Windows Server 2012 R2

Tomáš „Kanty“ Kantůrek
tomaskan@microsoft.com
Microsoft

Miroslav Knotek
knotek@kpcs.cz
KPCS CZ, s.r.o.

Windows Server 2012 Windows 8 Windows Azure Microsoft System Center 2012

What is new in Windows Server 2012 R2

BYOD

- Workplace Join
- Work Folders
- Web Application Proxy

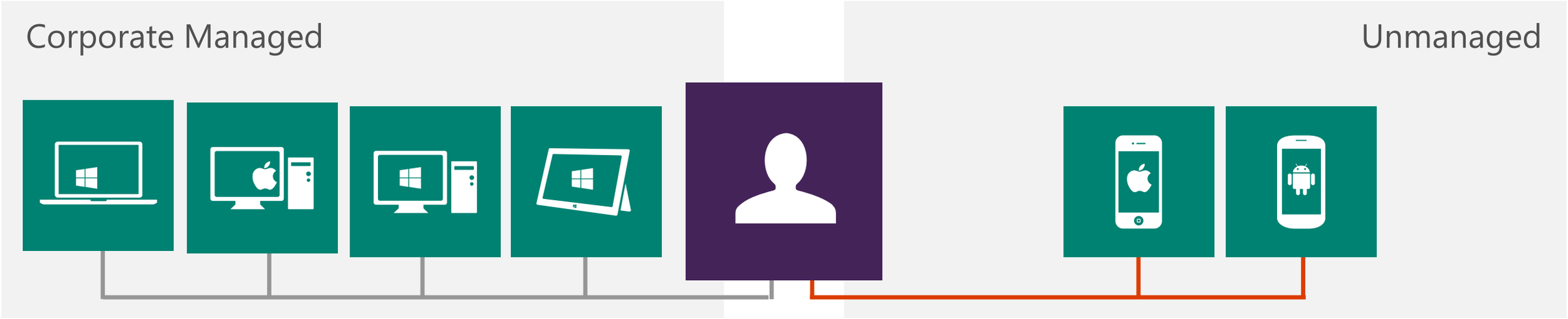
What's happening?

Before

Corporate Managed

What's happening?

Now



90%

of enterprises will have two or more mobile operating systems to support in 2017

GARTNER
GARTNER PRESS RELEASE, GARTNER SAYS TWO-THIRDS OF ENTERPRISES WILL ADOPT A MOBILE DEVICE MANAGEMENT SOLUTION FOR CORPORATE LIABLE USERS THROUGH 2017, OCTOBER 25, 2012, HTTP://WWW.GARTNER.COM/NEWSROOM/ID/2213115

32%

of employees use two or three PCs for work from multiple locations

FORRESTER RESEARCH
THE STATE OF WORKFORCE TECHNOLOGY ADOPTION: GLOBAL BENCHMARK 2012, FORRESTER RESEARCH, INC., APRIL 12, 2012

Mobility is the new normal

67%

of the people who use a smartphone for work and 70% of people who use a tablet for work are **choosing the devices themselves**

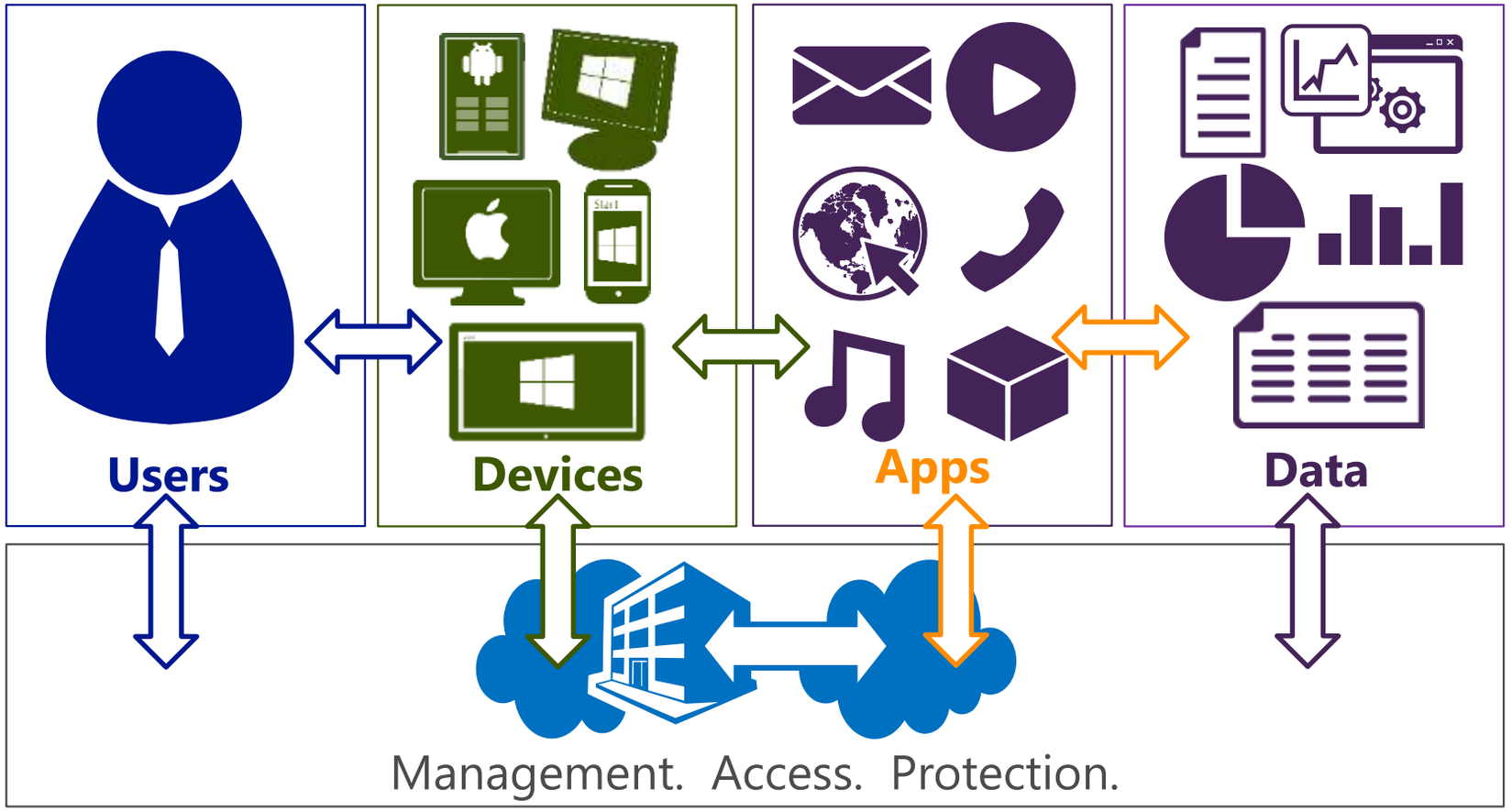
FORRESTER RESEARCH
BRING THE BUSINESS CASE FOR A BRING-YOUR-OWN-DEVICE (BYOD) PROGRAM, FORRESTER RESEARCH, INC., OCTOBER 23, 2012

905M

tablets in use for work and home globally by 2017

FORRESTER RESEARCH
2013 MOBILE WORKFORCE ADOPTION TRENDS, FORRESTER RESEARCH, INC., FEBRUARY 4, 2013

People-centric IT



Enable users

Allow users to work on the devices of their choice and provide consistent access to corporate resources.

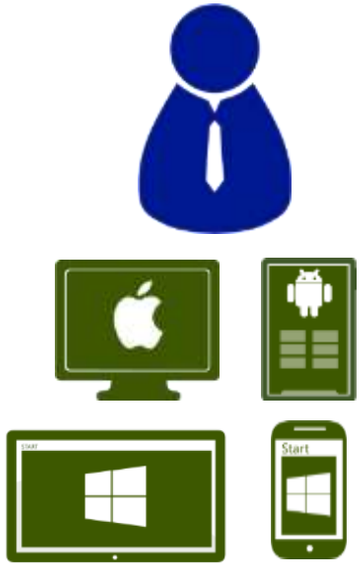
Hybrid Identity

Deliver a unified application and device management on-premises and in the cloud.

Protect your data

Help protect corporate information and manage risk.

Registering and Enrolling Devices



Users can **register** BYO devices for **single sign-on** and access to corporate data with **Workplace Join**. As part of this, a **certificate** is installed on the device

Windows Intune

Users can **enroll devices** which configure the device for management with Windows Intune. The user can then use the **Company Portal** for easy access to corporate applications

Microsoft System Center 2012 R2 Configuration Manager

Data from **Windows Intune** is sync with **Configuration Manager** which provides **unified management** across both on-premises and in the cloud

Windows Azure Active Directory Multi-Factor Authentication

Web Application Proxy

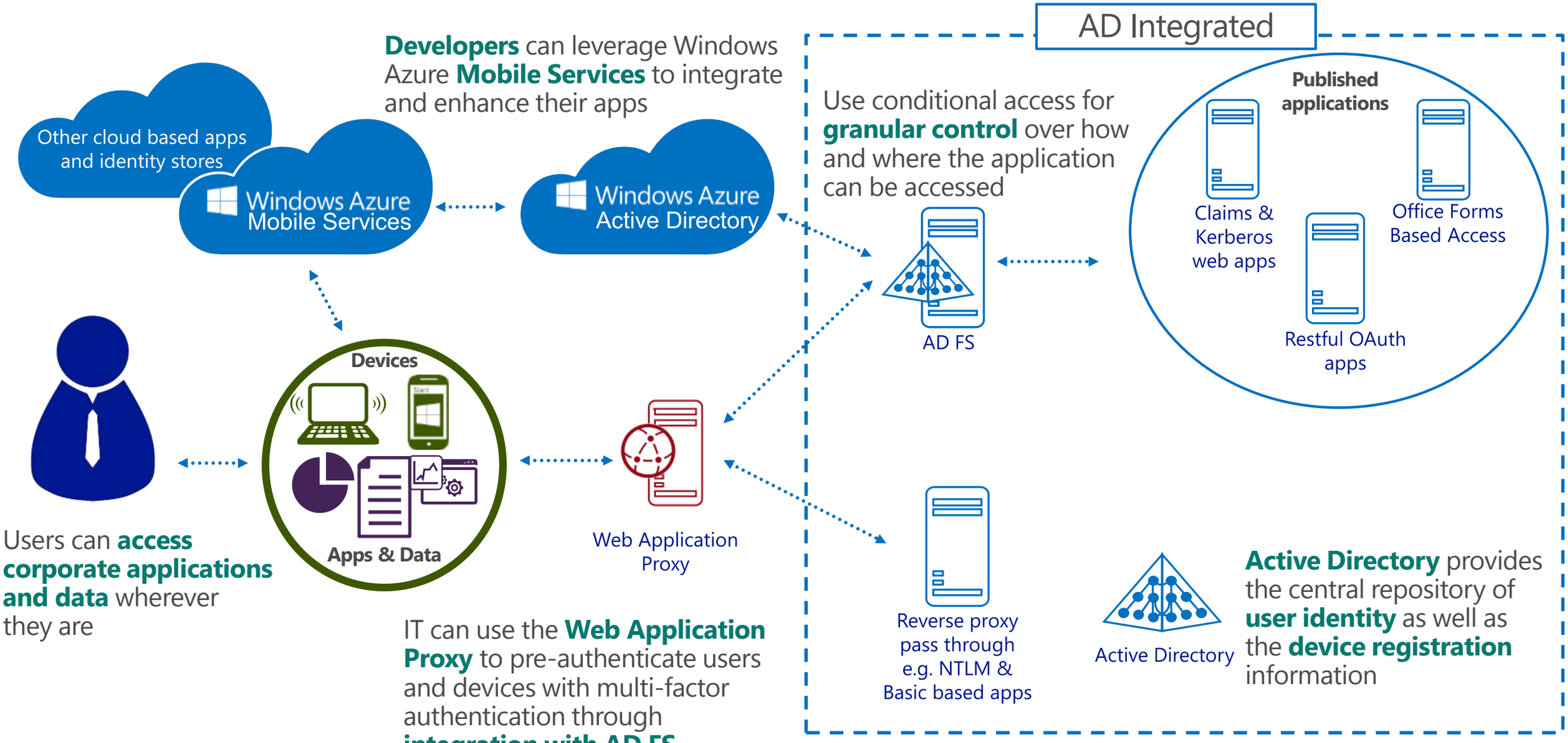
AD FS

IT can **publish access** to corporate resources with the **Web Application Proxy** based on device awareness and the users identity. **Multi-factor authentication** can be used through **Windows Azure Multi-Factor Authentication** integration with Active Directory Federation Services.

Windows Server Active Directory

As part of the registration process, a new **device record** is created in Active Directory, establishing a link between the user and their device

Publish access to resources with the Web Application Proxy

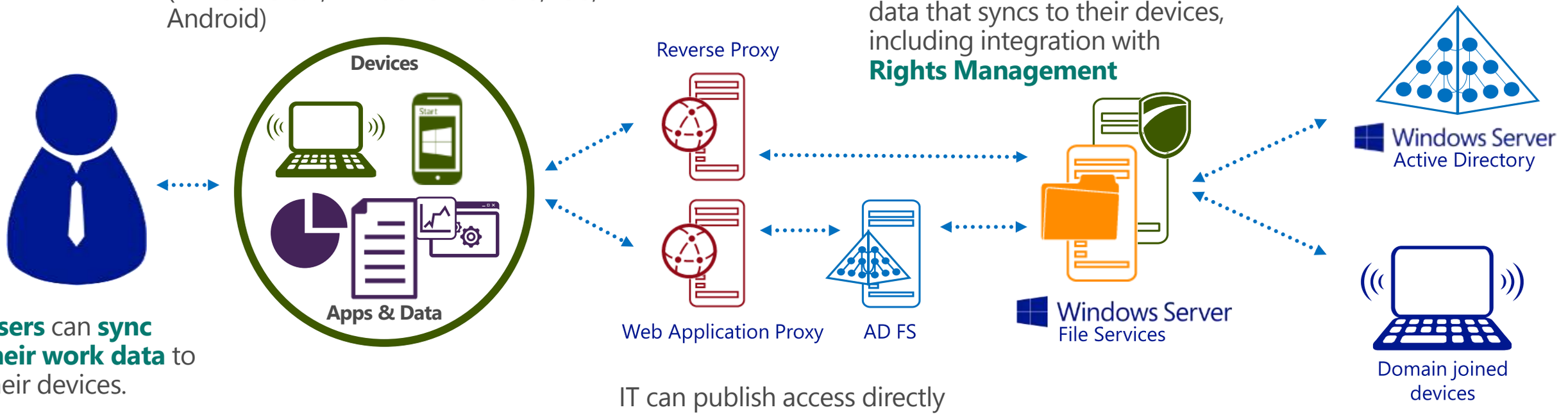


Make corporate data available to users with Work Folders

IT can **selectively wipe** the corporate data from **managed devices** (Windows 8.1, Windows Phone 8, iOS, Android)

IT can configure a File Server to provide **Work Folder sync shares** for each user to store data that syncs to their devices, including integration with **Rights Management**

Active Directory discoverability provides users Work Folders location



Users can **sync their work data** to their devices.

