

NSX for vShield Endpoint 升级指南

Update 5

修改日期：2017 年 11 月 20 日

VMware NSX Data Center for vSphere 6.2



vmware®

您可以从 VMware 网站下载最新的技术文档：

<https://docs.vmware.com/cn/>。

VMware 网站还提供了最近的产品更新。

如果您对本文档有任何意见或建议，请将反馈信息发送至：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

目录

- 1 NSX for vShield Endpoint 升级指南 4**
 - [阅读支持文档 5](#)
 - [NSX for vShield Endpoint 系统要求 5](#)
 - [NSX 所需的端口和协议 6](#)

- 2 vCloud Networking and Security 到 NSX 升级 9**
 - [准备 vCloud Networking and Security 到 NSX for vShield Endpoint 升级 9](#)
 - [从 vCloud Networking and Security 5.5.x 升级到 NSX 6.2.x for vShield Endpoint 16](#)

- 3 在 NSX for vShield Endpoint 中使用合作伙伴服务 24**
 - [在 NSX for vShield Endpoint 中升级合作伙伴服务 24](#)
 - [部署合作伙伴服务 24](#)
 - [在 NSX for vShield Endpoint 中使用服务编排 25](#)

NSX for vShield Endpoint 升级指南

1

本手册（《NSX for vShield Endpoint 升级指南》）介绍了如何使用 vSphere Web Client 升级 VMware® NSX™ 系统。此信息包括分步升级说明以及建议的最佳做法。

目标读者

本手册专供使用 vCloud Networking and Security 以仅提供 Endpoint 功能，以及升级到 NSX 以部署和管理 vShield Endpoint 以仅提供防病毒卸载功能的用户使用。本手册的目标读者为熟悉虚拟机技术和虚拟数据中心操作且经验丰富的系统管理员。本手册假定您熟悉 VMware vSphere 5.5 或 6.0，包括 VMware ESXi、vCenter Server 和 vSphere Web Client。

如果需要使用 NSX 的任何其他功能（包括逻辑交换机、逻辑路由器、Distributed Firewall 或 NSX Edge），请参见 NSX 升级指南。

VMware 技术出版物词汇表

VMware 技术出版物提供了一个词汇表，其中包含一些您可能不熟悉的术语。有关 VMware 技术文档中使用的术语的定义，请访问 <http://www.vmware.com/support/pubs>。

本章讨论了以下主题：

- [阅读支持文档](#)
- [NSX for vShield Endpoint 系统要求](#)
- [NSX 所需的端口和协议](#)

阅读支持文档

除了本升级指南之外，VMware 还发布了其他多本提供升级过程支持的文档。

发行说明

在开始升级之前，请查看发行说明。NSX 发行说明中介绍了已知升级问题和解决办法。在开始升级过程之前阅读升级问题可节省时间和精力。请参阅 <https://docs.vmware.com/cn/VMware-NSX-for-vSphere/index.html>。

产品互操作性列表

验证与其他 VMware 产品的互操作性，例如，vCenter。请参见 VMware 产品互操作性列表 (http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php) 中的互操作性 (Interoperability) 选项卡。

验证是否支持从当前 NSX 版本到目标版本的升级途径。在升级途径 (Upgrade Path) 选项卡中，从产品菜单中选择 VMware NSX。

兼容性指南

验证合作伙伴解决方案与 NSX 的兼容性，请参见《VMware 兼容性指南》，网址为 <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>。

NSX for vShield Endpoint 系统要求

在安装或升级 NSX 之前，请考虑您的网络配置和资源。您可以在每个 vCenter Server 中安装一个 NSX Manager，在每个 ESXi™ 主机上安装一个 Guest Introspection 实例，并在每个数据中心安装多个 NSX Edge 实例。

硬件

表 1-1. 硬件要求

| 设备 | 内存 | vCPU | 磁盘空间 |
|---------------------|-----------------------------|---------------------|-------|
| NSX Manager | 16 GB (某些 NSX 部署规模为 24 GB*) | 4 (某些 NSX 部署规模为 8*) | 60 GB |
| Guest Introspection | 1 GB | 2 | 4 GB |

作为一般准则，如果您的 NSX 受管环境包含超过 256 个管理程序或 2000 个虚拟机，您应该将 NSX Manager 资源增加到 8 个 vCPU 和 24 GB RAM。

有关特定规模的详细信息，请联系 VMware 支持人员。

有关为虚拟设备增加内存和 vCPU 分配的信息，请参见《vSphere 虚拟机管理》中的“分配内存资源”和“更改虚拟 CPU 数目”。

软件

下面是建议的 VMware 产品版本。

- VMware vCenter Server 5.5U3
- VMware vCenter Server 6.0U2

客户端和用户访问权限

- 如果按名称将 ESXi 主机添加到 vSphere 清单中，请确保正向和反向名称解析正常工作。否则，NSX Manager 将无法解析 IP 地址。
- 添加和打开虚拟机电源的权限
- 访问存储虚拟机文件的数据存储的权限，以及将文件复制到该数据存储的帐户权限
- 在 Web 浏览器中启用 cookie 以访问 NSX Manager 用户界面
- 从 NSX Manager 中，确保可以从要部署的 ESXi 主机、vCenter Server 和 NSX 设备中访问端口 443。需要使用该端口在 ESXi 主机上下载 OVF 文件以进行部署。
- 使用的 vSphere Web Client 版本支持的 Web 浏览器。请参见《vCenter Server 和主机管理》文档中的“使用 vSphere Web Client”以了解详细信息。

