**Checklist: Best practices for SQL Server on Azure VMs**

* Article
* 03/20/2025
* 23 contributors

Feedback

**In this article**

1. [Overview](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-checklist?view=azuresql#overview)
2. [Manually install SQL Server to an Azure VM](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-checklist?view=azuresql#manually-install-sql-server-to-an-azure-vm)
3. [VM size](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-checklist?view=azuresql#vm-size)
4. [Storage](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-checklist?view=azuresql#storage)

Show 6 more

**Applies to:**  [SQL Server on Azure VM](https://learn.microsoft.com/en-us/sql/sql-server/sql-docs-navigation-guide#applies-to)

This article provides a quick checklist as a series of best practices and guidelines to optimize performance of your SQL Server on Azure Virtual Machines (VMs).

For comprehensive details, see the other articles in this series: [VM size](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-vm-size?view=azuresql), [Storage](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-storage?view=azuresql), [Security](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/security-considerations-best-practices?view=azuresql), [HADR configuration](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/hadr-cluster-best-practices?view=azuresql), [Collect baseline](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-collect-baseline?view=azuresql).

Enable [SQL Assessment for SQL Server on Azure VMs](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-assessment-for-sql-vm?view=azuresql) and your SQL Server will be evaluated against known best practices with results on the [SQL VM management page](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/manage-sql-vm-portal?view=azuresql) of the Azure portal.

For videos about the latest features to optimize SQL Server VM performance and automate management, review the following Data Exposed videos:

* [Caching and Storage Capping](https://learn.microsoft.com/en-us/shows/data-exposed/azure-sql-vm-caching-and-storage-capping-ep-1-data-exposed)
* [Automate Management with the SQL Server IaaS Agent extension](https://learn.microsoft.com/en-us/shows/data-exposed/azure-sql-vm-automate-management-with-the-sql-server-iaas-agent-extension-ep-2)
* [Use Azure Monitor Metrics to Track VM Cache Health](https://learn.microsoft.com/en-us/shows/data-exposed/azure-sql-vm-use-azure-monitor-metrics-to-track-vm-cache-health-ep-3)
* [Get the best price-performance for your SQL Server workloads on Azure VM](https://learn.microsoft.com/en-us/shows/data-exposed/azure-sql-vm-get-the-best-price-performance-for-your-sql-server-workloads-on-azure-vm)
* [Using PerfInsights to Evaluate Resource Health and Troubleshoot](https://learn.microsoft.com/en-us/shows/data-exposed/azure-sql-vm-using-perfinsights-to-evaluate-resource-health-and-troubleshoot-ep-5)
* [Best Price-Performance with Ebdsv5 Series](https://learn.microsoft.com/en-us/shows/data-exposed/azure-sql-vm-best-price-performance-with-ebdsv5-series)
* [Optimally Configure SQL Server on Azure Virtual Machines with SQL Assessment](https://learn.microsoft.com/en-us/shows/data-exposed/optimally-configure-sql-server-on-azure-virtual-machines-with-sql-assessment)
* [New and Improved SQL Server on Azure VM deployment and management experience](https://learn.microsoft.com/en-us/shows/data-exposed/new-and-improved-sql-on-azure-vm-deployment-and-management-experience)

**Overview**

While running SQL Server on Azure Virtual Machines, continue using the same database performance tuning options that are applicable to SQL Server in on-premises server environments. However, the performance of a relational database in a public cloud depends on many factors, such as the size of a virtual machine, and the configuration of the data disks.

There's typically a trade-off between optimizing for costs and optimizing for performance. This performance best practices series is focused on getting the *best* performance for SQL Server on Azure Virtual Machines. If your workload is less demanding, you might not require every recommended optimization. Consider your performance needs, costs, and workload patterns as you evaluate these recommendations.

