SOPHOS
Security made simple.

Sophos Anti-Virus for VMware vShield
startup guide

Product version: 1.1
Document date: March 2014

Contents

1 About this guide

This guide is intended for administrators who want to protect a network of virtual machines (VMs) against viruses and other threats.

The guide describes how to install Sophos Anti-Virus for VMware vShield on VMware ESXi hosts to provide anti-virus scanning for guest VMs, with just a vShield Endpoint Thin Agent on each VM.

Below are links to other documents you might find useful.

Need help setting up the VMware and vShield environment?

See the Sophos guide *VMware and vShield: an overview of setup*.

See also these articles from VMware:

■ *Installing vCloud Networking and Security 5.5.x best practices*

■ *Guest operating systems that are supported for vShield Endpoint Thin Agent*

Need information on alternative ways to protect VMs?

Go to *www.sophos.com/en-us/support/knowledgebase/110507.aspx*.

Need to upgrade Sophos Anti-Virus for VMware vShield?

See the *Sophos Anti-Virus for VMware vShield upgrade guide*.

2 About Sophos Anti-Virus for VMware vShield

Sophos Anti-Virus for VMware vShield is a security virtual machine (VM). You set it up as follows:

- You install a Sophos security VM on each VMware ESXi host so that it can protect the guest VMs that are running on the host.

- You use Sophos Enterprise Console on another computer to manage the security VMs and keep them up to date with the latest anti-virus software.
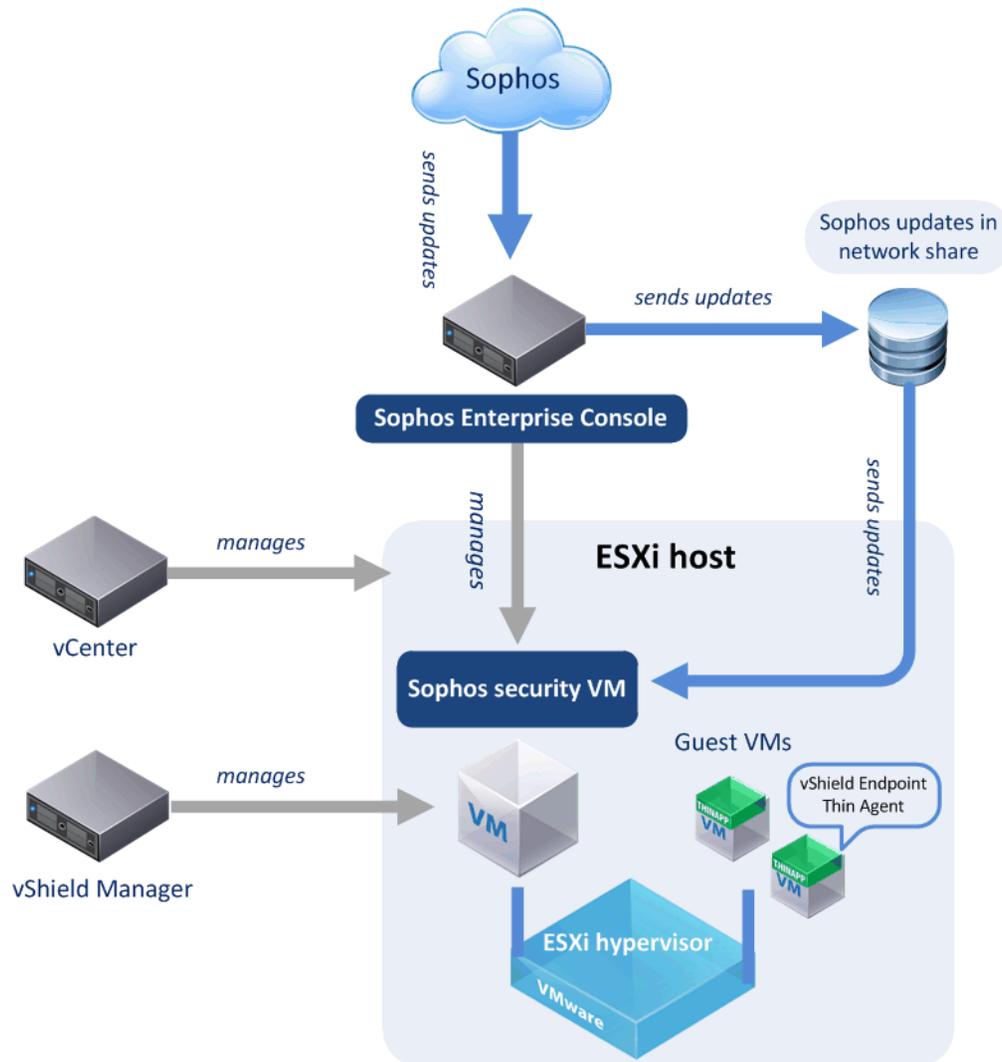
Which guest VMs can be protected?

The Sophos security VM can protect guest VMs that run Windows operating systems. For full details, see *Guest VMs* (section 4.1.3).

How does scanning work?

When a guest VM tries to access a file:

■ A vShield Endpoint Thin Agent running on the VM notifies the Sophos security VM.

■ The security VM scans the file, if the file has changed or if a detection update has occurred since the file was last scanned.

■ If the security VM detects a threat, access to the file is blocked, and the security VM sends an alert to Enterprise Console.

The security VM can also perform a full scan of all the guest VMs. In this case:

■ The security VM schedules scans so as to ensure that the ESXi host is not placed under a high load.

■ If the security VM detects a threat, it sends an alert to Enterprise Console.

How is the security VM managed?

Enterprise Console displays the status of the security VM, including how up to date it is and whether it has detected any threats.

Enterprise Console also enables you to configure scanning by means of a policy.

How do you deal with threats?

Depending on the threat that has been detected and the damage that it has caused, you can:

■ Delete the affected guest VM and reclone it from the template image.

■ Revert the affected guest VM to the previous known clean snapshot.

■ Use the free Sophos Virus Removal Tool.

■ Use Sophos Endpoint Security and Control for Windows.

How is the security VM updated?

Enterprise Console keeps the security VM updated.

Enterprise Console downloads the latest software updates, threat data, and threat detection engine from Sophos and puts them in a network share. The security VM automatically fetches updates from there.

When Sophos releases a major new version of the security VM, you can upgrade as described in the *Sophos Anti-Virus for VMware vShield upgrade guide*.

3 Key steps in installation

Installation involves these key steps, which are described in the sections that follow:

■ Check the system requirements.

- Check for incompatible anti-virus products.

- Install the Sophos requirements.

