ASA ：多情景模式远程访问(AnyConnect)VPN

简介

本文档介绍如何使用CLI在多情景(MC)模式下在思科自适应安全设备(ASA)防火墙上配置远程访问(RA)虚拟专用网络(VPN)。它显示了Cisco ASA在多情景模式下支持/不支持的功能和RA VPN的许可要求。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA AnyConnect SSL配置
- ASA多情景配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- AnyConnect安全移动客户端版本4.4.00243
- 两个ASA5525(带ASA软件版本9.6(2))

注意：从思科软件下载(仅限注册客户)下载AnyConnect VPN客户端包。

注意：本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

多情景是一种虚拟化形式，它允许应用程序的多个独立副本在同一硬件上同时运行，每个副本（或虚拟设备）对用户来说都显示为一个单独的物理设备。这允许单个ASA对多个独立用户显示为多个ASA。ASA系列自初始发布以来一直支持虚拟防火墙；但是，ASA中没有对远程访问的虚拟化支持。为9.0版本增加了对多情景的VPN LAN2LAN(L2L)支持。

注意：从9.**5.2**到ASA的VPN远程访问(RA)连接的基于多情景的虚拟化支持。

从9.**6.2**开始，我们支持闪存虚拟化，这意味着我们可以为每个情景提供Anyconnect映像。

多情景功能历史记录

ASA 9.6(2)中新增的功能

功能	
用于多情景模式的预填充/用户名自证书功能	AnyConnect SSL支持已扩展，允许在多情景模式下
远程访问VPN的闪存虚拟化	现在，多情景模式下的远程访问VPN支持闪存虚拟化
多情景设备支持的AnyConnect客户端配置文件	多情景设备支持AnyConnect客户端配置文件。要使用
在多情景模式下对AnyConnect连接进行状态故障切换	现在，多情景模式下的AnyConnect连接支持状态故障
多情景模式支持远程访问VPN动态访问策略(DAP)	您现在可以在多情景模式下按情景配置DAP。
多情景模式支持远程访问VPN CoA（授权更改）	您现在可以在多情景模式下为每个情景配置CoA。
多情景模式支持远程访问VPN本地化	全球支持本地化。只有一组本地化文件在不同上下文
支持每个情景的数据包捕获存储。	此功能的目的是允许用户将捕获直接从情景复制到外

ASA 9.5(2)中的功能

功能	
AnyConnect 4.x及更高版本(仅SSL VPN;不支持IKEv2)	基于多情景的虚拟化支持，用于VPN远程访问(RA)与ASA的连接。
集中式AnyConnect映像配置	• 闪存未虚拟化。 • AnyConnect映像在管理情景中全局配置，且配置适用于所有情景
AnyConnect映像升级	多情景设备支持AnyConnect客户端配置文件。要使用ASDM添加新配置文
AnyConnect连接的环境资源管理	• 可配置以控制每个情景的最大许可证使用量 • 允许每个情景的许可证突发的可配置性

