基于 AWS 平台的 FortiManager 操作手册

版本 6.2

FORTINET 文档库
https://docs.fortinet.com

FORTINET 视频指南
https://video.fortinet.com

FORTINET 博客
https://blog.fortinet.com

客户服务与支持
https://support.fortinet.com

FORTINET 培训认证计划
https://www.fortinet.com/support-and-training/training.html

NSE 学院
https://training.fortinet.com

FORTIGUARD 中心
https://fortiguard.com/

最终用户许可协议
https://www.fortinet.com/doc/legal/EULA.pdf

意见反馈
电子邮箱：techdoc@fortinet.com

2020 年 2 月 18 日
FortiManager 6.2 AWS 平台 手册
02-620-611776-20200218

目录

关于面向 AWS 平台的 FortiManager

FortiManager 从安全运营角度提供了对 Fortinet Security Fabric 架构的可视性，支持真正的安全效能和安全威胁预见，以识别和了解威胁多维度，并加快采取有效响应行为和风险补救措施。

可量化的安全解决方案信息可生成能衡量的责任指标，并使用这些指标来衡量比较您企业内部和业界同行的安全准备情况。

集中式变更管理可帮助您更新策略和对象，维护配置模板并轻松配置 无线 AP、交换机、SD-WAN 和 SDN 接口等变更，从而规避安全事件，并下发应用配置变更和策略更新。

网络管理员能够将设备按逻辑分组划入不同管理域 (ADOM)，以有效应用策略并分发内容安全/固件更新，从而更好地控制其网络环境。FortiManager 是一款多功能网络安全管理产品，可通过集中中央管理和配置提供多样化部署类型、增长灵活性、并且通过 API 接口高级定制以及提供简易许可。高级定制（通过 API）和简单许可。

支持的实例类型

您可以将面向 AWS 平台的 FortiManager 部署为虚拟机。

以下为发布在 AWS 平台 Marketplace 上的各个 FortiManager 支持的实例类型。支持的实例可能会随时更改，恕不另行通知。

自带许可 (BYOL)

BYOL 清单支持以下实例类型。建议使用 m4.large 实例类型。

- c4.2xlarge
- c4.4xlarge
- c4.8xlarge
- c4.large
- c4.xlarge
- c5.2xlarge
- c5.4xlarge
- c5.9xlarge
- c5.18xlarge
- c5.large
- c5.xlarge
- d2.2xlarge
- d2.4xlarge
- d2.8xlarge
- d2.xlarge
- h1.2xlarge
- h1.4xlarge
- h1.8xlarge
- h1.16xlarge
- m4.2xlarge
- m4.4xlarge
- m4.10xlarge
- m4.16xlarge

- m4.large
- m4.xlarge
- m5.2xlarge
- m5.4xlarge
- m5.12xlarge
- m5.24xlarge
- m5.large
- m5.xlarge
- c5.12xlarge
- c5.24xlarge
- m5.16xlarge
- m5.8xlarge

按需订阅

产品名称	支持的实例类型	推荐的实例类型
FortiManager 集中式安全管理平台（最多可托管 2 台设备）	• m5.large • m5.xlarge • t2.medium	m5.large
FortiManager 集中式安全管理平台（最多可托管 10 台设备）	• h1.2xlarge • h1.4xlarge • h1.8xlarge • m5.2xlarge • m5.4xlarge • m5.12xlarge • m5.large • m5.xlarge • t2.large • t2.xlarge • m5.8xlarge	
FortiManager 集中式安全管理平台（最多可托管 30 台设备）	• h1.2xlarge • h1.4xlarge • h1.8xlarge • h1.16xlarge • m5.2xlarge • m5.4xlarge • m5.12xlarge • m5.24xlarge • m5.large • m5.xlarge • t2.2xlarge • t2.large • t2.xlarge • m5.16xlarge • m5.8xlarge	

FortiManager 集中式安全管理平台（最多可托管 100 台设备）	• h1.2xlarge • h1.4xlarge • h1.8xlarge • h1.16xlarge • m5.2xlarge • m5.4xlarge • m5.12xlarge • m5.24xlarge • m5.large • m5.xlarge • t2.2xlarge • t2.large • t2.xlarge • m5.16xlarge • m5.8xlarge	m5.xlarge
FortiManager 集中式安全管理平台（最多可托管 500 台设备）	• h1.2xlarge • h1.4xlarge • h1.8xlarge • h1.16xlarge • m5.2xlarge • m5.4xlarge • m5.12xlarge • m5.24xlarge • m5.large • m5.xlarge • t2.2xlarge • t2.xlarge • m5.16xlarge • m5.8xlarge	m5.2xlarge

型号

虚拟机版 FortiManager 基于托管设备的数量、每天的日志记录量和存储容量来颁发许可证。请参阅价格表，并通过经销商/分销商订购 SKU。这些 SKU 也称为 BYOL 型号。

您可以使用不同的 CPU 和 RAM 规格来部署虚拟机版 FortiManager，并在各个各大私有云和公有云平台上安装部署它们启动它们。

许可

您必须拥有许可证才能部署面向 AWS 平台 的虚拟机版 FortiManager。

订单类型

AWS 平台通常有两种订单类型：BYOL 和按需订阅。

BYOL 提供的是永久（常规系列和 v 系列）许可，而不是按需许可，按需许可是按小时订阅 Marketplace 上列出的产品。BYOL 许可证可通过经销商或分销商购买，许可证价格每季度调整一次，并在公开价格表中列出。私有云和公有云平台的 BYOL 许可证购买流程都相同。首次通过 GUI 或 CLI 访问实例时，必须先激活许可证，才能开始使用各种功能。

对于按需订阅，实例创建完成后即可使用虚拟机版 FortiGate。Marketplace 产品页面中介绍了不同托管设备数量和不同单位时间价格（每小时或每年）所对应的产品等级。

对于 BYOL 和按需订阅，云厂商将根据计算实例的资源消耗情况、存储等分别收费，而不是根据设备（在本例中为虚拟机版 FortiGate）上运行的软件收费。

BYOL 通常订购产品和服务组合，包括支持权利。您必须联系 Fortinet 支持部门，并提供您的客户信息，才能获得按需许可支持。请参阅 Marketplace 产品页面的*支持信息*。1

购买按需许可只需订阅 Marketplace 上的产品即可。但是，您必须联系 Fortinet 支持部门，并提供您的客户信息，才能获得支持权利。请参阅创建支持帐户（见第 8 页）。有关最新的按需定价和支持详细信息，请参见以下 Marketplace 上的产品页面：

