Deployment Guide

Deploying the BIG-IP LTM System v9 with Oracle E-Business Suite 11i

Important: This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support. For a list of current guides, see https://f5.com/solutions/deployment-guides.

Introducing the BIG-IP and Oracle 11i configuration

Oracle and F5 have developed and tested an effective way to direct traffic for Oracle E-Business Suite 11i deployments using the BIG-IP application traffic management device. When deployed with Oracle 11i, the BIG-IP product ensures fast delivery, always-on access, peak security and easy expansion for applications running on Oracle.

With Oracle E-Business Suite 11i and F5 Networks award-winning application traffic management products, enterprises achieve increased security, a higher level of availability and better performance from their Oracle-based applications, while increasing the return on investment of their e-business infrastructures.

For more information on the BIG-IP system, see
http://www.f5.com/products/big-ip/

For more information on the Oracle E-Business Suite 11i, see
http://www.oracle.com/applications/home.html

Prerequisites and configuration notes

The following are prerequisites for this Deployment Guide:

◆ You must have an Oracle 11i deployment running version 11.5.9 or later, with the latest recommended patches.

◆ You have configured your Oracle 11i deployment according to the procedures outlined in Option 2.2, *HTTP Layer Hardware Load Balancing,* of the following Oracle MetaLink document:

   http://metalink.oracle.com/metalink/plsql/ml2_documents.showFra meDocument?p_database_id=NOT&p_id=217368.1
   You need a MetaLink user account to access this file. If you do not have an account, contact Oracle.

◆ The BIG-IP system must be running version 9.0 or later (the step-by-step configuration procedures in this Deployment Guide are for 9.0 or later, for versions 4.5.x and 4.6.x, see
   www.f5.com/pdf/deployment-guides/oracle11i-bigip45-dg.pdf.

◆ Briefly review the basic configuration tasks and the few pieces of information, such as IP addresses, that you should gather in preparation for completing the BIG-IP system configuration.

◆ **Note**

All of the configuration procedures in this Deployment Guide are performed on the BIG-IP system. For specific information on how to configure Oracle 11i, consult the Oracle Documentation.
This document is written with the assumption that you are familiar with both the BIG-IP system and Oracle 11i. For more information on configuring these products, consult the appropriate documentation.

Configuration example

The BIG-IP system provides intelligent traffic management and high availability for Oracle 11i deployments. Through advanced health checking capabilities, the BIG-IP product recognizes when resources are unavailable or under-performing and directs traffic to another resource. The BIG-IP device tracks Oracle end-user sessions, which ensures the client maintains session state with the servers. The following diagram shows an example deployment with Oracle 11i and the BIG-IP system.
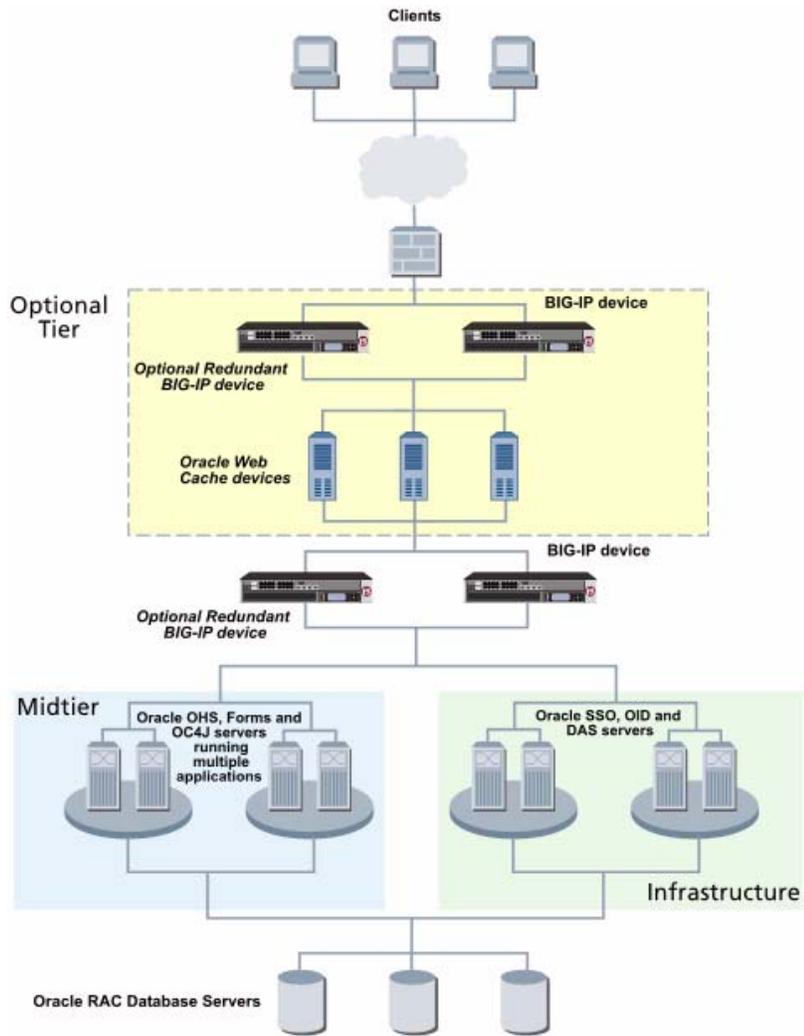

