vSphere Management Assistant Guide

vSphere 6.5

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-002327-00

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 VMware vSphere® Management Assistant and includes reference information forvSphere Management Assistant CLIs and libraries. To view the current version of VMware API and SDK documentation, go to http://www.vmware.com/support/pubs/sdk_pubs.html.

Important The vMA 6.5 release is the last release of vSphere Management Assistant. No future updates to vMA are expected. As alternatives to vMA, you can use PowerCLI or vCLI. For information, see vSphere Management Assistant Deprecation.

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 *vSphere Management Assistant Guide*, is revised with each release of the product or when necessary. A revised version can contain minor or major changes.

Revision	Description
15NOV2016	vMA 6.5 release
12MAR2015	vMA 6.0 release
31OCT2013	vMA 5.5 release
10SEP2012	vMA 5.1 release
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 capabilities of vMA, 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 vSphere Management Assistant 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.

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. The administrators can use vMA to run scripts or the agents can use vMA to interact with ESXi hosts and vCenter Server systems without having to authenticate each time.

This chapter includes the following topics:

vMA Capabilities

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

Important The vMA 6.5 release is the last release of vSphere Management Assistant. No future updates to vMA are expected. As alternatives to vMA, you can use PowerCLI or vCLI. For information, see vSphere Management Assistant Deprecation.

- As an administrator, you can add vCenter Server systems and ESXi hosts as targets and run scripts and programs on these targets. After you authenticate while adding a target, you need not log in 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 pre-configured with two user accounts.
  - 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 applicable.

- vMA can run agent code that makes proprietary hardware or software components compatible with VMware ESXi. The code currently runs in the service console of existing ESXi hosts. You can modify most of the 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.

Important The vMA 6.5 release is the last release of vSphere Management Assistant. No future updates to vMA are expected. As alternatives to vMA, you can use PowerCLI or vCLI. For information, see vSphere Management Assistant Deprecation.

vMA includes the following components:

Components	Description
SUSE Linux Enterprise Server 11 SP3	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	The interface to the hyper visor.
vSphere CLI	Commands for managing vSphere from the command line. See the *vSphere Command-Line Interface Installation* and *Reference Guide*.
vSphere SDK for Perl	A 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	The Runtime engine for Java-based applications built with the vSphere Web Services SDK.
vi-fastpass	Authentication component.

vSphere Authentication Mechanism

The vMA 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 can use vi-fastpass or Active Directory authentication. For vi-fastpass authentication, the credentials that a user has on the VMware vCenter Server system or VMware 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 "ConfigurevSphere Management Assistant for Active Directory Authentication," on page 15 Configure vMA for Active Directory Authentication.

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 are asked for a user name and password.

You can initialize vi-fastpass in two ways:

- Run `vifptarget`. For more information about this script, see "vifptarget command for vi-fastpass initialization," on page 29

Call the `Login` method in a Perl or Java application. For more information about this method, see "VmaTargetLib Reference," on page 37.

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

Each time you log in to vMA, you must run the`vifptarget`command or the `Login` method at least once. The target that you select in the`vifptarget` command is the default target. Target servers remain targets across reboots. To set another host as the target, use the `--server` command 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 vMA samples are available in the `/opt/vmware/vma/samples` file after vMA is installed.

Table 1-1.

Command	Description
`bulkAddServers.pl`	A Perl sample that adds multiple targets to vMA.
`mcli.pl`	A Perl sample that runs a vSphere CLI command on multiple vMA targets listed in a file supplied as an argument. You must run `vifptarget` before running this script.
`listTargets.pl`	A Perl sample that retrieves information and version of vMA targets using `VmaTargetLib`.
`listTargets.sh`	A Java sample that demonstrates use of `VmaTargetLib`.

vMA Use Cases

The following are a few examples of a typical vMA use case.

Writing or Converting Scripts

You can run existing vSphere CLI or VMware 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

You can use vMA to write or convert agents.

You can write a new agent in Perl in the following situations.

- When a partner or customer writes a new agent in Perl, the Perl script must import the `VmaTargetLib` Perl module and all VMware vSphere SDK for Perl modules. Instead of calling the VMware vSphere SDK for Perl `subroutine Util::Connect(targetUrl, user name, 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 VMware 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.

Getting Started with vMA 2

You should have some experience setting up a Linux system and working in a Linux environment. The getting started 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.

Important The vMA 6.5 release is the last release of vSphere Management Assistant. No future updates to vMA are expected. As alternatives to vMA, you can use PowerCLI or vCLI. For information, see vSphere Management Assistant Deprecation.

