# 适用于 ACI 的 Cisco ASA Device Package 软件 1.3(12) 版本的发行说明

**Revised: 2019 年 12 月 25 日**

# 适用于 ACI 的 Cisco ASA Device Package 的发行说明

## 下载软件

使用您的 Cisco.com 登录凭证从以下位置获取 Cisco ASA Device Package 软件图像：

https://software.cisco.com/download/release.html?mdfid=283123066&flowid=22661&softwareid=286279676

## 可用的 APIC 产品

从 1.2(7.8) 开始，适用于 ACI 的 Cisco ASA Device Package 软件有两个版本：

- 思科 ASA 设备包 - 插入阵列的策略协调。您可以通过此版本从 APIC 配置 ASA 的许多重要功能，包括（但不限于）以下内容：
  - 接口
  - 路由
  - Access-list
  - NAT
  - TrustSec
  - 应用检测
  - NetFlow
  - 高可用性
  - 站点到站点 VPN
- 思科 ASA 设备包 - 插入阵列。此版本包含原始版本的以下功能：
  - 接口
  - 动态路由
  - 静态路由

## 支持的版本

Cisco ASA Device Package 软件仅支持其随附的 APIC 版本。

支持云协调器模式的 Cisco ASA Device Package 1.3(x) 是 Cisco ASA Device Package 1.2(x) 的一个超集。想要使用云协调器模式的客户应该使用 Cisco ASA Device Package 1.3(x) 和 APIC 3.1(x) 或更高版本。不想使用云协调器模式的客户应使用 Cisco ASA Device Package 1.2(x) 和 APIC 3.0(x) 或更低版本。

使用 ASA 9.12(x) 和更高版本时，使用 Cisco ASA Device Package 1.3(12.x)（支持云协调器模式）或 1.2(12.x)（无云协调器模式）和更高版本。否则，它将因 CSCvo59053 而失败。

下表列出了每个受支持平台支持的 Cisco ASA 软件版本：

| 平台 | 软件版本 |
|---|---|
| Cisco ASA 5500-X（5512 至 5555） | ASA 8.4(x) 和更高版本 |
| Cisco ASA 5585-X（SSP 10 至 SSP 60） | |
| 思科 Firepower 9300 安全设备 | ASA 9.6(1) 和更高版本 |
| Cisco Firepower 41xx 安全设备 | |
| Cisco Firepower 21xx 安全设备 | ASA 9.8(1) 和更高版本 |
| Cisco ASAv | ASA 9.2(x) 和更高版本<br>（Cisco ASA 和 APIC 兼容性矩阵） |

# 安装软件

有关如何安装设备软件包的说明，请参阅“软件下载”页面上超链接的对应版本的《**Cisco ASA 快速入门指南：APIC 集成**》。

**注释** 要从较低版本升级到较高版本，如果您的 APIC 版本有 CSCuv4353 的修补程序，则无需删除以前的软件包。否则，在安装较高版本之前，请从 APIC 中删除较低的版本。

# 漏洞搜索

作为注册的 Cisco.com 用户，请使用思科漏洞搜索工具登录以查看有关每个错误或警告的更多信息。

# 1.3(12) 版中已解决的警告问题

表 *1: Cisco ASA Device Package* 版本 *1.3(12)* 中已解决的警告

| 警告 | 说明 |
|---|---|
| CSCvn10162 | ASA DP 将 9.10 视为低于 9.3，其中部分 BGP 测试用例失败。 |
| CSCvo59053 | ASA DP 不可与 ASA 9.12 配合使用 |
| CSCvo59063 | 针对 ASA 9.12 的 S2SVPN 回归测试失败 |
| CSCvo60821 | ASA 中不建议对 SNMPv3 使用 MD5 |
| CSCvp48153 | ASA DP 需要单臂图的功能配置文件 |
| CSCvp53867 | 新的 DH 组支持 IKEv2 和 IPSec PFS 组 |
| CSCvp55263 | 不推荐在 ASA 9.13 中使用 3DES 和 AES-GMAC |

