Session 09
Azure PaaS / SaaS

Anton Boyko
Microsoft Regional Director
Microsoft Azure MVP
me@boykoant.pro

Housekeeping

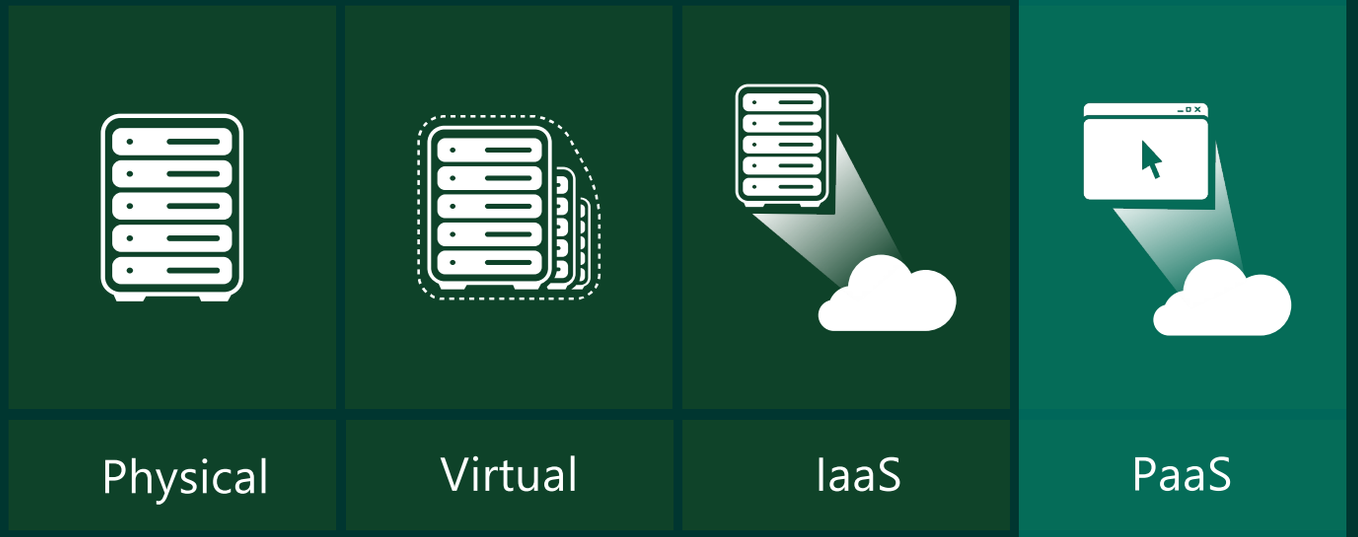
- Please keep yourself muted unless you are participating in the conversation, so we can have a more clear recording.
- If you have questions – don’t hesitate and ask.

Azure SQL Database

Microsoft Relational Storage Options

Microsoft Azure

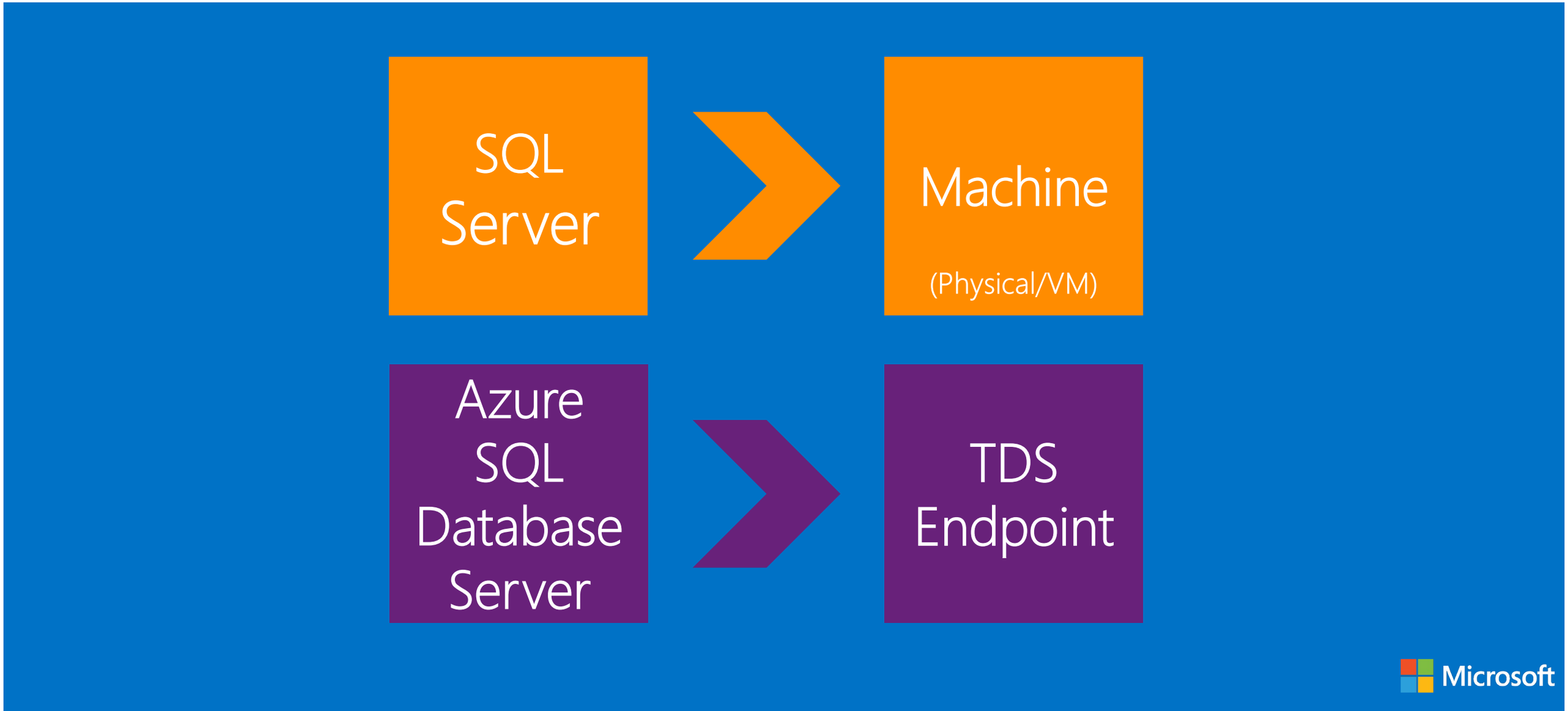
A Continuous offering



From private to public Cloud

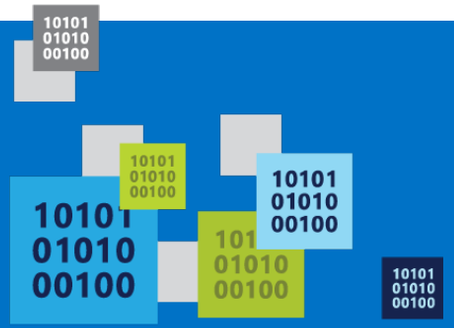
Microsoft

A Server is not a machine



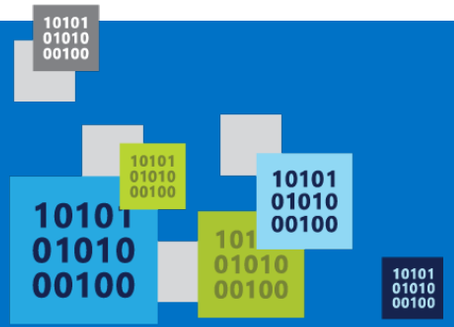
SQL Database
The Basics

- SQL Server database technology “as a Service”
- Fully Managed
- Enterprise-ready with automatic support for HA, DR, Backups, replication and more



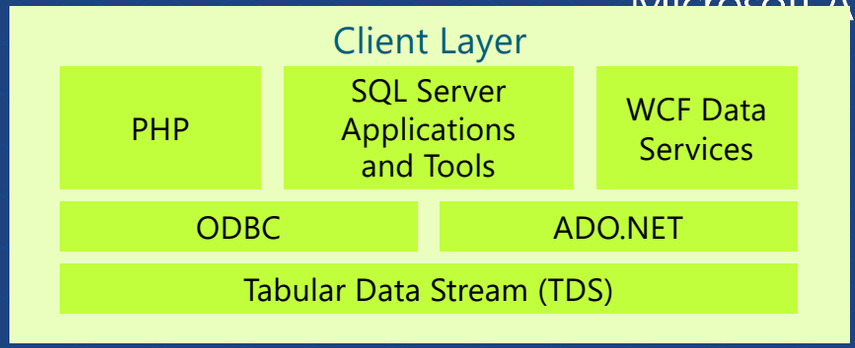
SQL Database The Basics

- Scale out with ElasticScale
- Built-in regional database replicas for additional protection
- Uptime SLA of 99.99%



