vSphere Management Assistant Guide

vSphere 5.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-000570-00

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

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

Contents

About This Book

The *vSphere Management Assistant Guide* explains how to deploy 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.

NOTE The topics in which this documentation uses the product name "ESXi" are applicable to all supported releases of ESX and ESXi.

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
20JAN2012	Chapter 2, section “Configure Unattended Authentication for Active Directory Targets” is updated.
24AUG2011	vMA 5.0 release.
13JUL2010	vMA 4.1 release
16NOV2009	Chapter 1 is enhanced to provide details about vMA’s enhanced capabilities, authentication mechanisms and the changes to the samples. Chapter 2 provides information about configuring vMA for Active Directory. It also explains how to reconfigure a target server. Chapter 3 provides information about the new `vifptarget` and `vifp reconfigure` commands. It also describes the VmaTargetLib library.
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 ESXi hosts and vCenter Server systems. Developers can create agents that interact with ESXi hosts and vCenter Server systems.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation go to http://www.vmware.com/support/pubs.

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 1

The vSphere Management Assistant (vMA) is a SUSE Linux Enterprise Server 11-based virtual machine that includes prepackaged software such as the vSphere command-line interface, and the vSphere SDK for Perl. vMA allows administrators to run scripts or agents that interact with ESXi hosts and vCenter Server systems without having to authenticate each time.

The chapter includes the following topics:

To get started with vMA right away, go to "Getting Started with vMA" on page 11.

vMA Capabilities

vMA provides a flexible and authenticated platform for running scripts and programs.

- As administrator, you can add vCenter Server systems and ESXi hosts as targets and run scripts and programs on these targets. Once you have authenticated while adding a target, you need not login again while running a vSphere CLI command or agent on any target.
- As a developer, you can use the APIs provided with the `VmaTargetLib` library to programmatically connect to vMA targets by using Perl or Java.
- vMA enables reuse of service console scripts that are currently used for ESXi administration, though minor modifications to the scripts are usually necessary.
- vMA comes preconfigured with two user accounts, namely, vi-admin and vi-user.
  - As vi-admin, you can perform administrative operations such as addition and removal of targets. You can also run vSphere CLI commands and agents with administrative privileges on the added targets.
  - As vi-user, you can run the vSphere CLI commands and agents with read-only privileges on the target.
- You can make vMA join an Active Directory domain and log in as an Active Directory user. When you run commands from such a user account, the appropriate privileges given to the user on the vCenter Server system or the ESXi host would be applicable.
- vMA can run agent code that make proprietary hardware or software components compatible with VMware ESX. These code currently run in the service console of existing ESX hosts. You can modify most of these agent code to run in vMA, by calling the vSphere API, if necessary. Developers must move any agent code that directly interfaces with hardware into a provider.

vMA Component Overview

When you install vMA, you are licensed to use the virtual machine that includes all vMA components.

vMA includes the following components.

- SUSE Linux Enterprise Server 11 SP1 – vMA runs SUSE Linux Enterprise Server on the virtual machine. You can move files between the ESXi host and the vMA console by using the `vifs` 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 a scripting interface to the vSphere API. The SDK includes utility applications and samples for many common tasks.
- Java JRE version 1.6 – Runtime engine for Java-based applications built with vSphere Web Services SDK.
- vi-fastpass - Authentication component.

vSphere Authentication Mechanism

vMA's authentication interface allows users and applications to authenticate with the target servers using vi-fastpass or Active Directory. While adding a server as a target, the Administrator can determine if the target needs to use vi-fastpass or Active Directory authentication. For vi-fastpass authentication, the credentials that a user has on the vCenter Server system or ESXi host are stored in a local credential store. For Active Directory authentication, the user is authenticated with an Active Directory server.

When you add an ESXi host as a fastpass target server, vi-fastpass creates two users with obfuscated passwords on the target server and stores the password information on vMA:

- vi-admin with administrator privileges
- vi-user with read-only privileges

The creation of vi-admin and vi-user does not apply for Active Directory authentication targets. When you add a system as an Active Directory target, vMA does not store any information about the credentials. To use the Active Directory authentication, the administrator must configure vMA for Active Directory. For more information on how to configure vMA for Active Directory, see "Configure vMA for Active Directory Authentication" on page 14.

After adding a target server, you must initialize vi-fastpass so that you do not have to authenticate each time you run vSphere CLI commands. If you run a vSphere CLI command without initializing vi-fastpass, you will be asked for username and password.

