Windows Server 2022

Celebrating 12 years (6 different OS)
of Brent presenting on what's new in Windows Server

LouMUG

Agenda

- Versions
  - Essentials is dead
  - Hyper-V free is dead
  - Azure Edition is new
- Security
  - Secured core Server
  - Hardware root-of-trust
  - Firmware protection
  - Virtualization-based security (VBS)
- Connectivity
  - DNS-over-HTTPS
  - SMB AES-256
  - Failover cluster comms encryption
  - SMB Direct and RDMA encryption
  - SMB over QUIC

Agenda

- Azure
  - ARC enabled Windows Servers
  - Windows Admin Center
  - Azure automanage
- Containers
- Storage Migration Service new features
- Storage Spaces Direct Improvements
- Random improvements
  - Scale
  - Nested AMD virtualization
  - Edge browser
  - Networking performance
  - ReFS file-level snapshots
  - SMB compression
- Features removed or no longer developed

Disclosure/Context

- This is not a ‘fun’ release, it’s largely incremental and ‘under the covers’
- I’ve not gotten to directly play with a lot of this
- Microsoft:
  - is a for-profit company, like many of us
  - makes way more money on subscriptions (the cloud)
  - therefore wants everyone on subscriptions (the cloud)
- Throughout this presentation:
  - Many things will seem cynical towards their business model
  - Many things will point out how they’re forcing their business model (the cloud)

Why do you care?

- Windows Server 2008/R2 reached end of **extended** support 1/14/2020.
  - Unless you move it to Azure, then you get 3 years of extended
- Windows Server 2012/R2 reaches end of **extended** support 10/10/23
  - 94 weeks or 662 days from now
  - Unless you move it to Azure, then you get 3 years of extended
- Windows Server 2016 reaches end of **mainstream** support 1/11/22
  - 3 weeks or 25 days from now
- Windows Server 2016 reaches end of **extended** support 1/12/2027
  - 264 weeks or 1852 days from now

Versions

There are FOUR now.

- Windows Server 2022 Essentials
- Windows Server 2022 Standard
- Windows Server 2022 Datacenter
- Windows Server 2022 Datacenter: Azure Datacenter

Versions

Hyper-V Free is Dead.

- What was Hyper-V Free?
  - Completely free version of hyper-v that could cluster up to 64 nodes
  - Core only, no UI
- To run any Windows VMs, you still needed licensing
- So basically no one ever used it

Versions

Essentials is Dead.

- What was Essentials?
  - Windows Server license for up to 25 users/50 devices
  - Provided client backup
  - Remote web access
- The license still exists, just like in 2019
- It just activates as Windows Standard with no extra features
- “Move to Microsoft 365 Business”

Versions: Azure Edition

- Spoiler: only available in Azure
  - Azure proper
  - Azure Stack HCI (on premise subscription)
- Cannot run on bare metal
- Includes everything that Datacenter does, plus:
  - Azure Extended Network
  - Hotpatching
  - SMB over QUIC

Security

Secured Core Server

- OEM Certified hardware
- It’s a label that says that several security features are in place to protect the OS
- This has been out for a while for PCs and is now coming to servers
- The three key tenants are in the next slides

Security

Hardware Root-of-Trust

- Trusted Platform Module (TPM) 2.0 crypto-processor chips
  - Provides a hardware-based store for cryptographic keys and data
  - Can verify the server starts with legit code
  - A piece of this has been used for years for BitLocker

Security

Firmware Protection

- Firmware has the lowest level access
- AV can’t touch firmware
- Dynamic Root of Trust for Measurement – analyzes the boot process to see if it’s been tampered with
- Kernel Direct Memory Access ensures memory isolation for PCI devices

Security

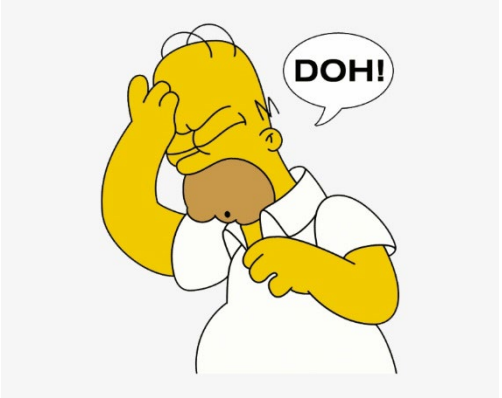
Virtualization-based Security (VBS)

