Microsoft

DA-DP-TS324

Best Practices for Azure Databricks architecture, security and networking

Bhanu Prakash

Azure Databricks

Fast, easy, and collaborative Apache Spark™-based analytics platform

Increase productivity

Build on a secure, trusted cloud

Scale without limits

Built with your needs in mind

- Role-based access controls
- Effortless autoscaling
- Live collaboration
- Enterprise-grade SLAs
- Best-in-class notebooks
- Simple job scheduling

Seamlessly integrated with the Azure Portfolio

Our customers have three common objectives

"We want to extend to untapped sources"

Modern Data Warehouse

"We want to use ML and AI to get deeper insights from our data"

Advanced Analytics

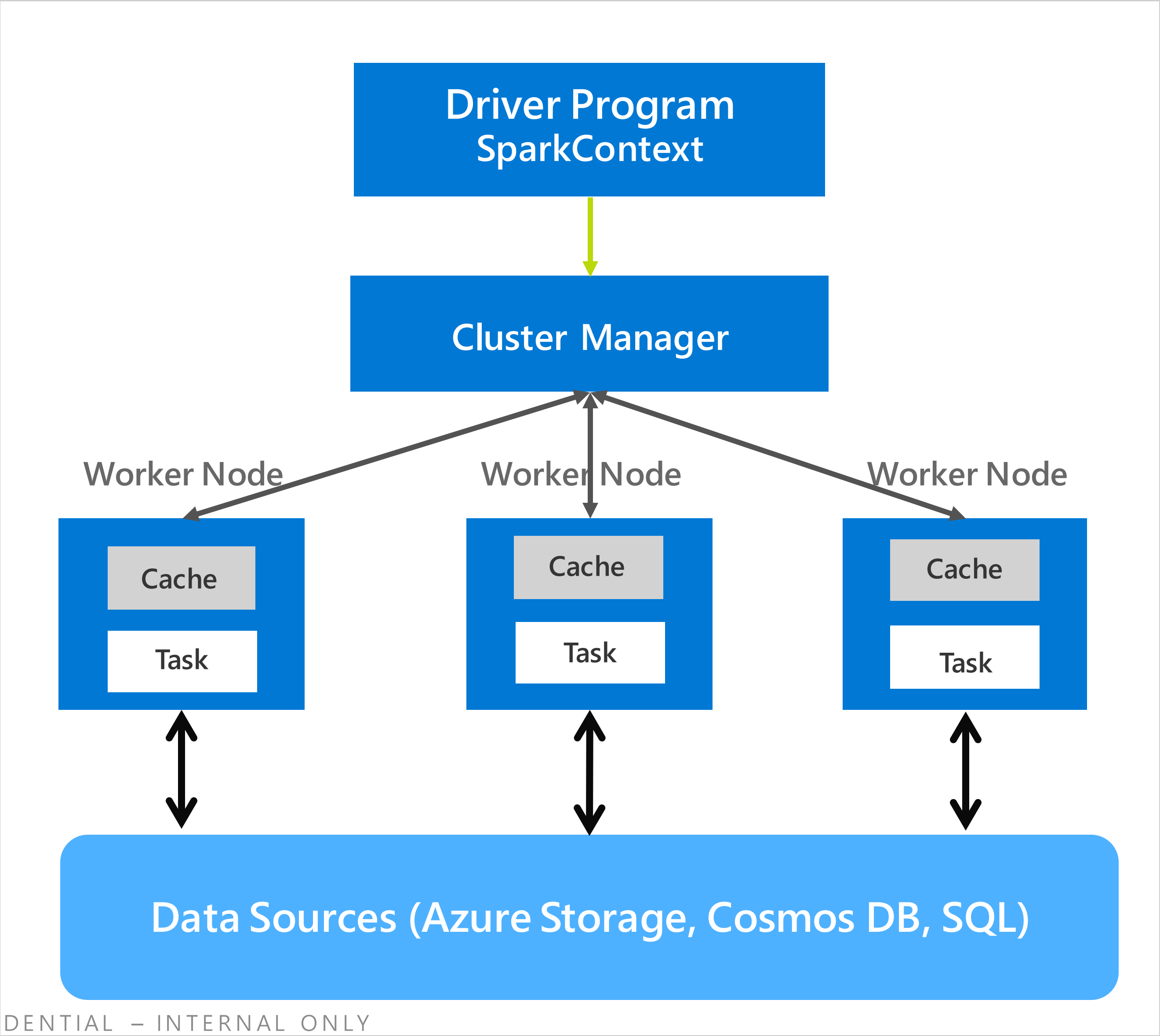
"We want to get insights from our devices in real-time"

