

vSphere Management Assistant Guide

vSphere 4.0

EN-000116-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

© 2008, 2009 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware, the VMware “boxes” logo and design, Virtual SMP, and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.

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

Contents

Contents	3
About This Book	5
1 Introduction to vMA	7
vMA Capabilities	7
vMA Component Overview	7
vSphere Authentication Component	8
vSphere Logging Component	9
vMA Samples	9
vMA Use Cases	9
Writing or Converting Scripts	9
Writing or Converting Agents	10
2 Getting Started with vMA	11
Hardware and Software Prerequisites	12
vMA Prerequisites and Capabilities	12
Required Authentication Information	12
Deploy vMA	13
Configure vMA	13
Enable the vi-user Account	14
Add Target Servers to vMA	15
Add Multiple Target Servers	16
Remove Target Servers from vMA	17
Modifying Scripts	17
Shut down vMA	18
Delete vMA	18
Troubleshooting vMA	19
3 vMA Interfaces	21
vMA Interface Overview	21
vifpinit Command for vi-fastpass Initialization	22
vifp Target Management Commands	22
vifp addserver	22
vifp removeserver	23
vifp rotatepassword	24
vifp listservers	25
Target Management Example Sequence	25
vilogger Daemon and Log Management Commands	26
Management Service Interface for vilogd	26
vilogger enable	26
vilogger disable	27
vilogger updatepolicy	28
vilogger list	28
Using the vifplib Library	29
vifplib Reference	29

Enumerating Targets	29
Querying Targets	30
Programmatic Login	30
Appendix: Updating vMA with vima-update	31
Introduction to vima-update	31
Use vima-update	31
Use vima-update with Update Depots	32
vima-update Troubleshooting	32
Index	33

About This Book

The VMware® vSphere Management Assistant (vMA) is a virtual machine that includes prepackaged software such as a Linux distribution, the vSphere command-line interface (CLI), and the vSphere SDK for Perl. Administrators can use vMA to run scripts and agents to manage ESX/ESXi and vCenter Server systems.

The *vSphere Management Assistant Guide* explains how to install and use vMA and includes reference information for vMA CLIs and libraries.

To view the current version of this book, as well as all VMware API and SDK documentation, go to http://www.vmware.com/support/pubs/sdk_pubs.html.

Revision History

This book, the *vSphere Management Assistant Guide*, is revised with each release of the product or when necessary. A revised version can contain minor or major changes. [Table 1](#) summarizes the significant changes in each version of this book.

Table 1. Revision History

Revision	Description
21MAY2009	vMA 4.0 documentation
27OCT2008	VIMA 1.0 documentation

Intended Audience

This book is for administrators and developers with some experience setting up a Linux system and working in a Linux environment. Administrators can use the vMA automated authentication facilities and the software packaged with vMA to interact with ESX/ESXi hosts and vCenter Server systems. Developers can create agents that interact with ESX/ESXi hosts and vCenter Server systems.

Document Feedback

VMware welcomes your suggestions for improving our documentation. Send your feedback to docfeedback@vmware.com.

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current versions of other VMware books, go to <http://www.vmware.com/support/pubs>.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to <http://www.vmware.com/support>.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to <http://www.vmware.com/support/services>.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to <http://www.vmware.com/services>.

Introduction to vMA

The vSphere Management Assistant (vMA) is a virtual machine that includes prepackaged software such as a Linux distribution, the vSphere command-line interface, and the vSphere SDK for Perl. vMA allows administrators to run scripts or agents that interact with ESX/ESXi and vCenter Server systems without having to explicitly authenticate each time. vMA can also collect ESX/ESXi and vCenter Server logging information and store the information on vMA for analysis.

This chapter introduces vMA and explores usage scenarios. The chapter includes the following topics:

- [“vMA Capabilities”](#) on page 7
- [“vMA Component Overview”](#) on page 7
- [“vMA Use Cases”](#) on page 9

To get started with vMA right away, go to [“Getting Started with vMA”](#) on page 11.

vMA Capabilities

vMA supports administrators of ESX/ESXi and vCenter Server systems by offering a flexible and authenticated platform for running scripts and programs.

- vMA supports the following targets:
 - vMA supports vCenter Server targets. If you set up an authenticated vCenter Server target, you can run most commands on all ESX/ESXi hosts that vCenter Server system manages without additional authentication.
 - vMA supports a single ESX/ESXi target or multiple ESX/ESXi targets. When you set up multiple ESX/ESXi targets, you can interact with all target servers without additional authentication.
- vMA facilitates reuse of service console scripts that are currently used for ESX administration, though minor modifications to the scripts are usually necessary.
- vMA comes preconfigured with two accounts, vi-admin and vi-user. When you log in to vMA as vi-user, you can perform only tasks on ESX/ESXi target servers that do not require administrative privileges. For vCenter Server targets, log in as vi-admin in all cases.

Agents that make proprietary hardware or software components compatible with VMware ESX currently run in the service console of existing ESX servers. You can modify most agent code to run in vMA, calling the vSphere API and CIM providers if necessary. Developers must move any agent code that directly interfaces with hardware into a CIM (Common Information Model) provider.

vMA Component Overview

When you accept the vMA End User License Agreement (EULA) and install vMA, you are licensed to use the resulting virtual machine that includes all vMA components. You can use the `vima-update` utility from inside vMA to download updates and VMware components, including the operating system. See [“Appendix: Updating vMA with vima-update”](#) on page 31.

The following components are included in vMA.

- 64-bit Enterprise Linux compatible with Red Hat Enterprise Linux (RHEL) 5.2 and CentOS 5.2 – While the ESX service console runs on the ESX host, vMA runs Linux on the virtual machine. You can move files from the ESX/ESXi host to the vMA console (and back) using the `vi fs vSphere CLI` command.
- VMware Tools – Interface to the hypervisor.
- vSphere CLI – commands for managing vSphere from the command line. See the *vSphere Command-Line Interface Installation and Reference Guide*.
- vSphere SDK for Perl – Client-side Perl framework that provides an easy-to-use scripting interface to the vSphere API. The SDK includes utility applications and samples for many common tasks.
- SMI-S – vMA includes the VMware implementation of the CIM profiles compatible with the Storage Management Initiative Specification (SMI-S version 1.0.2) of the Storage Network Industry Association. With vMA 4.0, you can specify ESX/ESXi and vCenter Server systems as target servers. The script that establishes the SMI-S target server uses the credential store and not the vMA authentication mechanism (`vi-fastpass`).
- Java JRE version 1.5 – Runtime engine for Java-based applications built with the vSphere Web Services SDK.

An SNMP Server that enables monitoring of vMA is included. vMA does not export any configuration using SNMP and does not export or proxy SNMP information about its target servers. The SNMP Server supports the following core SNMP MIBs:

- RFC 3418 – SNMPv2-MIB
- RC 2863 – IF-MIB
- RFC 4293 – IP-MIB
- RFC 2790 – HOST-RESOURCES-MIB

vMA also includes an authentication component (`vi-fastpass`) and a logging component (`vi-logger`).

vSphere Authentication Component

By default vSphere CLI commands and vSphere SDK for Perl scripts running in vMA or from a system on which the package is installed must specify authentication information, either on the command line or by other means.

