# Guardium VM

## Installation Guide

## Version 6.1

Guardium®

SAFEGUARDING DATABASES™

# Contents



230 Third Ave, Waltham, Massachusetts 02451 T. 877 487 9400 F. 781 487 7900 www.Guardium.com



Document Version 6.1 January 28, 2008

# Introduction

Guardium provides a unified, cross-platform solution that both protects databases in real time and automates the entire compliance auditing process. The solution supports all major database platforms, enterprise applications, and operating systems (UNIX, Linux, Windows, and z/OS).

The solution is delivered as a non-invasive, network-based appliance (G1000, G2000, and G5000) or as a Guardium VM (Virtual Machine), installed directly on VMware's robust infrastructure foundation, ESX Server.

Guardium VM leverages even further already existing resources in an IT environment, by increasing utilization of servers, storage and networks in a virtualized datacenter.

The Guardium VM can be deployed in a variety of operational modes:

- **Collector** – Non-invasively inspects the data stream and enables monitoring of all database access activities, with continuous fine-grained auditing and reporting, real-time policy-based alerting and database access controls.
- **Aggregator** – In distributed enterprise environments, organizations can have multiple Guardium appliances monitoring different geographic locations or business units. To enable an enterprise view, all of the data from multiple appliances is aggregated in a central repository, the Aggregator.
- **Central Manager** – Rather than requiring each appliance to be managed separately, the Central Manager provides a single point of control for defining enterprise-wide policies and reports (including security health metrics). In addition, it allows administrators to remotely view system log files and main statistics, configure systems, and restart them when needed. The Central Manager can be either combined with an Aggregator or deployed as a standalone unit.

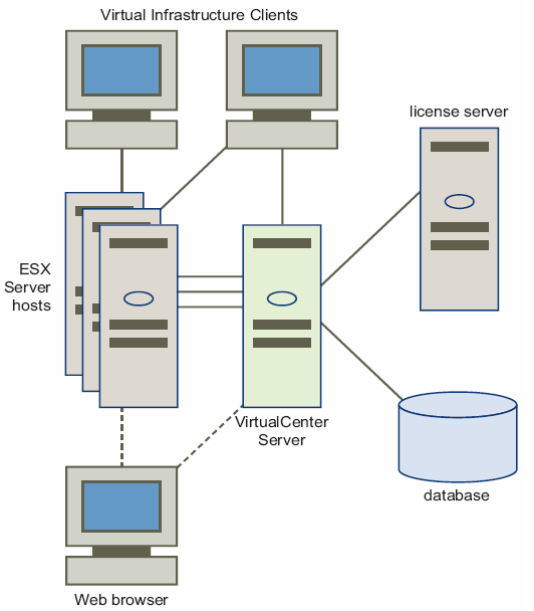
## About this Document

This document describes how to install the Guardium VM as a guest virtual machine under the VMware ESX Server. You must install ESX Server and be familiar with that product before installing the Guardium VM. This document does not describe how to install or configure ESX Server. See the VMware Infrastructure documentation for detailed information on all aspects of installing an using VMware ESX Server: http://www.vmware.com/support/pubs/vi_pubs.html.

## Target Audience

This document is intended for the person who installs the Guardium VM on an already existing ESX server.

# VMware Infrastructure Overview




The VMware ESX Server on which you will install the Guardium VM is one component of the VMware infrastructure illustrated to the right (from the VMware Quick Start Guide). Although not all VMware Infrastructure components are required to support the Guardium VM, you should be familiar with all components that are in use at your installation.

**ESX Server**: This component is used to configure and control VMware virtual machines on a physical host referred to as the ESX Server host. To install a Guardium VM, you first define a virtual machine on an ESX Server host, and then install and configure the Guardium VM software on that virtual machine. You can create multiple Guardium VMs on an ESX Server host.

**VI Client (Virtual Infrastructure Client)**: You use the VI Client to connect to a standalone ESX Server, or to a VirtualCenter Server. In the latter case, you can administer multiple virtual machines created over multiple ESX Server hosts.

**Web Browser**: Use a Web browser to download and use the VI Client software from an ESX Server host or the VirtualCenter server.