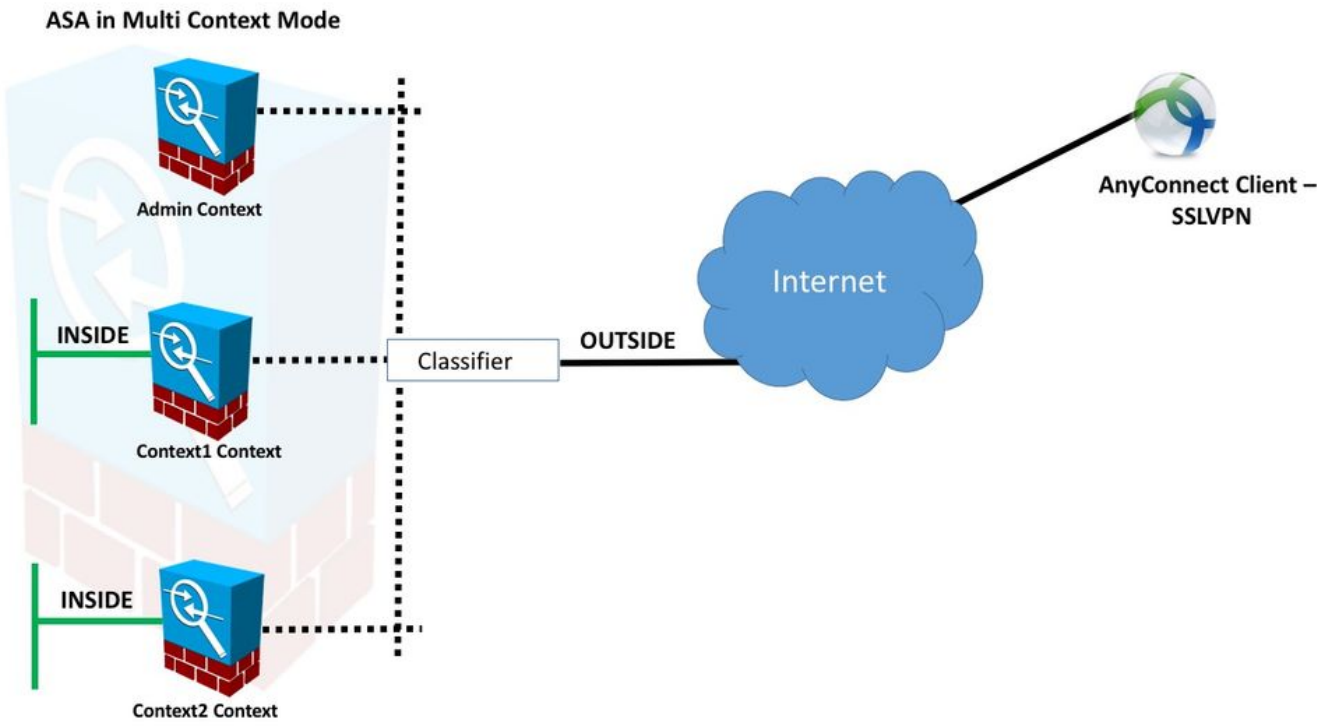
许可

- 需要AnyConnect Apex许可证
- 忽略/不允许Essentials许可证
- 可配置以控制每个情景的最大许可证使用量
- 允许每个情景的许可证突发的可配置性

配置

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图



注意： 本示例中的多个情景共享一个接口(OUTSIDE)，然后分类器使用接口唯一（自动或手动）MAC地址转发数据包。有关安全设备如何在多情景中对数据包进行分类的详细信息，请参阅ASA如何对数据包分类