The vMA authentication component, `vi-fastpass`, supports unattended authentication to an ESX/ESXi or vCenter Server system. After `vi-fastpass` has been enabled, applications can use the vSphere CLI, the vSphere SDK for Perl, or the vSphere Web Services SDK without user intervention. Applications can also use the SMASH Server Management APIs, either directly or through the Web Services for Management Perl interface. These applications can be unattended cron jobs that wake up intermittently to collect data or perform operations on an ESX/ESXi or vCenter Server system.

When you add an ESX/ESXi system as a target server, `vi-fastpass` creates two users with obfuscated passwords on the target server:

- `vi-admin` (administrator privileges)
- `vi-user` (read-only privileges)

`vi-fastpass` stores the obfuscated password information for the target server on vMA.

NOTE The passwords are obfuscated, not encrypted.

After the target server has been added, you must initialize `vi-fastpass`. Use one of the following methods:

- Run `vi fpinit`.
- Call `LoginByFastpass` in a Perl or Java program.

If the target server is an ESX/ESXi system, you can then run vSphere SDK for Perl scripts and vSphere CLI commands or scripts against ESX/ESXi systems without additional authentication. If the target server is a vCenter Server system, you can run vSphere SDK for Perl scripts and most vSphere CLI commands against any ESX/ESXi hosts managed by that vCenter Server system. Use the `--vhost` option to specify the ESX/ESXi system to run against.

Target servers remain targets across reboots, but initialization with `vi fpinit` or `LoginByFastpass` is required each time you log out and log in again.

vSphere Logging Component

The vSphere logging component, `vi-logger`, collects log files from target ESX/ESXi hosts according to the specified log policy. `vi-logger` consists of a log daemon (`vi logd`) that collects and processes log files and the `vi logger` CLI that supports logger configuration.

The log daemon starts when vMA boots. The daemon starts collecting logs when logging is enabled on a specified target server for a specified log. The daemon does not download logs that were created before logging was enabled on vMA. The daemon wakes up periodically to retrieve log information according to the log policy. If the time difference between the ESX/ESXi host and vMA is more than one second, the log daemon adjusts the time stamps in the log to correspond to the vMA time and time zone. If the ESX/ESXi host and vMA are time synchronized, no time stamp adjustment is necessary.

By default, `vi logd` places the logs in `/var/log/vmware`. To specify a different log location, change the `/etc/vmware/viconfig/vilogdefaults.xml` file. `vi logd` places the logs in the new location if `vi-admin` has access to it.

vMA Samples

vMA samples illustrate the vMA CLIs and the `vi plib` library. The samples are available in vMA at `/opt/vmware/vima/samples`. Each sample includes a README file.

- `vi top` – Java example that shows the CPU, memory, disk, and network resources consumed by each ESX/ESXi target server and the number of virtual machines running on the target server. This sample does not support vCenter Server system targets.
- `multiversion.pl` – Perl example that displays the version for all vMA targets without requiring a user name or password. This sample supports both ESX/ESXi targets and vCenter Server system targets.
- `bulkAddServers.pl` – Perl sample that adds multiple targets to vMA.
- `mcli.pl` – Perl sample that runs a vSphere CLI command on multiple vMA targets specified in a file supplied as an argument. You must run `vi fpinit` before running this script.

vMA Use Cases

This section lists a few typical use cases.

Writing or Converting Scripts

Partners and customers can run existing vSphere CLI or vSphere SDK for Perl scripts from vMA. To set target servers and initialize `vi-fastpass`, the script can use the `login_by_fastpass` command, which is available in Perl and Java. If the target server is a vCenter Server system, all ESX/ESXi hosts managed by that system become `vi-fastpass` targets.

Writing or Converting Agents

Partners or customers can use vMA to write or convert agents.

- A partner or customer writes a new agent in Perl.

When a partner or customer writes a new agent in Perl, the Perl script must import the `vifplib` Perl module and all vSphere SDK for Perl modules. Instead of calling the vSphere SDK for Perl subroutine `Util::Connect(targetUrl, username, password)`, the agent calls `Vifplib::LoginByFastpass(targetServerName)`. The server that `targetServerName` represents must be a vMA target.

- A partner or customer runs an agent written in Perl or Java in the service console and wants to port the agent to vMA.

The agent uses code similar to the following Perl-like pseudo code to log in to ESX/ESXi hosts:

```
LoginToMyEsx() {
  SessionManagerLocalTicket tkt = SessionManager.AcquireLocalTicket(userName);
  UserSession us = sm.login(tkt.userName, tkt.passwordFilePath);
}
```

The partner changes the agent to use code similar to the following pseudo-code instead:

```
LoginToMyEsx() {
  hostname[] = vifplib.EnumerateHosts();
  UserSession us = vifplib.LoginByFastpass(hostname[0]);
}
```

This pseudo-code assumes only one vMA target. For multiple target servers, the code can specify any target server or loop through a list of target servers.

- A partner or customer runs an agent written in Perl outside the ESX/ESXi system and ports the agent to vMA.

Instead of calling the vSphere SDK for Perl method `Util::Connect()`, the agent calls the `vifp` library method `Vifplib::LoginByFastpass()`.

Getting Started with vMA

Administrators who set up vMA, you should have some experience setting up a Linux system and working in a Linux environment. This chapter explains how to deploy and configure vMA, how to add and remove target servers, and how to prepare and run scripts. The chapter also includes troubleshooting information.

Read [Chapter 1, “Introduction to vMA,”](#) on page 7 for background information on vMA functionality and available vMA components.

IMPORTANT You cannot upgrade a vMA 1.0 system to vMA 4.0.

This chapter includes the following topics:

- [“Hardware and Software Prerequisites”](#) on page 12
- [“vMA Prerequisites and Capabilities”](#) on page 12
- [“Required Authentication Information”](#) on page 12
- [“Deploy vMA”](#) on page 13
- [“Configure vMA”](#) on page 13
- [“Enable the vi-user Account”](#) on page 14
- [“Add Target Servers to vMA”](#) on page 15
- [“Add Multiple Target Servers”](#) on page 16
- [“Remove Target Servers from vMA”](#) on page 17
- [“Modifying Scripts”](#) on page 17
- [“Shut down vMA”](#) on page 18
- [“Delete vMA”](#) on page 18
- [“Troubleshooting vMA”](#) on page 19

Hardware and Software Prerequisites

To set up vMA, you must have the following hardware and software:

- ESX/ESXi host – Because vMA runs a 64-bit Linux guest operating system, the ESX/ESXi host on which it runs must support 64-bit virtual machines.

The ESX/ESXi host must have one of the following CPUs:

- AMD Opteron, rev E or later
- Intel processors with EM64T support with VT enabled.