You can initialize vi-fastpass by using one of the following methods:

- Run `vifptarget`. For more information about this script, see "vifptarget Command for vi-fastpass Initialization" on page 27.
- Call the `Login` method in a Perl or Java program. For more information about this method, see "VmaTargetLib Reference" on page 33.

After setting up a target using the `vifptarget` command, you can run vSphere CLI commands or scripts that use vSphere SDK for Perl without providing any authentication information. To run commands against an ESXi host that is managed by a vCenter Server, you can use the `--vihost` option.

Each time you log in to vMA, you must run the `vifptarget` command or the `Login` method once. The target that you specify in the `vifptarget` command is the default target. Target servers remain targets across reboots. You can override it by using the `--server` option of the vSphere CLI commands as shown in the following example:

```
vifptarget -s esx1.foo.com
vicfg-nics -l   #lists the nics on esx1.foo.com
vicfg-nics -l --server esx2.foo.com #lists the nics on esx2.foo.com
```

vMA Samples

vMA samples illustrate the vMA CLIs and the `VmaTargetLib` library. The samples are available in vMA at `/opt/vmware/vma/samples`.

- `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 `vifptarget` before running this script.
- `listTargets.pl` - Perl sample that retrieves information and version of vMA targets using VmaTargetLib.
- `listTargets.sh` - Java sample that demonstrates use of VmaTargetLib.

vMA Use Cases

This section lists a few typical use cases.

Writing or Converting Scripts

You 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 `VmaTarget.login()` method of `VmaTargetLib`.

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 `VmaTargetLib` 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 `VmaTargetLib::VmaTarget.login()`.

- 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 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(String myESXName) {
  VmaTarget target = VmaTargetLib.query_target(myESXName);
  UserSession us = target.login();
  }
  ```

  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 ESXi host and ports the agent to vMA.

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

Getting Started with vMA

2

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 previous version of vMA to vMA 5.0. You must install a fresh vMA 5.0 instance.

This chapter includes the following topics:

- "Update vMA" on page 24
- "Configure Automatic vMA Updates" on page 25

Hardware Requirements

To set up vMA, you must have an ESXi host. Because vMA runs a 64-bit Linux guest operating system, the ESXi host on which it runs must support 64-bit virtual machines.

The 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 do not have VT support enabled, do not support a 64-bit guest operating system. For detailed hardware requirements, see the *Hardware Compatibility List* on the VMware Web site.

By default, vMA uses one virtual processor, and requires 3GB of storage space for the vMA virtual disk. The recommended memory for vMA is 600MB.

Software Requirements

You can deploy vMA on the following systems:

- vSphere 5.0
- vSphere 4.1 or later
- vSphere 4.0 Update 2 or later
- vCenter Application 5.0

You can deploy vMA by using a vSphere Client connected to an ESXi host or by using a vSphere Client connected to vCenter Server 5.0, vCenter Server 4.1 or later, vCenter Server 4.0 Update 2 or later, or vCenter Application 5.0.

You can use vMA to target ESX/ESXi 3.5 Update 5, ESX/ESXi 4.0 Update 2 or later, ESX/ESXi 4.1 or later, ESXi 5.0, vCenter Server 4.0 Update 2 or later, vCenter Server 4.1 or later, and vCenter Server 5.0 systems.

At runtime, the number of targets a single vMA instance can support depends on how it is used.

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.

  If you are using a vCenter Server target, you do not need passwords for the ESXi hosts that the vCenter Server system manages, unless you run commands that do not support vCenter Server targets.
- ESXi host – You must have the root password or the user name and password for a user with administrative privileges for each ESXi host you add as a vMA target. You do not need the authentication information when you remove a target host.
- vMA – When you first configure 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`.

Deploy vMA

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

IMPORTANT You cannot upgrade an earlier version of vMA to vMA 5.0. You must install a fresh vMA 5.0 instance.

To deploy vMA

1 Use a vSphere Client to connect to a system that is running the supported version of ESXi or vCenter Server.

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 **Deploy from a file or URL** if you have already downloaded and unzipped the vMA virtual appliance package.

5 Click **Browse**, select the OVF, and click **Next**.

6 Click **Next** when the OVF template details are displayed.

7 Accept the license agreement and click **Next**.

8 Specify a name for the virtual machine.

You can also accept the default virtual machine name.

9 Select an inventory location for the virtual machine when prompted.

If you are connected to a vCenter Server system, you can select a folder.

10 If connected to a vCenter Server system, select the resource pool for the virtual machine.

By default, the top-level root resource pool is selected.

11 If prompted, select the datastore to store the virtual machine on and click **Next**.

12 Select the required disk format option and click **Next**.

13 Select the network mapping and click **Next**.

IMPORTANT Enure that vMA is connected to the management network on which the vCenter Server system and the ESXi hosts that are intended vMA targets are located.

14 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 at First Boot

When you start the vMA virtual machine the first time, you can configure it.

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.

4 When prompted, specify a host name for vMA.

   The name can contain 64 alphanumeric characters. You can change the vMA host name later by modifying the `/etc/HOSTNAME` and `/etc/hosts` files, as you would for a Linux host. You can also use the vMA console to change the host name.

   For a DHCP configuration, the host name is obtained from the DNS server.

5 When prompted, specify a password for the vi-admin user.

   If prompted for an old password, press Enter and continue.

   The new password must conform to the vMA password policy. The password must have at least:

   - Eight characters
   - One upper case character
   - One lower case character
   - One numeral character
   - One symbol such as #, $

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

   This user has root privileges.

vMA is now configured and the vMA console appears. The console displays the URL from which you can access the Web UI.

vMA Console and Web UI

vMA provides two interfaces, the console, which is a command-line interface and the browser-based Web UI.

From the console, you can do the following tasks:

- Log in as vi-admin
- Add servers to vMA
- Run commands from the vMA console
- Configure the network settings and proxy server settings
- Configure the timezone settings.

The web UI enables you to do the following tasks:

- Log in as vi-admin
- Configure the network settings and proxy server settings
- Configure the timezone settings.
- Update vMA

Configure vMA for Active Directory Authentication

Configure vMA for Active Directory authentication so that ESXi hosts and vCenter Server systems added to Active Directory can be added to vMA without having to store the passwords in vMA's credential store. This is a more secure way of adding targets to vMA.

Ensure that the DNS server configured for vMA is the same as the DNS server of the domain. You can change the DNS server by using the vMA Console or the Web UI.

Ensure that the domain is accessible from vMA. Also, ensure that you can ping the ESXi and vCenter server systems that you want to add to vMA and that pinging resolves the IP address to `<targetservername.domainname>`, where domainname is the domain to which vMA is to be added.

To add vMA to a domain

1 From the vMA console, run the following command:

```
sudo domainjoin-cli join <domain-name> <domain-admin-user>
```

2 When prompted, provide the Active Directory administrator's password.

On successful authentication, the command adds vMA as a member of the domain. The command also adds entries in the `/etc/hosts` file with `vmaHostname.domainname`.

3 Restart vMA.

Now, you can add an Active Directory target to vMA. For steps to do this, see "Add Target Servers to vMA" on page 17.

To check vMA's domain settings

From the vMA console, run the following command:

```
sudo domainjoin-cli query
```

The command displays the name of the domain to which vMA has joined.

To remove vMA from the domain

From the vMA console, run the following command:

```
sudo domainjoin-cli leave
```

The vMA console displays a message stating whether vMA has left the Active Directory domain.

Configure Unattended Authentication for Active Directory Targets

To configure unattended authentication (authentication from vi-admin or root context) to Active Directory targets, you must renew the Kerberos tickets for the domain user using which the target is added. Unattended authentication is supported for ESXi4.1 Update 3 and later. You must ensure that the Active Directory is set up for unattended log in.

To configure unattended authentication for Active Directory targets

1 On any Windows Server 2003 computer that is part of the domain to which vMA is added, download and install the Ktpass tool from the Microsoft web site.

2 Open the command prompt and run the following command:

```
ktpass /out foo.keytab /princ foo@VMA-DC.ENG.VMWARE.COM /pass ca... /ptype KRB5_NT_PRINCIPAL
              -mapuser <vma-dc>\<foo>
```

where, <vma-dc> is the name of the domain and foo is the user having permissions for the vCenter administration.

This command creates a file called `foo.keytab.`

3 Move the `foo.keytab` file to `/home/local/VMA-DC/foo`.

You can use WinSCP and log in as user **`vma-dc\foo`** to move the file.

4 (Optional) Make sure that the user vma-dc\foo on vMA owns the `foo.keytab` file by using the following commands:

```
ls -l /home/local/VMA-DC/foo/foo.keytab
chown 'vma-dc\foo' /home/local/VMA-DC/foo/foo.keytab
```

5 On vMA, create a script in `/etc/cron.hourly/kticket-renew` with the following contents:

```
#!/bin/sh
su - vma-dc\\foo -c '/usr/bin/kinit -k -t /home/local/VMA-DC/foo/foo.keytab foo'
```

This script will renew the ticket for the user foo every hour.

You can also add the above script to a service in `/etc/init.d` to refresh the tickets when vMA is booted.

Troubleshooting Unattended Authentication

If you are not able to authenticate from vMA or cannot add vMA to the domain controller, verify the following conditions:

- Your DNS server setup in vMA resolves the IP address or host name of the vCenter server to a fully qualified domain name (FQDN) and that the FQDN contains the domain name to which vMA is added.
- The command `vifp listservers` shows the name of vCenter server as the FQDN that contains the domain name to which vMA is added as the suffix.
- The date and time settings on vMA, the domain controller and the vCenter server are the same. Verify the time zone as well. The time may vary by an hour, but a large time skew might cause authentication problems.

Enable the vi-user Account

As part of configuration, vMA creates a vi-user account with no password. However, you cannot use the vi-user account until you have specified a vi-user password.

IMPORTANT The vi-user account has limited privileges on the target ESXi hosts and cannot run any commands that require sudo execution. You cannot use vi-user to run commands for Active Directory targets (ESXi or vCenter Server). To run commands for the Active Directory targets, use the `vi-admin` user or log in as an Active Directory user to vMA.

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, a message about root user privileges appears, and you are prompted for the vi-admin password.

3 Specify the vi-admin password.

4 When prompted, type and confirm the password for vi-user.

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

When you add 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 ESXi hosts, and the user can run only commands on target ESXi hosts that do not require administrative privileges.

vMA User Account Privileges

Table 2-1 lists the privileges that the different user accounts have for vCLI usage against different targets.

Table 2-1. Account Privileges for vCLI Usage

Target	Authentication Policy	vi-admin	vi-user	domain user
ESXi	fpauth	Y	Y	N
ESXi	adauth	Y	N	Y
vCenter Server	fpauth	Y	N	N
vCenter Server	adauth	Y	N	Y

Add Target Servers to vMA

After you configure vMA, you can add target servers that run the supported vCenter Server or ESXi version.

For vCenter Server and ESXi system targets, you must have the name and password of a user who can connect to that system.

See "vifp addserver" on page 28 for the complete syntax.

To add a vCenter Server system as a vMA target for Active Directory Authentication

1 Log in to vMA as vi-admin.

2 Add a server as a vMA target by running the following command:

```
vifp addserver vc1.mycomp.com --authpolicy adauth --username ADDOMAIN\\user1
```

Here, `--authpolicy adauth` indicates that the target needs to use the Active Directory authentication.

If you run this command without the `--username` option, vMA prompts for the name of the user that can connect to the vCenter Server system. You can specify this user name as shown in the following example:

```
Enter username for machinename.example.com: ADDOMAIN\user1
```

If `--authpolicy` is not specified in the command, then `fpauth` is taken as the default authentication policy.

3 Verify that the target server has been added.

The display shows all target servers and the authentication policy used for each target.

```
vifp listservers --long
server1.mycomp.com              ESX        adauth
server2.mycomp.com              ESX        fpauth
server3.mycomp.com              ESXi       adauth
vc1.mycomp.com                vCenter      adauth
```

4 Set the target as the default for the current session:

```
vifptarget --set | -s <server>
```

5 Verify that you can run a vSphere CLI command without authentication by running a command on one of the ESXi hosts, for example:

```
esxcli --server <VC_server> --vihost <esx_host> network nic list
```

The command runs without prompting for authentication information.

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

To add a vCenter Server system as a vMA target for fastpass Authentication

1 Log in to vMA as vi-admin.

2 Add a server as a vMA target by running the following command:

```
vifp addserver vc2.mycomp.com --authpolicy fpauth
```

Here, `--authpolicy fpauth` indicates that the target needs to use the fastpass authentication.

3 Specify the username when prompted:

```
Enter username for machinename.example.com: MYDOMAIN\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.

6 Verify that the target server has been added.

The display shows all target servers and the authentication policy used for each target.

```
vifp listservers --long
server1.mycomp.com              ESX         adauth
server2.mycomp.com              ESX         fpauth
server3.mycomp.com              ESXi        adauth
vc1.mycomp.com                 vCenter      adauth
vc2.mycomp.com                 vCenter      fpauth
```

7 Set the target as the default for the current session.

```
vifptarget --set | -s <server>
```

8 Verify that you can run a vSphere CLI command without authentication by running a command on one of the ESXi hosts, for example:

```
esxcli --server <VC_server> --vihost <esx_host> network nic list
```

The command runs without prompting for authentication information.

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

To add an ESXi host as a vMA target

1 Log in to vMA as vi-admin.

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

```
vifp addserver <servername>
```

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

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

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

vMA does not retain the root password. Instead, vMA adds vi-admin and vi-user to the ESXi host, and stores the obfuscated passwords that 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 Remove users added by vMA from the target server only if you deleted the vMA virtual machine but did not remove the target servers.

