Microsoft

SQL Server 2016 and Windows Server 2016: Better Together

Technical white paper (April 2016)

Copyright

Contents

Introduction

Windows Server and Microsoft SQL Server teams are collaborating closely to ensure that the combination of these products is greater than the sum of their parts. IT decision makers can take advantage of a better enterprise data platform enabled by several key Windows Server 2016 features working in concert with SQL Server 2016 features. Both products offer best-in-class performance, scalability, availability, and security. With Windows Server and SQL Server, Microsoft is pushing the limits of hardware capabilities and bringing the latest enterprise technologies to market. Both products are offering improvements to availability and disaster recovery features, providing an unprecedented level of interoperability in a variety of environments. Concepts such as Just Enough Administration (JEA) and new technologies in access control and encryption ensure that data is protected from threats and risks—both external and internal. Simply put, Windows Server 2016 and SQL Server 2016, both world-class products on their own, are better together.

Performance and scale

Raised caps on memory and core counts

Windows Server stands on the leading edge of vertical scalability while SQL Server continues to keep pace with operating system capabilities, fully supporting the maximum memory and core count enabled by Windows Server. This is particularly effective in large-scale data warehouse scenarios, where massive symmetric multiprocessing (SMP) scale and terabytes of memory are the key to optimal performance.

Latest technologies

Both Windows Server and SQL Server are continuously evolving in order to support the latest enterprise technologies, thus providing cutting-edge performance and availability. Examples of these technologies include Storage Class Memory (SCM) and Storage Spaces Direct.

SCM, such as Non-Volatile Dual Inline Memory Modules (NVDIMM), is an emerging technology. Essentially non-volatile memory for a system, SCM is protected from data loss in the event of power interruption, system failures, and restarts. The implications of durable memory capabilities in a server operating system and data management system are vast, and apt to bring sweeping changes to the enterprise. One such example is how SQL Server has leveraged this technology to eliminate some I/O bottlenecks when persistent memory is present.

Storage Spaces Direct is a new innovation in storage technology that brings high availability and scalability to servers with local storage, including solid state disks.

> *Storage Spaces Direct enables service providers and enterprises to use industry standard servers with local storage to build highly available and scalable software defined storage. Using servers with local storage decreases complexity, increases scalability, and enables use of storage devices that were not previously possible, such as SATA solid state disks for lower cost flash storage, or NVMe solid state disks for better performance. Storage Spaces Direct removes the need for a shared SAS fabric, simplifying deployment and configuration. Instead it uses the network as a storage fabric, leveraging our investments in SMB3 and SMB*

Direct (RDMA) for high-speed and low-latency storage. To scale out, simply add more servers to increase storage capacity and I/O performance.[1]

Each currently in development (as of the writing of this paper), these particular technologies represent areas of enhanced interoperability between Windows Server and SQL Server as well as the ongoing evolution of both products.

Domain-independent high availability

Traditionally, Windows Server Failover Clustering and SQL Server availability groups have required nodes to be members of the same Active Directory Domain. This domain requirement restricts organizations seeking to implement availability and/or recovery solutions, but which do not have a homogenous domain environment. There are several scenarios in which high availability (HA)/disaster recovery (DR) is needed, but single domain membership is impractical or not possible. Windows Server 2016 enables Failover Clusters without the need for membership to the same domain, domain trust, or even in environments without any domain membership. SQL Server 2016 builds on this with the ability to have domain independent availability groups, bringing the full AlwaysOn feature set to a larger audience.

Domain-independent high availability represents an unprecedented level of interoperability for data solutions in a variety of environments. This capability opens the door for a number of scenarios for which HA was not viable:

Scenario: Multi-national enterprise

It is not uncommon for data centers in different geographical locations to be in different domains, especially in the cases of operational centers located in different countries. These infrastructures are generally managed by disparate IT teams/orgs, often independent of each other. Access to these resources is usually restricted to regional or local business units. An effective availability or disaster recovery solution (particularly DR) is based upon failover resources being in separate physical locations. As seen in the figure below, two or more operational centers spread throughout the world are now able to utilize AlwaysOn features despite resources being joined to completely different domains.