Opteron 64-bit processors earlier than rev E, and Intel processors that have EM64T support but not VT support enabled, do not support a 64-bit guest operating system. For detailed hardware requirements, see the *Hardware Compatibility List*.

- vSphere Client – You need a vSphere Client for deploying vMA.

vMA Prerequisites and Capabilities

You can deploy vMA on the following systems:

- vSphere 4.0 – You can deploy vMA to ESX/ESXi systems using a vSphere Client connected directly to the ESX/ESXi system or using a vSphere Client connected to a vCenter Server 4.0 system.
- ESX/ESXi 3.5 Update 2 and later – You can deploy on ESX/ESXi 3.5 Update 2 or later using a vSphere 4.0 Client.

You can use vMA to target ESX/ESXi 3.5 Update 2 or later, ESX/ESXi 4.0, or vCenter Server 4.0 systems.

By default, vMA uses one virtual processor. 5GB of storage space is required for the vMA virtual disk. 512MB of memory is recommended for vMA.

At runtime, the number of targets a single vMA instance can support depends on how it is used. Factors that affect the number of targets include how many log files vMA is collecting, how often vMA updates the log files, and how often data are added to those log files. Those factors depend on how you set up logging from vMA and on the level of activity on the host. vMA has been tested with over 100 targets under normal load conditions.

Required Authentication Information

Before you begin vMA configuration, obtain the following user name and password information:

- vCenter Server system – If you want to use a vCenter Server system as the target server, you must be able to connect to that system. You do not need that authentication information when you remove the vCenter Server target host.

If you are using a vCenter Server target, you do not need passwords for the ESX/ESXi systems that vCenter Server system manages, unless you run commands that do not support vCenter Server targets.

- ESX/ESXi host – You must have the root password or the user name and password for a user with administrative privileges for each ESX/ESXi host you add as a vMA target. You must have the same authentication information when you remove a target host.
- vMA – When you first log in to vMA, vMA prompts for a password for the vi-admin user. Specify a password and remember it for subsequent logins. The vi-admin user has root privileges on vMA.

IMPORTANT The root user account is disabled on vMA. To run privileged commands, type `sudo <command>`. By default, only vi-admin can run commands that require `sudo`.

By default, `vi fp` commands do not require a password even though they are `sudo` commands. See your Linux documentation for information about changing that default.

Deploy vMA

You can deploy vMA using a file or from a URL. To deploy from a file, download and unzip the vMA ZIP file before you start the deployment process.

IMPORTANT You cannot upgrade from VIMA 1.0 to vMA 4.0. You must deploy the vMA 4.0 OVF instead.

To deploy vMA

- 1 Log in to a 4.0 vSphere Client connected to an ESX/ESXi 4.0, ESX/ESXi 3.5 Update 2 or later, or vCenter Server 4.0 system.
- 2 If connected to a vCenter Server system, select the host to which you want to deploy vMA in the inventory pane.
- 3 Select **File > Deploy OVF Template**.
The Deploy OVF Template wizard appears.
- 4 Select one of these options:

Option	Description
Deploy from file	Select this option if you have already downloaded and unzipped the vMA virtual appliance package. Click Browse , select the OVF, and click Next .
Deploy from URL	Select this option and click Next . Type http://www.vmware.com/go/importvma/vma4.ovf into the field and click Next .

- 5 Click **Next** when the download details are displayed.
- 6 Accept the license agreement.
- 7 Specify a name (optional) and select a location for the virtual machine when prompted.
If you are connected to a vCenter Server system, you can select a folder.
- 8 If connected to a vCenter Server system, select the resource pool for the virtual machine.
You can leave the default, which is the top-level root resource pool.
- 9 If prompted, select the datastore to store the virtual machine on and click **Next**.
- 10 Select the network mapping and click **Next**.

IMPORTANT Make sure vMA is connected to the management network on which the vCenter Server and ESX/ESXi systems that are intended vMA targets are located.

- 11 Review the information and click **Finish**.

The wizard deploys the vMA virtual machine to the host that you selected. The deploy process can take several minutes.

Next you configure your vMA virtual machine. You perform this task when you log in to vMA the first time.

Configure vMA

When you start the vMA virtual machine the first time, vMA prompts you for the following information:

- Host name for vMA.
- Network configuration for the virtual machine: IP address, subnet mask, DNS Server, and gateway.
By default, vMA uses DHCP.
- Password for the vi-admin user.

After the information has been specified, vMA is considered configured.

To configure vMA

- 1 In the vSphere Client, right-click the virtual machine, and click **Power On**.
- 2 Select the **Console** tab.
- 3 Answer the network configuration prompts.

If multiple network adapters are on the host, you can later use the vSphere Client to add a second network adapter to vMA.

- 4 When prompted, specify a host name for vMA.

The name can include alphanumeric characters and cannot be longer than 64 characters.

You can later change the vMA host name by modifying the `/etc/sysconfig/network` file, as you would for any Linux host.

- 5 When prompted, specify a password for the vi-admin user on this virtual machine.

This user has root privileges.

The prompt uses the Linux `passwd` utility:

- If you specify a password considered insecure, for example, a dictionary word or a word with less than six characters, a `Bad Password` message is displayed. Choose a different password. For information about requirements for secure passwords, search the Internet for “Linux secure password.”
- You can use special characters directly at the prompt. You do not need to precede special characters with escape characters or surround words that contain special characters in quotes.

You can later change the password for the vi-admin user using the Linux `passwd` command.

vMA is now configured and prompts you to log in as vi-admin. As vi-admin, you can add servers to vMA and run commands from the vMA console.

Enable the vi-user Account

As part of configuration, vMA creates a vi-user account. Initially, that user has no password. You cannot use the vi-user account until you have specified a vi-user password.

IMPORTANT The vi-user account has limited privileges on target ESX/ESXi systems and cannot run any `vi logger` commands or any commands that require sudo execution. “[vMA Interfaces](#)” on page 21 lists `vi logger` commands and indicates which commands require sudo execution.

On vCenter Server targets, vi-user is not supported. Log in as vi-admin.

To enable the vi-user account

- 1 Log in to vMA as vi-admin.
- 2 Run the Linux `passwd` command for vi-user as follows:

```
sudo passwd vi-user
```

If this is the first time you use `sudo` on vMA, an information message about root user privileges appears, and you are prompted for the vMA root password.

You are prompted for the root password again after a certain time period has elapsed.

- 3 (Optional) If you are prompted for the vMA root password, specify the vi-admin password.
- 4 When prompted, type and confirm the password for vi-user.

After vi-user has been enabled on vMA, that account has normal privileges on vMA but is not in the sudoers list.

When you add ESX/ESXi target servers, vMA creates two users on each target:

- vi-admin has administrative privileges on the target system.
- vi-user has read-only privileges on the target system. vMA creates vi-user on each target that you add, even if vi-user is not currently enabled on vMA.

When a user is logged in to vMA as vi-user, vMA uses that account on target ESX/ESXi hosts, and the user can run only commands on target ESX/ESXi hosts that do not require administrative privileges.

