

Preventing Denial-of-Service Attacks

This article describes the preventing Denial-of-Service attacks feature of IBM® Informix® Dynamic Server (IDS) beginning with version 10.

What is Denial-of-Service attacks ?

Denial of service (DoS) attacks denies service to valid users trying to access the database. For example, an attacker might flood your database server with requests, rendering your database server temporarily unavailable or unusable. Denial of service attacks are problematic because they are easy to achieve and can be anonymous. Dynamic Server provides multiple listener threads available to handle connections and imposes limits on the availability of the listener VP for incomplete connections.

What it does ?

This feature reduces the risk of a hostile Denial-of-Service attack by making it more difficult to overwhelm the listener VP that handles connections.

How to use it ?

Dynamic Server introduces two new configuration parameters to prevent Denial-of-Service attacks. You can customize this feature with the following two new configuration parameters:

- **LISTEN_TIMEOUT** - Sets the incomplete connection timeout period
- **MAX_INCOMPLETE_CONNECTIONS** - Restricts the number of incomplete requests for connections

LISTEN_TIMEOUT specifies the number of seconds the server waits for a connection. It can be set to a lower number to guard against faulty connection requests that might indicate a Denial of Service attack. The default incomplete connection timeout period is reduced from 60 to 10 seconds.

MAX_INCOMPLETE_CONNECTIONS specifies the maximum number of incomplete connections in a session. After this number is reached, an error message is written in the online message log stating that the server might be under a Denial of Service attack. The default maximum number of incomplete connections is 1024.

Depending on the machine capability of holding the threads (in number), you can configure **MAX_INCOMPLETE_CONNECTIONS** to a higher value and depending on the network traffic, you can set **LISTEN_TIMEOUT** to a lower value to reduce the chance that an attack can reach the maximum limit. Both the **LISTEN_TIMEOUT** and the **MAX_INCOMPLETE_CONNECTIONS** configuration parameters can be changed using the **onmode -wf** option or superseded for a session with the **onmode -wm** option.