- FortiManager 集中式安全管理平台（最多可托管 2 台设备）
- FortiManager 集中式安全管理平台（最多可托管 10 台设备）
- FortiManager 集中式安全管理平台（最多可托管 30 台设备）
- FortiManager 集中式安全管理平台（最多可托管 100 台设备）
- FortiManager 集中式安全管理平台（最多可托管 500 台设备）

按需部署虚拟机版 FortiGate 实例不支持使用虚拟域 (VDOM)。如果您打算使用 VDOM（VDOM 虚拟域），请改为部署 BYOL 实例。

创建支持帐户

面向 AWS 平台的虚拟机版 FortiManager 支持按需和 BYOL 许可模式。请参阅订单类型（见第 7 页）。

如要获得 Fortinet 技术支持，确保产品正常运行，您必须进行一些操作才能激活您的权利。权利激活后，Fortinet 支持团队将能够在系统中获取您的注册信息找到您的注册信息。

首先，如果您没有 Fortinet 帐户，请在客户服务与支持页面创建一个 Fortinet 帐户。

自带许可

您必须获得许可证才能激活虚拟机版 FortiManager。如果许可证尚未激活，那么在登录虚拟机版 FortiManager 时会看到许可证上传界面，并且无法继续进行虚拟机版 FortiManager 配置。

您可以通过任意 Fortinet 注册合作伙伴获得 BYOL 许可模式的许可证。如果没有注册合作伙伴联系方式，请联系 AWS 平台 sales@fortinet.com，以获得许可证购买帮助。

购买许可证或获得评估许可证（有效期 60 天）后，您将会收到一份包含激活码的 PDF 文件。

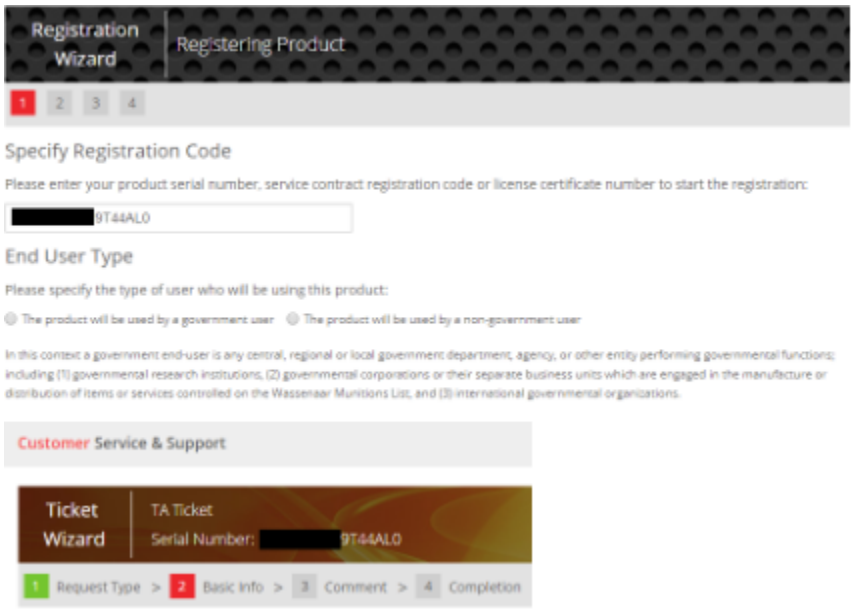
注册 BYOL 许可证：

1. 请前往 Customer Service & Support（客户服务与支持页面）创建新帐户或使用现有帐户登录。
2. 请前往 *Asset > Register/Activate*（*资产 > 注册 > 激活*）开始注册。在 *Specify Registration Code*（*指定注册码*）字段中输入许可证激活码，然后选择 *Next*（*下一步*）继续注册。在其他字段中输入您的详细信息。
3. 注册结束时，将许可证 (.lic) 文件下载到电脑上。稍后您需要上传此许可证，以激活虚拟机版 FortiManager。

许可证注册完成后，Fortinet 服务器可能需要 30 分钟来完全识别新许可证。在上传许可证 (.lic) 文件时，如果收到许可证无效的错误消息，请等待 30 分钟之后重试。

按需订阅

1. 部署并启动虚拟机版 FortiManager 按需 Elastic Compute Cloud (EC2) 实例，并登录虚拟机版 FortiManager GUI 管理控制台。
2. 从仪表盘中复制虚拟机版 FortiManager 序列号。
3. 请前往 Customer Service & Support（客户服务与支持页面）创建新帐户或使用现有帐户登录。
4. 请前往 *Asset* > *Register/Activate* （*资产* > *注册* > *激活*）开始注册。
5. 在 *Specify Registration Code*（*指定注册码*）字段中输入序列号，然后选择 *Next* 继续注册。在其他字段中输入您的详细信息。
6. 注册完成后，请联系 Fortinet 客户支持部门，并提供您的 FortiManager 实例序列号以及与 Fortinet 帐户关联的电子邮箱。



在 AWS 平台上部署 FortiManager

自带许可 (BYOL) 是永久许可，而非按需订阅（即按小时订阅）。BYOL 许可由经销商或分销商提供。

您可将虚拟机版 FortiManager 部署至 AWS 平台 Elastic Compute Cloud (EC2)。在部署虚拟机版之前，您必须拥有 Amazon Elastic Compute Cloud (EC2) 帐户。您可以使用 AWS 平台 Marketplace 启动流程或直接从 EC2 控制台部署虚拟机版 FortiManager。

有了 BYOL 许可后，FortiManager 在 AWS 平台 上的部署步骤如下：

1. 初始部署（见第 10 页）
2. 注册和下载许可证（见第 14 页）
3. 连接到 FortiManager（见第 15 页）
4. 添加更多存储空间（可选）（见第 15 页）

