



ESXi 5.0 最新教程

ESXi 5.0 最新教程

在上期的《[vSphere 5.0 最新教程](#)》中，大家了解了 vSphere 5.0 的一些列技巧。这里就为大家双手奉上姊妹篇《ESXi 5.0 最新教程》。本期技术手册我们将为大家解决有关 ESXi 5.0 升级、配置、安全以及内存管理等多方面的技术问题。

ESXi 5.0 升级

该升级你的 ESXi 5.0 啦，选择稳妥的 ESXi 5.0 Update 1，还是想尝鲜升级到最新的 ESXi 5.1，这里都给您提供手把手的升级过程。有图有真相哦。

- ❖ 八图将 ESXi 5.0 升级至 ESXi 5.0 Update 1
- ❖ 六图轻松从 ESXi 5.0 升级至 ESXi 5.1

ESXi 5.0 配置

远程 Linux 服务器是存储 VMware ESXi syslog 事件的好地方，VMware ESXi 使用 syslog 记录重要事件的信息，在发生灾难时便于您进行分析。

- ❖ 在远程 Linux 上存储 VMware ESXi syslog 事件
- ❖ 配置 VMware ESXi syslog 实现日志集中管理
- ❖ VMware ESXi 网络时间同步：时间是关键

ESXi 5.0 内存管理

ESXi 主机启用 SSH 以及 VMware HA 集群没有配置管理网络冗余都会引起黄色告警，这里对这两种情况进行解读并提供相应的调整建议以及在内存管理方面的收获。

- ❖ 如何处理 ESXi 主机的黄色告警
- ❖ 从内存告警谈 ESXi 主机内存管理——VM 内存介绍
- ❖ 从内存告警谈 ESXi 主机内存管理——内存构成

ESXi 5.0 安全

保卫你的 VMware 架构安全是个多层的过程：需要保护 ESXi 主机、虚拟机和 hypervisor 本身。VMware ESXi 在 vSphere 5 中占据主导地位，这个 hypervisor 伴随着新的 ESXi 安全考虑。

- ❖ VMware ESXi 安全六问六答：保卫 hypervisor 与主机

八图将 ESXi 5.0 升级至 ESXi 5.0 Update 1

VMware 在三月 15 日发布了 ESXi 5.0 的第一个补丁更新 ESXi 5.0 Update 1，距离 ESXi 5.0 的正式发布已有 7 个月之久。ESXi 5.0 Update 1 提供的新增功能主要包括：在硬件方面，ESXi 5.0 Update 1 对 AMD 和 Intel 最新的处理器提供了支持，同时对相关设备的驱动程序进行了升级：增加了对适用于 Intel C600 系列芯片集的本机存储驱动程序的支持，并将 LSI MegaRAID SAS 驱动程序版本升级至 5.34；在软件方面：ESXi 5.0 Update 1 对 Mac OS X Server Lion 10.7.2 和 10.7.3 客户操作系统提供了支持，另外在 ESXi 5.0 Update 1 中包含最新版本的 [VMware Tools](#)，进一步增强虚拟机的客户机操作系统的性能。



此外，ESXi 5.0 Update 1 针对 [ESXi 5.0](#) 中存在的各类问题包括客户机操作系统、许可、网络、安全、服务器配置、升级和安装、vMotion 以及 Storage vMotion 等进行了修复。以客户机操作系统为例，在 ESXi 5.0 中对 Windows 2008 R2 客户机操作系统执行热克隆自定义操作，可能会失败并出现“未找到自动检查（auto check not found）”的错误消息，而且虚拟机将一直重新引导。

了解 ESXi 5.0 Update 1 的新增功能后，如果你准备使用 ESXi 5.0 Update 1，最简单的方法就是使用 ESXi 5.0 Update 1 ISO 镜像文件。VMware-VMvisor-Installer-5.0.0.update01-623860.x86_64.iso 在裸机上进行交互式安装。如果主机上已经安装了 ESXi 5.0，使用此安装镜像也可以完成从 ESXi 5.0 到 ESXi 5.0 Update 1 的升级，而且该安装镜像也支持从 ESXi 4.0 直接升级至 ESXi 5.0 Update 1。如下图所示执行交互式升级需要根据实际情况在以下三个选项中做出选择。



图 1. ESXi 5.0 Update 1 升级选项

另外 VMware 专门为 ESXi 5.0 定制了升级至 ESXi 5.0 Update 1 的升级工具包: update-from-esxi5.0-5.0_update01.zip, 顾名思义, 该工具包并不支持 ESXi 5.0 以前的版本。

由于交互式安装、升级 ESXi 5.0 Update 1 的步骤与《图解交互式方式安装 ESXi 5.0 的过程》一文中介绍的内容并无太多差异, 所以本文介绍如何采用升级工具包完成从 ESXi 5.0 到 ESXi 5.0 Update 1 的升级。

下载升级工具包

首先我们需要到 VMware 官方网站 (<http://www.vmware.com/cn/support/>) 下载 ESXi 5.0 的升级工具包, 选择“下载 ESX/ESXi 补丁程序”链接, 如图 1 所示在“Download Patches”页面下选择“ESXi (Embedded and Installable)”版本为 5.0.0, 然后点击“search”按钮进行补丁查询。

Download Patches

Use the search tool to find patches available for VMWare products. To download products, product updates, drivers and tools, visit the [Downloads](#) page.

Search by Product

Select a product and version. To narrow the results further, enter a release date and/or patch type.

Note: Patches are available for:

- ESX: Patch bundle for ESX Classic
- ESXi: Patch bundle for ESX Embedded and Installable
- VEM: Patch bundle for Cisco Nexus Virtual Ethernet Module for ESX/ESXi

ESXi (Embedded and Installable) ▾ 5.0.0 ▾ Release Date All Categories ▾ All Severities ▾

图 2. 查找 ESXi 5.0 补丁更新程序

在查询结果中包括了“update-from-esxi5.0-5.0_update01”文件，可以看到其大小为 590.5 MB，Build Number 为 623860，发布日期为 3 月 15 日，该软件包中包括了各类驱动程序以及软件包（VIB）。

Release Name	Description	Bulletin List	Category	Severity
	Updates the ESXi 5.0 net-rx-nic vib Details	ESXi500-201203209-UG KB 2010822	Bug Fix	Important
	Updates the ESXi 5.0 scsi-mpt2sas driver Details	ESXi500-201203210-UG KB 2011435	Bug Fix	Important
	Updates the ESXi 5.0 esx-base vib Details	ESXi500-201203201-UG KB 2010814	Bug Fix	Critical
	Updates the ESXi 5.0 misc-drivers vib Details	ESXi500-201203205-UG KB 2010818	Bug Fix	Important
	Updates ESXi 5.0 scsi-megaraid-sas vib Details	ESXi500-201203204-UG KB 2010817	Enhancement	Important
<input checked="" type="checkbox"/> update-from-esxi5.0-5.0_update01 Download	Updates the ESXi 5.0 tools-light vib Details	ESXi500-201203202-UG KB 2010815	Bug Fix	Important
Product: ESXi (Embedded and Installable) 5.0.0 md5sum:55c25bd990e2881462bc5b66fb5f6c39 sha1sum:ecd871bb09b649c6c8c13de82d579d4b7dcadc88 Download Size 590.5 MB	Updates the ESXi 5.0 tools-light vib Details	ESXi500-201203102-SG KB 2011433	Security	Moderate
Build Number: 623860 KB 2010823	Updates the ESXi 5.0 esx-base vib Details	ESXi500-201203101-SG KB 2011432	Security	Important
Release Date: 03/15/2012	Updates the ESXi 5.0 scsi-aacraid driver Details	ESXi500-201203211-UG KB 2011436	Bug Fix	Important
	Updates the ESXi 5.0 ehci-ehci-hcd vib Details	ESXi500-201203203-UG		