# 重要说明

- ASAv 不支持多情景模式。
- 支持动态 EPG 的 ACE 需要 ASA 映像 9.3.2 或更高版本。

# 当服务设备的 BGP 对等配置不完整时，策略管理器会锁定

使用此解决办法消除警告 CSCuw0342：

症状：当用于服务设备 BGP 对等的 I3Out 包含不完整的配置 (CSCuw03425) 时，策略管理器就会崩溃。

条件：用于服务设备 BGP 对等的 I3Out 缺失 l3extRsNodeL3OutAtt。

解决方法：确保 l3Out 包含 l3extRsNodeL3OutAtt。此问题将在后续版本中解决。

以下显示含有 l3extRsNodeL3OutAtt 的 BGP XML 示例：

```
<polUni>
<fvTenant name="tenant1">
<l3extOut name="StaticExternal">
<l3extLNodeP name="bLeaf-101">
<l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="190.0.0.11">
<ipRouteP ip="50.50.50.0/24">
<ipNexthopP nhAddr="40.40.40.102/32"/>
</ipRouteP>
</l3extRsNodeL3OutAtt>
<l3extLIfP name="portIf">
<l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/15]" ifInstT="ext-svi" encap="vlan-3843"
```

```
addr="40.40.40.100/28" mtu="1500"/>
</l3extLIfP>
</l3extLNodeP>
<l3extInstP name="ExtInstP">
<l3extSubnet ip="50.50.50.0/24" scope="export-rtctrl"/>
</l3extInstP>
<l3extRsEctx tnFvCtxName="tenant1ctx1"/>
</l3extOut>
</fvTenant>
</polUni>
```

# 如果在 APIC 注册后更改了 ASA 的版本，手动重新同步 APIC

使用此解决办法消除警告 CSCuw89163：

症状：有些命令不起作用。例如，**网络**和**邻居**命令的信息不显示 (CSCva89163)。

条件：如果您使用的 ASA 版本与在 APIC 中注册的版本不同，则不会随 APIC 自动重新注册。因此，如果您使用的是较旧版本的 ASA，某些命令可能不受支持。

解决方法：完成以下步骤，手动让 ASA 与 APIC 重新同步：

**过程**

---

**步骤 1** 在 APIC GUI 的**租户**选项卡上，展开左窗格中的 **L4-L7 服务**。

**步骤 2** 展开 **L4-L7 设备**。

**步骤 3** 展开运行 APIC 的防火墙。

**步骤 4** 右键单击运行 APIC 的设备，然后选择**重新查询设备验证**。

---

# 更改具体接口时 ASA 配置不回滚

使用此解决办法消除警告 CSCuw65130：

症状：桥接模式下，为部署的图形在 lif 配置下更改集群接口时，新接口可能无法在 ASA 上正确更新。

条件：更改 ASA 设备群集接口配置时。

解决方法：在进行任何设备更改之前，将图表与合同分离，然后再附加。

# 桥接模式下第二个图形将不正确的配置推送到 ASA

使用此解决办法消除警告 CSCuw68860：

症状：当在桥接模式下的 ASA 中的一组新集群接口上部署第二个或后续图形时，用户可能会看到未在正确的网桥组下配置群集接口。这将导致配置问题，进而造成与 ASA 中使用默认名称的现有群集接口发生冲突。