有了按需许可后，FortiManager 在 AWS 平台 上的部署步骤如下：

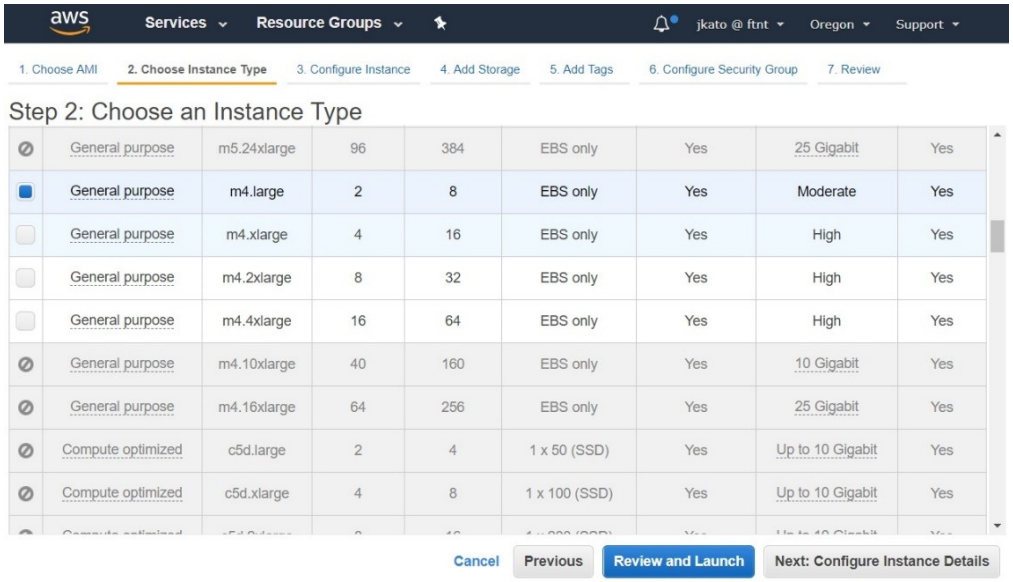
1. 初始部署（见第 10 页）
2. 添加更多存储空间（可选）（见第 15 页）

初始部署

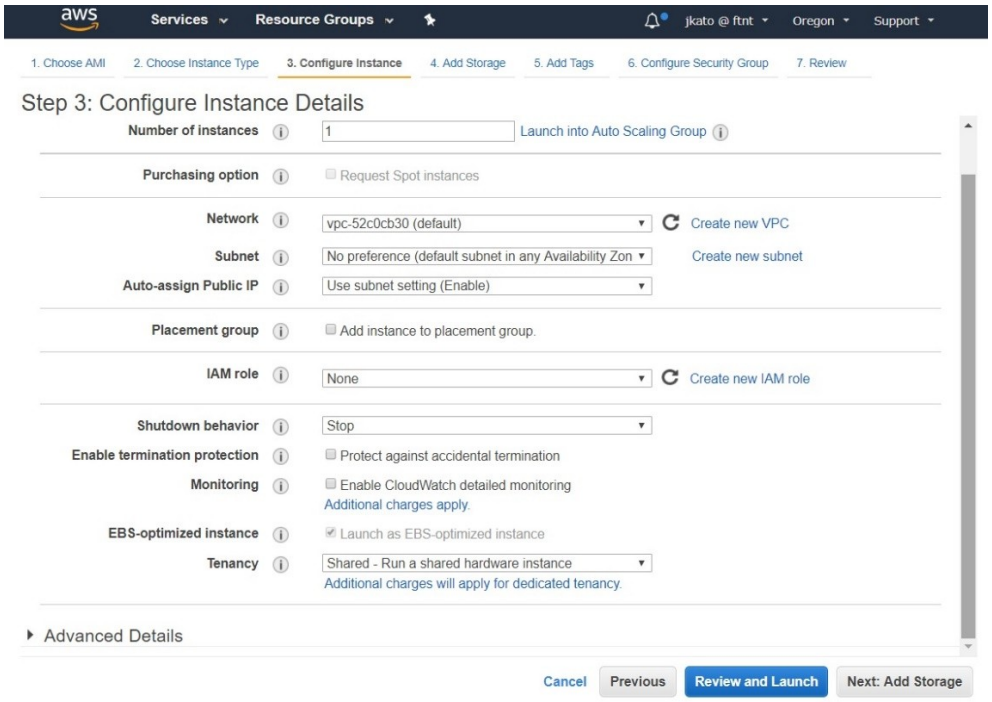
本示例在 EC2 控制台部署了一个 FortiManager 实例。

在 EC2 控制台部署 FortiManager 实例：

1. 启动虚拟机版 FortiManager 实例：
   a. 在 AWS 平台 Marketplace 上找到 FortiManager 产品。根据您要管理的设备数量选择 FortiManager 版本。
   b. 软件配置完成后，点击 *Continue to Launch（继续启动）*。BYOL 实例请选择 *Launch through EC2（通过 EC2 启动）*，然后点击 *Launch（启动）*.
2. 选择一种支持的实例类型。点击 *Next: Configure Instance Details（下一步：配置实例详细信息）*。



3. 配置各种属性：
   a. *网络*：确保选择连接到互联网网关的 VPC。默认情况下，VPC 连接到互联网网关。
   b. *子网*
   c. 启用*自动分配公共 IP 地址*
   d. 其他按需配置，具体取决于您的 IT 基础设施架构要求需求。
      点击 ***Next: Add Storage***（*下一步：添加存储空间*）。



4. 您可以通过选择以下任一选项来配置磁盘：
   a. 磁盘均保留默认值。或者您可以稍后添加其他磁盘。
   b. 增加第二卷磁盘容量。第二卷用于日志记录。
   c. 添加其他磁盘。

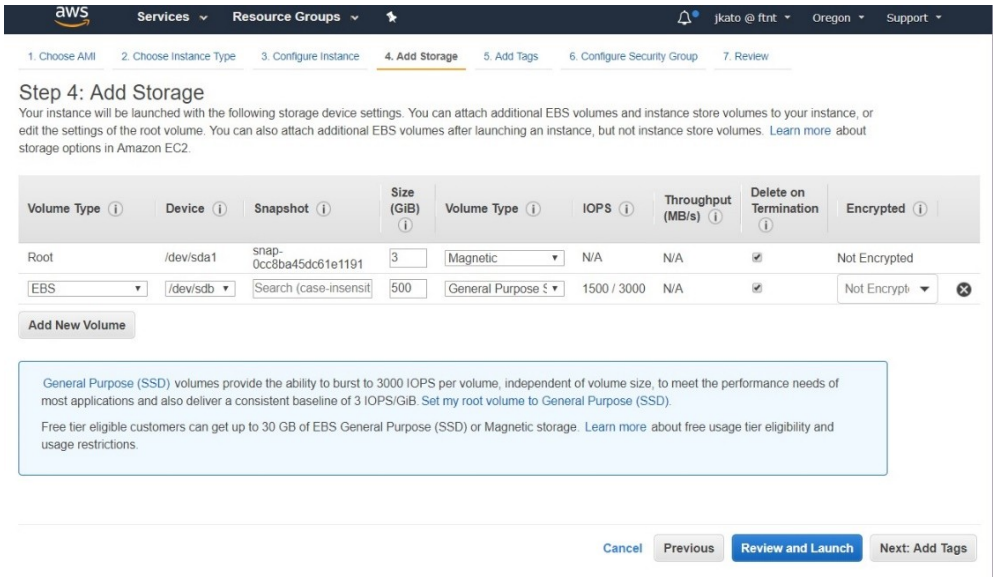
您可将卷类型配置为 *EBS*，将设备配置为 */dev/sdb*，并根据要求配置大小。您有权根据所购 BYOL 许可证的许可限制使用磁盘。