How It Works – Architecture of the Service

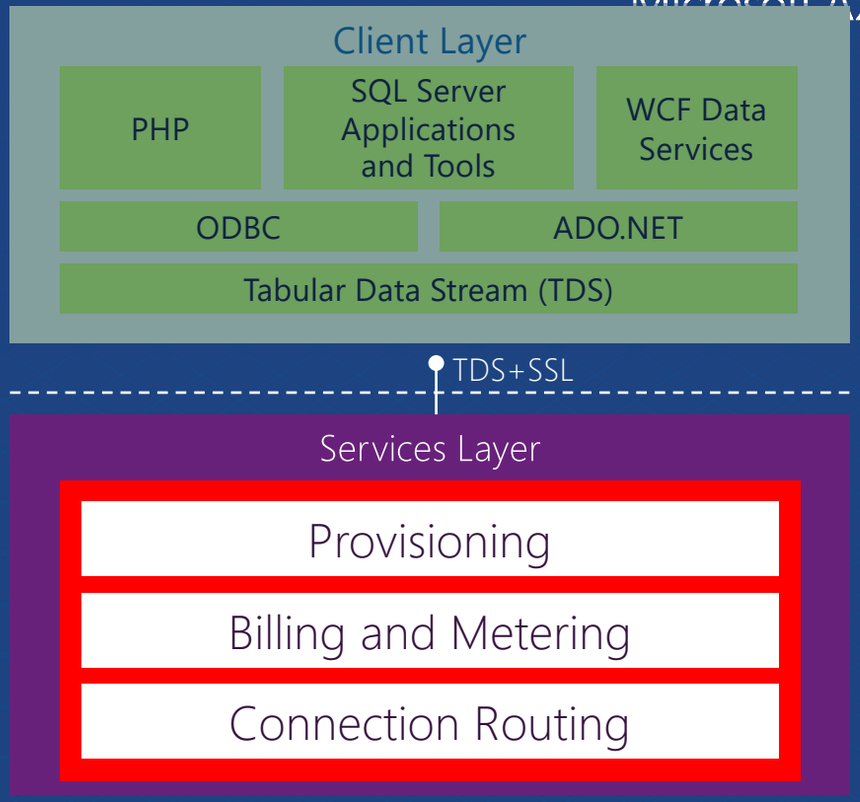
Applications communicate directly with SQL Database using TDS.



How It Works – Architecture of the Service

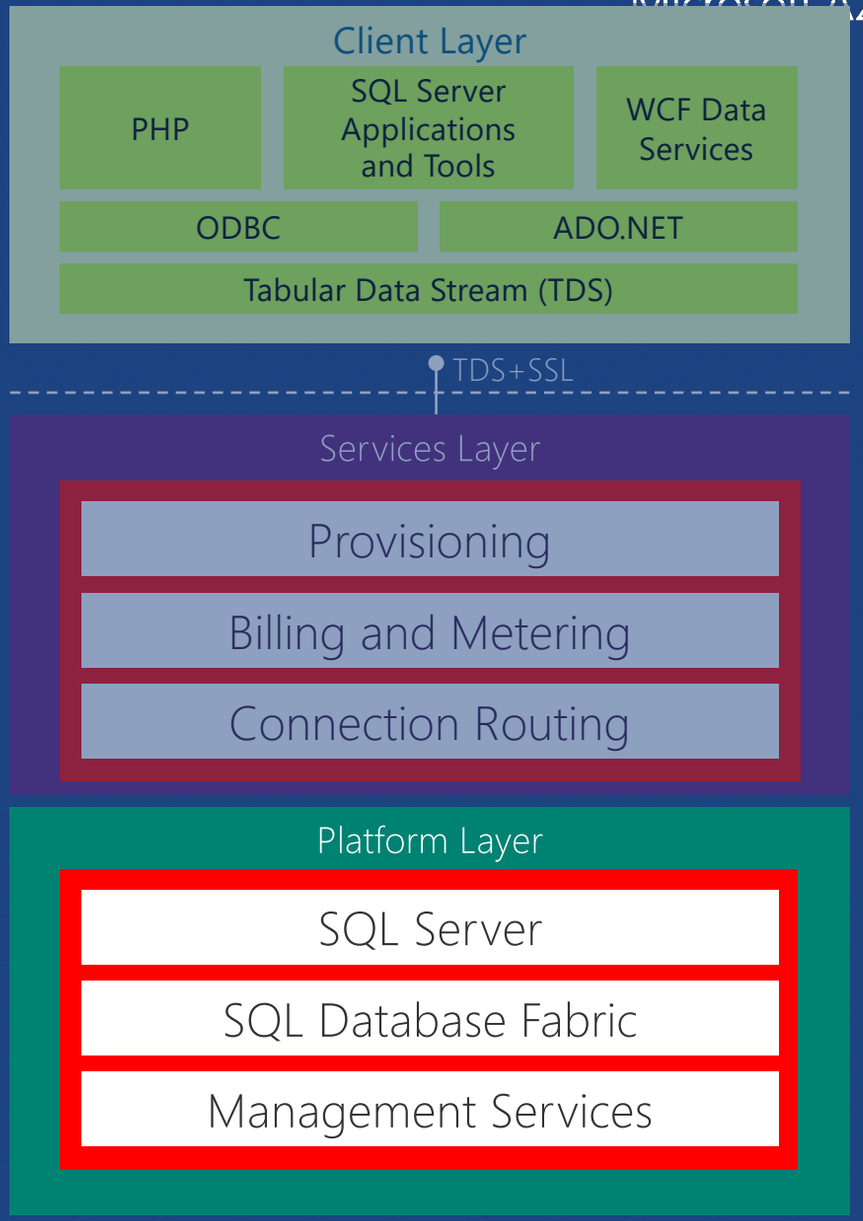
Microsoft Azure

Gateway between Client layer and Platform layer.



