

Karl Vogel

Address - 3154 Kerry Dr. Beaver creek, OH 45434	Email - vogelke@pobox.com
Phone - H:937-429-8812 C:937-241-9868	References on request

Work History and Security Clearance:

- Dec 1986 - Present: Programmer & System Administrator (contractor). Operate and maintain several Unix servers at the Mobility Directorate, Wright Patterson AFB, OH. Current clearance is Secret.
- Sep 1981 - Apr 1986: Applications Programmer, Foreign Technology Division (now NASIC) while serving as an officer at WPAFB. Had TS/SCI clearance.

Hardware Experience:

- Sun E450, V890, and M3000 servers running Solaris v2.5.1 - 10.
- IBM x3400 servers running BSD Unix and Red Hat Enterprise Linux.
- Workstations running Solaris-11.1, RHEL-6.x, FreeBSD, OpenBSD.

Security Experience:

- I can write, deploy, and troubleshoot SELinux policies.
- I have a mostly-automated setup for checking system logs for anomalies -- occasionally I modify the checks to weed out false alarms. You can see a description here: <https://bezoar.hcst.net/src/logfiles/>

Software Experience:

- Operating Systems: Linux, Solaris, BSD Unix (FreeBSD and OpenBSD), IBM MVS.
- Languages: C, Fortran, Perl, XML, PostScript.
- Web: HTML, CSS Bootstrap, CSS Grid, CGI.
- CI/CD: I have experience building from source on Linux, BSD, and Solaris.
- DBMS: Built SQLite and Postgres databases from source and installed for use with a filename DB; some scripting experience with Oracle (dumping the database, extracting fields for web programming).

Professional Awards:

- 1999: Award from BrigGen Johnson for Y2K prep work.
- 2000: C-17 System Program Office Team of the Quarter
- 2002: Certificate of Appreciation from Colonel Owen, Directorate commander.
- 2008: 516th Aeronautical Systems Wing Team of the Quarter
- 2012: Recognized by Commander of 88th Comm Group and Deputy Director of Mobility Directorate for finding suspicious access attempts on one of our servers.

Network Experience:

- SMTP (Mail transport protocol).
- TCP/IP setup and troubleshooting.
- Minor NETBIOS troubleshooting when using Samba software to provide MS Windows file-sharing from Unix servers.

Certificates:

- Security+ 2011

Education:

- Courses in Software Engineering and Digital Signals Processing at Air Force Institute of Technology.
- BS, Mechanical & Aerospace Engineering, Cornell University.

Best Qualities:

- I pay attention to detail, and I document what I do.
- I take responsibility for my skills. My head belongs to me, and the contents thereof are my problem. 95% of my admin and coding skills are self-taught. I bought over 200 books on everything from Ansible to ZSH -- they're in my office.
- I know how to munge -- turn semi-structured data into something useful. If you have information in an inconvenient format and want to extract some of it into a CSV or JSON file, I'd be very surprised if I couldn't write a script to do it. I prefer perl; it's not fancy, but it's currently maintained and reliable.
- I'll write something that's needed without having to be told. I created a local dataset which was updated whenever I added or removed a user. This way, I knew when the account was added or removed, what groups the user is supposed to be in, any notes for special requirements, etc. This was handy for the occasional question about when someone actually came on-board, who approved their access to a given share, etc. I also wrote scripts which used the servers to check the computer-room temperature at 10-minute intervals, and send me an IM if they go more than 8-10 degrees past their normal level (i.e., AC failure).
- I generally like answering questions from users, and I can turn a vague request into something actionable. When we ran our own file-servers, sometimes I'd get an email that wasn't very specific, like "I need access to the G drive". This requires poking around in other files -- we keep records of when users login listing the drives they have available -- so I could figure out what they needed without requesting more information.
- I like writing short tutorials or howto's for things like backups, security, or shortcuts on Unix systems. See <https://www.reddit.com/user/vogelke/> for examples -- I contribute to the sysadmin and linux lists. I can also show sanitized examples of system site-logs which hold soup-to-nuts descriptions of sizing, installation, and trouble-shooting servers.
- I don't mind coming in at odd hours if there's a legitimate emergency. We had a building-wide power/AC failure over the weekend of July 11-12, 2009. I got network and temperature warning text messages from 5 hosts at 11:50 pm on the 11th, which allowed me to come in and shut servers off before they suffered any heat damage or used up the UPS batteries. I've also had to come in after 3am and call Civil Engineering because a building switch failed.

Additional Experience:

- I've run STIG OS checks on Solaris and Linux servers for several years. All systems now run at level GREEN (90% plus compliance).
- Configured and installed bare-metal servers running Linux, BSD, and Solaris. Installed a 750-Gbyte fileserver plus an equal-sized backup server for the C-130, C-5, and KC-767 wing users using Dell desktop workstations plus enterprise-class drives.

These boxes used Samba plus the Base domain-controllers for logins -- this allowed UNIX servers to act like Windows file-servers. These boxes ran around-the-clock from March 2004 through May

2011. I always installed Samba from source, which let me add audit capabilities to automatically track which users have modified which files.