Real-time Analytics

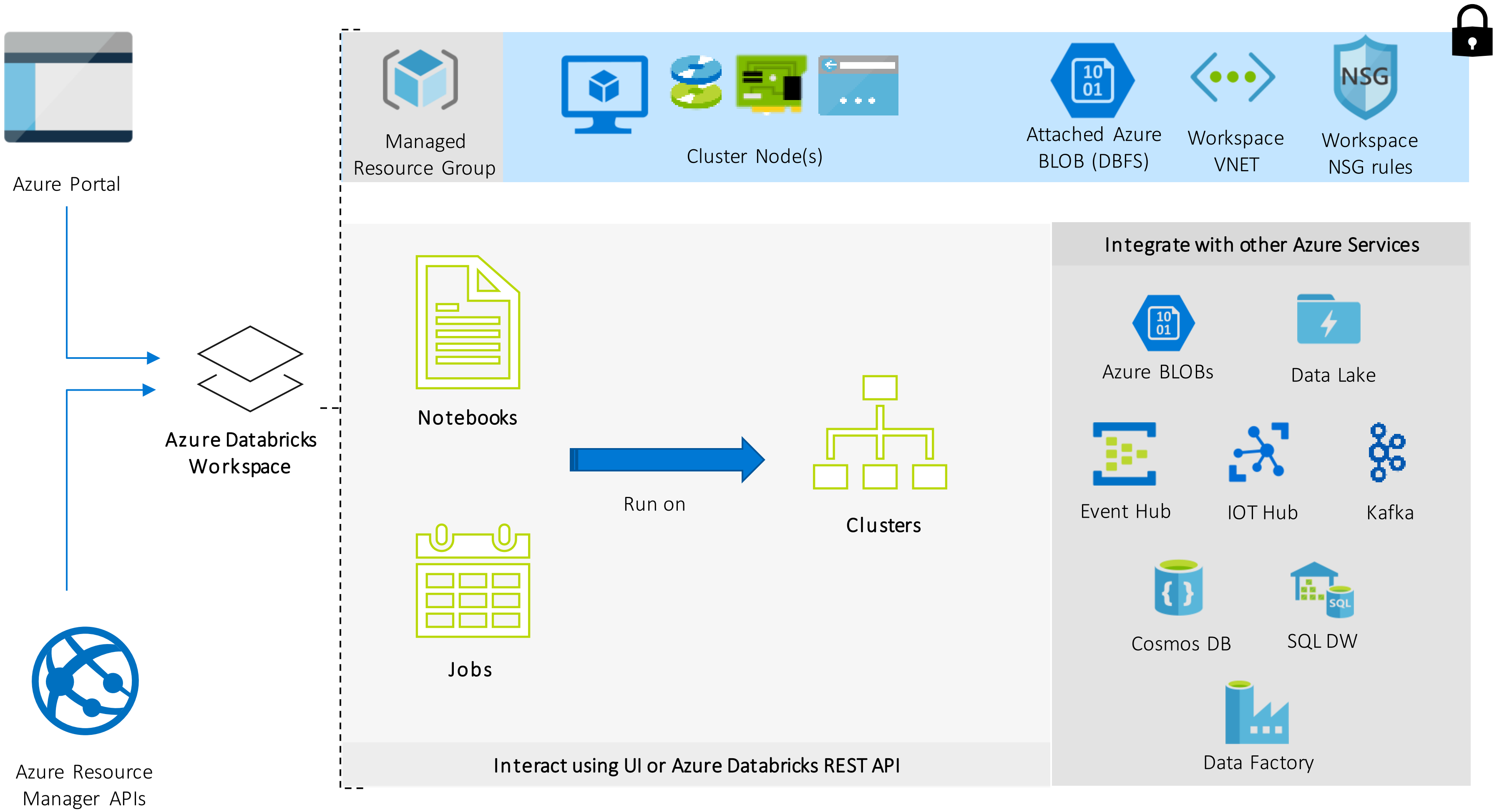
Architecture and Deployment

General Spark Cluster Architecture

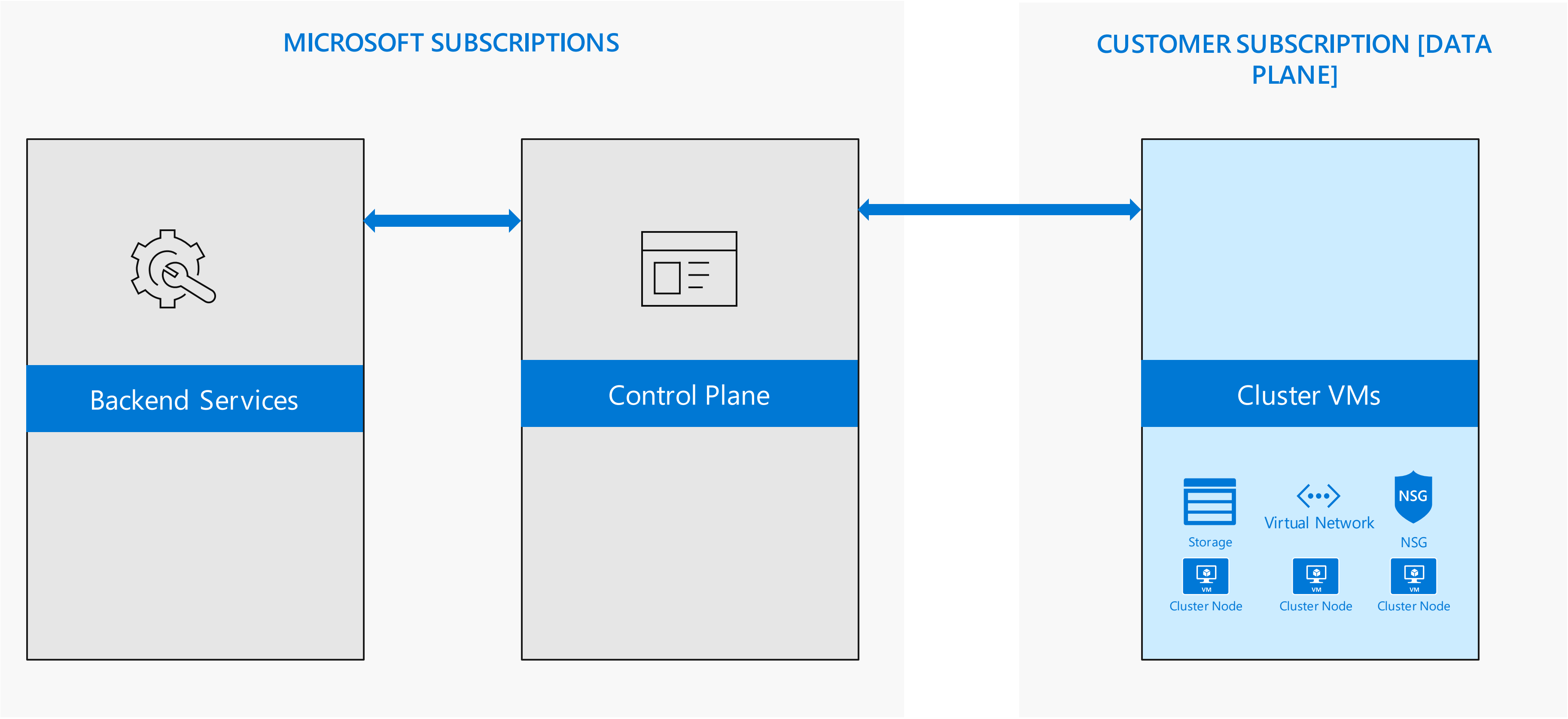
- Spark is designed to run on a Cluster
- A cluster is a set of VMs
- Spark can horizontally scale, bigger workload = Add more VMs
- Azure Databricks can automatically scale up and down
- Data can read from Azure Storage or Azure Datalake Storage