For background information about vMA functionality and available vMA components, see Chapter 1, "Introduction to vMA," on page 7.

Note You cannot upgrade an earlier version of vMA to vMA 6.0. You must install a new vMA 6.0 instance.

This chapter includes the following topics:

Hardware Requirements

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

The VMware 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
- Intel processors that have EM64T support but do not have VT support enabled, and do not support a 64-bit guest OS.

For detailed hardware requirements, see the Hardware Compatibility List on the VMware Web site.

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

Software Requirements

The following are the software requirements for vMA.

You can deploy vMA on the following versions of vSphere:

- vSphere 6.0
- vSphere 5.5 and later
- vSphere 5.1 and later
- vSphere 5.0 and later

You can deploy vMA by using a vSphere Web Client connected to an ESXi host or by using a vSphere Web Client connected to vCenter Server 6.0, vCenter Server 5.5 or later, vCenter Server 5.1 or later, or vCenter Server 5.0 or later.

You can use vMA to target ESXi 5.0 and later systems, including ESXi 6.0.

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 login credentials:

- 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.

  Note You can log in to vCenter Server only if they are in a domain that has been added as a vCenter Single Sign-On Identity Source. vCenter Single Sign-On administrator users can add identity sources from the vSphere Web Client. For more information about adding a vCenter Single Sign-On Identity Source, see *vSphere documentation*.

  If you are using vCenter Server Appliance, for SSO authentication, add a CM server entry to `/etc/hosts` of vMA and ensure that the date and time is synchronized between vMA and CM server.

- 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.

  Note You can enable the root account if the root account password is set by `sudo passwd` in the appliance. To run privileged commands, type `sudo passwd root`. By default, only vi-admin can run commands that require sudo. The root account is solely used to set configuration options related to security and meeting compliance standards.

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 The vMA 6.5 release is the last release of vSphere Management Assistant. No future updates to vMA are expected. As alternatives to vMA, you can use PowerCLI or vCLI. For information, see vSphere Management Assistant Deprecation.

Note You cannot upgrade an earlier version of vMA to vMA 6.0. You must install a new vMA 6.0 instance.

Procedure

1. Use a vSphere Web Client to connect to a system that is running the supported version of ESXi or vCenter Server.
2. If connected to a vCenter Server instance, 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 Enter 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 VMware vCenter Server system, you can select a folder.

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

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

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

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

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

   Note Ensure that vMA is connected to the management network on which the VMware vCenter Server system and the VMware 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 selected host. The deployment 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.

Procedure

1 In the vSphere Web Client, right-click the virtual machine and click **Power On**.

2 Select the **Console** tab.

3 To configure the network settings, select the appropriate menu item.

   You can configure each of the various network settings such as an IP address, the host name, DNS, the proxy server, and the default gateway, by selecting the appropriate menu item.

   The host 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 may 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.

   If you use a static IPv4 network configuration to configure the IP address, DNS, default gateway, and host name, then you must also configure a default IPv6 gateway during the first-boot network configuration, else the vMA might be unreachable in the network after log in.

   Ensure that you finish the network configuration at the first boot. If you skip the network configuration, the appliance takes the default network configuration from the Guest OS, which might lead to some inconsistencies. Note: You can configure only one network adapter in vMA. You cannot add and configure multiple network adapters in vMA.

   Note You can configure only one network adapter in vMA. You cannot add and configure multiple network adapters in vMA.

4 When prompted, enter 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 be nine characters long.
- At least one upper case character
- At least one lower case character
- At least one numeral character
- At least one symbol such as #, $

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

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 perform 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 vSphere Management Assistant for Active Directory Authentication

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

Add vMA to a domain

Use the following procedure to add vMA to a domain.

Prerequisites

- Verify 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.
- Verify that the Active Directory domain is accessible from vMA.

- You must be able to ping the ESXi and vCenter Server systems that you want to add to vMA.
- Verify that pinging resolves the IP address to *targetservername.domainname*, where domain name is the domain to which vMA is to be added.

Procedure

1 Run the following command from the vMA console:

`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.

What to do next

Add an Active Directory target to vMA. See "Adding Target Servers," on page 18

Check Domain Settings

Use the following procedure to check vMA domain settings.

Prerequisites

Add a domain in vMA.

Procedure

- 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.

Remove vMA From the Domain

Use the following procedure to remove vMA from the domain.

Prerequisites

A domain must exist in vMA.

Procedure

- Run the following command from the vMA console, to remove vMA from the domain: `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 ESXi 4.1 Update 3 and later.

Prerequisites

Verify that the Active Directory is set up for unattended log in.