NSX 所需的端口和协议

以下端口必须处于打开状态才能使 NSX 正常工作。

表 1-2. NSX 所需的端口和协议

| 源 | 目标 | 端口 | 协议 | 用途 | 敏感 | TLS | 身份验证 |
|----------------|----------------|----------------|-----|--------------------|----|-----|----------------|
| 客户端 PC | NSX Manager | 443 | TCP | NSX Manager 管理接口 | 否 | 是 | PAM 身份验证 |
| 客户端 PC | NSX Manager | 80 | TCP | NSX Manager VIB 访问 | 否 | 否 | PAM 身份验证 |
| ESXi 主机 | vCenter Server | 443 | TCP | ESXi 主机准备 | 否 | 否 | |
| vCenter Server | ESXi 主机 | 443 | TCP | ESXi 主机准备 | 否 | 否 | |
| ESXi 主机 | NSX Manager | 5671 | TCP | RabbitMQ | 否 | 是 | RabbitMQ 用户/密码 |
| ESXi 主机 | NSX Controller | 1234 | TCP | 用户方代理连接 | 否 | 是 | |
| NSX Controller | NSX Controller | 2878、2888、3888 | TCP | 控制器群集 - 状态同步 | 否 | 是 | IPsec |
| NSX Controller | NSX Controller | 7777 | TCP | 内部控制器 RPC 端口 | 否 | 是 | IPsec |
| NSX Controller | NSX Controller | 30865 | TCP | 控制器群集 - 状态同步 | 否 | 是 | IPsec |

表 1-2. NSX 所需的端口和协议（续）

| 源 | 目标 | 端口 | 协议 | 用途 | 敏感 | TLS | 身份验证 |
|-------------------------|-------------------|--|-----|----------------------|----|-----|----------------|
| NSX Manager | NSX Controller | 443 | TCP | 控制器与 Manager 通信 | 否 | 是 | 用户/密码 |
| NSX Manager | vCenter Server | 443 | TCP | vSphere Web Access | 否 | 是 | |
| NSX Manager | vCenter Server | 902 | TCP | vSphere Web Access | 否 | 是 | |
| NSX Manager | ESXi 主机 | 443 | TCP | 管理和置备连接 | 否 | 是 | |
| NSX Manager | ESXi 主机 | 902 | TCP | 管理和置备连接 | 否 | 是 | |
| NSX Manager | DNS 服务器 | 53 | TCP | DNS 客户端连接 | 否 | 否 | |
| NSX Manager | DNS 服务器 | 53 | UDP | DNS 客户端连接 | 否 | 否 | |
| NSX Manager | Syslog 服务器 | 514 | TCP | Syslog 连接 | 否 | 否 | |
| NSX Manager | Syslog 服务器 | 514 | UDP | Syslog 连接 | 否 | 否 | |
| NSX Manager | NTP Time Server | 123 | TCP | NTP 客户端连接 | 否 | 是 | |
| NSX Manager | NTP Time Server | 123 | UDP | NTP 客户端连接 | 否 | 是 | |
| vCenter Server | NSX Manager | 80 | TCP | 主机准备 | 否 | 是 | |
| REST 客户端 | NSX Manager | 443 | TCP | NSX Manager REST API | 否 | 是 | 用户/密码 |
| VXLAN 隧道端点 (VTEP) | VXLAN 隧道端点 (VTEP) | 8472 (NSX 6.2.3 之前的默认值) 或 4789 (新安装的 NSX 6.2.3 及更高版本中的默认值) | UDP | VTEP 之间的传输网络封装 | 否 | 是 | |
| ESXi 主机 | ESXi 主机 | 6999 | UDP | 防止 VLAN LIF 上的 ARP | 否 | 是 | |
| ESXi 主机 | NSX Manager | 8301、8302 | UDP | DVS 同步 | 否 | 是 | |
| NSX Manager | ESXi 主机 | 8301、8302 | UDP | DVS 同步 | 否 | 是 | |
| Guest Introspection 虚拟机 | NSX Manager | 5671 | TCP | RabbitMQ | 否 | 是 | RabbitMQ 用户/密码 |

表 1-2. NSX 所需的端口和协议（续）

| 源 | 目标 | 端口 | 协议 | 用途 | 敏感 | TLS | 身份验证 |
|----------------|----------------|------|-----|-------------------------|----|-----|----------------|
| 主 NSX Manager | 辅助 NSX Manager | 443 | TCP | 跨 vCenter NSX 通用同步服务 | 否 | 是 | |
| 主 NSX Manager | vCenter Server | 443 | TCP | vSphere API | 否 | 是 | |
| 辅助 NSX Manager | vCenter Server | 443 | TCP | vSphere API | 否 | 是 | |
| 主 NSX Manager | NSX 通用控制器群集 | 443 | TCP | NSX Controller REST API | 否 | 是 | 用户/密码 |
| 辅助 NSX Manager | NSX 通用控制器群集 | 443 | TCP | NSX Controller REST API | 否 | 是 | 用户/密码 |
| ESXi 主机 | NSX 通用控制器群集 | 1234 | TCP | NSX 控制层面协议 | 否 | 是 | |
| ESXi 主机 | 主 NSX Manager | 5671 | TCP | RabbitMQ | 否 | 是 | RabbitMQ 用户/密码 |
| ESXi 主机 | 辅助 NSX Manager | 5671 | TCP | RabbitMQ | 否 | 是 | RabbitMQ 用户/密码 |