Add Target Servers to vMA

After you have configured vMA, you can add target servers. vMA supports target servers that run vCenter Server version 4.0 or ESX/ESXi version 3.5 Update 2 or later.

The following tasks illustrate how you add a target server. For vCenter Server system targets, you must have the name and password of a user who can connect to that system. For ESX/ESXi systems, you must have the root password.

See “[vifp addserver](#)” on page 22 for the complete syntax.

To add a vCenter Server system as a vMA target

- 1 Log in to vMA as the administrator user (vi-admin).
- 2 Run `addserver` to add a server as a vMA target.


```
sudo vifp addserver <servername>
```
- 3 Specify the name of a user privileged to connect to the vCenter Server system when prompted.


```
Enter username for pdp-dhcp189.eng.vmware.com: user1
```
- 4 Specify the password for that user when prompted.


```
user1@machine.company.com's password: <not echoed to screen>
```
- 5 Review and accept the security risk information.


```
This will store username and password in credential store which is a security risk. Do you want to continue?(yes/no): yes
```
- 6 Verify that the target server has been added. The display shows all target servers, in the following example, two ESX hosts, one ESXi host, and one vCenter Server system.


```
vifp listservers
server1.mycomp.com      ESX
server2.mycomp.com      ESX
server3.mycomp.com      ESXi
vc42.mycomp.com         vCenter
```
- 7 Initialize vi-fastpass:


```
vifpinit <targetserver>
```

If there is only one target server, you do not have to specify it.
- 8 Verify that you can run a vSphere CLI command without authentication by running a command on one of the ESX/ESXi hosts, for example:


```
vicfg-nics -l --vihost <esx_host>
```

The command completes without prompting for authentication information.

IMPORTANT If the name of a target server changes, you must remove the target server using `vifp removeserver` with the old name, then add the server using `vifp addserver` with the new name.

To add an ESX/ESXi host as a vMA target

1 Log in to vMA as the administrator user (vi-admin).

2 Run `addserver` to add a server as a vMA target:

```
sudo vifp addserver <servername>
```

You are prompted for the root user password for the target server.

```
root@<servername>'s password:
```

3 Specify the root password for the ESX/ESXi host that you want to add.

vMA does not retain the root password. Instead, vMA adds vi-admin and vi-user users to the ESX/ESXi host and stores the obfuscated passwords it generates for those users in the VMware credential store.

In a vSphere Client connected to the target server, the Recent Tasks panel displays information about the users that vMA adds. The target server's Users and Groups panel displays the users if you select it.



CAUTION Do not remove users added by vMA from the target server, unless you deleted the vMA virtual machine and forgot to remove the target servers.

4 Verify that the target server has been added:

```
vifp listservers
```

5 Initialize vi-fastpass for use of vSphere SDK for Perl and vSphere CLI scripts on the target server.

```
vifpinit <servername>
```

The server name is optional.

6 Verify that you can run a vSphere CLI command without authentication by running a command, for example:

```
vicfg-nics -l
```

IMPORTANT If the name of a target server changes, you must remove the target server using `vifp removeserver` with the old name, then add the server using `vifp addserver` with the new name.

Add Multiple Target Servers

If you add a single target server to vMA and initialize vi-fastpass, vSphere CLI commands and vSphere SDK for Perl scripts that you run on vMA are executed against that server.

If you have added a multiple target servers, vMA executes commands against the first server that you added by default. It is best to specify the server explicitly when running commands.

To use multiple target servers

1 Add the first server.

```
sudo vifp addserver <server1>
```

2 Add a second server and run `vifpinit`.

```
sudo vifp addserver <server2>
vifpinit
```

The command initializes all current target servers.

NOTE Running `vifpinit` always initializes all current target servers. If you add multiple servers in sequence, you do not have to call `vifpinit` for each server.

3 Run vSphere CLI or vSphere SDK for Perl scripts, specifying the server to run the command against but not the authentication information. For example:

```
vicfg-nics --server server2 --list
```

Remove Target Servers from vMA

Before you delete a vMA virtual machine, remove all target servers from vMA. If you do not remove target ESX/ESXi servers, the vi-admin and vi-user users remain on the target servers.

To remove a vCenter Server system from vMA

- 1 Log in to vMA as a user with connection privileges.
- 2 Run `removeserver` once for each vCenter Server system that is a vMA target.

```
sudo vifp removeserver <servername>
```

The vCenter Server system is no longer a vMA target.

To remove an ESX/ESXi host from vMA

- 1 Log in to vMA as the administrator user (vi-admin).
- 2 Run `removeserver` once for each server that is a vMA target.

```
sudo vifp removeserver <servername>
```

You are prompted for the root password for that server as follows:

```
root@<servername>'s password:
```

- 3 Specify the root password for the server you want to remove.

The Recent Tasks panel of the target server displays information about the vi-admin and vi-user users being removed. The Users and Groups panel of the target server no longer displays the users.

Modifying Scripts

You can modify service console scripts to run from vMA.

- **Linux commands** – Scripts running in vMA cannot use Linux commands in the way that they do on the ESX service console. The Linux installation is running on vMA, not on the ESX/ESXi host.
- **Access to ESX/ESXi files** – If you need access to folders or files on an ESX/ESXi host, you can make that host a target server and use the `vi fs vSphere` CLI command to view, retrieve, or modify folders and files.
- **References to localhost** – Scripts cannot refer to `localhost`.
 - If vMA has only one target server initialized for vi-fastpass, all commands apply to that target server.
 - If vMA has multiple target servers initialized for vi-fastpass, specify the host name or the IP address for the target server.
- **Programmatic connection** – In Perl scripts or Java programs, call `login_by_fastpass` and specify the host to connect to. The directory `/opt/vmware/vima/samples` contains examples in Perl and Java. vMA handles authentication if the server has been established as a target server. Programs can use `vifplib` library commands. See [“Using the vifplib Library”](#) on page 29.
- **No proc nodes** – Some service console scripts still use VMware `proc` nodes, which were officially made obsolete with ESX Server 3.0 and are not available in ESX/ESXi 4.0 and later. You can extract information that was available in VMware `proc` nodes using the vSphere CLI commands available on vMA.
- **Target specification** – You must specify the target server when you run commands or scripts.

You can use the following vMA components for modifying scripts that include `proc` nodes and Linux commands:

Table 2-1. vMA Components for Use in Scripts

vMA Component	Use	For more information
vSphere CLI commands	Manage ESX/ESXi hosts and virtual machines.	<i>vSphere Command-Line Interface Installation and Reference Guide.</i>
<code>vi fs</code> vSphere CLI command	Perform common operations, such as copy, remove, get, and put, on files and directories.	<i>vSphere Command-Line Interface Installation and Reference Guide.</i>
vSphere SDK for Perl	Access the vSphere API, a Web Services based API for managing, monitoring, and controlling the lifecycle of all vSphere components.	<i>vSphere SDK for Perl Programming Guide.</i>
vSphere SDK for Perl utility applications	Perform common administrative tasks.	<i>vSphere SDK for Perl Utility Applications Reference.</i> Commands are on vMA in <code>/usr/lib/vmware-vccli/apps</code>
vSphere SDK for Perl WS Management component	Access CIM/SMASH data. ESX/ESXi supports many Systems Management Architecture for Server Hardware (SMASH) profiles, enabling system management client applications to check the status of underlying server components such as CPU, fans, power supplies, and so on.	Documented in the <i>vSphere SDK for Perl Programming Guide.</i>

Shut down vMA

Before you power off vMA, shut down the virtual machine.