Figure 1.1 BIG-IP Oracle 11i configuration example

Configuring the BIG-IP system for deployment with Oracle 11i

To configure the BIG-IP for directing traffic to the Oracle devices, you need to complete the following procedures:

- *Connecting to the BIG-IP device using the Configuration utility*
- *Creating the HTTP health monitor*
- *Creating the pool*
- *Creating a profile*
- *Creating the virtual server*
- *Synchronizing the BIG-IP configuration if using a redundant system*

The BIG-IP system offers both web-based and command line configuration tools, so that users can work in the environment that they are most comfortable with. This Deployment Guide contains procedures to configure the BIG-IP system using the BIG-IP web-based Configuration utility only. If you are familiar with using the **bigpipe** command line interface you can use the command line to configure the BIG-IP device, however, we recommend using the Configuration utility.

For an added level of automation and intelligence, you can also use the iControl programmatic interface. iControl has proven itself as the first and only Web services (SOAP/XML) API and SDK for network devices. iControl sets a new standard for how applications can monitor, control, and automate network device functions to provide optimal management and operation efficiency in the datacenter. iControl provides a powerful option for enabling applications to work more cohesively with the network for enhanced control, performance, and reliability. For more information on iControl, visit **http://devcentral.f5.com/.**

◆ **Tip**

*We recommend you save your existing BIG-IP configuration before you begin the procedures in this Deployment Guide. To save your BIG-IP configuration, see **Appendix A: Backing up and restoring the BIG-IP system configuration**, on page 1-14.*

Connecting to the BIG-IP device using the Configuration utility

Use the following procedure to access the BIG-IP web-based Configuration utility using a web browser.

To connect to the BIG-IP system using the Configuration utility

1. In a browser, type the following URL:
   https://<administrative IP address of the BIG-IP device>
   A Security Alert dialog box appears, click **Yes**.
   The authorization dialog box appears.

2. Type your user name and password, and click **OK**.
   The Welcome screen opens.

   Once you are logged onto the BIG-IP system, the Welcome screen of the new Configuration utility opens. From the Configuration utility, you can configure and monitor the BIG-IP system, as well as access online help, download SNMP MIBs and Plug-ins, and even search for specific objects.

Creating the HTTP health monitor

The first step is to set up health monitors for the Oracle devices. This procedure is optional, but very strongly recommended. For this configuration, we use the default ICMP health monitor (configured after the pool in the *Adding an ICMP monitor* section), and as well as a slightly customized HTTP monitor.

The HTTP monitor is an Extended Content Verification (ECV) monitor, which checks nodes (IP address and port combinations), and can be configured to use **send** and **recv** statements in an attempt to retrieve explicit content from nodes. We configure the health monitors first in version 9.0, as ECV health monitors are now associated at the pool level.

