FreeBSD and Windows Environments

FreeBSD is Uniquely Positioned to Help Deploy, Virtualize, and Serve Microsoft Windows Production Environments

Michael Dexter

EuroBSDcon 2024, Dublin, Ireland

Read The Paper!

Bonus! This is a tutorial!

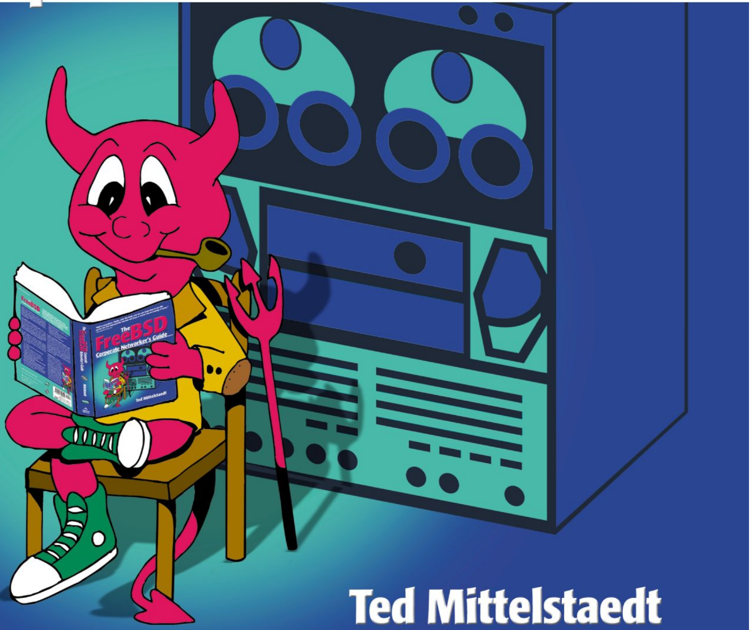
callfortesting.org/log/FreeBSD-Windows-MichaelDexter.pdf

Introduction

This all Started With a Book

"BSD is everywhere. Finally, with this book, you too can learn how to use the system that first deployed the Internet and plays a crucial role in running it today."
—Marshall Kirk McKusick

The FreeBSD Corporate Networker's Guide



Ted Mittelstaedt

Introduction

Ted “wrote the book”, metaphorically and literally

Introduction

A few things have changed since 2000

- Jail had JUST arrived
- SMP
- 64-Bit Addressing
- UEFI/GPT
- libxo/libucl
- `pkg(8)`
- Packet Filter
- DTrace
- ZFS
- `bhyve(8)` / Xen

Introduction

A few things have not changed since 2000

- The License
- /usr/src – buildworld
- /usr/ports – packages
- The Unix Environment
- NFS
- SSH
- CTRL-T
- The BSDCons

Introduction

A few things have changed in the last year

- `bsddialog(1)`
- Packaged Base
- mount -t nullfs -f
- mkimg/makefs -t zfs
- ZFS VM-IMAGEs

- OpenZFS 2.2.x
- GPU PCI Pass-Through
- TPM Pass-Through
- bhyve/ARM64
- Samba 4.19.x

Introduction

It took time but...

FreeBSD 14.x is *Really* Good

OpenZFS 2.2.x is *Really* Good

Samba 4.19 *Supports Functional Level 2016*

Introduction

Furthermore...

Search "`zfs initramfs`" to verify that...

FreeBSD is the *only* truly Tier-1 OpenZFS platform

Vendors have the staff, hobbyists have the time

Introduction

Furthermore...

The licenses will not change anytime soon

“Many of those Linux drivers are for reference”

ZFS on Linux with 100GbE is 20% slower

The World doesn’t need more GPL Violators

Introduction

Windows

The best-available implementation of the Win64 API used by many business applications, best-available hardware drivers, plus additional applications and features

Introduction

Windows: A few things have not changed over the years...