图 3. 从 ESXi 5.0 升级至 ESXi 5.0 Update 1 的软件工具包

升级 ESXi 5.0

如图 4 所示，首先我们需要使用 [vSphere Client 5.0](#) 连接至 ESXi 5.0 主机，然后将升级工具包“update-from-esxi5.0-5.0_update01.zip”文件上传至 ESXi 5.0 主机的一个数据存储中。

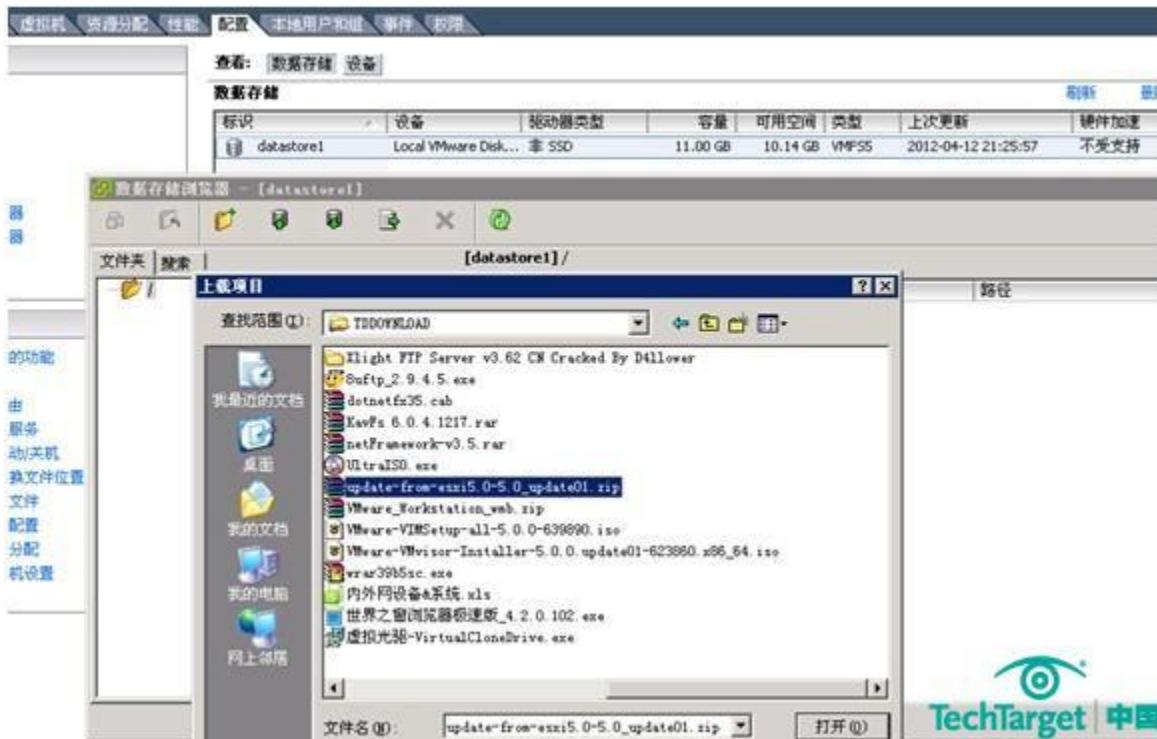


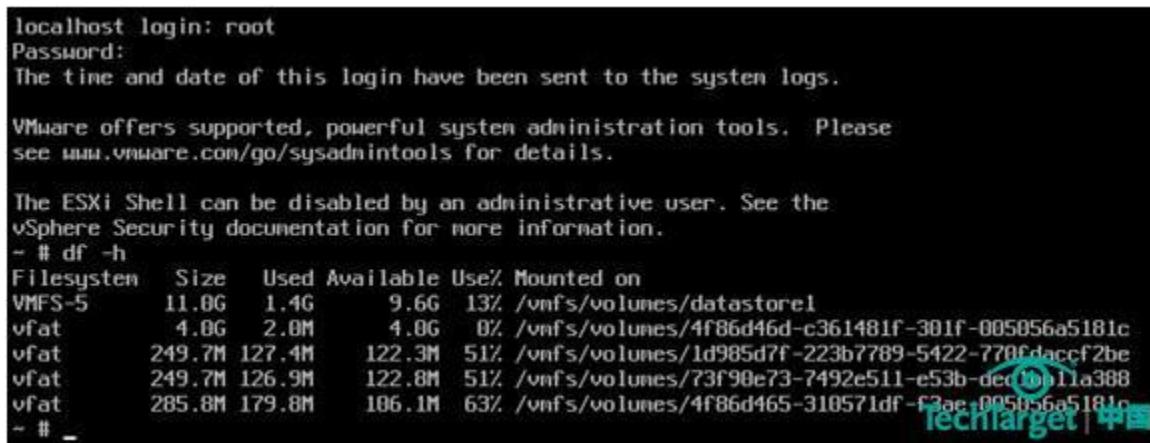
图 4. 使用 vSphere Client 5.0 将升级包上传至数据存储中

接下来将该 ESXi 5.0 主机上的虚拟机迁移至其他 ESXi 主机，然后通过直接控制台 UI (DCUI) 登录到 ESXi 5.0 主机，按“F2”键，在弹出的身份认证界面输入 root 用户的密码后就可以登录到直接控制台。进入“TroubleShooting Options”选项，然后启用 ESXi Shell。



图 5. 启用 ESXi Shell

启用 ESXi Shell 后在直接控制台 UI 中通过“Alt+F1”组合键就可以访问本地的 ESXi Shell 了。如下图所示，输入用户名、口令后就可以登录到本地的 ESXi Shell。使用“df -h”命令可以查看本地文件系统信息。



```
localhost login: root
Password:
The time and date of this login have been sent to the system logs.

VMware offers supported, powerful system administration tools. Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
- # df -h
Filesystem  Size  Used Available Use% Mounted on
VMFS-5     11.0G  1.4G    9.6G  13% /vmfs/volumes/datastore1
vfat       4.0G   2.0M    4.0G   8% /vmfs/volumes/4f86d46d-c361481f-301f-005056a5181c
vfat      249.7M 127.4M   122.3M  51% /vmfs/volumes/1d985d7f-223b7789-5422-770fdaccf2be
vfat      249.7M 126.9M   122.8M  51% /vmfs/volumes/73f90e73-7492e511-e53b-de01011a388
vfat      285.8M 179.8M   106.1M  63% /vmfs/volumes/4f86d465-310571df-f3ae-005056a5181c
- # _
```

图 6. 登录到 ESXi Shell 中，查看本地文件系统

进入到“update-from-esxi5.0-5.0_update01.zip”文件所在目录，执行升级：

```
# cd /vmfs/volumes/datastore1/
#esxcli software vib install -d= "/vmfs/volumes/datastore1/update-from-
esxi5.0_update01.zip"
```

升级时间只需要短短的几分钟，升级完成后将看到如下提示，但是需要重新启动系统：“Reboot Required: true”。

```
- # cd /vmfs/volumes/datastore1/  
/vmfs/volumes/4f86d46c-2eec0cef-86d9-005056a5181c # ls  
update-from-esxi5.0-5.0_update01.zip  
/vmfs/volumes/4f86d46c-2eec0cef-86d9-005056a5181c # esxcli software vib install -d="/vmfs/volumes/datastore1/update-from-esxi5.0-5.0_update01.zip"  
Installation Result  
Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.  
Reboot Required: true  
VIBs Installed: VMware_bootbank_ehci-ehci-hcd_1.0-3vnu.500.1.11.623860, VMware_bootbank_esx-base_5.0.0-1.11.623860, VMware_bootbank_nisc-drivers_5.0.0-1.11.623860, VMware_bootbank_net-be2net_4.0.88.0-lvnu.500.0.7.515841, VMware_bootbank_net-e1000_8.0.3.1-2vnu.500.0.7.515841, VMware_bootbank_net-e1000e_1.1.2-3vnu.500.1.11.623860, VMware_bootbank_net-nx-nic_4.0.557-3vnu.500.1.11.623860, VMware_bootbank_sata-ahci_3.0-6vnu.500.1.11.623860, VMware_bootbank_sata-ata-piix_2.12-4vnu.500.1.11.623860, VMware_bootbank_scsi-nparaid-sas_5.34-1vnu.500.1.11.623860, VMware_bootbank_scsi-npt2sas_06.00.00.00-6vnu.500.1.11.623860, VMware_bootbank_scsi-rste_2.0.2.0088-lvnu.500.1.11.623860, VMware_bootbank_scsi
```

