The following is what I have worked with over the years and sums up the main systems, services and tools that I have used. As a Linux/Unix administrator, I have a good and wide knowledge of the ecosystem, so this is far from a complete list, but rather an example to give a view of my work experience and knowledge in the field.

Server knowledge:

- Linux and Unix server administration, security and hardening, server ecosystem design etc. (RHEL, Ubuntu Server, Solaris and *BSD mainly, plus many other distros) This includes infrastructure design, maintenance, upgrades, obsoletion and migrations and autonomous deployment, either with containers, VMWare, Proxmox or pure hardware servers and/or clusters.
- Microsoft Server and Active Directory management, group policies and pool management, upgrades and patch deliveries along with device management.
- Setup of Testing, Development, Staging and Production environments for all aforementioned systems.

Networking:

- Cisco routers, switches, ASA and PIX. Core network management, localnet, intranet and customer asset management.
- Virtual network interfaces, bridges and vlan tagging on Linux, Unix and Windows Server
- IPTABLES firewall management
- UFW firewall management

Note: Networking is not my focus at work anymore, and it's been a few years since I was networking properly.

Service knowledge:

- DNS setup, maintenance and deployment with either Named/Bind, systemd resolve, local host management on *nix systems and Windows AD zone management.
- NFS and various other network storage solutions, disk management with multipath, file system pools on both LVM and ZFS f.ex.
- DHCP services in various forms, either on routers or on servers.
- Webeservers, Apache and Nginx, either to serve content and or proxypassing services and load balancing and serving content from JBoss/Tomcat/Glassfish engines.
- Mysql/Mariadb and MSSQL server management along with support for Oracle Enterprise Business Suite, deployment of SQL servers and clusters.
- Nagios monitoring, global ecosystem wise, everything from servers to services, mounts, ports, files, databases, connections and system resources plus so much more that can, could and should be monitored.
- ELK stack (Elasticsearch/Logstash/Kibana) setup and usage alongside data/logging management from various sources.
- Graylog and Syslog/Syslog-ng, both centralized and local with log analytics.

- Ansible/Puppet centralized management of various assets, services, users, files and deployment.
- MRTG graphs of various sources, for example for monitoring of network traffic set up in Cacti, Nagios or Snort.
- GIT versioning systems, f.e locally hosted Gitlab for development teams and administrators.
- CI/CD testing and deployment pipelines with Gitlab, Github and Jenkins f.e.
- Certificate management, f.e locally with certbot as a standalone or with Let's Encrypt ACME or other official CA.

CLI and scripting/programming knowledge:

- Shell scripting in bash/sh/zsh for system tasks, maintenance and administrative tasks.
- HTML and CSS for interfaces, structure and look.
- Python scripting/programming to some level of extent, mainly backend and CLI.
- PHP scripting/programming to some level of extent, both frontend and backend.
- Pearl scripting/programming to some level of extent, for CLI.

Note: I am by no means a programmer, but I can script/program to finish the task at hand and I can both read, understand and change already written code.
Here is my personal open GitHub repo for reference: https://github.com/eddinn

Standards:

- ISO 27001 - Information Security Management (Working by and implementation on servers, user control and other assets).
- ISO 9001 Quality Management (Working by and implementation).

I hope this is sufficient and please feel free to contact me if you need any further information.

-Edvin Dunaway