- Install the Sophos security VM.

- Install the vShield Endpoint Thin Agent (if not already installed).

- Check that the security VM is working.

4 Check the system requirements

This section tells you the requirements and how to check that you comply with them.

It also tells you about any information (such as computer details) that you should gather now so that you will have it available when you install the security VMs.

It covers:

- VMware requirements.

- Guest VM requirements.

- Sophos requirements (Sophos software you need before you install the Sophos security VMs).

4.1 VMware requirements

This section shows you the VMware software you need.

The requirements shown are the minimum. Note that Sophos Anti-Virus supports version 5.5 of the VMware and vShield products.

For help with setting up VMware software, see the Sophos guide *VMware and vShield: an overview of setup*. You can also read these VMware knowledgebase articles:

- *Installing vCloud Networking and Security 5.5.x best practices*

- *Guest operating systems that are supported for vShield Endpoint Thin Agent*

4.1.1 ESXi host

You should install the following on each host that will run a Sophos security VM:

- VMware ESXi host 5.1 or later.

Hardware requirements

The ESXi host must be able to allocate the following resources for the Sophos security VM:

- 2 CPUs.

- 16 Gb disk space.

■ 2 Gb RAM.

Notes

By default, 2 CPUs are allocated. If you have many guest VMs to protect, you can configure more CPUs after you install the security VM. This guide tells you how.

The Sophos security VM reserves memory. High-availability and load-balancing systems make automatic choices based on resource reservations for the VMs in your VMware environment, so these choices could be different after you install the security VM. You should not remove the security VM memory reservation.

4.1.2 vCenter and vSphere

You require the following vCenter and vSphere software.

Software	Version	Notes
vCenter	Version 5.1 or later.	You will also need: The network address. An administrator account. For permissions needed, see *Appendix: vCenter administrator account* (section 17). A read-only account. This may be a local or domain user. Local user names are case-sensitive.
vSphere Client	Version 5.1 or later.	

4.1.3 Guest VMs

The Sophos security VM can protect guest VMs that meet these requirements.

Virtual hardware

The VMware virtual hardware must be version 7 or later.

Tip: If you have virtual hardware that came as default with ESXi version 4.x or later, you already meet this requirement.

Note: For information on upgrading virtual hardware versions, see *VMware Knowledge Base article 1010675*.

Operating system

Guest VMs should run one of the following operating systems:

■ Windows 8 (32- and 64-bit)

■ Windows Server 2012

■ Windows 7 (32- and 64-bit)

■ Windows Server 2008 R2 (64-bit)

■ Windows Server 2008 (32- and 64-bit)

■ Windows Vista (32-bit)

■ Windows Server 2003 R2 (32- and 64-bit)

■ Windows Server 2003 (32- and 64-bit)

■ Windows XP (32-bit)

4.1.4 vShield

You require the following vShield software.

Software	Version	Notes
vShield Manager	Version 5.1 or later. To check that it's installed: 1. Restart vSphere Client. 2. In vSphere Client, click the ESXi host on which you want to install the security VM. 3. Check that the **vShield** tab is visible.	You will also need: The network address. A vShield Administrator or Enterprise Administrator account.
vShield Endpoint	Version 5.1 or later. Must be installed on each ESXi host that will run the Sophos security VM. To check that it's installed: 1. In vSphere Client, click the ESXi host on which you want to install the security VM. 2. On the **vShield** tab, **General** page, if the **vShield Endpoint** row is listed with version 5.1.0 or later in the **Installed** column, then the appropriate version of vShield Endpoint is installed. Otherwise, click **Install**.	

Software	Version	Notes
vShield Endpoint Thin Agent	Must be installed on each guest VM that needs protection. **Note:** You can install the Thin Agent after you install the Sophos security VM. This guide tells you how. To check whether it's installed: 1. In vSphere Client, click the ESXi host on which you want to install the security VM. 2. Ensure that the guest VMs that you want to check are turned on. 3. On the **vShield** tab, **Endpoint** page, look for the guest VMs in the computer list, displayed as "vm". 4. Check that the **Description** shows "Thin Agent enabled".	Supports Windows operating systems only. This is part of VMware Tools and can be automatically upgraded.

4.1.5 vMotion

Sophos security VMs are automatically excluded from vMotion. This ensures that a security VM always remains on its ESXi host to protect guest VMs.

You do not need to make any changes to your settings.

4.2 Sophos requirements

You need the following Sophos software before you can install and use the Sophos security VM. If you don't have this software, follow the instructions in *Install Sophos requirements* (section 6).

Note: Ensure that Sophos Anti-Virus for Windows (which is included in Sophos Endpoint Security and Control) is **not** installed on guest VMs that you intend to protect with the Sophos security VM. This avoids the conflicts that can arise between any two anti-virus products on the same computer.

Software	Version	Notes
Sophos Enterprise Console	Version 5.1 or later.	
Sophos Anti-Virus for VMware vShield network share	No minimum version.	You must set up a network share where Enterprise Console makes the latest updates

Software	Version	Notes
		available for your security VM. This guide tells you how to set up the share.

5 Check for incompatible anti-virus products

You cannot use Sophos Anti-Virus for VMware vShield to protect guest VMs that run other anti-virus products. This is because files might be scanned multiple times (due to the design of VMware vShield).

This limitation applies to VMs that run other anti-virus products from Sophos or products from other vendors. It also applies to VMs with Sophos gateway or server products that include or require anti-virus components. So you cannot protect guest VMs that run:

- Sophos Endpoint Security and Control for Windows (includes Sophos-Virus for Windows).
- PureMessage for Microsoft Exchange.
- PureMessage for Lotus Domino.
- Sophos for Sharepoint.
- Sophos Anti-Virus for NetApp.
- Any third-party software that integrates SAV Interface.

6 Install Sophos requirements

Before you install Sophos security VMs, you should:

- Install Sophos Enterprise Console (if you do not already have it). You use this to download protection software and to manage the VMs you protect.
- Create a Sophos Anti-Virus for VMware vShield network share. The share is used to keep security VMs up to date.

The following sections describe how to do this.

Already using Enterprise Console?

⚠ **Warning:** If you already use Enterprise Console to manage other Sophos products but now want to add Sophos Anti-Virus for vShield, your customer credentials might not let you set up the Sophos network share. If this happens, contact Technical Support.

6.1 Install Enterprise Console

If you already have Enterprise Console installed, go to *Create a Sophos Anti-Virus share* (section 6.2).

You should install Enterprise Console on a Windows computer that will be on the same network as the security VMs.