- Administered e-mail system before the base moved to Exchange; maintained user accounts and system distribution lists. I have experience with three common mail-transport programs used by Unix systems: sendmail, postfix, and qmail. Our main Sun server ran qmail and postfix instead of sendmail since around 2001, allowing us to avoid many security patches.
- Performed hourly backups and daily file-integrity checks, and restored files from backups as required. Installed an identical server for storing backups in a separate location, which made things much safer. We still have incremental backups that are over 10 years old. These came in handy while defending the Mobility Directorate from a lawsuit; I was deposed by the opposition about our backup practices.
- Maintained the Directorate web server:
 1. Added several form-based surveys for things like quality of work environment.
 2. Installed a file-manager for external Boeing users which allowed them to safely upload and download files via HTTPS, create folders, etc.
 3. Local users could take quarterly security training via the web. The weblogs made sure that users actually looked at every slide; this was one of the limitations of simply mailing a PowerPoint presentation to everyone. A separate webpage listed the current completion statistics for everyone in the Wing, telling the security office who completed the briefing, who started it, and who ignored it. We caught several people who would read the first and last pages of the briefing and then complain that they didn't get credit.
 4. Wrote a conference-room scheduler which was in use by the C-17 SPO for about 5 years. It allowed reservations for up to a year in advance, automatically-recurring reservations, bump privileges for certain groups in certain rooms, checks against double-booking, and automatic notification of MIS personnel in case video-teleconferencing assistance was needed. User feedback indicated that this program was easier to use than its replacement (Outlook).
 5. Wrote a form which allowed people to send comments or suggestions to the Wing executive officer. This was done to ensure confidentiality, which is not possible with email.
- Installed packet filters on 4 production Unix servers to implement some firewall-like protections. The software used was "iptables" for Linux and "ipf" for Solaris.
- At one time, I managed seven servers, some of which were production file/db servers and some of which are replacement/upgrade boxes to which we're migrating. These boxes run Solaris 10/11.1 and Linux. I've been using Solaris since 1994, and BSD/Linux since 2004.

Older servers:

1. Main server (Sun V890): 534 Gbytes, about 1.7 million files
2. Main backup (Supermicro): 3 Tbytes, about 9.3 million files
3. Secondary server (IBM x3400): 2.8 Tbytes, 1.5 million files
4. Secondary backup (IBM x3400): 2.8 Tbytes, 1.5 million files

Current servers:

1. Main server (NexServ 1U rack) 6.5 Tbytes, about 5.3 million files
 2. Main backup (NexServ 1U rack) 5.5 Tbytes, about 17 million files
 3. Oracle server (HP 240Z) 150 Gbytes, about 960,000 files
- I update OpenSSH (secure network connection), OpenSSL (secure web connection), Apache (webserver), and sudo (selectively grant operator privileges) software on all production hosts when

security fixes come out. I always build from signed sources because the vendor releases are almost guaranteed to be out of date. The C-17/Mobility webserver ran under Apache on our main Sun server for several years before that functionality was taken over by the base.

- Installed a logserver to archive logfiles from my workstation and all other Unix servers. This was useful when we had to look up, say, web or FTP access requests from a year ago on one particular server. I have records going back to 2001 for some hosts; total log size is approximately 54 Gbytes. The logserver also pinged all production hosts once per minute, and sent me an IM if any of my hosts lost connectivity for 3 consecutive minutes. This made it easy to create graphs showing system uptime.

Publications:

- Thu, 1 Aug 1991
Article: A source code generator for C
Dr. Dobb's Journal Vol 16 No 8, ISSN 1044-789X
Karl Vogel, Control Data Corporation.
<http://www.ddj.com/documents/s=3D1059/ddj9108b/9108b.html>

An extensible, language-independent code generator that writes the outline of a program before dropping you into the editor of your choice.

- Thu, 1 Dec 1994
Mentioned in: Exploring Expect (Nutshell Handbook) by Don Libes
Publisher: O'Reilly Media, Inc.; 1st edition (1 Dec 1994) 602 pages
ISBN: 1565920902
- Mon, 24 May 2004
Contributed to: BSD Hacks (Paperback) by Dru Lavigne
Publisher: O'Reilly Media, Inc.; 1st edition, 448 pages
ISBN: 0596006799
- Thu, 15 Dec 2005
Article: Organizing my stuff
<https://bezoar.hcst.net/portfolio/doc/organizing-my-stuff/>

How I keep track of things on my Unix workstation. The original version was written for the O'Reilly webpage in 2005, but they've removed the link. I put a copy here.

- Tue, 25 Jul 2006
Article: My sysadmin toolbox
<http://www.linux.com/archive/feature/55919>

Here are some of the things I use all the time, including a number of scripts I've written myself to leverage already useful Unix tools; they're not flashy, but they save me a ton of keystrokes.

- Fri, 16 Jan 2009
Article: Using Hyperestraier to search your stuff
<http://tldp.org/LDP/LGNET/158/vogel.html>

Describes how to set up an open-source text-indexer called Hyperestraier to allow fast desktop searching.