[1] Microsoft Windows Server Team. "Moving forward in the cloud world with software-defined storage." Windows Server Blog. 29 October 2015. https://blogs.technet.microsoft.com/windowsserver/2015/10/29/moving-forward-in-the-cloud-world-with-software-defined-storage/

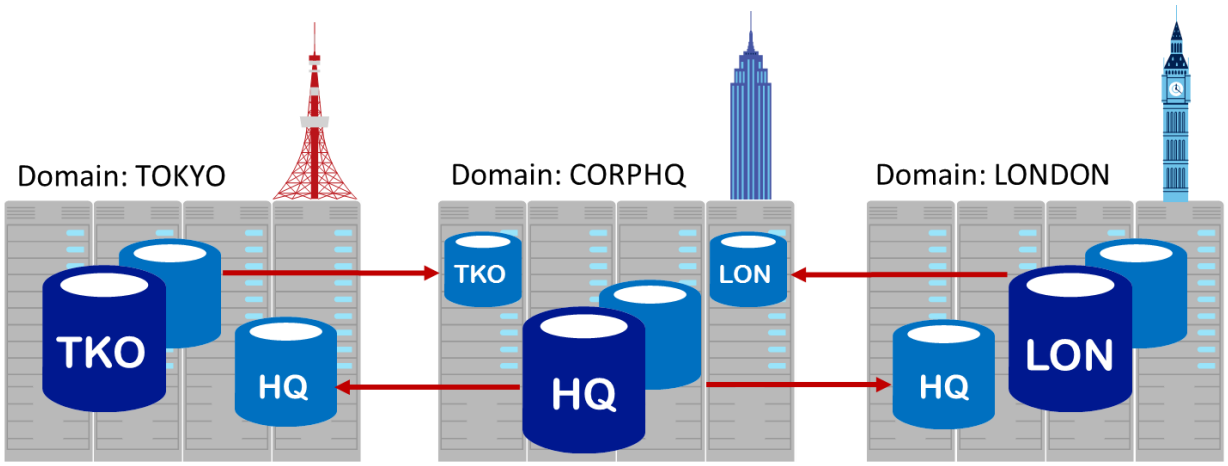

Figure 1: Multiple sites providing failover for each other

Scenario: No Active Directory domain

Not every enterprise runs exclusively on Windows platforms. Many infrastructures entail a mix of operating systems, and therefore do not exclusively use Active Directory domains—perhaps not at all. Domain-independent availability allows for on-site SQL Server instances to be replicated to other sites, or even Azure based replicas, without the need for domain membership. Servers can remain in workgroups and still be Availability Group members, with all AlwaysOn features enabled.

