solução de problemas do cliente AnyConnect VPN - Problemas comuns](#)
- [Gerenciamento, monitoramento e solução de problemas de sessões do AnyConnect](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)
- https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.pdf