4 Verify that the target server has been added:

```
vifp listservers
```

5 Set the target as the default for the current session.

```
vifptarget --set | -s <server>
```

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

```
esxcli network nic list
```

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.

Running vSphere CLI for the Targets

If you have added multiple target servers, by default, vMA executes commands on the first server that you added. You should specify the server explicitly when running commands.

To run vSphere CLI for the targets

1 Add servers as vMA targets.

```
vifp addserver <server1>
vifp addserver <server2>
```

2 Verify that the target server has been added:

```
vifp listservers
```

3 Run `vifptarget`.

```
vifptarget –s <server2>
```

The command initializes the specified target server. Now, this server will be taken as the default target for the vSphere CLI or vSphere SDK for Perl scripts.

4 Run vSphere CLI or vSphere SDK for Perl scripts, by specifying the target server. For example:

```
esxcli ––server server2 network nic list
```

Reconfigure a Target Server

You can reconfigure a target server if you want to perform any of the following tasks:

- Change the authentication mode of a vMA target from vi-fastpass to Active Directory or vice versa.
- Change the configured user for the Active Directory target.
- Recover users for the vi-fastpass target. A user needs to be recovered if the credential store on vMA is corrupted or if the credentials of users corresponding to vMA users are modified and not reflected in vMA.

To change the authentication policy

1 Log in to vMA as vi-admin.

2 Run `reconfigure`

```
vifp reconfigure <servername> ––authpolicy <authpolicy>
```

3 When prompted, provide your credentials.

- If you reconfigure an Active Directory target to vi-fastpass authentication, then specify the root password for ESXi targets and the root username and password for vCenter targets.
- If you reconfigure a vi-fastpass target to Active Directory authentication, then specify the root username for the target.

To change the configured user or to recover users

1 Log in to vMA as vi-admin.

2 Run `reconfigure.`

```
vifp reconfigure <servername>
```

3 When prompted, provide your credentials.

- If you reconfigure an Active Directory target, specify a username for the target.
- If you reconfigure a vi-fastpass target, specify the root password of the ESXi target, and the password for username used to add the vCenter Server target.

Example 2-1. Adding and Reconfiguring a Target

```
vi-admin@example-dhcp:~> vifp addserver 90.100.110.120
Enter username for 90.100.110.120: administrator
administrator@90.100.110.120's password:
This will store username and password in credential store which is a security risk. Do you want
               to continue?(yes/no): yes

vi-admin@example-dhcp:~> vifp reconfigure 90.100.110.120
administrator@90.100.110.120's password:
vi-admin@example-dhcp:~>
```

Remove Target Servers from vMA

Before you delete a vMA virtual machine, remove all target servers from vMA. If you do not remove target ESXi hosts, 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 vi-admin.

2 To remove a target vCenter Server system from vMA, run the following command:

```
vifp removeserver <servername>
```

The vCenter Server system is no longer a vMA target.

To remove an ESXi host from vMA

1 Log in to vMA as vi-admin.

2 To remove an ESXi host that is a vMA target, run the following command:

```
vifp removeserver <host>
```

The Recent Tasks panel of the target server displays information about the vi-admin and vi-user users that are 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 because the Linux commands are running on vMA and not on the ESX host.
- **Access to ESXi files** – If you need access to folders or files on an ESXi host, you can make that host a target server and use the `vifs` vSphere CLI command to view, retrieve, or modify folders and files.
- **References to localhost** – Scripts cannot refer to `localhost`.
  - If vi-fastpass is initialized, all commands that do not specify `--server` apply to the default target.
  - If vi-fastpass is initialized, all commands that specify hostname or IP of the target apply to the target specified.
- **Programmatic connection** – In Perl scripts or Java programs, you can call `VmaTarget.login()` method of `VmaTargetLib` and specify the host to connect to. The directory `/opt/vmware/vma/samples` contains examples in Perl and Java. vMA handles authentication if the server has been established as a target server. Programs can use `VmaTargetLib` library commands. See "Using the VmaTargetLib Library" on page 33.
- **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.

Table 2-2 lists the vMA components that you can use for modifying scripts that include `proc` nodes and Linux commands.