**Manually install SQL Server to an Azure VM**

If you plan to manually install SQL Server on an Azure VM, consider the following:

* Make sure you have a product key ready for your installation.
* Avoid [unsupported](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-vm-size?view=azuresql#supportability) configurations such as:
  + More than 64 vCores per NUMA node.
  + Storage with 8-KB sector size.
  + Azure Virtual Machine Scale Sets.
* If they don't already exist, create the folders for your SQL Server installation and data files prior to launching the installation media.
* Copy the installation media to a local drive instead of installing directly from the mounted ISO.
* After installation, register your SQL Server VM with the [SQL Server IaaS Agent Extension](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-server-iaas-agent-extension-automate-management?view=azuresql) to automate management tasks.
* Place the tempdb database on the [local SSD ephemeral storage](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/tempdb-ephemeral-storage?view=azuresql) when possible.

**VM size**

The checklist in this section covers the [VM size best practices](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-vm-size?view=azuresql) for SQL Server on Azure VMs.

* Identify workload performance characteristics to determine the appropriate VM size for your business.
* If you're migrating to Azure, use tools like [Data Migration Assistant](https://www.microsoft.com/download/details.aspx?id=53595) and [SKU recommendation](https://learn.microsoft.com/en-us/sql/dma/dma-sku-recommend-sql-db) to find the right VM size for your existing SQL Server workload, and then migrate with [Azure Data Studio](https://learn.microsoft.com/en-us/azure/dms/tutorial-sql-server-to-virtual-machine-online-ads).
* Use Azure Marketplace images to deploy your SQL Server VMs as the SQL Server settings and storage options are configured for optimal performance.
* Use VM sizes with 4 or more vCPUs.
* Use memory optimized virtual machine sizes for the best performance of SQL Server workloads.
  + The [Edsv5-series](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-vm-size?view=azuresql#edsv5-series), and the [Msv3 and Mdsv3-series](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-vm-size?view=azuresql#msv3-and-mdsv3-series) offer an optimal memory-to-vCore ratio recommended for OLTP workloads.
  + The [Mbdsv3-series VMs](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-vm-size?view=azuresql#mbsv3-and-mbdsv3-series) offer the best performance for SQL Server workloads on Azure VMs. Consider this series first for mission critical OLTP and data warehouse SQL Server workloads.
  + The [Ebdsv5-series](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-vm-size?view=azuresql#ebdsv5-series) provides a high I/O throughput-to-vCore ratio, along with a memory-to-vCore ratio of 8:1. This series offers the best price-performance for SQL Server workloads on Azure VMs. Consider these VMs first for most SQL Server workloads.
  + The [M-series family](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-vm-size?view=azuresql#memory-optimized-m-series-vms) offers VMs with the highest memory allocation in Azure.
  + The [Mbsv3 and Mbdsv3 series](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-vm-size?view=azuresql#mbsv3-and-mbdsv3-series) VMs provide a high memory allocation and the highest I/O throughput-to-vCore ratio amongst the M-series family, along with a consistent memory-to-vCore ratio of at least 8:1.
* Start development environments with the lower-tier D-Series, B-Series, or Av2-series and grow your environment over time.
* Check [VM supportability](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-vm-size?view=azuresql#supportability) to avoid unsupported configurations.

**Caution**

SQL Server isn't supported on VM sizes that deploy with an uninitialized ephemeral disk. To learn more, review [**VM deployment and SQL Server failures**](https://learn.microsoft.com/en-us/troubleshoot/sql/azure-sql/sql-deployment-fails-drive-not-ready).

**Storage**

The checklist in this section covers the [storage best practices](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-storage?view=azuresql) for SQL Server on Azure VMs.