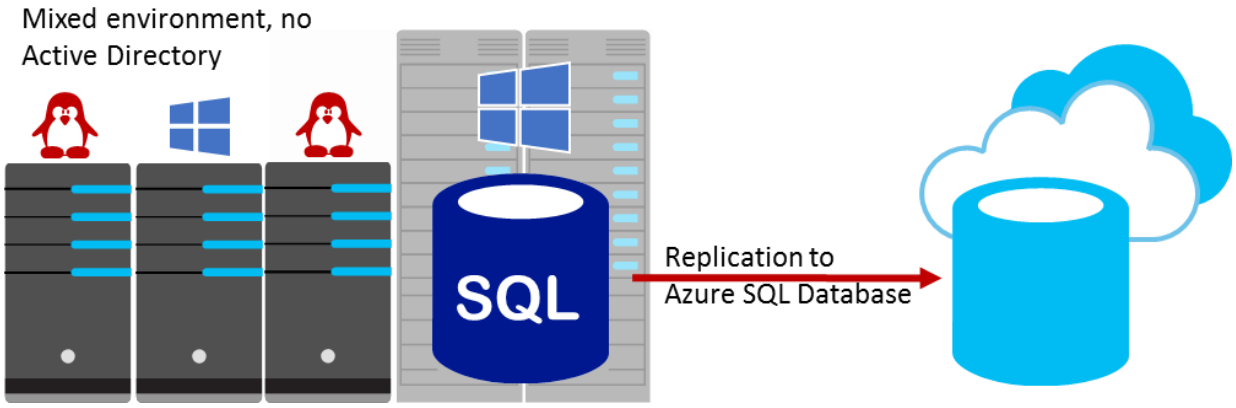

Figure 2: Mixed OS environment with Azure secondary replica

Security

For years, SQL Server has consistently been rated as the most secure database platform as measured by security incidents. With the new releases, both Windows Server and SQL Server have added significant security enhancements and features that result in an extremely secure and reliable platform overall.

Smaller footprint, better privilege management

Windows Server has produced editions that have progressively reduced threat area and patches while offering better availability, such as Core and Nano.[2] The smaller OS footprints result in a number of optimizations:

- Fewer resource requirements – better availability for applications
- Fewer running processes and services – better stability
- Fewer updates and patches – less downtime
- Reduced threat area – easier ability to monitor and prevent attacks

Windows Server 2016 introduces features such as Just-In-Time (JIT) administration and Just Enough Administration (JEA). JIT administration provides high-privileged access to resources, for a limited period of time, to accomplish a specific task. JEA is a security technology that enables delegated administration for anything that can be managed with Windows PowerShell. With JEA, you can:

- Reduce the number of administrators on your machines by leveraging virtual accounts that perform privileged actions on behalf of regular users
- Limit what users can do by specifying which cmdlets, functions, and external commands they can run
- Better understand what your users are doing with "over the shoulder" transcriptions that show you exactly what commands a user executed during a session

JEA enables the configuration of a role for an administrator, providing access to all necessary commands but nothing more. This allows the administrator to effect repairs without having access to browse the file system or run potentially dangerous scripts.[3]

Data security

SQL Server has also had a particular focus on security features with new capabilities such as Always Encrypted, which provides end-to-end encryption of specific column data. Row-Level Security restricts read and write access to data based upon specified security predicates. Dynamic Data Masking obfuscates data from users as needed through user-defined patterns. SQL Server is also taking advantage of the ability to offload expensive encryption tasks to the hardware in modern server, if it is present. These capabilities are surfaced by Windows Server and make the adoption of encryption technologies much more attractive.

[2] As of the writing of this paper, SQL Server supports installation on Windows Server Core; support for Windows Server Nano is still under development.

[3] GitHub. "Just Enough Administration." https://github.com/PowerShell/JEA#just-enough-administration

Scenario: Windows security and SQL Server security

Domain or system administrators generally do not require access to data stored in an operational database. Similarly, database administrators should not have access to stored data—particularly where personal or financial data is involved.

With JEA, a system administrator is able to perform critical changes to a database server's operating system, without being granted any unnecessary permissions that would allow modifications to the SQL Server instance, any databases housed on the server, or data.

With Dynamic Data Masking, database administrators are able to make modifications, implement and test views or table-valued functions with risk of exposure to sensitive data. Columns protected by data masking ensures that query results are obfuscated for all users except those with proper authorization to access unmasked data.

With Row Level Security, end users (or tenants) receive filtered query results. Rows not pertinent to the requestor are seamlessly excluded from the results, preventing potential data breaches.