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.

Procedure

1 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`.

2 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.

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

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

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

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

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

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

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

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

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.

Note 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-user or log in as an Active Directory user to vMA.

To enable the vi-user account

Procedure

1 Log in to vMA as vi-admin.

2 Run the Linux password command for vi-user as follows:`sudo passwd vi–user`

When you run the `sudo` command for the first time on vMA, a message about root user privileges appears, and you are prompted for the vi-admin password.

3 Enter the vi-admin password.

4 When prompted, enter 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 **sudo** users 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. The user can run only commands on target ESXi hosts that do not require administrative privileges.

vMA User Account Privileges

The list of privileges that different user accounts have for vCLI usage against different targets are listed in the following table:

Table 2-1. Account Privileges for vCLI Usage

Target	Authentication Policy	vi-admin	vi-user	domain user
ESXi	fpauth	Yes	Yes	No
ESXi	adauth	Yes	No	Yes
vCenter Server	fpauth	Yes	No	No
vCenter Server	adauth	Yes	No	Yes

Adding Target Servers

After you configure vSphere Management Assistant, 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 credentials of a user who can connect to that system.

For more information about the complete syntax, see "vifp addserver," on page 31.

Add a vCenter Server System as a vMA target for Active Directory Authentication

Use the following procedure to add a vCenter Server system as a vMA target for Active Directory authentication.

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

Procedure

1 Log in to vMA as vi-admin.

2 To add a server as a vMA target, run 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 username 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 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. If the name of a target server changes, you must remove the target server by running `vifpremoveserver` with the old name, and then add the server using `vifp addserver` with the new name.

Add a vCenter Server System as a vMA Target for Fastpass Authentication

Use the following procedure to add a vCenter Server system as a vMA target for fastpass authentication.

Procedure

1 Log in to vMA as vi-admin.

2 To add a server as a vMA target, run 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.

Add an ESXi Host as a vMA Target for Active Directory Authentication

Use the following procedure to add an ESXi host as a vMA target for Active Directory authentication.

Procedure

1 Log in to vMA as vi-admin.

2 Add an ESXi server as a vMA target by running the following command: `vifp addserver server3.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 ESXi Server. 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, for example: `esxcli 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 for Fastpass Authentication

Use the following procedure to add an ESXi host as a vMA target for fatspass authentication.

Procedure

1 Log in to vMA as vi-admin.

2 Add an ESXi server as a vMA target by running the following command: **`vifp addserver server2.mycomp.com --authpolicy fpauth`**

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

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 Web 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 have deleted the vMA virtual machine, but did not remove the target servers.

4 Review and accept the security risk information.

5 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
```

6 Set the target as the default for the current session. **`vifptarget --set | -s <server>`**

7 Verify that you can run a vSphere CLI command without authentication by running a command, for example:**`esxcli 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.

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, as 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 the hostname or IP of the target apply to the target specified.
- Programmatic connection – In Perl scripts or Java applications, 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. Applications can use `VmaTargetLib` library commands. See "Using the VmaTargetLib Library," on page 36.
- 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 by running the vSphere CLI commands available on vMA.
- Target specification – You must specify the target server when you run commands or scripts.

The following table 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
vSphere CLI commands	Manage ESXi hosts and virtual machines. For more information, see *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. For more information, see *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 life cycle of all vSphere components. For more information, see *vSphere SDK for Perl Programming*
vSphere SDK for Perl utility applications	Perform common administrative tasks. For more information, see *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 the underlying server components such as CPU, fans, power supplies. For more information, see *vSphere SDK for Perl Programming Guide.*

Running vSphere CLI for the Targets

If you have added multiple target servers, you should specify the target server explicitly when running commands. By default, vMA executes commands on the server that is configured as the default target by using the `vifptarget –s` command. If none of the added target servers are configured as the default target and no target server is explicitly specified when running the vSphere CLI commands, then the commands are run against the vMA itself.

Procedure

1 Add servers as vMA targets.

```
vifp addserver server1
```

```
vifp addserver server2
```

2 Check whether the target server has been added:

```
vifp listservers
```

3 Run `vifptarget`.

```
vifptarget –s server2
```

The command initializes the specified target server. This server is set 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.

```
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 conversely.
- Change the configured user for the Active Directory target.
- Recover users for the vi-fastpass target. A user must 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.

Change the Authentication Policy

You can change the authentication mode of a vMA target.