To configure a health monitor from the BIG-IP Configuration utility

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**. The Monitors screen opens.

2. Click the **Create** button.
   The New Monitor screen opens.

3. In the **Name** box, type a name for the Monitor.
   In our example, we type **oracle_http_monitor**.

4. From the **Type** list, select **http**.
   The HTTP Monitor configuration options appear.

5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91.**

6. In the Send String and Receive Rule sections, you can add a Send String and Receive Rule specific to the device being checked.

   Important Note:
   *When using the **GET** send string, you must end the string by including the HTTP protocol at the end of the statement. Use the following syntax:*
   GET <fully qualified path name> HTTP/1.0
   For example:
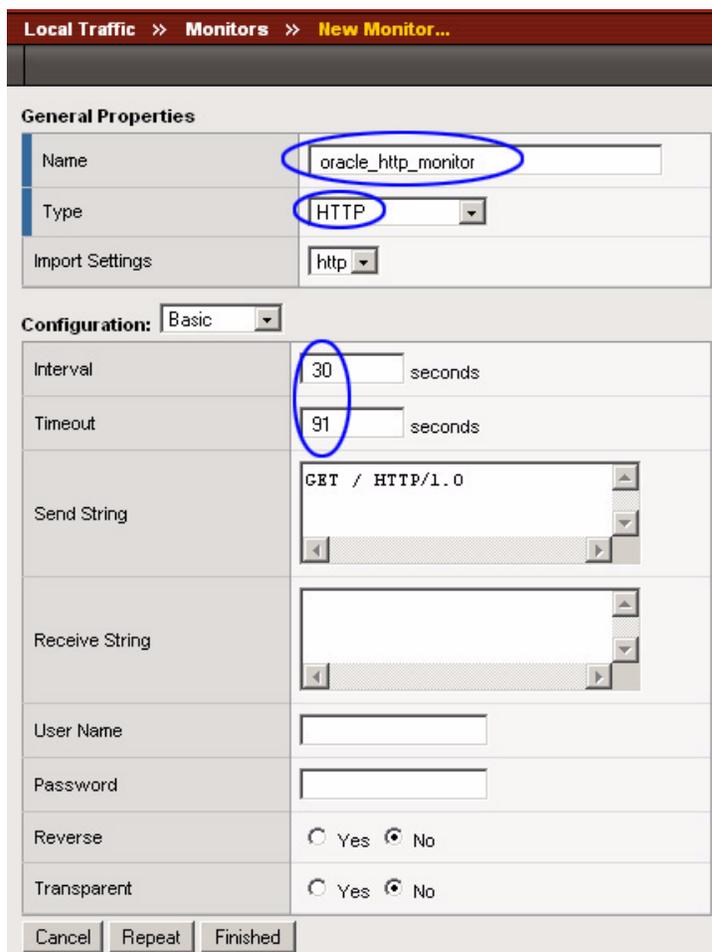   *GET /www/support/customer_info_form.html HTTP/1.0*

Figure 1.2 Creating the HTTP Monitor

7. Click the **Finished** button.
    The new monitor is added to the Monitor list.

Creating the pool

The first procedure in this configuration is to configure a pool for the Oracle devices. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this Deployment Guide, we configure one pool for our Oracle devices.

To create the application server pool from the Configuration utility

1. On the Main tab, expand **Local Traffic**.

2. Click **Pools**.
   The Pool screen opens.

3. In the upper right portion of the screen, click the **Create** button.
   The New Pool screen opens.

   *Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.*

4. In the **Name** box, enter a name for your pool.
   In our example, we use **oracle_http**.

5. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the HTTP health monitor* section, and click the Add (**<<**) button. In our example, we select **oracle_http_monitor**.

6. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
   In our example, we select **Predictive (member)**.

7. In this pool, we leave the Priority Group Activation **Disabled**.

8. In the New Members section, make sure the **New Address** option button is selected.

9. In the **Address** box, add the first server to the pool. In our example, we type **150.150.150.7**.

10. In the **Service Port** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list.
    In our example, we type **8000**.

