Guidelines for Hosting an OSN Pod

This note outlines the steps that a site needs to take in order to host an OSN Pod. The intention is to make pod hosting as simple and hands-off as possible, so that sites can focus on making productive use of the OSN as a distributed storage system. Feedback on how to improve any part of the process is welcomed.

There are six principal areas to consider when preparing to host a pod.

Cost and staffing considerations – We can work with you to find funding. Since hardware is often funded by capital grants, we have worked hard to keep the staff and facility commitments light.

Network access – Since the OSN depends on high bandwidth connectivity between pods, every site must have a path to Internet2. Pods are located in Science DMZs in order to avoid firewall bandwidth constraints and to simplify site-level security considerations. Access at 100gbps is preferred, but sites may participate with 40gbps or 10gbps connections.

Software installation and maintenance – OSN pods are centrally monitored and provisioned, so that software installation and maintenance can be hands-off in all but a few circumstances.

Hardware installation and maintenance – OSN pods are designed to accommodate a variety of physical environments while ensuring enough uniformity to enable efficient operation at a scale of hundreds of sites. Since the OSN is a distributed system, it can tolerate some downtime at each individual site.

Security – The OSN follows guidelines established by the Trusted CI Center of Excellence. We have designed the pod software and hardware to allow for a modest set of site-level security requirements, principally in the areas of network configuration and physical access.

Participation in governance and devops – We welcome participation in either governance or devops, but it is not required if you prefer to treat the OSN pod as an appliance, and focus on making productive use of the OSN as a whole.

Cost and Staffing Considerations

A Pod site must be capable of covering the cost of participating in the OSN. Any source of support is acceptable, as long as it does not impose requirements that conflict with OSN policies and practices. As noted earlier, we can work with you to find funding.

Costs that need to be covered are:

- Pod hardware cost, following the current revision of the specification
  We strongly recommend bundling a five year warranty with the purchase to cover replacement of failed components and on-site service when needed.
- Space, power, and cooling for pod equipment
- Access to Internet 2, including network access fees.
- Ability to pay ongoing software licensing fees, if any (e.g. Lastpass)
- Staffing for the roles described below

Pod hardware monitoring is managed centrally, so we are able to notify you when hardware issues occur.

Pod hardware will cost approximately $90K, and local staffing needs should not exceed two person-weeks of effort per year after the installation is complete. Space, Power, Cooling, and Network Access costs will vary depending on local conditions, and can be determined from the information provided in the network access and Hardware Installation and Maintenance sections below.

To allow for efficient capacity planning, a Pod site must be willing to commit to at least two years of participation in the OSN, starting from the date on which its pod goes live. Except under extraordinary circumstances such as natural disasters, sites must provide at least 6 months notice before starting to offload data and deactivate a pod.

Staffing

A site must be able to fill the following roles. When appropriate, a single person may fill two or more of these roles. These roles pertain to administration of pods only. Data sets are administered separately.

Principal Investigator - Responsible for the overall relationship between the site and the OSN, including ensuring that all roles are staffed, and arrangements for space/power/cooling and network access are in place.

Site Operations Liaison - The point of contact for software and hardware maintenance operations that require physical presence, including replacement of failed hardware when detected by OSN monitoring, and Troubleshooting of network access or performance problems when detected by OSN monitoring.

Primary and Secondary Security Point of Contact - The point of contact for OSN-related security questions, updates and issues, and for response in the event that site-level action is needed to mitigate a security incident.

Network Access

An OSN site must have a path to Internet2, with primary and backup routes available on all segments of the path. Access at 100gbps is preferred, but sites may participate with 40gbps or 10gbps connections. The OSN Pod must reside outside the site's firewall, preferably in a recognized science DMZ.

Each OSN pod needs a /28 public IP address block for end user access plus three public IP host addresses for monitoring and provisioning.

Software Installation and Maintenance

Pod software provisioning, monitoring, and maintenance are managed centrally, so that on-site system administration is only needed to: (1) initiate a bare metal reboot (e.g. when the system is first installed); or (2) run a diagnostic that can only be run locally.

Hardware Installation and Maintenance

To minimize hardware installation and maintenance effort, an OSN pod is delivered as a fully configured rack.

Availability – The OSN is designed to provide high availability without imposing unnecessarily high costs on any single site. Since the OSN is a distributed system, it can tolerate some downtime at each individual site. UPS and generator backed power are therefore preferred, but not required. Facility design and operation for pod sites are expected to support less than 24 hours of planned downtime and less than 12 hours of unplanned downtime per year.

Space – An OSN pod consists of three servers, a JBOD, and cables that interconnect them. The hardware fits in 7U (12.25 inches) of rack space. The JBOD is 1139 mm (44.8") deep.

Power and cooling – An OSN pod is air cooled, with peak power consumption of approximately 3.5KW. Each of the three servers connects to two C13 outlets for redundant power. The JBOD connects to two C19 outlets for redundant power.

Security

The OSN follows guidelines from the Trusted CI Center of Excellence. Since software and storage provisioning, management, and monitoring are handled centrally, site security requirements are driven primarily by physical security considerations:

- Pod cabinets must be locked, with keys available to named individuals only.
- All physical access to a pod must be logged.
- The physical configuration of the pod equipment must not be changed unless it is done in cooperation with the OSN.
- Local staff has completed relevant institutional requirements for cybersecurity training.

As noted above, each site must have a primary and secondary point of contact for security.

Participation in Governance and Devops

A site may choose to become an active participant in OSN governance and/or devops but it is not required to do so. If this is of interest, please let us know and we can discuss both your interests and possible sources of support.