Procedure

1 Log in to vMA as vi-admin.

2 Run the `reconfigure` command.

```
vifp reconfigure servername --authpolicy authpolicy
```

3 When prompted, provide your credentials.

- To reconfigure an Active Directory target to vi-fastpass authentication, specify the root password for ESXi targets and the root user name and password for vCenter targets.
- To reconfigure a vi-fastpass target to Active Directory authentication, specify the root user name for the target.

Change the Configured User or To Recover Users

You can change the configured user for the Active Directory target.

Procedure

1 Log in to vMA as vi-admin.

2 Run `reconfigure`.

```
vifp reconfigure servername
```

3 When prompted, provide your credentials.

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

Note If the target server is not initialized as the default target, then you must run the `vifptarget -s` command against the target server to reinitialize it with the new credentials after you reconfigure the target.

Example: 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.

Remove a vCenter Server System from vMA

You can remove a vCenter Server system from vMA virtual machine.

Procedure

1 Log in to vMA as vi-admin.

2 Run the following command to remove a target vCenter Server system from vMA:

`vifp removeserver servername`

The vCenter Server system is no longer a vMA target.

Remove an ESXi Host from vMA

You can remove a ESXi host from vMA.

Procedure

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 user names.

Configure Automatic Updates for vMA

You can configure automatic download of vMA updates.

To configure automatic updates

Procedure

1 Access the Web UI.

2 Log in as vi-admin.

3 Click the **Update** tab, and then the **Status** tab.

4 Click **Automatic check for updates**.

5 Set the schedule for performing the automatic checks.

6 In the **Update Repository** section, select a repository.

7 Click **Save Settings**.

Configure vMA to Use a Static IP Address

During the first boot of vMA, you can configure vMA to use a DHCP server or a static IP address.

The DHCP server assigns a network address that permits 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 must 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.

Procedure

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

2 Select menu option **6** to configure the IP address.

3 To configure an IPv6 address, press **y** and press Enter.

   a Press Enter to specify a static IP address and provide the IP address and Netmask.

   b Press **y** and press Enter to confirm the IP address.

4 To configure an IPv4 address, press **y** and press Enter.

   a Press Enter to specify a static IP address and provide the IP address and Netmask.

   b Press **y** and press Enter to confirm the IP address.

5 To configure the other network settings, such as DNS and default gateway, select the appropriate menu option and provide the required network configuration details.

Configure a Static IP Address from the Web UI

You can configure a static IP address from the Web UI.

Procedure

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

Use the following procedure to configure vMA to use a DHCP server from the console.

Procedure

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

2 Select menu option **6** to configure the IP address.

3 To configure an IPv6 address, press **y** and press Enter.

   a Press **y** and press Enter to use a DHCP server.

   b Provide the details of the DHCP server.

4 To configure an IPv4 address, press **y** and press Enter.

   a Press **y**, and press Enter to use a DHCP server.

   b Provide the details of the DHCP server.

5 To configure the other network settings, such as DNS and default gateway, select the appropriate menu option and provide the required network configuration details.

Configure vMA to Use a DHCP Server from the Web UI

Use the following procedure to configure vMA to use a DHCP server from the Web UI.

Procedure

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 vSphere Update Manager.

Setting the Time Zone from the Console

Use the following steps to set the time zone from the console.

Procedure

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 selected information and the time that is set is displayed on the screen.

4 Type **1** if the information is correct.

vMA sets the time zone.

Setting the Time Zone from the Web UI

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

Procedure

1 Access the Web UI and log in.

2 On the **System** tab, click **Time Zone**.

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

4 Click **Save Settings**.

Shut Down vMA

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

Shut Down vMA from vSphere Web Client

The following procedure lists the steps to shut down vMA from the vSphere Web Client.

Procedure

1 To shut down the operating system, run a Linux command such as the `halt` command on the vMA command line.

2 Power off the vMA virtual machine from the vSphere Web Client.

To Shut Down vMA from the Web UI

The following procedure lists the steps to shut down vMA from the Web UI.

Procedure

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

2 On the **Information** tab, click **Shutdown**.

Delete vMA

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

Note 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.

Prerequisites

Remove all vMA target servers you added. For more information, see "Remove Target Servers from vMA," on page 24.

Procedure

1 Shut down vMA.

2 Power off the virtual machine by using the vSphere Web Client.

3 In the vSphere Web Client, right-click the virtual machine and select **Delete from Disk**.

Update vMA

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

Important You cannot upgrade an earlier version of vMA to vMA 6.0. You need to install a new vMA 6.0 instance.