Users can **register their devices** to be able to sync data when IT enforces **conditional access**

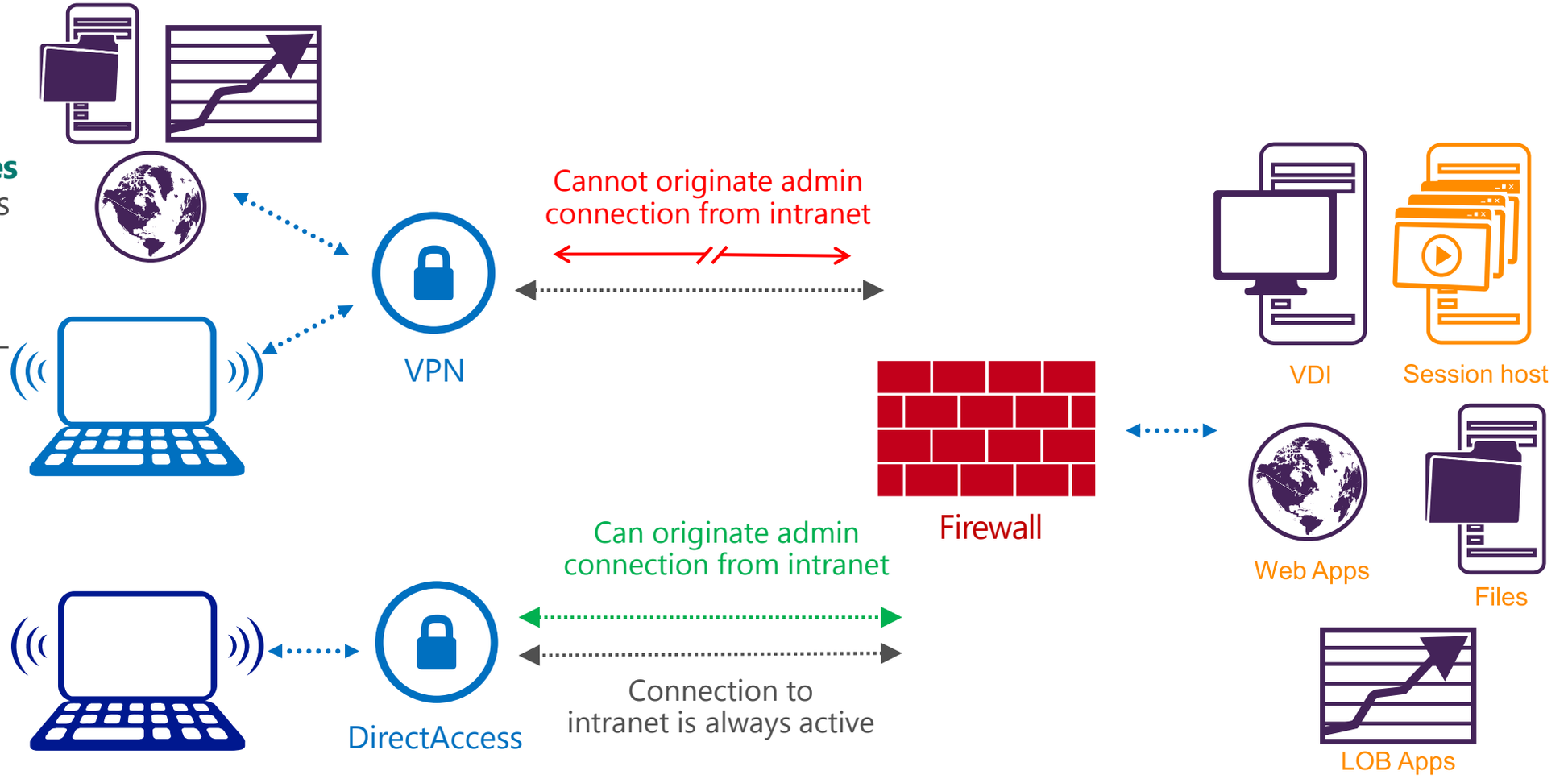
IT can publish access directly through a reverse proxy (such as the **Web Application Proxy**, or **conditional access** can be enforced through integration with **AD FS**

Effective working with Remote Access

An **automatic VPN connection** provides automated starting of the VPN **when a user launches** an application that requires access to corporate resources.

Traditional VPNs are user-initiated and provide **on-demand** connectivity to corporate resources.

With **DirectAccess**, a users PC is **automatically** connected whenever an Internet connection is present.



Hybrid Identity

Challenges

Providing **users** with a **common identity** when they are accessing resources that are located both on-premises in a corporate environment, and in cloud-based platforms.

Managing multiple identities and keeping the information in sync across environments is a **drain on IT** resources.

Solutions

Users have a **single sign-on experience** when accessing all resources, regardless of location.

Users and IT can leverage their common identity for access to **external resources through federation**.

IT can **consistently manage identities** across on-premises and cloud-based identity domains.

Delivering a seamless user authentication experience

Cloud Authentication

Multi-Factor Authentication can be configured through **Windows Azure**

User attributes are synchronized using DirSync **including the password hash**, Authentication is completed against **Windows Azure Active Directory**

Federated Authentication with Single Sign-On

AD FS provides **conditional access** to resources, **Work Place Join** for device registration and integrated **Multi-Factor Authentication**

User attributes are synchronized using DirSync, **Authentication is passed back through federation** and completed against **Windows Server Active Directory**

Protect your data

Challenges

As users **bring their own devices** in to use for work, they will also want to **access sensitive information** and have access to this information locally on the device.

A significant amount of **corporate** data can only be found **locally on user devices**.

IT needs to be able to **secure, classify, and protect data** based on the content it contains, not just where it resides, including **maintaining regulatory compliance**.

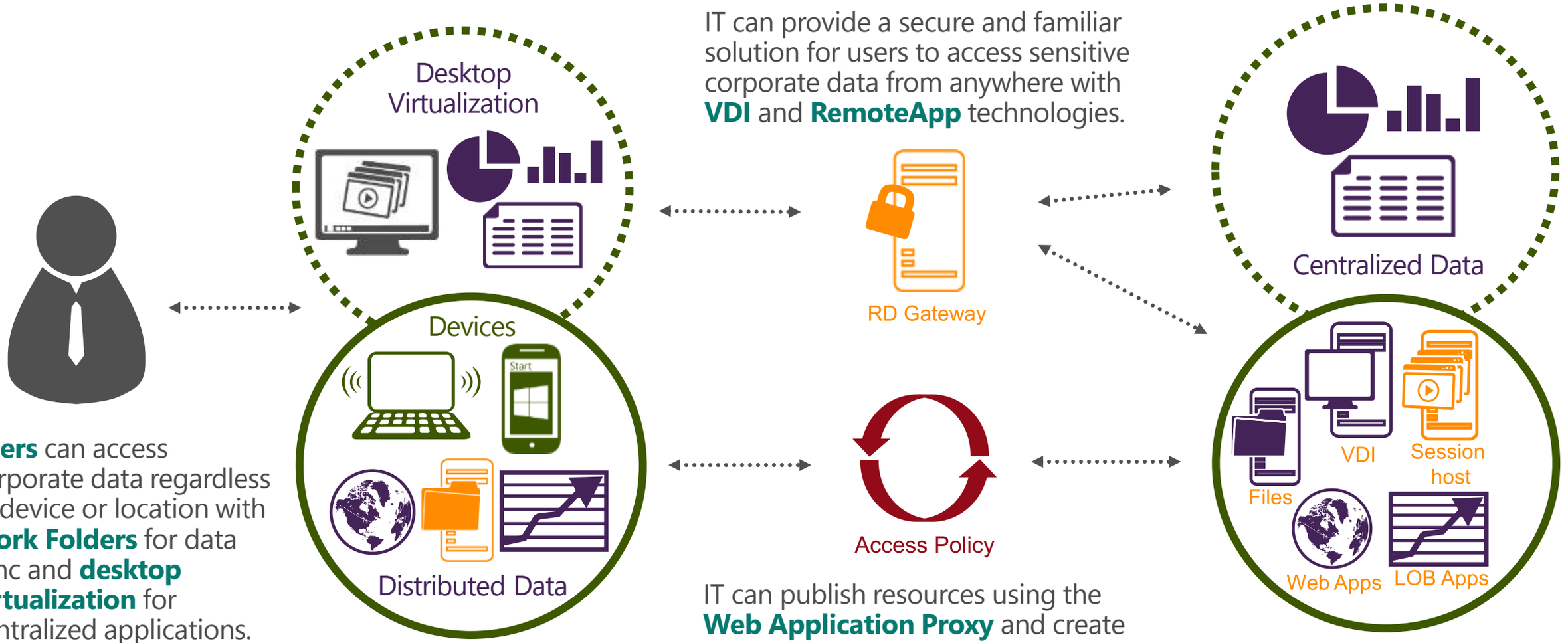
Solutions

Users can work **on the device of their choice** and be able to access **all their resources**, regardless of location or device.

IT can enforce a set of **central access and audit polices**, and be able to protect sensitive information **based on the content of the documents**.

IT can **centrally audit and report** on information access.

Policy based access to corporate information



Users can access corporate data regardless of device or location with **Work Folders** for data sync and **desktop virtualization** for centralized applications.

IT can provide a secure and familiar solution for users to access sensitive corporate data from anywhere with **VDI** and **RemoteApp** technologies.

IT can publish resources using the **Web Application Proxy** and create business-driven access policies with **multi-factor authentication** based on the content being accessed.

IT can audit user access to information based on **central audit policies**.

Deep dive: Workplace Join

Associates the device with a user

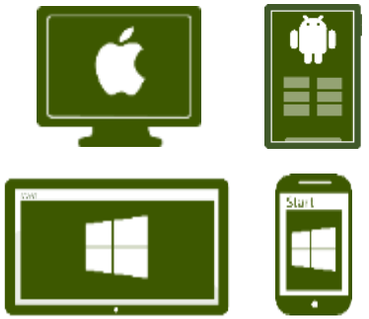
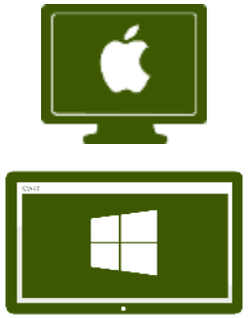
- Provides a seamless second factor authentication

Enables a better end user experience with SSO

- Avoids risks involved in saving passwords with each application
- Avoids users having to repeatedly enter their credentials

Enabled by device registration service in AD FS

Expanded domain join capabilities

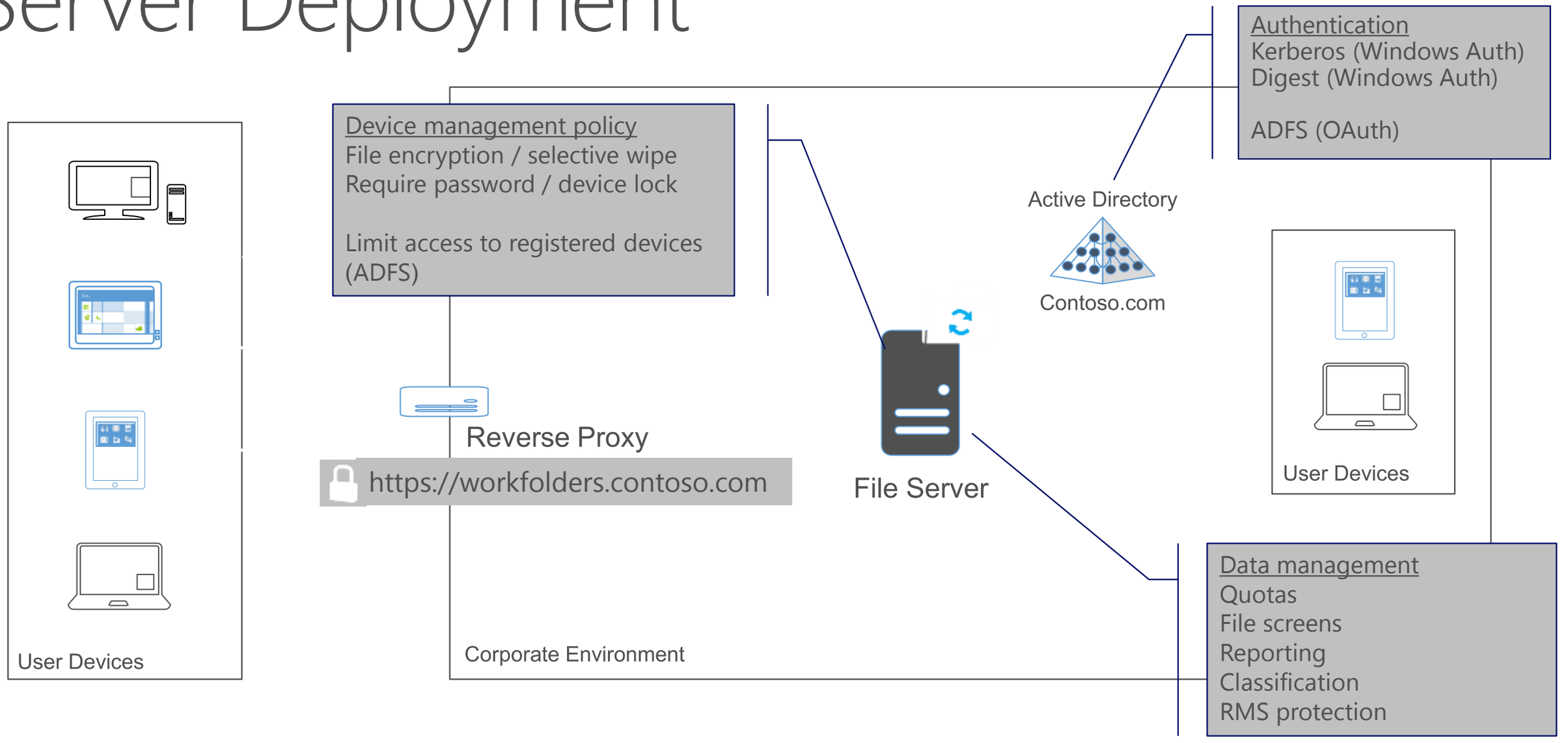
	Not Joined	Workplace Joined	Domain Joined
			
	User provided devices are “unknown” and IT has no control. Partial access may be provided to corporate information.	Registered devices are “known” and device authentication allows IT to provide conditional access to corporate information	Domain joined computers are under the full control of IT and can be provided with complete access to corporate information
Browser session single sign-on	✓	✓	✓
Seamless 2-Factor Auth for web apps	✗	✓	✓
Enterprise apps single sign-on	✗	✓	✓
Desktop Single Sign-On	✗	✗	✓

Demo: workplace join
http://go.microsoft.com/?linkid=9842896

Deep dive: Work Folders

- HTTPS sync of a user's files to all their devices
- Simple to deploy, use and manage
  - Centralize, protect and manage data
  - Encryption of data in transit and at rest, as well as remote data wipe
  - Easily separate work and personal data
  - Simple, intuitive user experience
  - Can leverage AD DS, Group Policy, Intune… or not. Your call.
- Leverage existing investment
  - Still a Windows file server
  - No SharePoint, no third parties, no cloud
  - Leverage all aspects of the Windows File Server stack
- Win8.1, Win7 (coming), IOS on iPad (coming)