* Monitor the application and [determine storage bandwidth and latency requirements](https://learn.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance#counters-to-measure-application-performance-requirements) for SQL Server data, log, and tempdb files before choosing the disk type.
* If available, configure the tempdb data and log files on the D: local SSD volume when you deploy a [new virtual machine](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/storage-configuration?view=azuresql#new-vms), or after you've [installed SQL Server manually](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/tempdb-ephemeral-storage?view=azuresql). The SQL IaaS Agent extension handles the folder and permissions needed upon re-provisioning.
* To optimize storage performance, plan for highest uncached IOPS available and use data caching as a performance feature for data reads while avoiding [virtual machine and disks capping](https://learn.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance#throttling).
* When using the [Ebdsv5 or Ebsv5](https://learn.microsoft.com/en-us/azure/virtual-machines/ebdsv5-ebsv5-series) series SQL Server VMs, use [Premium SSD v2](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/storage-configuration-premium-ssd-v2?view=azuresql) for the best price performance. You can deploy your SQL Server VM with Premium SSD v2 by using the Azure portal (currently in preview).
* If your workload requires more than 160,000 IOPS, use [Premium SSD v2](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-storage?view=azuresql#premium-ssd-v2) or [Azure Ultra Disks](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-storage?view=azuresql#azure-ultra-disk).
* Place data, log, and tempdb files on separate drives.
  + For the data drive, use [premium P30 and P40 or smaller disks](https://learn.microsoft.com/en-us/azure/virtual-machines/disks-types#premium-ssds) to ensure the availability of cache support. When using the [Ebdsv5 VM series](https://learn.microsoft.com/en-us/azure/virtual-machines/ebdsv5-ebsv5-series), use [Premium SSD v2](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/storage-configuration-premium-ssd-v2?view=azuresql) which provides better price-performance for workloads that require high IOPS and I/O throughput.
  + For the log drive plan for capacity and test performance versus cost while evaluating either [Premium SSD v2](https://learn.microsoft.com/en-us/azure/virtual-machines/disks-types#premium-ssd-v2) or Premium SSD [P30 - P80 disks](https://learn.microsoft.com/en-us/azure/virtual-machines/disks-types#premium-ssds)
    - If submillisecond storage latency is required, use either [Premium SSD v2](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/storage-configuration-premium-ssd-v2?view=azuresql) or [Azure ultra disks](https://learn.microsoft.com/en-us/azure/virtual-machines/disks-types#ultra-disks) for the transaction log.
    - For M-series virtual machine deployments, consider [write accelerator](https://learn.microsoft.com/en-us/azure/virtual-machines/how-to-enable-write-accelerator) over using Azure ultra disks.
  + Place [tempdb](https://learn.microsoft.com/en-us/sql/relational-databases/databases/tempdb-database) on the [temporary disk](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/tempdb-ephemeral-storage?view=azuresql) (the temporary disk is ephemeral, and defaults to D:\) for most SQL Server workloads that aren't part of a failover cluster instance (FCI) after choosing the optimal VM size.
    - If the capacity of the local drive isn't enough for tempdb, consider sizing up the VM. For more information, see [Data file caching policies](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-storage?view=azuresql#data-file-caching-policies).