Follow the instructions in the *Enterprise Console quick startup guide*. When you are prompted to select the platforms you want to protect, include **VMware vShield**. This creates the Sophos Anti-Virus network share.

After installation, see *Check access to the Sophos Anti-Virus update share* (section 6.3).

6.2 Create a Sophos Anti-Virus update share

If you have just made a new installation of Enterprise Console and included protection for VMware vShield, you can skip this section.

1. In Enterprise Console, on the **View** menu, click **Update Managers**.

2. Set up a "subscription" to Sophos Anti-Virus for VMware vShield :

    a) In the **Software Subscriptions** pane, click **Add** at the top of the pane.

    b) In the **Software Subscription** dialog box, type a name in the **Subscription name** text box.

    c) In the platform list, select **VMware vShield** and in the version box select **Recommended**.
        Note: If you cannot see **VMware vShield** in the list, your customer credentials need updating. Contact Technical Support.

    d) Click **OK**.

3. Configure the update manager to use this subscription:

    a) In the **Update Managers** pane, select the update manager that is installed on this server. Right-click it and click **View/Edit configuration**.

    b) In the **Configure update manager** dialog box, on the **Subscriptions** tab, ensure that the new subscription is in the **Subscribed to** list.

    c) Click **OK**.

Now continue to the next section.

6.3 Check access to the Sophos Anti-Virus update share

You need to locate the Sophos Anti-Virus update share and ensure that it can be accessed using either valid credentials or a guest account.

Note: Unless you specified otherwise, the Sophos Anti-Virus share is accessed by the user account set up during installation of Enterprise Console. It is described there as the "Update Manager" account and most customers give it the username SophosUpdateMgr.

1. In Enterprise Console, on the **View** menu, click **Bootstrap Locations**.

   A list of locations is displayed.

2. Find the location for Sophos Anti-Virus for VMware vShield, the "savvshield" share, and make a note of it. You will need this when you install the Sophos security VMs.

   You will need the Fully Qualified Domain Name for this location.

3. If the share is on Windows Server 2008 or 2012, you might need to change Windows Firewall settings on the server temporarily to enable the Sophos security VM installer to access it.

   The following **Inbound** rules must be set to **On** (which is the default):

   - File and Printer Sharing (NB-Datagram-In)
   - File and Printer Sharing (NB-Name-In)
   - File and Printer Sharing (NB-Session-In)

   You can set these rules to **Off** again after you have installed your security VMs.

Notes:

If you have a customised installation of Enterprise Console or you created an additional network share for updating the security VM, note that:

- If credentials are required, they will need to be stored on security VMs after they are installed, so we recommend that you use read-only credentials.

- If the network share is on a different computer to Enterprise Console (or the Update Manager component of Enterprise Console), ensure that it can also be accessed using an account that has write-access.

7 Install Sophos security VMs

You install a Sophos security VM on each ESXi host where you want to protect guest VMs.

Installation involves these steps, which are described in the sections that follow:

- Check that you have the passwords you need.

- Check that systems are synchronized.

- Download the installer.

- Install security VMs.

- Set up Enterprise Console to manage security VMs.

7.1 Check that you have the passwords you need

When you run the security VM installer, you need to enter certain passwords. You should make sure that you have the passwords for the following accounts:

■ The vCenter Administrator account.

■ The vCenter read-only user account, used to query information from vCenter during security VM operation.

■ The vShield Administrator account.

■ The account used to access the Sophos Anti-Virus network share (or "Sophos Update folder").

Note: The vCenter user account is stored on the security VMs. Therefore we recommend that the account is read-only.

7.2 Check that systems are synchronized

You must ensure that the time is synchronized on the Enterprise Console server and on each ESXi host where you install the security VM.

You can use NTP (Network Time Protocol) synchronization for each vCenter server or each host.

⚠ **Warning:** If the time is not synchronized, you can install security VMs but you cannot manage them from Enterprise Console.

7.3 Download the installer

The following steps assume that you have a MySophos account and that you have associated your license credentials with it. If you need help, go to *www.sophos.com/en-us/support/knowledgebase/111195.aspx*.

Notes:

■ You can download the installer at any computer and then copy it to the computer where you will use it.

■ You cannot use the installer on a Windows XP or Windows Server 2003 computer.

To download the installer:

1. Go to *www.sophos.com/en-us/support/downloads/*.

2. Type your MySophos username and password.

   You see a webpage that shows your license or licenses.

3. Find and download Sophos Anti-Virus for VMware vShield.

   The download is a package that contains the installer and other files.

4. Ensure that the installer download is on a Windows computer that has access to vCenter and vShield Manager over the network. The installer does not currently support the use of a proxy, so installation or uninstallation of the security VM must be done on the local network.

   Note: This computer is not used for management or protection of your security VM or guest VMs after installation.

7.4 Install the security VMs

To install security VMs, do as follows.

Remember: You cannot use the installer on a Windows XP or Windows Server 2003 computer.

Tip: You might want to install a single security VM as a test and then install more later. We make this easy with an option to re-run the installer with your previous settings, as explained at the end of this section.

1. Double-click the installer you downloaded.

   A wizard runs to guide you through the installation.

2. Accept the license agreement.
3. Click **Install** to extract the installation files to a folder on your computer.
4. Select **Install new security VMs**.
5. Check that you have installed all the **Prerequisites for installation**.
6. Enter your vCenter details.

   When you enter the administrator usernames, they should be in exactly the same form that you would use to log in to vCenter using vSphere Client, that is, with or without the domain prefix as required and using the same capitalization.

   a) Enter your vCenter address.

   b) Enter your vCenter administrator username and password.

   c) Enter the vCenter read-only username and password. This is used to query information from vCenter during security VM operation. You can use a domain or a local (to vCenter) username.

      The installer does not check that these credentials are read-only.

7. Enter your vShield Manager address and administrator credentials.

   The administrator name should be in exactly the same form that you would use to log in to vShield Manager web interface, that is, with or without the domain prefix as required and using the same capitalization.

8. The wizard displays your hosts. Select the host or hosts on which you want to install the security VM.

    Note: The installer will give security VMs names based on the host name or IP address, as you will see later.

9. Enter your Sophos Update folder details. This is the Sophos Anti-Virus network share that you created earlier.

    a) Enter the location. Use a UNC path **including the fully qualified domain name**, or a web address (if the share is on a web server).

        For example:

        \\<Your server name.domain name>\sophosupdate\CIDs\Sxxx\savvshield

        Tip: To check the location, go to Enterprise Console. On the **View** menu, click **Bootstrap Locations** and look for the "savvshield" share.

    b) Enter the username and password. You (or another administrator) set up this user account during Enterprise Console installation. It is described there as the "Update Manager" account and most customers give it the username SophosUpdateMgr.