图 7. 将 ESXi 5.0 升级至 ESXi 5.0 Update 1

ESXi 主机完成重启后，在直接控制台 UI 中可以看到 ESXi 5.0 VMkernel 的构建版本已经升级至 623860 了，升级完成。

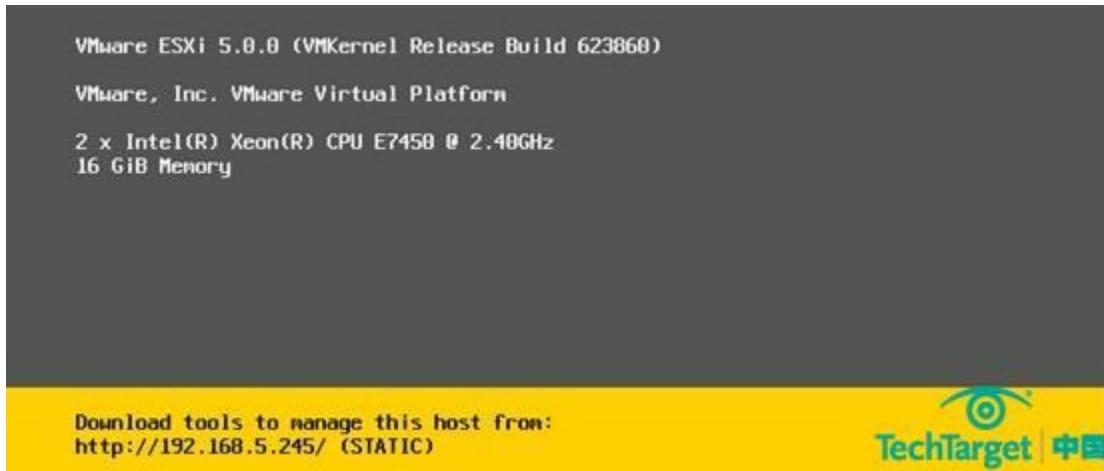


图 8. 完成升级，ESXi 5.0 Update 1 VMkernel 构建版本为 623860

六图轻松从 ESXi 5.0 升级至 ESXi 5.1

9月10日VMware在官方网站正式开放了vSphere 5.1产品的下载，允许用户对vSphere 5.1进行评估。评估的产品包括英文版及中文版，不需要使用测试许可，可以免费试用60天。在《[VMware开放vSphere 5.1评估](#)》一文中我们介绍了如何下载vSphere 5.1镜像软件，本文继续介绍如何从现有的ESXi 5.0升级至ESXi 5.1。

首先将需要升级的ESXi 5.0主机上的虚拟机通过[vMotion](#)迁移到其他ESXi主机，然后将ESXi 5.1的安装光盘放入ESXi主机的光驱，重启ESXi主机就可以开启ESXi的升级过程了。如下图1所示，直接按回车键，开始安装ESXi 5.1。

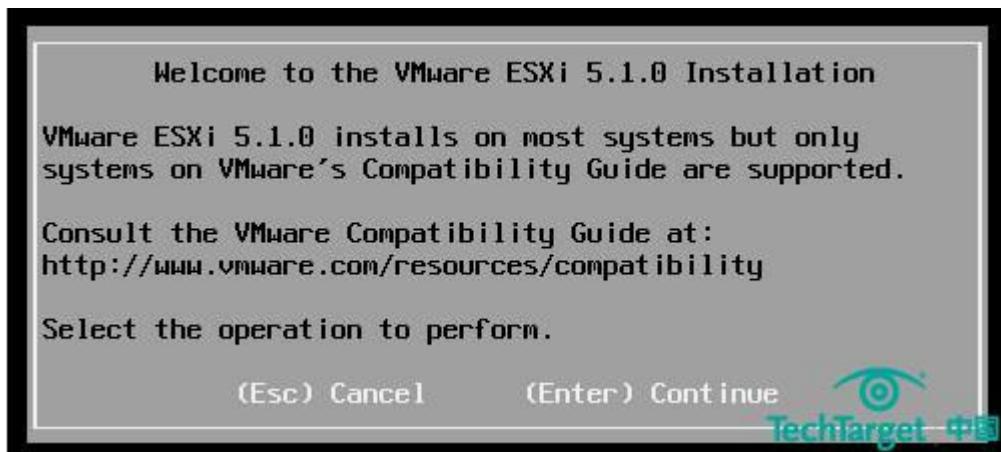


图1. 安装 VMware ESXi 5.1

如图2所示，按“F11”接受VMware最终用户许可协议，开始ESXi 5.1的升级过程。

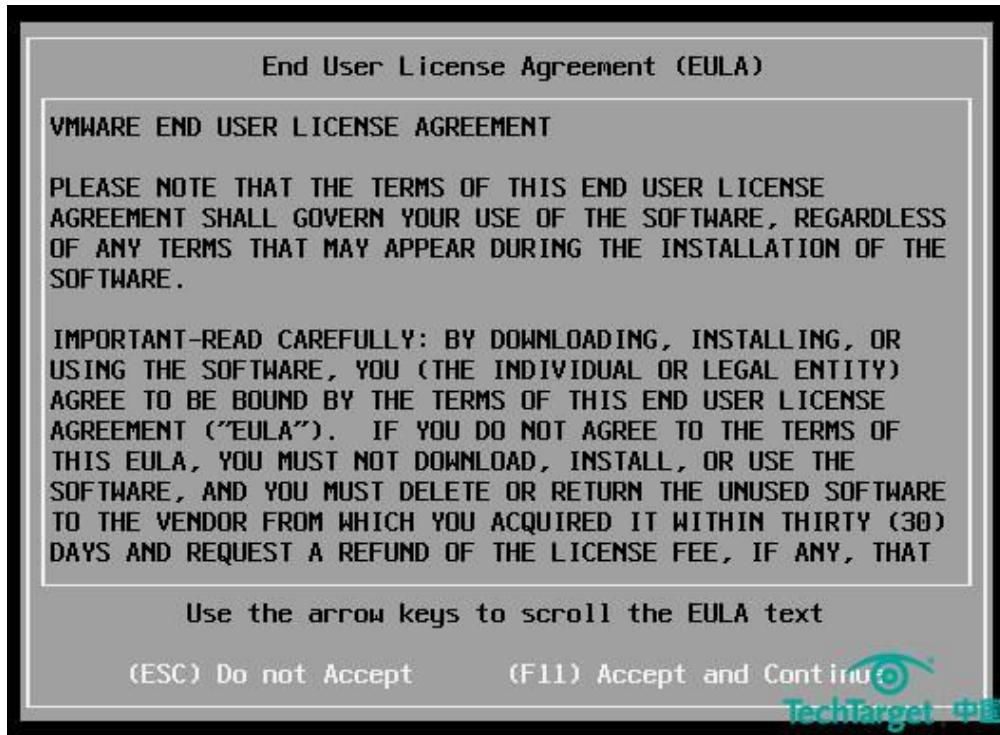


图 2. 最终用户许可协议

如图 3 所示，在升级至 VMware ESXi 5.1 时有三种方式可供选择。第一种方式最为常见，那就是升级 VMware ESXi 同时保留当前的 VMFS 数据存储格式（VMFS 5）及数据。第二种方式是重新安装 ESXi 同时保留当前的 VMFS 数据存储格式（VMFS 5）及数据。和第一种方式的不同之处在于第二种方式将会丢失现有设置，如果选择这种方式会重新安装 ESXi，在升级之后必须将虚拟机重新添加到虚拟机清单当中。第三种方式是全新安装 VMware ESXi 5.1，会覆盖原来的 VMFS 数据存储。建议用户选择第一种升级方式。



