



VMware ESX Server

Third-Party Software in the Service Console

In general, VMware recommends that users avoid running third-party software in the VMware ESX Server service console. Clear exceptions to this policy are software packages explicitly identified in ESX Server compatibility guides.

This technical note outlines the reasons for this recommendation and guidelines developers should follow when writing software to run in the ESX Server service console. It covers the following topics:

- [Background on the Recommendation on page 1](#)
- [Third-Party Software Guidelines on page 2](#)
- [Additional Notes for Users on page 3](#)
- [Notes for Independent Software Vendors on page 4](#)

Background on the Recommendation

Adhering to the policy of avoiding third-party software in the service console ensures better system reliability and future upgradeability.

VMware generally does not recommend that components be installed in the service console for the following reasons:

- The components may have unintended performance-related interactions with ESX Server.
- Over time, VMware may change (add, remove, or update) the components in the ESX Server service console, and third-party software may become incompatible as such changes occur.

A recommended alternative to installing software in the ESX Server service console is installing such software in a virtual machine running on each ESX Server host. In many cases, this provides equivalent functionality without the risk and impact of running the software in the service console.



Third-Party Software Guidelines

Third-party software in the service console must not modify any of the RPM files listed below, because these RPM files have been specially modified to suit the needs of VMware ESX Server. Future upgrades of ESX Server will definitely overwrite any changes that a third party makes to the files included in these RPMs.

- `VMware-*.rpm`
- `*vmw.rpm`
- `kernel-*`
- `busybox`
- `initscripts`
- `kudzu`
- `mkinitrd`
- `pam`
- `pam_passwdqc`
- `parted`
- `sysvinit`
- `tzdata`
- `util-linux`
- `mingetty`
- `rpm`
- `util-linux`

You may change the RPMs in the following list, but changing these may make your machine less secure or may have other side-effects on other processes in the service console. The normal operation of ESX Server does not depend on these modules. VMware has made changes solely to do things such as improve security (for example, disabling SSH as root user), remove library interdependencies, and remove setuid bits. Future upgrades of ESX Server are likely to overwrite any changes that a third party makes to the files included in these RPMs.

- `samba`
- `openssh`
- `vixie-cron`
- `iputils`
- `shadow-utils`

For all other RPMs — that is, those not included in either of the lists above — ESX Server does not have any special dependencies on them. Modify them at your own risk.



Additional Notes for Users

- X cannot be run on the ESX Server service console. VMware does not ship the X libraries
- `redhat-config-*` functions do not work in the ESX Server service console. VMware does not ship them. If you try to install them, they will not work properly and may interfere with proper ESX Server operation because ESX Server uses its config files (in `/etc`) in a different way than the standard RedHat utilities.
- VMware Virtual Machine File System (VMware VMFS) is not like a normal, local file system. Do not treat `/vmfs` like a general-purpose file system. For example, do not store temporary or data files under `/vmfs`. Operations such as `chmod`, `chown`, and any commands that use the `open()` function or that otherwise modify file properties that are very fast on normal nondistributed file systems are significantly more costly on distributed file systems like VMware VMFS. Avoid these operations unless absolutely necessary. For example, as a result of the high expense of `open()` calls, `tail -f file` is relatively safe, but `watch tail file` can cause problems.
- For checking free space on the VMware VMFS file system, `df` doesn't work, so VMware provides `vdF` instead.
- For performance and data placement reasons, do not use `scp` or `cp`; instead, use `vmkfstools`, the Virtual Machine Importer tool from VMware, or the SDK APIs to manipulate your virtual disks. You should see very significant performance improvements if you use the recommended tools.
- Do not load kernel modules or unsupported device drivers into the service console. Such software may jeopardize stability of the service console and manageability of your ESX Server host.
- To archive a virtual machine or make a template, you can use VirtualCenter or use the `vmkfstools` command-line interface. If you use `vmkfstools`, VMware recommends that you use `vmkfstools -d thin` to make a space-efficient archive, and not `vmkfstools -d 2gbsparse`. VirtualCenter follows this same guideline.
- Do not do frequent operations like `ls -lR` to inventory the contents of a VMware VMFS file system. Use the SDK APIs to perform virtual machine inventories.
- Beware of filling up space on the root partition because doing so will affect the application of upgrades and patches. If the file system is completely filled, you will not be able to manage the ESX Server host using VI Client. Keep at least several hundred MB free, and be sure to proactively test an ESX Server upgrade if you feel that you may be consuming too much disk space.
- Third-party software must live within the compute resources available within the ESX Server service console, including CPU, memory, disk, and network resources. Specifically, it must not
 - Consume CPU cycles at a sustained rate for more than a few seconds in such a way that it starves other service console processes (as measured by the `top` command in the service console).
 - Have such a large memory footprint that the service console has to swap. By default, 272MB of RAM is allocated to the service console and is shared by all the processes running within the service console. You can use the `vmstat` command in the service console to determine whether the service console is swapping. You can increase the



RAM allocated to the service console through an advanced setting option on a host using the VI Client user interface.

- Write to disk at sustained rates for more than a few seconds.
- Consume network resources for more than a few seconds

Violating any of the above could

- Affect performance or severely inhibit your ability to use the VI Client or Web Access to manage the ESX Server host, including all operations from those user interfaces such as starting, stopping, and snapshotting virtual machines.
- Cause VirtualCenter to lose its connection to manage the ESX Server host.

Notes for Independent Software Vendors

VMware recommends that, if possible, you use standard APIs such as the VMware Software Development Kit or CIM SMI-S or SNMP to access VMware management information. Doing so will allow your software to avoid the need to run directly within the ESX Server service console.

As an alternative to running in the service console, run your software in a virtual machine. If your software is Linux-based, you can redistribute a virtual machine (a virtual machine's hard disk is represented as a single, large file) with your software preinstalled.

The only circumstance in which you might have to resort to running the software within the ESX Server service console is when you require direct access to hardware.

Contact the VMware alliance group for additional documentation, white papers, and guidance regarding how to manage VMware Infrastructure.