To shut down the vMA virtual machine

- 1 Shut down the operating system using a Linux command such as the `halt` command on the vMA command line.
- 2 Power off the vMA virtual machine using the vSphere Client.

Delete vMA

If you intend to deploy a newer version of vMA, or if you no longer need vMA, you can delete the vMA virtual machine.

IMPORTANT If you delete vMA without removing all servers, the `vi-admin` and `vi-user` users remain on the target ESX/ESXi hosts. The next time you add the host to a vMA instance, vMA creates a user name with a different numeric extension.

To delete the vMA virtual machine

- 1 Remove all vMA target servers you added. See [“Remove Target Servers from vMA”](#) on page 17.
- 2 Power off the virtual machine using the vSphere Client.
- 3 In the vSphere Client, right-click the virtual machine and select **Delete from Disk**.

Troubleshooting vMA

You can find troubleshooting information for all VMware products in VMware Knowledge Base articles and information about vMA known issues in the release notes. This section explains a few commonly encountered issues that are easily resolved.

Table 2-2. Troubleshooting vMA

Issue	Resolution
You can deploy vMA but when you start up the virtual machine, an error results.	Check whether your setup meets the hardware and software requirements listed in “Hardware and Software Prerequisites” on page 12.
You add a server but the vSphere CLI command or Perl script still prompts for authentication.	Run <code>vi fp init</code> for the target server.
You have added multiple servers. How can you know where vMA runs vSphere CLI commands if you do not specify <code>--server</code> ?	After a call to <code>vi fp init</code> , your prompt changes to include the current target.
You want to enable DNS resolution in vMA.	You can configure the DNS resolution name server for vMA by updating the <code>/etc/resolv.conf</code> file. Add the following line for each DNS server in your network: <code>nameserver <dns server ip address></code> Type <code>man resolv.conf</code> for details on that file. If vMA is set up for DHCP, and the network is restarted, changes you made to <code>/etc/resolv.conf</code> are lost.

vMA Interfaces

vMA interfaces allow you to initialize vi-fastpass, add, remove, and list target servers, manage passwords, and manage the vi-logger vMA component. The interfaces are available as Perl commands and Java methods.

The chapter includes the following topics:

- [“vMA Interface Overview”](#) on page 21
- [“vifpinit Command for vi-fastpass Initialization”](#) on page 22
- [“vifp Target Management Commands”](#) on page 22
- [“Target Management Example Sequence”](#) on page 25
- [“vilogger Daemon and Log Management Commands”](#) on page 26
- [“Using the vifplib Library”](#) on page 29
- [“vifplib Reference”](#) on page 29

vMA Interface Overview

[Table 3-1](#) shows which interfaces include which command and method.

Table 3-1. vMA Interface Overview

Interface / Library	Commands	Methods	For More Information
vifpinit	vifpinit		“vifpinit Command for vi-fastpass Initialization” on page 22.
vifp (administrative interface)	addserver removeserver rotatepassword listservers		“vifp Target Management Commands” on page 22.
vilogger (logging interface)	enable disable updatepolicy list		“vilogger Daemon and Log Management Commands” on page 26.
vifplib (library)	enumerate_targets query_target login_by_fastpass	enumerateTargets queryTarget loginByFastpass	“Using the vifplib Library” on page 29.

vifpinit Command for vi-fastpass Initialization

Initializes vi-fastpass for the vSphere CLI and the vSphere SDK for Perl.

Usage

```
vifpinit [<server>]
```

Description

The `vifpinit` command enables vi-fastpass authentication for vSphere CLI and vSphere SDK for Perl commands.

You can establish multiple servers as target servers, and then call `vifpinit` once to initialize all servers for vi-fastpass authentication. You can then run commands against any target server without additional authentication. VMware recommends that you use the `--server` option to specify the server to run commands on.

The command also establishes the default execution server to run commands on if the `--server` option is not specified:

- If there is only one server, it is the execution server.
- If there are multiple servers and you called `vifpinit` without specifying a server, the first server is the execution server.
- If you call `vifpinit <server>`, the specified server becomes the execution server.

The vMA prompt displays the current default execution server. If you remove that default server, the prompt does not change until you have explicitly changed to a different default execution server.

While hosts remain target servers across vMA reboots, you must run `vifpinit` after each logout to enable vi-fastpass for vSphere CLI and vSphere SDK for Perl commands.

vifp Target Management Commands

The `vifp` interface allows administrators to add, list, and remove target servers and to manage the vi-admin user's password.

IMPORTANT With the exception of `listservers`, all `vifp` commands require superuser privileges. Because vi-admin has superuser privileges, you can prefix the commands with `sudo`, for example, `sudo vifp addserver <server>`.

vifp addserver

Adds a vCenter Server or ESX/ESXi system as a vMA target server.

Usage

```
sudo vifp addserver
  <server>
  [--protocol <http | https>]
  [--portnumber <portnum>]
  [--servicepath <servicepath>]
  [--username <username>]
  [--password <password>]
```

Description

After a server is a vMA target, you must run `vifpinit <server>` before you run vSphere CLI commands or vSphere SDK for Perl scripts against that system. The system remains a vMA target across vMA reboots, but running `vifpinit` again is required after each logout. See [“vifpinit Command for vi-fastpass Initialization”](#) on page 22.

After you run `vi fp init`, you can run vSphere CLI or vSphere SDK for Perl commands and scripts and you are no longer prompted for authentication information, as follows:

- If you add a vCenter Server system as a vMA target, you can run most commands on all ESX/ESXi systems that the vCenter Server system manages using the vSphere CLI `--vihost` option. The *vSphere CLI Installation and Reference Guide* includes a table that shows which commands cannot target a vCenter Server system.
- If you add only one ESX/ESXi host, you can run commands without specifying the target.
- If you add multiple ESX/ESXi hosts, specify the target to avoid confusion.

See [“Add Target Servers to vMA”](#) on page 15 and [“Add Multiple Target Servers”](#) on page 16.

IMPORTANT If you change a target server’s name, you must remove it, then add it to vMA with the new name. Changing the name can mean explicitly changing the name or giving a name to a target server that does not have a host name.