条件：桥接模式下，在 ASA 中使用一组新的采用默认接口名称的群集接口进行图形部署。

解决方法：配置图形时，在图形参数的**接口相关配置**下重命名群集接口名称。

# 恢复带外配置

此增强功能可消除警告 CSCvb90258：

症状：ASA 矩阵插入 (FI) 设备软件包 (DP) 不支持将配置保存在带外。

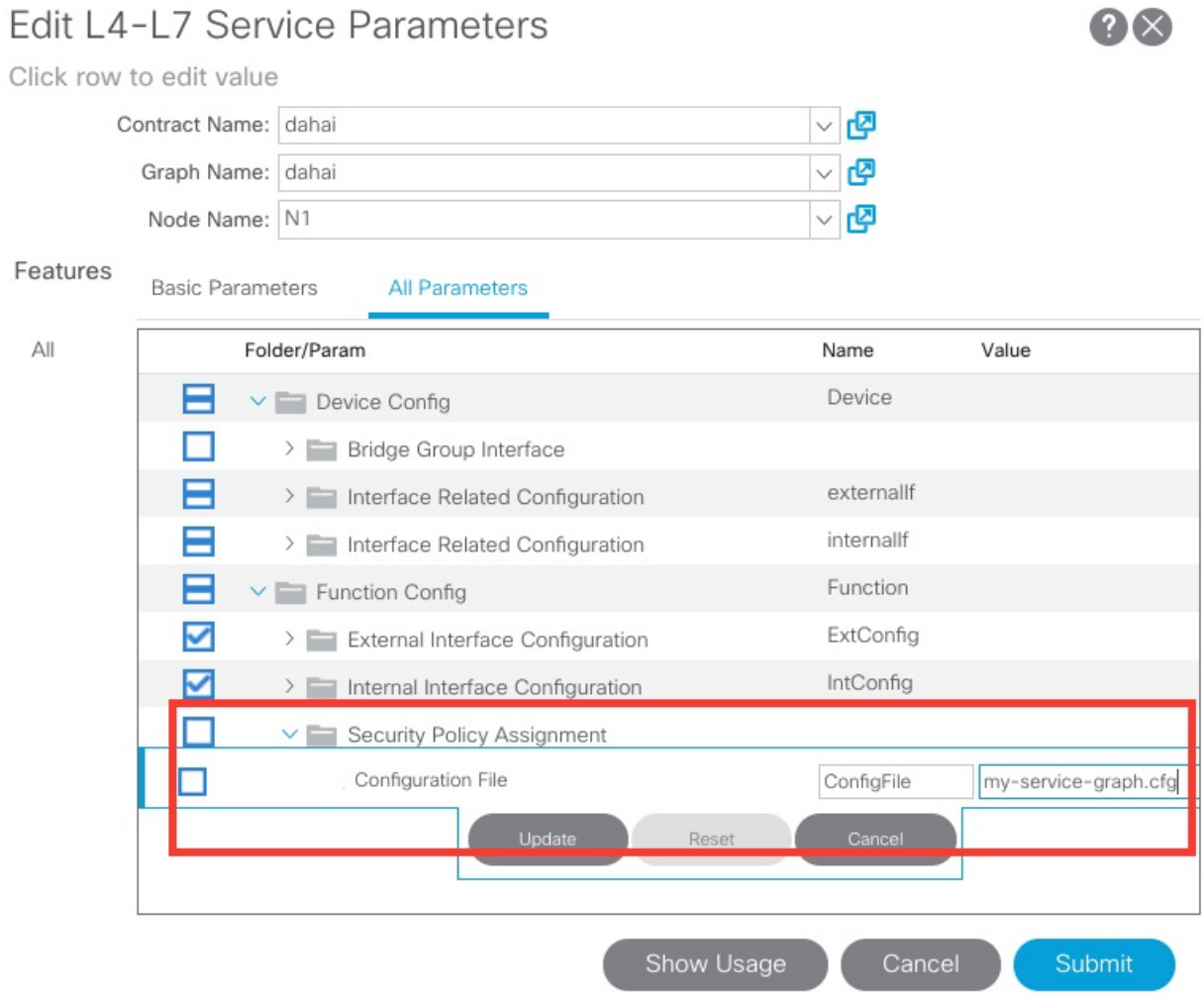
条件：ASA-FI-DP 只支持路由和接口配置。它不支持将安全策略绑定命令（如 `access-group` 和 `nat`）配置到服务图。要将安全策略分配给服务图，必须手动配置设置。如果在删除服务图后重新呈现服务图，则必须手动配置绑定。

解决方法：借助此增强功能，您可以将安全策略绑定命令保存到文件，以便重新附加服务图后 ASA-FI-DP 可以应用。

XML：`vnsMFunc` 下添加了名为 `SecurityPolicyAssignment` 的文件夹，使得您可以输入具有要分配给服务图的安全策略的配置的名称。

```
<vnsMFunc name="Firewall">
<vnsMFolder key="ExIntfConfigRelFolder" dispLabel="External Interface Configuration"
description="A list of additional interface parameters for external connector"...>
<vnsMFolder key="InIntfConfigRelFolder" dispLabel="Internal Interface Configuration"
description="A list of additional interface parameters for internal connector" ...>
<vnsMConn name="external" ...>
<vnsMConn name="internal" ...>
 <vnsMFolder key="SecurityPolicyAssignment"
   dispLabel="Security Policy Assignment"
   description="Assign the security policy in the named file to the service-graph">
  <vnsMParam key="ConfigFile"
    dispLabel="Configuration File"
    dType="str"
    description="Specify the name of the file that contains the out of band configuration specific to the
service-graph"/>
  </vnsMFolder>
 </vnsMFunc>
```

APIC：




- 如果文件在 ASA 上，输入文件的名称。
- 如果文件在 FTP 服务器上，请输入：`tftp://<ip-address>/<filename>`
- 如果文件在 FTP 服务器上，则输入：`ftp://<ip-address>/<filename>`

文件的内容应该是您必须在带外输入的命令，这些命令引用服务图中使用的接口。例如：

```
access-group <acl-name> [in|out] interface <nameif>
nat (<nameif>, <nameif>) …
service-policy <policy-name> interface <nameif>
crypto map <map-name> interface <nameif>
crypto ike2 enable <nameif>
```

以下是此类具有接口 `externalInt` 和 `internalInt` 的服务图的文件示例：

```
access-group access-group external_access_acl in interface externalInt
nat (internalInt,externalInt) source static real_obj mapped_obj
nat (internalInt,externalInt) source dynamic any mapped_obj interface
```

没有引用接口的命令不是文件的一部分，因为在您删除服务图时它们不会删除。此类命令的示例包括：

```
access-list
object network
object service
object-group network
object-group service
```

# 相关文档

- 思科 ACI 基础知识
- 思科 ACI 安全解决方案
- 思科 APIC 第 4-7 层服务部署指南
- 思科 APIC 产品支持
- 思科 ASA 系列规划图
- 思科 Firepower 管理中心

美洲总部
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

亚太区总部
CiscoSystems(USA)Pte.Ltd.
Singapore

欧洲总部
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco 在全球拥有 200 多个办事处。相关地址、电话和传真号码可见于
Cisco 位于 www.cisco.com/go/offices 上的网站。