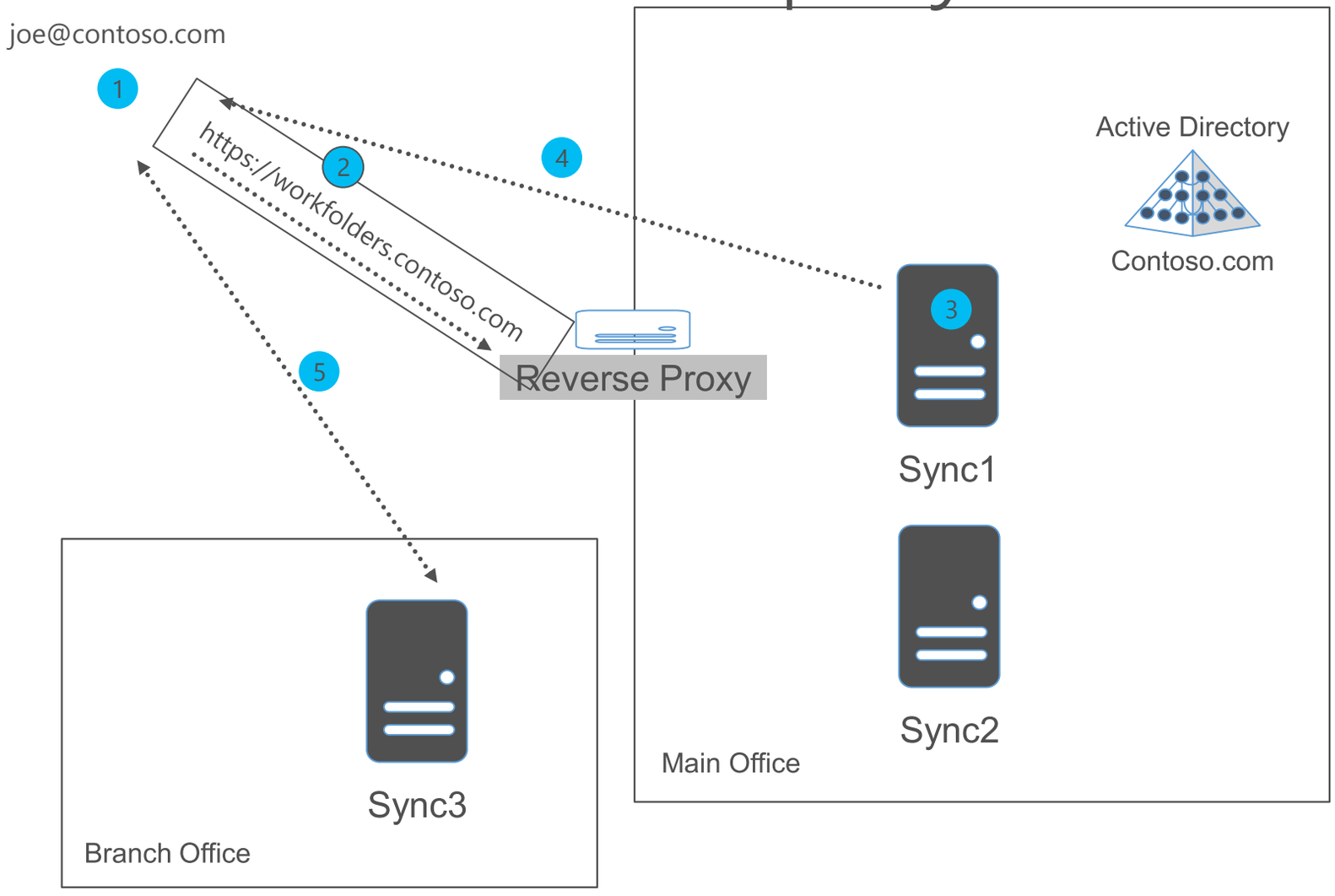
Server Deployment



File Sync Solutions

	Consumer / personal data	Individual work data	Team / group work data	Personal devices	Data location
SkyDrive	✓			✓	Public cloud
SkyDrive Pro		✓	✓	✓	SharePoint / Office 365
Work Folders		✓		✓	File server
Folder Redirection / Client-Side Caching		✓			File server

Multi-server deployments: Auto Discovery



1. Joe enters: joe@contoso.com
2. Auto discovery uses: https://workfolders.contoso.com
3. Request gets to Sync1.contoso.com which looks up Joe's sync server in AD
4. Redirect Joe's device to Sync3.contoso.com
5. Sync commences between Joe's device and Sync3.contoso.com

Demo: work folders

Deep dive: Web Application Proxy

IW:
Productivity

- Access corpnet apps from every device from everywhere, Windows and non-Windows
- The IW device can be un-managed, dis-joined (and even not workplace-joined)
- SSO

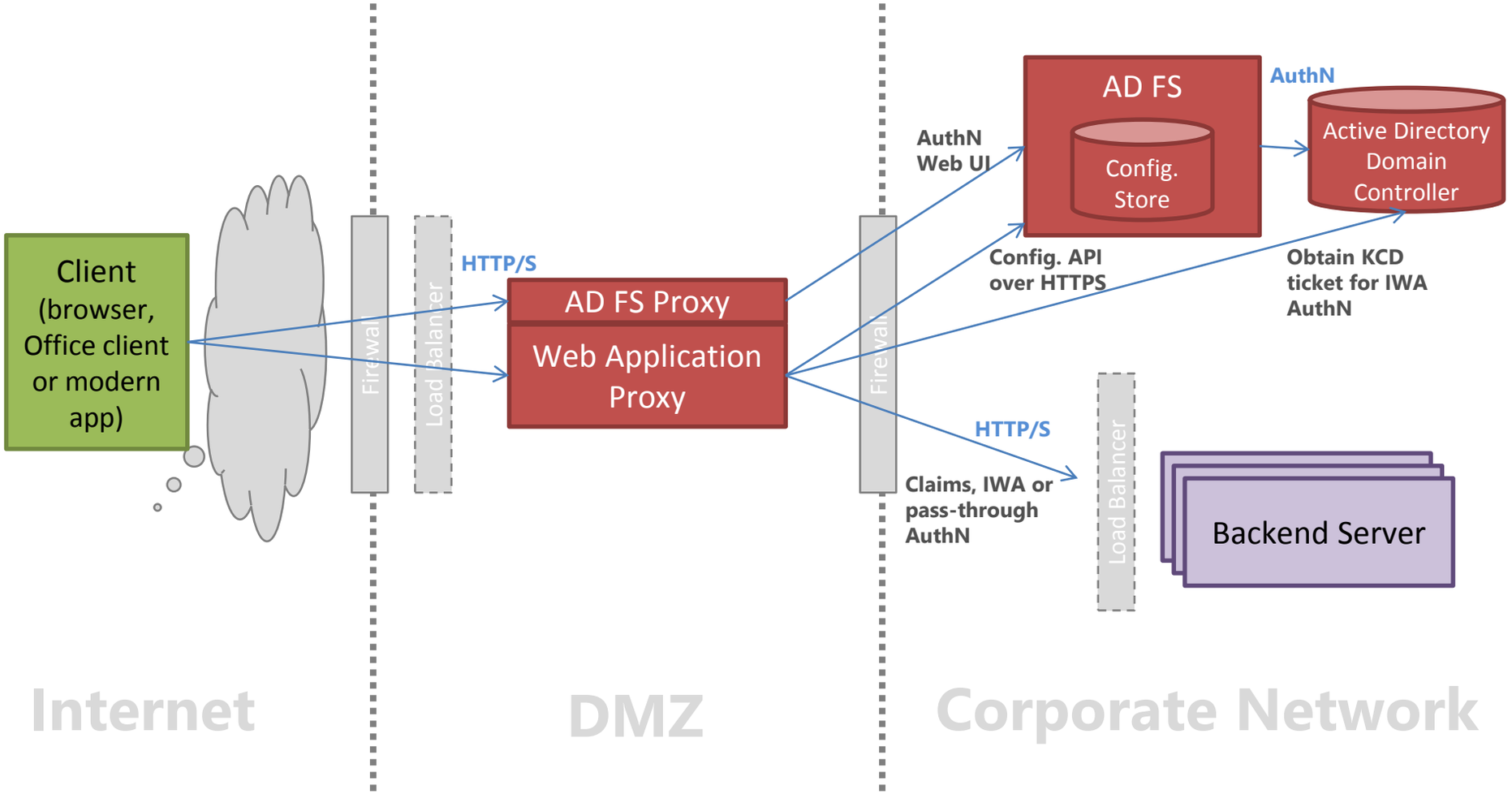
IT Pro:
Manage Risk

- Selectively publish apps form corpnet
- Control access per app, user, device, location
- Better protection with pre-authentication
- No changes in existing apps
- No changes in devices (clientless)

Reverse proxy services

- Network Isolation: incoming web traffic cannot directly access BE server (even after pre-authentication, and even in pass-through)
- Publishing is selective per internal application endpoint
- Web protocols only: HTTP, HTTPS
- DOS protection for BE server: incoming traffic is throttled and queued, to protect BE servers
- URL translation: well-written corpnet apps can remain with internal non-FQDN URLs (http://hr); 2012 R2 provides HTTP header level translation
- HTTPS-only endpoints are published externally (even in pass-through)
- HTTPS to HTTP translation: internal URLs can remain HTTP
- ADFS Proxy services: connecting through to internal ADFS, DRS

Network topology



Relation to TMG, ARR

- TMG is commonly used for publishing
  - Especially Exchange publishing scenarios with client certificate authentication
  - You can help identify critical capabilities in TMG required for great publishing experience for WAP scenarios

- IIS ARR is occasionally mentioned as reverse proxy
  - Especially for Lync 2013 and for URL translation scenarios
  - The intended enterprise offering for web publishing is WAP, as part of Windows Server 2012 conditional access platform

Identity capabilities for BYOD

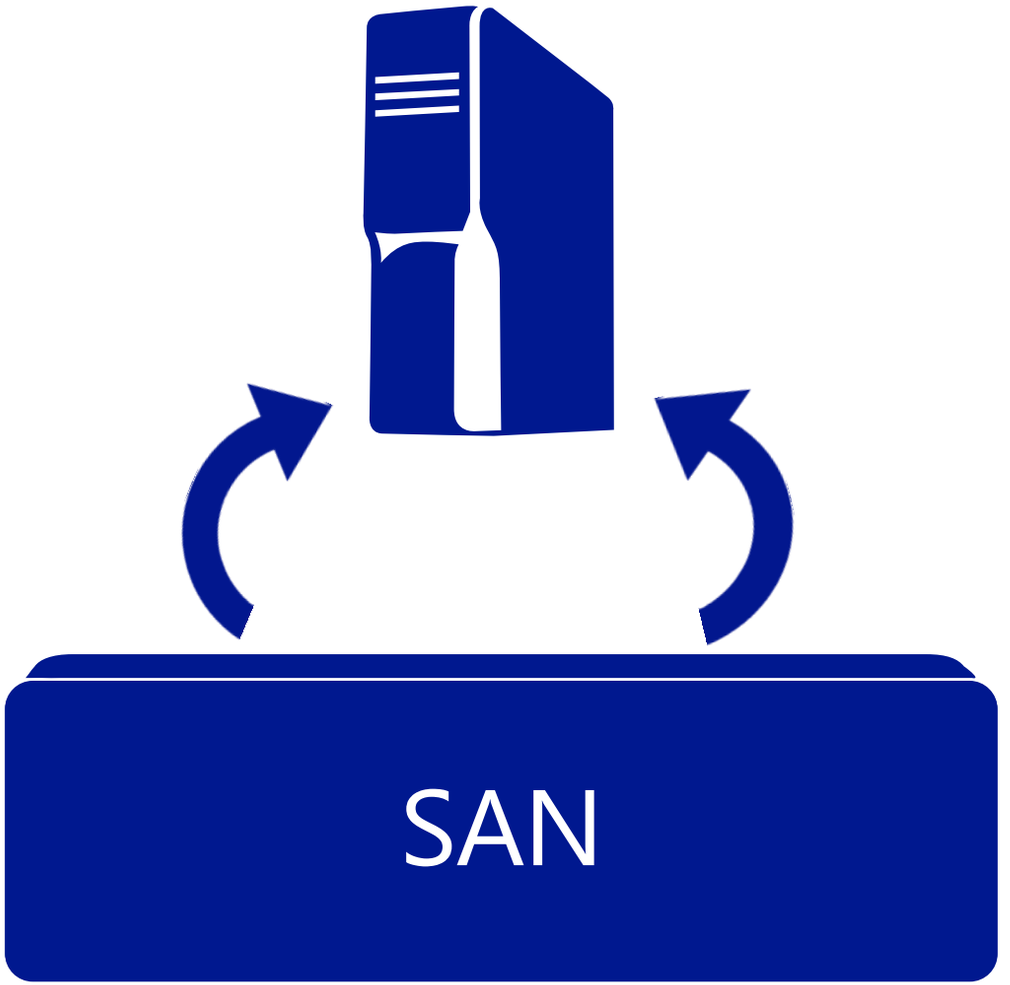
AD Workplace Join	Users join their device to their workplace, making the device known to the company's Active Directory
Single Sign On (SSO)	Users sign-in once to their company from any application and are not prompted for credentials by every company application when using workplace joined devices.
Work From Anywhere	Businesses enable users to work from anywhere while adhering to their IT governance policies around risk management
Multi-factor Authentication	Businesses require additional factors of authentication when business critical resources are accessed or when there is perceived risk
Multi-factor Access Control	Businesses set conditional access control to resources based on four core pivots: the user, the device used, the user's network location and use of additional auth factors
AD Authentication Library	ISVs build enterprise apps that delivery SSO and allow enterprises to set the access control policies based on user, device and network location, and MFA

What is new in Windows Server 2012 R2

Storage

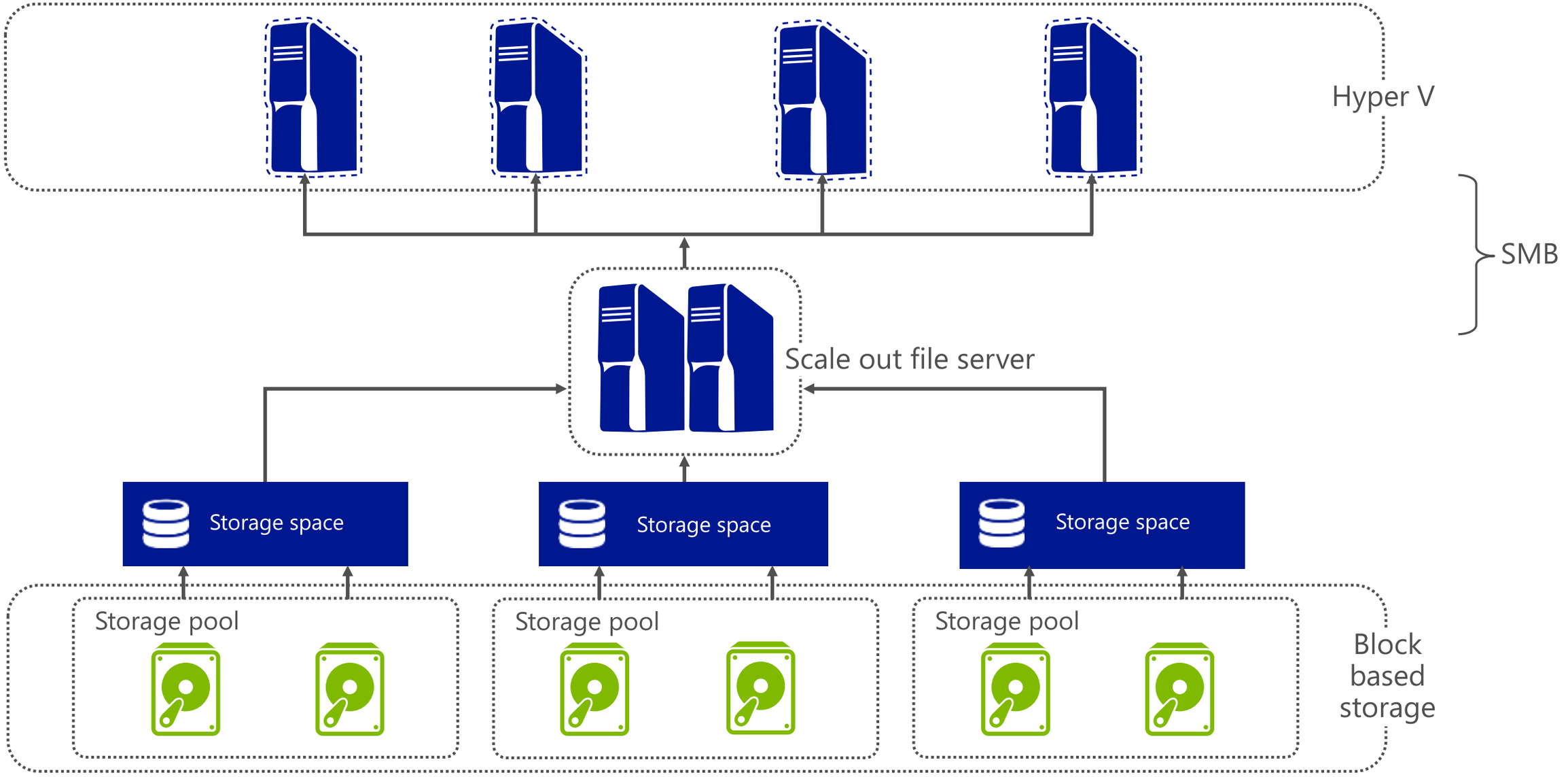
What did we want to accomplish?