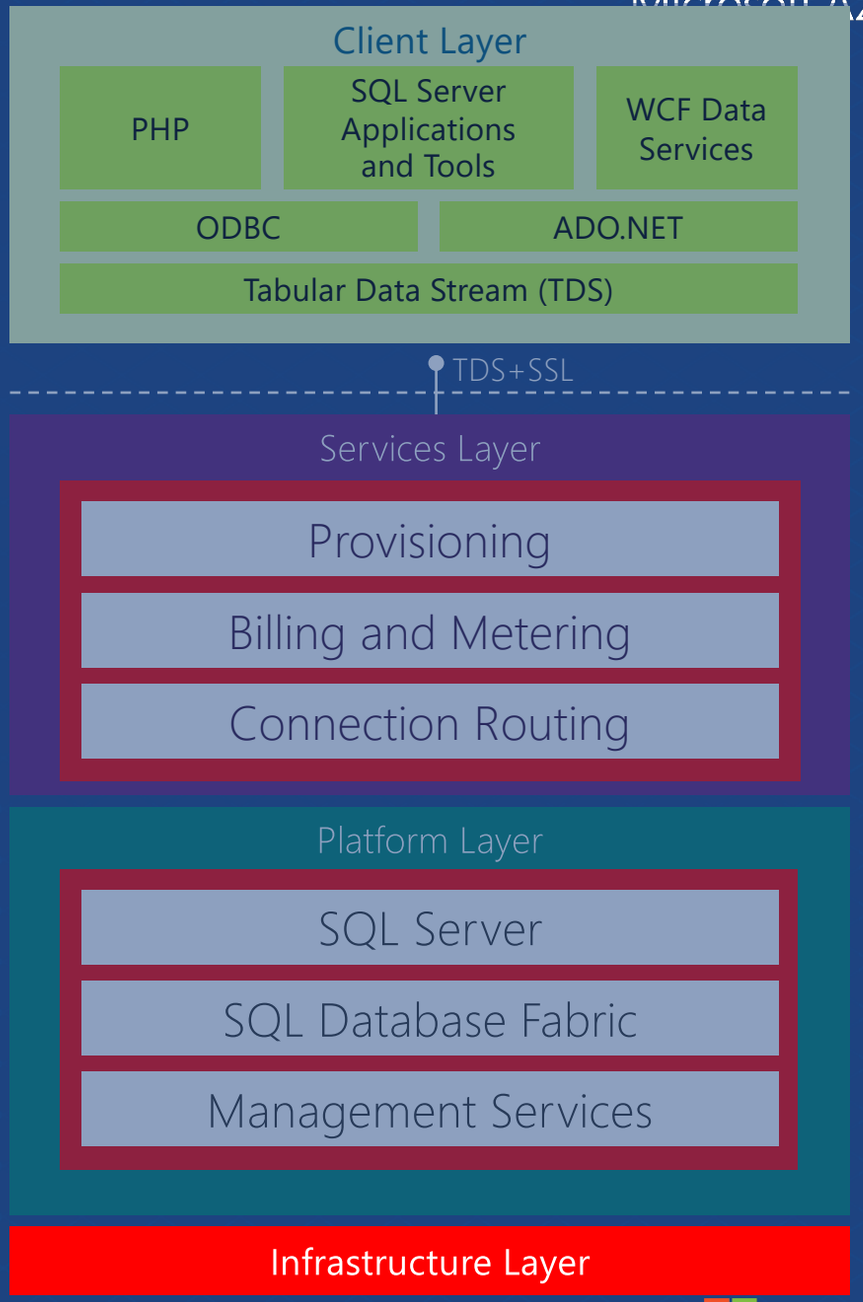
Microsoft

How It Works – Architecture of the Service



Includes physical servicers and services that support the Services layer.

How It Works – Architecture of the Service

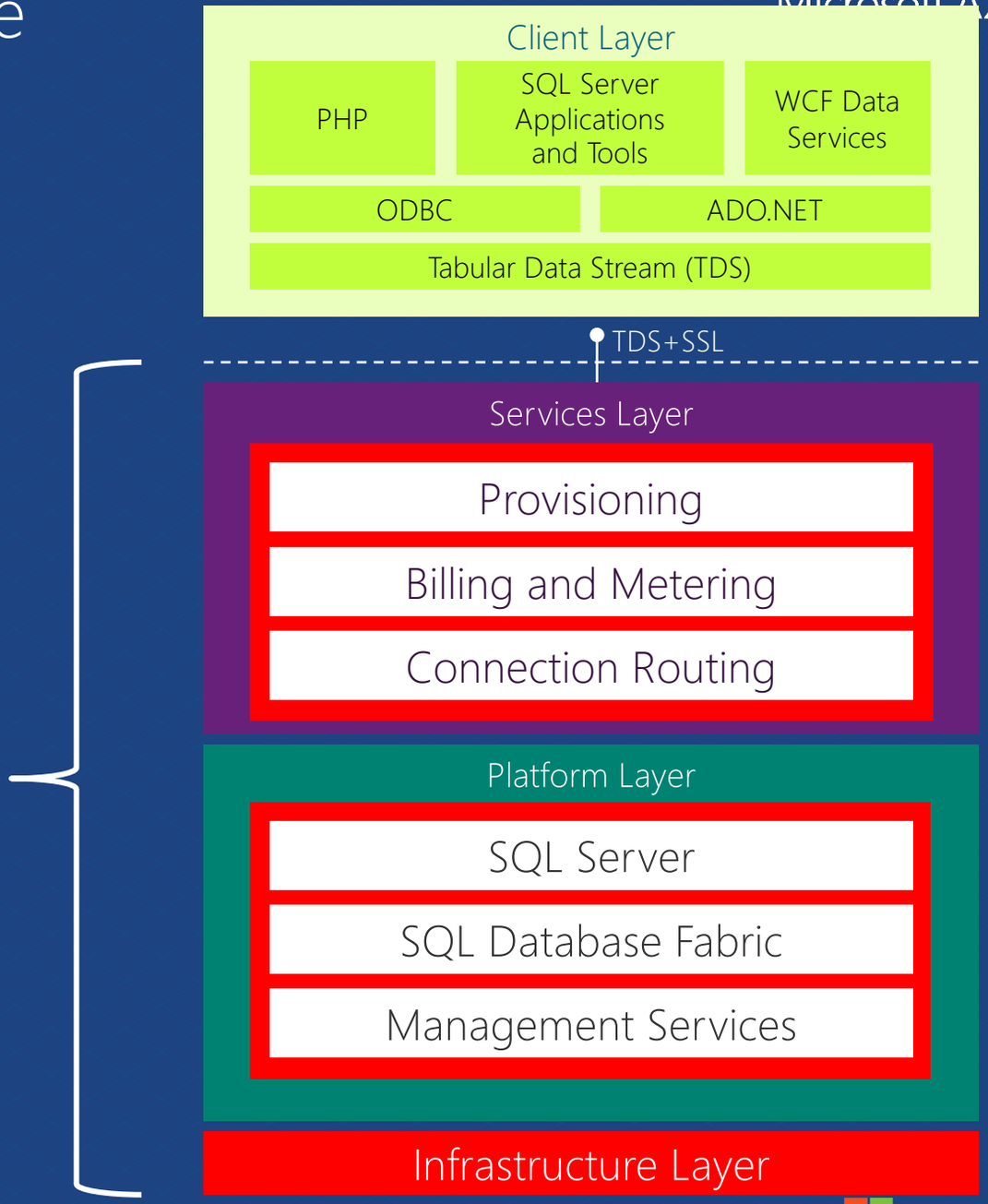


Administration of the physical HW and OS.

How It Works – Architecture of the Service

Microsoft Azure

Microsoft Azure SQL Database PaaS



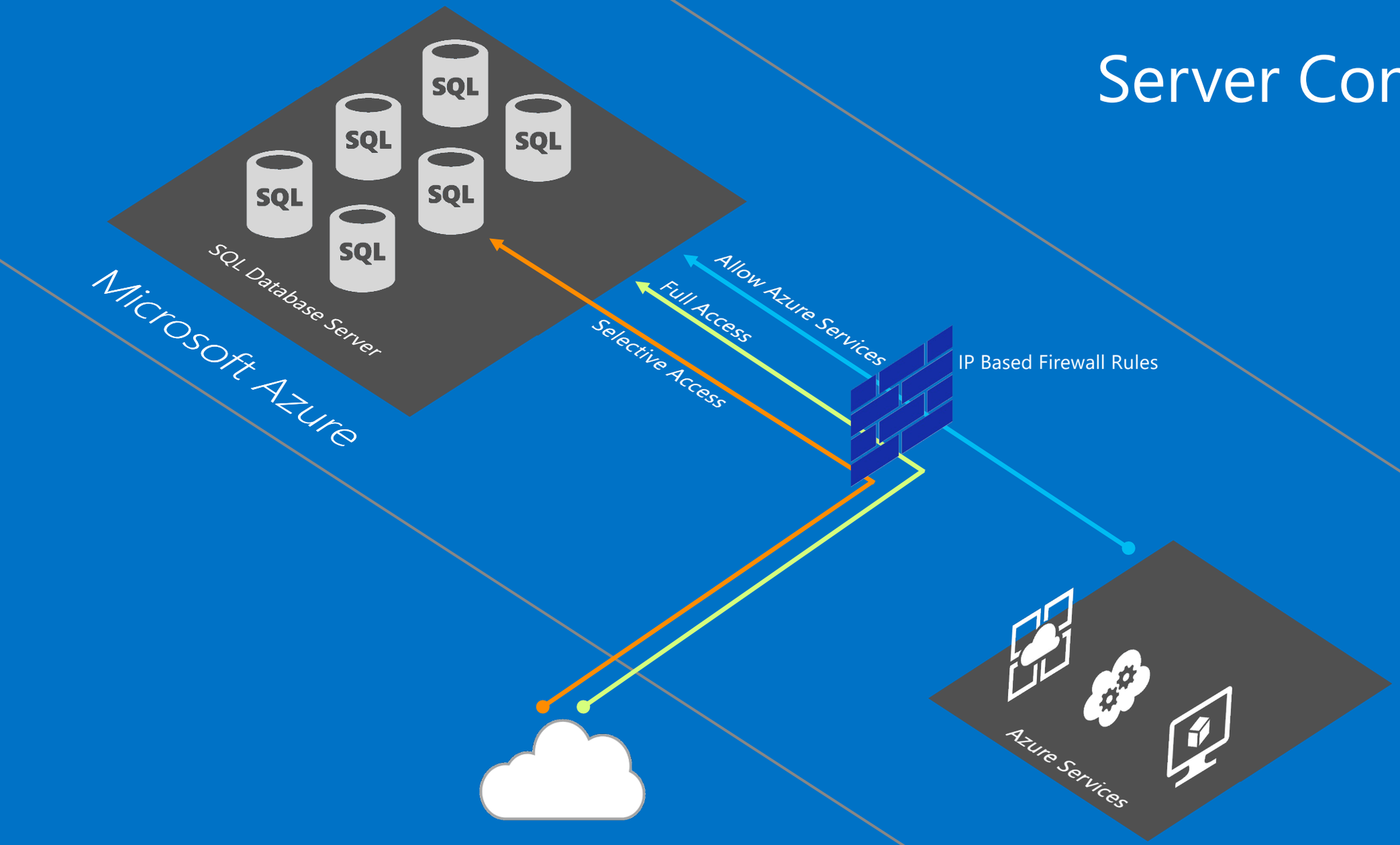
Microsoft

SQL Database Server

- The Service head contains databases
- Connect via automatically generated FQDN: {name}.database.windows.net
- Initially contains only a master database