Options

Option	Description
<code>server</code>	Name or IP address of the ESX/ESXi or vCenter Server system to add as a vMA target.
<code>protocol</code>	Connection protocol. Default is <code>https</code> .
<code>portnumber</code>	Connection port number of <code><server></code> . Default is <code>443</code> .
<code>servicepath</code>	Service path URL of <code><server></code> . Default is <code>/sdk</code> .
<code>username</code>	User who connects to <code><server></code> . If <code><server></code> points to an ESX/ESXi system, the default is <code>root</code> . The user must have superuser privileges on <code><server></code> . If <code><server></code> points to a vCenter Server system, there is no default. You are prompted for a user name if you do not specify one using this option. The user must have privileges to connect to the vCenter Server system.
<code>password</code>	Password of the user specified by <code>username</code> .

Example

```
sudo vi fp addserver my_vCenter
```

Adds a vCenter Server system as a vMA target. You are prompted for a user name and password. The user must have login privileges on the vCenter Server system.

```
sudo vi fp addserver myESX42
```

Adds an ESX/ESXi system to vi-fastpass. You are prompted for the root password for the target system.

vi fp removeserver

Removes a specified vMA target that was previously added with `vi fp addserver`.

Usage

```
sudo vi fp removeserver
  <server>
  [--protocol <http | https>]
  [--portnumber <portnum>]
  [--servicepath <servicepath>]
  [--username <username>]
  [--password <password>]
  [--force]
```

Description

If the target is an ESX/ESXi system, you need superuser privileges for removal. If the target is a vCenter Server system, any user with connection privileges can remove the target. You only have to specify the `--server` option, and no password is required.

Run `vifp removeserver` for each vMA target before you delete the vMA instance. If you do not run `vifp removeserver`, the `vi-user` and `vi-admin` users remain on the target server. If you later add a server on which `vi-admin` and `vi-user` already exist to vMA, vMA uses replacement user names for those accounts. Run `vifp removeserver` to avoid having multiple users created by vMA on each target server.

Options

Option	Description
<code>server</code>	Name or IP address of the ESX/ESXi or vCenter Server system to remove.
<code>protocol</code>	Connection protocol. Default is <code>https</code> .
<code>portnumber</code>	Connection port number of <server>. Default is 443.
<code>servicepath</code>	Service path URL of <server>. Default is <code>/sdk</code> .
<code>username</code>	User who connects to <server>. For ESX/ESXi systems, default is <code>root</code> and the user must have superuser privileges on <server>.
<code>password</code>	Password of the user specified by <code>--username</code> . Use the password you used when adding the server.
<code>force</code>	Forces removal of the server.

Examples

```
sudo vifp removeserver <vCenter_Address>
```

Removes a vCenter Server system. You are not prompted for a password.

```
sudo vifp removeserver <esx_Address>
```

Removes an ESX/ESXi system. You are prompted for the root password for the target system.

vifp rotatepassword

Specifies `vi-admin` and `vi-user` password rotation parameters.

IMPORTANT This command applies only to ESX/ESXi target servers. You cannot rotate passwords for vCenter Server systems.

Usage

```
sudo vifp rotatepassword
  [--now [--server <server>] |
  --never |
  --days <days>]
```

Description

vMA changes passwords for `vi-admin` and `vi-user` both in the local credential store and on the target server or target servers based on the specified options. vMA attempts the password rotation at midnight, vMA time.

For example, if you add `server1` on 9/1, and `server2` on 9/2, and call `vifp rotatepassword --days 7`, vMA rotates the password for `server1` at midnight on 9/8 and the password for `server2` at midnight on 9/9. vMA rotates the `server1` password again on 9/15 and the `server2` password again on 9/16. If you call `vifp rotatepassword --days 3`, vMA rotates the `server1` password on 9/18 and the `server2` password on 9/19.

If one or more of the target servers is down when vMA attempts password rotation, vMA repeats the attempt the next day at midnight, vMA time.

Options

Option	Description
now	Immediately rotates the password for all servers or a specified server.
server	ESX/ESXi host to rotate the password for. Use <code>--server</code> only with <code>--now</code> .
never	Never rotate the password for any target server.
days	Rotate the password for all target servers after the specified number of days.

Examples

```
sudo vifp rotatepassword --now
```

Immediately rotates passwords of all ESX/ESXi vMA target servers.

```
sudo vifp rotatepassword --now --server <serverAddress>
```

Immediately rotates the password of a specific server.

```
sudo vifp rotatepassword --days 5
```

Sets the password rotation policy to rotate the password of all ESX/ESXi vMA targets every five days.

```
sudo vifp rotatepassword
```

Displays the current password rotation policy.

vifp listservers

Lists target systems. Includes for each system whether it is an ESX, ESXi, or vCenter Server system.

Usage

```
listservers
```

Description

You can use this command to verify that `addserver` succeeded. This command does not require administrator privileges on vMA.

Example

```
vifp listservers
```

Lists all servers that are vMA targets, for example:

```
server1.mycomp.com      ESX
server2.mycomp.com      ESX
server3.mycomp.com      ESXi
vc42.mycomp.com         vCenter
```

Target Management Example Sequence

The following sequence of commands adds an ESX host, lists servers, runs `vifpinit` to enable vi-fastpass, runs a vSphere CLI command, and removes the ESX host.

```
sudo vifp addserver server1.company.com
root@server1.company.com's password: <password, not echoed to screen>
vifp listservers
server1.company.com      ESX
vifpinit server1.company.com
vicfg-mpath --list
cdrom vmhba0:1:0 (0MB has 1 paths and policy of fixed
    Local 0:7:1 vmhba0:1:0 On active preferred
....
sudo vifp removeserver server1.company.com
root@server1.company.com's password: <password, not echoed to screen>
```

vilogger Daemon and Log Management Commands

You can use the `vilogger` interface to have vMA collect log files from the target ESX/ESXi or vCenter Server hosts according to the specified log policy. You can manage the daemon using the daemon management interface and specify the log policy using the `vilogger` CLIs.

Management Service Interface for vilogd

The `vilogd` daemon performs the log collection. The daemon starts each time vMA boots.

You can explicitly stop or restart the daemon at any time if you are logged in as `vi-admin` using the commands in [Table 3-2](#).

Table 3-2. Explicit Manipulation of the vilogd Daemon

Command	Action
<code>sudo /sbin/service vmware-vilogd start</code>	Starts the <code>vilogd</code> daemon.
<code>sudo /sbin/service vmware-vilogd stop</code>	Stops the <code>vilogd</code> daemon.
<code>sudo /sbin/service vmware-vilogd restart</code>	Restarts the <code>vilogd</code> daemon.
<code>/sbin/service vmware-vilogd status</code>	Checks the status of the <code>vilogd</code> daemon.

The `vilogd` daemon collects the logs listed when you run [“vilogger list”](#) on page 28.

vilogger enable

Enables log collection for the specified vMA target.

Usage

```
vilogger enable
  [--server <vMA_target>]
  [--logname <logname>]
  [--collectionperiod <period_in_seconds>]
  [--numrotation <rotation>]
  [--maxfilesize <size_in_MB>]
```

Description

You can enable logging for a single target or for all vMA targets. You can enable logging selectively for specific log files. By default, logging is disabled for a target when you add it to vMA. You must enable logging explicitly.