图 3. 选择正确的升级方式

在图 3 中选择第一种升级方式并按回车键后，将会看到如下图所示的升级提示：将系统从 ESXi 5.0 升级至 ESXi 5.1，所使用的数据存储为：
mpx.vmhba1:C0:T0:L0。按 F11 键开始升级过程。



图 4. 按 F11 确认升级

经过数分钟的升级后，如下图 5 所示，将会看到如下提示信息：系统成功升级至了 ESXi 5.1，评估周期为 60 天。在评估周期结束后如果想继续使用 ESXi 5.1 必须使用新的许可。取出安装光盘后，按回车键重启服务器然后就可以开始使用 ESXi 5.1 了。



图 5. 重启服务器 完成升级过程

服务器重启完成后，进入到直接控制台 UI 下，可以看到 ESXi5.0 已经成功升级至 ESXi 5.1 了，VMkernel 的构建版本为 799733。

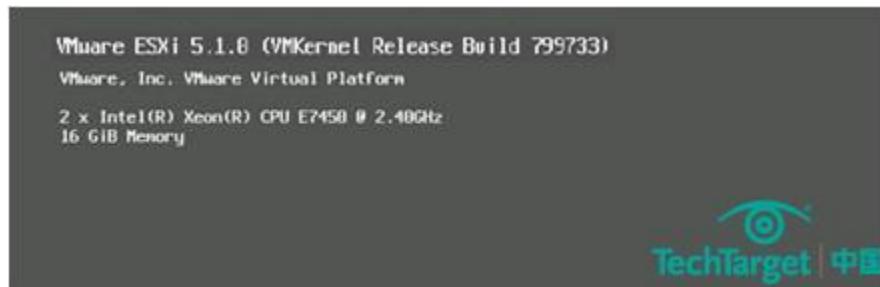


图 6. 成功升级至 ESXi 5.1

在远程 Linux 上存储 VMware ESXi syslog 事件

远程 Linux 服务器是存储 VMware ESXi syslog 事件的好地方，尤其是发生灾难时。

例如，发生安全漏洞，最基本的你要分析是啥出错了。VMware ESXi 使用 [syslog](#) 记录重要事件的信息，如如网络接口状态的更改，或链接到存储区域网络的改变。通过检查 ESXi syslog 事件，可以追溯虚拟环境中的问题。

但是，如果 VMware ESXi syslog 事件存储在产生它们的同个服务器上时，发生问题时就不能访问关键信息。这也是为什么要使用远程服务器在外部存储 syslog 信息的原因，便于保护登录架构。拥有一些额外的硬软件，加上 ESXi hypervisor，可设置便宜的远程 Linux 服务器来记录 VMware ESXi syslog 事件。

为 ESXi syslog 事件配置远程 Linux 服务器

默认下，syslog 在主机上存储 ESXi 登录。最好设置一台外部登录主机，Linux 是最方便的平台。

Linux 有各种版本，无论选择何种作为登录主机都行。我在本文中使用的是 [OpenSUSE](#)，它是个免费的 Linux 版本，是 SUSE Linux Enterprise Server 的基础。

执行 OpenSUSE 默认安装后，需要配置运行在 OpenSUSE 上的登录服务器 rsyslogd。首先，配置 syslog 从其他主机接收日志消息，选择是否想通过 [Transmission Control Protocol](#) (TCP) 或 [User Datagram Protocol](#) (UDP) 接收日志文件。默认下，rsyslogd 使用 UDP 作为传输机制。如果底层网络受信任，这是个很好的选择。但是，如果日志信息通过不受信任的网络连接传输的话，就有可能丢失包，这时 TCP 就是确保信息传输到日志主机的好选择。

第一次使用 rsyslog 日志主机时，我推荐 UDP。不过在需要增加可靠性时，你可以轻松切换到 TCP。

要在 syslog 主机上启动 UDP 日志接收的话，打开配置文件 /etc/rsyslog.d/remote.conf 并编辑，如 gedit 或 vi。确保以下两行位于文件前列：

```
$ModLoad imudp.so
```

\$UDPServerRun 514

现在已在远程 Linux 服务器上启用了 rsyslog，重启。使用命令服务 rsyslogd 进行重启。接下来，配置 ESXi 主机发送它们的 syslog 事件到你新配置的远程 Linux 服务器。

在本系列第二部分，将介绍如何配置 vSphere 以发送信息到远程主机。

配置 VMware ESXi syslog 实现日志集中管理

更改 VMware ESXi 配置来实现日志集中管理的过程很简单。当数据中心出现问题时，日志集中管理能够帮助你避免 ESXi syslog 消息丢失。如果不改变默认的配置，当主机出现问题时本地存储的日志将不可用，而且在主机重启后日志也将被清空——也就是说，有价值的日志信息都将丢失。

我已经描述了如何在远程的 Linux 服务器上配置集中日志主机以[获取 VMware ESXi syslog 事件](#)。现在，你需要对 ESXi 主机进行配置以便将所有的日志消息都发送到远程 Linux 服务器上。

找到 ESXi syslog 参数并更改

登录到 vSphere Client 后，你可以通过两种方式访问 ESXi syslog 消息。被选定主机的事件选项卡对记录了所有日志，其中包括记录事件的目标主机。通过 vSphere Client 界面打开日志消息后，可以看到事件的详细说明，这其中包括了相关的事件，能够帮助你找到究竟发生了什么。

localhost.dynamic.ziggo.nl VMware ESXi, 5.0.0, 469512

Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions

Show all entries ▾

Description	Type	Date Time	Task	Target	User
Userroot@192.168.1.51 logged in	info	14-1-2012 10:35:35			root
Userroot@127.0.0.1 logged in	info	14-1-2012 10:05:26			root
Userroot logged out	info	14-1-2012 10:05:20			root
Userroot@127.0.0.1 logged in	info	14-1-2012 10:05:20			root
Host has booted.	info	14-1-2012 10:05:19		localhost.dynamic.z...	
USB configuration has changed.	info	14-1-2012 10:05:19		localhost.dynamic.z...	
Firewall configuration has changed. Operation 'enable' for rule set CIMHttpsServer succeeded.	info	14-1-2012 10:05:17		localhost.dynamic.z...	
Firewall configuration has changed. Operation 'enable' for rule set CIMHttpServer succeeded.	info	14-1-2012 10:05:17		localhost.dynamic.z...	
Login to iSCSI target iqn.2011-05.com.example:198130ff-da50-4638-8d8f-f32cd42b4d48 on vmhba34 failed. The iSCSI initiator could not establish a network connection to the target.	error	14-1-2012 10:05:15		localhost.dynamic.z...	
VMware Host Agent started	info	14-1-2012 10:05:11		localhost.dynamic.z...	
Configuration file for Unknown cannot be found	info	14-1-2012 10:05:09		Unknown User	
iSCSI discovery to 192.168.1.100 on vmhba34 failed. The iSCSI Initiator could not establish a network connection to the discovery address.	error	14-1-2012 10:05:08		localhost.dynamic.z...	
Firewall configuration has changed. Operation 'enable' for rule set vpxdHeartbeats succeeded.	info	14-1-2012 10:05:01		localhost.dynamic.z...	
Physical NIC vmnic3linkstate is up.	info	14-1-2012 10:05:00		localhost.dynamic.z...	
Physical NIC vmnic2linkstate is up.	info	14-1-2012 10:05:00		localhost.dynamic.z...	
Physical NIC vmnic1linkstate is up.	info	14-1-2012 10:05:00		localhost.dynamic.z...	
Physical NIC vmnic0linkstate is up.	info	14-1-2012 10:05:00		localhost.dynamic.z...	

Event Details

Type: info Time: 14-1-2012 10:05:19 Target: localhost.dynamic.ziggo.nl

Description:

14-1-2012 10:05:19, Host has booted.