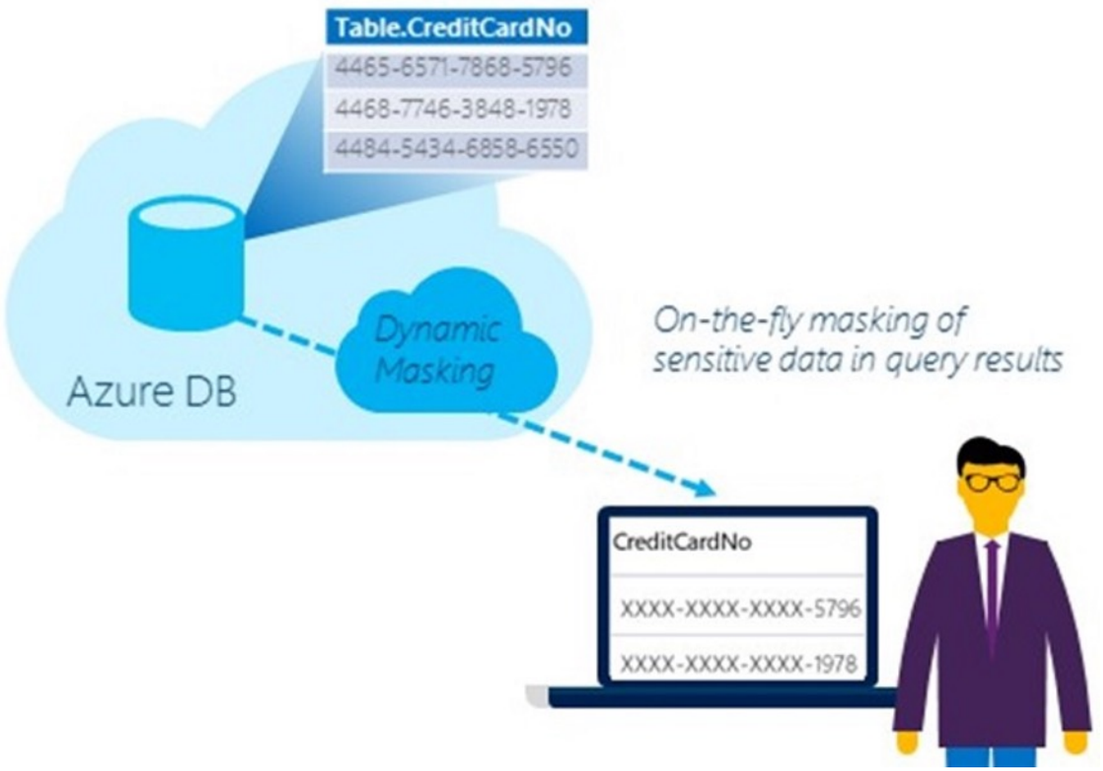
Microsoft

Server Connectivity



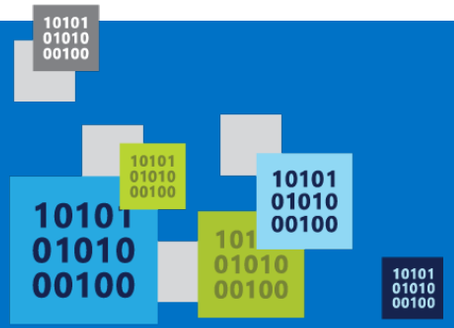
Microsoft

Dynamic Data Masking



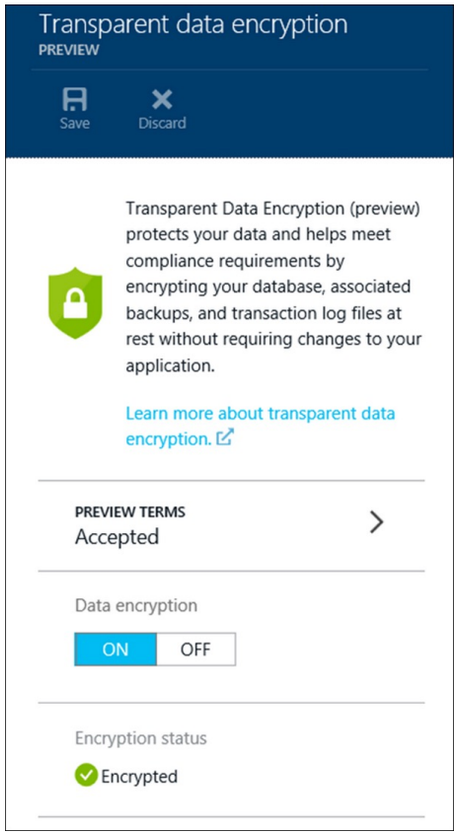
- Limits sensitive data exposure
- Prevents unauthorized access to data
- Policy-based security – no changes to data or application
- Meet regulatory compliance
- Dev/Test production data without compromising data

Protect Sensitive Data

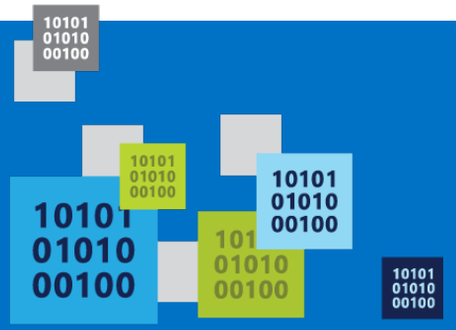


Limit Exposure of Sensitive Data

Transparent Data Encryption (TDE)



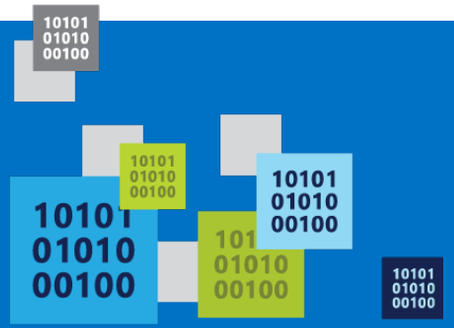
- Encrypted database, backups, and transaction log at rest
- 2-click provisioning
- Reduced attack surface area
- No code changes to existing applications
- Database encryption key - AES-256
- Meet regulatory compliance
- Accelerated hardware encryption



Encrypt and Protect Database

Row-Level Security (RLS)

- Fine-grained access over rows
- Access restrictions logic contained in database
- Simplified design and coding of security
- Meet regulatory compliance
- Reduced surface area of your security system



Fine-grained Access Over Rows

Point-in-time restore - “oops recovery”

- Auto backups
- Backups in Azure Storage and geo-replicated
- Creates a side-by-side copy, non-disruptive
- Backups retention policy: 7, 14 or 35 days
- Automated export of logical backups for long-term backup protection

Geo-restore – Emergency data recovery when you need it most

- Available in all tiers: Basic, Standard and Premium
- Built on geo-redundant Azure Storage
- Recover to any Azure region

Standard geo-replication

- Opt-in for Standard & Premium databases
- Creates a stand-by secondary
- Replicate to pre-paired Azure region
- Automatic data replication, asynchronous
- Opt-in via REST API, PowerShell or Azure Portal
- Microsoft-managed, RTO<24h, RPO<1 hr

Active geo-replication

- Self-service activation in Premium
- Create up to 4 readable secondaries
- Replicate to any Azure region
- Automatic data replication, asynchronous
- REST API, PowerShell or Azure Portal
- RTO<1h, RPO<5m, you choose when to failover

Auditing

- Configurable to track & log database activity
- Dashboard views in the portal for at-a-glance insights
- Pre-defined Power View reports for deep visual analysis on Audit log data
- Audit logs reside in your Azure Storage account
- Available in Basic, Standard, and Premium