The remaining major components of the VMware Infrastructure are not required for the installation of Guardium, but may be used at your installation.

**VirtualCenter Management Server** (**Optional**): This component runs on a remote Windows machine, and can be used to manage multiple virtual machines on multiple ESX Server hosts. It offers a single point of control over all the ESX Server hosts.

**Database** (**Optional**): The VirtualCenter Server uses a database to store configuration information for the infrastructure. The database is not needed if the VirtualCenter Server is not used.

**License Server** (**Optional**): Stores and manages the licenses needed to maintain a VMware Infrastructure.

# Installation

## Overview

The Guardium VM is a software-only solution licensed and installed on a guest virtual machine on a VMware ESX Server. To install the Guardium VM, follow the steps outlined below. Each of the installation procedures is described in detail, in a separate section.

If you are installing multiple Guardium VM systems in a VMware VirtualCenter Management Server environment, you can easily create a template system from the first Guardium VM that you create, and then clone that template as necessary. Then all you need to do is set the IP address and install the License Activation Patch on each cloned system. See the note following Step 7 for more information about this.

# Installation Procedures

## Step 1. Verify System Compatibility

1. Verify that the host is compatible with VMware's ESX Server (version 3.x or later); see the VMware document entitled Systems Compatibility Guide for ESX Server, which is available online in PDF format.
2. Verify that a virtual machine installed on the host will be able to provide the minimum recommended resources described in the table below, for either a Guardium VM Collector, Central Manager, or Aggregator.

**Guardium VM Minimum Recommended Resources**

| Resource | Collector | Aggregator[3] | Central Manager[3] |
|---|---|---|---|
| **CPU (core)** [1] | 1 | 1 | 1 |
| **Memory** | 4GB | 4GB | 1GB |
| **Ports**[2] | 1 | 1 | 1 |
| **Disk Size** | 120GB | 300GB | 80GB |
| **CD Drive** | 1 | 1 | 1 |

1. Tested on dual-core machines.
2. Each port can be an actual NIC, or a virtual switch that can be configured to use multiple NICs, optionally with failover IP teaming.
3. A single Guardium VM can be configured as both an aggregator and Central Manager. In that case, the Aggregator resources are required.

## Step 2. Install VMware ESX Server

If it is not already installed, install VMware ESX Server. VMware provides installation instructions on their Web site to assist in installing and configuring the VMware Infrastructure and ESX server. Note that ESX server is only supported on a specific set of hardware devices. For more information, see the VMware Virtual Infrastructure documentation.

## Step 3. Connect Network Cables

Before defining any virtual switches that will be used for the Guardium VM, you will need to connect the appropriate NICs to the network. You will not be able to assign NICs to virtual networks or switches until the NICs are physically connected.

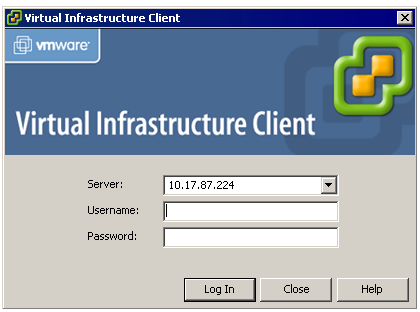
The following table describes how the Guardium VM uses network interfaces. Refer to this table to make the appropriate connections before configuring the virtual switches for use by the Guardium VM.

**Guardium VM Network Interface Use**

| Interface | Description |
|---|---|
| **Primary Management (eth0)** | The connection over which you will configure and manage the Guardium VM, using the browser based Administrator and User portals, and the command line interface (CLI) console. This is also the interface over which the Guardium VM communicates with all other Guardium components, which can include:<br>• Other virtual or real Guardium appliances, which can be collectors, aggregators, or a Central Manager<br>• S-TAP or CAS clients, which are Guardium software agents installed on database servers<br>• Backup systems, which can be FTP or SCP servers, Centera or TSM archive storage systems |
| **Secondary Management (eth3)** | Optional. A second NIC can be configured as a failover device if the primary management interface becomes unavailable. To do this in the VMware environment, you simply define this adapter as a Standby Adapter in the virtual network defined for the primary management NIC. |