        Note that:

        ■ If you specify a domain user, you must include the domain name.

        ■ The credentials are stored on the security VM.

10. Create a **Support** password.

    You need this password in order to view your protected guest VMs. You also need it if you want Sophos technical support to troubleshoot your installation remotely. They will use it to collect logs, which you will be able to review before they are sent to Sophos.

    You can use special characters and spaces in your password.

11. Select the time zone that the security VM will use to schedule scans.

12. Configure the IP settings for security VMs.

    By default, IP addresses are assigned dynamically by DHCP. If your network policy requires you to use static addresses, select that option and enter the details.

13. Select the type of datastore on which you want to install the security VM.

    If you select **Select from list of visible datastores for each host**, a list is displayed.

    The security VM protects all guest VMs on an ESXi host that have vShield Endpoint Thin Agent installed, even if their templates are stored in different datastores.

14. Select a VM network. This enables the security VM to communicate with Enterprise Console. The default is **VM network**.

15. At the **Summary of installation** page, you can see full installation details, including your security VM names. Click **Install**.

16. At the **Installation complete** page, you can see whether installation of any security VMs failed. If it did, check the log for details.

    Tip: If you want to install more security VMs, leave the installer open and click **Start Over** when you are ready to start again. The installer will use your previous settings as defaults.

The security VMs are installed. There can be a delay while security VMs are configured because a full update of the Sophos Anti-Virus scanner is taking place.

Follow the instructions in the next two sections to:

■ Check that you can see the security VMs in vSphere Client and Enterprise Console.

■ Set up Enterprise Console to manage the security VMs.

7.5 Check that security VMs are installed

This section tells you how to check that security VMs are installed and have the resources they need.

Check that you can see security VMs

When the security VMs have been installed, you should see the following:

In vSphere Client

The security VMs should be shown within twenty minutes, in the **Endpoints** list on the **vShield** tab for each host.

Note: If you do not yet have the vShield Endpoint Thin Agent installed on any guest VMs, this does not happen.

In Enterprise Console

The security VMs are registered and placed in the **Unassigned** group of computers.

The security VM names are based on the host name or, if it does not have a name, IP address. This helps you match security VMs with hosts (if you have multiple security VMs). Here are some examples.

Host name or address	Sophos security VM name
MyESXhost	MyESXhost-SSVM
192.0.2.0	192.0.2.0-SSVM

If you change the name of a security VM after installation, it is still shown in Enterprise Console with the name assigned during installation.

Check whether you need to configure resources

Usually you do not need to configure resources for the security VM. Note that:

■ **The installer reserves memory for the Sophos security VMs.** High-availability and load-balancing systems make automatic choices based on resource reservations for the VMs in your VMware environment, so these choices could be different after you install the security VMs. You should not remove the security VM memory reservation.

■ **If you have a large number of guest VMs** (70 or more) on a single host, ensure that the security VM has enough processing power for scanning. See *Appendix: Set the CPU configuration* (section 18).

■ **Sophos security VMs are automatically excluded from vMotion.** This ensures that a security VM always remains on its ESXi host to protect guest VMs.

You are ready to set up Enterprise Console to manage the security VMs.

7.6 Set up Enterprise Console to manage the security VMs

1. In Sophos Enterprise Console, create an updating policy and an anti-virus and HIPS policy. Right-click each policy and select **Reset Policy to Factory Defaults**.

2. Double-click the new updating policy to open it.

3. In the **Updating policy** dialog box:

   a) Click the **Subscription** tab and select the subscription for VMware vShield

   b) Click the **Primary Server** tab and ensure that the location of the update folder includes the **fully qualified domain name**. Save the policy.

4. Create a new computer group to contain the security VMs.

5. Apply the new policies to the new group.

6. Drag the security VMs from the **Unassigned** group to the new group.

Now install the vShield Endpoint Thin Agent (if not already installed), as described in the next section.

To check that security VMs are working, see *Check that security VMs are working* (section 9).

For general advice on post-installation and maintenance tasks, see *Maintain the security VMs* (section 10)

8 Install the vShield Endpoint Thin Agent

If you do not have the vShield Endpoint Thin Agent installed on the guest VMs, you should install it now.

This section tells you how to:

■ Check whether the agent is already installed (if you are not sure).

■ Prepare to install the agent.

■ Install the agent.

8.1 Check whether the agent is already installed

To check whether the vShield Endpoint Thin Agent is already installed:

1. In vSphere Client, click the ESXi host on which you want to install a security VM.
2. Ensure that the guest VMs that you want to check are turned on.
3. On the **vShield** tab, **Endpoint** page, look for the guest VMs in the computer list, displayed as "vm".
4. Check whether the **Description** shows "Thin Agent enabled".

If the agent is not installed, continue to *Prepare to install the agent* (section 8.2).

8.2 Prepare to install the agent

Before you install the agent, you should prepare as follows. The steps depend on whether you already have anti-virus software on guest VMs.

If you already have anti-virus software

If you already have anti-virus software (whether Sophos software or another vendor's software) installed on your guest VMs, you should:

1. Ensure the guest VMs are turned on.
2. Uninstall the anti-virus software.
3. Do not restart the guest VMs when you are prompted.

You are now ready to install the agent.

If you do not have anti-virus software

If you do not have anti-virus software protecting your guest VMs, make sure that none of them are connected to the live network.

You are now ready to install the agent.

8.3 Install the agent

You install the vShield Endpoint Thin Agent as one of the components of VM Tools.

The Thin Agent is not included in a standard VM Tools installation, so you must do one of the following:

■ Install VM Tools with the **Custom** option and include the Thin Agent (also called "vShield Drivers") in your selected components.

■ Upgrade VM Tools in order to add the Thin Agent component.

The following sections tell you how to do this manually (interactively) or automatically (non-interactively).

Note: This guide assumes that you use vSphere Client to install the agent, but you can use other VMware management software, as described in *Installing and Configuring VMware Tools*.

8.3.1 Install the agent manually

To install the agent interactively on a guest VM:

1. Power on the VM and check that the guest operating system is running.
2. Log in to the VM as an administrator.
3. In vSphere Client, select the menu command to mount the VMware Tools virtual disk on the guest operating system. The command depends on the version of vSphere Client you use.

Version	Command
vSphere Client	Select **Inventory** > **Virtual Machine** > **Guest** > **Install/Upgrade VMware Tools.** **Note:** To locate a virtual machine: ■ Select a datacenter or cluster. ■ Click the **Virtual Machines** tab.
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions** > **Guest OS** > **Install/Upgrade VMware Tools.** **Note:** To locate a virtual machine: ■ Select a datacenter, folder, cluster, resource pool, host, or vApp. ■ Click the **Related Objects** tab and click **Virtual Machines**.