Table 2-2. vMA Components for Use in Scripts

vMA Component	Description	For more information
vSphere CLI commands	Manage ESXi hosts and virtual machines.	*vSphere Command-Line Interface Installation and Reference Guide*.
`vifs` vSphere CLI command	Perform common operations, such as copy, remove, get, and put, on files and directories.	*vSphere Command-Line Interface Installation and Reference Guide*.
vSphere SDK for Perl	Access the vSphere API, a Web services based API for managing, monitoring, and controlling the lifecycle of all vSphere components.	*vSphere SDK for Perl Programming Guide*.
vSphere SDK for Perl utility applications	Perform common administrative tasks.	*vSphere SDK for Perl Utility Applications Reference.* Commands are on vMA in `/usr/lib/vmware-vcli/apps`
vSphere SDK for Perl WS Management component	Access CIM/SMASH data. 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.	*vSphere SDK for Perl Programming Guide*.

Configure vMA to Use a Static IP Address

During the first boot, vMA prompts you to specify whether to use a DHCP server or a static IP address when it starts. The DHCP server assigns a network address, allowing you to run the virtual machine without setup. This network address might change after the virtual machine has been powered off longer than the DHCP lease time. Most server applications should be configured to a static network address that is constant and well-known.

Configure a Static IP Address from the Console

You can configure a static IP address from the vMA console or the web UI.

To configure a static IP address from the console

1 In the console, select Configure Network and press Enter.

2 At the Use a DHCP server instead of a static IP address prompt, type no.

3 When prompted, provide the following information:

- IP Address
- Netmask
- Gateway
- DNS Server 1
- DNS Server 2
- Host name

4 When prompted, specify whether you need a proxy server to reach the Internet. If you answer yes, type the IP address and the port number of your proxy server.

5 Type y if the values on the review screen are correct. If the values are incorrect, enter no and repeat the procedure.

Configure a Static IP Address from the Web UI

You can configure a static IP address from the vMA console or the web UI.

To configure a static IP address from the web UI

1 Log in to the web UI.

2 Open the Network page and click the Address tab.

3 Select the Use the following IP settings option and provide the IP addresses for the following:

- IP Address
- Netmask
- Gateway
- Preferred DNS Server
- Alternate DNS Server
- Host name

4 Click Save Settings.

Configure vMA to Use a DHCP Server

You can reconfigure vMA to use a DHCP server instead of using a static IP address.

Configure vMA to Use a DHCP Server from the Console

To configure vMA to use a DHCP server from the console

1 On the vMA console, select Configure Network and press Enter.

2 At the Use a DHCP server instead of a static IP address prompt, type y.

3 When prompted, specify whether you need a proxy server to reach the Internet.

If you answer yes, type the IP address and port number of your proxy server.

A review of the network settings appears.

4 Type y if the values on the review screen are correct.

Configure vMA to Use a DHCP Server from the Web UI

To configure vMA to use a DHCP server from the web UI

1 Log in to the web UI.

2 Open the Network page and click the Address tab.

3 Select the Obtain configuration from DHCP server option.

4 Click Save Settings.

Setting the Time Zone

By default, the virtual hardware clock is maintained in Coordinated Universal Time (UTC), which vMA converts to local time. You can, however, set it to a local time, which is important for the update repository and VMware vCenter Update Manager.

Setting the Time Zone from the Console

You can set time zone from the console as described here.

To set the time zone from the console

1 On the console, select Set Timezone and press Enter.

2 When prompted, select your continent or region and press Enter.

3 When prompted, select your country and press Enter.

The screen displays the information that you have selected and the time that will be set.

4 Type 1 if the information is correct.

vMA sets the timezone.

Setting the Time Zone from the Web UI

You can set the time zone from the web UI by using the following steps.

To set the time zone from the Web UI

1 Access the web UI and log in.

1 Click the System tab then click the Time Zone button.

2 From the Time Zone Settings list, select your country and city.

3 Click Save Settings.

Shut Down vMA

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

To shut down vMA from vSphere Client

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.

To shut down vMA from the Web UI

3 Log in to the Web UI as vi-admin.

4 In the Information tab, click Shutdown.

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 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 20.

2 Shut down vMA.

3 Power off the virtual machine by using the vSphere Client.

4 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. Table 2-3 explains a few commonly encountered issues that are easily resolved.