ASA 9.6.2版及更高版本的以下配置过程说明了一些可用的新功能。9.6.2版（及9.5.2版以上版本）之前的ASA配置过程的差异记录在本文附录A中。

系统情景和自定义情景中设置远程访问VPN的必要配置如下所述：

系统情景中的初始配置

首先，在系统情景中配置故障切换、VPN资源分配、自定义情景和Apex许可证验证。本节和下一节将介绍操作步骤和配置

步骤1.故障切换配置。

```
 !! 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
```

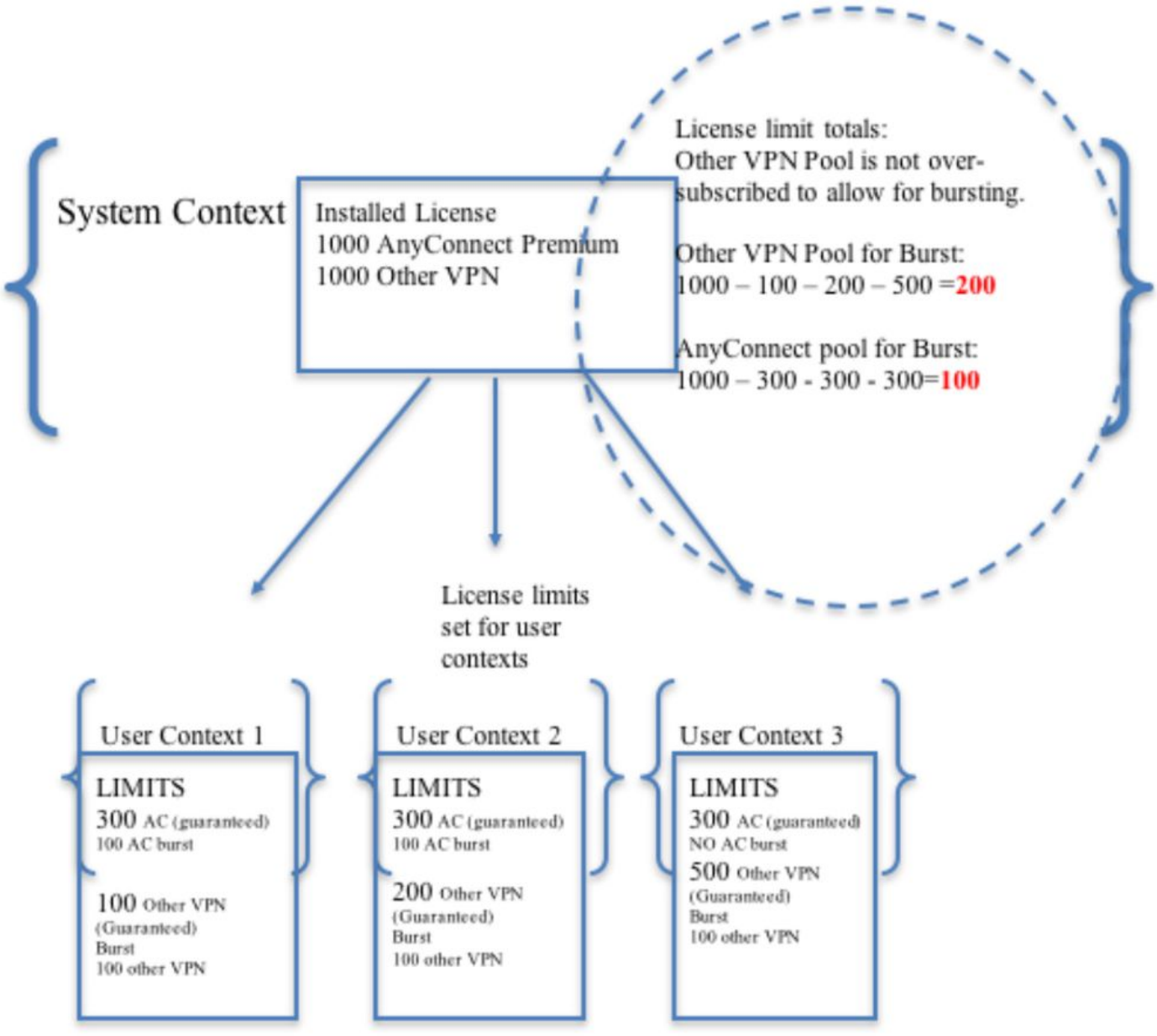
步骤2.分配VPN资源。

通过现有类配置进行配置。许可证数量或每个情景的许可证总数百分比允许

为MC RAVPN引入的新资源类型：

- VPN AnyConnect:对上下文有保证，且不能超订用
- VPN突发AnyConnect:允许超出保证限制的情景额外许可证。突发池由不保证对情景的任何许可证组成，并且允许在先到先服务的基础上突发情景

VPN许可证调配模型：



注意：ASA5585最多提供10,000个Cisco AnyConnect用户会话，在本例中，每个情景分配4000个Cisco AnyConnect用户会话。

```
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
```

步骤3.配置情景并分配资源。

> **注意：**在本示例中，GigabitEthernet0/0在所有情景中共享。

```
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
```

步骤4.验证ASA上是否安装了Apex许可证，请参阅以下链接了解更多详细信息。

激活或停用激活密钥

步骤5.配置Anyconnect映像包。根据使用的ASA版本，有两种方式加载Anyconnect映像和配置RA VPN。如果版本为9.6.2及更高版本，则可以使用闪存虚拟化。有关9.6.2以上版本的信息，请参阅附录A

> **注意：**在9.6.2及更高版本中，我们支持闪存虚拟化，这意味着我们可以为每个情景提供Anyconnect映像。

闪存虚拟化

远程访问VPN需要闪存来存储各种配置和映像，如AnyConnect软件包、主机扫描软件包、DAP配置、插件、自定义和本地化等。在9.6.2之前的多情景模式中，用户情景无法访问闪存的任何部分，并且闪存仅通过系统情景进行管理并可供系统管理员访问。

为了解决此限制，同时保持闪存上文件的安全性和隐私性，并且能够在情景之间公平共享闪存，在多情景模式下为闪存创建了虚拟文件系统。此功能的目的是允许AnyConnect映像基于每个情景进行配置，而不是全局配置。这允许不同用户安装不同的AnyConnect映像。此外，通过允许共享