有关磁盘大小和设备许可数量的最高限额范围的更多详细信息，请参阅产品列表页面。

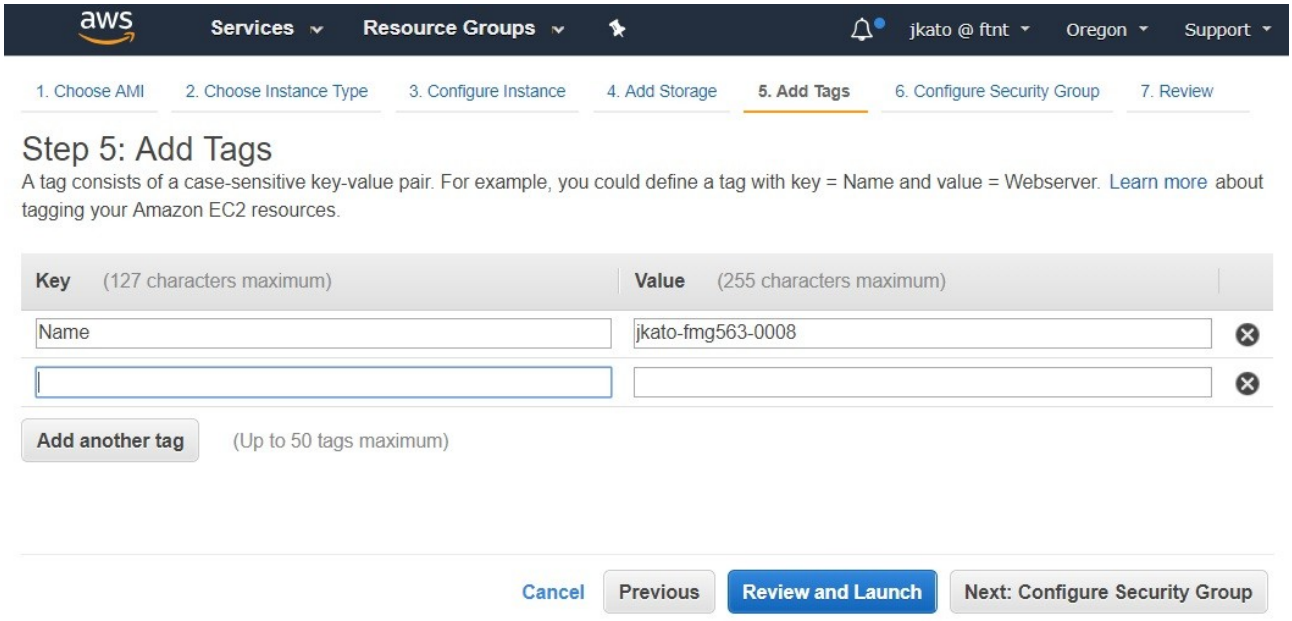
FortiManager 系统将为系统使用和意外配额溢出，采取预留一定的磁盘空间。其余空间可分配给设备。报告存储在预留空间中。下文介绍了相对于总可用磁盘空间（根设备之外）的预留磁盘配额：

- **小型磁盘**（小于或等于 500 GB）：系统预留 20% 或 50GB 的磁盘空间，以较小者为准。
- **中型磁盘**（小于或等于 1TB）：系统预留 15% 或 100GB 的磁盘空间，以较小者为准。
- **大型磁盘**（小于或等于 5TB）：系统预留 10% 或 200GB 的磁盘空间，以较小者为准。
- **超大型磁盘**（大于 5TB）：系统预留 5% 或 300GB 的磁盘空间，以较小者为准。如要在此时添加更多存储，请依照添加更多存储空间（可选）中的说明进行操作。

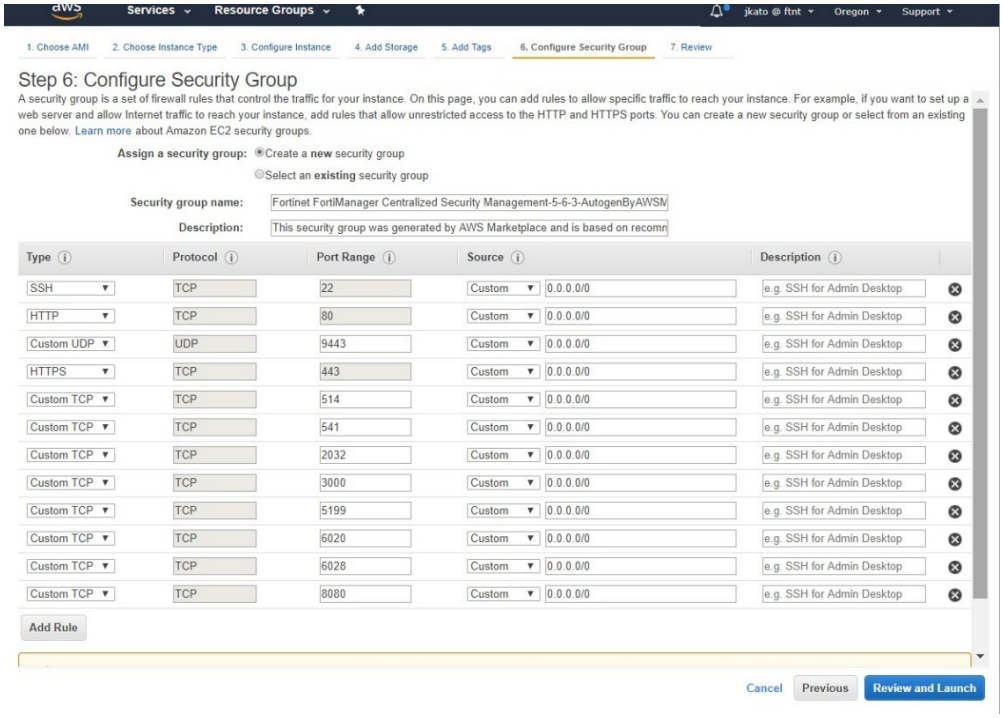
点击 Next: Add Tags（下一步：添加标签）。



5. 按需创建或添加标签。使用名称标签来区分 EC2 实例名称非常方便。此外，您还可以将此部分留空，然后点击 *Next: Configure Security Group（下一步：配置安全组）*继续操作。

