Veritas™ Disaster Recovery Advisor Upgrade Best Practices

AIX, ESX, HP-UX, Linux, Solaris, Windows Server

6.1.1

Symantec

Veritas Disaster Recovery Advisor Upgrade Best Practices

Product version: 6.1.1

Document version: 1.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/contact_techsupp_static.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology

Router, gateway, and IP address information

Problem description:

- Error messages and log files
- Troubleshooting that was performed before contacting Symantec
- Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears

on page 2 of each guide. The latest product documentation is available on the Symantec Web site.

https://sort.symantec.com/documents

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com.

6

Contents

Veritas Disaster Recovery Advisor

Introduction

Veritas Disaster Recovery Advisor (DRA) version 6.1.1 introduces a set of new features and offers a stable and scalable solution that lets you diagnose High Availability (HA) and Disaster Recovery (DR) risks in your IT environment.

This document describes how to upgrade the current DRA deployment in your organization. It describes the upgrade procedures for different deployment architectures. Keep in mind that some of the tasks and requirements described below are optional and depend on the available resources of your organization.

To upgrade to version 6.1.1, you must interrupt DRA's functionality while you install the software and update the database. Carefully review the information below to help you conduct a successful and quick upgrade.

You can only upgrade to version 6.1.1 from version 6.1 with any applied hot fix. If you are running a version of DRA older than 6.1, upgrade to 6.1 before you perform the steps in this document.

Single master server upgrade

A single server (also referred to as a “master server”) deployment consists of one DRA instance installed on one host. A single server is responsible for both data collection and data analysis.

Typically, a single server deployment includes a local installation of the Oracle 11g Standard Edition (or higher) database engine, which DRA manages autonomously. If your deployment uses a remote Oracle database, see “Remote Oracle database considerations” on page 11.

Upgrading to DRA 6.1.1 requires the installation of new software files and the updating of the Oracle database. The upgrade package performs both these tasks automatically.

To upgrade a single server environment, you must stop DRA operations, including data collections and data analysis. During this interruption:

1. Scheduled tasks, including scans, risk analyses, and reports, are not executed.
2. Users cannot access the DRA user interface.

During the upgrade, the DRA Oracle database (local or remote) should be up and running so it can receive and perform update commands.

If you encounter a problem during the upgrade, you can perform a rollback operation returning to the original DRA system files and a backed up version of the database.

Master server and data collectors architecture upgrade

A master server and data collectors architecture lets you distribute data collections between the master server and the data collector servers, while only the master server analyzes the data. As with single master server, the Oracle database might be placed locally on the master server or remotely on a different host.

Unlike the single server architecture, DRA is operational even when one, some, or all the data collectors are in `Disabled` mode.

The procedure for upgrading the master server in a data collector architecture is the same as upgrading a single master server.

Data collector upgrade

Data collectors do not require a software upgrade. After the master server is upgraded, a data collector automatically pulls all the new upgraded files it needs from the master server during the connection established between the master server and the collector. All data collectors are automatically upgraded after the upgrade of master server is complete, and the Apache Tomcat service is started.

To upgrade only a limited set of data collectors, do the following:

1. From the Configuration tab, disable the data collectors before the upgrade.
2. After you upgrade the master server, enable the data collectors selected for the upgrade. They are automatically upgraded.

Note: The same rules apply to a roll back operation. The data collectors are automatically downgraded after the master server is rolled back and the Apache Tomcat service is started.

The scope defined for data collectors in `Disabled` mode is not successfully scanned until the data collectors are brought online and automatically updated during startup.

Remote Oracle database considerations

DRA communication with the Oracle database is transparent in terms of local or remote Oracle placement.

During the upgrade, you do not have to bring down the Oracle database. All the upgrade operations are executed from the DRA master server.

Even though the database is not brought down, Symantec recommends that you inform and include your DBA (or anyone else responsible for the remote Oracle database) as part of the upgrade plan.

Rollback considerations

If DRA is implemented in your production environment, it is safe to assume that the system files are backed up alongside the DRA database (being local or remote). This back up should be sufficient to restore DRA in case of a disaster or maintenance failure — an upgrade being one example. However, you should take extra measures to allow a quick rollback to the most recent state in case there are upgrade complications.