跨 vCenter NSX 和增强型链接模式的端口

如果您有一个跨 vCenter NSX 环境，并且 vCenter Server 系统处于增强型链接模式，则要从任何 vCenter Server 系统中管理任何 NSX Manager，每个 NSX Manager 设备必须具有到该环境中每个 vCenter Server 系统的所需连接。

vCloud Networking and Security 到 NSX 升级

2

本章讨论了以下主题：

- 准备 vCloud Networking and Security 到 NSX for vShield Endpoint 升级
- 从 vCloud Networking and Security 5.5.x 升级到 NSX 6.2.x for vShield Endpoint

准备 vCloud Networking and Security 到 NSX for vShield Endpoint 升级

为确保 NSX 升级成功，请务必查看发行说明以了解升级问题，确保使用正确的升级顺序，以及确保基础架构为升级工作做好了恰当准备。以下准则可用作升级前对照表。



小心 不支持降级：

- 请务必先备份 NSX Manager，然后再执行升级。
- 成功升级 NSX Manager 后，无法对 NSX 进行降级。

VMware 建议在您的公司定义的维护期限内完成升级工作。

以下准则可用作升级前对照表。

- 1 验证 vCloud Networking and Security 是否为 5.5 版。如果不是，请参见《vShield 安装和升级指南》5.5 版以了解升级说明。
- 2 验证是否打开了所需的所有端口。请参见 [NSX 所需的端口和协议](#)。
- 3 验证 vCenter 是否满足 NSX 6.2.x 系统要求。请参见 [NSX for vShield Endpoint 系统要求](#)。
- 4 验证是否可以检索 vSphere Distributed Switch 的上行链路端口名称信息。请参见 <https://kb.vmware.com/kb/2129200>。
- 5 如果部署了任何 vShield Endpoint 合作伙伴服务，请在升级之前验证兼容性：
 - 在大多数情况下，可以将 vCloud Networking and Security 升级到 NSX 而不影响合作伙伴解决方案。但是，如果您的合作伙伴解决方案与要升级到的 NSX 版本不兼容，则在升级到 NSX 之前，您需要将合作伙伴解决方案升级到兼容版本。
 - 请参阅《VMware Networking and Security 兼容性指南》。请参见 <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>。

- 请参阅合作伙伴文档以了解兼容性和升级详细信息。
- 6 如果在环境中安装了数据安全，请在升级 vShield Manager 之前将其卸载。请参见[卸载 vShield Data Security](#)。
- 7 如果将 Cisco Nexus 1000V 作为外部交换机提供程序，您必须在升级到 NSX 之前将这些网络迁移到 vSphere Distributed Switch。在安装 NSX 后，您可以将 vSphere Distributed Switch 迁移到逻辑交换机。
- 8 验证您是否具有 vShield Manager、vCenter 和其他 vCloud Networking and Security 组件的最新备份。请参见[vCloud Networking and Security 备份和还原](#)。
- 9 创建一个技术支持包。
- 10 使用 nslookup 命令确保正向和反向域名解析正常工作。
- 11 如果正在环境中使用 VUM，请确保在 vCenter 中将 bypassVumEnabled 标记设置为 true。该设置配置 EAM 以将 VIB 直接安装到 ESXi 主机中，即使安装了 VUM 以及/或者 VUM 不可用。请参见<http://kb.vmware.com/kb/2053782>。
- 12 下载并暂存升级包，并使用 md5sum 进行验证。请参见[下载 vShield Manager 到 NSX 升级包并检查 MD5](#)。
- 13 最佳做法是，保持环境中的所有操作为静默模式，直到完成了升级的所有部分。
- 14 不要关闭或删除任何 vCloud Networking and Security 组件或设备，除非要求这样做。

vShield Endpoint 升级对运行产生的影响

vCloud Networking and Security 升级过程可能需要一些时间。您必须了解 vCloud Networking and Security 组件在升级过程中的运行状况。

要将 vCloud Networking and Security 升级到 NSX 6.2，您必须按以下顺序升级 NSX 组件：

- vShield Manager
- vShield Endpoint

VMware 建议在单个中断时段内运行升级，以尽可能缩短停机时间并避免由于某些 vCloud Networking and Security 管理功能在升级过程中无法访问而给 vCloud Networking and Security 用户带来混乱。但是，如果您的站点要求导致无法在单个中断时段内完成升级，以下信息可帮助 vCloud Networking and Security 用户了解哪些功能在升级过程中可用。

vCenter 升级

如果您正在使用 vCenter 嵌入式 SSO 并且想要将 vCenter 5.5 升级到 vCenter 6.0，则 vCenter 可能会断开与 vShield Manager 的连接。如果您已使用 root 用户名向 vShield 注册 vCenter 5.5，则会出现这种情况。从 NSX 6.2 开始，使用 root 进行 vCenter 注册的做法已弃用。要解决此问题，请使用 administrator@vsphere.local 用户名重新向 vShield 注册 vCenter，而不要使用 root。

如果您正在使用外部 SSO，则不需要进行任何更改。您可以保留相同的用户名（例如 admin@mybusiness.mydomain），而且 vCenter 不会断开连接。

vShield Manager 升级

升级过程中：

- vShield Manager 配置受到阻止。vShield API 服务不可用。您不能对 vShield 配置进行任何更改。现有虚拟机通信将继续工作。

升级后：

- 您可以进行所有 vShield 和 NSX 配置更改。

vShield Endpoint 迁移到 Guest Introspection

在 NSX 6.x 中，vShield Endpoint 重命名为 Guest Introspection。在升级 NSX Manager 后，如果导航到**网络和安全 > 安装 > 服务部署**，Guest Introspection 服务将显示**升级**链接。从 vCloud Networking and Security 升级到 NSX 时，将在启用 Guest Introspection 的群集中的每个主机上部署 Guest Introspection 虚拟设备和 Guest Introspection 主机代理。