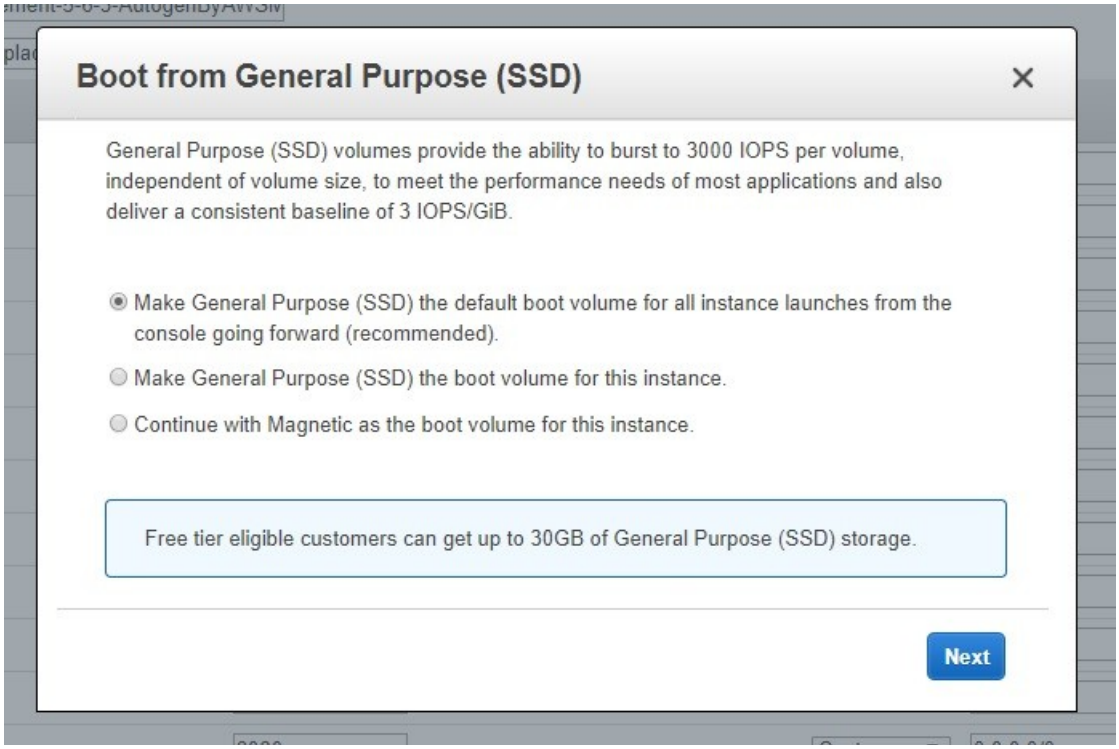


6. 查看默认配置的所有开放端口。通常，这些端口将保持原样。通过 SSH 或 HTTPS 协议访问 FortiManager 管理控制台。访问 GUI 需要打开 HTTPS 端口。请参阅此处，了解每个端口的使用用途用途。



7. 查看配置并启动实例：

   a. 点击 *Review and Launch（查看并启动）*。系统可能会弹出窗口，询问您是否要将通用 (SSD) 设置为默认启动卷。选择所需选项，然后点击 *Next（下一步）*。



   b. 查看配置，然后点击 *Launch（启动）*。

   c. 选择一个密钥对，选中确认复选框，然后点击 *Launch Instance（启动实例）*。

8. 按需订阅虚拟机版 FortiManager 实例需要连接到 FortiCare，以获得有效的许可证。否则，虚拟机版 FortiManager 将出于自我保护而自动关闭。确保：

   - 安全组和 ACL 允许出站能连接到 https://directregistration.fortinet.com:443。

- 公共 IP 地址（默认值或 EIP）已被分配。

注册和下载许可证

您可以通过任意 Fortinet 注册合作伙伴获得 BYOL 许可模式的许可证。如果没有注册合作伙伴联系方式，请联系 AWS 平台 sales@fortinet.com，以获得许可购买帮助。

购买许可证或获得评估许可证（有效期 60 天）后，您将会收到一份包含激活码的 PDF 文件。

注册下载许可证：

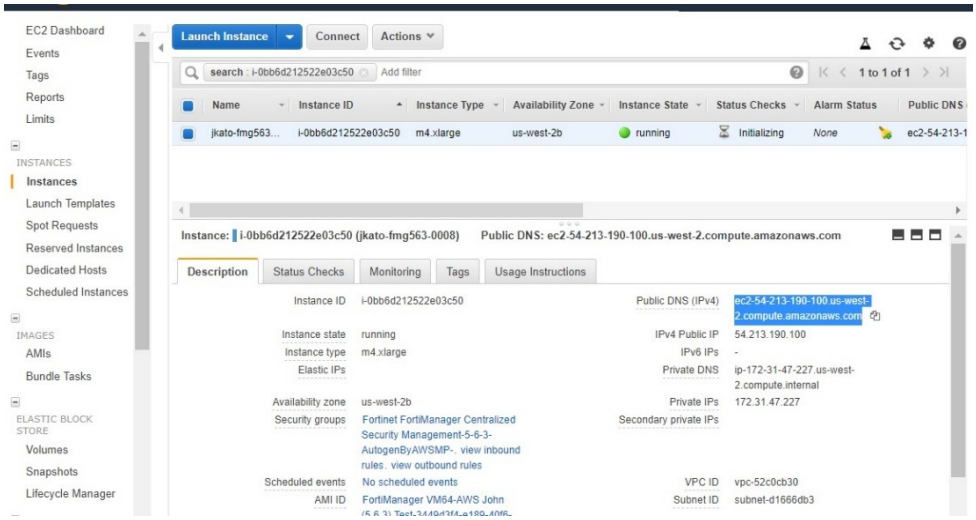
1. 请前往 Customer Service & Support（客户服务与支持页面）创建新帐户或使用现有帐户登录。
2. 请前往 *Asset* > *Register/Activate*（*资产* > *注册* > *激活*）开始注册。在 *Specify Registration Code*（*指定注册码*）字段中输入许可证激活码，然后选择 *Next*（*下一步*）继续注册。在其他字段中输入您的详细信息。
3. 注册结束时，将许可证 (.lic) 文件下载到电脑上。稍后您需要上传此许可证，以激活虚拟机版 FortiWeb。
4. 注册许可证后，Fortinet 服务器可能需要 30 分钟来完全识别新许可证。在上传许可证 (.lic) 文件时，如果收到许可证无效的错误消息，请等待 30 分钟之后重试。