- Help customers reduce storage costs.
- Build a scalable, high performance storage solution powered by Windows.
- Build SAN like capabilities in the OS.
- Help optimize SAN investments.
- Simplify storage management and provisioning.
- Innovate with partners.



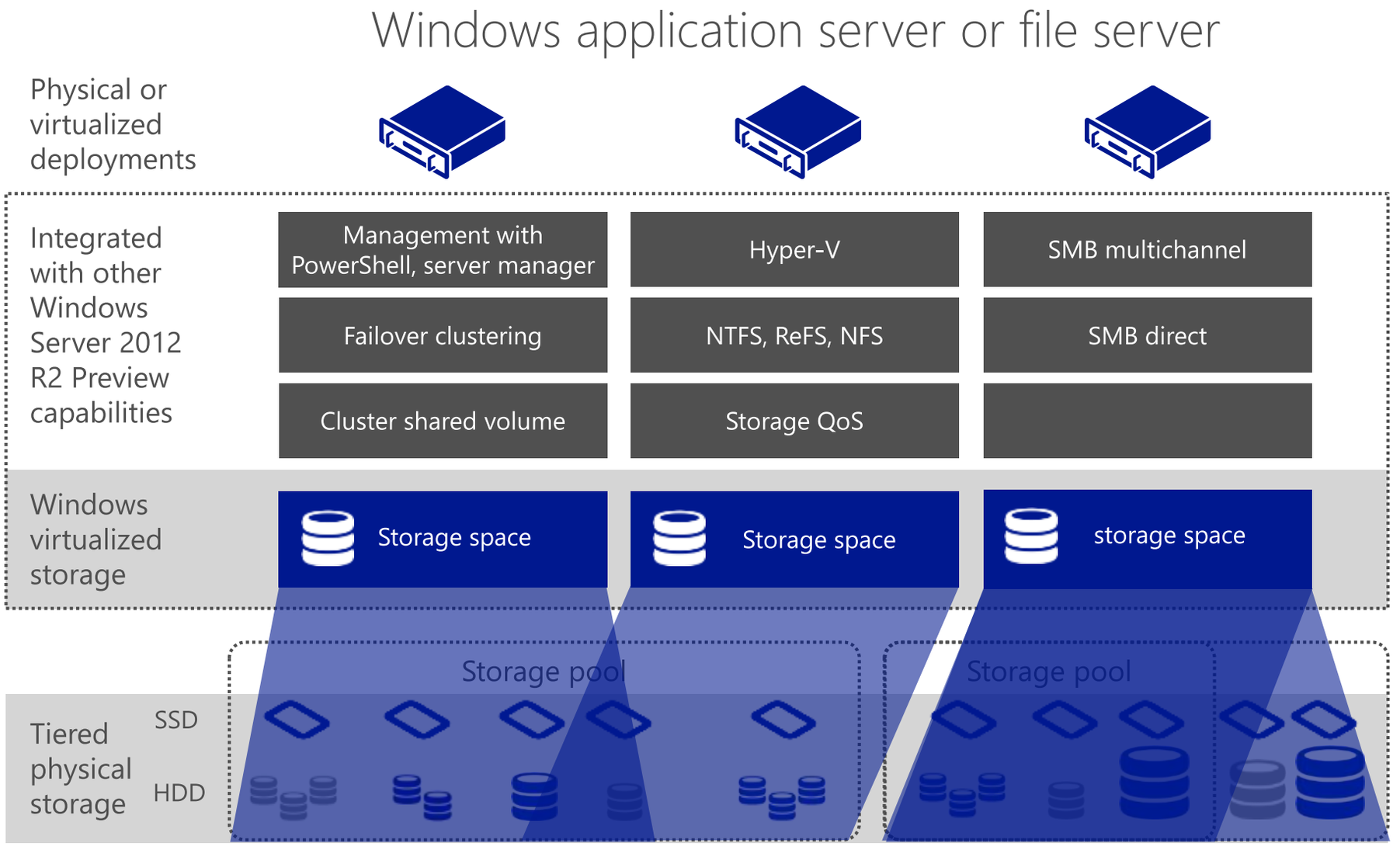
Cloud deployment storage vision

ENTERPRISE-CLASS
STORAGE PLATFORM
BUILT ON WINDOWS



ENTERPRISE-CLASS STORAGE PLATFORM BUILT ON WINDOWS

Storage Spaces

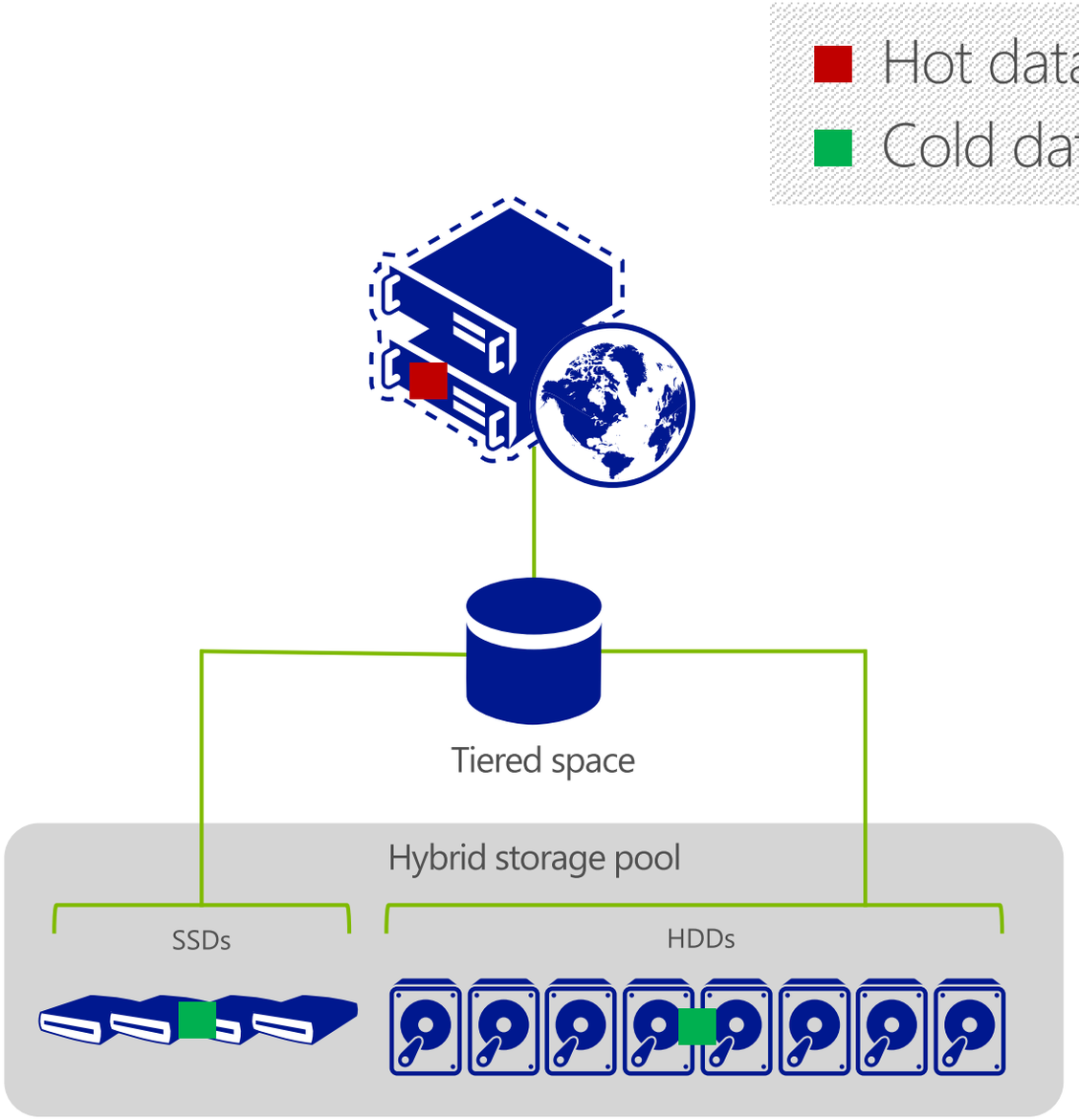


- Virtualization of storage with storage pools and storage spaces.
- Storage resilience and availability with commodity hardware.
- Data automatically tiered across memory, SSD and spinning disks.
- Write-back cache to absorb spike in random writes.
- Resiliency and data redundancy through n-way mirroring or parity mode.
- Utilization optimized through thin and trim provisioning and enclosure awareness.
- Integration with other Windows Server 2012 capabilities.
- SSD, Serial Attached SCSI (SAS) and Serial AT Attachment (SATA) interconnects.

Hybrid storage pools & tiered storage

ENTERPRISE-CLASS STORAGE PLATFORM BUILT ON WINDOWS

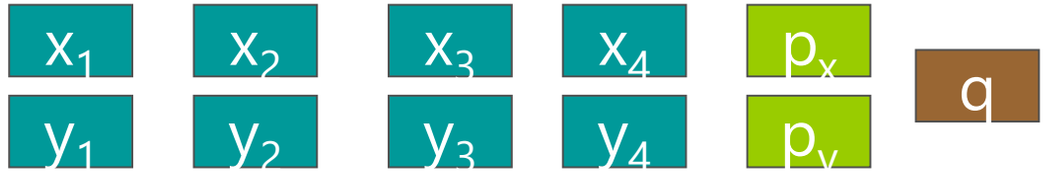
- SSDs and HDDs used as different tiers in the same storage pool.
- Windows automatically tracks data temperature and moves them at sub-file level.
- Write-back cache improves performance for real-world workloads.
- Only hot regions of a file (VHD, database, etc.) need to move to SSDs, the cold regions can reside on HDDs.
- Ability to pin files to different tiers



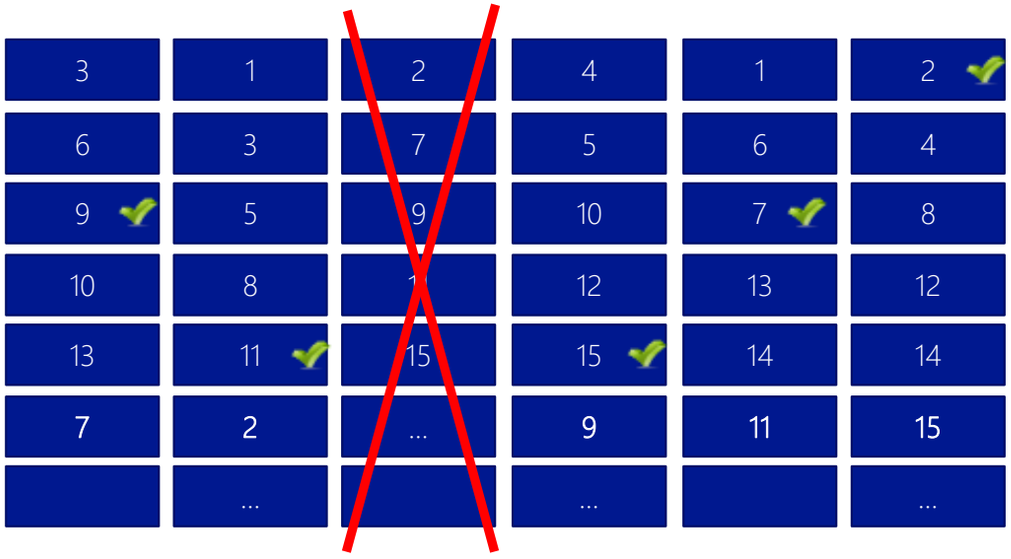
Demo: storage pools & tiered storage

Storage Spaces – Erasure Coding and Rebuild

- Support for Erasure Coding
  - Lower cost storage using LRC encoding
  - Tolerates up to 2 failures
  - Suitable for large sequential I/O
- Parallel rebuild of failed drives
  - Pseudo-random distribution weighted to favor less used disks
  - Reconstructed space is spread widely and rebuilt in parallel

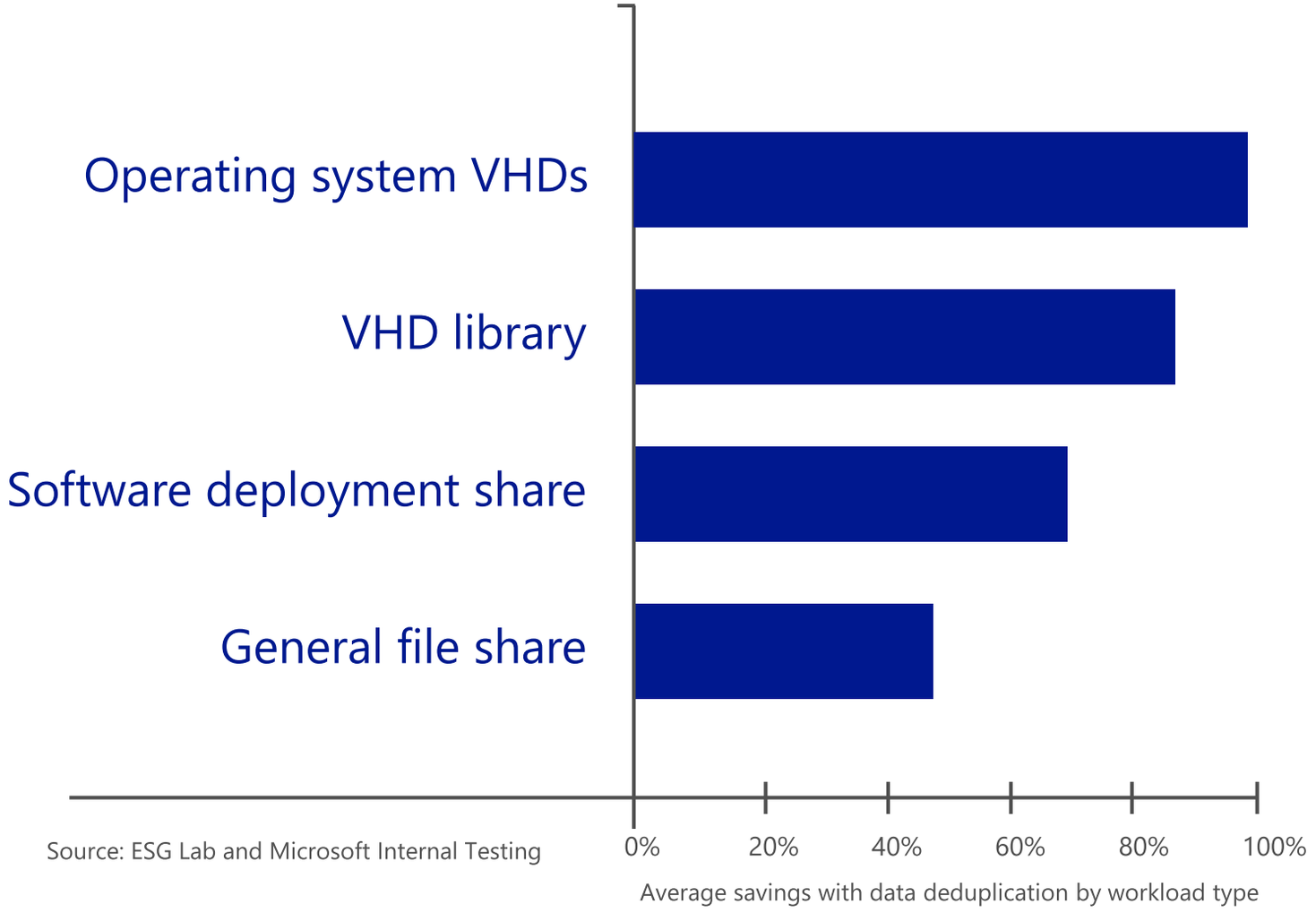


Erasure Coding in Spaces



Parallel Rebuild

Efficient storage through Data Deduplication



Source: ESG Lab and Microsoft Internal Testing

Average savings with data deduplication by workload type

Maximize capacity by removing duplicate data.