  + For failover cluster instances (FCI) place tempdb on the shared storage.
    - If the FCI workload is heavily dependent on tempdb disk performance, then as an advanced configuration place tempdb on the local ephemeral SSD (default D:\) drive, which isn't part of FCI storage. This configuration needs custom monitoring and action to ensure the local ephemeral SSD (default D:\) drive is available all the time as any failures of this drive won't trigger action from FCI.
* Stripe multiple Azure data disks using [Storage Spaces](https://learn.microsoft.com/en-us/windows-server/storage/storage-spaces/overview) to increase I/O bandwidth up to the target virtual machine's IOPS and throughput limits.
* Set [host caching](https://learn.microsoft.com/en-us/azure/virtual-machines/disks-performance#virtual-machine-uncached-vs-cached-limits) to **read-only** for data file disks.
* Set [host caching](https://learn.microsoft.com/en-us/azure/virtual-machines/disks-performance#virtual-machine-uncached-vs-cached-limits) to **none** for log file disks.
  + Don't enable read/write caching on disks that contain SQL Server data or log files.
  + Always stop the SQL Server service before changing the cache settings of your disk.
* When migrating several different workloads to the cloud, [Azure Elastic SAN](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/storage-configuration-azure-elastic-san?view=azuresql) can be a cost-effective consolidated storage solution. However, when using Azure Elastic SAN, achieving desired IOPS/throughput for SQL Server workloads often requires overprovisioning capacity. While not typically appropriate for single SQL Server workloads, you can attain a cost-effective solution when combining low-performance workloads with SQL Server.
* For development and test workloads, and long-term backup archival consider using standard storage. It isn't recommended to use Standard HDD/SSD for production workloads.
* [Credit-based Disk Bursting](https://learn.microsoft.com/en-us/azure/virtual-machines/disk-bursting#credit-based-bursting) (P1-P20) should only be considered for smaller dev/test workloads and departmental systems.
* To optimize storage performance, plan for highest uncached IOPS available, and use data caching as a performance feature for data reads while avoiding [virtual machine and disks capping/throttling](https://learn.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance#throttling).
* Format your data disk to use 64-KB allocation unit size for all data files placed on a drive other than the temporary D:\ drive (which has a default of 4 KB). SQL Server VMs deployed through Azure Marketplace come with data disks formatted with allocation unit size and interleave for the storage pool set to 64 KB.
* Configure the storage account in the same region as the SQL Server VM.
* Disable Azure geo-redundant storage (geo-replication) and use LRS (local redundant storage) on the storage account.
* Enable the [SQL Best Practices Assessment](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-assessment-for-sql-vm?view=azuresql) to identify possible performance issues and evaluate that your SQL Server VM is configured to follow best practices.
* Review and monitor disk and VM limits using [Storage IO utilization metrics](https://learn.microsoft.com/en-us/azure/virtual-machines/disks-metrics#storage-io-utilization-metrics).
* [Exclude SQL Server files](https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/security/antivirus-and-sql-server) from antivirus software scanning, including data files, log files, and backup files.
* [Resize the storage pool appropriately](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-storage?view=azuresql#resize-storage-pools-appropriately).