Full-Text Search

- Fast and flexible indexing of textual data
- Data types: char, varchar, nchar, nvarchar, text, ntext, image, xml, varbinary(max), or FILESTREAM
- Handles high query volume
- Common use cases:
  - Searching websites, product catalogs, news items and more
  - Document management systems
  - Any applications that need to provide search capabilities over data stored in a SQL Database

Dynamic Management Views (DMV)

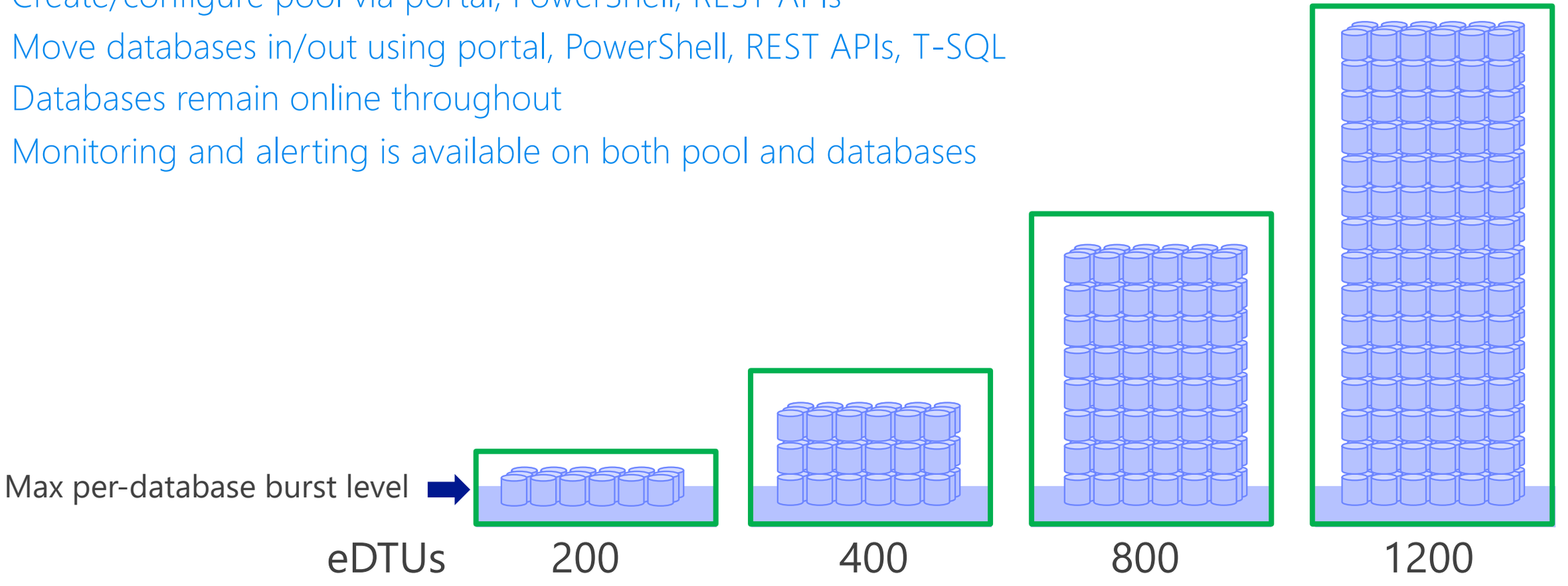
- Monitor common database, execution and transaction related events in near-real time
- Diagnose blocked or long-running queries, resource bottlenecks, poor query plans, and more
- Help improve capacity planning
- Use familiar T-SQL language

Purchase models

- Single database vs Elastic pool
- DTU vs vCore

Elastic Database Model

- Elastic databases, Elastic database pools
- Pooled resources leveraged by many databases
- Create/configure pool via portal, PowerShell, REST APIs
- Move databases in/out using portal, PowerShell, REST APIs, T-SQL
- Databases remain online throughout
- Monitoring and alerting is available on both pool and databases



Example (DTU / premium)

eDTUs per pool	Included storage per pool [1]	Max storage per pool [1,2]	Max number databases per pool	Max eDTUs per database	Price for eDTUs and included storage [3]
125	250 GB	1 TB	50	125	$684.38/month
250	500 GB	1 TB	100	250	$1,368.75/month
500	750 GB	1 TB	100	500	$2,737.50/month
1,000	1 TB	1 TB	100	1,000	$5,475.00/month
1,500	1.5 TB	1.5 TB	100	1,000	$8,212.51/month
2,000	2 TB	2 TB	100	1,750	$10,950.00/month
2,500	2.5 TB	2.5 TB	100	1,750	$13,687.50/month
3,000	3 TB	3 TB	100	1,750	$16,425.00/month
3,500	3.5 TB	3.5 TB	100	1,750	$19,162.50/month
4,000	4 TB	4 TB	100	4,000	$21,900.00/month

Example (vCore / standard)

Standard-series (Gen 5)

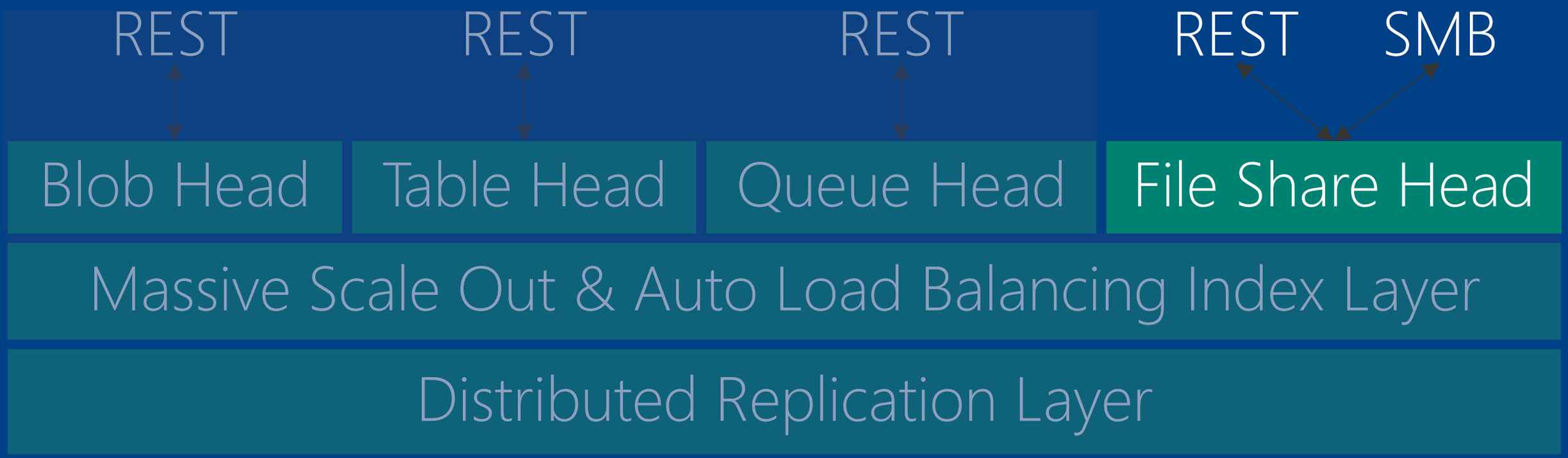
Standard-series (Gen 5) logical CPUs are based on Intel E5-2673 v4 (Broadwell) 2.3 GHz, Intel SP8160 (Skylake), Intel Xeon Platinum 8272CL 2.5 GHz (Cascade Lake) and Intel(R) Xeon Scalable 2.8 GHz processor (Ice Lake) processors. In the standard-series (Gen 5), 1 vCore = 1 hyper thread. The standard-series (Gen 5) logical CPU is great for most relational database servers.

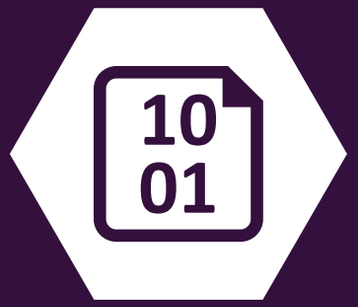
vCORE	Memory (GB)	Max Number Of Databases Per Pool	Pay as you go	1 year reserved capacity [2]	3 year reserved capacity [2]
2	10.2	100	**$390.42**/month	**$304.79**/month ~22% savings	**$255.95**/month ~34% savings
4	20.4	200	**$780.83**/month	**$609.57**/month ~22% savings	**$511.90**/month ~34% savings
6	30.6	500	**$1,171.24**/month	**$914.36**/month ~22% savings	**$767.85**/month ~34% savings
8	40.8	500	**$1,561.65**/month	**$1,219.14**/month ~22% savings	**$1,023.79**/month ~34% savings
10	51	500	**$1,952.06**/month	**$1,523.92**/month ~22% savings	**$1,279.74**/month ~34% savings

Questions?