4. Now start the installation procedure. The command depends on whether you are upgrading/reinstalling VM Tools or installing it for the first time.

Installation type	Command
Upgrade	In the **Install/Upgrade VMware Tools** dialog box, select **Interactive Tools Upgrade** and click **OK**.
First time installation	In the **Install VMware Tools** information screen, click **OK**.

5. When prompted, confirm that you want to run the setup program.

    If autorun is enabled for the CD-ROM drive in the guest operating system, the VMware Tools installation wizard is started.

    Note: If autorun is not enabled, you can launch the wizard manually. Click **Start** > **Run** and enter D:\setup.exe, where D: is your first virtual CD-ROM drive.

6. The installation wizard guides you through the installation. You should:

    ■ Select **Modify** if you are upgrading. Select a **Custom** installation if you are installing for the first time.
    ■ On the **Custom setup** page, select **VMCI driver** > **vShield Drivers** .

7. If the Windows **New Hardware** wizard is run, complete the wizard. You can accept the defaults at each page.

    Windows may run this wizard because you have installed drivers that simulate a change to the hardware installed on the machine.

8. When prompted, restart the virtual machine.

8.3.2 Install the agent automatically

You can automate installation of the Thin Agent.

See the sample instructions in the *VMware vSphere Documentation Center*.

After installation, restart the guest VM.

9 Check that security VMs are working

This section tells you how to check that:

■ A Sophos security VM is working.
■ The guest VMs are protected with on-access scanning.

Note: Guest VMs are shown as UNPROTECTED on the vShield tab in the vSphere Client console. This refers only to vShield App protection, not to Sophos protection provided by vShield Endpoint. You should ignore this and follow the instructions in this section to check that VMs are protected.

9.1 Check the status in vSphere Client

You check the status of a security VM in vSphere Client as follows.

Important:

There can be a delay of up to 20 minutes between activating a security VM and seeing its status in vSphere Client change.

1. In vSphere Client, on the **vShield** tab, **Endpoint** page, look for the security VM in the computer list.

   The **Description** should show "vShield Endpoint Solution, Sophos Anti-Virus for VMware vShield, enabled" and there should be no critical errors under **Endpoint Status**.

2. If the **Description** does not show "enabled" and there is a critical error, perform the relevant action according to this table:

Description	Action
There is a protocol version mismatch with the vShield Endpoint module.	Ensure that the vShield Endpoint module and the security VM have protocols that are compatible with each other.
vShield Endpoint could not establish a connection to the security VM.	Ensure that the security VM is powered on and that the network is configured properly.
The security VM is not reporting its status even though guests are connected.	Internal error. Contact your VMware support representative.

3. Look for the guest VMs in the computer list, displayed as "vm."

   The **Description** should show "Thin agent enabled".

4. If the Description does not show "enabled", turn on a guest VM that is turned off, or restart a guest VM.

   This should trigger the status to update.

9.2 Check that on-access scanning is working

On-access scanning is your main method of protection against threats. Whenever you copy, move, or open a file, or start a program, the security VM scans the file or program and grants access to it only if it does not pose a threat to your computer.

Important: Ensure that Sophos Anti-Virus for Windows is *not* installed on any guest VMs that are protected with a security VM.

To check that a security VM is scanning files on access:

1. Go to *eicar.org/86-0-Intended-use.html*. Copy the EICAR test string to a new file. Give the file a name with a .com extension and save it to one of the guest VMs.

2. Try to access the file from the guest VM.

3. In Sophos Enterprise Console, in the computer list in the lower right part of the window, click the **Status** tab.

4. In the list of computers, look for the security VM. In the **Alerts and errors** column, Enterprise Console should display `Virus/spyware detected`. It should also display that EICAR is not cleanable.

5. Delete the EICAR file that you created.

   Before you delete the EICAR file, you must stop vShield Endpoint Thin Agent on the affected guest VM:

   As an Administrator, in a Command Prompt window, type:

   net stop vsepflt

   To restart the agent after deleting EICAR, type:

   net start vsepflt

6. In Enterprise Console, clear the alert.

   a) In the computer list in the lower right part of the window, right-click the security VM and select **Resolve Alerts and Errors**.

   b) In the **Resolve Alerts and Errors** dialog box, on the **Alerts** tab, select the alert and click **Acknowledge**.

9.3 Troubleshoot on-access scanning

If on-access scanning is not working:

1. Ensure that the security VM is in a group whose anti-virus policy specifies that on-access scanning should be turned on:

    a) In Enterprise Console, in the **Groups** pane, right-click the group that contains the security VM and select **View/Edit Group Policy Details**. Check which anti-virus and HIPS policy is used.

    b) In the **Policies** pane, double-click **Anti-virus and HIPS**.

    c) Double-click the policy that is used by the group that contains the security VM.

    d) In the **On-access scanning** panel, ensure that the **Enable on-access scanning** check box is selected. Click **OK**.

    e) In the computer list, right-click the security VM and select **Comply with**. Then select **Group anti-virus and HIPS policy**.

2. Ensure that each guest VM has vShield Endpoint Thin Agent installed:

    a) On each guest VM, run the VMware Tools setup wizard.

    b) On the **Custom Setup** page, ensure that **VMware Device Drivers** > **VMCI Driver** > **vShield Drivers** is selected for installation.

3. If on-access scanning is still not working, contact *Sophos technical support* (section 19).

10 Maintain the security VMs

This section gives advice on post-installation and maintenance tasks.

- **You must power on a security VM manually whenever the ESXi host is taken out of maintenance or standby mode.** Do this before you power on the guest VMs, so that the guest VMs are protected immediately.

- **If you want to change settings after installation**, you must uninstall and re-install the security VM.

- **If you want to uninstall security VMs**, run the installer again and select removal, as described in the uninstallation section of this guide. You cannot uninstall a security VM by deleting it in vCenter.

11 View the protected guest VMs

You can view all the guest VMs that are protected by your security VMs.

You view protected guest VMs by using a feature included in the Sophos Anti-Virus installer.

1. In the same directory to which you extracted the installer, double-click `ssvmtool.exe`.

   Tip: If you used default settings, the installer will be in the C:\SSVM_1_x_x directory, where 1.x.x is the version number.

   A wizard runs.