Related Events: Show

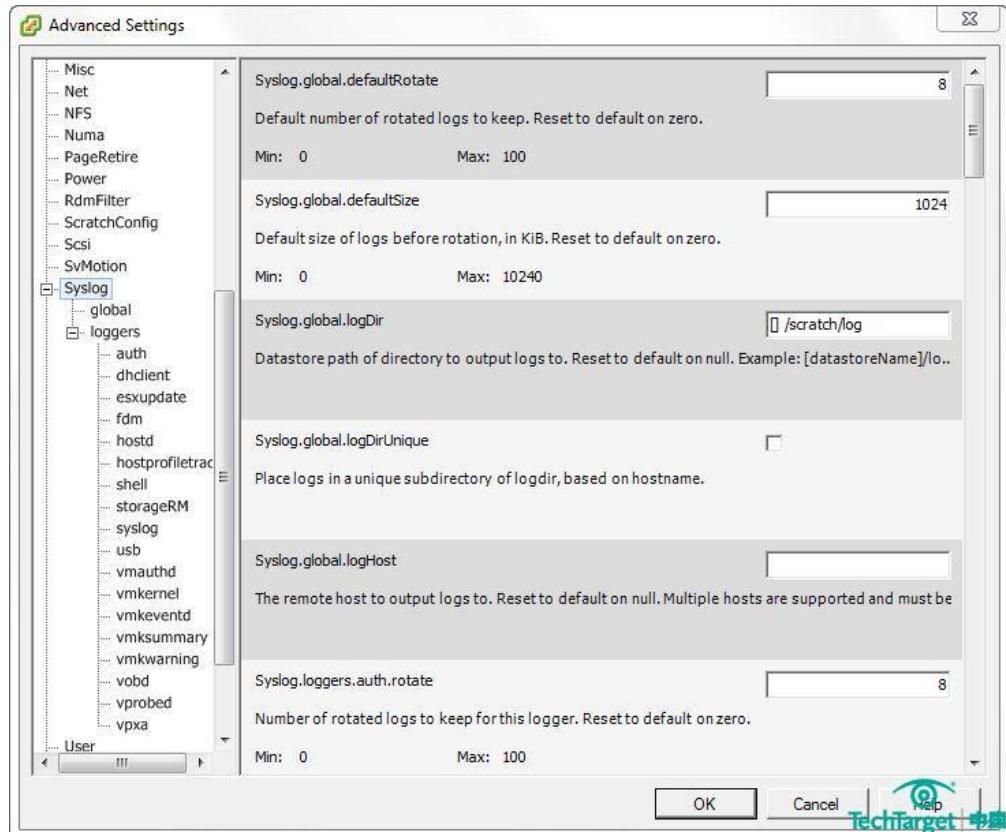
在被选定主机的事件页面能够看到所有的日志事件

也可以通过视图>管理菜单看到日志消息。这时你将会发现系统日志选项，能够访问被选定 ESXi 主机上的三个日志文件。

- /var/log/hostd.log: 你可以找到这台 ESXi 主机的日志记录;
- /var/log/vmkernel.log: 这个文件由 vmkernel 生成; 以及
- /var/log/vpxa.log: 这个文件包括了来自 vCenter 代理的日志消息。

究竟哪个日志文件包括了你正在寻找的消息可能并不是很明显。但是相关的文件只有这三个，因此找到与特定事件相关的信息也不是非常困难的事儿。

为了启用集中日志管理，首先需要在 vSphere Client 中选定 [ESXi 主机](#)，然后选择配置选项卡。接下来单击高级设置，这将打开与你所选定的 ESXi 主机相关的一些高级设置。单击 Syslog 查看适用于 ESXi 主机的日志事件。



在高级设置界面配置 ESXi Syslog 参数

默认情况下，ESXi 在 localhost 上也就是本机上存储所有的日志。为了指定远程日志主机的名字，需要从 Syslog 主菜单条目中选择 Syslog.global.logHost 参数并指定消息将要发送的目的地的统一资源标识符 URI。在 URI 中需要指定协议（TCP 或者 UDP）、主机名或者 IP 地址以及端口号（比如，`udp://192.168.1.62:514`）。更改这些参数后，单击确定激活新的配置。从现在开始，主机将会将日志发送到远程的 syslog 主机，实现集中的日志管理。

其他的 ESXi syslog 选项

位于高级>Syslog 选项卡下的其他大多数参数都和本机的日志配置有关。一个有用的参数就是位于 Syslog 属性之下的 Syslog.global.logDirUnique。启用这个

参数后将在日志服务器上基于主机名创建一个单独的子目录。为所有的主机创建单独的子目录将使查找特定 ESXi 主机的日志变得更加容易。

在全局和日志选项卡下还有其他一些与 ESXi syslog 相关的选项，但是只有在本地 ESXi 主机上存放日志时配置这些选项才有意义。一旦设置了远程集中日志管理，就不需要改变这些日志选项了。

VMware ESXi 网络时间同步：时间是关键

在虚拟架构中，由于服务依赖服务器，所以网络时间同步对于服务器保持一致非常重要。对于 VMware ESXi 主机，可用 vSphere Client 实施网络时间协议 NTP 同步。

需要同步 ESXi 主机的理由有很多。例如，如果主机与 [Active Directory](#) 集成，需要时间实现同步。在创建和重新获得快照的时候也需要时间保持一致，因为快照保存的是服务器状态的实时镜像。幸好，使用 vSphere Client 设置网络时间同步非常简单。

VMware 网络时间同步过程

要配置 NTP 同步，选择主机，在 Configuration 列表上选择 Time Configuration under Software。就可以看见主机上现有的时间同步。接下来点击属性，跳出 Time Configuration 窗口，能看到主机目前的时间。确保不要与实际时间相差太大，如果主机时间比实际时间多出 1000 秒的话，就太“疯狂”啦，同步就很难。

在为主机设置本地时间后，选择 NTP Client Enabled。为主机激活 NTP 时间同步。重启服务器，查看 Options 确保已启用 NTP。然后可以访问 NTP Startup Policy，选择 Start and stop with host。

但是时间同步的工作还未完成。现在，需要选择与 [VMware ESXi](#) 主机应该同步的 NTP 服务器。点击 NTP Settings 可看见目前的 NTP 服务器列表。默认下是空的。点击 Add 添加你要使用的 NTP 服务器的名称或地址。界面会提示你地址，但你也能输入一个能通过 DNS 的名称。

如果你不知道使用哪一台 NTP 服务器用于 VMware 网络时间同步的话，在 .ntp.org 池中的互联网 NTP 服务器也同样可用。只需要从该组中选择一台服务器添加到 NTP 服务器列表中。当然，如果你想同步内部的或专有的 NTP 服务器的话，应该至少制定两台 NTP 服务器。

这时，确保重启 NTP 服务器的选择已选。点击三次 OK 保存和适用更改。在 ESXi 主机的配置屏幕上，现在能看到 NTP Client 在运行，也能显示主机目前所使用的 NTP 服务器列表。

随着 ESXi 主机同步到正确的时间，所有依赖于时间的服务与事件都能正常运行。最重要的是，不会浪费时间精力去修改配置错误的网络时间。

如何处理 ESXi 主机的黄色告警

当我们登录到 vCenter Server 对虚拟化环境进行管理时，有时会在 ESXi 主机图标的右下方发现黄色的告警。通过检查可以发现 ESXi 主机的运行状况是正常的，黄色告警实际上只是为了引起管理人员的注意。本文对引起黄色告警的两种情况（ESXi 主机启用 SSH 以及 VMware HA 集群没有配置管理网络冗余）进行解读并提供相应的调整建议。

ESXi 主机启用 SSH

为了能够通过 SSH 客户端访问 ESXi 主机，我们需要登录到 [ESXi 主机](#) 的管理控制台开启主机的 ESXi Shell。如下图 1 所示，当开启 ESXi Shell 后，就会在 ESXi 主机图标的右下方发现黄色的告警，在 ESXi 主机的摘要选项下可以看到这一提示信息。