Works with live VHD/VHDX files on remote VDI storage.

Increased scale and performance.

- Better VM performance in VDI scenario
- Low CPU and memory impact.
- Configurable compression schedule.
- Transparent to primary server workload.

Improved reliability and integrity.

- Redundant metadata and critical data.
- Checksums and integrity checks.
- Increase availability through redundancy.

Faster file download times with BranchCache.

SAN vs. Microsoft solution feature comparison

Traditional storage
with FC/iSCSI storage array

- Storage tiering.
- Data deduplication.
- RAID resiliency groups.
- Pooling of disks.
- High availability.
- Persistent write-back cache.
- Copy offload.
- Snapshots.

Windows file server cluster
with storage spaces

- Storage tiering. (new with R2)
- Data deduplication. (enhanced with R2)
- Flexible resiliency options. (enhanced with R2)
- Pooling of disks.
- Continuous availability.
- Persistent write-back cache. (new with R2)
- SMB copy offload.
- Snapshots.

What is new in Windows Server 2012 R2

File Services

What's New for SMB in Windows Server 2012 R2

Feature/functionality	New or updated	Summary
Automatic rebalancing of Scale-Out File Server clients	New	This functionality improves scalability and manageability for Scale-Out File Servers. SMB client connections are tracked per file share (instead of per server), and clients are then redirected to the cluster node with the best access to the volume used by the file share. This improves efficiency by reducing redirection traffic between file server nodes. Clients are redirected following an initial connection and when cluster storage is reconfigured.
Improved performance of SMB Direct (SMB over RDMA)	Updated	Improves performance for small I/O workloads by increasing efficiency when hosting workloads with small I/Os (such as an online transaction processing (OLTP) database in a virtual machine). These improvements are evident when using higher speed network interfaces, such as 40 Gbps Ethernet and 56 Gbps InfiniBand.
Improved SMB event messages	Updated	SMB events now contain more detailed and helpful information. This makes troubleshooting easier and reduces the need to capture network traces or enable more detailed diagnostic event logging. By default, the most relevant event channels are turned on, so you instantly capture all of the essential information. In addition, some events now include details on configuration and troubleshooting solutions.
VHDX files as shared storage for guest clustering	New	Simplifies the creation of guest clusters by using shared VHDX files for shared storage inside the virtual machines. You can use this feature with VHDX files that are stored in Cluster Shared Volumes (CSV) or SMB Scale-Out file shares.

What's New for SMB in Windows Server 2012 R2

Feature/functionality	New or updated	Summary
Hyper-V Live Migration over SMB	New	Enables you to perform a live migration of virtual machines by using SMB 3.0 as a transport. This allows you to take advantage of key SMB features, such as SMB Direct and SMB Multichannel, by providing high speed migration with low CPU utilization.
Improved SMB bandwidth management	New	Enables you to configure SMB bandwidth limits to control different SMB traffic types. There are three SMB traffic types: default, live migration, and virtual machine.
Support for multiple SMB instances on a Scale-Out File Server	New	Provides an additional instance on each cluster node in Scale-Out File Servers specifically for CSV traffic. A default instance can handle incoming traffic from SMB clients that are accessing regular file shares, while another instance only handles inter-node CSV traffic. This feature improves scalability and reliability of traffic between CSV nodes.
SMB 1.0 is now an optional feature	Updated	The SMB 1.0 features, including the legacy computer browser service and Remote Administration Protocol (RAP), are now separate and can be eliminated. These features are still enabled by default, but if you have no older SMB clients, such as Windows XP or Windows Server 2003, you can remove the SMB 1.0 features to increase security and potentially reduce patching.

What's New in DFS Replication in Windows Server 2012 R2

Feature/functionality	New or updated?	Description
Windows PowerShell module for DFS Replication	New	Provides Windows PowerShell cmdlets for performing the majority of administration tasks for DFS Replication, as well as new functionality. 42 new cmdlets
Database cloning for initial sync	New	Provides support for bypassing initial replication when creating new replicated folders, replacing servers, or recovering from a disaster. 500GB and 100,000 files once took **13 hours to initial sync**. **Now** takes as little as **2 minutes**. 64TB and 70M files would take 5 months. Now takes as little as 32 hours
Database corruption recovery	New	Provides support for rebuilding corrupt databases without unexpected data loss caused by non-authoritative initial sync.
Cross-file RDC disable	New	Provides the option to disable cross-file remote differential compression (RDC) between servers.
File staging tuning	New	Provides the option to configure variable file staging sizes on individual servers.
Preserved file restoration	New	Provides the capability to restore files from the ConflictAndDeleted and PreExisting folders.
Unexpected shutdown database recovery improvements	Updated	Enables automatic recovery after a loss of power or an unexpected stopping of the DFS Replication service.
Membership disabling improvements	Updated	Stops DFS Replication private folder cleanup when disabling a server's membership in a replicated folder.

What is new in Windows Server 2012 R2

Failover clustering

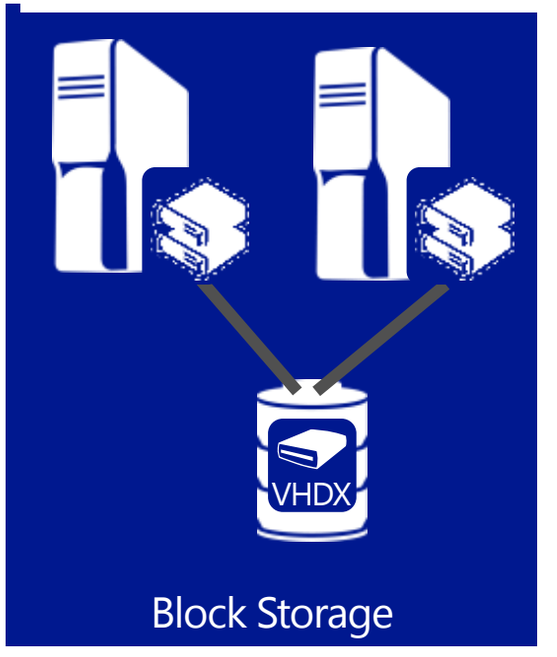
Guest Clustering with Shared Virtual Disks

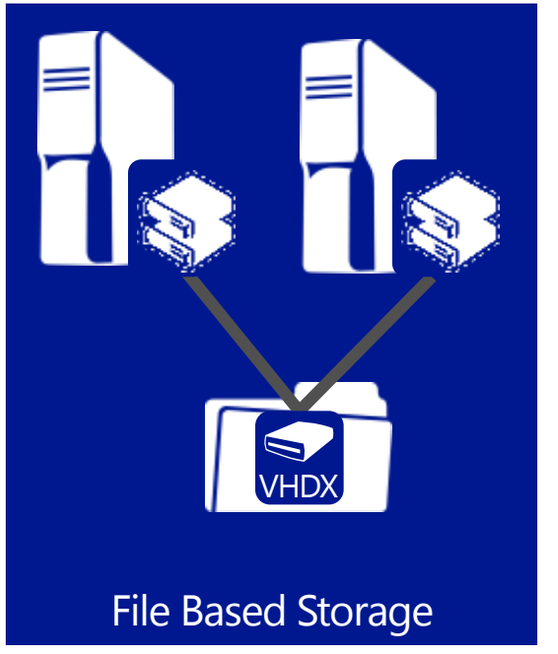
Guest Clustering

- Guest Clustering with commodity storage
- Sharing VHDX files provides shared storage for Hyper-V Failover Clustering
- Maintains separation between infrastructure and tenants

Virtual SAS

- VM presented a shared virtual SAS disk
- Appears as shared SAS disk to VM
- Used for data disk only





Guest Clustering

- Guest Clustering shared storage deployment options with Windows Server 2012 R2:

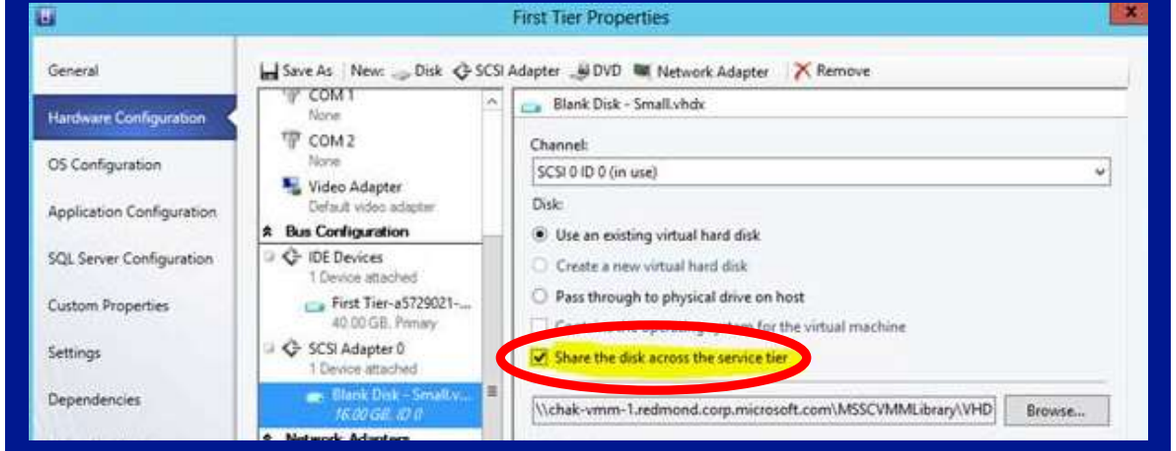
	Windows Server 2012	Windows Server 2012 R2
Fibre Channel	✓	✓
iSCSI	✓	✓
File (SMB)	✓	✓
Shared VHDX		✓

Creating Shared VHDX Example

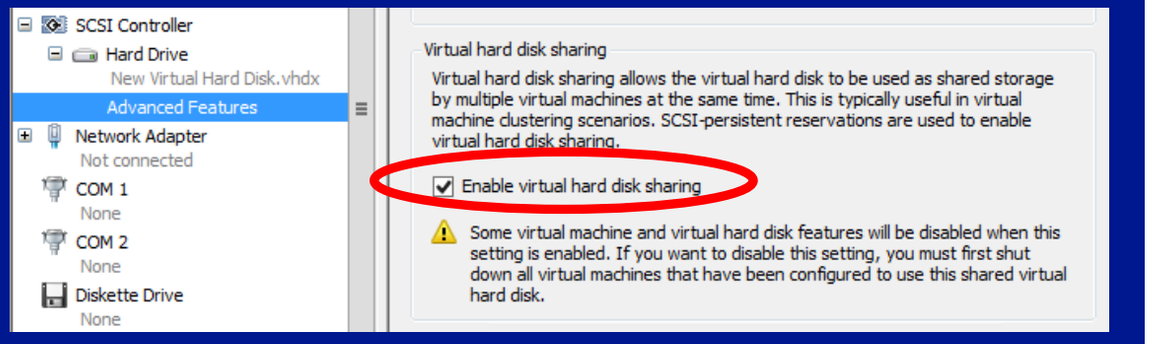
Example of creating and attaching a shared VHDX to two existing VMs

```
PS C:\> New-VHD -Path C:\ClusterStorage\Volume1\Shared.VHDX -Fixed -SizeBytes 30GB

PS C:\> Add-VMHardDiskDrive -VMName Node1 -Path C:\ClusterStorage\Volume1\Shared.VHDX -ShareVirtualDisk

PS C:\> Add-VMHardDiskDrive -VMName Node2 -Path C:\ClusterStorage\Volume1\Shared.VHDX -ShareVirtualDisk
```

SCVMM

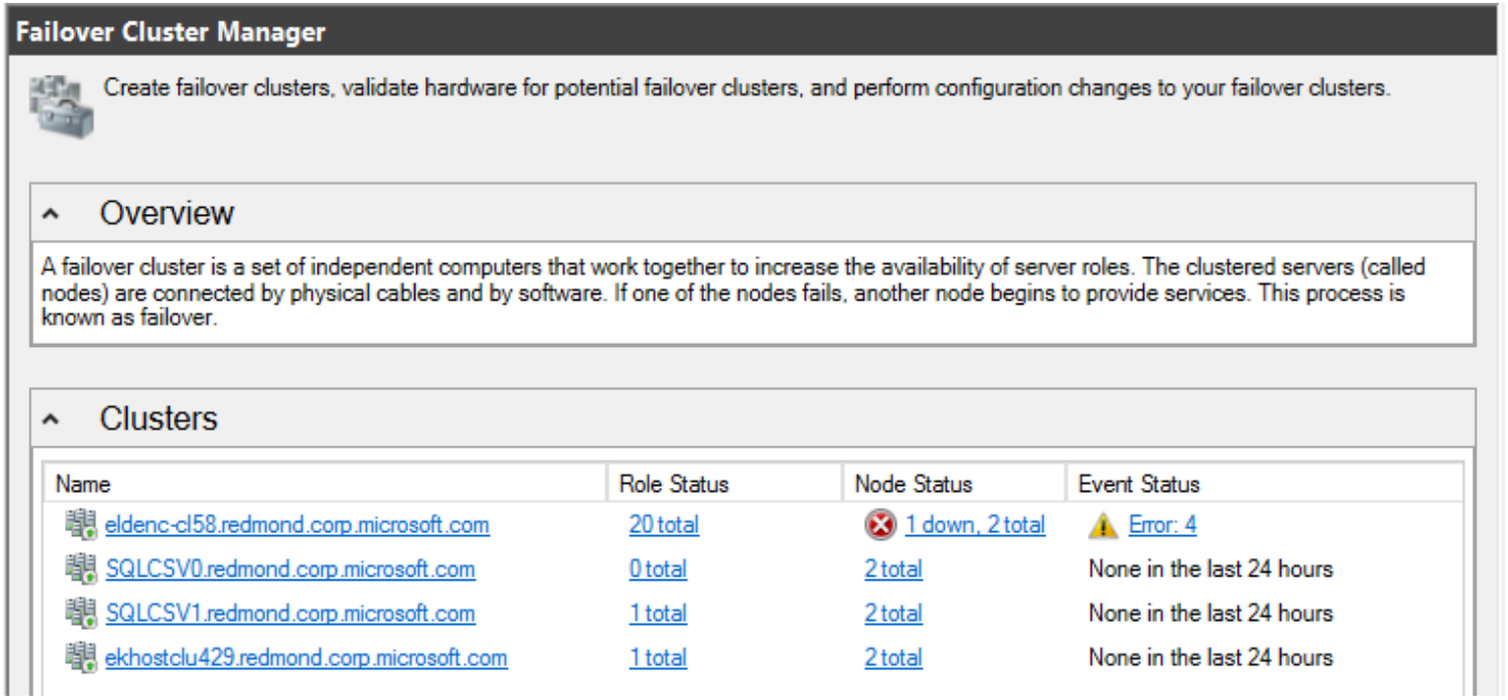


Hyper-V VM Settings



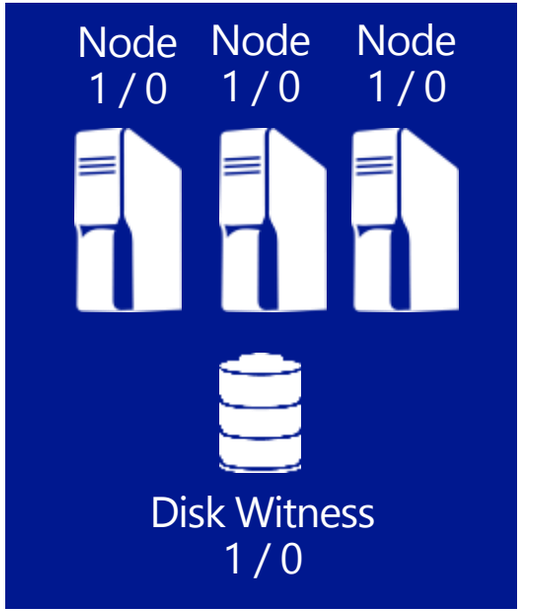
Cluster Dashboard

- New Cluster Dashboard for Status at a Glance
- Focused at multi-cluster management