升级过程中：

- 在虚拟机发生变化（如添加虚拟机、执行 vMotion 或删除虚拟机）时，NSX 群集中的虚拟机将失去保护。

升级后：

- 在添加虚拟机、执行 vMotion 或删除虚拟机期间，将保护虚拟机。

验证 vShield Endpoint 工作状态

开始升级之前，请务必测试 vCloud Networking and Security 工作状态。否则，一旦升级后出现问题，您将无法确定这些问题是由升级过程导致的还是在升级过程之前便已经存在。

开始升级 vCloud Networking and Security 基础架构之前，请勿假定一切正常。请务必先进行检查。

您可以将以下过程作为升级前检查表。

步骤

- 1 确定管理用户 ID 和密码。
- 2 验证所有组件的正向和反向名称解析是否正常工作。
- 3 验证您是否可以登录到所有 vSphere 和 vShield 组件。
- 4 记下 vShield Manager、vCenter Server 和 ESXi 的当前版本。
- 5 目视检查 vShield 环境，确保所有状态指示灯均显示为绿色、正常或已部署。
- 6 验证是否已配置 syslog。
- 7 验证合作伙伴解决方案是否正常工作。

例如，您可以使用 EICAR Standard Anti-Virus Test File 测试防病毒功能：

<http://www.eicar.org/86-0-Intended-use.html>。

- 8 （可选）如果拥有测试环境，请在升级生产环境之前测试升级和升级后功能。

将本地管理员用户迁移到 CLI 管理员用户

在 NSX 6.x 系列之前，用户管理员是本地数据库用户。自 NSX 6.0 起，用户管理员已成为 CLI 用户。为实现向后兼容性，您可以采取一些步骤来迁移管理员用户。

对于 vCloud Networking and Security 5.x 系列，CLI 中的管理员用户和 UI (VSM) 中的管理员用户是两个不同的用户。CLI 管理员用户的密码由操作系统管理，而 VSM 用户的密码由用户的本地数据库管理。更改 CLI 管理员用户的密码时，该更改不会影响 VSM 管理员用户的密码。同样，更改 VSM 管理员用户的密码时，该更改也不会影响 CLI 管理员用户的密码。

对于 NSX 6.x 系列，VSM 用户数据库已弃用。CLI 用户可以直接登录到 NSX Manager。

在升级方案中，为实现向后兼容性，管理员用户同时存在于 CLI 数据库和 Web UI 数据库中。在这种情况下，如果 CLI 用户的密码已更改，该更改不会反映在 UI 或 REST API 调用中。在 NSX 6.x 系列之前，CLI 用户无法登录到 UI 或 REST API。

在 NSX 6.x 系列的全新（首次）部署中，CLI 用户和 NSX Manager（UI 或 REST）是相同的，并且凭据也相同。

如果希望升级后的 NSX 部署像 NSX 6.x 的全新部署一样工作，您有以下两个选项可选择。

- 选项 1 - 更改管理员数据库用户的密码。

您可以使用以下 REST API 更改密码。此选项要求您知道旧密码。

PUT URI /api/2.0/services/usermgmt/user/local/<userId>

```
<userInfo>
  <userId></userId>
  <password></password>
  <fullname></fullname>
  <email></email>
  <accessControlEntry>
    <role></role>
    <resource>
      <resourceId></resourceId>
      ...
    </resource>
  </accessControlEntry>
</userInfo>
```

例如，使用 curl:

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X PUT
https://<vsm-ip>/api/2.0/services/usermgmt/user/local/admin -d
'<userInfo><userId>admin</userId><password>123</password><fullname>admin</fullname><email>admin@com
pany.com</email><accessControlEntry><role>security_admin</role><resource><resourceId>datacenter-312
</resourceId></resource></accessControlEntry></userInfo>'
```

该 API 可用于更新本地用户帐户和密码。如果未提供密码，则保留现有密码。URI 中的 userId 变量应与 XML 中指定的用户 ID 相同。

- 选项 2 - 移除 Web UI 管理员用户并向 CLI 管理员用户添加一个角色。完成此更改后，您可以使用 CLI 用户凭据登录到 NSX Manager，而且对 CLI 管理员用户进行的密码更改会反映在 NSX Manager 管理员用户上。

由于 Web UI 管理员用户是 `super_user`，因此您需要先添加另一个具有 `super_user` 特权的用户才能删除 Web UI 管理员用户。

- 添加具有 `super_user` 角色的新用户 `tempadmin`。

例如，使用 `curl`：

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X PUT
https://<vsm-ip>/api/2.0/services/usermgmt/user/local/admin -d
'<userInfo><userId>tempadmin</userId><password>123</password><fullname>tempadmin</fullname><email>tempadmin@company.com</email><accessControlEntry><role>super_user</role><resource><resourceId>datacenter-312</resourceId></resource></accessControlEntry></userInfo>'
```