11. Click the **Add** button to add the member to the list.

12. Repeat steps 9-11 for each server you want to add to the pool.
    In our example, we repeat these steps three times for the remaining servers, **150.150.150.8** and **.9** (see Figure1.3).
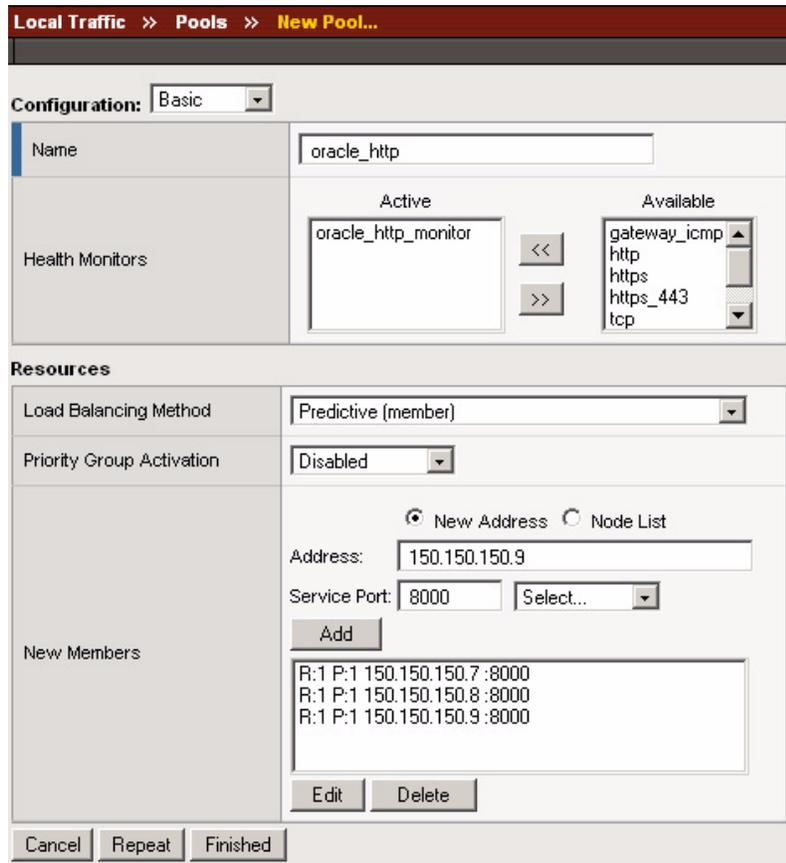
13. Click the **Finished** button.

Figure 1.3 *Adding the oracle_http pool*

Adding an ICMP monitor

We recommend that in addition to the HTTP monitor, you also add a simple ICMP monitor to the Oracle nodes. An ICMP type of monitor simply determines whether the status of a node is up or down. In the following procedure, we should you how to create default ICMP monitor.

To create an ICMP monitor

1. On the Main tab, expand **Local Traffic**.

2. Click **Nodes**.
   The Node screen opens showing all currently configured nodes.

3. On the Menu bar, click **Default Monitor**.
   The Default Monitor screen opens.

4. From the Available list, select **icmp**, and click the Add (**<<**) button to add it to the Active list (see Figure 1.4).
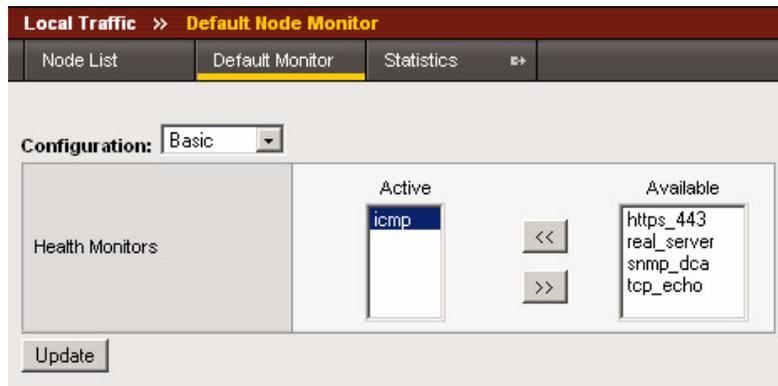
5. Click the **Update** button.