A rollback lets you to return to full functionality in DRA 6.1 while giving you the time to investigate the upgrade failure with Symantec Technical Support.

The steps required to backup all the necessary components and the rollback actions are described below. Before you start the upgrade, review these actions.

Custom changes

You can customize your DRA deployment to best serve your requirements. The upgrade wizard is designed to detect these changes and inform you at the end of the upgrade operation. The custom changes are isolated and are not implemented in the new version.

If you are aware of any custom changes to your DRA deployment, tell Symantec Technical Support before the upgrade so they can inspect and adjust to the upgrade. Otherwise, if the system alerts you of such changes right after the upgrade wizard, continue with your upgrade plan and contact Technical Support for further help.

Work plan

The upgrade work plan consists of the following operations:

1. Review the DR A 6.1.1 documentation.
2. Estimate how long the upgrade will take and set the upgrade time frame.
3. Prepare the required resources for the upgrade.
4. Notify Symantec Technical Support of the time frame and work plan.
5. Shut down the system (master server).
6. Backup the master server.
7. Upgrade the master server.
8. Validate the master server upgrade.
9. Perform a complete or gradual upgrade of the data collectors.
10. Perform final validation checks.

Note: In the case of an unexpected error or upgrade failure, rollback DRA, investigate the failure, resolve the issue, and retry the upgrade starting with step 2.

You should prepare an organizational change management document to include the information in the list above. Depending on your internal requirements and standards, you might also add other considerations.

Official documentation

To prepare for the new version of DRA, end users and maintenance personnel should review the changes in scanning requirements, new features, and other information. You can download the latest documents at:

https://sort.symantec.com/documents

- **Getting Started Guide**
  Provides an overview of the software included in the release. It also explains how to obtain a product license and describes the method for installing DRA.
- **Release Notes**
  Introduces new features, system requirements, known issues in the current version, API changes, and more.
- **Deployment Requirements**
  Includes detailed system requirements for scanning supported items.

- **Support Requirements**
  Includes detailed information on DRA's support matrix, including storage arrays, management consoles, virtual platform products, hosts operating systems, database systems, cluster and multipath software.
- **User's Guide**
  Describes how to install the DRA software and perform DRA tasks.

Some changes, such as the new enhanced Dashboard and Scan Scheduling engine, will aid in the quick adoption to the system once the upgrade complete.

Upgrade time frame

Downtime duration

To upgrade DRA, you need a period of time in which system functionality is stopped, including scope scanning, data analysis, reporting, and user interface access. Table 1-1 summarizes the estimated upgrade time based on system usage (during which the system is down).

Table 1-1 Estimated upgrade time

Scope	Master Resources	Time
<100 hosts	2 CPUs, 4GB	~30 minutes
100 – 500 hosts	2 CPUs, 8GB	~2 hours
500 – 1000 hosts	4 CPUs, 16GB	~4 hours
>1000 hosts	4 CPUs, 16GB	>6 hours

Upgrade times are based on various conditions together with those shown in the table. Symantec recommends planning a full day for a master upgrade in case of a prolonged upgrade, optional post upgrade tasks (such as custom change implementation), or a rollback in case the upgrade fails.

Deciding on the upgrade time frame

Because DRA is part of the change management process in the organization, its value is measured by its ability to identify various risks that may arise in the scanned environments. To remain protected from and informed by these risks, you should schedule the DRA upgrade for a time in which no major maintenance events are scheduled for the production and DR environment (the scanned scope).

User notification

It is important to notify all of DRA's relevant parties about the upcoming upgrade time frame. Users should be aware that access to DRA user interface and scheduled reporting via email will be unavailable until the end of the master server upgrade.

Depending on the upgrade plan, the data collectors can be upgraded all at once or gradually in sets of one or more. In the latter case, the scope covered by the non-upgraded data collectors is not covered by DRA.