Azure Storage

Azure Storage Architecture





Microsoft Azure
Storage Blob

Two Types of Blobs Under the Hood

Block Blob

Page Blob

Block Blob

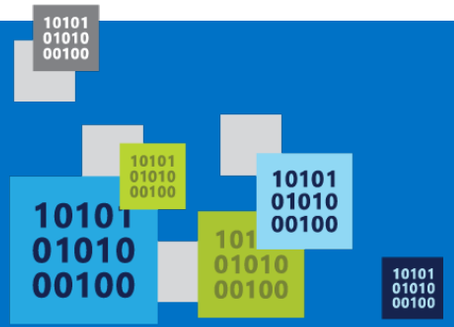
Targeted at streaming workloads

Each blob consists of a sequence of blocks

Each block is identified by a Block ID

Size limit 200GB per blob

Optimistic Concurrency via Etags



Page Blob

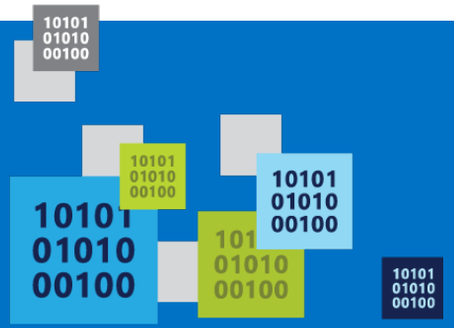
Targeted at random read/write workloads

Each blob consists of an array of pages

Each page is identified by its offset from the start of the blob

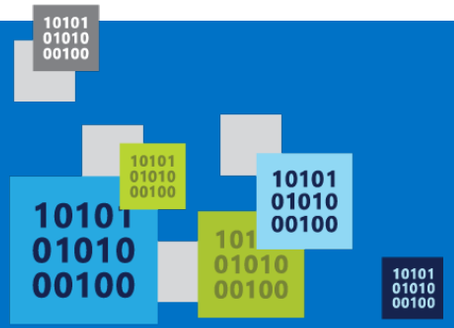
Size limit 1TB per blob

Optimistic or Pessimistic (locking) concurrency via leases



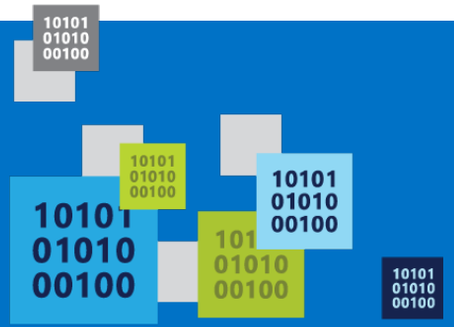
Blob Details – Containers

- A container holds a set of blobs
- Set access policies at the container level
- Associate Metadata with Container
- List the blobs in a container
- Including Blob Metadata and MD5
  no search on metadata WHERE MetadataValue = ?



Blob Details – Throughput

- Effectively in Partition of 1
- Target of 60MB/s per Blob



PutBlob

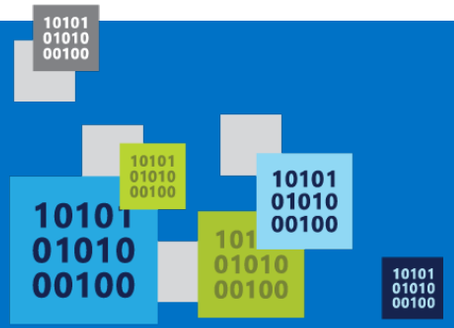
GetBlob

DeleteBlob

CopyBlob

SnapshotBlob

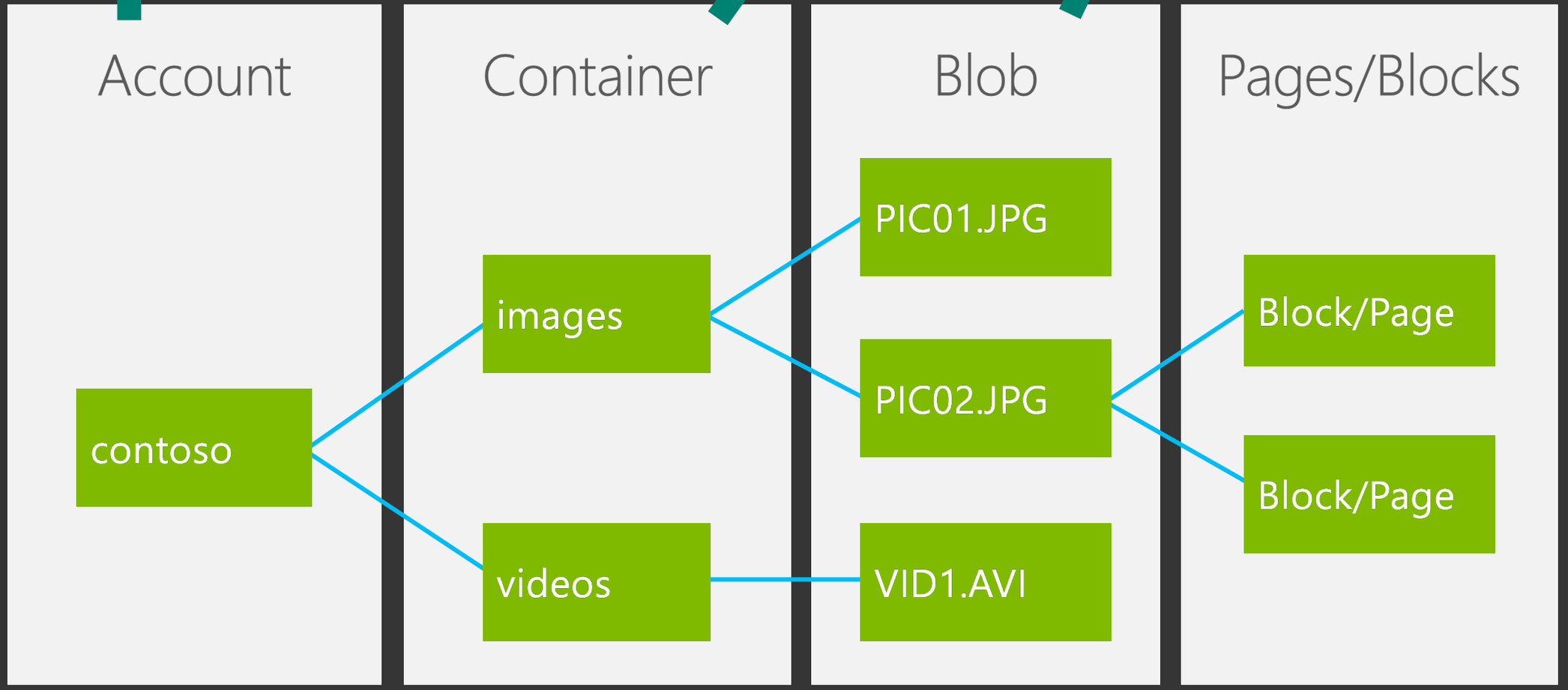
LeaseBlob



Blob Details – Main Web Service Operations

Blob Storage Concepts

`http://{account}.blob.core.windows.net/{container}/{blobname}`

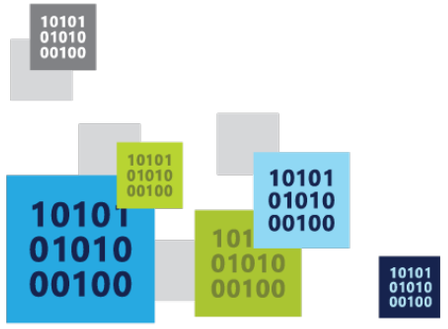


Blob Details – Blob always accessed by name

Can include '/' or other delimiter in name

e.g. /<container>/myblobs/smurf.png

blob name



Blob sample listing

Microsoft Azure

http://adventureworks.blob.core.windows.net/
Products/Bikes/SuperDuperCycle.jpg
Products/Bikes/FastBike.jpg
Products/Canoes/Hybrid.jpg
Products/Canoes/Flatwater.jpg
Products/Canoes/Whitewater.jpg
Products/Tents/PalaceTent.jpg
Products/Tents/ShedTent.jpg