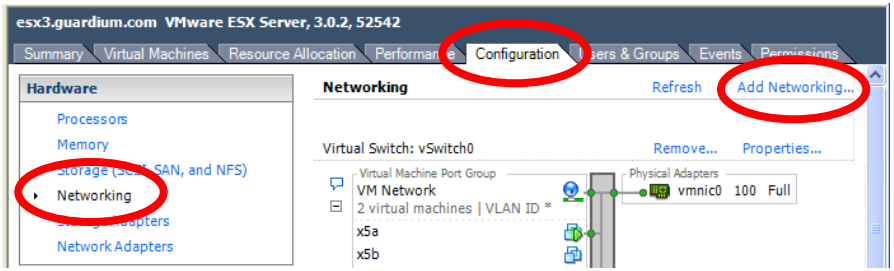
## Step 4. Configure the Guardium VM Management Port

The default configuration for a new VMware ESX Server installation creates a single port group for use by the VMware service console and all virtual machines. For the Guardium VM, we strongly recommend that you **do not** share ports with the VMware console or any other virtual machine. Follow the instructions below to create one or more virtual switches to be used by Guardium VM.




1. Open the VMware VI Client, and log on to either a VirtualCenter Server, or the ESX Server host on which you want to create a new virtual machine.
2. If logged into a VirtualCenter Server, click **Inventory** in the navigation bar, expand the inventory as needed to display the managed host or cluster on which you will install Guardium VM.
3. In the inventory display, click on the host or cluster on which you will install Guardium VM.

4. Click the **Configuration** tab, click **Networking** in the Hardware box, and then click **Add Networking** in the upper right portion of the panel.

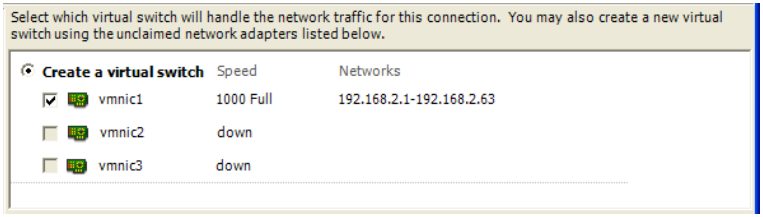



This opens the **Add Network Wizard**, which is used for a variety of purposes.

We will use the Add Network Wizard here to define a new virtual switch for the Guardium VM network interface. This is the connection over which you will access the Guardium VM management console, and over which the Guardium VM will communicate with other Guardium components (S-TAPs, for example, which are software agents you will install later on one or more database servers).

5. In the Connection Types box, select **Virtual Machine** and click **Next**.

6. In the Network Access panel, select **Create a virtual switch**, and mark the unclaimed network adapter that you will use for the Guardium VM network interface:

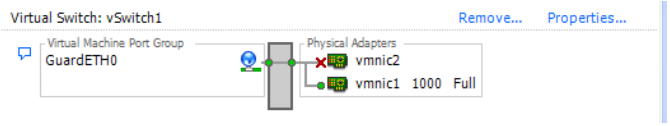



7. Optionally mark a second unclaimed network adapter if want to use VMware's IP teaming capability to provide a secondary (failover) network interface. Later (below), you will designate this second adapter as a Standby Adapter (and of course you will have to cable both NICs appropriately).

8. Click **Next** to continue to the Connection Settings page of the Add Network Wizard.

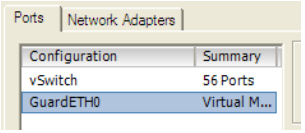
9. In the **Network Label** box, enter a name for the virtual machine port group, for example: **GuardETH0**, and click **Next**.

10. In the Summary page, click **Finish**. The new virtual switch will display in the Configuration tab.



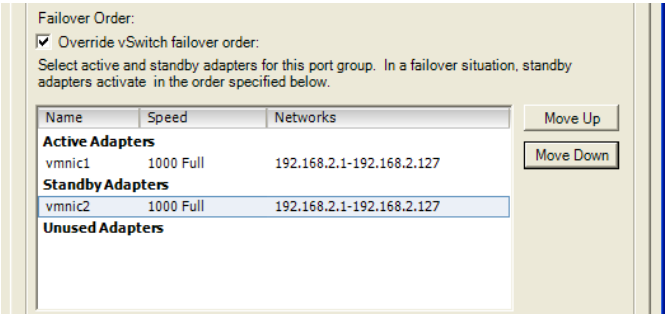

11. Optional. If you have defined a second adapter for failover purposes:

    a. Click the **Properties** link for the virtual switch just created (see above) to open the virtual switch Properties panel:



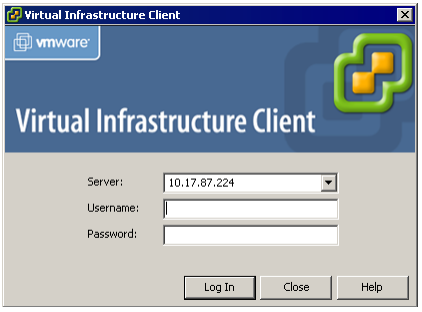

    b. Click the **Ports** tab and select the virtual port group just created (**GuardETH0** in the example above), and click the **Edit** button at the bottom of the panel.

    c. In the virtual port group Properties panel, click the **NIC Teaming** tab, mark the **Override vSwitch Failover** box, and then move the second adapter to the **Standby Adapters** list:




    d. Click **OK** to close the virtual port group Properties box, and click **Close** to close the virtual switch Properties box.

## Step 5. Create a new Virtual Machine

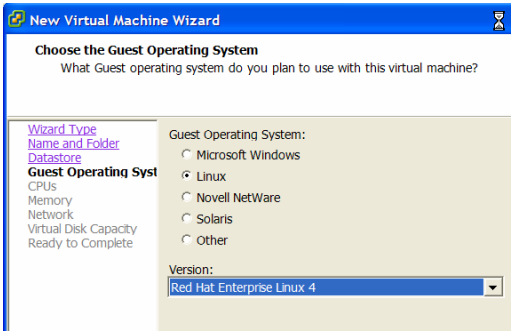



If you have not already done so, create a new virtual machine on which to install Guardium VM.

Perform this task using the VMware VI Client.

1. Open the VMware VI Client, and log on to either a VirtualCenter Server, or the ESX Server host on which you want to create a new virtual machine.

2. If logged into a VirtualCenter Server, click **Inventory** in the navigation bar, expand the inventory as needed, and select the managed host or cluster to which you want to add the new virtual machine.
3. From the File menu, select **New – Virtual Machine** to open the configuration Type panel of the New Virtual Machine wizard.
4. Select **Typical** as the configuration type, and click **Next** to continue with the Name and Folder panel.
5. On the Name and Folder panel:
   a. Enter a name for the new virtual machine in the **Virtual Machine Name** field. This name appears in the VI Client inventory and is also used as the name of the virtual machine's files.
   b. To set the inventory location for the new virtual machine, select a folder or the root location of a datacenter from the list under **Virtual Machine Inventory Location**.
   c. Click **Next**.
6. If your host or cluster contains resource pools, the Resource Pool panel displays, and you must:
   a. Select the resource (host, cluster, or resource pool) in which you want to run the virtual machine.
   b. Click **Next**.
7. On the Datastore panel, optionally select a datastore in which to store the new virtual machine files, and click **Next**.
8. On the *Choose the Guest Operating System* panel, select **Linux** , select **Red Hat Enterprise Linux 4** from the Version box, and click **Next**.




The operating system will not be installed now, but the OS type is needed to set appropriate default values for the virtual machine.

*For the next four panels, refer to the following table.*

**Guardium VM Minimum Recommended Resources**

| Resource | Collector | Aggregator | Central Manager |
|---|---|---|---|
| **CPU (core)** | 1 | 1 | 1 |
| **Memory** | 4GB | 4GB | 1GB |
| **Ports**[2] | 1 | 1 | 1 |
| **Disk Size** | 120GB | 300GB | 80GB |
| **CD Drive** | 1 | 1 | 1 |

9. On the Virtual CPUs panel, select number of CPUs recommended for the type of Guardium VM being installed, and click **Next**.
10. On the Memory panel, select the amount of memory recommended for the type of Guardium VM being installed, and click **Next**.
11. On the Network panel, select 1 as the number of ports required, and click **Next**.
12. For the selected port, use the **Network** pull-down menu to choose a port group configured for virtual network use. (You should have defined this port group in the previous procedure.)
13. For the selected port group, mark the **Connect at Power On** check box (it should be marked by default), and click **Next**.
14. On the Virtual Disk Capacity panel, enter the amount of disk space to reserve for the new virtual machine in the Disk Size field.
15. On the Ready to Complete panel, verify your settings and click **Finish**.