Inconsistent, arthritis-inducing keyboard layout

Difficulty preserving date stamps on folders

Folder views that do not automatically refresh

Different file and folder sort order

GUI-managed until Registry editing

Introduction

Windows: A few things have not changed over the years...

WindowsPE 11 still looks like Windows 7

XML-mapped configuration, except when not

XML-mapped configuration, except no export

Unnecessarily-Log-PowerShell-Commands

“Administrator” rather than “admin” or “root”

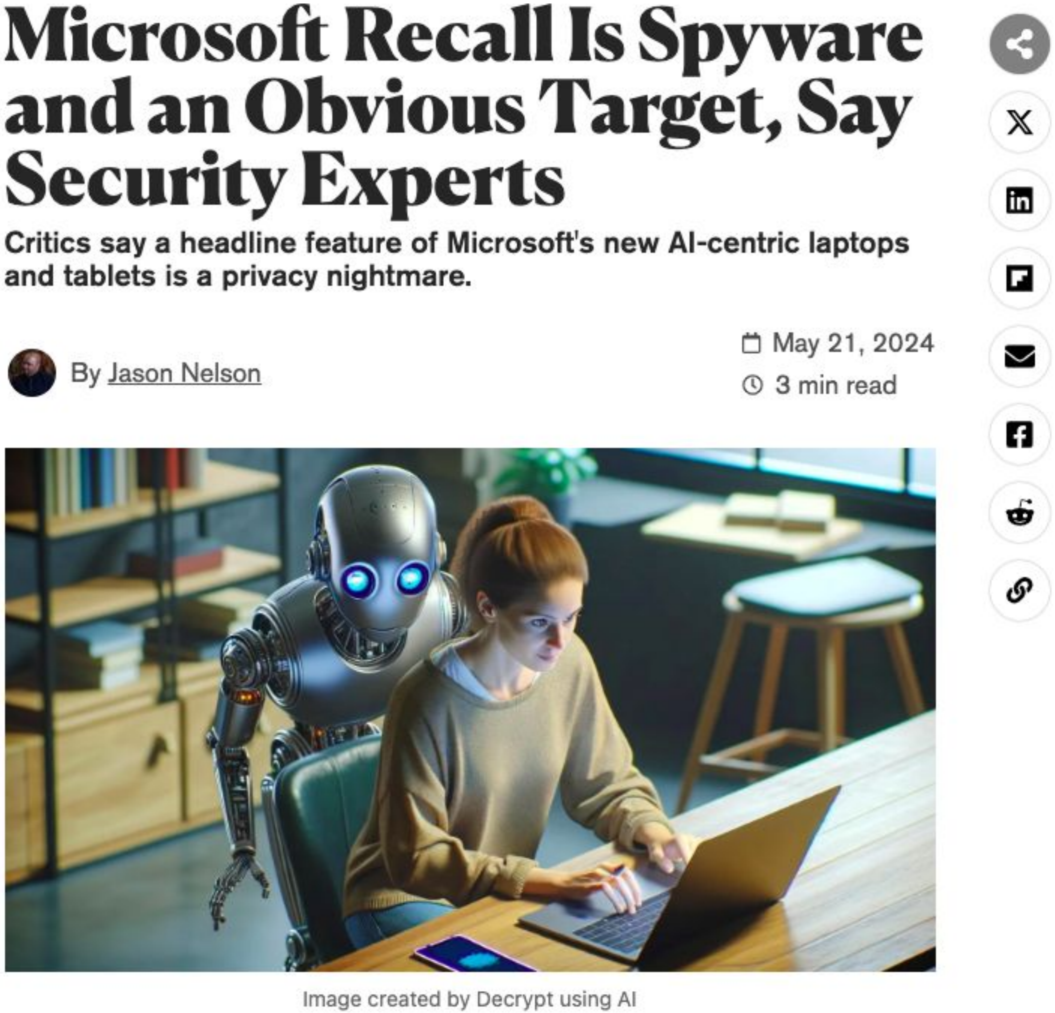
Introduction

Windows: A few things *have* changed over the years...