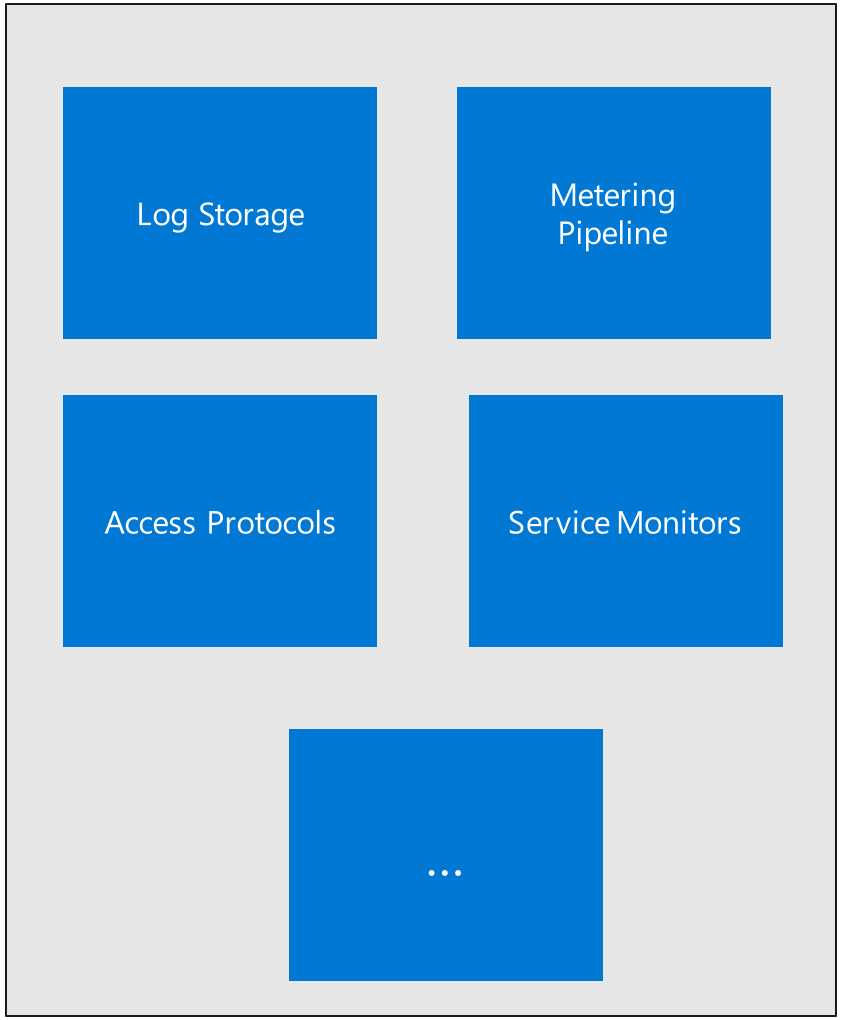
Azure Databricks – Customer view

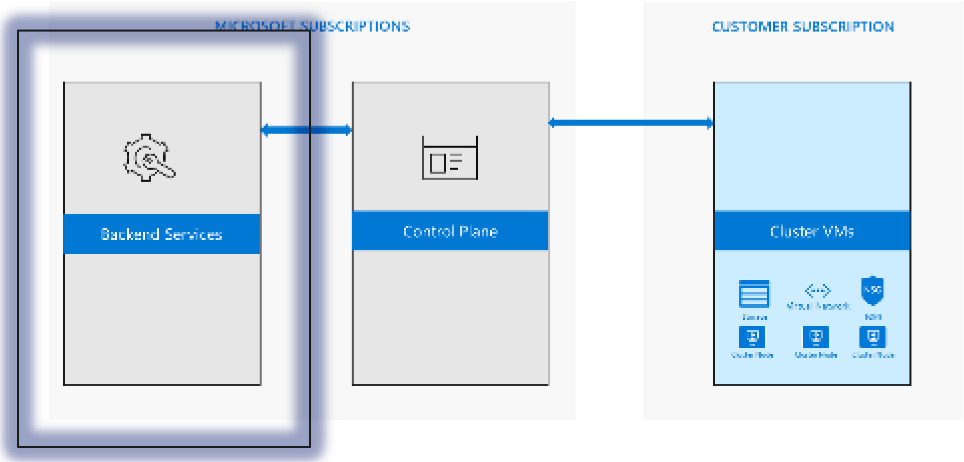


High Level Concepts