This completes the definition of the new virtual machine. The operating system has not yet been installed, so if you attempt to start the virtual machine, that activity will fail.

### Step 6. Install the Guardium Virtual Appliance

Perform this task using the VMware Virtual Infrastructure Client.

1. Open the VMware VI Client, and log on to either a VirtualCenter Server, or the ESX Server host on which you want to create a new virtual machine.
2. If logged into a VirtualCenter Server, click **Inventory** in the navigation bar, expand the inventory as needed, and select the virtual machine on which you want to install the Guardium VM.
3. On the Summary tab, click **Edit Settings**.

4. Select **CD/DVD Drive 1**.
5. Select one of the following options to determine from where the virtual CD-ROM device will read the Guardium Installation program. ***We strongly recommend the first option below***:
    - **Datastore ISO File** – Connect to the Guardium Installation ISO file on a datastore. If you have not already done so, copy the Guardium ISO file to a datastore accessible from the ESX Server host on which the virtual machine is installed. Click the **Browse** button to select the file.

      **Caution:** For the remaining options you will place the Guardium Installation CD in a CD-ROM drive. If you reboot any system with a Guardium Installation CD in its CD-ROM drive, you will install Guardium on that system, wiping out the host operating system and files.

    - **Client Device** – Connect to a CD-ROM device on the system on which you are running the VI Client. If you select this option, insert the Guardium CD in the CD-ROM drive of the system on which the VI Client is running.
    - **Host Device** – Connect to a CD-ROM device on the ESX Server host machine on which the virtual machine is installed. If you select this option, choose the device from a drop-down menu, and insert the Guardium CD in the CD-ROM drive of the ESX Server host machine.
6. Click **OK**.
7. Click **Power On** to start the virtual machine.
8. If you selected **Client Device** as your CD/DVD Drive option, click **Virtual CDROM(ide0:0)** in the toolbar, and select the local CD-ROM device to connect to.
9. Click the **Console** tab to display the virtual machine console. You will need to respond to several prompts during the installation process.

   **Note** The passwords you supply in the next two steps are temporary. They will be replaced when you apply the License Activation patch, by the values shown on your copy of the License Key File for the appliance. You can change these values after the system has been activated.

10. When prompted for the ***cli*** password, enter a temporary password for use when logging in to the Guardium CLI, which you will need to do to set the IP configuration parameters for the appliance.
11. When prompted for the **GUI admin** password, enter a temporary password for use when logging in to the Guardium administrator portal, as the privileged *admin* user.

12. When asked if building a Collector or Aggregator, enter **y** for a Collector, or **n** for an Aggregator.
13. Reply **No** to the **Master Passkey** prompt.

**Caution:** If a CD-ROM drive was used, the CD ejects when the installation completes. Be sure to remove the installation CD from that drive.

If the ISO file was used, be sure to "remove" the ISO CD ROM by changing the virtual CD/DVD back to a Client or Host Device.

Otherwise, the next time it is rebooted, you will install Guardium on the host machine, wiping out the host machine operating system and all files.

The machine will reboot automatically, and you will be prompted to log in as the ***cli*** user.

14. Enter the temporary ***cli*** password you supplied previously.

In the following steps you will supply various network parameters to integrate the Guardium VM into your environment, using *cli* commands.

In the *cli* syntax, variables are indicated by angled brackets, for example: **<ip_address>**

Replace each variable with the appropriate value for your network and installation (but do not include any brackets).