- 使用 `tempadmin` 删除 Web UI 管理员用户。

例如，使用 `curl`：

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X
DELETE https://<vsm-ip>/api/2.0/services/usermgmt/user/admin
```

- 向 CLI 管理员用户添加 `super_user` 角色。

例如，使用 `curl`：

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X
POST https://<nsx-ip>/api/2.0/services/usermgmt/role/admin?isCli=true -d
'<accessControlEntry><role>super_user</role></accessControlEntry>'
```

卸载 vShield Data Security

如果在环境中安装了 Data Security，请在升级到 NSX 之前将其卸载。

从 NSX 6.2.3 开始，NSX 数据安全功能将被弃用。在 NSX 6.2.3 中，您可以自行决定继续使用该功能，但要注意，在将来的 NSX 版本中将移除该功能。

步骤

- 1 从 vShield Manager 5.5 清单面板中，展开 **数据中心 (Datacenters)** 文件夹，然后导航到安装了 vShield Data Security 的主机。
- 2 在安装了 vShield Data Security 的每个主机上，完成以下步骤以将其卸载。
 - a 单击该主机，然后在“vShield 主机准备”窗格的 **摘要 (Summary)** 选项卡中单击 vShield Data Security 的 **卸载 (Uninstall)** 链接。
 - b 在“选择要卸载的服务”窗格中，确认选择了 vShield Data Security，然后单击 **卸载 (Uninstall)** 按钮。

将卸载 vShield Data Security，并且“vShield 主机准备”窗格将状态显示为未安装。

vCloud Networking and Security 备份和还原

要在出现故障时将系统还原到工作状态，就必须正确备份所有 vCloud Networking and Security 组件，这点至关重要。

vShield Manager 备份包含所有 vShield 配置，包括虚拟线路和路由实体、安全性、vApp 规则以及在 vShield Manager UI 或 API 中配置的任何其他内容。需要单独备份 vCenter 数据库和相关的元素（如虚拟交换机）。

建议至少定期备份 vShield Manager 和 vCenter。备份频率和计划可能因业务需求和运行流程而异。建议在配置频繁更改时经常执行 vCloud Networking and Security 备份。

vShield Manager 备份可以按需执行，也可以按每小时、每日或每周的频率执行。

建议在以下情况下执行备份：

- 在 vCloud Networking and Security 或 vCenter 升级之前。
- 在 vCloud Networking and Security 或 vCenter 升级之后。
- 在执行 vCloud Networking and Security 组件零日部署和初始配置后，例如，在创建虚拟交换机、Edge、安全性和防火墙策略后。
- 基础架构或拓扑更改之后。
- 执行重大第 2 日更改之后。

要将整个系统回滚到指定时间的状态，建议将 vCloud Networking and Security 组件备份与其他交互组件（如 vCenter、云管理系统和运行工具等）的备份计划保持同步。

按需备份 vShield Manager 数据

您可以随时执行按需备份以备份 vShield Manager 数据。

步骤

- 1 从 vShield Manager 清单面板中，单击**设置和报告 (Settings & Reports)**。
- 2 单击**配置 (Configuration)**选项卡。
- 3 单击**备份 (Backups)**。
- 4 （可选）如果不希望备份系统事件表，请选中**排除系统事件 (Exclude System Events)**复选框。
- 5 （可选）如果不希望备份审核日志表，请选中**排除审核日志 (Exclude Audit Logs)**复选框。
- 6 键入保存备份的系统的主机 IP 地址 (**Host IP Address**)。
- 7 键入备份系统的主机名称 (**Host Name**)。
- 8 键入登录到备份系统所需的用户名 (**User Name**)。
- 9 键入与备份系统的用户名关联的密码 (**Password**)。
- 10 在**备份目录 (Backup Directory)**字段中，键入存储备份的绝对路径。

11 在文件名前缀 (Filename Prefix) 中键入一个文本字符串。

此文本将被预置到备份文件名中，以便在备份系统中识别这些备份文件。例如，如果键入 **ppdb**，则生成的备份的名称为 **ppdbHH_MM_SS_DayDDMonYYYY**。

12 输入密码短语 (Pass Phrase) 以确保备份文件安全。

在 vCloud Networking and Security 中，密码短语是可选的。在 NSX 中，密码短语是必需的。

13 从传输协议 (Transfer Protocol) 下拉菜单中，选择 SFTP 或 FTP。**14 单击备份 (Backup)。**

在完成后，备份将显示在该表单下方的表中。

15 单击保存设置 (Save Settings) 以保存配置。

请注意，如果所有备份保存在单个目录中，您可能在查看备份时遇到问题。最佳做法是，时常将备份文件移动到存档文件夹中。

备份 vSphere Distributed Switch

可以将 vSphere Distributed Switch 和分布式端口组配置导出到文件。

该文件保留有效的网络配置，使这些配置能够分发到其他部署。

该功能仅在 vSphere Web Client 5.1 或更高版本中可用。VDS 设置和端口组设置将作为导入内容的一部分进行导入。

最佳做法是在针对 VXLAN 为群集做好准备之前导出 VDS 配置。有关详细说明，请参见 <http://kb.vmware.com/kb/2034602>。

备份 vCenter

为保护 NSX 部署，请务必备份 vCenter 数据库并生成虚拟机快照。

请参考您使用的 vCenter 版本对应的 vCenter 文档，了解 vCenter 备份和还原步骤以及最佳做法。

有关虚拟机快照，请参见 <http://kb.vmware.com/kb/1015180>。

与 vCenter 5.5 有关的有用链接：

- <http://kb.vmware.com/kb/2057353>
- <http://kb.vmware.com/kb/2034505>
- <http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf>