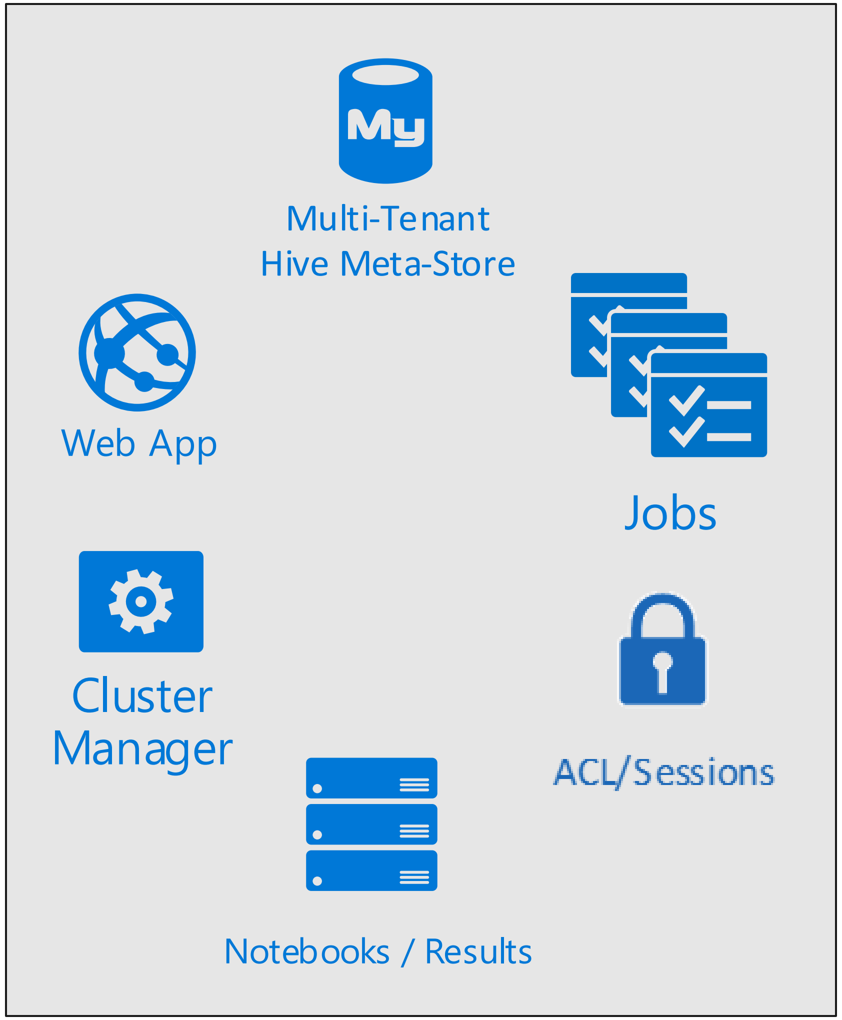


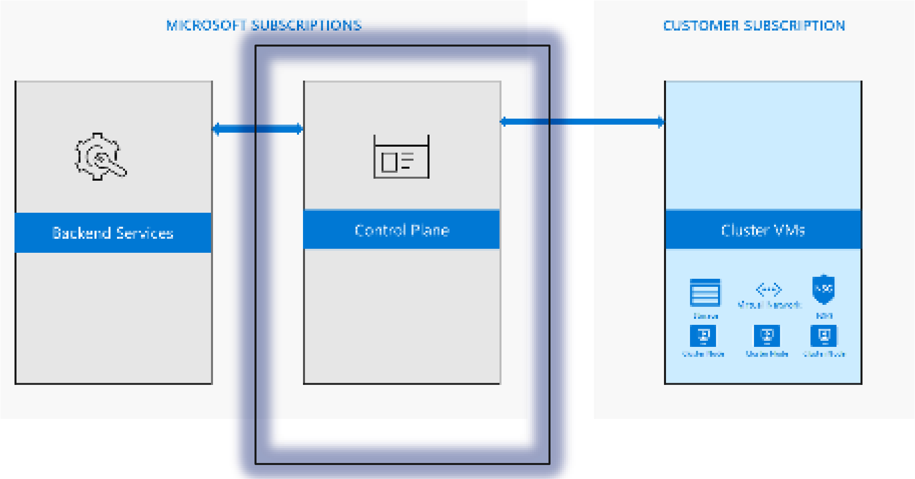
Backend Services