By default, `vilogd` places the logs in `/var/log/vmware`. To specify a different log location, change the `/etc/vmware/viconfig/vilogdefaults.xml` file. When you start `vmware-vilogd` the next time, it places the logs in the new location if `vi-admin` has access to it. See [“vilogger list”](#) on page 28 for a listing of the logs collected on ESX, ESXi, and vCenter Server systems.

Options

Option	Description
<code>server</code>	IP address or name of the vMA target to enable log collection for. Default is all vMA targets.
<code>logname</code>	Log to enable. Default is all logs. You can display the list using <code>vilogger list</code> .
<code>collectionperiod</code>	Logs are collected at regular intervals. This option specifies the interval, in seconds. Specify a number between 10 and 3600. Default is 10.
<code>maxfilesize</code>	Maximum size of the log file before rollover, in MB. Specify a number between 1 and 1024. Default is 5MB.
<code>numrotation</code>	Number of log files to keep before the oldest file is overwritten. Specify a number between 1 and 1024. Default is 5.

Examples

vilogger enable

Enables log collection for all vMA targets using the default values for collection period, log rotation, and log size.

vilogger enable --server myServer42

Enables log collection for the myServer42 vMA target using default values for collection period, log rotation, and log size.

vilogger enable --server myServer42 --logname messages

Enables log collection for the /var/log/messages log for the myServer42 ESX/ESXi system using the default values for collection period, log rotation, and log size.

vilogger enable --collectionperiod 60

Enables log collection for all vMA target servers using a collection period of 60 seconds.

vilogger enable --numrotation 8

Enables log collection for all vMA target servers with log rotation set to 8.

vilogger enable --maxfilesize 10

Enables log collection for all vMA target servers with the maximum log file size set to 10MB.

vilogger disable

Disables log collection for a vMA target.

Usage

```
vilogger disable
  [--server <server>]
  [--logname <logname>]
  [--force]
```

Description

Disables all log collection for a specified vMA target or for all vMA targets. The command also allows you to disable logging on a per-log-file basis.

When the server is unreachable, `vilogger disable` fails. Use `vilogger disable --force` to disable logging for unreachable hosts.

Options

Option	Description
server	Name or IP address of the vMA target to disable log collection for. Default is all vMA targets.
logname	Log to disable. Default is all logs. You can display the list using <code>vilogger list</code> .
force	Forces disabling of logging. When vMA cannot reach the target server, <code>vilogger disable</code> fails. Use <code>vilogger disable --force</code> to disable logging for the target server.

Examples

vilogger disable --server myserver42 --logname messages

Disables log collection for the /var/log/messages log for the myserver42 ESX host.

vilogger disable --server myserver42

Disables all log collection for the myserver42 ESX host.

vilogger disable

Disables all log collection.

villogger updatepolicy

Customizes log collection parameters.

Usage

```
villogger updatepolicy
  [--server <server>]
  [--logname <logname>]
  [--collectionperiod <period_in_seconds>]
  [--numrotation <rotation>]
  [--maxfilesize <size_in_MB>]
```

Description

Allows you to specify the number of rotations, collection period, and maximum log size for a specific server or for all servers. This command changes collection policies only for logs that are already enabled.

Options

Option	Description
server	Name or IP address of the vMA target to set collection parameters for. Default is all vMA targets.
logname	Log to change collection parameters for. Default is all logs enabled for the specified server or servers. You can display the list of available logs using <code>villogger list</code> .
collectionperiod	Logs are collected at regular intervals. This option specifies the interval, in seconds. Specify a number between 10 and 3600. Default is 10.
maxfilesize	Maximum size of the log file before rollover, in MB. Specify a number between 1 and 1024. Default is 5MB.
numrotation	Number of log files to keep before the oldest file is overwritten. Specify a number between 1 and 1024. Default is 5.

Examples

```
villogger updatepolicy --server myserver42 --logname messages --collectionperiod 30
```

Updates the log collection period to 30 seconds for previously enabled logs.

```
villogger updatepolicy --server myserver42 --maxfilesize 7
```

Updates the maximum log file size for all enabled logs for the specified ESX/ESXi system (myserver42) to 7MB.

villogger list

Lists available logs.

Usage

```
villogger list
  [--server <server>]
  [--logname <logname>]
```

Description

Lists the names of all logs available for collection from all target servers or from the specified target server. The command lists the log files and whether log collection is enabled or disabled for each log.

The following logs are included for VMware ESX systems:

- `/var/log/messages` (service console and user-level daemon messages; no VMkernel messages)
- `/var/log/vmkernel`
- `/var/log/vmksummary`
- `/var/log/vmkwarning`
- `hostd.log` (host agent log)
- `vpaxa.log` (vCenter Server agent log; included if the system is managed by a vCenter Server system)

The following logs are included for VMware ESXi systems. The `messages` log contains the same information that you can find in the `vmkernel`, `vmkwarnings`, and `hostd` logs on ESX systems. The `vmksummary` log does not exist on ESXi system.

- `/var/log/messages` (VMkernel logs and warnings, host daemon messages, and other user-level daemon messages)
- `hostd.log` (host agent log)
- `vpxa.log` (vCenter Server agent log; included if the system is managed by a vCenter Server system)

For vCenter Server systems, `vilogger` collects only `vpxd.log` files. If a vCenter Server system is the vMA target, `vilogger` does not automatically collect the log files of the ESX/ESXi hosts the vCenter Server system manages.

vMA does not collect log files for virtual machines.

If logging is enabled, the `list` command also displays the following information:

- Location of the file where the collected logs are stored in vMA
- Collection period
- Number of log rotations to maintain
- Maximum size the log file can grow to before it is rotated.

Example

`vilogger list`

Lists the logging status for all vMA target servers.

Using the `vifplib` Library

The `vifplib` library allows you to programmatically connect to vMA targets using Perl or Java. This section explains how to use `vifplib` to connect to a single target or multiple targets, and includes a reference to each command.

Agents can link with `vifplib` and use vi-fastpass functionality. The library implements the methods discussed in “Using the `vifplib` Library” on page 29. See the `VIFPLIB` java library for a more detailed reference to the Java interface. You can find samples in `/opt/vmware/vima/samples`.

The `vifplib` library allows you to enable vi-fastpass authentication and to query and enumerate multiple targets with the following commands:

- `EnumerateTargets` – Retrieves a list of all servers that are vMA targets.
- `QueryTarget` – Retrieves connection information for target servers.
- `LoginByFastpass` – Connects to the target servers.

vifplib Reference

You can use the following `vifplib` commands in Perl or Java programs.

Enumerating Targets

Usage

Perl	<code>enumerate_targets</code>
Java	<code>enumerateTargets()</code>

Description

Returns a list of all target vCenter Server or ESX/ESXi systems that were added to this vMA instance using `vifp addserver`.

Options

No options

Returns

Returns a list of all target servers.