与 vCenter 6.0 有关的有用链接：

- <https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html>
- <http://kb.vmware.com/kb/2110294>

下载 vShield Manager 到 NSX 升级包并检查 MD5

vShield Manager 到 NSX 升级包含有升级 NSX 基础架构所需的所有文件。在升级 vShield Manager 之前，您需要先下载适用于要升级到的版本的升级包。

前提条件

一个 MD5 校验和工具。

步骤

- 1 将 vShield Manager 到 NSX 升级包下载到 vShield Manager 可浏览到的位置。升级包文件名称具有类似于 `VMware-vShield-Manager-upgrade-bundle-to-NSX-releaseNumber-NSXbuildNumber.tar.gz` 的格式。

- 2 验证升级文件名是否以 `tar.gz` 结尾。

部分浏览器可能会更改文件扩展名。例如，如果下载文件的名称是：

`VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.gz`

则将其更改为：

`VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.tar.gz`

否则，在上载升级包后，将显示以下错误消息：“升级包文件 `VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.gz` 无效，升级文件名称的扩展名应为 `tar.gz`”。

- 3 使用 MD5 校验和工具将 VMware 网站上显示的升级包官方 MD5 校验和与该校验和工具计算而得的 MD5 校验和相比较。

a 在 MD5 校验和工具中，浏览到该升级包。

b 使用该工具计算升级包的校验和。

c 粘贴 VMware 网站上列出的校验和。

d 使用该工具比较两个校验和。

如果两个校验和不匹配，请重复升级包下载过程。

从 vCloud Networking and Security 5.5.x 升级到 NSX 6.2.x for vShield Endpoint

要升级到 NSX 6.2.x，您必须按照本指南中介绍的顺序升级 vCloud Networking and Security 组件。

必须按以下顺序升级 vCloud Networking and Security 组件：

- 1 vShield Manager 到 NSX Manager
- 2 vShield Endpoint 到 NSX Guest Introspection

在 vShield Endpoint 中将 vShield Manager 升级到 NSX Manager

NSX 基础架构升级过程的第一步是升级 NSX Manager 设备。



小心 请不要卸载已部署的 vShield Manager 设备实例。

前提条件

- 确认您已完成准备 [vCloud Networking and Security](#) 到 [NSX for vShield Endpoint](#) 升级中所述的所有升级准备任务。
- 确认 vShield Manager 具有足够的磁盘空间以升级到 NSX Manager。请参见 [NSX for vShield Endpoint 系统要求](#)。
- 在升级到 NSX 6.2.x 之前，将 vShield Manager 虚拟设备的预留内存增加到至少 16 GB 并分配 4 个 vCPU。

请参见 [NSX for vShield Endpoint 系统要求](#)。

步骤

- 1 将 NSX 升级包下载到 vShield Manager 可以浏览到的位置。升级包文件的名称类似于 `VMware-vShield-Manager-upgrade-bundle-to-NSX-release-buildNumber.tar.gz`。
- 2 从 vShield Manager 5.5 清单面板中，单击 **设置和报告**。
- 3 单击 **更新** 选项卡，然后单击 **上载升级包**。
- 4 单击 **选择文件**，选择 `VMware-vShield-Manager-upgrade-bundle-to-NSX-release-buildNumber.tar.gz` 文件，然后单击 **打开**。
- 5 单击 **上载文件**。
上载文件需要几分钟时间。
- 6 单击 **安装** 以开始升级过程。
- 7 单击 **确认安装**。升级过程将重新引导 vShield Manager，因此您可能会失去与 vShield Manager 用户界面的连接。不会重新引导其他任何 vShield 组件。
- 8 在重新引导后，打开 Web 浏览器窗口并键入 IP 地址以登录到 NSX Manager 虚拟设备，例如，`https://10.10.10.10`。升级的 NSX Manager 具有与 vShield Manager 相同的 IP 地址。
“摘要”选项卡将显示刚安装的 NSX Manager 的版本。
- 9 导航到 **主页 > 管理 vCenter 注册**，并确认 vCenter Server 状态为已连接。
- 10 关闭任何正在访问 vSphere Web Client 的现存浏览器会话。等待几分钟，清除浏览器缓存，然后重新登录到 vSphere Web Client。
- 11 如果已在 vShield Manager 上启用 SSH，则升级后必须也在 NSX Manager 上启用 SSH。登录到 NSX Manager 虚拟设备，然后单击 **查看摘要**。在系统级别组件中，为 SSH 服务单击 **开始**。

重要 从 vCloud Networking and Security 5.x 升级到 NSX 6.x 后，您必须使用 CLI 管理登录凭据登录到 NSX Manager。以前，在 vCloud Networking and Security 中需要使用两个密码，一个用于 CLI，另一个用于 UI。从 NSX 6.x 开始，只需要使用一个密码。例如：

vCloud Networking and Security 中的密码

- mypassword#123 用于 CLI
- mypassword#456 用于 UI

升级到 NSX 后的密码

- mypassword#123 用于 CLI
- mypassword#123 用于 UI

在升级 NSX Manager 后，您必须注销并重新登录到 vSphere Web Client。

如果在 vSphere Web Client 中未正确显示 NSX 插件，请清除浏览器的缓存和历史记录。如果未执行此步骤，则当您在 vSphere Web Client 中对 NSX 配置进行更改时，可能会看到类似以下内容的错误：“出现内部错误 - 错误 #1009 (An internal error has occurred - Error #1009)”。