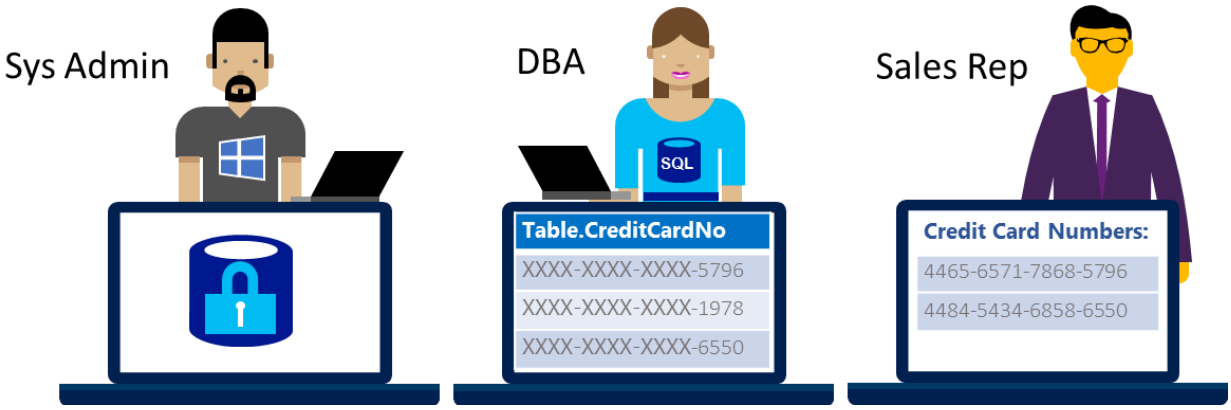

Figure 3: JEA, DDM, and RLS keep data secure in multiple situations

Together, Windows Server and SQL Server security features significantly reduce risk of a breach in a number of ways. A reduced OS footprint decreases potential exposure to threats. Tighter reigns on administrative capabilities and better monitoring scales down the likelihood of rogue admin-type attacks. End-to-end encryption for data both in motion and at rest, granular read/write access control, and data obfuscation all lessen the risk of data breach.

Conclusion

Together, Windows Server 2016 and SQL Server 2016 are delivering the best in next-generation scalability, availability, and security features. With these products, Microsoft is extending the limits of hardware capabilities and bringing the latest enterprise technologies to market. Improved availability and disaster recovery features offer unprecedented interoperability in a variety of environments. Windows Server and SQL Server provide new technologies in access control and encryption, ensuring that data is protected from threats and risks—both external and internal. The strong collaborative effort between Windows Server and SQL Server teams continues to bring new innovation and features together to provide a better enterprise data platform.

More information

The following websites offer more information about topics discussed in this paper:

- SQL Server 2016. "What's New in Database Engine." Microsoft Developer Network. 8 March 2015. https://msdn.microsoft.com/en-us/library/bb510411.aspx
- Microsoft Windows Server Team. "Next-generation storage for the software-defined datacenter." Windows Server Blog. 5 May 2015. https://blogs.technet.microsoft.com/windowsserver/2015/05/05/next-generation-storage-for-the-software-defined-datacenter/
- Microsoft Windows Server Team. "Protecting your datacenter and cloud from emerging threats." Windows Server Blog. 5 May 2015. https://blogs.technet.microsoft.com/windowsserver/2015/05/05/protecting-your-datacenter-and-cloud-from-emerging-threats/
- Microsoft Windows Server Team. "Protecting your datacenter and cloud from emerging threats." Windows Server Blog. 18 Nov 2015. https://blogs.technet.microsoft.com/windowsserver/2015/11/18/protecting-your-datacenter-and-cloud-november-update/
- Microsoft Windows Server Team. "4 datacenter challenges and how Windows Server 2016 software defined networking can help." Windows Server Blog. 4 November 2015. https://blogs.technet.microsoft.com/windowsserver/2015/11/04/4-datacenter-challenges-and-how-windows-server-2016-software-defined-networking-can-help/
- "What's New in Failover Clustering in Windows Server Technical Preview." Windows Server library. 19 August 2015. https://technet.microsoft.com/en-us/library/dn765474.aspx
- "Storage Spaces in Windows Server 2016 Technical Preview." Windows Server library. 4 February 2016. https://technet.microsoft.com/en-us/library/mt126109.aspx
- "Storage Replica in Windows Server 2016 Technical Preview." Windows Server library. 19 November 2015. https://technet.microsoft.com/en-us/library/mt126104.aspx