- Seriously? We're reusing THAT acronym?
- Hardware virtualization features isolate a region of memory from the normal OS
- Credential Guard puts user credentials and secrets in a virtual container the OS can't directly access
- Hypervisor Based Code Integrity checks kernel mode drivers in virtualized environment before starting
- User mode code integrity can require apps to be signed in order to load
- Hypervisor assigns page permissions so that even if someone gets access, memory is read-only except to specific kernels

Security

Connectivity

- Supports and defaults to TLS 1.3
- DNS client supports DNS-over-HTTPS (DoH)
  - Can be set to require DoH, Request DoH, or only use plain-text
  - Server has to be on known list of DoH servers
    - This list is currently (default) microscopic, Cloudflare, Google, Quad 9




```
PS C:\Users\Brent> get-dnsclientdohserveraddress

ServerAddress         AllowFallbackToUdp AutoUpgrade DohTemplate
-------------         ------------------ ----------- -----------
149.112.112.112       False              False       https://dns.quad9.net/dns-query
9.9.9.9               False              False       https://dns.quad9.net/dns-query
8.8.8.8               False              False       https://dns.google/dns-query
8.8.4.4               False              False       https://dns.google/dns-query
1.1.1.1               False              False       https://cloudflare-dns.com/dns-query
1.0.0.1               False              False       https://cloudflare-dns.com/dns-query
2001:4860:4860::8844  False              False       https://dns.google/dns-query
2001:4860:4860::8888  False              False       https://dns.google/dns-query
2606:4700:4700::1001  False              False       https://cloudflare-dns.com/dns-query
2606:4700:4700::1111  False              False       https://cloudflare-dns.com/dns-query
2620:fe::fe           False              False       https://dns.quad9.net/dns-query
2620:fe::fe:9         False              False       https://dns.quad9.net/dns-query
```

Security

Connectivity

- SMB AES-256
  - SMB Encryption has been around for as long as SMB 3.x (Server 2012)
  - Now we're implementing AES-256 to replace 128.
- Failover cluster comms encryption
  - East/West traffic can now be encrypted between servers
- SMB Direct and RDMA encryption
  - SMB Direct with RDMA allows direct data placement
  - Way lower latency, higher bandwidth
  - Did not support encryption for direct data placement
  - Now it encrypts before placing data

Security

Connectivity

- SMB over QUIC
  - Only supported on Datacenter: Azure Edition
  - QUIC is an IETF-standardized protocol has been around for 9 years
    - Creates multiple UDP streams for data and handles error correction higher
    - Trying to get away from inherent limitations of TCP
    - Always encrypted and requires TLS 1.3
  - Uses edge file servers to transfer data without the need of a VPN
  - Only works between 2022 and Windows 11
  - Requires PKI

Azure

Yep, we have to talk about the cloud.

- Azure ARC enabled Windows Servers
  - Isn't unique to 2022, but is listed as a what's new in 2022:
    - Windows Server 2008 R2 SP1, Windows Server 2012 R2, 2016, 2019, and 2022 (including Server Core)
    - Ubuntu 16.04, 18.04, and 20.04 LTS (x64)
    - CentOS Linux 7 and 8 (x64)
    - SUSE Linux Enterprise Server (SLES) 12 and 15 (x64)
    - Red Hat Enterprise Linux (RHEL) 7 and 8 (x64)
    - Amazon Linux 2 (x64)
    - Oracle Linux 7
  - Allows a connected server to be managed in Azure
  - Apply Azure policy (governance) for $6 per server per month
  - Microsoft Defender for Cloud integration
  - Azure sentinel (security log collection/hunting)
  - Azure automation and monitoring

Azure

- Windows Admin Center (not officially tied to Server 2022)
  - Supports new features for Server 2022
  - New Security tool mostly for Server 2022 features
  - Has additional Azure buttons
  - Twice as fast at managing Hyper-V/clusters
  - “Deploying Windows Admin Center in Azure is not only simpler and more reliable, but also more performant than deploying it on-premises”
- Azure automanage – hotpatch – Only in Datacenter: Azure Edition
  - Installs updates without requiring a reboot
  - Cumulative updates become a baseline every 3 months and are reboots, everything else is live

