vSphere Management Assistant Guide

vSphere 4.1

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-000319-00

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

Copyright © 2008–2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

Contents

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.

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
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 is now a CentOS-based virtual machine. 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 ESX/ESXi hosts and vCenter Server systems. Developers can create agents that interact with ESX/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.

1 Introduction to vMA

The vSphere Management Assistant (vMA) is a CentOS-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 ESX/ESXi and vCenter Server systems without having to authenticate each time. vMA can also collect and store ESX/ESXi and vCenter Server logs for analysis.

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 servers and ESX/ESXi systems 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.
- 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 ESX 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, ESX, or ESXi system 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 and Common Information Model (CIM) providers, 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 resulting virtual machine that includes all vMA components. You can use the `vma-update` utility from inside vMA to download updates and VMware components, including the operating system. See "Appendix: Updating vMA with vma-update" on page 35.

vMA includes the following components.

- CentOS release 5.3 64-bit Enterprise Linux – vMA runs CentOS on the virtual machine. You can move files between the ESX/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.
- SMI-S – vMA includes the VMware implementation of the CIM profiles compatible with the Storage Management Initiative Specification (SMI-S version 1.0.2) of the Storage Network Industry Association. With vMA 4.1, you can specify ESX/ESXi and vCenter Server systems as target servers. The script that establishes the SMI-S target server uses the VmaTargetLib library.
- Java JRE version 1.6 – Runtime engine for Java-based applications built with the vSphere Web Services SDK.

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

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

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

vSphere Authentication 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, ESX, or ESXi system are stored in a local credential store. For Active Directory authentication, the user is authenticated with an Active Directory server.

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

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

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

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 using one of the following methods:

- Run `vifptarget`. For more information about this script, see "vifptarget Command for vi-fastpass Initialization" on page 24.
- Call the `Login` method in a Perl or Java program. For more information about this method, see "VmaTargetLib Reference" on page 32.

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 ESX or ESXi system that is managed by a vCenter server, you can use the `–vihost` option.

You need to run the `vifptarget` command or the `Login` method once, each time you log in to vMA. 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
```

vSphere Logging Component

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

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

By default, `vilogd` places the logs in `/var/log/vmware`. To specify a different log location, change the `/etc/vmware/vMA/vMA.conf` file. `vilogd` places the logs in the new location.

vMA Samples

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

- `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 `vifplib` Perl module and all vSphere SDK for Perl modules. Instead of calling the vSphere SDK for Perl subroutine `Util::Connect(targetUrl, username, password)`, the agent calls `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 ESX/ESXi hosts:

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

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

  ```
  LoginToMyEsx(String myESXName) {
  VmaTarget target = VmaTargetLib.queryTarget(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 ESX/ESXi system and ports the agent to vMA.

  Instead of calling the vSphere SDK for Perl method `Util::Connect()`, the agent calls the `vifp` library method `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 can upgrade a vMA 4.0 system to vMA 4.1 GA. However, you cannot upgrade a VIMA 1.0 system to vMA 4.1.

This chapter includes the following topics:

Hardware Requirements

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

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

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

Opteron 64-bit processors earlier than rev E, and Intel processors that have EM64T support but 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 5GB of storage space for the vMA virtual disk. The recommended memory for vMA is 512MB.

Software Requirements

You must have the following software to deploy vMA:

- vSphere 4.1
- vSphere 4.0 – You can deploy vMA to ESX/ESXi systems using a vSphere Client connected directly to the ESX/ESXi system or using a vSphere Client connected to a vCenter Server 4.0 system.
- ESX/ESXi 3.5 Update 2 and later – You can deploy on ESX/ESXi 3.5 Update 2 or later using a vSphere 4.0 Client.
- vSphere Client – You need a vSphere Client for deploying vMA.

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

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

Required Authentication Information

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

- vCenter Server system – If you want to use a vCenter Server system as the target server, you must be able to connect to that system.

  If you are using a vCenter Server target, you do not need passwords for the ESX/ESXi systems that vCenter Server system manages, unless you run commands that do not support vCenter Server targets.
- ESX/ESXi host – You must have the root password or the user name and password for a user with administrative privileges for each ESX/ESXi host you add as a vMA target. You do not need the authentication information when you remove a target host.
- vMA – When you first log in to vMA, vMA prompts for a password for the vi-admin user. Specify a password and remember it for subsequent logins. The vi-admin user has root privileges on vMA.