Table 2-3. Troubleshooting vMA

Issue	Resolution
You can deploy vMA but when you start up the virtual machine, an error occurs.	Check whether your setup meets the hardware and software requirements listed in "Hardware Requirements" on page 12.
You add a server but the vSphere CLI command or Perl script still prompts for authentication.	Run `viftarget` for the target server.
You have added multiple servers. You do not know where vMA runs vSphere CLI commands if you do not specify `--server`.	After a call to `vifptarget`, 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 `/etc/resolv.conf` file. Add the following line for each DNS server in your network: `nameserver <dns server ip address>` Type `man resolv.conf` for details on that file. If vMA is set up for DHCP, and the network is restarted, changes you made to `/etc/resolv.conf` are lost.
Problems while adding Active Directory target or configuring vMA for Active Directory.	If you are unable to authenticate from vMA or cannot add vMA to the domain controller, check the following: ■ Your DNS server setup in vMA resolves the IP address or host name of the vCenter server to an FQDN and the FQDN contains the domain name to which vMA is added. ■ The `vifp listserver` command shows the name of vCenter as the FQDN that contains the domain name to which vMA is added as the suffix. ■ The date and time settings on vMA, the domain controller and vCenter Server are identical. Check the time zone as well. The time may not exactly be the same but may vary by an hour. However, a large skew in the time may cause authentication problems.

This release of vMA provides the `vma-support` script that enables you to collect various system configuration information and other logs. You can run this script by issuing the following command:

```
> sudo vma-support
```

The script generates the information and log bundle and appends it to the `vmware.log` file on the ESXi host on which vMA is deployed.

Update vMA

You can download software updates including security fixes from VMware and components included in vMA, such as the SUSE Linux Enterprise Server updates and JRE.

IMPORTANT You cannot upgrade a previous version of vMA to vMA 5.0. You need to install vMA 5.0.

To update vMA

1 Access the Web UI.

2 Log in as vi-admin.

3 Click the Update tab and then the Status tab.

4 Open the Settings tab and then from the Update Repository section, select a repository.

5 Click Check Updates.

6 Click Install Updates.

Configure Automatic vMA Updates

You can configure automatic download of vMA updates.

To configure automatic updates

1 Access the Web UI.

2 Log in as vi-admin.

3 Click the Update tab and then the Settings tab.

4 Click Automatic check for updates.

5 Set the schedule for performing the automatic checks by selecting a day and time from the drop down lists.

6 In the Update Repository section, select a repository.

7 Click Save Settings.

vMA Interfaces 3

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

This chapter includes the following topics:

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
`vifptarget`	`vifptarget`		"vifptarget Command for vi-fastpass Initialization" on page 27.

`vifp` (administrative interface)	`addserver`
	`removeserver`
	`rotatepassword`
	`listservers`
	`reconfigure`
			"vifp Target Management Commands" on page 28.

`VmaTargetLib` (library)	`enumerate_targets`
	`query_target`
	`login`
	`logout`
		`enumerateTargets`
		`queryTarget`
		`login`
		`logout`
			"Using the VmaTargetLib Library" on page 33.

vifptarget Command for vi-fastpass Initialization

You can run this command to perform the following tasks:

- Initialize vi-fastpass for the vSphere CLI and the vSphere SDK for Perl.
- Reset fastpass target
- Display the initialized fastpass target

Usage

```
vifptarget
--set     | -s <server>
--clear   | -c
--display | -d
--help    | -h
```

Description

The `vifptarget` command enables seamless authentication for remote vSphere CLI and vSphere SDK for Perl commands.

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

The vMA prompt displays the current default execution server. If you remove that default server, the server name is removed from the prompt but the vi-fastpass environment is not cleared and the vCLI commands can still run seamlessly against all the targets.

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

Options

Option	Description
`set`	Initializes the fastpass target.
`display`	Displays the initialized fastpass target.
`clear`	Clears the vi-fastpass environment.
`help`	Display help for the command.

Example

`vifptarget --set | -s <server>`

Initializes the fastpass target.

`vifptarget --display | -d`

Displays the initialized fastpass target.

`vifptarget --clear | -c`

Clears the vi-fastpass environment.

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.

vifp addserver

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

Usage

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

Description

After a server is added as a vMA target, you must run `vifptarget <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 `vifptarget` again is required after each logout. See "vifptarget Command for vi-fastpass Initialization" on page 27.

After you run `vifptarget`, 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 ESXi hosts 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 ESXi host, you can run commands without specifying the target.
- If you add multiple ESXi hosts, specify the target to avoid confusion.

See "Add Target Servers to vMA" on page 17 and "Running vSphere CLI for the Targets" on page 19.

IMPORTANT If you change a target server's name, you must remove it, and then add it to vMA with the new name.

Options

Option	Description
`server`	Name or IP address of the ESXi host or vCenter Server system to add as a vMA target.
`authpolicy`	Sets the authentication policy to fastpass authentication or the Active Directory authentication. The default value is `fpauth`.
`protocol`	Connection protocol. HTTPS by default.
`portnumber`	Connection port number of the target server. The default is 443.
`servicepath`	Service path URL of the target server. The default is `/sdk`.
`username`	User who connects to the target server. If the target server points to an ESXi host, the default is root. The user must have superuser privileges on the ESXi host. If the target server 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.
`password`	Password of the user specified by `username`.