Azure Extended Network

Only in DataCenter: Azure Edition

- Allows you to create VMs for a VXLAN portal for IP mobility
- Setup one on premise (in your Azure Stack HCI)
- Setup one in Azure
- Both can operate as if they’re layer 2 connected despite being routed
- Excellent for migrations or DR testing

Containers

Smaller, faster, easier (the same story as the last time)

- Image reduced by 40%, again.
- 30% faster startup time
- Optimized integration with Azure AD
- Can run MSDTC and Message Queuing
- Optimizations to simplify Kubernetes experience
- WAC can assist with containerizing .NET apps

Storage Migration Service New Features

More use cases.

- Migrate local users/groups
- Migrate from/to failover clusters
- Migrate from a Samba based Linux server
- ‘more easily’ sync to Azure using Azure File Sync
- Migrate to new networks ‘such as Azure’.
- Migrate NetApp CIFS

Storage Spaces Improvements

- Storage Spaces Direct:
  - Adjustable storage repair speed
    - Pick whether you want it to prioritize front-end performance, or repairing
  - Faster repair and resync
    - Only moves data that it needs, instead of everything (data tracking)
- Normal Storage Spaces
  - Storage bus cache (previously only S2D)
  - Requires Failover clustering installed, but NOT a member of a cluster

Random Improvements

- Scale
  - Up to 64 physical sockets, 2048 logical cores, and 48TB of RAM
- Nested AMD virtualization
  - Mostly for labing… and Azure
- Edge browser
  - Not only available, installed by default… IE is still there.
- ReFS file-level snapshots
  - Read-only point in time using quick metadata – mostly for VHD/VHDX backups
- SMB compression