15. Set the primary IP address and network mask for the Guardium VM:

```
store network interface 1 ip <ip_address>
store network interface 1 mask <subnet_mask>
```

16. Set the default router IP address:

```
store network routes def <default_router_ip>
```

17. Set the DNS server IP address (only the first is required):

```
store network resolver 1 <resolver_1_ip>
store network resolver 2 <resolver_2_ip>
store network resolver 3 <resolver_3_ip>
```

18. An SMTP server is required to send system alerts. Enter the following commands to set your SMTP server IP address, set a return address for messages produced by Guardium VM, and enable SMTP alerts on startup.

```
store alerter smtp relay <smtp_server_ip>
store smtp email returnaddr <first.last@company.com>
store alerter state startup on
```

19. Use the following two commands to set the host and domain names for the Guardium VM. We recommend using the same host name that you used for the virtual machine on which you are installing Guardium. For example if you created a virtual machine named Guard123 on the ESX virtual host, use Guard123 in the **store system hostname** command .

    ```
    store system hostname <host_name>
    store system domain <domain_name>
    ```

20. There are two options for setting the date and time for the Guardium VM. Do one of the following:

    **Date/Time Option 1:** Specify an NTP server host name and enable its use (the NTP server specified must be accessible from the Guardium VM):

    ```
    store system ntp server <ntpserver_name>
    store system ntp state on
    ```

    **OR**

    **Date/Time Option 2:** Set the time zone, date and time. First, enter the following command to display a list of time_zone strings.

    ```
    store system clock timezone list

    Timezone:                Description:
    ---------                -----------
    Africa/Abidjan:
    Africa/Accra:
    Africa/Addis_Ababa:
    Africa/Algiers:
    .
    .
    .
    ```

    The most common US time zone strings are:

    ```
    America/New_York:        Eastern Time
    America/Chicago:         Central Time
    America/Denver:          Mountain Time
    America/Los_Angeles:     Pacific Time
    ```

    Locate and copy your Timezone string to the clipboard – do not include the colon character (:) – and repeat the previous command replacing the keyword **list** with your *time_zone* string. For example, for US Eastern time you would select *America/New_York* and enter the following command:

    ```
    store system clock timezone America/New_York
    ```

    Now use the following command to store the date and time, in the format: `YYYY-mm-dd hh:mm:ss`
    For example: `2007-07-12 10:40:00`

    ```
    store system clock datetime <date_time>
    ```

21. If this Guardium VM is a collector, enter the following command:

    ```
    store unit type stap
    ```

22. If this Guardium VM is a central manager, enter the following command:

    ```
    store unit type manager
    ```

23. Validate all settings. Enter the following commands one at a time to verify that you have entered your network configuration parameters correctly. If any of the values have been entered incorrectly, refer to the instructions above and replace the value.

    ```
    show system full
    show network interface all
    show network routes def
    show network resolver all
    show alerter smtp relay
    show system clock timezone
    show system clock datetime
    show system ntp all
    show unit type
    ```

24. After making certain that a Guardium Installation CD (if used) is not still present in the CD-ROM drive, reboot the system by entering the following command:

    ```
    restart system
    ```

### Step 7. Install Guardium Maintenance Patches

There may not be any maintenance patches included with the installation materials. If any are included, apply them as described below.

1. Log in to the Guardium VM console, as the *cli* user, using the temporary *cli* password you defined in the previous installation procedure. You can do this using any console connection supported by VMware (VI Client, WebAccess, etc.), or by using an *ssh* client.

2. Do one of the following:

   **If installing from a patch CD**, Insert the CD into the Guardium CD drive, enter the following command, and skip ahead to step 3:

   ```
   store system patch install cd
   ```

   **If installing from a network location**, enter the following command (selecting either **ftp** or **scp**):

   ```
   store system patch install [ftp | scp]
   ```

   And respond to the following prompts (be sure to supply the full path name to the patch file):

```
Host to import patch from:
User on <hostname>:
Full path to patch, including name:
Password:
```

3. You will be prompted to select the patch to apply:

   ```
   Please choose one patch to apply (1-n,q to quit):
   ```

   Type the number of the patch to apply, and then press Enter.

4. To install additional patches, repeat steps 2 and 3 above.

### Step 7a: (Optional) Installing Multiple Guardium VMs

To install multiple Guardium VMs, you can repeat the above procedures for each appliance, or you can minimize your work by cloning the first Guardium VM created (to this point), and following the steps outlined below. Be sure to perform this procedure before applying the activation patch to the first Guardium VM (as described later).