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

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 can upgrade a vMA 4.0 system to vMA 4.1. However, you cannot upgrade a VIMA 1.0 system to vMA 4.1

To deploy vMA

1 Use a vSphere Client to connect to a system that is running ESX/ESXi 4.1, ESX/ESXi 4.0, ESX/ESXi 3.5 Update 2 or later, or vCenter Server 4.0.

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 file** 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 download details are displayed.

7 Accept the license agreement.

8 (Optional) Specify a name for the virtual machine.

9 Select a 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 network mapping and click **Next**.

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

13 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.

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

4 When prompted, specify a host name for vMA.

The name can include upto 64 alphanumeric characters.

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

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

This user has root privileges.

The prompt uses the Linux `passwd` utility:

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

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

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

Configure vMA for Active Directory Authentication

Configure vMA for Active Directory authentication so that ESX and vCenter servers 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. If you want to change the DNS server, you can use the following command:

```
sudo system-config-network-tui
```

Ensure that the domain is accessible from vMA. Also, ensure that you can ping the vCenter server systems that you want to add to vMA and that pinging resolves the vCenter IP address to `<VCservername.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 16.

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.

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/kerberos/bin/kinit -k -t /home/local/VMA-DC/foo/foo.keytab foo'
```

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

For every domain user who adds a target to vMA, update this script in order to renew the ticket. Also, install a keytab file for every such user. If more than one target uses the same domain user, then only one entry is sufficient for all those targets.

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 listserver` 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 ESX/ESXi systems and cannot run any `vilogger` commands or any commands that require sudo execution.

You cannot use vi-user to run commands for Active Directory targets (ESX or vCenter). 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 vMA root password.

3 If you are prompted for the vMA root password, specify the vi-admin password.

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

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

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

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

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

Add Target Servers to vMA

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

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

See "vifp addserver" on page 24 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
```

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 ESX/ESXi hosts, for example:

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

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 ESX/ESXi hosts, for example:

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

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 ESX/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 ESX/ESXi host that you want to add.

vMA does not retain the root password. Instead, vMA adds vi-admin and vi-user to the ESX/ESXi host, and stores the encrypted 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:

```
vicfg-nics -l
```

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

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 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.

3 Verify that the target server has been added:

```
vifp listservers
```

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

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

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

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

Use the following command for an Active Directory target:

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

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, specify the root user name on the target server.

To change the configured user or to recover users

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

2 Run `reconfigure.`

```
vifp reconfigure <servername>
```

3 When prompted, specify the root user name on the target server.

Remove Target Servers from vMA

Before you delete a vMA virtual machine, remove all target servers from vMA. If you do not remove target ESX/ESXi 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 a user that can connect to the vCenter Server system.

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 ESX/ESXi host from vMA

1 Log in to vMA as vi-admin.

2 To remove an ESX/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. The Linux installation is running on vMA, not on the ESX/ESXi host.
- **Access to ESX/ESXi files** – If you need access to folders or files on an ESX/ESXi host, you can make that host a target server and use the `vifs` vSphere CLI command to view, retrieve, or modify folders and files.

- **References to localhost** – Scripts cannot refer to `localhost`.
  - If vMA has only one target server initialized for vi-fastpass, all commands apply to that target server.
  - If vMA has multiple target servers initialized for vi-fastpass, specify the host name or the IP address for the target server.
- **Programmatic connection** – In Perl scripts or Java programs, 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 `vifplib` library commands. See "Using the VmaTargetLib Library" on page 32.
- **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 2-1 lists the vMA components that you can use for modifying scripts that include `proc` nodes and Linux commands.

Table 2-1. vMA Components for Use in Scripts

vMA Component	Description	For more information
vSphere CLI commands	Manage ESX/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. ESX/ESXi supports many Systems Management Architecture for Server Hardware (SMASH) profiles, enabling system management client applications to check the status of underlying server components such as CPU, fans, power supplies, and so on.	*vSphere SDK for Perl Programming Guide*.

Shut Down vMA

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

To shut down the vMA virtual machine

1 Shut down the operating system using a Linux command such as the `halt` command on the vMA command line.

2 Power off the vMA virtual machine using the vSphere Client.

Delete vMA

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

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

To delete the vMA virtual machine

1 Remove all vMA target servers you added. See "Remove Target Servers from vMA" on page 19.

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

Table 2-2. Troubleshooting vMA

Issue	Resolution
You can deploy vMA but when you start up the virtual machine, an error 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.

vMA Interfaces 3

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

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 24.

`vifp` (administrative interface)	`addserver`
	`removeserver`
	`rotatepassword`
	`listservers`
	`reconfigure`
			"vifp Target Management Commands" on page 24.