Figure 1.4 *Adding a default ICMP monitor*

◆ **Tip**

*If you do not want the ICMP check to monitor all of your nodes, you can remove the monitor from specific nodes. To remove the monitor: From the Nodes screen click the Address of the nodes you do not want to monitor with the ICMP check, and from the **Health Monitors** list, select **None**, then click the **Update** button.*

Creating a profile

BIG-IP version 9.0 and later use profiles. A *profile* is an object that contains user-configurable settings, with default values, for controlling the behavior of a particular type of network traffic, such as HTTP connections. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

In our example, you create an HTTP profile. If your Oracle E-Business Suite 11i deployment requires SSL, you also need to create an SSL profile.

Creating an HTTP profile

For most Oracle deployments using HTTP, you could simply use the default HTTP profile. However, we recommend you create a new profile based on the HTTP profile, so in the future, if you need to change any of the profile settings, you do not overwrite the default profile by mistake. Before you

start creating this profile, you can view the settings for the default HTTP profile to see if it is applicable for your network (From the Local Traffic menu, click **Profiles**, then click **HTTP**).

To create a new HTTP profile based on the default HTTP profile

1. On the Main tab, expand **Local Traffic**.

2. Click **Profiles**.
   The HTTP Profiles screen opens.

3. In the upper right portion of the screen, click the **Create** button.
   The New HTTP Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **oracle_http_profile**.

5. Modify any of the settings as applicable for your network.

6. Click the **Finished** button.

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

Creating a SSL profile

If your Oracle deployment uses SSL, you also need to create an SSL profile. Before creating the SSL profile on the BIG-IP system, you must have a certificate/key pair issued by a recognized certificate authority. The applet used by Oracle 11i does not work with the BIG-IP device's self-signed certificates. For information on installing a key/certificate pair on the BIG-IP device, see the ***BIG Configuration Guide for Local Traffic Management***, Chapter 7, *Managing SSL Traffic*.

◆ **Important**

*To prepare your Oracle 11i deployment for load balancing SSL, you must follow the procedures outlined in Option 2.2, **HTTP Layer Hardware Load Balancing**, of the following Oracle MetaLink document: **http://metalink.oracle.com/metalink/plsql/ml2_documents.showFrameDoc ument?p_database_id=NOT&p_id=217368.1***
Specifically, option 2.2.3 contains steps relevant to the SSL accelerator.

◆ **Note**

If you are not using SSL in your deployment, you do not need to perform this procedure.

To create a new SSL profile based on the default SSL profile

1. On the Main tab, expand **Local Traffic**.

2. Click **Profiles**.
   The HTTP Profiles screen opens.

3. From the Menu bar's **SSL** menu, select **Client**.
   The Client SSL Profiles screen opens.

4. In the upper right portion of the screen, click the **Create** button.
   The New Client SSL Profile screen opens.

5. In the **Name** box, type a name for this profile. In our example, we type **oracle_https_profile**.

6. In the Configuration section, click a check in the **Custom** boxes for **Certificate** and **Key**, and select the appropriate certificate and key from the list.

   *Important: You must already have installed an SSL certificate and Key pair issued by a recognized certificate authority. If you do not have an SSL certificate and key, you must obtain one, and then refer to the **BIG Configuration Guide for Local Traffic Management** guide for installation instructions.*

7. Modify any of the settings as applicable for your network.

8. Click the **Finished** button.

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

Creating the virtual server

The next step in this configuration is to define a virtual server that references the profile and pool you created. For this virtual server, we use the Cookie Persistence profile, which is cookie persistence, insert mode, the recommended persistence method for Oracle E-Business Suite.

To create the HTTP virtual server using the Configuration utility

1. On the Main tab, expand **Local Traffic**.

2. Click **Virtual Servers**.
   The Virtual Server screen opens.

3. In the upper right portion of the screen, click the **Create** button.
   The New Virtual Server screen opens.

4. In the **Name** box, type a name for this virtual server. In our example, we type **oracle_http_vs**.
   If your Oracle deployment uses SSL, and you created an SSL profile in the preceding procedure, type **oracle_ssl_vs**.