Dynamic Witness

- Witness vote dynamically/automatically adjusted based on cluster membership with dynamic quorum
  - Odd node votes (3) + no witness vote (0) = 3
  - Even node votes (2) + witness vote (1) = 3
- Automatic functionality



New Recommendation

Always configure a witness with Windows Server 2012 R2

Clustering will determine when it is best to use the Witness

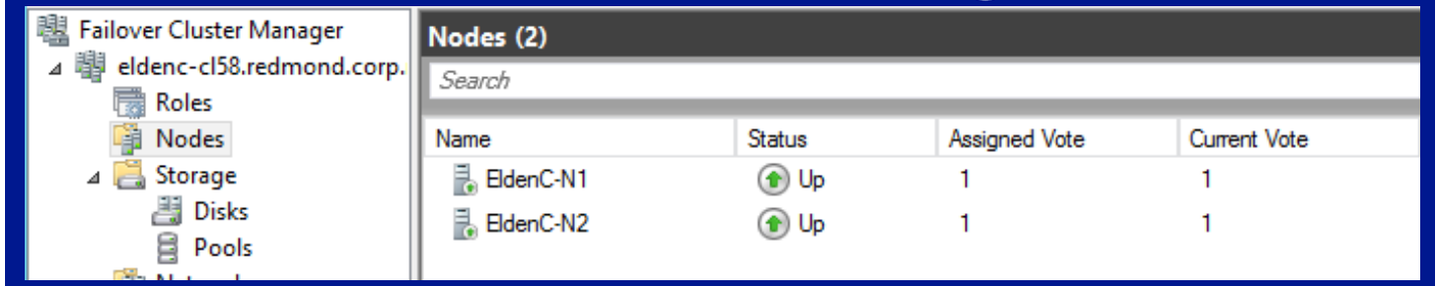
Configure Disk Witness if shared storage, otherwise FSW

Intuitive Quorum Configuration UI

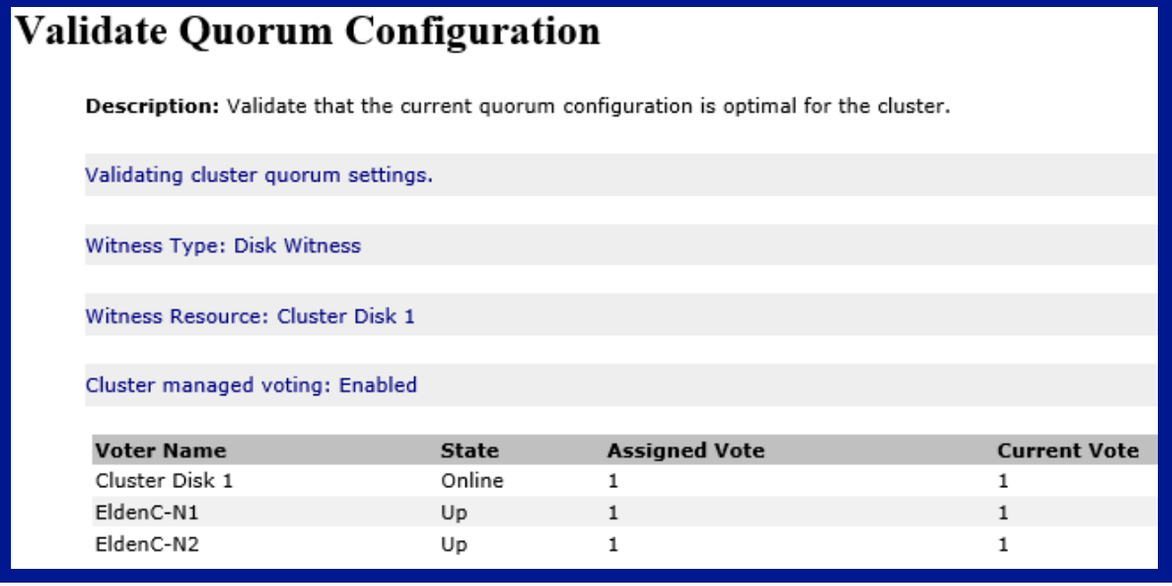
- Node vote weights and dynamic quorum status easy & quick to view

- Removed legacy concepts of ‘quorum modes’
  - ~~Node Majority~~
  - ~~Node and Disk Majority~~
  - ~~Node and File Share Witness Majority~~

Failover Cluster Manager



Validate



Validate Quorum Configuration

Description: Validate that the current quorum configuration is optimal for the cluster.

Validating cluster quorum settings.

Witness Type: Disk Witness

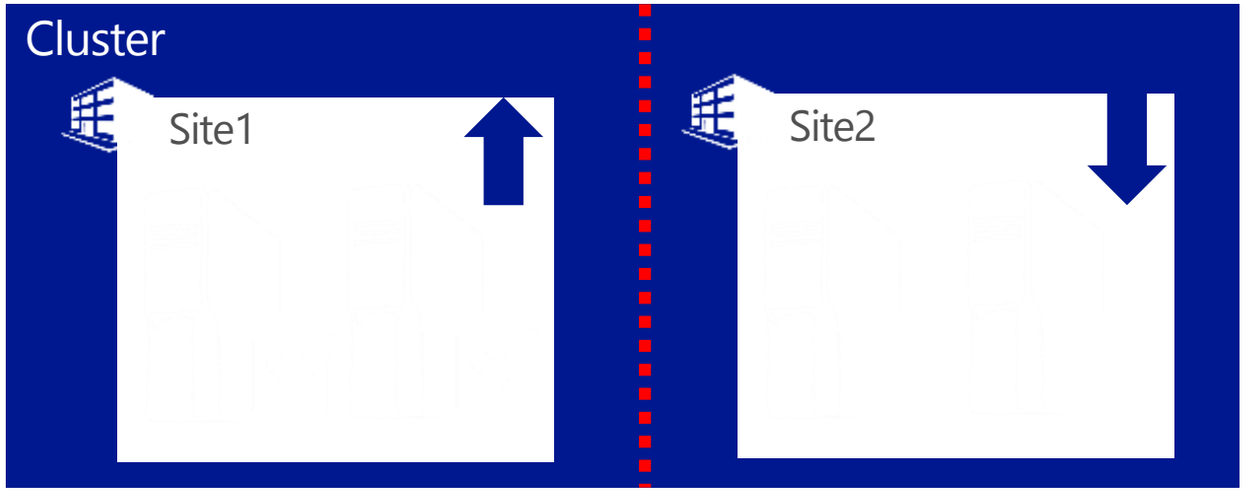
Witness Resource: Cluster Disk 1

Cluster managed voting: Enabled

Voter Name	State	Assigned Vote	Current Vote
Cluster Disk 1	Online	1	1
EldenC-N1	Up	1	1
EldenC-N2	Up	1	1

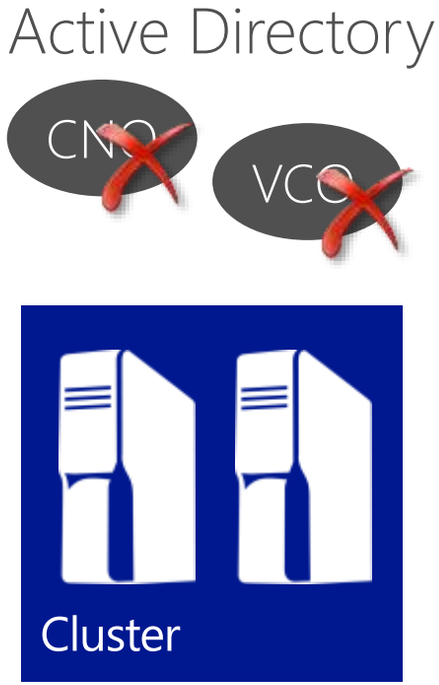
Tie Breaker

- Cluster will survive simultaneous 50% loss of votes
  - Balanced multi-site clusters with complete site partition
- One site automatically elected to win
  - Site without `LowerQuorumPriorityNodeID` cluster common property wins
  - Nodes in the other site drop out of the cluster



Reducing Cluster Dependencies

- Active Directory-detached cluster Network Names
  - Enables creating a cluster without computer objects
  - `New-Cluster –AdministrativeAccessPoint DNS`
- Simplifies cluster deployments
  - Best fit for SQL Server Clusters
- Flexibility to create clusters with or without Active Directory integration
  - Still required that Nodes are domain joined



Considerations with AD Agnostic Clusters

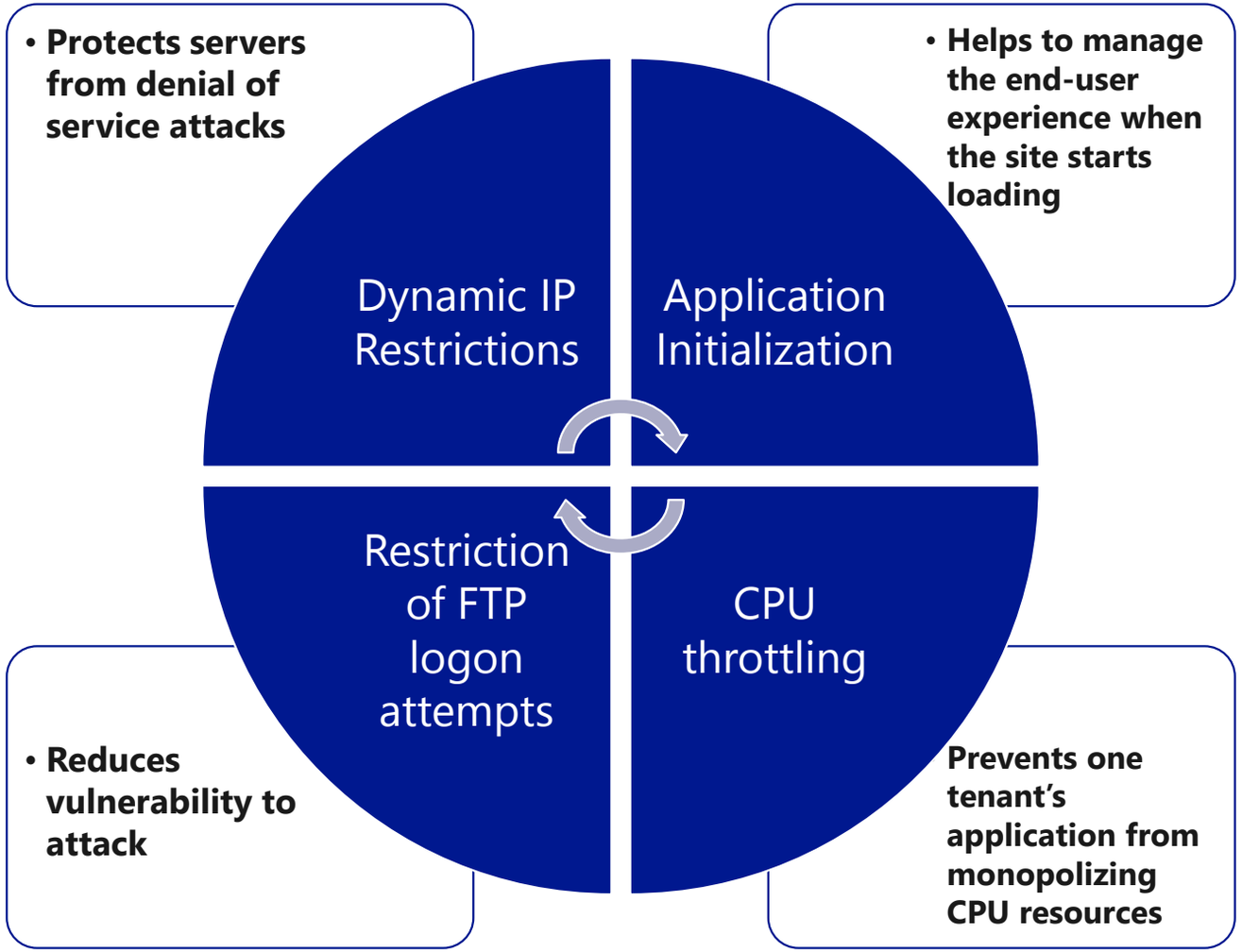
- What to consider when choosing a model
  - No computer objects, means no Kerberos authentication to the name
  - NTLM only client authentication against cluster names
    - Intra-cluster authentication still leverages Kerberos

Role	Position	Notes
MSMQ Clusters	Not Supported	MSMQ stores properties in AD
File Server Clusters	Not Recommended	Kerberos for SMB preferred
Hyper-V Clusters	Not Recommended	No live migration support
SQL Server Clusters	Supported	Best fit if using SQL Authentication