连接到 FortiManager

连接到 FortiManager：

1. 登录 EC2 控制台，导航（导向）至 FortiManager 实例。查找可以通过 Internet 访问的公共 DNS 或弹性 IP 地址。

   （查找 FortiManager 实例可以通过 Internet 访问的公共 DNS 或弹性 IP 地址）



2. 打开浏览器，输入 https://<公共 DNS 或弹性 IP 地址>。
3. 部署完成后，使用用户名“admin”登录 FortiManager。初始密码是实例 ID。强烈建议您在首次登录时更改初始密码。
4. 前往*系统设置*，查看仪表盘上的系统状态。检查磁盘空间是否充足。如果磁盘空间不足，您必须添加磁盘/卷。

添加更多存储空间（可选）

您可以在启动后向 FortiManager 添加更多存储。创建一个 EBS 存储，并将其添加到 EC2 控制台上的 FortiManager 实例，

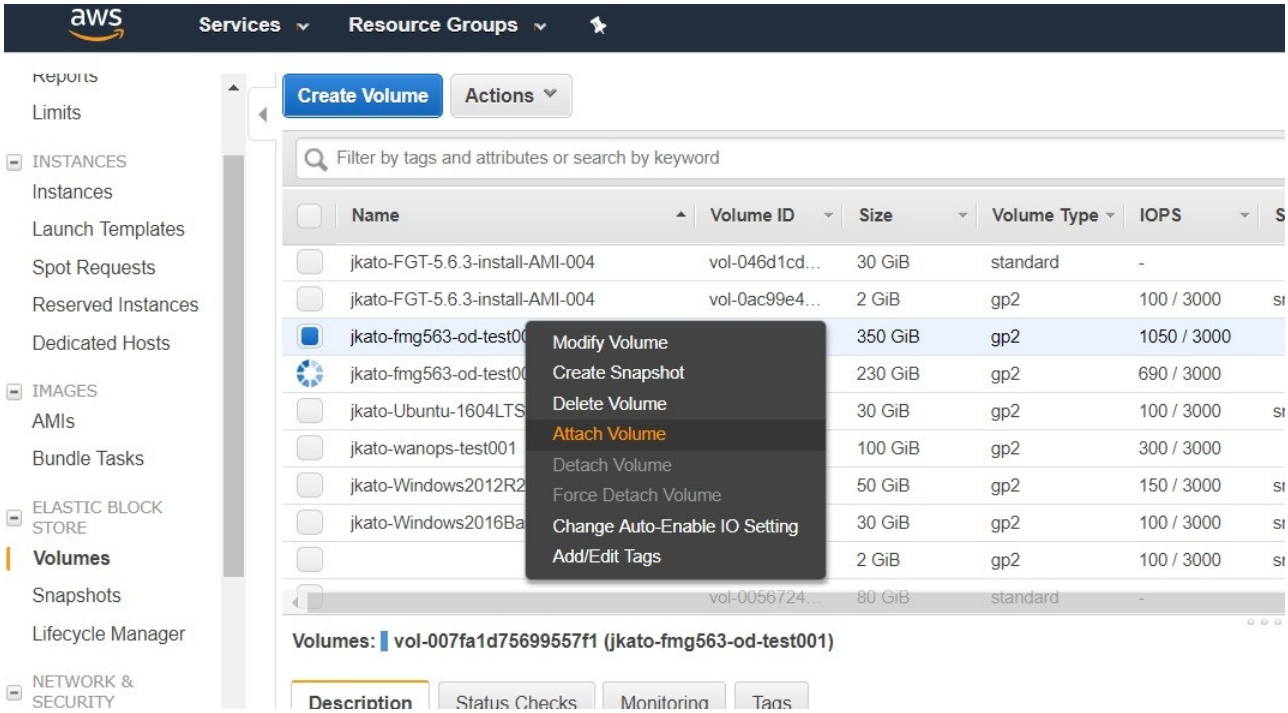
然后通过 GUI 或 SSH 上的 CLI 窗口访问 FortiManager，运行 exec lvm extend 命令来实现添加存储。

有关详细信息，请参阅技术说明：在虚拟机版 FortiAnalyzer/虚拟机版 FortiManager 中扩展磁盘空间。

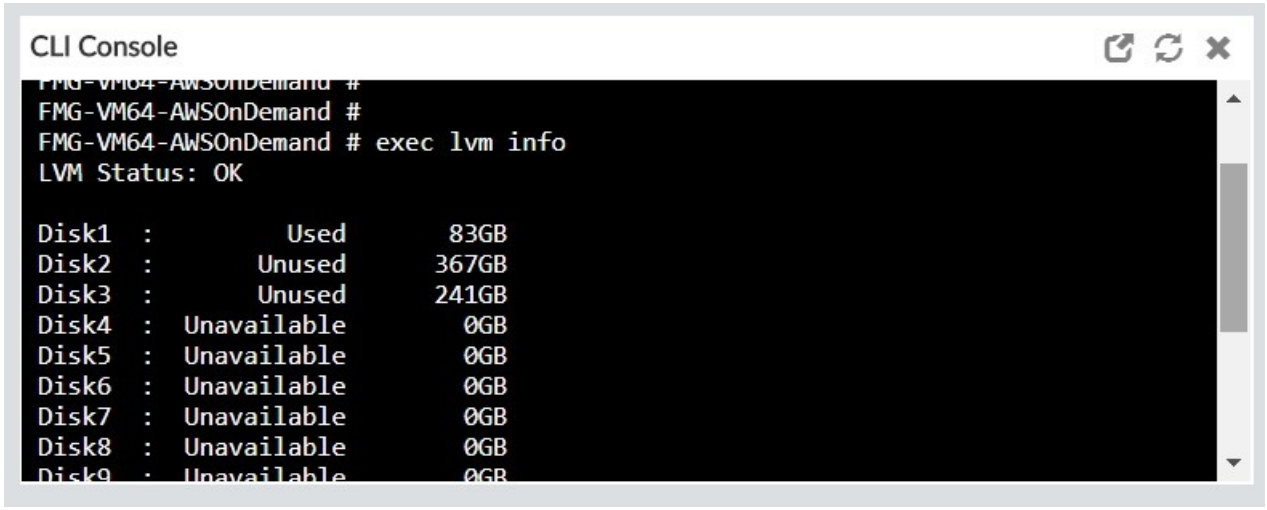
本示例创建并添加了两个磁盘卷。

添加更多存储空间：

1. 在 EC2 控制台中，创建一个磁盘卷，并将其添加到 FortiManager EC2 实例。



2. 使用 GUI 或 SSH 登录 FortiManager。如果使用 GUI，请打开 CLI。
3. 运行 exec lvm info 命令，检查磁盘状态已经添加了两个卷，目前状态*尚未使用*。



