Oracle Net Listener
Connection Rate Limiter

An Oracle White Paper
October 2007

ORACLE®

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Introduction

The Oracle Network Listener is the first point of contact for any client connection to the database. The Listener brokers client requests, handing them off to appropriate database servers. In a typical server configuration, the Listener is the only entity listening for client connection requests, and thus is the first line of defense against Denial-of-Service attacks. This paper describes a new feature in the Listener – Connection Rate Limiter – which allows a DBA to specify limits on the number of new connections handled by the listener. This throttling allows a database server system to better handle sudden spikes in connection requests.

Logon Storms

A Logon storm is a sudden spike in the number of client connection requests. Logon storms can occur due to a variety of factors. They could be malicious like a DoS attack. Or they could occur due to administrative actions – such as a middle tier coming online.

The process of starting a database session has inherent CPU costs associated with it - from the creation of a new OS process to attaching to the SGA. Every system has a limit above which the spawning of new database sessions can starve existing sessions of CPU resources. This could result in many unexpected consequences including application timeouts, increased response times, un-responsiveness and other cascading effects.

The Solution

The Listener, in 11g, supports throttling of incoming connections. With the Connection Rate Limiter feature, a DBA can specify limits on the number of new connections handled by the listener. When a limit is specified, the Listener imposes an artificial limit on the number of new connections it handles every second. This slows down the rate of database session creation, which lowers the the amount of CPU resources used for servicing incoming connections.

This feature is enabled by using the two listener.ora parameters described below.

CONNECTION_RATE_<LISTENER_NAME>

> This parameter specifies a global rate that is enforced across all listening endpoints that are rate limited. This parameter should be set to a positive integer indicating the number of connections that the listener should handle per second.

RATE_LIMIT

> This parameter indicates that a particular listening endpoint is rate limited. This is specified in the ADDRESS section of the listener endpoint configuration. For example,

```
LISTENER=(ADDRESS=

            (PROTOCOL=tcp)

            (HOST=sales-server)(PORT=1521)

            (RATE_LIMIT=yes))
```

> This parameter can be configured in two ways:
>
> 1. When the parameter is set to "yes", the endpoint is included in the enforcement of a listener-wide connection rate. This has to be used in conjunction with the CONNECTION_RATE_LISTENER parameter.
>
> 2. When a value greater than 0 is specified, the rate limit is enforced at the endpoint level.

This flexibility in configuration allows endpoints used for listener administration and database service registration to be unregulated, while throttling the client connection endpoints. The rate limit to be specified is system dependent, and will vary with machine configuration, system load and other factors. Please refer to the Net Reference Guide for more information.

Analysis

To illustrate the benefits of rate limiting the Listener, the results of a simple experiment are shown below.

An Oracle 11g single instance database was setup in a dedicated server configuration. 150 simultaneous SQL*Plus connections were initiated from a different host. The total (system + user) CPU utilization and the number of database sessions were plotted against time.

The experiment was conduced with two configurations – one with the connection rate limiter enabled, and one without. Database and host activity was kept to the minimum to illustrate the impact of session creation on CPU usage.
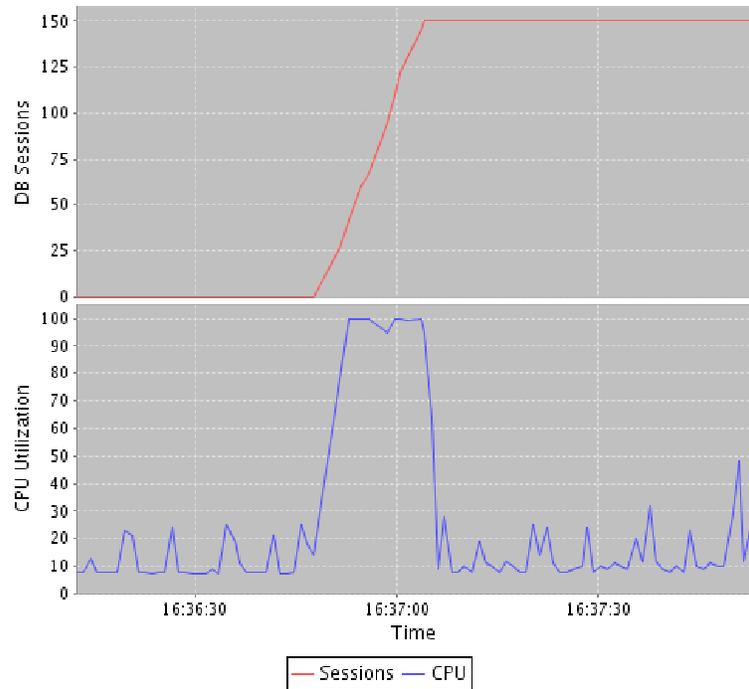
The figure above shows the impact of creating 150 sessions without the connection rate limiter feature. CPU utilization (system + user) is pegged at 100% for the duration of session creation. Depending on the load on the system, existing processes may be starved of CPU during this period.
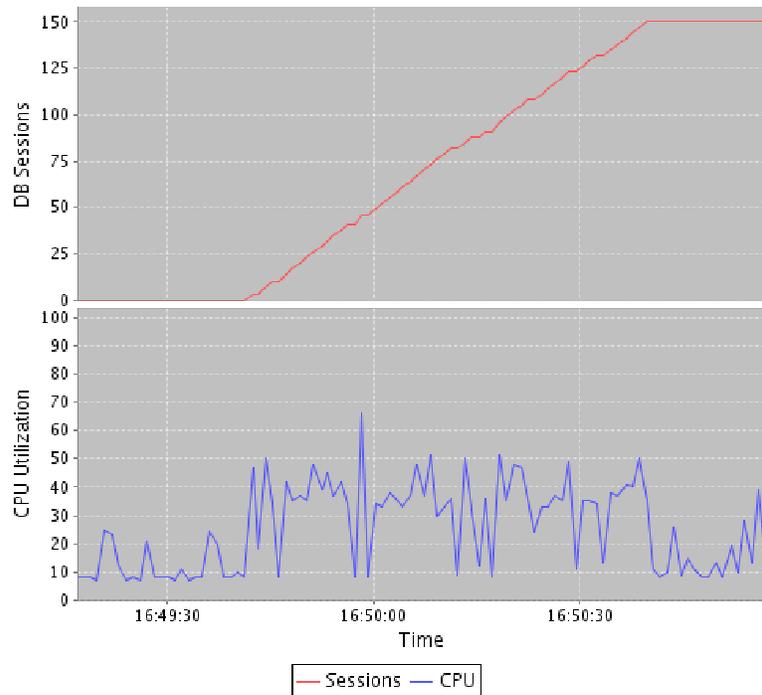
The second figure above shows the impact of enabling the Rate Limiter feature. A limit of 3 connections a second was imposed on the listener. As seen from the graph, the number of DB sessions increases linearly. The CPU utilization hovers around 50% during the session creation period. This leaves spare CPU cycles for other processes to use.

Conclusion

The Connection Rate Limiter can be an effective tool in maintaining Quality –of-Service guarantees during logon storms. With a suitable rate limit value, the Listener can mitigate some of the negative effects of a DoS attack no penalty under normal operating conditions.

ORACLE

Oracle Net Listener Connection Rate Limiter
October 2007
Author: Karthik Rajan

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com