Windows and Windows Server have become gaslighting OneDrive/Azure marketing gateways

“Your organization's policies do not allow you to…”

“Cloud-based backup” – “We think you’ll really like this.”



Microsoft Recall Is Spyware and an Obvious Target, Say Security Experts

Critics say a headline feature of Microsoft's new AI-centric laptops and tablets is a privacy nightmare.

By Jason Nelson

May 21, 2024

3 min read

Image created by Decrypt using AI

Introduction

Modern Windows and Windows Server *must be contained*

FreeBSD is the best-available platform for that

The only OpenZFS-integrated platform on Earth critical

Deployment

Deployment

As a end-user facing operating system, Windows withholds *much* administrative information

Deployment

As an administrator-facing operating system,
Windows Server withholds *much*...
administrative information

Deployment

Hardware facts should not be secrets

The open source `dmidecode(8)`, `acpidump(8)`, `diskinfo(8)`, and `smartctl(8)` allow you to collect hardware facts like serial numbers, product keys, and disk facts and health information

Some of this information is available from `wmic` and add-on utilities

Deployment

Hardware facts should not be secrets

Boot to FreeBSD, have the information in seconds:

`github.com/michaeldexter/pchw`

Optionally tab-formatted for use in a spreadsheet or database:

```
sh generate-tsv.sh my-new-laptop
LENOVOThinkPad T490  20N20042US  Notebook  ABCD1234   1.80  06/21/2023
Intel(R) Core(TM) i7-8665U CPU @ 1.90GHz  No Asset Information
```

Deployment

Hardware facts should not be secrets

If `pchw.sh` finds an NVMe drive, it will provide the syntax to change its LBA format from say, 512b to 4Kn using FreeBSD's excellent `nvmecontrol(8)`

```
nvmecontrol format -f 01 nvme0ns1
shutdown -r now Possibly with devctl(8)
```

Deployment

WHICH of course will destroy all data on the drive

PRO TIP: Treat all existing and perhaps new systems as if you are performing a forensics investigation

FreeBSD’s `camdd(8)` is fast and very good at this

```
camdd -i file=/dev/da1,bs=1M -o file=4tb.raw
```

Deployment

You may want `sysutils/ddrescue`

```
ddrescue -d -r3 /dev/da1 4tb-ddrescue.raw ddrescue.log
```

Save those disk images to ZFS, snapshot them, boot them in bhyve, Xen, or QEMU when someone remembers they used that one system for that one application or account...

Deployment

At an extreme, you may want Klennet Recovery

Proprietary

Often Successful

Always under bhyve

Deployment

You may need `gpart(8)` to destroy partitions

```
gpart destroy -F /dev/ada0
```

Windows and macOS are somewhat terrible at this

Firmware updating: Your mileage may vary...

Windows tools vs. FreeBSD tools like `mpr|s|tutil(8)`

Deployment

```
efibootmgr
BootCurrent: 001d
BootOrder  : 0001, 0000, 001B, 001C, 001D, 001E, 001F,
0020, 0021, 0022, 0012, 0011, 0023, 0024
 Boot0001* Windows Boot Manager
 Boot0000* FreeBSD
...
+Boot001D* NVMe0

efibootmgr --delete -b 0001
```

Deployment

FreeBSD can mount NTFS partitions with `sysutils/fusefs-ntfs`

```
kldload fusefs
ntfs-3g -o ro /dev/md0p2 /mnt

ls /mnt/
$RECYCLE.BIN WindowsImageBackup
```

It’s slow, but it works

Deployment

FreeBSD can also mount SMB shares with `mount_smbfs(8)`

```
mount_smbfs -W MYDOMAIN \
//user@myserver/mysmb_share /mnt

ls /mnt/
$RECYCLE.BIN
```