图 1. ESXi 主机 SSH 启用告警

为了保证 ESXi 主机的正常运行，ESXi Shell 默认是关闭的，在生产环境中也不建议启用 SSH。此时消除告警的方法就是登录到 ESXi 控制台中，选中下图中的“Disable ESXi Shell”，然后单击回车键 ESXi Shell 就将关闭。



图 2. 在 ESXi 主机控制台下禁用 ESXi Shell

但是为了对 ESXi 主机进行故障诊断，有时需要暂时启用 SSH。在启用 SSH 的情况下是否能够消除 ESXi 主机图标的右下方的黄色告警呢？实际上在不关闭主机 SSH 的情况下，消除告警只需要进行如下两个操作：

- (1) 进入配置选项卡，选择软件的高级设置选项



图 3. ESXi 主机配置选项卡

(2) 在弹出的“高级设置”对话框中选中“UserVars”，在右侧的配置参数中，选择 UserVars.SuppressShellWarning，将文本框中的值从 0 改为 1，然后单击确定即可。这样就忽略了对 ESXi Shell 的告警。



图 4. 禁用 ESXi Shell 告警信息

ESXi 主机没有冗余的管理网络

除了开启主机的 ESXi Shell 会导致出现黄色的告警之外，如果 ESXi 主机没有配置冗余的管理网络同样会出现类似的告警信息。

如下图 5 所示，以 [ESXi 4.1](#) 主机构成的 HA 集群为例，可以在摘要选项卡下看到由于主机没有配置冗余的管理网络导致出现黄色告警。由于 HA 集群中的所有 ESXi 主机需要借助管理网络传递心跳信息，所以 VMware 建议配置冗余的管理网络，否则就会在集群中没有配置冗余管理网络的 ESXi 主机图标的右下方显示告警信息。



图 5. ESXi 主机没有冗余的管理网络导致告警

选择 ESXi 主机的配置选项卡，通过硬件部分的网络选项可以发现这台 ESXi 4.1 主机管理网络所在的虚拟交换机是 vSwitch0，配置了两块网络适配器，但是其中的 vmnic1 的连接状态是断开的。因此该 ESXi 主机提示了管理网络没有冗余的告警。



图 6. 检查 ESXi 主机的管理网络

通过检查 vmnic1 的物理连接状态，发现其对端连接的物理交换机端口松动，导致连接中断。连接恢复正常后，管理网络所在的虚拟交换机 vSwitch0 连接的物理适配器就有两个了，此时告警就消除了。

如果 ESXi 主机的网卡数量有限，同时又要实现管理网络和虚拟机网络的分离，那么可能无法为管理网络分配冗余的适配器。在这种情况下是否有办法消除黄色告警呢？为了消除这个告警需要按照以下步骤操作：

- (1) 选中 HA 集群，在弹出的右键菜单中选择“编辑设置”；
- (2) 在弹出的集群设置会话框中，选择“VMware HA”选项，然后选择右侧的“高级选项”按钮；



图 7. 配置 HA 集群

(3) 在弹出的高级选项对话框中，在选项中输入“das.ignoreRedundantNetWarning”，在选项值中输入“true”，然后单击确定即可；

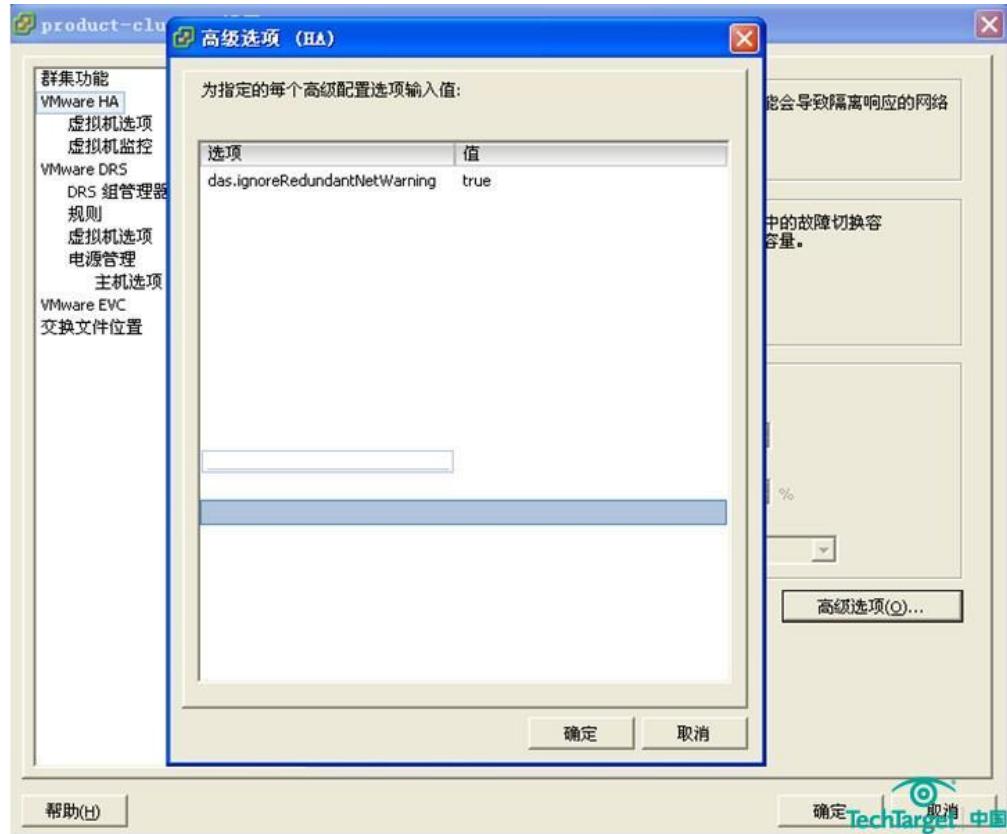


图 8. 忽略 HA 集群的无管理网络冗余告警

(4) 为了使配置生效，需要先关闭集群的 HA 功能，然后再启用。如下图所示，选择集群功能选项，在右侧的功能选项中将“打开 VMware HA”前面的复选框取消掉并单击“确定”按钮即可关闭或开启集群的 HA 功能。



图 9. 关闭并开启集群的 HA 功能

请注意，在 vSphere 4.1 环境下，由于 HA 集群借助管理网络传递心跳信息，所以建议为 HA 集群中的所有主机配置冗余的管理网络。

为了解决由于管理网络发生故障导致 HA 集群无法传递心跳信息以及其他问题，VMware 在 [vSphere 5.0](#) 中重新设计了 HA 架构，在 HA 集群中的每台 ESXi 主机运行一个特别的、独立于 vpxd 代理（用于和 vCenter Server 进行通信）的故障域管理器（Fault Domain Manager），FDMs 默认仍然通过主机管理网络进行通信，当管理网络不可用时集群中的 ESXi 主机能够通过 Datastore 进行通信。

作为管理人员，在对虚拟化环境进行日常的维护过程中，需要留意各类告警信息以及相应的告警提示。通过对告警信息进行分析，能够预先发现虚拟化环境可能存在的问题。虽然本文提供了通过参数配置简单地忽略各类告警信息的方法，但是还是建议优先采用消除告警的方法，只有消除了不利因素，才能保证虚拟化环境更加稳定的运行。

从内存告警谈 ESXi 主机内存管理——VM 内存介绍

在上篇文章《[从内存告警谈 ESXi 主机内存管理——内存构成](#)》中，我们主要介绍了 ESXi 主机内存构成和虚拟机内存构成，这里我们继续进行虚拟机内存介绍。