`vilogger` (logging interface)	`enable`
	`disable`
	`updatepolicy`
	`list`
			"vilogger Daemon and Log Management Commands" on page 28.

`VmaTargetLib` (library)	`enumerate_targets`
	`query_target`
	`login`
	`logout`
		`enumerateTargets`
		`queryTarget`
		`login`
		`logout`
			"Using the VmaTargetLib Library" on page 32.

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 prompt does not change until you have explicitly changed to a different default execution server.

While hosts remain target servers across vMA reboots, you must run `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`	Resets the fastpass target.
`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
```

Resets the fastpass target.

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 or ESX/ESXi system 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 24.

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

See "Add Target Servers to vMA" on page 16 and "Running vSphere CLI for the Targets" on page 18.

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 ESX/ESXi or vCenter Server system to add as a vMA target.
`authpolicy`	Sets the authentication policy to fastpass authentication or the Active Directory authentication.
`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 ESX/ESXi system, the default is root. The user must have superuser privileges on the ESX/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 ESX/ESXi system 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 ESX/ESXi system, you need superuser privileges for removal. If the target is a vCenter Server system, any user with connection privileges can remove the target. You only have to specify the `<server>` option, 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 add a server on which vi-admin and vi-user already exist, to vMA, vMA uses replacement user names for those accounts. Run `vifp removeserver` to avoid having multiple users created by vMA on each target server.

Options

Option	Description
`server`	Name or IP address of the ESX/ESXi or 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 ESX/ESXi systems, 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 <esx_Address>`

Removes an ESX/ESXi system.

vifp rotatepassword

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

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

Usage

```
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`	ESX/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 ESX/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 ESX/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 ESX/ESXi or vCenter Server system to be reconfigured.
`authpolicy`	Indicates if the target uses the fastpass authentication or the Active Directory authentication.
`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 ESX/ESXi system, 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 ESX host, lists servers, runs `vifptarget` to enable vi-fastpass, runs a vSphere CLI command, and removes the ESX 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
vicfg-mpath --list
cdrom vmhba0:1:0 (0MB has 1 paths and policy of fixed
    Local 0:7:1 vmhba0:1:0 On active preferred
.....
vifp removeserver server1.company.com
root@server1.company.com's password: <password, not echoed to screen>
```

vilogger Daemon and Log Management Commands

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

Management Service Interface for vilogd

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

You can stop or restart the daemon at any time if you are logged in as vi-admin. Table 3-2 lists the commands that you can use to perform these activities.

Table 3-2. vilogd Daemon Commands

Command	Action
`sudo /sbin/service vmware-vilogd start`	Starts the `vilogd` daemon.
`sudo /sbin/service vmware-vilogd stop`	Stops the `vilogd` daemon.
`sudo /sbin/service vmware-vilogd restart`	Restarts the `vilogd` daemon.
`/sbin/service vmware-vilogd status`	Displays the status of the `vilogd` daemon.

vilogger enable

Enables log collection for the specified vMA target.

Usage

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

Description

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

By default, `vilogd` places the logs in `/var/log/vmware`. To specify a different log location, make changes to the `/etc/vmware/vMA/vMA.conf` file. When you start `vmware-vilogd` the next time, it places the logs in the new location if vi-admin has access to it. See "vilogger list" on page 31 for a listing of the logs collected on ESX, ESXi, and vCenter Server systems.

Options

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

Examples

`vilogger enable`

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

`vilogger enable --server myServer42`

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

```
vilogger enable --server myServer42 --logname messages
```

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

```
vilogger enable --collectionperiod 60
```

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

```
vilogger enable --numrotation 8
```

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

```
vilogger enable --maxfilesize 10
```

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

vilogger disable

Disables log collection for a vMA target.

Usage

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

Description

Disables all log collection for a specified vMA target or for all vMA targets. The command also allows you to disable logging for specific log files.

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

Options

Option	Description
`server`	Name or IP address of the vMA target to disable log collection for. Default is all vMA targets.
`logname`	Log that you want to disable. Disables all logs by default. You can display the list using `vilogger list`.
`force`	Forces disabling of logging. When vMA cannot reach the target server, `vilogger disable` fails. Use `vilogger disable --force` to disable logging for the target server.

Examples

```
vilogger disable --server myserver42 --logname messages
```

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

```
vilogger disable --server myserver42
```

Disables all log collection for the myserver42 ESX host.