Querying Targets**Usage**

```
Perl          query_target (<servername>)
Java          queryTarget (string <servername>)
```

Description

Allows the caller, for example, an agent, to retrieve login credentials from a vMA target and to use those credentials to connect to the vMA target.

Options

Option	Description
servername	One of the servers added to this vMA instance using <code>vi fp addserver</code> . Can be an ESX/ESXi system or a vCenter Server system.

Returns

Returns a `VIUserInfo` object that contains details of the user that can be used to connect to the vMA target specified using `<servername>`.

Programmatic Login**Usage**

```
Perl          login_by_fastpass (<servername>)
Java          loginByFastpass
              (VimPortType <service>,
               ManagedObjectReference <svcRef>,
               String <servername>)
```

Description

Allows a calling program to log in to a target server programmatically.

Options

Option	Language	Description
service	Java	Java service instance.
svcRef	Java	Java service Managed Object Reference.
servername	Java, Perl	One of the servers added to this vMA instance using <code>vi fp addserver</code> .

Returns

Returns a session that the agent can use to run commands on the host.

Appendix: Updating vMA with vima-update

vMA includes the `vima-update` utility, which can download software updates including security fixes from VMware and for components included in vMA, such as the Enterprise Linux and JRE. No other update mechanisms are available for vMA.

IMPORTANT You cannot use `vima-update` to upgrade a VIMA 1.0 system to vMA 4.0.

This appendix introduces `vima-update` and includes a reference and examples for its use. The appendix includes the following topics:

- [“Introduction to vima-update”](#) on page 31
- [“Use vima-update”](#) on page 31
- [“Use vima-update with Update Depots”](#) on page 32
- [“vima-update Troubleshooting”](#) on page 32

If `vima-update` returns an error, see the *ESX 4 Patch Management Guide*.

Introduction to vima-update

You can use `vima-update` to download patches for vMA. VMware will host a depot of vMA updates online. The URL of the update depot is specified in the `/etc/vmware/esxupdate/vimaupdate.conf` file.

VMware notifies customers when vMA updates become available. Customers can then evaluate whether they want the current set of updates, and can install it. Later updates include changes made by all previously released updates.

You can connect to the depot URL directly or specify a proxy server in the `/etc/vmware/esxupdate/vimaupdate.conf` file. If no proxy server is specified, `vima-update` requires a direct connection to the Internet.

Use vima-update

You can use `vima-update` to scan for updates and to install updates.

You can specify a proxy server by editing the `/etc/vmware/esxupdate/vimaupdate.conf` file before you use `vima-update`. For example:

```
# Proxy settings
# Uncomment these options if a proxy is required to access the
# URL specified in vima.depot

#proxy = http://proxy.example.com
#proxyport = 12345
```

To scan for updates

- 1 Log in to vMA as vi-admin.
- 2 Run the following command:
`sudo vima-update scan`
- 3 [Optional] If prompted, provide the vi-admin password

vMA lists applicable bulletins with updates.

To update vMA

- 1 Log in to vMA as vi-admin.
- 2 Run `vima-update` to install all updates or update to a particular version, specified by bulletin ID.
Each bulletin consists of one or more updates. Later bulletins include the updates of previous bulletins.

Task	Command
To update vMA to the current version.	<code>sudo vima-update update</code>
To update vMA to a specified update level. Includes changes from all preceding updates.	<code>sudo vima-update -b <bulletinID> update</code>

Examples

The following examples assumes a depot is available.

sudo vima-update scan

Lists applicable bulletins with updates.

sudo vima-update -b 'vma 4.01' update

Updates vMA to patch level 4.01.

sudo vima-update update

Applies all currently available updates.

Use vima-update with Update Depots

The *ESX Patch Management Guide* explains how you can use `esxupdate` with local depots. You can use `vima-update` with local depots as well.

To use vima-update with local depots

- 1 Download the depot to a local server, as described in the *ESX 4 Patch Management Guide*.
- 2 Edit the depot = `http://...` line in the `/etc/vmware/esxupdate/vimaupdate.conf` file.
- 3 Run the update, as described in [“Use vima-update”](#) on page 31.

vima-update Troubleshooting

If you call `vima-update`, and the URL specified in the `/etc/vmware/esxupdate/vimaupdate.conf` file is wrong or returns an unexpected file, a message that includes `Encountered error MetadataDownloadError:...Failed to download metadata` appears.

Check the URL and supply one that points to vMA updates.

Index

A

adding target servers **15**
addserver command **22**
authentication component **8**
authentication prerequisites **12**

C

CentOS **8**
configuring vMA **13**

D

default target **22**
deleting vMA **18**
deploying vMA **13**
deployment URL **13**
DHCP **13**
disabling logging **27**
DNS resolution **19**

E

enabling logging **26**
ESX/ESXi 3.5 Update 2 **12**
ESX/ESXi systems, vMA target **16**
example sequence **25**

H

hardware prerequisites **12**
host name **14**

I

initialization **22**
insecure passwords **14**

J

Java JRE **8**

L

Linux **8**
list logs **28**
listservers command **25**
local update depots **32**
localhost **17**
log management commands **26**
logging
 component **9**
 disabling **27**
 enabling **26**

list **28**
setting policy **28**

M

managing logs **28**
modifying scripts **17**
multiple target servers **16**

N

name change **15, 16**
network configuration **14**
network setup **14**

P

passwords
 ESX/ESXi hosts **12**
 vCenter Server systems **12**
 vi-admin **13**
proc nodes **17**

R

Red Hat Enterprise Linux **8**
removeservers command **23**
removing target servers **17**
RHEL **8**
root user account **12**
rotatepassword command **24**
rotatepassword example **24**

S

scripts, modifying **17**
shutting down vMA **18**
SMI-S **8**
SNMP **8**
storage required for vMA **12**
sudo **12**

T

target servers
 commands **22**
 multiple **16**
 name change **15, 16**
 removing **17**
 single **15**
targets, default **22**
technical support resources **5**
troubleshooting vMA **19**

U

update depots **32**
 updating vMA **31**
 URL for deployment **13**

V

vCenter Server systems, vMA target **15**

VI CLI

vifpinit **22**
 vifs **17**
 without vi-fastpass **16**

vi-admin

insecure password **14**
 privileges **15**
 setting password **13, 14**

vi-fastpass

initialization **22**
 overview **8**

vifp addserver **22**vifp listservers **25**vifp removeserver **23**vifp rotatepassword **24**vifp target management **22**vifpinit command **22**vifplib **29**vifs command **17**vilogd interface **26**

vilogger

daemon **26**
 disable command **27**
 enable command **26**
 list command **28**
 updatepolicy command **28**

vi-logger component **9**vima-update **31**

introduction **31**
 local depots **32**
 troubleshooting **32**
 using **31**

vi-user

privileges **15**
 setup **14**

vMA

component overview **7**
 getting started **11**
 interface overview **21**
 samples **9**
 use cases **9**

vMA targets

ESX/ESXi systems **16**
 vCenter Server systems **15**

VMware Tools **8**vSphere CLI **8**vSphere SDK for Perl **8**