It’s slow, not great about metadata, but it works

Deployment

FreeBSD can also mount SMB shares with `sysutils/fusefs-smbnetfs`

```
mkdir ~/.smb
cp /usr/local/share/doc/smbnetfs-0.6.3/smbnetfs.conf \
~/.smb/
vi ~/.smb/smbnetfs.auth
  auth 10.0.0.20 <user> <password>
chmod 600 ~/.smb/smbnetfs.auth
```

Deployment

```
vi ~/.smb/smbnetfs.host
  host 10.0.0.20 visible=true
mkdir ~/mnt
kldload fusefs
smbnetfs ~/mnt
ls ~/mnt/10.0.0.20
HelloWorld.txt
umount ~/mnt/10.0.0.20
```

Deployment

Data Copying/Transfering/Replication

There are at least three `rsync(8)` implementations for Windows

Yet “robust file copy” is still useful

```
robocopy D:\ E:\backups\previous-d-drive /MIR /FFT
/R:2 /W:1 /Z /XJD
```

(+/- `rsync(8)` equivalent syntax) Bonus! `net/openrsync` is ported!

Deployment

Bitlocker

Microsoft's Self-Imposed Ransomware

```
pkg install devel/libbde
bdemount -p <password> /dev/ada0p2 /mnt
```

Deployment

Bitlocker

As with any encryption, use it with extreme caution

Some vendors will not tell you that a system shipped with it, will wipe the key with a BIOS update, and you are separated from your data, free of charge

Deployment

PRO TIP: USB to IDE|SATA|NVMe adapters are your friend

PRO TIP: FreeBSD `VM-IMAGE`s are your friend

```
github.com/michaeldexter/occambsd/blob/main/imagine.sh
```

```
sh imagine.sh -r FreeBSD-14.0 -z -m -t /dev/da0
```

`-m` keeps it mounted – You could pkg add to the device from a FreeBSD host...

Deployment

FYI: FreeBSD raw `VM-IMAGE`s are simply boot images

They don’t know or care if they are on
real or virtualized hardware

The same is true of Debian “`nocloud`”, OmniOS “`cloud`”, and
raw images with Windows installed under a hypervisor

Deployment

FreeBSD, OmniOS, Debian, RouterOS... and Windows!

github.com/michaeldexter/occambsd/blob/main/imagine.sh

```
sh imagine.sh -x autounattend_xml/win2025.xml -o \
/path/to/your/windows-server/2025/insider-program.iso
sh /root/imagine-work/windows/bhyve-windows-iso.sh
```

wait a few minutes...

```
sh /root/imagine-work/windows/boot-windows-amd64-ntfs.sh
```

Deployment

Precisely how I updated a camera's firmware at the conference!

Deployment

`autounattend.xml` is your friend

`win10.xml win11.xml win2012.xml win2016.xml`
`win2019.xml win2022.xml win2025.xml`

No recovery partition, set Administrator password, create “root” user, enable RDP, SAC, disable Windows 11 TPM requirements...

All in minutes

Deployment

Finally...

Thank you OpenBSD!

Modern Windows and Windows Server have reasonable SSH/SSHd support

FreeBSD has reasonable RDP support with `net/xrdp` and a GPU driver or `net/tigervnc-server`

Deployment

```
pkg install -y xrdp tigervnc-server
```

```
service xrdp onestart
service xrdp-sesman onestart
```

Clipboard Sharing!

Connect with Microsoft Remote Desktop

And... connect to Windows RDP with `net/remmina`

Virtualization

Virtualization

FreeBSD’s bhyve hypervisor has supported Windows and Windows Server virtual machines since 2015

There were early quirks like needing to leaving an empty CD-ROM device for Windows Server, but largely down to setting the Low Pin Count (lpc) device to PCI slot 31

TPM Pass-Through arrived in FreeBSD 14.0

Virtualization

Thank you Hans!

TPM *emulation* is under review!