GET http://.../products?comp=list&prefix=Tents

```
<Blobs>
        <Blob><Name>Tents/PalaceTent.jpg</Name>[...]</Blob>
        <Blob><Name>Tents/ShedTent.jpg</Name>[...]</Blob>
</Blobs>
```

Microsoft

Blob sample listing full response

```
<Blobs>
        <Blob>
                <Name>Tents/PalaceTent.jpg</Name>
                <Url>https://readinesscloudcamp.blob.core.windows.net/products/Tents/PalaceTent.jpg</Url>
                <LastModified>Wed, 17 Dec 2014 09:00:26 GMT</LastModified>
                <Etag>0x8D1E7EF08F31520</Etag>
                <Size>150027</Size>
                <ContentType>image/jpeg</ContentType>
                <ContentEncoding />
                <ContentLanguage />
        </Blob>
        <Blob>
                <Name>Tents/ShedTent.jpg</Name>
                <Url>https://readinesscloudcamp.blob.core.windows.net/products/Tents/ShedTent.jpg</Url>
                <LastModified>Wed, 17 Dec 2014 09:00:26 GMT</LastModified>
                <Etag>0x8D1E7EF08EA6257</Etag>
                <Size>150027</Size>
                <ContentType>image/jpeg</ContentType>
                <ContentEncoding />
                <ContentLanguage />
        </Blob>
</Blobs>
```

Blob sample listing with maxresults

Microsoft Azure

http://adventureworks.blob.core.windows.net/
Products/Bikes/SuperDuperCycle.jpg
Products/Bikes/FastBike.jpg
Products/Canoes/Hybrid.jpg
Products/Canoes/Flatwater.jpg
Products/Canoes/Whitewater.jpg
Products/Tents/PalaceTent.jpg
Products/Tents/ShedTent.jpg

http://.../products?comp=list&prefix=Canoes&maxresults=2

<Blob>Canoes/Hybrid.jpg</Blob>
<Blob>Canoes/Flatwater.jpg</Blob>
<NextMarker>1!28!Q2Fub2VzL1doaXRld2F0ZXIuanBn</NextMarker>

Microsoft

Blob sample listing with maxresults

Microsoft Azure

http://adventureworks.blob.core.windows.net/
Products/Bikes/SuperDuperCycle.jpg
Products/Bikes/FastBike.jpg
Products/Canoes/Hybrid.jpg
Products/Canoes/Flatwater.jpg
Products/Canoes/Whitewater.jpg
Products/Tents/PalaceTent.jpg
Products/Tents/ShedTent.jpg

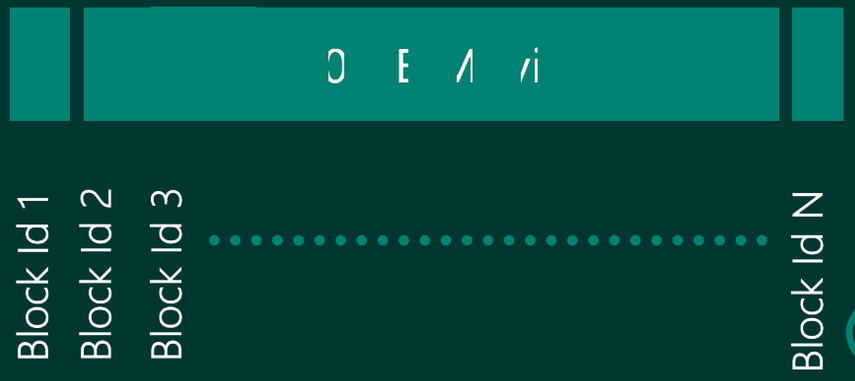
http://.../products?comp=list&prefix=Canoes&maxresults=2
&marker=1!28!Q2Fub2VzL1doaXRld2F0ZXIuanBn

<Blob>Canoes/Whitewater.jpg</Blob>
</NextMarker>

Microsoft

Uploading a Block Blob

Uploading

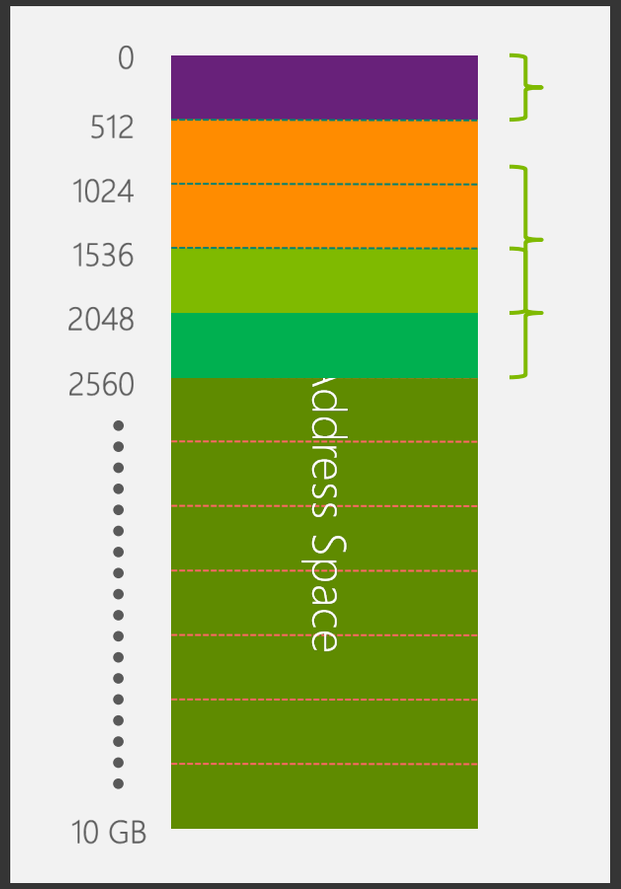


THE BLOB

```
blobName = "TheBlob.wmv";
PutBlock(blobName, blockId1, block1Bits);
PutBlock(blobName, blockId2, block2Bits);
.....
PutBlock(blobName, blockIdN,
blockNBits);
PutBlockList(blobName,
                    blockId1,...,blockIdN);
```

TheBlob.wmv

Page Blob – Random Read/Write



Create blob and specify Blob Size = 10 Gbytes

Fixed Page Size = 512 bytes

Random Access Operations:

PutPage[512, 2048)

PutPage[0, 1024)

ClearPage[512, 1536)

PutPage[2048,2560)

GetPageRange[0, 4096) returns valid data ranges:

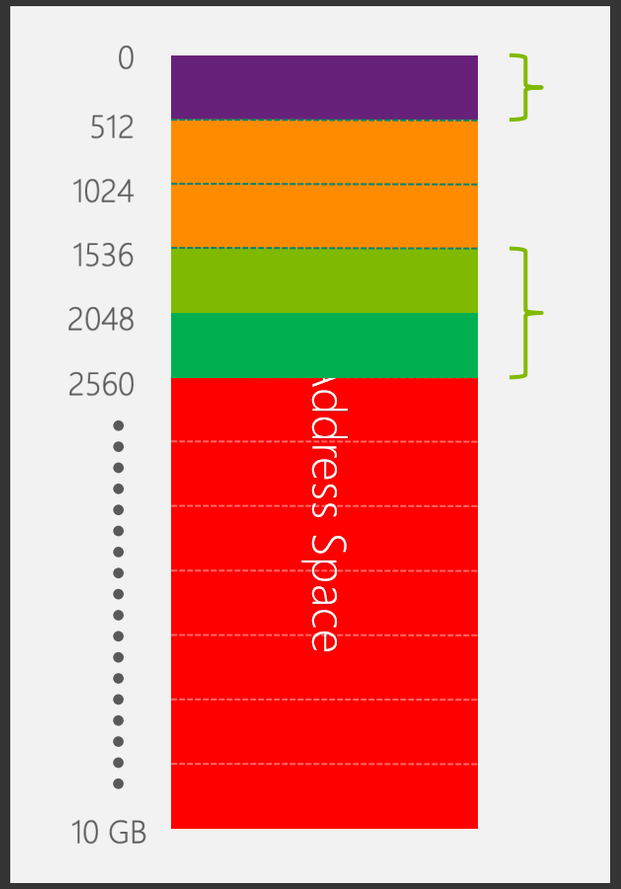
[0,512) , [1536,2560)

GetBlob[1000, 2048) returns:

All 0 for first 536 bytes

Next 512 bytes data stored in [1536,2048)