Preparations

Server and software

Master server resources

Before you upgrade DRA, make sure the master server meets the following minimum requirements:

- More than 40GB of free disks space (on the drive where DRA is already installed)
- Memory consumption of no more than 40% on idle operation
- CPU consumption of no more than 30% on idle operation

External updates

You should also consider upgrading the Windows operating system on the DRA host as part of the upgrade plan. Examples of these tasks include installing the latest Service Pack and available security and KB patches. Moreover, you should apply other IT requirements, such as system agents and other organizational software packages, to bring the master server to peak condition and to avoid future downtime for these tasks.

Software packages

DRA 6.1.1 software comes as a single file that you should place on the master server. Contact Technical Support to receive a download link to the latest build version of DRA 6.1.1.

Backup plan

The complete backup of the DRA deployment lets you recover from upgrade in case of failure or any other unexpected event. If your deployment is already covered by an extensive backup procedure, make sure you are ready for a rollback; otherwise, follow the guidelines here.

1. Stop DRA to disable writing during backup. Open `services.msc` and `stop` the following services:
   Apache Tomcat WatchDog
   Apache Tomcat6
2. Use your organizational backup utility to back up (or manually copy and set aside) the following folders on the DRA server:
   - *Drive:*`\Program Files\Apache Software Foundation\Tomcat 6.0`
   - *Drive:*`\Program Files\Symantec\Disaster Recovery Advisor\DRA`
3. In case Oracle is installed locally, execute the following to export all database content:
   - Open the command prompt (**cmd**).
   - Navigate to *Drive:*`\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\DRA\`
   - Execute the following batch file:
     export_schema.bat ***username/password***
   - Once export process completes, locate the export file in *Drive:*`\oracle\admin\rgdb\dpdump` and copy it from the host.
4. If the Oracle database is remote, ask your DBA to perform a full database backup.
5. When you are done, start DRA by starting the services described in step 1.

Having the DRA system files and a database backup let you fully recover to the current server or to a new server.

Alternately, you can consider the following options:

- Stop DRA and Oracle to take a virtual machine snapshot.
- Stop DRA and Oracle to take a full disk image.

Rollback plan

The rollback plan mainly depends on the backup plan described above. You should initiate a rollback plan if:

- The master server hardware or operating system fails during or after the upgrade.
- The upgrade fails while you're using the upgrade wizard.
- You cannot bring up Tomcat after the upgrade.
- Data is corrupted or lost, or the user interface does not display correctly.

Before you decide on a rollback plan, Symantec encourages to you contact Technical Support, with whom you should coordinate the upgrade.

You can restore the backup files and start DRA using the following procedure. If you are relocating DRA to a new host, install DRA version 6.0 with the applicable hot fix package before performing these steps:

1. Stop DRA to disable writing during backup. Open `services.msc` and `stop` the following services:
   Apache Tomcat WatchDog
   Apache Tomcat6
2. Use your organizational backup utility to restore (or manually copy) the following folders to the DRA server:
   - *`Drive:`***`\Program Files\Apache Software Foundation\Tomcat 6.0`**
   - *`Drive:`***`\Program Files\Symantec\Disaster Recovery Advisor\DRA`**
3. In case Oracle is installed locally, execute the following to import all database content:
   - Copy the exported Oracle database file to:
     *`Drive:`***`\oracle\admin\rgdb\dpdump`**
   - Change the file name to `EXPDAT.DMP`.
   - Open the command prompt (`cmd`).
   - Navigate to: *`Drive:`***`\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\DRA\`**
   - Execute the following batch:
     `import_schema.bat` ***`username/password`***
4. If Oracle is remote, ask your DBA to perform a full database restore.
5. When you are done, you can start DRA by starting the services from step 1.

Note: You must reinstall the DRA 6.1 data collectors. For more information, see *Veritas Disaster Recovery Advisor User's Guide*.