**Security**

The checklist in this section covers the [security best practices](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/security-considerations-best-practices?view=azuresql) for SQL Server on Azure VMs.

SQL Server features and capabilities provide methods of securing data at the database level that can be combined with security features at the infrastructure level. Together, these features provide defense-in-depth at the infrastructure level for cloud-based and hybrid solutions. In addition, with Azure security measures, it's possible to encrypt your sensitive data, protect virtual machines from viruses and malware, secure network traffic, identify and detect threats, meet compliance requirements, and provides a single method for administration and reporting for any security need in the hybrid cloud.

* Use [Microsoft Defender for Cloud](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction) to evaluate and take action to improve the security posture of your data environment. Capabilities such as [Azure Advanced Threat Protection (ATP)](https://learn.microsoft.com/en-us/azure/azure-sql/database/threat-detection-overview?view=azuresql) can be used across your hybrid workloads to improve security evaluation and give the ability to react to risks. Registering your SQL Server VM with the [SQL IaaS Agent extension](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-agent-extension-manually-register-single-vm?view=azuresql) surfaces Microsoft Defender for Cloud assessments within the [SQL virtual machine resource](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/manage-sql-vm-portal?view=azuresql) of the Azure portal.
* Use [Microsoft Defender for SQL](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-sql-introduction) to discover and mitigate potential database vulnerabilities, as well as detect anomalous activities that could indicate a threat to your SQL Server instance and database layer.
* [Vulnerability Assessment](https://learn.microsoft.com/en-us/azure/defender-for-cloud/sql-azure-vulnerability-assessment-overview) is a part of [Microsoft Defender for SQL](https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-sql-introduction) that can discover and help remediate potential risks to your SQL Server environment. It provides visibility into your security state, and includes actionable steps to resolve security issues.
* Use [Azure confidential VMs](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/security-considerations-best-practices?view=azuresql#confidential-vms) to reinforce protection of your data in-use, and data-at-rest against host operator access. Azure confidential VMs allow you to confidently store your sensitive data in the cloud and meet strict compliance requirements.
* If you're on SQL Server 2022, consider using [Microsoft Entra authentication](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/configure-azure-ad-authentication-for-sql-vm?view=azuresql) to connect to your instance of SQL Server.
* [Azure Advisor](https://learn.microsoft.com/en-us/azure/advisor/advisor-security-recommendations) analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources. Use Azure Advisor at the virtual machine, resource group, or subscription level to help identify and apply best practices to optimize your Azure deployments.
* Use [Azure Disk Encryption](https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-windows) when your compliance and security needs require you to encrypt the data end-to-end using your encryption keys, including encryption of the ephemeral (locally attached temporary) disk.
* [Managed Disks are encrypted](https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption) at rest by default using Azure Storage Service Encryption, where the encryption keys are Microsoft-managed keys stored in Azure.
* For a comparison of the managed disk encryption options, review the [managed disk encryption comparison chart](https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption-overview#comparison)
* Management ports should be closed on your virtual machines - Open remote management ports expose your VM to a high level of risk from internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine.
* Turn on [Just-in-time (JIT) access](https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage) for Azure virtual machines
* Use [Azure Bastion](https://learn.microsoft.com/en-us/azure/bastion/bastion-overview) over Remote Desktop Protocol (RDP).
* Lock down ports and only allow the necessary application traffic using [Azure Firewall](https://learn.microsoft.com/en-us/azure/firewall/features) which is a managed Firewall as a Service (FaaS) that grants/ denies server access based on the originating IP address.
* Use [Network Security Groups (NSGs)](https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview) to filter network traffic to, and from, Azure resources on Azure Virtual Networks
* Use [Application Security Groups](https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups) to group servers together with similar port filtering requirements, with similar functions, such as web servers and database servers.
* For web and application servers use [Azure Distributed Denial of Service (DDoS) protection](https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview). DDoS attacks are designed to overwhelm and exhaust network resources, making apps slow or unresponsive. It's common for DDoS attacks to target user interfaces. Azure DDoS protection sanitizes unwanted network traffic, before it impacts service availability
* Use VM extensions to help address anti-malware, desired state, threat detection, prevention, and remediation to address threats at the operating system, machine, and network levels:
  + [Guest Configuration extension](https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/guest-configuration) performs audit and configuration operations inside virtual machines.
  + [Network Watcher Agent virtual machine extension for Windows and Linux](https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/network-watcher-windows) monitors network performance, diagnostic, and analytics service that allows monitoring of Azure networks.
  + [Microsoft Antimalware Extension for Windows](https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/iaas-antimalware-windows) to help identify and remove viruses, spyware, and other malicious software, with configurable alerts.
  + [Evaluate third party extensions](https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/overview) such as Symantec Endpoint Protection for Windows VM (/azure/virtual-machines/extensions/symantec)
* Use [Azure Policy](https://learn.microsoft.com/en-us/azure/governance/policy/overview) to create business rules that can be applied to your environment. Azure Policies evaluate Azure resources by comparing the properties of those resources against rules defined in JSON format.
* Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints are [different than Azure Policies](https://learn.microsoft.com/en-us/azure/governance/blueprints/overview#how-its-different-from-azure-policy).
* Use Windows Server 2019 or Windows Server 2022 to be [FIPS](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/security-considerations-best-practices?view=azuresql#fips-compliance) compliant with SQL Server on Azure VMs.

**SQL Server features**

The following is a quick checklist of best practices for SQL Server configuration settings when running your SQL Server instances in an Azure virtual machine in production:

* Enable [database page compression](https://learn.microsoft.com/en-us/sql/relational-databases/data-compression/data-compression) where appropriate.
* Enable [backup compression](https://learn.microsoft.com/en-us/sql/relational-databases/backup-restore/backup-compression-sql-server).
* Enable [instant file initialization](https://learn.microsoft.com/en-us/sql/relational-databases/databases/database-instant-file-initialization) for data files.
* Limit [autogrowth](https://learn.microsoft.com/en-us/troubleshoot/sql/admin/considerations-autogrow-autoshrink#considerations-for-autogrow) of the database.
* Disable [autoshrink](https://learn.microsoft.com/en-us/troubleshoot/sql/admin/considerations-autogrow-autoshrink#considerations-for-auto_shrink) of the database.
* Disable autoclose of the database.
* Move all databases to data disks, including [system databases](https://learn.microsoft.com/en-us/sql/relational-databases/databases/move-system-databases).
* Move SQL Server error log and trace file directories to data disks.
* Configure default backup and database file locations.
* Set max [SQL Server memory limit](https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/server-memory-server-configuration-options#use-) to leave enough memory for the Operating System. ([Use Memory\Available Bytes](https://learn.microsoft.com/en-us/sql/relational-databases/performance-monitor/monitor-memory-usage) to monitor the operating system memory health).
* Enable [lock pages in memory](https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/enable-the-lock-pages-in-memory-option-windows).
* Enable [optimize for adhoc workloads](https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/optimize-for-ad-hoc-workloads-server-configuration-option) for OLTP heavy environments.
* Evaluate and apply the [latest cumulative updates](https://learn.microsoft.com/en-us/sql/database-engine/install-windows/latest-updates-for-microsoft-sql-server) for the installed versions of SQL Server.
* Enable [Query Store](https://learn.microsoft.com/en-us/sql/relational-databases/performance/monitoring-performance-by-using-the-query-store) on all production SQL Server databases [following best practices](https://learn.microsoft.com/en-us/sql/relational-databases/performance/best-practice-with-the-query-store).
* Enable [automatic tuning](https://learn.microsoft.com/en-us/sql/relational-databases/automatic-tuning/automatic-tuning) on mission critical application databases.
* Ensure that all [tempdb best practices](https://learn.microsoft.com/en-us/sql/relational-databases/databases/tempdb-database#optimizing-tempdb-performance-in-sql-server) are followed.
* [Use the recommended number of files](https://learn.microsoft.com/en-us/troubleshoot/sql/performance/recommendations-reduce-allocation-contention#resolution), using multiple tempdb data files starting with one file per core, up to eight files.
* If available, configure the tempdb [data and log files on the D: local SSD volume](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/manage-sql-vm-portal?view=azuresql#storage). The SQL IaaS Agent extension handles the folder and permissions needed upon reprovisioning.
* Schedule SQL Server Agent jobs to run [DBCC CHECKDB](https://learn.microsoft.com/en-us/sql/t-sql/database-console-commands/dbcc-checkdb-transact-sql#a-checking-both-the-current-and-another-database), [index reorganize](https://learn.microsoft.com/en-us/sql/relational-databases/indexes/reorganize-and-rebuild-indexes#reorganize-an-index), [index rebuild](https://learn.microsoft.com/en-us/sql/relational-databases/indexes/reorganize-and-rebuild-indexes#rebuild-an-index), and [update statistics](https://learn.microsoft.com/en-us/sql/t-sql/statements/update-statistics-transact-sql#examples) jobs.
* Monitor and manage the health and size of the SQL Server [transaction log file](https://learn.microsoft.com/en-us/sql/relational-databases/logs/manage-the-size-of-the-transaction-log-file#Recommendations).
* Take advantage of any new [SQL Server features](https://learn.microsoft.com/en-us/sql/sql-server/what-s-new-in-sql-server-ver15) available for the version being used.
* Be aware of the differences in [supported features](https://learn.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-version-15) between the editions you're considering deploying.
* [Exclude SQL Server files](https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/security/antivirus-and-sql-server) from antivirus software scanning. This includes data files, log files, and backup files.

**Azure features**

The following is a quick checklist of best practices for Azure-specific guidance when running your SQL Server on Azure VM:

* Register with [the SQL IaaS Agent Extension](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-agent-extension-manually-register-single-vm?view=azuresql) to unlock a number of [feature benefits](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-server-iaas-agent-extension-automate-management?view=azuresql#feature-benefits).
* Use the best [backup and restore strategy](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/backup-restore?view=azuresql#decision-matrix) for your SQL Server workload.
* Ensure [Accelerated Networking is enabled](https://learn.microsoft.com/en-us/azure/virtual-network/create-vm-accelerated-networking-cli#portal-creation) on the virtual machine.
* Use [Microsoft Defender for Cloud](https://learn.microsoft.com/en-us/azure/security-center/index) to improve the overall security posture of your virtual machine deployment.
* Use [Microsoft Defender for Cloud](https://learn.microsoft.com/en-us/azure/security-center/azure-defender), integrated with [Microsoft Defender for Cloud](https://azure.microsoft.com/services/security-center/), for specific [SQL Server VM coverage](https://learn.microsoft.com/en-us/azure/security-center/defender-for-sql-introduction) including vulnerability assessments, and just-in-time access, which reduces the attack service while allowing legitimate users to access virtual machines when necessary. To learn more, see [vulnerability assessments](https://learn.microsoft.com/en-us/azure/security-center/defender-for-sql-on-machines-vulnerability-assessment), [enable vulnerability assessments for SQL Server VMs](https://learn.microsoft.com/en-us/azure/security-center/defender-for-sql-on-machines-vulnerability-assessment) and [just-in-time access](https://learn.microsoft.com/en-us/azure/security-center/just-in-time-explained).
* Use [Azure Advisor](https://learn.microsoft.com/en-us/azure/advisor/advisor-overview) to address [performance](https://learn.microsoft.com/en-us/azure/advisor/advisor-performance-recommendations), [cost](https://learn.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations), [reliability](https://learn.microsoft.com/en-us/azure/advisor/advisor-high-availability-recommendations), [operational excellence](https://learn.microsoft.com/en-us/azure/advisor/advisor-operational-excellence-recommendations), and [security recommendations](https://learn.microsoft.com/en-us/azure/advisor/advisor-security-recommendations).
* Use [Azure Monitor](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine) to collect, analyze, and act on telemetry data from your SQL Server environment. This includes identifying infrastructure issues with [VM insights](https://learn.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-overview) and monitoring data with [Log Analytics](https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-query-overview) for deeper diagnostics.
* Enable [Autoshutdown](https://learn.microsoft.com/en-us/azure/automation/automation-solution-vm-management) for development and test environments.
* Implement a high availability and disaster recovery (HADR) solution that meets your business continuity SLAs, see the [HADR options](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/business-continuity-high-availability-disaster-recovery-hadr-overview?view=azuresql#business-continuity-features) options available for SQL Server on Azure VMs.
* Use the Azure portal (support + troubleshooting) to evaluate [resource health](https://learn.microsoft.com/en-us/azure/service-health/resource-health-overview) and history; submit new support requests when needed.

**HADR configuration**

The checklist in this section covers the [HADR best practices](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/hadr-cluster-best-practices?view=azuresql) for SQL Server on Azure VMs.

High availability and disaster recovery (HADR) features, such as the [Always On availability group](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/availability-group-overview?view=azuresql) and the [failover cluster instance](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/failover-cluster-instance-overview?view=azuresql) rely on underlying [Windows Server Failover Cluster](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/hadr-windows-server-failover-cluster-overview?view=azuresql) technology. Review the best practices for modifying your HADR settings to better support the cloud environment.

For your Windows cluster, consider these best practices:

* Deploy your SQL Server VMs to multiple subnets whenever possible to avoid the dependency on an Azure Load Balancer or a distributed network name (DNN) to route traffic to your HADR solution.
* Change the cluster to less aggressive parameters to avoid unexpected outages from transient network failures or Azure platform maintenance. To learn more, see [heartbeat and threshold settings](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/hadr-cluster-best-practices?view=azuresql#heartbeat-and-threshold). For Windows Server 2012 and later, use the following recommended values:
  + **SameSubnetDelay**: 1 second
  + **SameSubnetThreshold**: 40 heartbeats
  + **CrossSubnetDelay**: 1 second
  + **CrossSubnetThreshold**: 40 heartbeats
* Place your VMs in an availability set or different availability zones. To learn more, see [VM availability settings](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/hadr-cluster-best-practices?view=azuresql#vm-availability-settings).
* Use a single NIC per cluster node.
* Configure cluster [quorum voting](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/hadr-cluster-best-practices?view=azuresql#quorum-voting) to use 3 or more odd number of votes. Don't assign votes to DR regions.
* Carefully monitor [resource limits](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/hadr-cluster-best-practices?view=azuresql#resource-limits) to avoid unexpected restarts or failovers due to resource constraints.
  + Ensure your OS, drivers, and SQL Server are at the latest builds.
  + Optimize performance for SQL Server on Azure VMs. Review the other sections in this article to learn more.
  + Reduce or spread out workload to avoid resource limits.
  + Move to a VM or disk that has higher limits to avoid constraints.