What is new in Windows Server 2012 R2

IIS

High-performance web applications

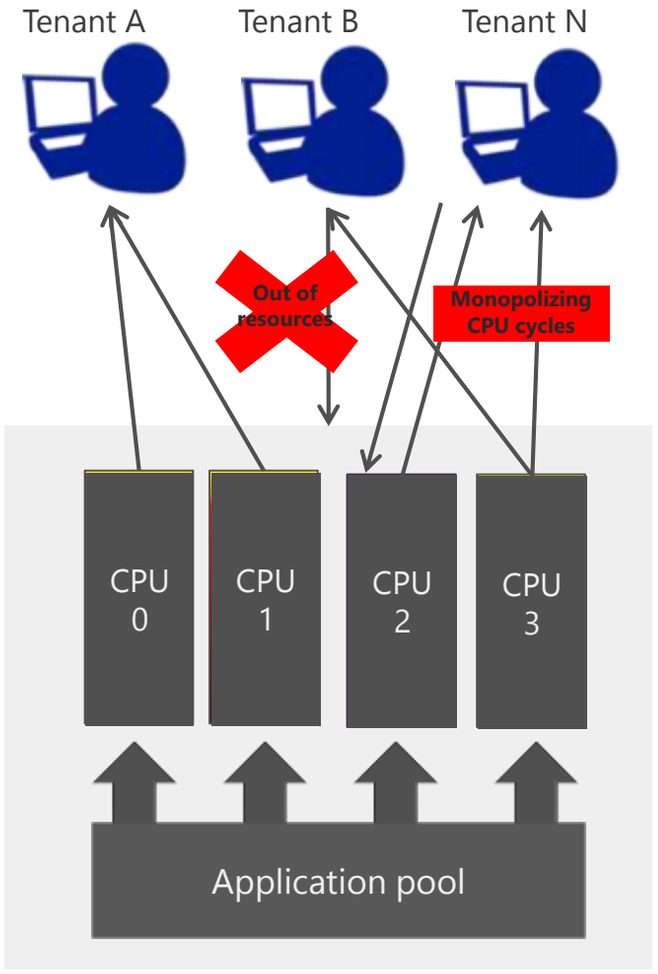


CPU Throttling

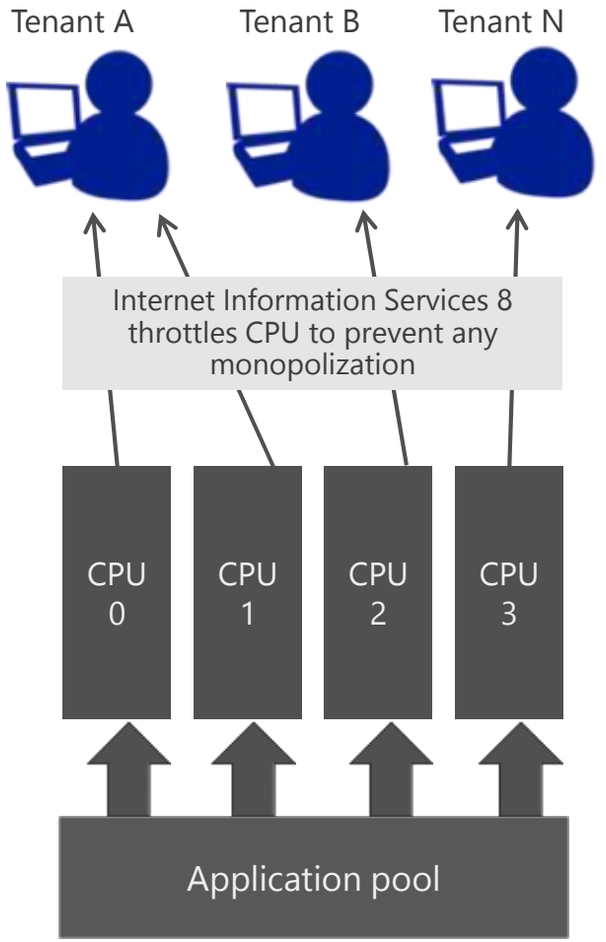
Benefits

- Prevents one tenant's application from monopolizing CPU resources
- Sets maximum CPU consumption per application pool
- Sandboxing process controls resource consumption per site
- By defining different-sized sandboxes for different tenants, hosters can create additional business opportunities based on resource consumption

Earlier scenario



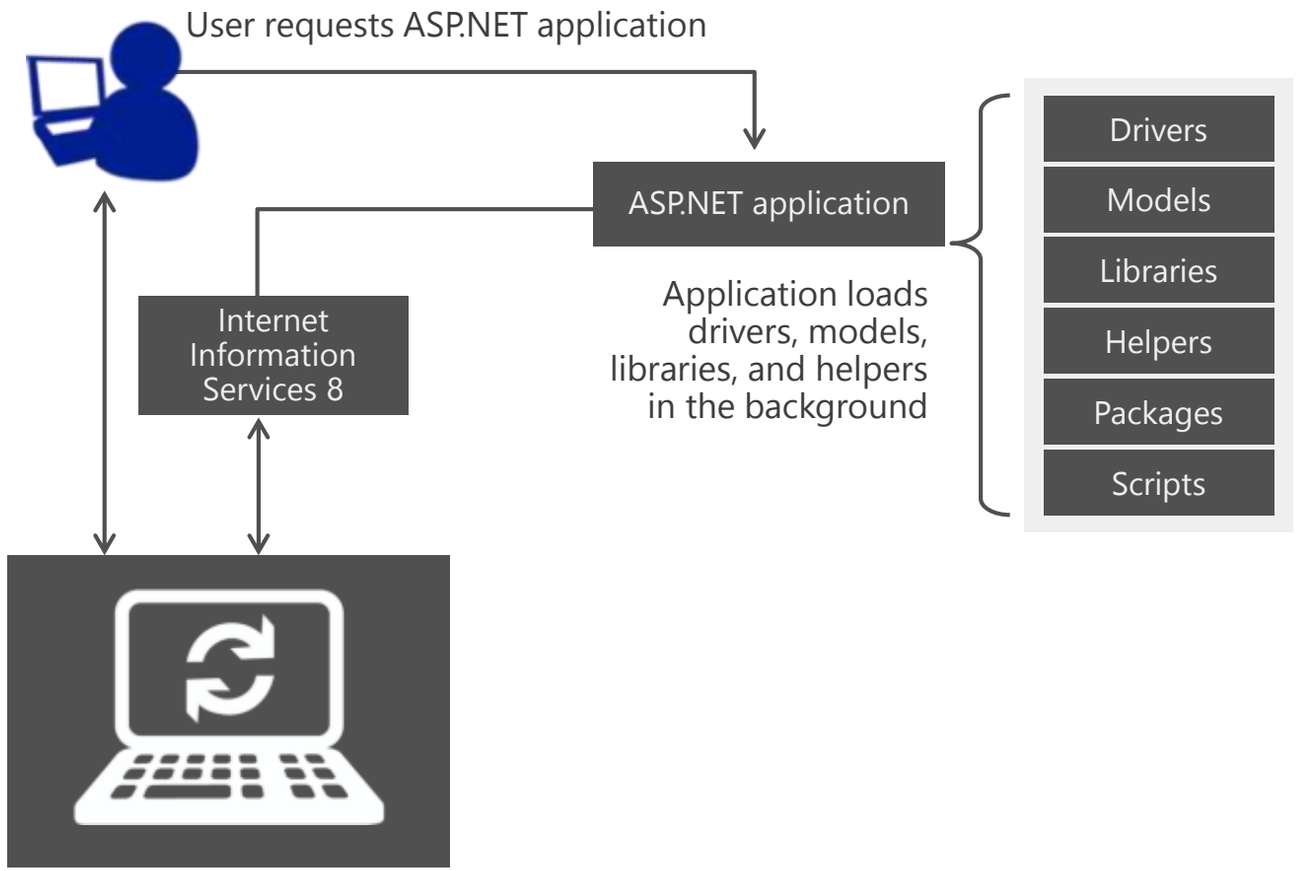
Windows Server 2012 R2 Preview



Application Initialization

Benefits

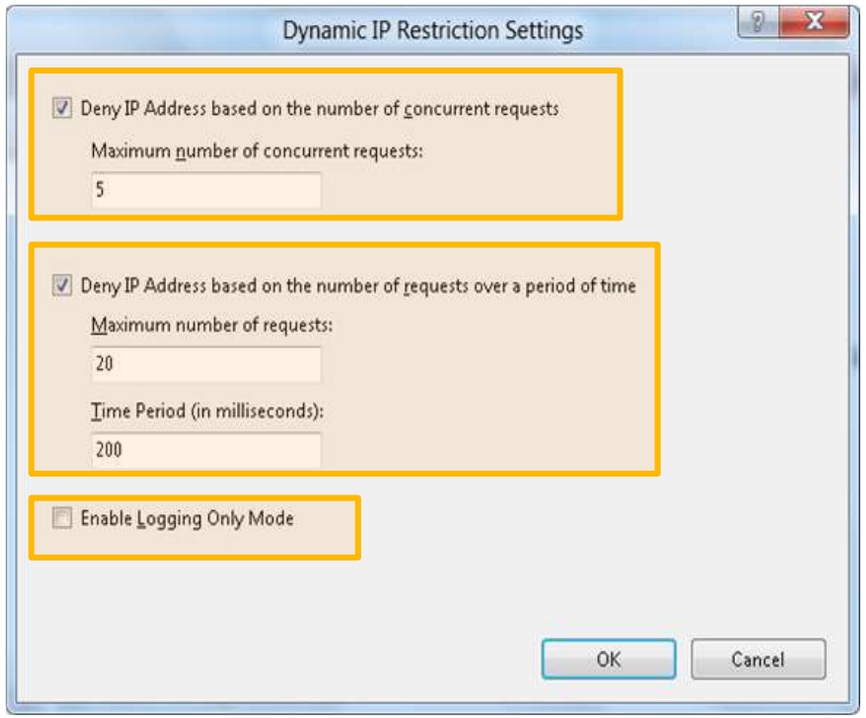
- Helps to manage the end-user experience when the site starts loading
- Returns static content as a splash page until an application has completed its initialization tasks
- Proactively performs initialization tasks for an application when it starts, to improve performance of first requests



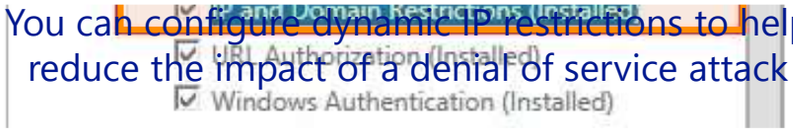
Dynamic IP Restrictions

Benefits

- Protects servers from denial of service attacks
- Filters and blocks IP address dynamically
- Specifies action when Internet Information Services blocks requests
- With Logging Only Mode, helps to determine potential impact for legitimate users
- Rules can be configured as static or dynamic



You can configure dynamic IP restrictions to help reduce the impact of a denial of service attack

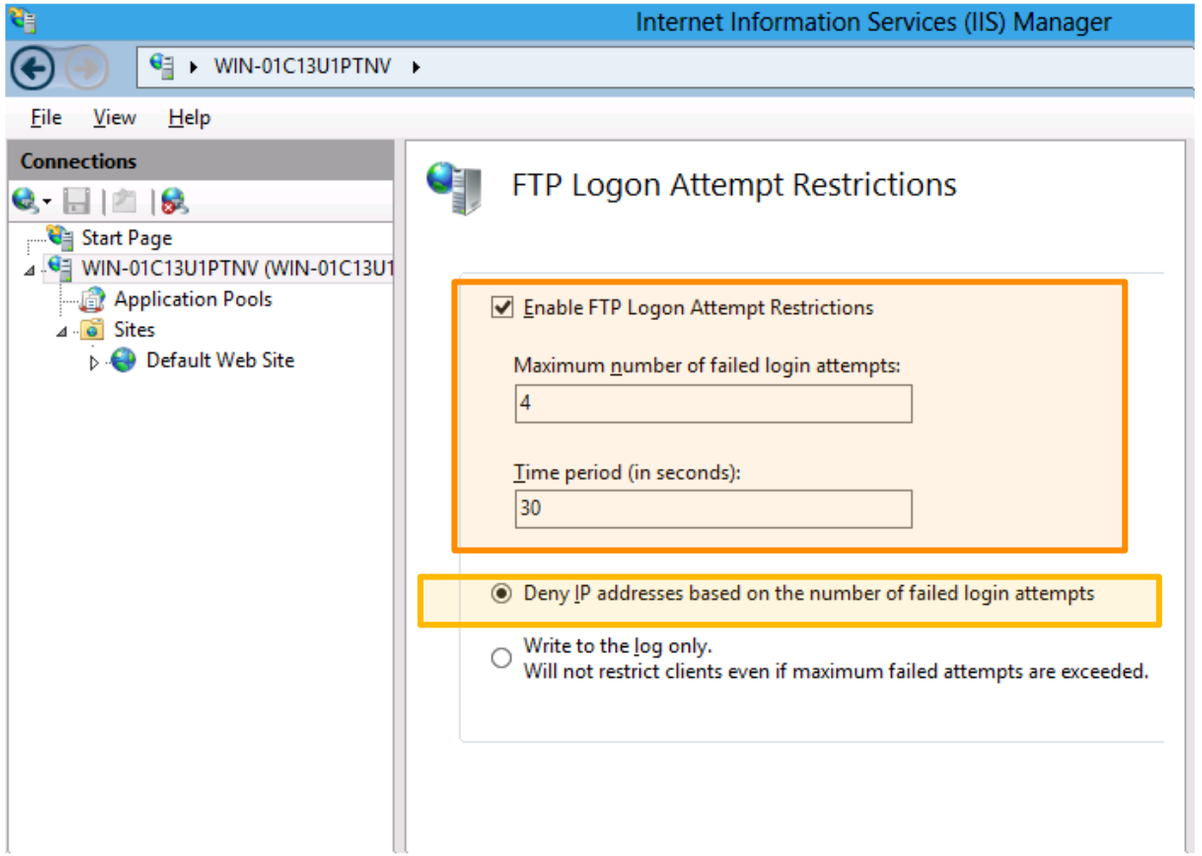


Dynamic IP restriction is an optional feature that must be explicitly installed using Server Manager

Restriction of FTP logon attempts

Benefits

- Reduces vulnerability to attack
- Dynamically limits the number of logon attempts
- Server blocks access from malicious users
- Log files track suspicious logon attempts

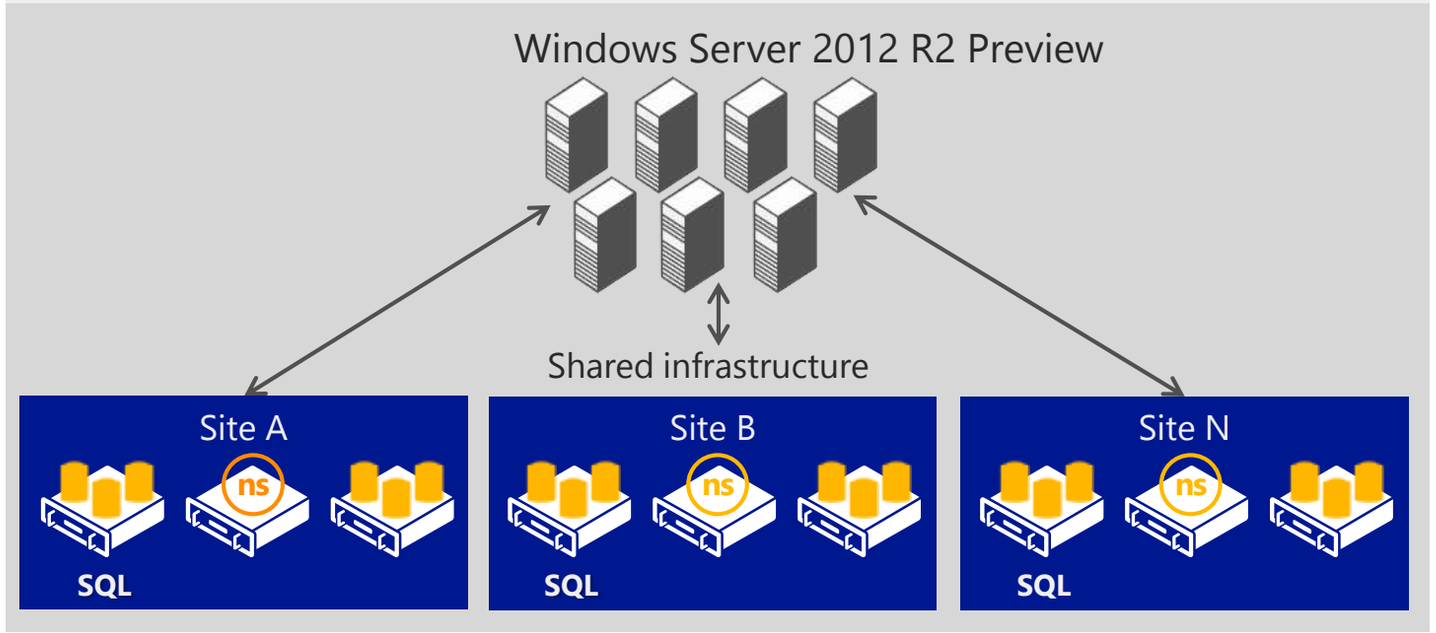


FTP network security can be configured to help reduce the impact of a denial of service attack