每台虚拟机的内存部分包括了两个方面的内容：主机内存、客户机内存。这几个概念看起来有些令人迷惑，我们简单介绍一下。

表格 1. 主机内存

参数	含义
已消耗	已分配给虚拟机的物理内存的实际消耗量
开销消耗	用于虚拟化目的的已消耗内存量

在上图中 4，主机内存已消耗的大小为 11.91GB，这和图 3 中的 12195MB 是完全相同的。

在运行过程中除了消耗为其分配的内存外，每个虚拟机还会消耗额外的开销内存以用于虚拟化。开销内存包括为虚拟机框架缓冲区和各种虚拟化数据结构（如卷影页表）预留的空间。开销内存的大小取决于虚拟 CPU 数量，为客户机操作系统配置的内存以及虚拟机的工作负载。在上图 4 中这台虚拟机的内存开销已经达到了 1.13GB。

表格 2. 客户机内存

参数	含义
专用	受主机内存支持且没有共享的内存量
已共享	共享的内存量。vSphere 采用透明页共享 (transparent page sharing) 技术实现了虚拟机内存的共享，因此在虚拟机中运行的工作负载消耗的内存通常要少于其在物理机上运行时所需的内存，能够高效地支持更高级别的过载。
缩减量	压缩缓存中的内存量。vSphere 提供了内存压缩缓存，能够在内存过载使用时改进虚拟机性能
虚拟增长	通过虚拟增长回收的内存量。vSphere 利用内存虚拟增长驱动程序 (vmmemctl) 与服务器协作回收客户机操作系统认为最不重要的页面
已交换	通过交换回收的内存量。当 vmmemctl 驱动程序不可用或未响应时，vSphere 会使用交换从虚拟机中强制回收内存

未访问过	客户机从未访问过的内存量
活动	客户机最近访问过的内存量

利用性能图表监视虚拟机内存使用

理解了上述概念将有利于我们开展虚拟机的性能调整工作。图 4 中看到的信息都是静态信息，为了获取虚拟机内存使用情况的动态信息，为内存调整提供依据，我们可以利用性能高级图表实时查看虚拟机内存使用情况，也可以查看在过去一天、一周乃至更长时间的虚拟机内存使用情况。下图 5 列出了在过去一个小时内存的实时使用情况，从下图中可以看到：

- 授权量大于消耗量，但两个值差距不大，所以为虚拟机分配的内存大小是合理的。
- 在过去的一个小时内，没有虚拟增长和已交换活动的发生，虚拟机运行状况稳定。

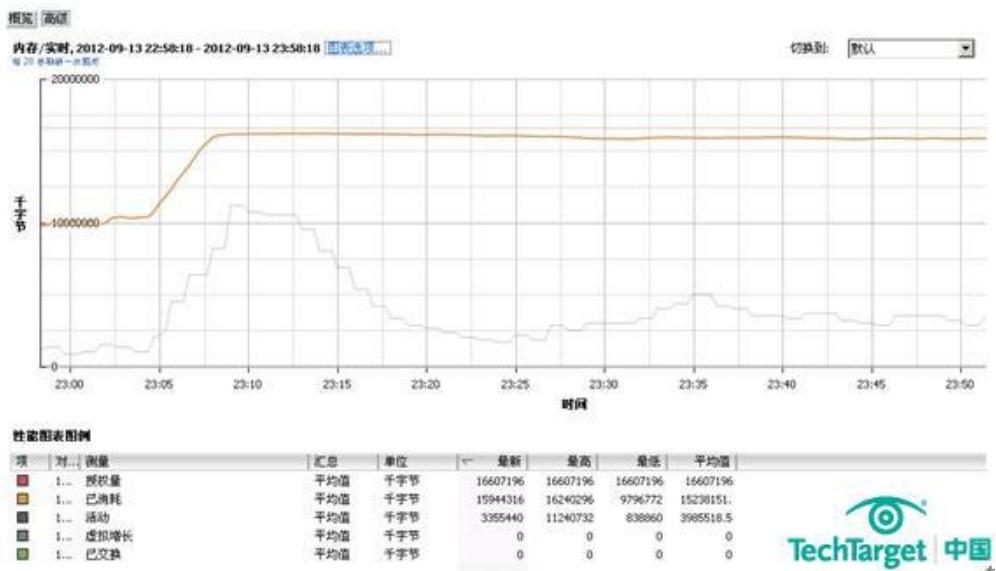


图 5. 利用性能监视图表查看虚拟机内存使用情况

虚拟机内存调整建议

在了解了 ESXi 主机、虚拟机内存的构成及相关概念并获取了虚拟机内存的动态性能视图后，我们就可以对虚拟机的内存进行调整了，本文给出的虚拟机内存调整建议如下：

(1) 我们应该针对虚拟机的运行情况对虚拟机的内存进行调整：在创建虚拟机时，为虚拟机配置的内存大小（图 5 中虚拟机内存的授权量）必须稍大于客户机内存平均使用情况（图 5 虚拟机内存中已消耗大小），这将使虚拟机能够适应工作负载高峰，而无需在客户机之间交换内存。

(2) 不应该为虚拟机分配过大的内存大小，这将导致更多内存使用情况开销，如图 4 中虚拟机的内存开销已经达到了 1.13GB。

(3) 如果内存释放活动（图 5 中虚拟增长参数）幅度大，但所有虚拟机的内存充足，则说明虚拟机并未受到内存方面的限制。如果内存释放活动幅度大，且客户操作系统正在交换内存（图 5 中已交换参数），那么说明虚拟机已经受到了内存方面的限制，此时要分两种情况考虑：

1. 如果 ESXi 主机的可用内存等于或少于 6%，则表示 ESXi 主机无法满足内存需求，这将导致可能会降低性能的内存回收，此时应该将运行的虚拟机迁移到集群中的其他主机中。

2. 如果 ESXi 主机具有足够的可用内存，则在主机上检查虚拟机和资源池的资源份额、预留和限制。确保主机设置的值足够大，而且不低于为虚拟机设置的相应值。

增强虚拟机性能建议

(1) 如果为虚拟机配置的内存太大，则应减少为虚拟机配置的内存大小，并更改缓存大小，这将为其他虚拟机提供更多的内存。

(2) 如果虚拟机的内存预留值设置大大高于活动内存设置，则减少预留设置，以便 VMkernel 可以回收空闲内存供主机上其他虚拟机使用。

(3) 验证是否在虚拟机上安装了 VMware Tools。虚拟增长驱动程序与 VMware Tools 一起安装，它对性能而言至关重要。

(4) 验证是否启用了虚拟增长驱动程序。通过虚拟增长和交换，VMkernel 定期回收没有使用的虚拟机内存，通常这不影响虚拟机性能。

(5) 将一个或多个[虚拟机迁移](#)到群集中的其它主机上。

(6) 如果上述措施都不能解决问题，那么可以考虑为 ESXi 主机增加物理内存了。

从内存告警谈 ESXi 主机内存管理——内存构成

在《[如何处理 ESXi 主机的黄色告警](#)》一文中我们提到了在没有冗余的管理网络或启用 SSH 的情况下，ESXi 主机图标右下方将会出现黄色的告警。除了上述配置导致告警之外，另一种常见的告警就是 ESXi 主机的内存使用率过高。

ESXi 主机内存告警

当 ESXi 主机的内存使用率过高时，将会在警报选项卡下的“已触发的警报”选项卡下看到“主机内存使用情况的告警”。通过“定义”选项卡，我们可以看到 [vSphere](#) 中预先定义的“主机内存使用情况”告警信息。右键单击“主机内存使用情况”，在弹出的右键菜单中选择“查看设置”，将弹出如下图 1 所示警报设置对话框。定位到“触发器”选项卡下，可以看到当主机内存使用率超过 90% 后，将会触发黄色告警，当主机内存使用率超过 95% 后将触发红色警示。



图 1. ESXi 主机预定义的内存使用情况告警

请注意：ESXi 主机内存瞬间的高使用率通常不会导致性能降低。例如同时启动多个虚拟机或虚拟机工作负载中出现高峰时，内存使用情况可能较高。但是持续较高的内存使用情况值（94% 或更高）则表示主机可能缺少满足要求所需要的内存。