4. 运行 exec lvmextend 命令。按照说明重新启动系统。

```
FMG-VM64-AWSOnDemand #
FMG-VM64-AWSOnDemand # exec lvm extend
Disk2 will be added to LVM.
Disk3 will be added to LVM.
This operation will need to reboot the system.
Do you want to continue? (y/n)y
```

5. 登录 FortiManager GUI 界面。前往仪表盘仪表盘界面，在 *System Resources* > *Disk Usage*（*系统资源* > *磁盘使用情况*）下查看磁盘空间是否已经增加。

Security Fabric 连接器与 AWS 平台相集成

您可以使用 FortiManager 创建面向 AWS 平台 的 Fabric 连接器的配置，并将其安装到 FortiOS。

FortiManager 中的 Fabric 连接器定义了连接器类型，并提供了 FortiOS 与产品通信和校验的信息。有些情况下，FortiGate 必须通过 Fabric 连接器与产品通信，而有些情况下，FortiGate 可直接与产品通信。

FortiOS 无需 Fabric 连接器即可直接与 AWS 平台 通信。以下是使用 FortiManager 创建面向 AWS 平台 的 Fabric 连接器的概述：

1. 创建面向 AWS 平台 的 Fabric 连接器对象。请参阅创建面向 AWS 平台 的 Fabric 连接器对象（见第 18 页）。
2. 将地址名称从 AWS 平台 导入到 Fabric 连接器对象。请参阅将地址名称导入到 Fabric 连接器（见第 20 页）。

导入的地址名称将被转换为防火墙地址对象。这些对象尚不包括 IP 地址。这些对象位于 *Firewall Objects* > *Addresses*（*防火墙对象* > *地址*）窗格中。

3. 在将用于创建新策略的策略包中，创建一个 IPv4 策略，并提供面向 AWS 平台 的防火墙地址对象。请参阅创建 IP 地址策略（见第 21 页）。
4. 将策略包安装到 FortiGate。请参阅安装策略包（见第 22 页）。

FortiGate 与 AWS 平台 进行通信，以使用 IP 地址动态填充防火墙地址对象。

如果过滤器名称导入 FortiManager 后发生更改，则必须再次修改过滤器。

创建面向 AWS 平台的 Fabric 连接器对象

您可以使用 FortiManager 创建面向 Amazon Web Services (AWS 平台) 的 Fabric 连接器，然后从 AWS 平台平台 导入地址名称，以自动创建动态对象并应用在策略中。当您将策略安装到一个或多个 FortiGate 设备时，FortiGate 会使用策略信息与 AWS 平台 通信，并使用 IP 地址动态填充对象。此配置不需要 Fortinet SDN 连接器。

在创建面向 AWS 平台的 Fabric 连接器时，您可指定 FortiGate 如何与 AWS 平台直接通信。如果启用了 ADOM 管理域，那么您可以为每个 ADOM 管理域创建一个 Fabric 连接器。

要求：

- FortiManager 6.0 ADOM 或使用更高版本
- FortiGate 由 FortiManager 管理。
- 托管的 FortiGate 可在 AWS 平台平台上配置。以下为配置过程摘要：

创建面向 AWS 平台的 Fabric 连接器对象：

1. 前往 *Fabric View* > *Fabric Connectors*（*Fabric 视图* >*Fabric 连接器*）。
2. 点击 *Create New*（*新建*）。*Create New Fabric Connector*（*创建新的 Fabric 连接器*）向导打开。
3. 在 SDN *下方，选*择 AWS 平台，然后点击 *Next*（*下一步*）。
4. 配置以下选项，然后点击 *OK*（*确定*）：

名称	输入 Fabric 连接器对象的名称。
类型	显示 *Amazon Web Services (AWS 平台)*。
AWS 平台 访问密钥 ID	输入 AWS 平台 的访问密钥 ID。
AWS 平台 秘密访问密钥	输入 AWS 平台 的访问密钥。
AWS 平台 区域名称	输入 AWS 平台 的区域名称。
AWS 平台 VPC ID	键入 AWS 平台 VPC ID。
更新间隔	规定动态防火墙对象的更新频率（以秒为单位）
状态	切换*打开*，以启用 Fabric 连接器对象。切换*关闭*，以禁用 Fabric 连接器对象。

为 Fabric 连接器配置动态防火墙地址

您不能将地址名称导入为 Microsoft Azure 平台和 Nuage 虚拟服务平台创建的 Fabric 连接器。相反，您必须创建 FortiGate 与 Microsoft Azure 和 Nuage 虚拟服务平台通信时可动态填充的动态防火墙对象。

为 Microsoft Azure Fabric 连接器配置动态防火墙地址：

1. 前往 *Policy & Objects* > *Object Configurations*（*策略和对象* > *对象配置*）。
2. 在树形菜单中，前往 Firewall Objects > Addresses（防火墙对象 > 地址）。
3. 在内容窗口中，点击 Create New（新建），然后选择 *Address*（*地址*）。
4. 填写以下 Microsoft Azure Fabric 连接器选项：

地址名称	输入防火墙地址对象的名称。
类型	选择 *Fabric 连接器地址*。
SDN	选择 Microsoft Azure Fabric 连接器。
过滤	键入 AWS 平台 实例的过滤器名称。

5. 根据需要设置其余选项，然后点击 *OK*（*确定*）。

为 Nuage Fabric 连接器配置动态防火墙地址：

1. 前往 *Policy & Objects* > *Object Configurations*（*策略和对象* > *对象配置*）。
2. 在树形菜单中，前往 Firewall Objects > Addresses（防火墙对象 > 地址）。
3. 在内容窗口中，点击 Create New（新建），然后选择 *Address*（*地址*）。
4. 填写以下 Nuage Fabric 连接器选项：

地址名称	输入防火墙地址对象的名称。
类型	选择 *Fabric 连接器地址*。
SDN	选择 Nuage 虚拟服务平台 Fabric 连接器。
组织	输入 Nuage 虚拟服务平台的组织名称
子网名称	输入 Nuage 虚拟服务平台的子网名称。
策略组	输入 Nuage 虚拟服务平台的策略组名称。