Page Blob – Random Read/Write

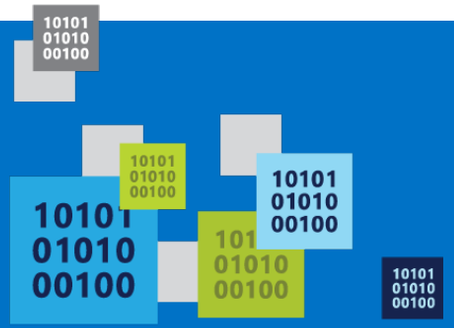


Sparse storage:
Only charged for pages with data stored in them

Shared Access Signatures

Fine grain access rights to blobs and containers

Sign URL with storage key – permit elevated rights



Shared Access Signatures – Two broad approaches

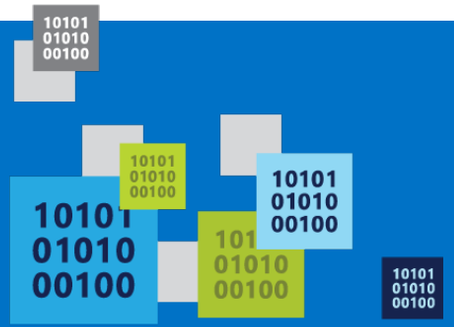
Ad-hoc:
Stored Access Policy

Policy based:
Shared Access Signature

Shared Access Signatures – Revocation

Use short time periods and re-issue

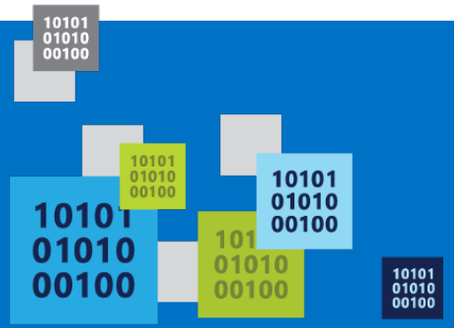
Use container level policy that can be deleted



Shared Access Signatures – Ad Hoc Signatures

Create Short Dated Shared Access Signature

- Signed resource Blob or Container
- AccessPolicy Start, Expiry and Permissions
- Signature HMAC-SHA256 of above fields

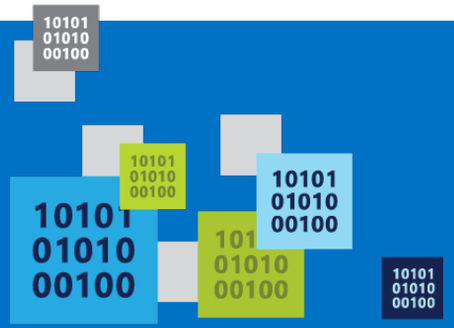


Shared Access Signatures – Ad Hoc Signatures

Use case

Single use URLs

E.g. Provide URL to mobile client to upload to container



Microsoft Azure
Storage Files

Sharing Files – The old way

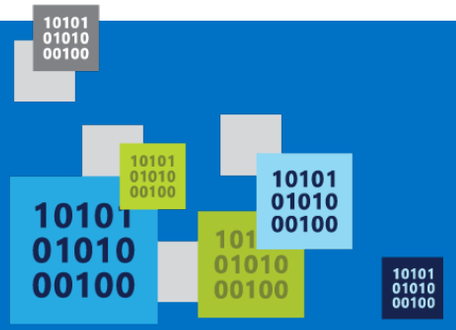
Setup an IaaS VM to host a File Share backed by an IaaS Disk

Write code to find the IaaS File Share from the rest of the VMs in your service.

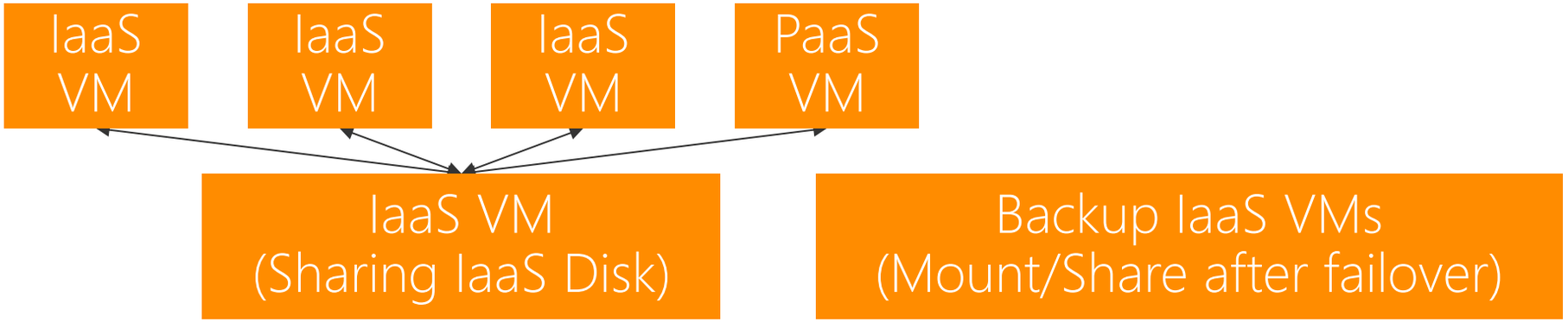
Write some code to provide high availability

Handle host upgrades, node failures

You can only access the File Share from other VMs

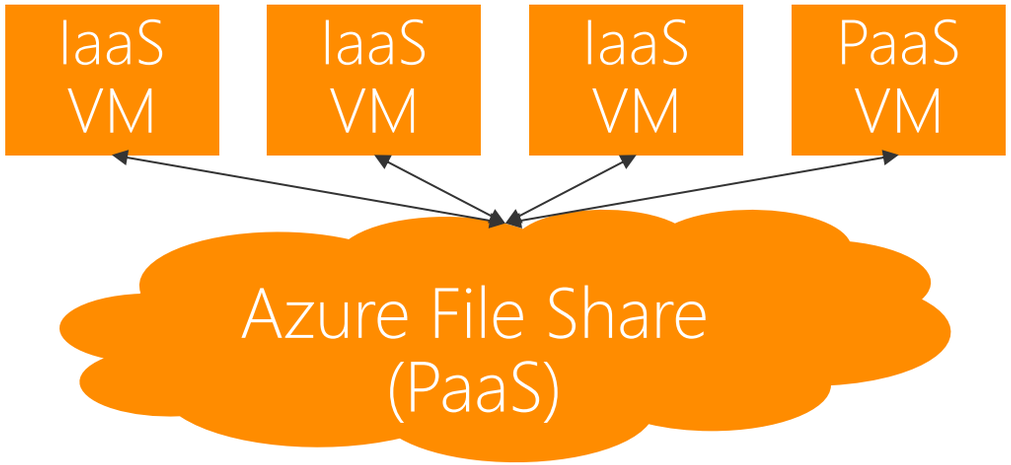


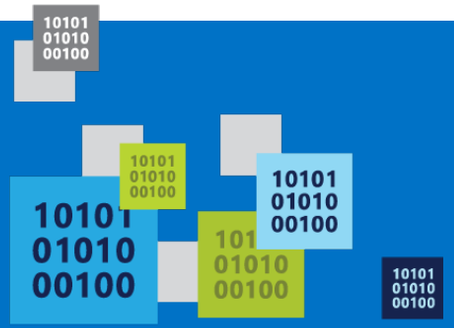
Sharing Files – The old way



Azure Files

- Shared Network File Storage for Azure
- Availability, durability, scalability are managed automatically
- Supports two interfaces: SMB and REST





Azure Files – Usage

- Share data across VMs and applications
- Share settings throughout services
- Dev/Test/Debug

Questions?

Homework

Do (1)

Create automation using both AZ CLI and Azure PowerShell CMDlets. For each script prepare the parameters file(s) that script will be able to parse.

Do (2)

Script that can create Storage Account.

Input parameters:

Region
Name
Pricing tier

Do (3)

Script that can configure automatic backups for Azure App Service to Storage Account (including connected databases).

Input parameters:

App Service name
Storage Account name
Schedule
Retention policy

Do (4)

Script that can delete all services from the Resource Group.

Input parameters:

Resource Group name.

Do (5)

Connect GitHub and Azure DevOps to your Azure Subscriptions.

Create pipelines that deploys the infrastructure to Azure using the scripts from above. Pipeline should allow to choose which resource group will be used to deploy the infrastructure.

Deadline

Recommended – by the end of the day 26.08.2022

Maximum – by the end of the day 26.08.2022