Example

`vifp 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.

`vifp addserver myESX42`

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

vifp removeserver

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

If the target is an 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, without the password.

Usage

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

Description

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 this server to vMA, vMA creates two more accounts on this server. Run `vifp removeserver` to avoid having multiple users created by vMA on each target server.

Options

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

Examples

`vifp removeserver <vCenter_Address>`

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

`vifp removeserver <esxi_Address>`

Removes an ESXi host.

vifp rotatepassword

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

IMPORTANT This command applies only to ESXi target servers with the `fpauth` authentication policy. You cannot rotate passwords for targets with adauth authentication policy and for vCenter Server targets.

Usage

```
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. vMA attempts the password rotation at midnight.

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

Options

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

Examples

vifp rotatepassword --now

Immediately rotates passwords of all ESXi vMA target servers.

vifp rotatepassword --now --server <server_address>

Immediately rotates the password of a specific server.

vifp rotatepassword --days 7

Sets the password rotation policy to rotate the password of all ESXi vMA targets every seven days.

For example, if you add server1 on 9/1, and server2 on 9/2, and run `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 then run `vifp rotatepassword --days 3`, vMA rotates the server1 password on 9/18 and the server2 password on 9/19.

vifp rotatepassword

Displays the current password rotation policy.

vifp listservers

Lists target systems.

Usage

```
listservers [-l | --long]
```

Description

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

Example

vifp listservers --long

Lists all servers that are vMA targets, for example:

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

vifp reconfigure

Reconfigures target systems. This can be done to change authentication policy or the configured Active Directory user.

Usage

```
reconfigure <server>
    [--authpolicy <fpauth | adauth>]
    [--protocol <http | https>]
    [--portnumber <portnum>]
    [--servicepath <servicepath>]
    [--username <username>]
    [--password <password>]
```

Description

You can use this command to reconfigure the authentication policy or the users. This command can be run only by administrators.

Options

Option	Description
`server`	Name or IP address of the ESXi host or the vCenter Server system to be reconfigured.
`authpolicy`	Indicates if the target uses the fastpass authentication or the Active Directory authentication. The default value is `fpauth`.
`protocol`	Connection protocol. HTTPS by default.
`portnumber`	Connection port number of the target server. The default is 443.
`servicepath`	Service path URL of the target server. The default is `/sdk`.
`username`	User who connects to the target server. If the target server points to an ESXi host, the default is root. The user must have superuser privileges on the target server. If the target server points to a vCenter Server system, the default user is the one configured for the vCenter system in the previous session. For example, if vCenter was added or reconfigured with the user name administrator in the previous session, the default user for the `vifp reconfigure` command is administrator.
`password`	Password of the user specified by `username`.

Target Management Example Sequence

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

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

Using the VmaTargetLib Library

The VmaTargetLib library allows you to programmatically connect to vMA targets by using Perl or Java. Agents can link with `VmaTargetLib` and use vi-fastpass functionality. The `VmaTargetLib` library allows you to enable vi-fastpass authentication and to query or list one or more targets with the following commands:

- `EnumerateTargets` – Retrieves a list of all servers that are vMA targets.
- `QueryTarget` – Retrieves connection information for a target server.
- `Login` – Connects to a target server.
- Logout – Logs you out of the target server.

See the `VmaTargetLib` java library for a more detailed reference to the Java interface. You can find samples in `/opt/vmware/vma/samples`.

VmaTargetLib Reference

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

Enumerating Targets

Usage

Perl	`enumerate_targets()`
Java	`enumerateTargets()`

Description

Returns a list of target vCenter Server or ESXi systems added to the vMA instance by using `vifp addserver`.

Options

None

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 use those credentials to connect to the vMA target.

Options

Option	Description
`servername`	One of the servers added to this vMA instance using `vifp addserver`. Can be an ESXi host or a vCenter Server system.

Returns

Returns a specific vMA target server.

Programmatic Login

Usage

Perl `VmaTarget.login()`

Java `VmaTarget.login()`

Description

Allows a 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 `vifp addserver.`

Returns

Returns 1 if successful and 0 otherwise.

Programmatic Logout

Usage

Perl `VmaTarget.logout()`

Java `VmaTarget.logout()`

Description

Allows a program to log out of a target server programmatically.

Options

Option	Language	Description
`servername`	Java, Perl	One of the servers added to this vMA instance using `vifp addserver.`

Index