For your SQL Server availability group or failover cluster instance, consider these best practices:

* If you're experiencing frequent unexpected failures, follow the performance best practices outlined in the rest of this article.
* If optimizing SQL Server VM performance doesn't resolve your unexpected failovers, consider [relaxing the monitoring](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/hadr-cluster-best-practices?view=azuresql#relaxed-monitoring) for the availability group or failover cluster instance. However, doing so may not address the underlying source of the issue and could mask symptoms by reducing the likelihood of failure. You may still need to investigate and address the underlying root cause. For Windows Server 2012 or higher, use the following recommended values:
  + **Lease timeout**: Use this equation to calculate the maximum lease time-out value:  
    Lease timeout < (2 \* SameSubnetThreshold \* SameSubnetDelay).  
    Start with 40 seconds. If you're using the relaxed SameSubnetThreshold and SameSubnetDelay values recommended previously, don't exceed 80 seconds for the lease timeout value.
  + **Max failures in a specified period**: Set this value to 6.
* When using the virtual network name (VNN) and an Azure Load Balancer to connect to your HADR solution, specify MultiSubnetFailover = true in the connection string, even if your cluster only spans one subnet.
  + If the client doesn't support MultiSubnetFailover = True you may need to set RegisterAllProvidersIP = 0 and HostRecordTTL = 300 to cache client credentials for shorter durations. However, doing so may cause additional queries to the DNS server.
* To connect to your HADR solution using the distributed network name (DNN), consider the following:
  + You must use a client driver that supports MultiSubnetFailover = True, and this parameter must be in the connection string.
  + Use a unique DNN port in the connection string when connecting to the DNN listener for an availability group.
* Use a database mirroring connection string for a basic availability group to bypass the need for a load balancer or DNN.
* Validate the sector size of your VHDs before deploying your high availability solution to avoid having misaligned I/Os. See [KB3009974](https://support.microsoft.com/topic/kb3009974-fix-slow-synchronization-when-disks-have-different-sector-sizes-for-primary-and-secondary-replica-log-files-in-sql-server-ag-and-logshipping-environments-ed181bf3-ce80-b6d0-f268-34135711043c) to learn more.
* If the SQL Server database engine, Always On availability group listener, or failover cluster instance health probe are configured to use a port between 49,152 and 65,536 (the [default dynamic port range for TCP/IP](https://learn.microsoft.com/en-us/windows/client-management/troubleshoot-tcpip-port-exhaust#default-dynamic-port-range-for-tcpip)), add an exclusion for each port. Doing so prevents other systems from being dynamically assigned the same port. The following example creates an exclusion for port 59999:  
  netsh int ipv4 add excludedportrange tcp startport=59999 numberofports=1 store=persistent

**Performance troubleshooting**

The following is a list of resources that help you further troubleshoot SQL Server performance issues.

* [Troubleshoot high-CPU-usage issues](https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/performance/troubleshoot-high-cpu-usage-issues)
* [Understand and resolve blocking problems](https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/performance/understand-resolve-blocking)
* [Troubleshoot slow-running queries](https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/performance/troubleshoot-slow-running-queries)
* [Troubleshoot slow performance caused by I/O issues](https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/performance/troubleshoot-sql-io-performance)
* [Troubleshoot query time-out errors](https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/performance/troubleshoot-query-timeouts)
* [Troubleshoot out of memory or low memory](https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/performance/troubleshoot-memory-issues)
* [Performance dashboard](https://learn.microsoft.com/en-us/sql/relational-databases/performance/performance-dashboard) provides fast insight into SQL Server performance state.

**Related content**

* [VM size](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-vm-size?view=azuresql)
* [Storage](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-storage?view=azuresql)
* [Security](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/security-considerations-best-practices?view=azuresql)
* [HADR settings](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/hadr-cluster-best-practices?view=azuresql)
* [Collect baseline](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-collect-baseline?view=azuresql)

Consider enabling [SQL Assessment for SQL Server on Azure VMs](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-assessment-for-sql-vm?view=azuresql).

Review other SQL Server Virtual Machine articles at [SQL Server on Azure Virtual Machines Overview](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-server-on-azure-vm-iaas-what-is-overview?view=azuresql). If you have questions about SQL Server virtual machines, see the [Frequently Asked Questions](https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/frequently-asked-questions-faq?view=azuresql).