5. In the **Destination** section, select the **Host** option button.

6. In the **Address** box, type the IP address of this virtual server. In our example, we use **192.168.200.10**.

7. In the **Service Port** box, there are two options depending on your configuration:

a) If you are using the standard configuration, and created an HTTP profile in the preceding procedure; in the **Service Port** section, type **80**, or select **HTTP** from the list.

Figure 1.5 *Adding an HTTP virtual server*

b) If your Oracle deployment uses SSL, and you created an SSL profile in the preceding procedure; in the **Service Port** section, type **443**, or select **HTTP** from the list.

Figure 1.6 *Adding an SSL virtual server*

8. In the Configuration section, leave the **Type** list at the default setting: **Standard**.
*Note: For more (optional) virtual server configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.*

9. In the **HTTP Profile** section, select the profile you created in the *Creating an HTTP profile* section. In our example, we select **oracle_http_profile** from the list.

Figure 1.7 *Selecting the HTTP profile for the virtual server*

If your Oracle deployment uses SSL, and you created an SSL profile; in the **SSL Profile** section, select the profile you created in the *Creating a SSL profile* section. In our example, we select **oracle_ssl_profile.**

Figure 1.8 *Selecting the SSL profile for the virtual server*

10. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **oracle_http**.

11. From the **Default Persistence Profile** list, select **cookie**.
This sets the persistence method to cookie persistence, Insert mode, where the cookie expires at the end of the session. If want to modify the default settings, including a specific expiration for the cookie, create a new persistence profile, based on the cookie profile.

Figure 1.9 Resources section of the add virtual server page

12. Click the **Finished** button.

Synchronizing the BIG-IP configuration if using a redundant system

If you are using a redundant BIG-IP configuration, the final step is to synchronize the configuration to the peer BIG-IP device.

To synchronize the configuration using the Configuration utility

1. On the Main tab, expand **System**.

2. Click **High Availability**.
The Redundancy screen opens.

3. On the Menu bar, click **ConfigSync**.

4. Click the **Self --> Peer** button.
The configuration synchronizes with its peer.

Appendix A: Backing up and restoring the BIG-IP system configuration

We recommend saving your BIG-IP configuration before you begin this configuration. When you save the BIG-IP configuration, it collects the following critical data and compress it into a single User Configuration Set (UCS) file:

- BIG-IP configuration files

- BIG-IP license and passwords

- SSL certificates

- SSH keys

Saving up and restoring the BIG-IP configuration

The Configuration Management screen allows you to save and restore all configuration files that you may edit to configure a BIG-IP system. These configuration files are called a User Configuration Set (UCS). The Configuration Management screen contains sections for saving and restoring a configuration. The list boxes in these sections display only files in the **/usr/local/ucs** directory. If you want to save or restore files from another directory, you must type the full path in the box.

To save the BIG-IP configuration using the Configuration utility

1. In the navigation pane, click **System Admin**.
    The User Administration screen displays.

2. Click the Configuration Management tab.
    The Configuration Management screen displays.

3. In the **Save Current Configuration** section, type the path where you want your configuration file saved or choose a path from the list box. If no path is specified, the BIG-IP saves files to **/usr/local/ucs**. The BIG-IP appends the extension.ucs to file names without it. In our example, we type **pre_oracle_backup.ucs.**

4. Click the **Save** button to save the configuration file.

To restore a BIG-IP configuration

1. In the navigation pane, click **System Admin**.
    The User Administration screen displays.

2. Click the Configuration Management tab.
    The Configuration Management screen displays.

3. In the **Restore a Configuration** section, choose the configuration file you want to restore from the list box, or type the path where your configuration files were saved.

4. Click the **Restore** button.
   To check the status of the restoration, click the **View Log** button. You should wait a few moments for the log file to start generating before you click **View Log**. Repeated clicking of this button will update your screen with the most current log file information until the restoration is complete.