PlanetLab Acceptable Use Policy (AUP)

PlanetLab Consortium

February 6, 2004

PlanetLab is an overlay testbed designed to allow researchers to experiment with network applications and services that benefit from distribution across a wide geographic area. All uses of PlanetLab should be consistent with this high-level goal.

Guidelines

As an overlay, PlanetLab is not a "testbed" in the usual sense of a controlled environment for experiments. It consists of computational resources hosted by organizations (principally research organizations like Universities) that donate their own time, rack-space, and network connectivity for the good of the community. Running an experiment on PlanetLab is fundamentally different from running it in a LAN-based lab or on an isolated wide-area testbed.

A good litmus test when considering whether an experiment is appropriate for PlanetLab is to ask what the network administrator at your organization would say about the experiment running on your local site. If the experiment disrupts local activity (e.g., uses more than its share of your site's Internet bandwidth) or triggers complaints from remote network administrators (e.g., performs systematic port scans), then it is not appropriate for PlanetLab. It is your responsibility to ensure that your use of PlanetLab falls within these constraints. This means you should debug your code in a controlled environment so you have confidence that you understand its behavior.

PlanetLab is also designed to allow experimental services to run continuously, thereby supporting an end-user community. As a consequence, PlanetLab could indirectly support users that have not officially registered with PlanetLab, and may even be unknown to you (the service provider). It is your responsibility to ensure that your users do not cause your service to violate the terms of this AUP. In particular, service providers should ensure that their users are not able to hijack the service and use it to attack or spam other nodes or network users.

PlanetLab is designed to support network measurement experiments that purposely probe the Internet. However, we expect all users to adhere to widely-accepted standards of network etiquette in an effort to minimize complaints from network administrators. Activities that have been interpretted as worm and denial-of-service attacks in the past (and should be avoided) include sending SYN packets to port 80 on random machines, probing random IP addresses, repeatedly pinging routers, overloading bottleneck links with measurement traffic, and probing a single target machine from many PlanetLab nodes.

It is likely that individual sites that host PlanetLab nodes will have their own AUPs. Users should not knowingly violate such local AUPs. Conflicts between site AUPs and PlanetLab's stated goal of supporting research into wide-area networks should be brought to the attention of PlanetLab administrators. The expectations placed on sites that host PlanetLab nodes are described in a companion document: *Hosting a PlanetLab Node*.

While the central PlanetLab authority is often the first point-of-contact for complaints about misbehaving services, it is our policy to put the complainant in direct contact with the researcher that is responsible for the service.

PlanetLab provides absolultely no privacy guarantees with regard to packets sent to/from slices. In fact, users should assume packets will be monitored and logged, for example, to allow other users to investigate abuse (see previous paragraph).

PlanetLab also does not provide any guarantees with respect to the reliability of individual nodes, which may be rebooted or reinstalled any time. Reinstalling a node implies that the disk is wiped, meaning that users should not treat the local disk as a persistent form of storage.

Overall Rules

- PlanetLab should not be used for any illegal or commercial activities. Use for research and educational purposes is allowed.

Node Usage Rules

- Use existing security mechanisms. For example, all access to PlanetLab nodes must be via SSH.
- Do not circumvent accounting and auditing mechanisms. This means you must associate your identity with the PlanetLab slice (account) in which your service runs, and you must not do anything to obfuscate the audit trail.
- No hacking attempts of the PlanetLab nodes. This includes "red team" (hacker test) experiments. All access is non-root.
- Avoid spin-wait for extended periods of time. If possible, do not spin-wait at all.

Network Usage Rules

- Do not use your PlanetLab slice (account) to gain access to any hosting site resources that you did not already have.
- Do not use one or more PlanetLab nodes to flood a site with so much traffic as to interfere with its normal operation. Use congestion controlled flows for large transfers.
- Do not do systematic or random port or address block scans. Do not spoof or sniff traffic.

Consequences

Violation of this AUP may result in any of the following:

- disabling the slice (account);
- removing the site from PlanetLab;
- informing the organization's administration.