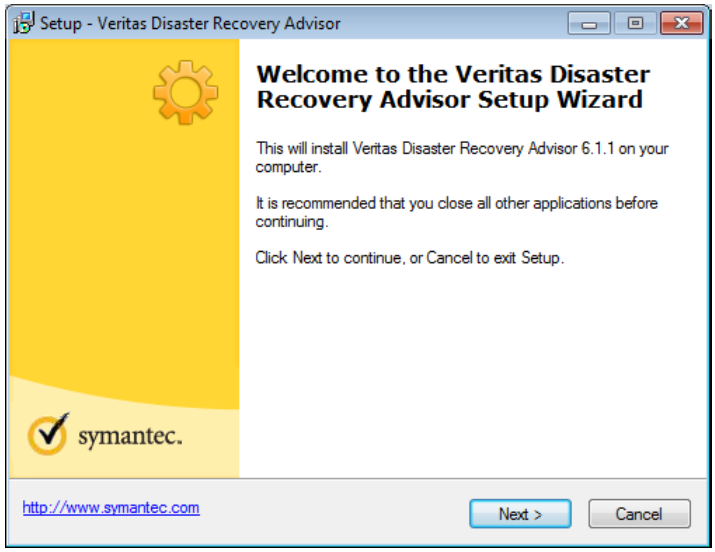
Master server upgrade

The following steps describe how to upgrade a master server in both a single or data collector architecture.

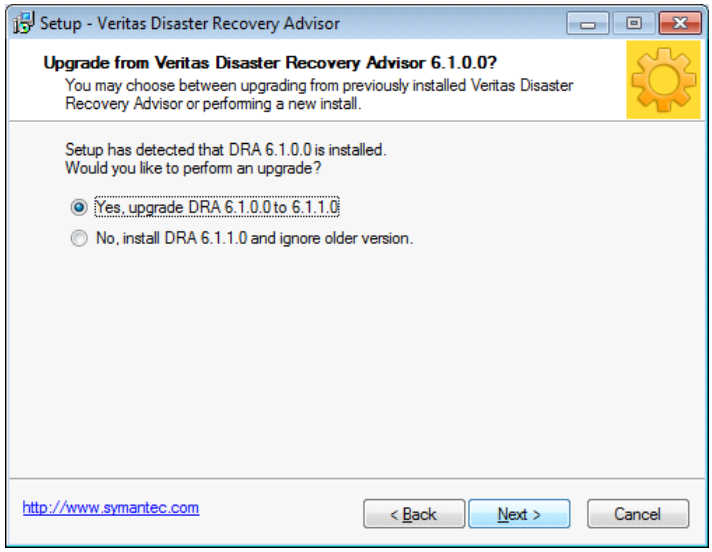
Upgrade tasks

1. Login as the local administrator.
2. Optional (gradual collector upgrade): If you have data collectors, login into the system as the `Admin` role user and `Disable` all the data collectors.
3. Stop the Apache Tomcat Service. Open `services.msc` and `stop` the following services:
   Apache Tomcat WatchDog
   Apache Tomcat6
4. Execute your files and database backup plan.

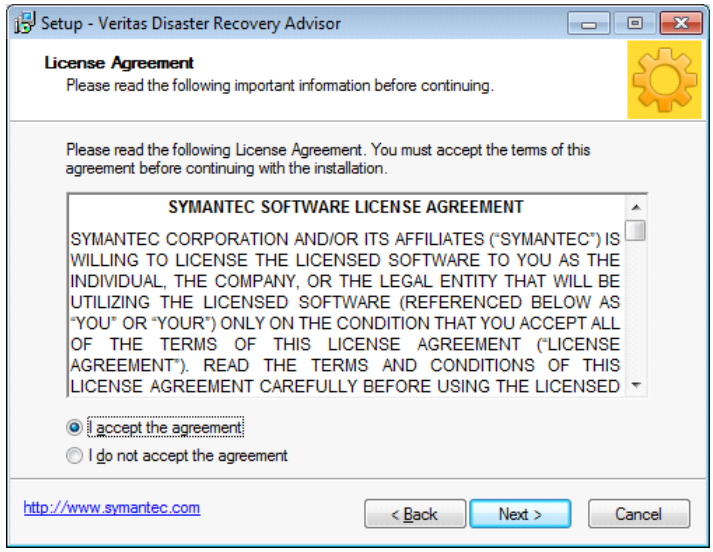
   Important: Make sure the database is up and running after the backup procedure.
5. Run the DRA 6.1.1 installation file (`DRA_6.1.1.exe`) that was supplied by Technical Support.
6. The wizard inspects the system requirements. If a warning message is displayed, review it carefully and decide whether you want to continue.
7. On the Setup Wizard Welcome screen, click **Next**.