High-density websites

Challenges for running high-density websites

- Isolation and security
- Scalability
- Centralized support
- Simplified management
- Extensibility



Features for enabling and managing the multitenant environment

- Server Name Indicator
- Centralized SSL Certificate Support
- NUMA scalability

Server Name Indicator

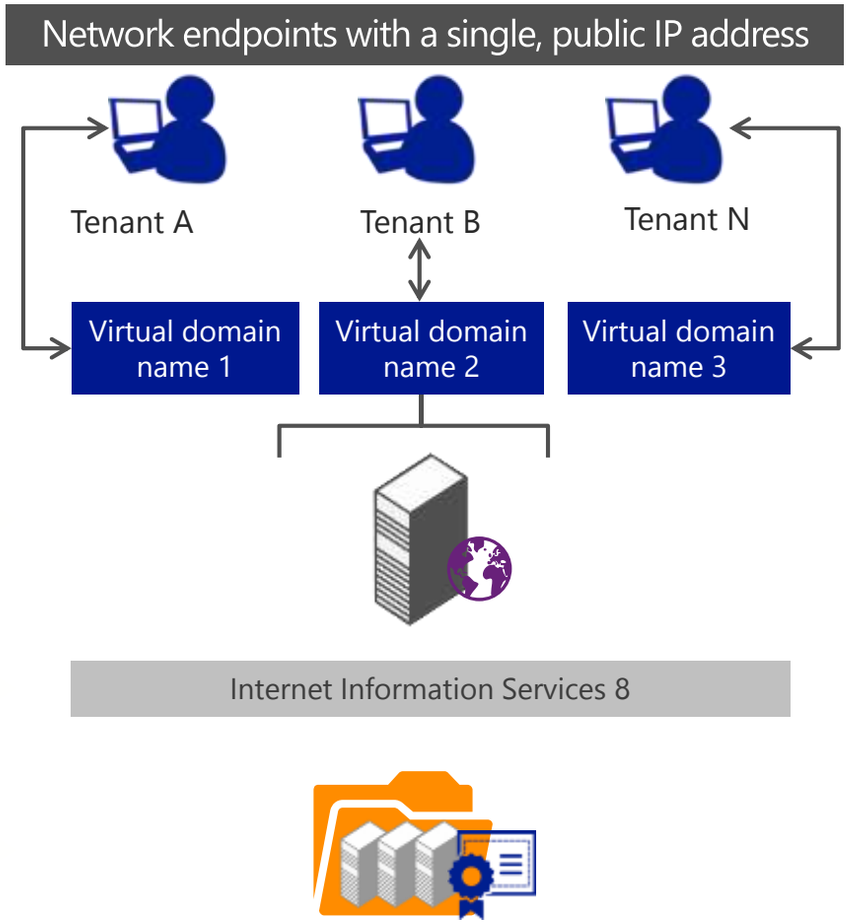
Benefits

- Easier certificate management
- Reduced hosting costs
- Increased site density
- Single, shared IP address

Multiple websites hosted on a single web server

Hosting-friendly web sever platform

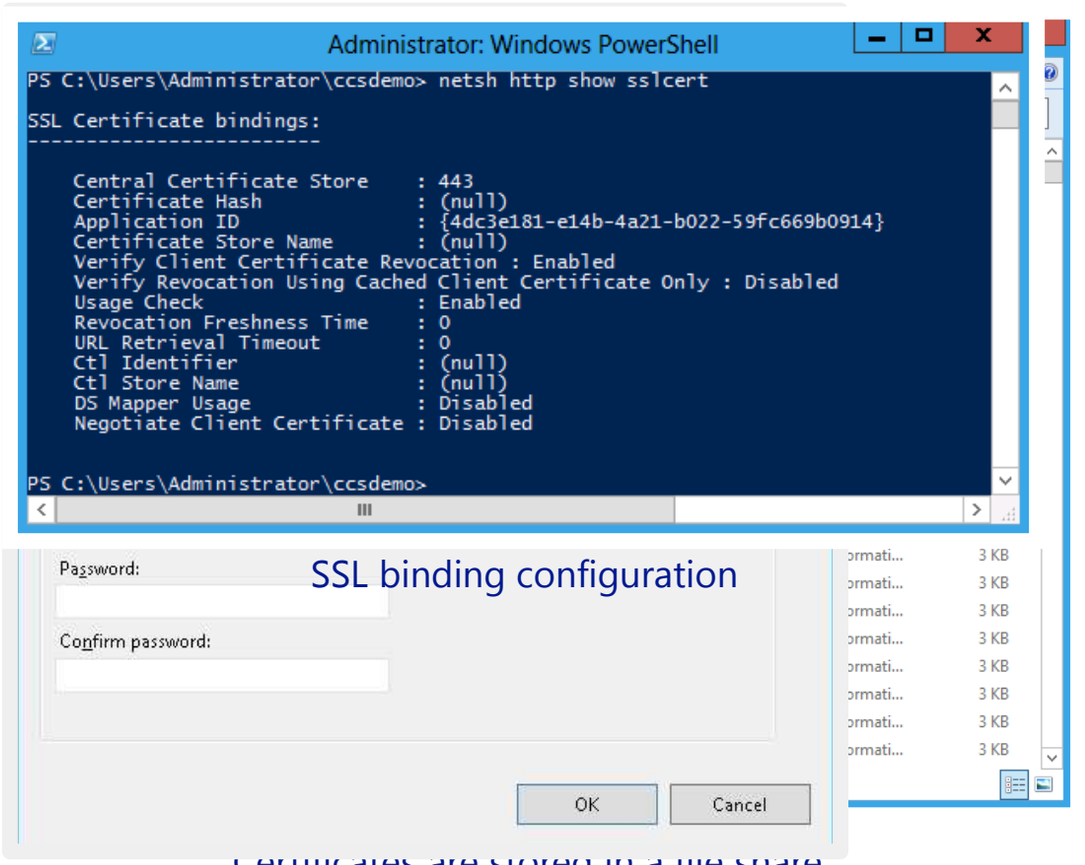
“Web hosting certificate store” can contain thousands of SSL certificates



Centralized SSL Certificate Support

Certificate management

- Shared SSL certificates are stored centrally
- New servers do not need certificate import
- SSL binding is implied by naming convention
- Only one implicit SSL binding to manage, regardless of number of configured SSL sites
- Certificate is updated by copying and replacing the existing file



SSL binding configuration

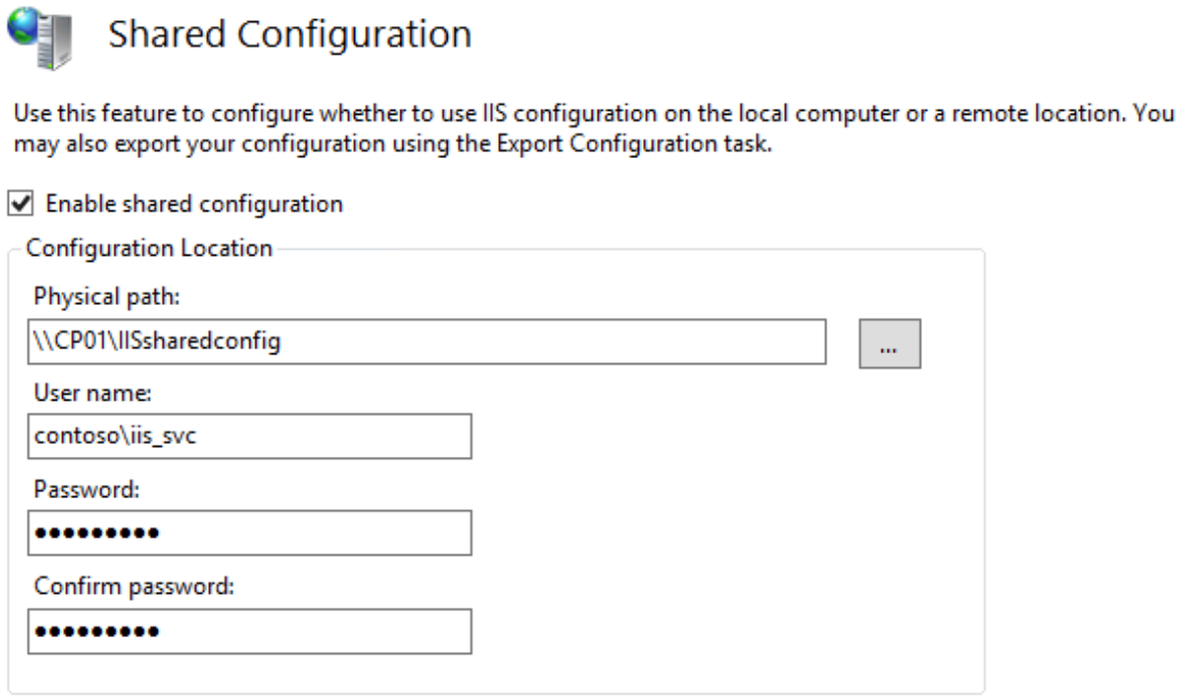
Certificates are stored in a file share

Internet Information Services is configurable to automatically bind to SSL certificates stored in the shared folder

Consistency through shared configuration

Benefits

- IT can maintain a consistent configuration across web servers
- Reduces time to operational readiness
- IT can automatically share encryption keys across servers for session state load distribution



Specify a shared location to store configurations

What is new in Windows Server 2012 R2

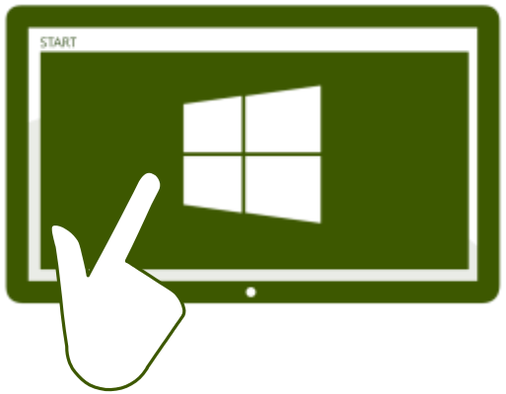
RDS -What is a rich user experience?

Adaptive graphics remoting based on content type

Crisp text always

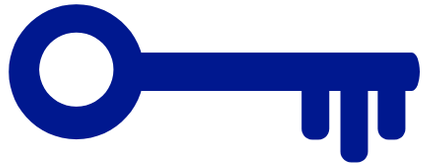
Aero always on, rich new Windows UI

Reconnect feature for ease of movement across devices



Ability to serve desktop apps to Windows RT tablet users

Full multitouch and gesture remoting



Full single sign-on

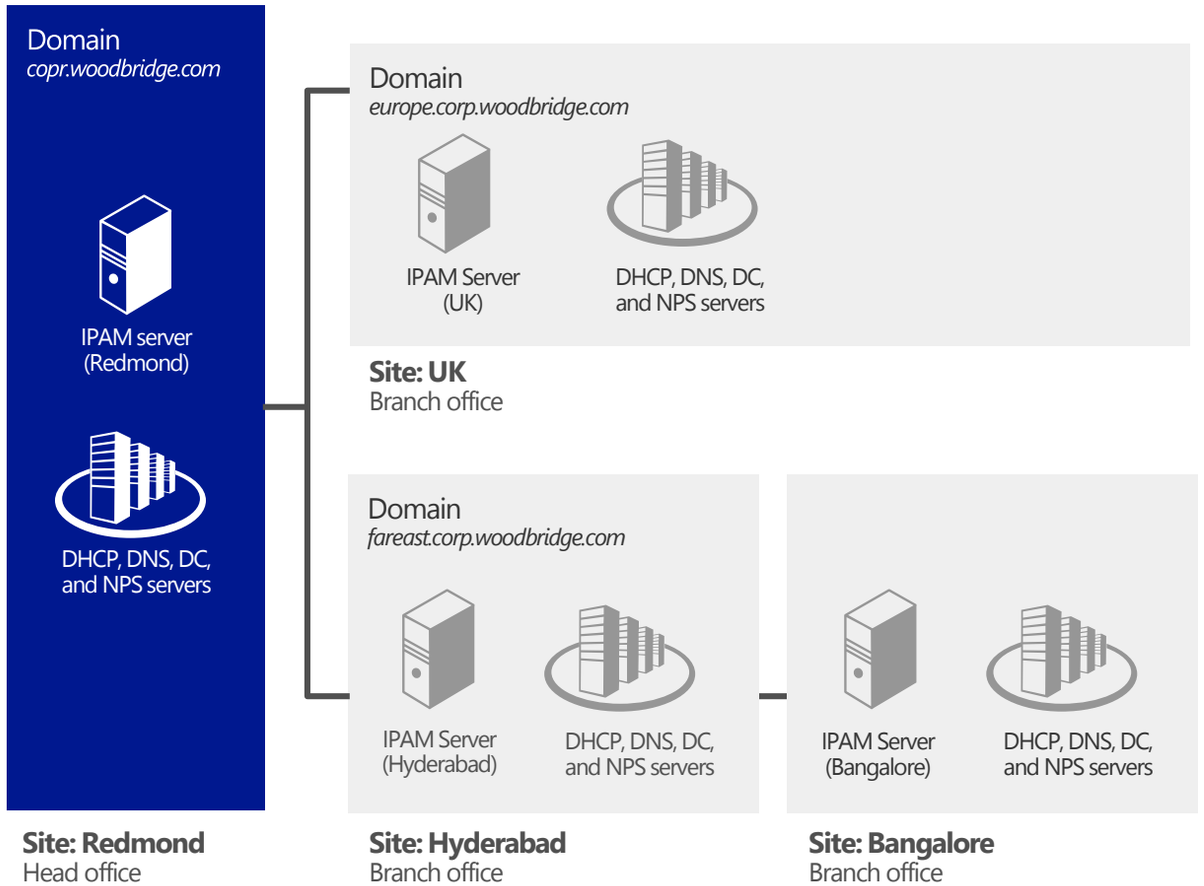
RemoteApp programs integrate seamlessly with local desktop

Windows Server 2012 R2

IP Address Management (IPAM)

- Inbox feature for integrated management of IP addresses, domain names, and device identities
- New in R2: virtualized IP address space management
- Tightly integrates with Microsoft DNS and DHCP servers
- Provides custom IP address space display, reporting, and management
- Audits server configuration changes and tracks IP address use
- Migrates IP address data from spreadsheets or other tools
- Remote SQL support

IPAM distributed architecture



Group Policy caching

- Windows Server 2012 R2 , when Group Policy gets the latest version of a policy from the domain controller, it writes that policy to a local store. Then if Group Policy is running in synchronous mode the next time the computer reboots, it reads the most recently downloaded version of the policy from the local store, instead of downloading it from the network. This reduces the time it takes to process the policy. Consequently, the boot time is shorter in synchronous mode. This is especially important if you have a latent connection to the domain controller, for example, with DirectAccess or for computers that are off premises. This behavior is controllable by a new policy called Configure Group Policy Caching.