5. 根据需要设置其余其它选项，然后点击 *OK（确定）*。

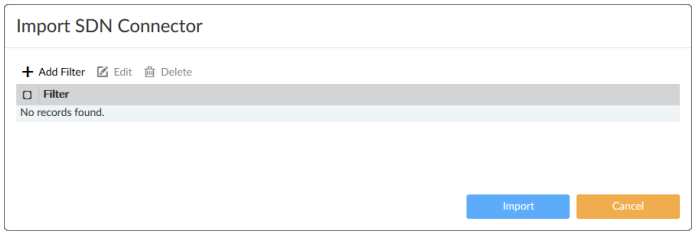
将地址名称导入 Fabric 连接器

配置 Fabric 连接器后，您可以将动态对象从 AWS 平台 等云平台导入 Fabric 连接器，并自动创建动态防火墙地址对象。

从 AWS 平台导入地址名称时，必须先添加过滤器以显示正确的实例，然后再导入地址名称。

导入 AWS 平台的地址名称：

1. 前往 *Policy & Objects* > *Object Configurations（策略和对象 > 对象配置）*。
2. 在树形菜单中，前往 Security Fabric > Fabric Connectors（Security Fabric > Fabric 连接器）。
3. 在内容窗口中，右击 Fabric 连接器，然后选择 *Import（导入）*。*Import SDN Connector（导入 SDN 连接器）*对话框打开。



4. 创建一个过滤器，以选择正确的 AWS 平台 实例：
   a. 点击 *Add Filter（添加过滤器）*。
   *Filter Generator（生成过滤器）*对话框打开。

   b. 点击 *Add Filter（添加过滤器）*，然后选择一个过滤器。

选择过滤器后，将出现实例的过滤列表。

   c. 点击 *OK（确定）*。

*Import SDN Connector（导入 SDN 连接器）*对话框打开，其中包含了过滤器。您可以添加更多过滤器，也可以编辑和删除过滤器。

   d. （可选）重复此操作过程，添加其他过滤器。

5. 选择过滤器，然后点击 *Import（导入）*。

地址名称将被导入并转换为动态防火墙地址对象，该对象将显示在 *Firewall Objects > Addresses（防火墙对象 > 地址）*窗口中。动态防火墙地址的名称使用以下命名规则：AWS 平台 - <随机标识符>。使用 *Details（详细信息）*列和实例 ID 来标识对象。

创建 IP 地址策略

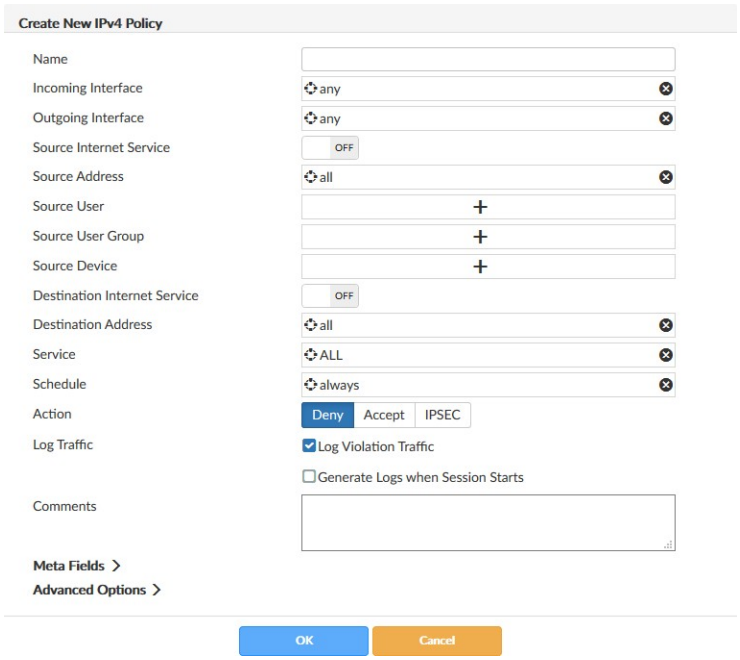
本部分将介绍如何创建新的 IPv4 和 IPv6 策略。

IPv6 安全策略是为 IPv6 网络和过渡网络创建的。过渡网络是指正在过渡转换到 IPv6 的网络，但必须仍然能够访问 Internet 或者必须能够通过 IPv4 网络进行连接。IPv6 策略允许这种特定类型的流量在 IPv6 和 IPv4 网络之间传输。

在 Policy & Objects（策略和对象）选项卡的 *Tools（工具）*菜单中选择 Display Options（显示选项）。在 *Policy（策略）*部分，选择 *IPv6 Policy（IPv6 策略）*复选框，以显示此选项。

新的 IPv4 或 IPv6 策略创建过程如下：

1. 确保您使用的是正确的 ADOM 管理域。
2. 前往 *Policy & Objects > Policy Packages（策略和对象 > 策略包）*。
3. 在树单中的策略包中创建新策略，选择 IPv4 Policy（IPv4 策略）或 *IPv6 Policy（IPv6 策略）*。如果您使用的是全局数据库 ADOM 管理域，请选择 *IPv4 Header Policy（IPv4 页眉策略）*、*IPv4 Footer Policy（IPv4 页脚策略）*或 *IPv6 Footer Policy（IPv6 页脚策略）*。
4. 点击 *Create New（新建）*，或者在 *Create New（新建）*菜单中选择 *Insert Above（在上方插入）* 或者 *Insert Below（在下方插入）*。策略将默认添加到列表底部，但在隐式策略之上。*Create New Policy（创建新策略）*窗口打开。



5. 填写选项。
6. 点击 *OK（确定）*，创建策略。

您可以在右键菜单中选择启用或禁用该策略。禁用该策略时，数字左侧的 *Seq.#（序列号）*一栏中将显示禁用图标。

安装策略包

安装策略包时，策略引用的对象被安装调用到目标设备。默认映射或按设备映射必须存在，否则安装将失败。

部分未在策略中直接引用的对象也需要安装到目标设备，例如 FSSO 轮询对象、地址和配置文件组以及 CA 证书。

将策略包安装到目标设备：

1. 确保您使用的是包含策略包的 ADOM 管理域。
2. 前往 *Policy & Objects* > *Policy Packages（策略和对象* > *策略包）*。
3. 选择一个策略包，然后从 *Install（安装）*菜单或右键菜单中选择 *Install Wizard（安装向导）*。*Install Wizard（安装向导）*打开。
4. 请按照安装向导中的步骤安装策略包。您可以选择安装策略包和设备设置，也可以选择仅安装接口策略。

变更日志

日期	变更说明
2019 年 10 月 3 日	首次发布。
2019 年 10 月 16 日	更新了在 AWS 平台上部署 FortiManager（见第 10 页）。
2019 年 10 月 22 日	更新了初始部署。