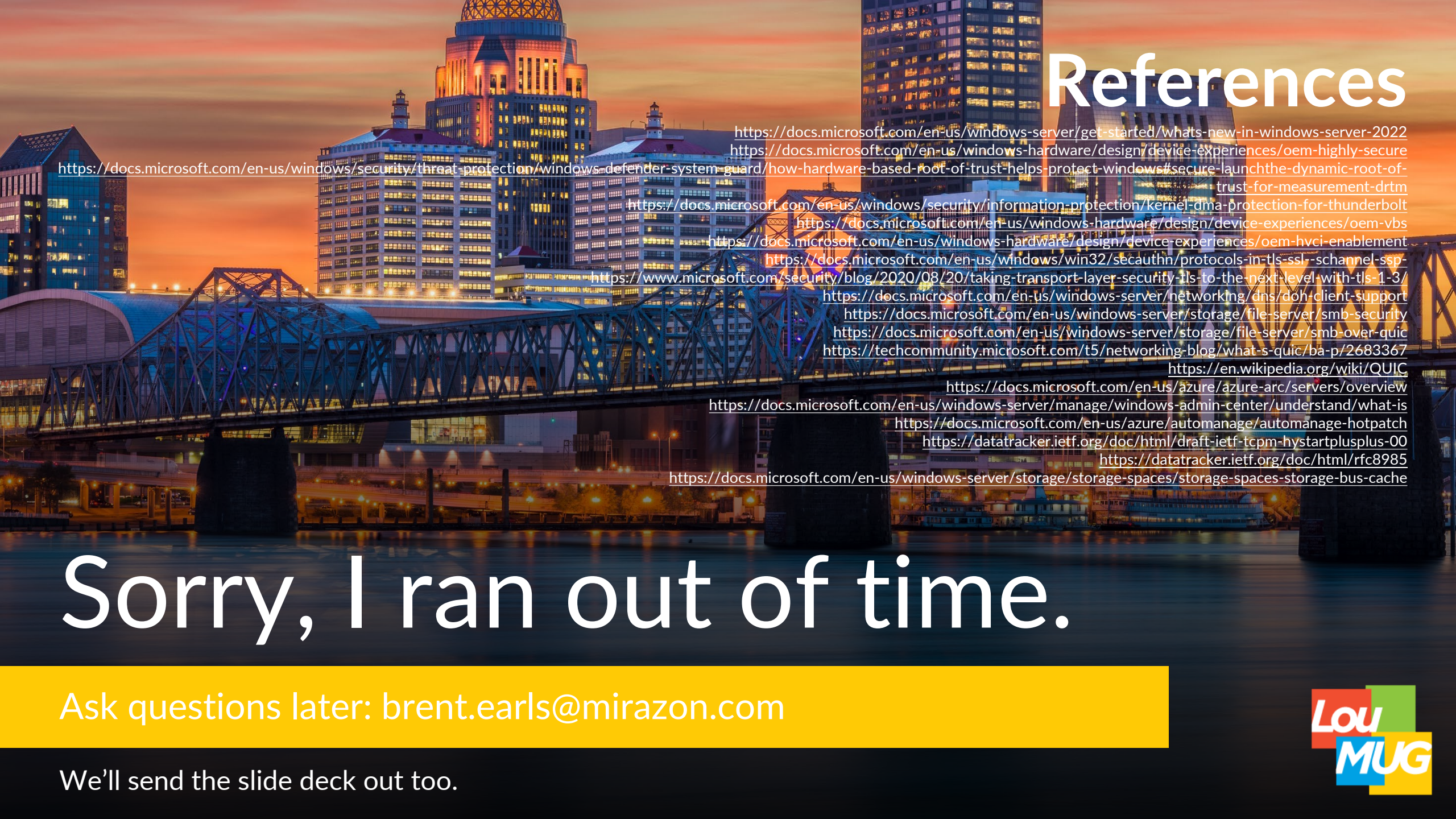
Random Improvements

- Networking performance
  - UDP
    - QUIC protocol “brings UDP to performance par of TCP”
    - UDP Segmentation Offload to NIC
    - UDP Receive Side Coalescing (like TCP RSC)
  - TCP new RFCs implemented by default
    - TCP HyStart++ (more quickly find ideal transmission rate)
    - RACK (reduce retransmit TimeOuts [RTO])
  - Hyper-V virtual switch
    - Updated receive Segmenet Coalescing (RSC)
- Hyper-V virtual switch cannot use normal teaming, only SET

Murders Most Foul

Features removed or no longer developed with Server 2022.

- Removed:
  - Semi-Annual channel
    - Surprise! No one wanted to be forced to update every 6 months
    - End of life is December 14, 2021 or May 10, 2022 depending on version
  - Internet Storage Name Service (iSNS)
    - For Windows server as an iSCSI target
- Features no longer being developed:
  - Guarded Fabric and Shielded Virtual Machines
  - Sconfig.cmd, now launch it from PowerShell “sconfig” (no joke, this is in the list)
  - Windows Deployment Serices boot.wim (instead use MDT or Endpoint Configuration Manager



References

https://docs.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2022
https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-highly-secure
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-system-guard/how-hardware-based-root-of-trust-helps-protect-windows#secure-launchthe-dynamic-root-of-trust-for-measurement-drtm
https://docs.microsoft.com/en-us/windows/security/information-protection/kernel-dma-protection-for-thunderbolt
https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs
https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-hvci-enablement
https://docs.microsoft.com/en-us/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp-
https://www.microsoft.com/security/blog/2020/08/20/taking-transport-layer-security-tls-to-the-next-level-with-tls-1-3/
https://docs.microsoft.com/en-us/windows-server/networking/dns/doh-client-support
https://docs.microsoft.com/en-us/windows-server/storage/file-server/smb-security
https://docs.microsoft.com/en-us/windows-server/storage/file-server/smb-over-quic
https://techcommunity.microsoft.com/t5/networking-blog/what-s-quic/ba-p/2683367
https://en.wikipedia.org/wiki/QUIC
https://docs.microsoft.com/en-us/azure/azure-arc/servers/overview
https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/what-is
https://docs.microsoft.com/en-us/azure/automanage/automanage-hotpatch
https://datatracker.ietf.org/doc/html/draft-ietf-tcpm-hystartplusplus-00
https://datatracker.ietf.org/doc/html/rfc8985
https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/storage-spaces-storage-bus-cache

Sorry, I ran out of time.

Ask questions later: brent.earls@mirazon.com

We'll send the slide deck out too.

LouMUG