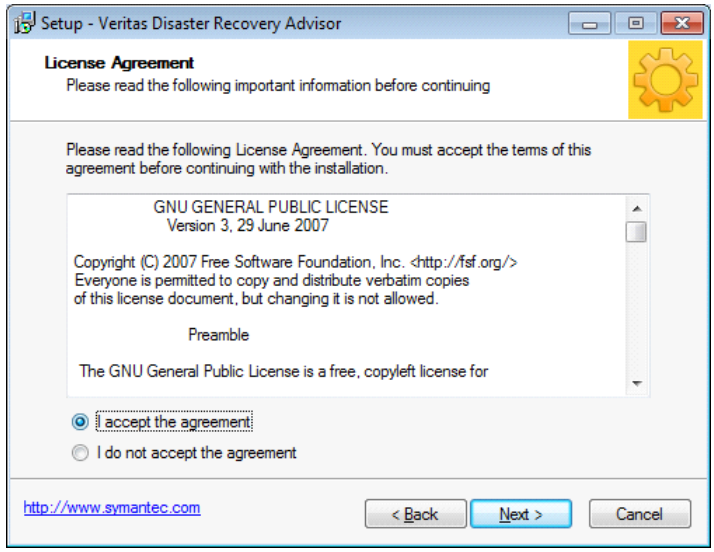
8 The wizard should automatically detect the current installed version and suggest the upgrade. Select **Yes**.



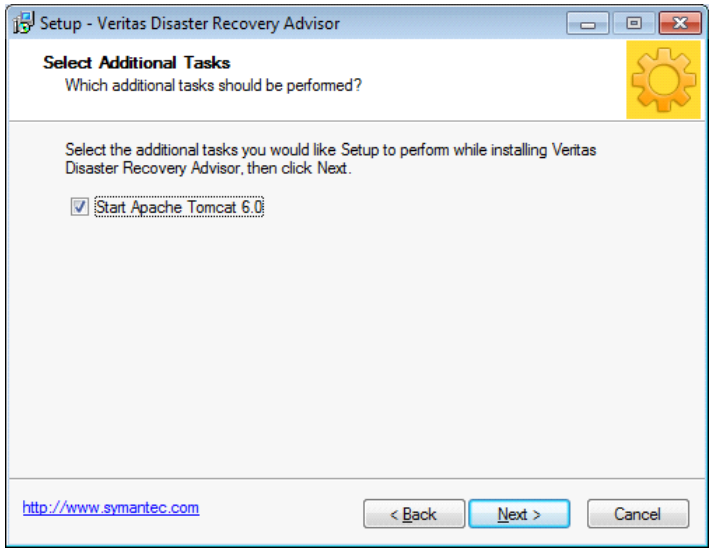
9 Accept the Symantec license agreement.



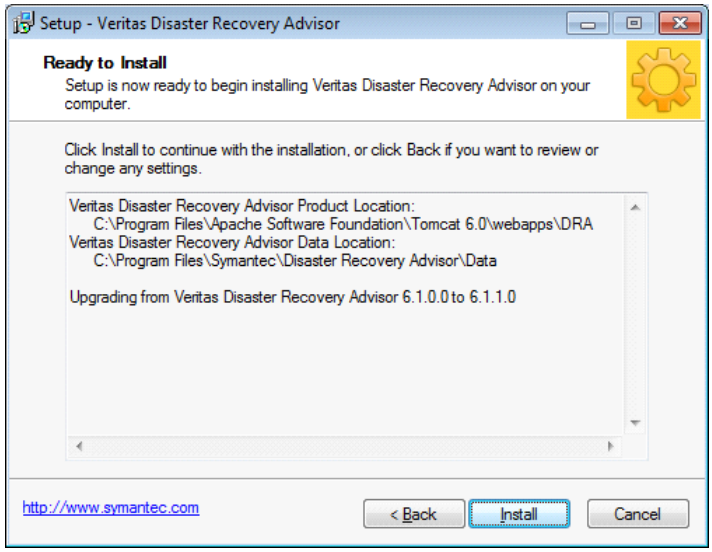
10 Accept the GNU license agreement.