2. Select **View protected guest VMs.**
3. Enter your vCenter address and credentials.
4. Enter your vShield Manager address and credentials.
5. Select the host or hosts where you want to view guest VMs.
6. Enter your **Support password**. This is the password you created when you installed your security VMs.
7. On the **Ready to find guest VMs** page, click **Find**.

   The wizard begins the search for guest VMs.

8. When the search is finished, click **View**.
9. A list of **Protected guest VMs found** is displayed.

   The list is also available as a file on your hard disk. To find it, click **Show file location**.

12 Run a full scan of all the guest VMs

A security VM can perform a full scan of all the guest VMs. It does this in such a way that the ESXi host is not placed under a high load. You can either run a scan immediately or at set times.

Note: To be able to run a full scan of all the guest VMs, either immediately or at set times, the security VM must not be in the Sophos Enterprise Console **Unassigned** group but in a group to which you have applied policies.

To run a full scan of all the guest VMs *immediately*:

■ In Enterprise Console, in the computer list in the lower right part of the window, right-click the security VM and select **Full system scan**.

   Alternatively, on the **Actions** menu, select **Full system scan**.

To run a full scan of all the guest VMs *at set times*:

■ In Enterprise Console, create a *scheduled scan*, as explained in the Enterprise Console Help, in the section about configuring the anti-virus and HIPS policy.

To view details of the scan after it has been run:

■ In Enterprise Console, in the computer list in the lower right part of the window, double-click the security VM to display the **Computer details** dialog box.

13 What happens if a security VM detects a threat

If a security VM detects a threat on one of the guest VMs, it sends an alert to Enterprise Console. Specifically:

■ An alert is displayed on the dashboard.

■ A red warning icon is displayed in the computer list, on the **Status** tab, next to the security VM in the **Alerts and errors** column.

If the security VM detects a threat *when a user tries to access a file*, a message may also be displayed on the guest VM informing the user that the file cannot be accessed, although this depends on the application used to access the file.

14 Deal with a threat

To deal with a threat that a security VM has detected:

■ Find out more about the threat and how to deal with it.

■ Clean up a guest VM.

■ Clear the alert from Enterprise Console.

The following sections guide you through the process.

14.1 Find out about the threat

To find out more about the threat and how to deal with it:

1. In Enterprise Console, in the computer list in the lower right part of the window, double-click the security VM to display the **Computer details** dialog box.

    In the **History** section, **Items detected** are listed. The name of the threat is shown in the **Name** column and the affected guest VM and file are shown in the **Details** column.

2. Click the name of the threat.

    This connects you to the Sophos website, where you can read a description of the item and advice on what actions to take against it.

You are ready to deal with the threat using one of the methods described in the next section.

14.2 Clean up the guest VM

You can clean up the affected guest VM by different methods, depending on how the VM has been affected.

Some viruses leave no side-effects. Others may make changes or corrupt data.

If you can accept the loss of data, simply restore the VM. Use one of these methods:

■ Delete the affected guest VM and reclone it from the template image. Run a full scan of the guest VM to ensure that it is clean.

■ Revert the affected guest VM to the previous known clean snapshot. Run a full scan of the guest VM to ensure that it is clean.

Alternatively, use Sophos software to remove the threat. Use one of these methods:

■ Install the free Sophos Virus Removal Tool on the affected guest VM to remove the threat. You can download the tool from *www.sophos.com/en-us/products/free-tools/virus-removal-tool.aspx*.

■ Install Sophos Endpoint Security and Control for Windows on the affected guest VM and use it to remove the threat. You can download it from *www.sophos.com/en-us/support/downloads/standalone-installers/esc-for-windows-2000-up.aspx*.

Important: If you use Sophos software, you should read the guidance in the next section, *Clean up with Sophos software* (section 14.2.1).

14.2.1 Clean up with Sophos software

If you use Sophos Virus Removal Tool or Sophos Endpoint Security and Control to clean up a threat, you must do as follows:

1. Install Virus Removal Tool or Endpoint Security and Control.
2. Stop the vShield Endpoint Thin Agent. As an Administrator, in a Command Prompt window, type:
   net stop vsepflt

3. Clean up the threat.

   Note: If you are using Endpoint Security and Control, uninstall it before you restart the guest VM or restart the Thin Agent.

4. Restart the Thin Agent. Type:
   net start vsepflt

14.3 Clear the alert from Enterprise Console

When you are sure that the affected guest VM is clean, clear the alert from Enterprise Console:

1. In Enterprise Console, in the computer list in the lower right part of the window, right-click the security VM and select **Resolve Alerts and Errors**.

2. In the **Resolve Alerts and Errors** dialog box, on the **Alerts** tab, select the alert and click **Acknowledge**.

The alert is no longer displayed in Enterprise Console.

15 Upgrade security VMs

Sophos security VMs automatically get the latest software updates, threat data, and threat detection engine from your Sophos network share.

However, when Sophos releases a major new version of the security VM, you must upgrade manually. For instructions, see the *Sophos Anti-Virus for VMware vShield upgrade guide*.

16 Uninstall security VMs

To uninstall security VMs, you run the Sophos Anti-Virus installer again.

Notes:

You cannot uninstall a security VM by deleting it in vCenter.

You will need your administrator credentials for vCenter and vShield Manager. Remember to enter them exactly as you would when you log in to vCenter or vShield.

1. In the same directory to which you extracted the installer, double-click ssvmtool.exe.

   Tip: If you used default settings, the installer will be in the C:\SSVM_1_x_x directory, where 1.x.x is the version number.

2. A wizard guides you through uninstallation. You should:

   ■ Accept the license agreement and extract the installer files.
   ■ Select **Remove existing security VMs**.
   ■ Enter your vCenter address and credentials.
   ■ Enter your vShield Manager address and credentials.
   ■ Select the hosts from which you want to remove Sophos security VMs.
   ■ At the summary page, click **Uninstall**.

The installer uninstalls the security VMs.

17 Appendix: vCenter administrator account

Your vCenter administrator account must have the following permissions:

- Datastore > Allocate space
- Network > Assign network
- vApp > Import
- vApp > vApp instance configuration
- Virtual machine > Configuration > Add new disk
- Virtual machine > Guest Operation > Guest Operation Modifications
- Virtual machine > Guest Operation > Guest Operation Program Execution
- Virtual machine > Guest Operation > Guest Operation Queries
- Virtual machine > Interaction > Power Off
- Virtual machine > Interaction > Power On
- Virtual machine > Inventory > Remove

18 Appendix: Set the CPU configuration

If you have a large number of guest VMs on a host, you should ensure that the security VM has enough processing power to scan the files they use when they all start up.

To do this, you edit the CPU configuration for the security VM.