如果在 vSphere Web Client 中不显示“网络和安全”选项卡，请重置 vSphere Web Client 服务器：

- 在 vCenter 5.5 中，打开 <https://<vcenter-ip>:5480>，然后重新启动 Web Client 服务器。
- 在 vCenter Server Appliance 6.0 中，以 root 用户身份登录到 vCenter Server shell，然后运行以下命令：

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- 在 Windows 上的 vCenter Server 6.0 中，您可以通过运行以下命令来执行该操作。

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

建议使用不同的 Web Client 管理运行不同 NSX Manager 版本的 vCenter Server，以避免运行不同版本的 NSX 插件时发生意外错误。

后续步骤

创建 NSX Manager 的备份。以前的 NSX Manager 备份仅对先前版本有效。请参见[为 vShield Endpoint 备份 NSX Manager 数据](#)。

为 vShield Endpoint 备份 NSX Manager 数据

您可以通过执行按需备份或调度备份来备份 NSX Manager 数据。

您可以通过 NSX Manager 虚拟设备 Web 界面或 NSX Manager API 配置 NSX Manager 备份和还原。备份频率可以调度为每小时、每日或每周。

备份文件保存到 **NSX Manager** 可访问的远程 **FTP** 或 **SFTP** 位置。**NSX Manager** 数据包括配置表、事件表和审核日志表。配置表包含在每个备份中。

仅支持在版本与备份版本相同的 **NSX Manager** 上执行还原。因此，请务必在执行 **NSX** 升级前后创建新的备份文件，即一个备份用于旧版本，另一个用于新版本。

步骤

- 1 登录到 **NSX Manager** 虚拟设备。
- 2 在“设备管理”下方，单击**备份和还原**。
- 3 要指定备份位置，请单击“FTP 服务器设置”旁边的**更改**。
 - a 键入备份系统的 IP 地址或主机名。
 - b 根据目标支持的内容，从**传输协议**下拉菜单中选择 **SFTP** 或 **FTP**。
 - c 根据需要编辑默认端口。
 - d 键入登录到备份系统所需的用户名和密码。
 - e 在**备份目录**字段中，键入用于存储备份的绝对路径。

要确定绝对路径，您可以登录到 **FTP** 服务器，导航到要使用的目录，然后运行 **present working directory** 命令 (**pwd**)。例如：

```
PS C:\Users\Administrator> ftp 192.168.110.60
Connected to 192.168.110.60.
220 server-nfs FTP server ready.
User (192.168.110.60:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> ls
200 PORT command successful.
150 Opening BINARY mode data connection for 'file list'.
datastore-01
226 Transfer complete.
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> cd datastore-01
250 CWD command successful.
ftp> pwd
257 "/datastore-01" is current directory.
```

- f 在**文件名前缀**中键入一个文本字符串。

此文本将被预置到每个备份文件名中，以便在备份系统中识别这些备份文件。例如，如果键入 **ppdb**，则生成的备份的名称为 **ppdbHH_MM_SS_DayDDMonYYYY**。

g 键入密码短语以确保备份安全。

您需要此密码才能还原备份。

h 单击**确定**。

例如：

4 对于按需备份，请单击**备份**。

新文件将添加到**备份历史记录**下。

5 对于调度备份，请单击“调度”旁边的**更改**。

a 从**备份频率**下拉菜单中，选择**按小时**、**按天**或**按周**。系统将根据所选的频率禁用“一周中的某天”、“每日时间”和“分钟”下拉菜单。例如，如果您选择“按天”，则将禁用“一周中的某天”下拉菜单，因为此字段不适用于每天频率。

b 对于按周备份，选择应该在一周中的哪一天备份数据。

c 对于按周备份或按天备份，选择开始备份的小时。

d 选择开始备份的分钟，然后单击**调度**。

6 要从备份中排除日志和流量数据，请单击“排除”旁边的**更改**。

a 选择要从备份中排除的项目。

b 单击**确定**。

7 保存 FTP 服务器的 IP/主机名、凭据、目录详细信息和密码。您需要此信息才能还原备份。

后续步骤

升级 vShield Endpoint。请参见在 [NSX for vShield Endpoint](#) 中升级到 [Guest Introspection](#)。

在 NSX for vShield Endpoint 中升级到 Guest Introspection

请务必升级 Guest Introspection 以便与 NSX Manager 版本相匹配。

注 可以从 vSphere Web Client 中升级 Guest Introspection 服务虚拟机。在升级 NSX Manager 后，您不需要删除服务虚拟机以进行升级。如果删除了服务虚拟机，服务状态将显示为失败，因为代理虚拟机丢失。单击**解决 (Resolve)**以部署新的服务虚拟机，然后单击**可升级 (Upgrade Available)**以部署最新的 Guest Introspection 服务虚拟机。

前提条件

确认 NSX Manager 已升级到 6.2.x。

步骤

- 1 在**安装 (Installation)**选项卡中，单击**服务部署 (Service Deployments)**。

| Service | Version | Installation Status | Service Status | Cluster | Datastore | Port Group | IP Address Range |
|---------------------|---------|--------------------------------|----------------|---------|------------|------------|------------------|
| Guest Introspection | 6.2.0 | Succeeded Upgrade Available | Up | Comp... | ds-site... | vds-sit... | GI Pool |