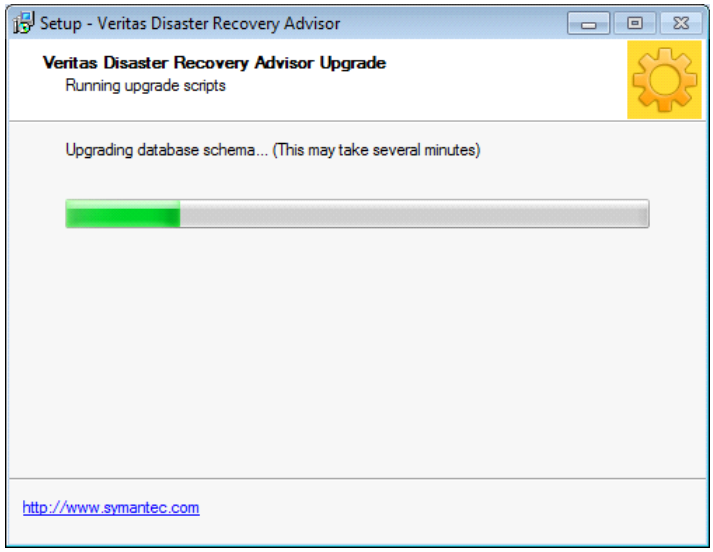
11 If you want the master server to start when the upgrade completes, select **Start Apache Tomcat 6.0**.



12 Confirm the information and press **Install**.

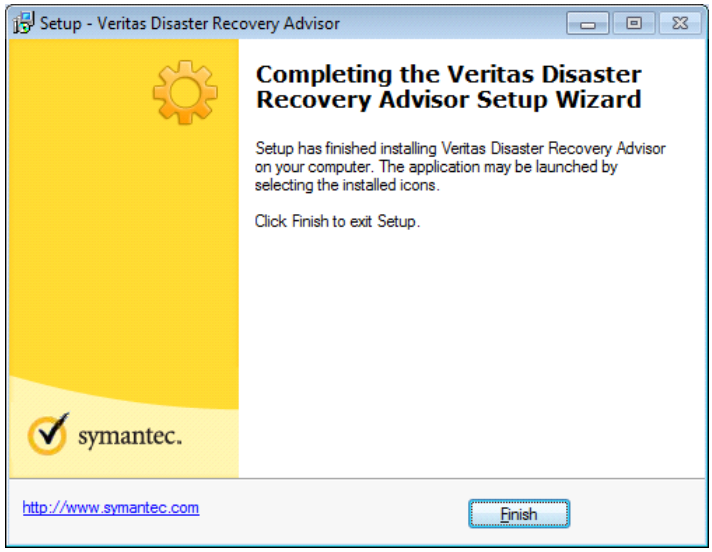


13 Depending on your system usage, the installation might take several hours. (See Table 1-1.)



14 If the wizard detects custom system changes that were applied to version 6.1, a message is displayed. Take note of the information and continue the upgrade.

15 At the end of the upgrade, click **Finish** to exit the Setup Wizard.



16 If you choose to start Apache Tomcat 6.0 during the installation, DRA automatically starts.

Additional changes

If information messages are displayed (step 14 on page 20), contact Technical Support to verify the deviations before you finish the upgrade work plan.

Data collector upgrade

As soon as the master server upgrade is complete and the Apache tomcat service starts, the data collectors are automatically upgraded.

If a gradual upgrade of collectors is the selected approach, upgrade the data collector after the master server upgrade while all the data collectors are still in `Disabled` mode.

When you bring a data collector online, it checks to see if there are any updates available from the master server, and if so, performs an immediate restart and file pull operation to update itself. Therefore, to upgrade a data collector, you should put it in `Enable` mode from the DRA user interface.

After the data collector is online and functional, perform a manual sample scan of that particular data collector's scope to verify scanning functionality. Repeat the operation for each data collector in your environment.