首先让我们了解一下 [ESXi 主机](#) 的内存构成。

ESXi 主机内存构成

服务器内存：服务器内存大小指的是为物理服务器配置的内存大小。VMkernel 管理所有的服务器内存，VMkernel 会将这种受管服务器内存的一部分拿来自己使用，剩余的内存可供虚拟机使用。

系统内存：由于 ESXi 是安装在服务器上的虚拟化操作系统，所以其本身也要使用一部分内存，我们将这部分内存称为系统内存。系统内存的大小通常为几百兆。

虚拟机内存：除系统内存之外，服务器内存都可供虚拟机使用，我们将服务器内存除去系统内存之外的部分称为虚拟机内存。

如下图 2 所示，在 ESXi 主机的配置选项卡下的“内存”选项卡下我们可以看到服务器内存为 65532.7MB，系统内存为 322.7MB，虚拟机可以使用的内存为 65210.0MB。系统内存与虚拟机内存的总和恰好等于服务器内存大小。



图 2. ESXi 主机内存构成

虚拟机内存构成

从图 2 可以看出，虚拟机内存占据了服务器内存的绝大部分。既然虚拟机使用了绝大多数内存资源，那么我们如何查看每台虚拟机所使用的内存情况呢？只要单击“虚拟机”选项卡，就可以看到在当前 ESXi 主机上运行的所有虚拟机了。如下图 3 所示，单击“主机内存-MB”标签，我们可以按照虚拟机内存使用量大小由高到低排序，可以看到目前使用内存最多的虚拟机所使用的主机内存为 12195MB。

ESXi, 5.0.0, 469512						
	性能	配置	任务与事件	警报	权限	映射
	存储视图	Hardware Status				
1	状况	状态	设备的空间	已用空间	主机 CPU - MHz	主机内存 - MB
nter_Orade	已打开电源	正常	166.05 GB	82.18 GB	1248	12195
ing	已打开电源	正常	215.17 GB	66.33 GB	72	5269
-lukiang	已打开电源	正常	116.05 GB	71.20 GB	384	4031
6.1	已打开电源	正常	144.65 GB	36.98 GB	48	5966
OS	已打开电源	正常	166.05 GB	38.91 GB	96	2736
ter	已打开电源	正常	96.05 GB	35.92 GB	288	3656
			48.05 GB	48.05 GB		3895

图 3. 虚拟机内存使用情况

如果要查看这一台虚拟机内存详细的使用情况，我们可以选定这台虚拟机，在其资源分配选项卡下看到内存的详细信息。

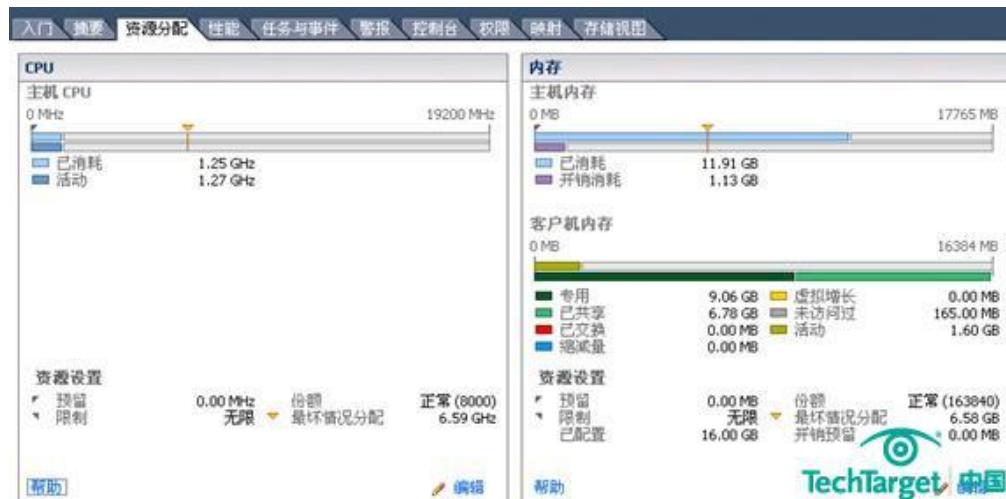


图 4. 虚拟机内存详细信息

这里我们重点谈到了 ESXi 主机内存构成和虚拟机内存构成，之后我们会继续介绍每台虚拟机的内存包括的两个方面的内容：主机内存、客户机内存。

VMware ESXi 安全六问六答：保卫 hypervisor 与主机

保卫你的 VMware 架构安全是个多层的过程：需要保护 ESXi 主机、虚拟机和 hypervisor 本身。VMware ESXi 在 [vSphere 5](#) 中占据主导地位，这个 hypervisor 伴随着新的 ESXi 安全考虑。

有多种方式保卫 VMware ESXi 的安全。要正确选择 ESXi 防火墙，添加网络安全，锁定用户账户，这些都非常重要。因此了解 vSphere 5 里的新安全功能是必须滴。

以下几个关于 [VMware ESXi 安全](#) 的问答有助于你了解需要保护的所有组件，加固你的架构，并熟悉一些新的 VMware 安全功能。

关于 VMware ESXi 安全你该关注什么？

ESXi 自身非常安全。像 VMware ESXi 这样的 [Type 1 hypervisor](#) 不是运行在主机操作系统上，这意味着操作系统不需要额外的保护。不过要启动 ESXi 安全，可以手动配置一些额外的 VMkernel 设置。你也应该确保 ESXi 网络的不同部分彼此独立，保护独立虚拟机的安全。

vSphere 5 安全有啥新鲜事？

你可能已听说 VMware 更新了 [vShield 5](#) 种的安全套件，但新的虚拟化平台也提供登录改进、ESXi 防火墙和安全部署 ESXi 的新方式。要启动 vSphere 安全，Auto Deploy 功能能帮助你一次部署大量主机，并使用 Host Profiles 配置这些主机确保一致性。例如，有了 [Auto Deploy](#) 后，可以确保一个集群中所有 ESXi 主机的防火墙设置是相同的。

我如何确保 ESXi hypervisor 安全？

通过实施物理与虚拟防火墙，最大程度确保 VMware hypervisor 安全。也要确保分配主机资源，防止单个虚拟机过量消耗导致断电。所以可以创建资源池并分配给每台虚拟机。在 vSphere 5 中，[Storage I/O Control](#) 与 Network I/O Control 功能提供额外的资源池。

每次只让一个用户访问一个虚拟机的控制台，这样也能确保 hypervisor 安全，这种情况发生在远程用户同时连接的时候。最后，不要让管理员拥有太多权

限。在 ESXi 主机上创建特殊用户账号并锁定 Mode，阻止他们通过 API、命令行工具与 [vSphere Client](#) 直接访问。

我需要关注哪些 VMware 安全漏洞？

有些区域黑客能轻易渗透：主机管理控制台、ESXi 远程控制台、虚拟机数据存储与网络。如果有人在数据存储中访问虚拟机磁盘文件的话，他们就可以拷贝整个虚拟机并在任何地方都能下载。要避免 VMware 安全漏洞，你也需要保护虚拟网络。当在虚拟 LAN 之间移动虚拟机时，服务器与网络组之间的错误传达会导致不正确的配置。

VMware 用户账户如何提供 ESXi 安全？

为每台主机创建用户账户并自定义这些账户能加强 ESXi 安全。VMware 有个默认的账户，但最好添加新的，有特权的账户。以便监控每台主机上谁在做什么。自定义 VMware 用户账户的过程很简单，可以分配权限给单个用户或用户组。

如何配置 VMware ESXi 防火墙？

vSphere 5 引入了新的 ESXi 防火墙，可与 vSphere Client 或命令行一起配置。默认下，这种无状态的防火墙不像 ESX Server 防火墙那样，为服务定义端口规则。VMware ESXi 防火墙还能指定（一系列）IP 地址，使得远程主机也能访问每个服务。