```
vilogger disable
```

Disables all log collection.

vilogger updatepolicy

Customizes log collection parameters.

Usage

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

Description

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

Options

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

Examples

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

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

`vilogger updatepolicy --server myserver42 --maxfilesize 7`

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

vilogger list

Lists available logs collected by the vilogd daemon.

Usage

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

Description

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

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

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

The following logs are available for VMware ESX systems:

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

The following logs are included for VMware ESXi systems.

- `/var/log/messages` (VMkernel logs and warnings, host daemon messages, and other user-level daemon messages). The `messages` log contains the same information that you can find in the `vmkernel`, `vmkwarnings`, and `hostd` logs on ESX systems. The `vmksummary` log does not exist on ESXi system.
- `hostd.log` (host agent log)
- `vpxa.log` (vCenter Server agent log; included if the system is managed by a vCenter Server system)

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

vMA does not collect log files for virtual machines.

Example

```
vilogger list
```

Lists the logging status for all vMA target servers.

Using the VmaTargetLib Library

The VmaTargetLib library allows you to programmatically connect to vMA targets by using Perl or Java. This section explains how to use VmaTargetLib to connect to a single target or multiple targets.

Agents can link with `VmaTargetLib` and use vi-fastpass functionality. The library implements the methods in "VmaTargetLib Reference" on page 32. See the `VIFPLIB` java library for a more detailed reference to the Java interface. You can find samples in `/opt/vmware/vma/samples`.

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

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

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 all target vCenter Server or ESX/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 to 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 ESX/ESXi system 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 a vMA target session that the agent can use to run commands on the host.

Programmatic Logout

Usage

Perl	`VmaTarget.logout()`
Java	`VmaTarget.logout()`

Description

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

Options

None

Appendix: Updating vMA with vma-update

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

This appendix includes the following topics:

Introduction to vma-update

You can use `vma-update` to perform the following tasks:

- Download patches for vMA.
- Upgrade vMA 4.0 to vMA 4.1.

IMPORTANT You cannot use `vma-update` to upgrade VIMA 1.0 to vMA 4.1. You also cannot use `vma-update` to upgrade VMware Tools. You need to upgrade VMware Tools manually.

VMware hosts a depot of vMA updates online. The URL of the update depot is specified in the `/etc/vmware/esxupdate/vmaupdate.conf` file.

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

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

Use vma-update

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

If you want to specify a proxy server, edit the `/etc/vmware/esxupdate/vmaupdate.conf` file before you use `vma-update`. For example:

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

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

To get information on a patch bulletin

1 Log in to vMA as vi-admin.

2 Run one of the following commands:

```
sudo vma-update info
```

This command gets information about the bulletin in the online depot.

```
sudo vma-update info --bundle=<offline-bundlezip-url>
```

Here, `<offline-bundlezip-url>` specifies the URL to the ZIP file in the local depot.

This command gets information about the bulletin in the local depot.

3 (Optional) If prompted, provide the vi-admin password.

vMA lists applicable bulletins with updates.

To scan for updates

1 Log in to vMA as vi-admin.

2 Run the following command:

```
sudo vma-update scan
```

This command scans the bulletin in the online depot.

```
sudo vma-update scan --bundle=<offline-bundlezip-url>
```

Here, `<offline-bundlezip-url>` specifies the URL to the ZIP file in the local depot.

3 (Optional) If prompted, provide the vi-admin password

vMA lists applicable bulletins with updates.

To update vMA

1 Log in to vMA as vi-admin.

2 Run `vma-update` to install all updates or update to a particular version, specified by bulletin ID.

Each bulletin consists of one or more updates. Later bulletins include the updates of previous bulletins.

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

Examples

The following examples assume a depot is available.

`sudo vma-update scan`

Lists applicable bulletins with updates.

`sudo vma-update -b 'vma 4.01' update`

Updates vMA to patch level 4.01.

`sudo vma-update update`

Applies all currently available updates.

Use vma-update with Update Depots

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

To use vma-update with local depots

1 Download the depot to a local server, as described in the *ESX 4 Patch Management Guide*.

2 Edit the `depot = http://...` line in the `/etc/vmware/esxupdate/vmaupdate.conf` file.

3 Run the update, as described in "Use vma-update" on page 35.

vma-update Troubleshooting

Table A-1 lists a few of the commonly encountered issues with vma-update utility.

Table A-1. Troubleshooting vMA

Issue	Resolution
If you run `vma-update`, and the URL specified in the `/etc/vmware/esxupdate/vmaupdate.conf` file is wrong, the following message appears: `Encountered error MetadataDownloadError:...Failed to download metadata .`	Check the URL and supply one that points to vMA updates.
`vma-update` results in an error.	See the exit codes and error messages for esxupdate utility in the *ESX 4 Patch Management Guide*.

Index

V