To update vMA

Procedure

1 Access the Web UI.

2 Log in as vi-admin.

3 Click the **Update** tab, and then the **Status** tab.

4 On the **Settings** tab, select a repository from the Update Repository section.

5 Click **Check Updates**.

6 Click **Install Updates**.

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

Following table 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 29

`vifp` (administrative interface)	`addserver`
	`removeserver`
	`rotatepassword`
	`listservers`
	`reconfigure`
			"vifp Target Management Commands," on page 31

`VmaTargetLib` (library)	`enumerate_targets`
	`query_target`
	`login`
	`logout`
		`enumerate_targets`
		`query_target`
		`login`
		`logout`
			"Using the VmaTargetLib Library," on page 36

vifptarget command for vi-fastpass initialization

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

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 further 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 reboot, you must run `vifptarget` after each log out to enable vi-fastpass for vSphere CLI and vSphere SDK for Perl commands.

Options

Options	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: 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 29.

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` command. 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 "Adding Target Servers," on page 18 and "Running vSphere CLI for the Targets," on page 22.

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

Table 3-2. 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`.

Table 3-2. Options (Continued)

Option	Description
`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*.

```
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 enter the `<server>` command, 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. To avoid having multiple users created by vMA on each target server, run the `vifp removeserver` command.

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`.

Option	Description
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.

`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.

Note 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.

`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]
[--sortby <name | ptype | apolicy | version | build>]
[--listby ptype [esx | esxi | vcenter] apolicy [adauth | fpauth] version
[v1-v2 | v] build [b1-b2| b] and [Repeat any of the above listby parameters]]
```

Description

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

```
vifp listservers
```

Lists all servers that are vMA targets, for example:

```
server1.mycomp.com       ESX      version number    build number
server2.mycomp.com       ESX      version number    build number
server3.mycomp.com       ESXi     version number    build number
vc42.mycomp.com          vCenter  version number    build number
```

```
vifp listservers -l
```

List all the servers in long format:

```
server1.mycomp.com       ESX      version number    build number
```

```
server1.mycomp.com       ESX      fpauth    version number    build number
server2.mycomp.com       ESX      fpauth    version number    build number
server3.mycomp.com       ESXi     fpauth    version number    build number
vc42.mycomp.com          vCenter  fpauth    version number    build number
```

```
vifp listservers --listby ptype ESX
```

List servers of ptype ESX:

```
vifp listservers --listby ptype ESXi
```

List servers of type ESXi:

```
server1.mycomp.com    ESXi   version number   build number
server2.mycomp.com    ESXi   version number   build number
server3.mycomp.com    ESXi   version number   build number
```

```
vifp listservers --listby ptype vcenter
```

List servers of type vCenter:

```
vc42.mycomp.com   vCenter    version number   build number
```

```
vifp listservers --listby ptype ESXi --sortby version
```

List servers of type ESXi and sort by version:

```
server1.mycomp.com      ESXi     5.0.0    build number
server2.mycomp.com      ESXi     5.5.0    build number
server3.mycomp.com      ESXi     6.0.0    build number
```

```
vifp listservers --listby ptype esxi version 5.5.0 --sortby version
```

List servers of type ESXi with 5.5.0 and sort by version:

```
server1.mycomp.com      ESXi     5.5.0    build number
server2.mycomp.com      ESXi     5.5.0    build number
```

```
vifp listservers --listby ptype esxi version 5.5.0 --sortby name
```

List servers of type ESXi and version 5.5.0 and sort by name:

```
server1.mycomp.com      ESXi     5.5.0     build number
server2.mycomp.com      ESXi     5.5.0     build number
```

vifp reconfigure

The `vifp reconfigure` command reconfigures target systems. You can 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. You need to have admin right to run this command.

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.`

Option	Description
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` command 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 connect to vMA targets programmatically 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 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 applications.

Enumerating Targets

This command returns a list of target vCenter Server or ESXi systems, which are added to the vMA instance.

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

This command allows a caller to retrieve login credentials from a vMA target and use the credentials to connect to the vMA target.

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

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

Returns

Returns a specific vMA target server.

Programmatic Login

This command allows an application to log in to a target server programmatically.

Usage

Perl: `VmaTarget.login()`

Java: `VmaTarget.login()`

Description

Allows an application to log in to a target server programmatically.

Options

Options	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

This command allows an application to log out of a target server programmatically.

Usage

Perl: `VmaTarget.logout()`

Java: `VmaTarget.logout()`

Description

Allows an application to log out of a target server programmatically.

Options

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

Troubleshooting with vMA

4

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

Table 4-1. 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.
Enable the 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 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 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. You can use the vma-support script 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 where vMA is deployed.

Troubleshooting Unattended Authentication

5

If you are unable 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.

Index

W