Directly from the Production User Calls

Virtualization

What matters is Virtualization with OpenZFS

Friends don’t let friends use Windows without OpenZFS backing storage

Virtualization *with OpenZFS*

OpenZFS is proven for mitigating or assisting with:

- Ransomware attacks
- Accidental data deletion
- Failed OS updates
- Staged OS and application installation
- Application data restoration

Virtualization *with OpenZFS*

Example staged application installation – *True story!*

- Install and snapshot the operating system
- Install old application version
- Import application data
- Upgrade the application
- Export application data
- Roll back the operating system
- Install new application version
- Re-import application data

Virtualization *with OpenZFS*

Eyes on the Prize

Corvin K has GPU pass-through working

Back a system with OpenZFS storage

Every system is suddenly ZFS snapshottable, sendable and bhyve bootable

Serving

“The Power To Serve”

Serving

FreeBSD *and* Windows have very good histories with iSCSI – *Because CIFS was terrible*

A quick example target on FreeBSD

```
truncate -s 10G /tmp/iscsi10G.raw
```

Serving

/etc/ctl.conf

```
portal-group default {
        discovery-auth-group no-authentication
        listen 10.0.0.20
}

target iqn.2014-09.org.freebsd:target0 {
        auth-group no-authentication
    portal-group default
        lun 0 {
                path /tmp/iscsi10G.raw
        size 10G
        }
}
```

Serving

Validate the file

```
ctld -f ctl.conf -t
```

Launch `ctld(8)` in debug mode

```
ctld -f ctl.conf -d
```

Connect with the Windows or FreeBSD initiator

Serving

Fun Fact

You can round-trip that `/tmp/iscsi10G.raw` image

Stop `ctld(8)`

Attach it with `mdconfig(8)`

Mount it with `ntfs-g3(8)`

The same with a ZVOL, adjusting the `vfs.zfs.vol.mode sysctl` as needed

Serving

Another Fun Fact

Enterprise versions of Windows and Windows Server have NFS servers and clients and someone, somewhere, has gotten them to work

Serving

Samba

Serving

Samba is an open source implementation of Microsoft’s Server Message Block (SMB) protocol

A *LOT* of data has passed through `samba(8)` on FreeBSD

Samba currently has 101 manual pages

`www.samba.org/samba/docs/man/`

Serving

The Samba Three Commandments

The Domain Controller is your DNS Server,
verify all aspects of DNS

Keep time in sync

Something extremely obscure

Serving

```
samba-tool domain provision --use-rfc2307 \
--realm=MYDOMAIN.MYDOMAIN.MYCOMPANY.LOCAL \
--domain=MYDOMAIN \
--server-role=dc \
--adminpass BigStrongPassword1! \
--option="ad dc functional level = 2016"
```

github.com/michaeldexter/freebsd-ad

Serving

Shower Thought...

Samba on ARM64 is proven

Windows Server does not support ARM64

If you are power-constrained, you *must* consider alternatives

Field Notes

If there is time

Field Notes

Daniel B’s Zelta

`github.com/bellhyve/zelta`

Field Notes

MAC Addresses are your friend

Use them for DHCP reservations

Generate them with one-liners

Assign them to VMs to see headless VMs with `arp -a`

Oh Proxmox

Field Notes

Happy IP Scanner!

github.com/michaeldexter/hipscan

```
192.168.116.2 22 80 443 8080
192.168.116.3 80
192.168.116.40 22 80
...
```

Field Notes

Going from an AD-joined account the local one?

```
<ComputerName>\<UserName>
```

```
.\<UserName>
```

Field Notes

The Production User Calls!

The Trifecta – Jail/Zones, OpenZFS, bhyve

callfortesting.org

All are welcome!

The Future

The Future

OpenZFS on Windows

Perhaps the shortest distance to bootability...

`github.com/maharmstone/quibble`

The Future

```
wmic diskdrive list brief

... DeviceID ...

\\.\PHYSICALDRIVE1

zpool.exe create -O casesensitivity=insensitive -O
normalization=formD -O compression=lz4 -O atime=off
-o ashift=12 tank PHYSICALDRIVE1
```

THANK YOU!

Michael Dexter

editor@callfortesting.org

@dexter@bsd.network