安装状态 (Installation Status)列显示可升级 (Upgrade Available)。

- 2 选择要升级的 Guest Introspection 部署。

将启用服务表上方的工具栏中的**升级 (Upgrade)** () 图标。

3 单击升级 (Upgrade) (↑) 图标并按照 UI 提示进行操作。

Confirm Upgrade

Upgrade Guest Introspection service

Datastore * ds-site-a-nfs01 ▼

Network * vds-site-a_Management... ▼

IP assignment * GI Pool ▼

Specify schedule:

☒ Upgrade now

☐ Schedule the upgrade 6:29 PM ▼

OK Cancel

在升级 Guest Introspection 后，安装状态为成功，服务状态为已连接。将在 vCenter Server 清单中显示 Guest Introspection 服务虚拟机。

后续步骤

在为特定群集升级 Guest Introspection 后，您可以升级任何合作伙伴解决方案。如果启用了合作伙伴解决方案，请参阅合作伙伴提供的升级文档。即使未升级合作伙伴解决方案，也会继续提供保护。

如果将合作伙伴解决方案升级到通过 NSX 认证的版本，您必须使用服务编排以根据合作伙伴解决方案创建策略以提供保护。请参见 NSX 管理指南中的“使用服务编排”。

升级后对照表

在完成升级后，请执行以下步骤。

步骤

- 1 在升级后，创建 NSX Manager 的当前备份。
- 2 检查是否在主机上安装了 VIB。

NSX 使用以下命令安装这些 VIB：

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

如果已安装 Guest Introspection，还要检查该 VIB 在主机上是否存在：

```
esxcli software vib get --vibname epsec-mux
```

3 重新同步主机消息总线。VMware 建议所有客户在升级后执行重新同步。

您可以使用以下 API 调用在每个主机上执行重新同步。

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>  
HTTP Method : POST
```

Headers:

```
Authorization : base64encoded value of username password  
Accept : application/xml  
Content-Type : application/xml
```

在 NSX for vShield Endpoint 中使用合作伙伴服务

通过使用 Guest Introspection，您可以在 NSX 部署中使用合作伙伴服务。

本章讨论了以下主题：

- 在 NSX for vShield Endpoint 中升级合作伙伴服务
- 部署合作伙伴服务
- 在 NSX for vShield Endpoint 中使用服务编排

在 NSX for vShield Endpoint 中升级合作伙伴服务

从 vCloud Networking and Security 升级到 NSX 后，您可能需要升级合作伙伴服务。

前提条件

请参阅合作伙伴服务文档以了解兼容性和升级详细信息。

步骤

- 1 升级合作伙伴管理解决方案。
- 2 在供应商的控制台上向 NSX Manager 注册合作伙伴服务。
请参阅合作伙伴服务文档以了解相应的说明。
- 3 关闭并删除旧合作伙伴服务虚拟机。

后续步骤

部署合作伙伴服务

部署合作伙伴服务

如果合作伙伴解决方案包含主机中驻留的虚拟设备，则可以先部署服务，然后向 NSX Manager 注册解决方案。

前提条件

请确保：

- 向 NSX Manager 注册合作伙伴解决方案。

- **NSX Manager** 可访问合作伙伴解决方案的管理控制台。

步骤

- 1 单击**网络和安全**，然后单击**安装**。
- 2 单击**服务部署**选项卡，然后单击**新建服务部署** (+) 图标。
- 3 在“部署网络和安全服务”对话框中，选择相应的解决方案。
- 4 在**指定调度**（在对话框的底部）中，选择**立即部署**以立即部署解决方案，或者选择部署日期和时间。
- 5 单击**下一步**。
- 6 选择要部署解决方案的数据中心和群集，然后单击**下一步**。
- 7 选择要添加解决方案服务虚拟机存储器的数据存储，或者选择**已在主机上指定**。

选定的数据存储在选定群集的所有主机上都必须可用。

如果选择了**已在主机上指定**，则在将数据存储添加到群集中之前，必须在主机的 **AgentVM 设置**中指定 **ESX 主机**的数据存储。请参见《vSphere API/SDK 文档》。

- 8 选择用于承载管理接口的分布式虚拟端口组。该端口组必须能够访问 **NSX Manager** 的端口组。

如果网络设置为**已在主机上指定**，则必须在群集内每个主机的**代理虚拟机设置 > 网络**属性中指定要使用的网络。请参见《vSphere API/SDK 文档》。

您必须先在主机上设置代理虚拟机网络属性，然后再将其添加到群集中。导航到**管理 > 设置 > 代理虚拟机设置 > 网络**，然后单击**编辑**以设置代理虚拟机网络。

选定的端口组必须在选定群集的所有主机上都可用。

- 9 在“IP 分配”中，选择以下其中的一项：

| 选择 | 目的 |
|-------------|------------------------------------|
| DHCP | 通过动态主机配置协议 (DHCP) 将 IP 地址分配给服务虚拟机。 |
| IP 池 | 将选定 IP 池中的某个 IP 地址分配给服务虚拟机。 |

- 10 单击**下一步**，然后在“即将完成”页面上单击**完成**。
- 11 监控部署，直到**安装状态**显示“成功”。如果状态显示“失败”，请单击“失败”旁边的图标并采取措施解决该错误。

后续步骤

现在可以通过 **NSX UI** 或 **NSX API** 使用合作伙伴服务。

在 NSX for vShield Endpoint 中使用服务编排

服务编排有助于置备网络和安全服务并将其分配给虚拟基础架构中的应用程序。

您可以使用服务编排创建安全组和安全策略。安全组可以包含静态和动态组成员定义。安全策略将服务应用于安全组。

请参阅 **NSX 管理指南**中的服务编排文档以了解相应的信息和说明。