AnyConnect映像，这些映像消耗的内存量可以减少。共享存储用于存储所有上下文通用的文件和软件包。

> **注意：** 系统情景管理员将继续对整个闪存以及专用和共享存储文件系统具有完全读写访问权限。系统管理员需要创建目录结构并将所有专用文件和共享文件组织到不同的目录中，以便这些目录可以配置为情景分别作为共享存储和专用存储访问。

每个情景都对其自己的专用存储具有读/写/删除权限，并且对其共享存储具有只读访问权限。只有系统情景才能对共享存储进行写访问。

在以下配置中，将配置自定义情景1以说明专用存储，配置自定义情景2以说明共享存储。

专用存储

您可以为每个情景指定一个专用存储空间。您可以在上下文（以及系统执行空间）中从此目录读/写/删除。 在指定路径下，ASA创建以情景命名的子目录。

例如，对于context1，如果为路径指定disk0:/private-storage，则ASA在disk0:/private-storage/context1/为此上下文创建子目录。

共享存储

每个情景可以指定一个只读共享存储空间。要减少可在所有情景（如AnyConnect软件包）之间共享的常见大型文件的重复，可以使用共享存储空间。

使用专用存储空间的配置

```
!! 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
```

使用共享存储空间的配置

```
!! 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
```

在各自的情景下验证映像

```
!! 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
```

步骤6.以下是系统情景中包括上述闪存虚拟化配置的配置摘要：

系统环境

```
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
```

步骤 7：配置两个自定义情景，如下所示

自定义情景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
```

自定义情景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
```

验证

使用本部分可确认配置能否正常运行。

验证是否安装了Apex许可证

ASA不明确识别AnyConnect Apex许可证，但它强制实施Apex许可证的许可证特征，包括：

- AnyConnect高级版许可到平台限制
- AnyConnect for Mobile
- Cisco VPN电话的AnyConnect
- 高级终端评估

当连接因未安装AnyConnect Apex许可证而被阻止时，将生成系统日志。

验证AnyConnect软件包是否在自定义情景（9.6.2及更高版本）中可用

```
! 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
```

如果自定义上下文下不存在映像，请参阅Anyconnect映像配置（9.6.2及更高版本）。

验证用户是否可以在自定义情景上通过AnyConnect进行连接

提示：为了更好地在全屏视频下显示视频。

```
!! 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
```

故障排除

本节提供可用于排除配置故障的信息。

[AnyConnect故障排除]

> **提示：**如果ASA未安装Apex许可证，AnyConnect会话将终止为以下系统日志：
>
> %ASA-6-725002：设备已完成与客户端OUTSIDE的SSL握手：10.142.168.86/51577到

10.106.44.38/443的TLSv1会话
%ASA-6-113012：AAA用户身份验证成功：本地数据库:用户=思科
%ASA-6-113009：AAA检索到用户= cisco的默认组策略(GroupPolicy_MC_RAVPN_1)
%ASA-6-113008：AAA事务状态接受：用户=思科
%ASA-3-716057：组用户IP <10.142.168.86>会话已终止，没有可用的AnyConnect Apex许可证
%ASA-4-113038：组用户IP <10.142.168.86>无法创建AnyConnect父会话。

附录A - 9.6.2之前版本的AnyConnect映像配置

AnyConnect映像在9.6.2之前的ASA版本的管理情景中全局配置（请注意，该功能从9.5.2开始可用），因为闪存未虚拟化，并且只能从系统情景访问。

步骤5.1.将AnyConnect软件包文件复制到系统情景中的闪存中。

系统环境:

```
ciscoasa(config)# show flash:

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

步骤 5.2 配置AnyConnect映像 在管理情景中。

管理情景：

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

注意：仅可在管理情景中配置AnyConnect映像。所有情景都自动引用此全局Anyconnect映像配置。

自定义情景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
```

自定义情景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
```

验证AnyConnect软件包是否安装在管理情景中且在自定义情景（9.6.2之前）中可用

```
!! 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
```

参考

[版本说明:9.5(2)]

[版本说明:9.6(2)]

相关信息

- Cisco ASA 5500 系列自适应安全设备
- AnyConnect VPN 客户端故障排除指南 - 常见问题
- 管理、监控和故障排除AnyConnect会话
- 技术支持和文档 - Cisco Systems
- https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.pdf