Note:

You can edit the CPU configuration at any time. However, if you do it after you have added the security VM to a computer group in Enterprise Console, you should wait until the security VM complies with the group policy.

1. Power off the security VM.
2. In vSphere Client, select the security VM.

3. Select **Edit Settings** > **Hardware** > **CPUs.** Then specify the number of CPUs.

The recommended number of CPUs depends on the number of guest VMs on the host, as shown below.

CPUs	Guest VMs
2	Up to 70
4	Up to 170
6	Up to 190

19 Technical support

You can find technical support for Sophos products in any of these ways:

■ Visit the SophosTalk community at *community.sophos.com/* and search for other users who are experiencing the same problem.

■ Visit the Sophos support knowledgebase at *www.sophos.com/en-us/support.aspx*.

■ Download the product documentation at *www.sophos.com/en-us/support/documentation/*.

■ Send an email to *support@sophos.com*, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

20 Legal notices

ACE™, TAO™, CIAO™, and CoSMIC™

ACE[1], TAO[2], CIAO[3], and CoSMIC[4] (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt[5] and his research group[6] at Washington University[7], University of California[8], Irvine, and Vanderbilt University[9], Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source, free software, you are free to use, modify, copy, and distribute–perpetually and irrevocably–the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us[10] know so we can promote your project in the DOC software success stories[11].

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies[12] around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE[13], TAO[14], CIAO[15], and CoSMIC[16] web sites are maintained by the DOC Group[17] at the Institute for Software Integrated Systems (ISIS)[18] and the Center for Distributed Object Computing of Washington University, St. Louis[19] for the development of open-source software as part of the open-source software community[20]. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledgethat any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, WashingtonUniversity, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me[21] know.

Douglas C. Schmidt[22]

References

1. http://www.cs.wustl.edu/~schmidt/ACE.html

2. http://www.cs.wustl.edu/~schmidt/TAO.html

3. http://www.dre.vanderbilt.edu/CIAO/

4. http://www.dre.vanderbilt.edu/cosmic/

5. http://www.dre.vanderbilt.edu/~schmidt/

6. http://www.cs.wustl.edu/~schmidt/ACE-members.html

7. http://www.wustl.edu/

8. http://www.uci.edu/

9. http://www.vanderbilt.edu/

10. mailto:doc_group@cs.wustl.edu

11. http://www.cs.wustl.edu/~schmidt/ACE-users.html

12. http://www.cs.wustl.edu/~schmidt/commercial-support.html

13. http://www.cs.wustl.edu/~schmidt/ACE.html

14. http://www.cs.wustl.edu/~schmidt/TAO.html

15. http://www.dre.vanderbilt.edu/CIAO/

16. http://www.dre.vanderbilt.edu/cosmic/

17. http://www.dre.vanderbilt.edu/

18. http://www.isis.vanderbilt.edu/

19. http://www.cs.wustl.edu/~schmidt/doc-center.html

20. http://www.opensource.org/

21. mailto:d.schmidt@vanderbilt.edu

22. http://www.dre.vanderbilt.edu/~schmidt/

Bzip2

This program, "bzip2", the associated library "libbzip2", and all documentation, are copyright © 1996-2010 Julian R Seward. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org

bzip2/libbzip2 version 1.0.6 of 6 September 2010

curl

Copyright (c) 1996 - 2013, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

file

Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994- Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GNU General Public License

Some software programs are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or similar Free Software licenses which, among other rights, permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires for any software licensed under the GPL, which is distributed to a user in an executable binary format, that the source code also be made available to those users. For any such software which is distributed along with this Sophos product, the source code is available by submitting a request to Sophos via email to *savlinuxgpl@sophos.com*. A copy of the GPL terms can be found at *www.gnu.org/copyleft/gpl.html*

Info-ZIP

Copyright © 1990–2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions—including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP—must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.
4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

libcap

Unless otherwise *explicitly* stated, the following text describes the licensed conditions under which the contents of this libcap release may be used and distributed:

Redistribution and use in source and binary forms of libcap, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.
2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU General Public License (v2.0 - see below), in which case the provisions of the GNU GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential conflict between the GNU GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL

libdnet

libmagic – file type detection

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

libtirpc

Copyright (c) Copyright (c) Bull S.A. 2005 All Rights Reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

lockfile

Copyright © 2007 Skip Montanaro.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense,

and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

log4cplus

Copyright (C) 2010, Vaclav Haisman. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Medusa web server

Medusa was once distributed under a 'free for non-commercial use' license, but in May of 2000 Sam Rushing changed the license to be identical to the standard Python license at the time. The standard Python license has always applied to the core components of Medusa, this change just frees up the rest of the system, including the http server, ftp server, utilities, etc. Medusa is therefore under the following license:

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting

documentation, and that the name of Sam Rushing not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SAM RUSHING DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL SAM RUSHING BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Sam would like to take this opportunity to thank all of the folks who supported Medusa over the years by purchasing commercial licenses.

mock

Copyright (c) 2003-2012, Michael Foord All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS AS IS AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ncurses

Copyright (c) 1998-2004,2006 Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

netaddr

License for incorporated software:

intset.py - Immutable integer set type

and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

■ The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Network Time Protocol

Copyright (c) University of Delaware 1992-2011

Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

OpenSSH

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1)

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland All rights reserved

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

[Tatu continues]

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library

- IDEA is no longer included, its use is deprecated

- DES is now external, in the OpenSSL library

- GMP is no longer used, and instead we call BN code from OpenSSL

- Zlib is now external, in a library

- The make-ssh-known-hosts script is no longer included

- TSS has been removed

- MD5 is now external, in the OpenSSL library

- RC4 support has been replaced with ARC4 support from OpenSSL

- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO

OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2)

The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com>

<http://www.core-sdi.com>

3)

ssh-keyscan was contributed by David Mazieres under a BSD-style license.

Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4)

The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
   @author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
   @author Paulo Barreto <paulo.barreto@terra.com.br

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER

CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6)

Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl
Theo de Raadt
Niels Provos
Dug Song
Aaron Campbell
Damien Miller
Kevin Steves
Daniel Kouril
Wesley Griffin

Per Allansson
Nils Nordman
Simon Wilkinson

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

Ben Lindstrom
Tim Rice
Andre Lucas
Chris Adams
Corinna Vinschen
Cray Inc.
Denis Parker
Gert Doering
Jakob Schlyter
Jason Downs
Juha Yrjölä
Michael Stone
Networks Associates Technology, Inc.
Solar Designer
Todd C. Miller
Wayne Schroeder
William Jones
Darren Tucker
Sun Microsystems
The SCO Group
Daniel Walsh
Red Hat, Inc
Simon Vallet / Genoscope

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8)

Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

"THE BEER-WARE LICENSE" (Revision 42): <phk@login.dknet.dk> wrote this file. As long as you retain this notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

b) snprintf replacement

Copyright Patrick Powell 1995 This code is based on code written by Patrick Powell (papowell@astart.com) It may be used for any purpose as long as this notice remains intact on all source code distributions

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:
Todd C. Miller
 Theo de Raadt
 Damien Miller
 Eric P. Allman
 The Regents of the University of California
 Constantin S. Svintsoff

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright * notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER

IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some code is licensed under an ISC-style license, to the following copyright holders:

Internet Software Consortium.
Todd C. Miller
Reyk Floeter
Chad Mynhier

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Some code is licensed under a MIT-style license to the following copyright holders:

Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

pyasn1

Copyright (c) 2005-2013, Ilya Etingof <ilya@glas.net> All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS AND CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

pycrypto

Distribute and use freely; there are no restrictions on further dissemination and usage except those imposed by the laws of your country of residence. This software is provided "as is" without warranty of fitness for use or suitability for any purpose, express or implied. Use at your own risk or not at all.

Incorporating the code into commercial products is permitted; you do not have to make source available or contribute your changes back (though that would be nice).

– –amk (www.amk.ca)

pysmb

Copyright (C) 2001-2013 Michael Teo <miketeo (a) miketeo.net>

This software is provided 'as-is', without any express or implied warranty. In no event will the author be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice cannot be removed or altered from any source distribution.

pysphere

Copyright (c) 2011, Sebastian Tello

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

■ Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

■ Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

■ Neither the name of copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Python

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, worldwide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright © 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 Python

strace

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

sudo

Copyright (c) 1994-1996, 1998-2013 Todd C. Miller <Todd.Miller@courtesan.com>

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Sponsored in part by the Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory, Air Force Materiel Command, USAF, under agreement number F39502-99-1-0512.

tcl

This software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, ActiveState Corporation and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES

THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. government, the Government shall have only "Restricted Rights" in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as "Commercial Computer Software" and the Government shall have only "Restricted Rights" as defined in Clause 252.227-7014 (b) (3) of DFARs. Notwithstanding the foregoing, the authors grant the U.S. Government and others acting in its behalf permission to use and distribute the software in accordance with the terms specified in this license.

TinyXML XML parser

www.sourceforge.net/projects/tinyxml

Original code by Lee Thomason (www.grinninglizard.com)

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Vim

1. There are no restrictions on distributing unmodified copies of Vim except that they must include this license text. You can also distribute unmodified parts of Vim, likewise unrestricted except that they must include this license text. You are also allowed to include executables that you made from the unmodified Vim sources, plus your own usage examples and Vim scripts.
2. It is allowed to distribute a modified (or extended) version of Vim, including executables and/or source code, when the following four conditions are met:

   a. This license text must be included unmodified.
   b. The modified Vim must be distributed in one of the following five ways:

    a. If you make changes to Vim yourself, you must clearly describe in the distribution how to contact you. When the maintainer asks you (in any way) for a copy of the modified Vim you distributed, you must make your changes, including source code, available to the maintainer without fee. The maintainer reserves the right to include your changes in the official version of Vim. What the maintainer will do with your changes and under what license they will be distributed is negotiable. If there has been no negotiation then this license, or a later version, also applies to your changes. The current maintainer is Bram Moolenaar <Bram@vim.org>. If this changes it will be announced in appropriate places (most likely vim.sf.net, www.vim.org and/or comp.editors). When it is completely impossible to contact the maintainer, the obligation to send him your changes ceases. Once the maintainer has confirmed that he has received your changes they will not have to be sent again.

    b. If you have received a modified Vim that was distributed as mentioned under 2.2.1 you are allowed to further distribute it unmodified, as mentioned at 1). If you make additional changes the text under 2.2.1 applies to those changes.

    c. Provide all the changes, including source code, with every copy of the modified Vim you distribute. This may be done in the form of a context diff. You can choose what license to use for new code you add. The changes and their license must not restrict others from making their own changes to the official version of Vim.

    d. When you have a modified Vim which includes changes as mentioned under 2.2.3, you can distribute it without the source code for the changes if the following three conditions are met:

        ■ The license that applies to the changes permits you to distribute the changes to the Vim maintainer without fee or restriction, and permits the Vim maintainer to include the changes in the official version of Vim without fee or restriction.

        ■ You keep the changes for at least three years after last distributing the corresponding modified Vim. When the maintainer or someone who you distributed the modified Vim to asks you (in any way) for the changes within this period, you must make them available to him.

        ■ You clearly describe in the distribution how to contact you. This contact information must remain valid for at least three years after last distributing the corresponding modified Vim, or as long as possible.

    e. When the GNU General Public License (GPL) applies to the changes, you can distribute the modified Vim under the GNU GPL version 2 or any later version.

  c. A message must be added, at least in the output of the ":version" command and in the intro screen, such that the user of the modified Vim is able to see that it was modified. When distributing as mentioned under 2.2.5 adding the message is only required for as far as this does not conflict with the license used for the changes.

  d. The contact information as required under 2.2.1 and 2.2.4 must not be removed or changed, except that the person himself can make corrections.

3. If you distribute a modified version of Vim, you are encouraged to use the Vim license for your changes and make them available to the maintainer, including the source code. The preferred

way to do this is by e-mail or by uploading the files to a server and e-mailing the URL. If the number of changes is small (e.g., a modified Makefile) e-mailing a context diff will do. The e-mail address to be used is <maintainer@vim.org>

4. It is not allowed to remove this license from the distribution of the Vim sources, parts of it or from a modified version. You may use this license for previous Vim releases instead of the license that they came with, at your option.

zlib compression tools

© 1995–2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

ZSI

Copyright (c) 2003, The Regents of the University of California, through Lawrence Berkeley National Laboratory (subject to receipt of any required approvals from the U.S. Dept. of Energy). Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University of California, Lawrence Berkeley National Laboratory, U.S. Dept. of Energy nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

You are under no obligation whatsoever to provide any bug fixes, patches, or upgrades to the features, functionality or performance of the source code ("Enhancements") to anyone; however, if you choose to make your Enhancements available either publicly, or directly to Lawrence Berkeley National Laboratory, without imposing a separate written license agreement for such Enhancements, then you hereby grant the following license: a non-exclusive, royalty-free perpetual license to install, use, modify, prepare derivative works, incorporate into other computer software, distribute, and sublicense such Enhancements or derivative works thereof, in binary and source code form.