1. Use the VMware virtual infrastructure server product to clone the first Guardium VM configured (as described above) to a template.
2. From the template, create a clone for each additional Guardium VM to be configured.
3. For each clone, log in to the Guardium VM console as the *cli* user, using the temporary *cli* password, and reset any of the IP configuration parameters that you set in the previous procedure. Typically, you will only need to reset the IP address and the host name, but you should review all of the IP configuration settings entered in the previous procedure:

   ```
   store network interface 1 ip <ip_address>
   store network interface 1 mask <subnet_mask>

   store system hostname <host_name>
   ```

   When you are done, enter the **restart system** command:

   ```
   restart system
   ```

4. For each Guardium VM, install the License Activation Patch as described in the following procedure.

### Step 8. Install License Activation Patch

The Guardium license key is an encrypted value that enables all of the options you have purchased for a single appliance. Each key is generated for a single Guardium appliance, which may be a Collector, Aggregator or Central Manager.

You install a license key by applying Guardium's **License Activation Patch**, which is distributed on a **License CD** with your installation kit.

To activate the license:

1. Log in to the Guardium VM console, as the *cli* user, using a console connection supported by VMware (VI Client, WebAccess, etc.). For this procedure, do *not* log in using an *ssh* client, because a network driver will be replaced and the network will not be available.
2. Upload the appropriate **License Activation Patch** for this appliance from CD or using SCP/FTP (remember that every appliance has a unique activation patch – you cannot apply the same activation patch to multiple appliances):

   **If installing from a License CD**, insert the CD into a CD drive on the server, enter the following command, and skip ahead to step 3:

   ```
   store system patch install cd
   ```

   **If installing from a network location**, enter one of the following commands:

   ```
   store system patch install scp
   ```

   **OR**

   ```
   store system patch install ftp
   ```

   And respond to the following prompts (be sure to supply the full path name to the patch file):

   ```
   Host to import patch from:
   User on <hostname>:
   Full path to patch, including name:
   Password:
   ```

3. You will be prompted to select the patch to apply:

   ```
   Please choose one patch to apply (1-n,q to quit):
   ```

   Type the number of the **License Activation Patch** to apply, and then press Enter.

   The license activation patch will restart the server. Your console session will be terminated as the appliance reboots. (To log in again via the *cli*, you will need to use the *cli* password from the license file.)
4. Allow several minutes for the appliance to restart, and then log into the Guardium *administrator* portal from a browser window (Microsoft Internet Explorer is the only browser officially supported).
5. To open the login page, type the Guardium VM address in the browser Address box, in the following format:

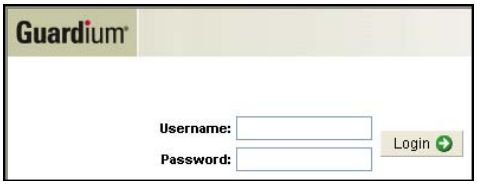
   **https://appliance_name:8443**

   **Note**: The address begins with the letters *https* (not the more common *http* protocol).

Substitute for the *appliance_name*, using either your hostname or its primary IP address. For example:

```
https://192.168.3.47:8443
https://guard02:8443
```

After typing the URL in the address box, press the Enter key to open Guardium Login Page:




6. Enter *admin* in the Username box, enter the *admin* password from the license file for this appliance, and click the Login button. This opens the Guardium Administrator portal. See the *Guardium Administrator Guide* for additional information about performing administrator tasks.

## Step 9. Install S-TAPs

S-TAP is a lightweight software agent installed on database servers. The agent continuously communicates with a Guardium appliance, designated as an S-TAP Host. It monitors and reports local and network database traffic to the S-TAP Host.

To install an S-TAP, do refer to one of the following documents:

- *Guardium S-TAP for Windows Installation and Configuration Guide*
- *Guardium S-TAP for Unix Installation and Configuration Guide*

To verify that the S-TAPs have been installed and are connected to the Guardium appliance:

1. Log in to the Guardium *administrator* portal.
2. Navigate to the **Tap Monitor** – **S-TAP** tab, and select **S-TAP Status** from the menu. All active S-TAPs should display with a green background. A red background indicates that the S-TAP is not active.