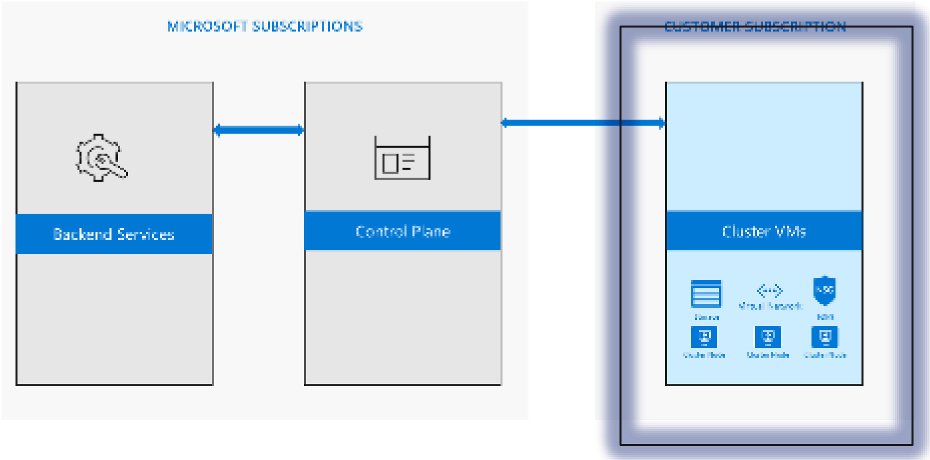


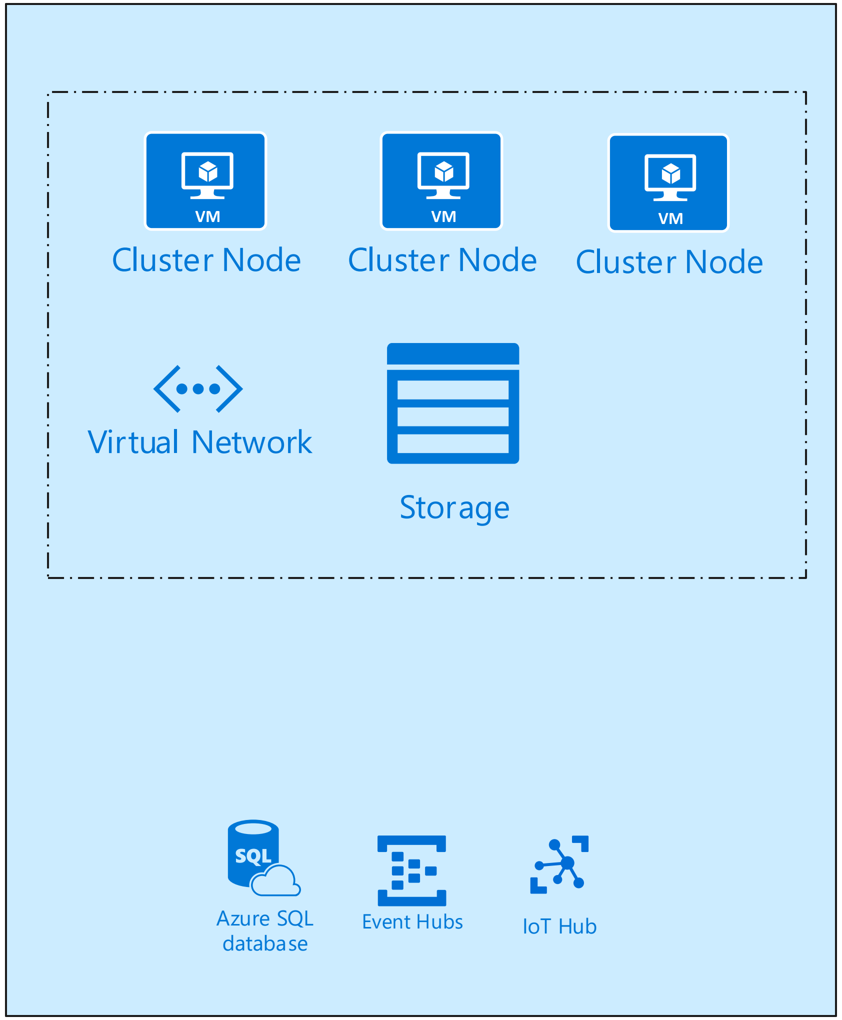
Control Plane





Customers Subscription [Data Plane]





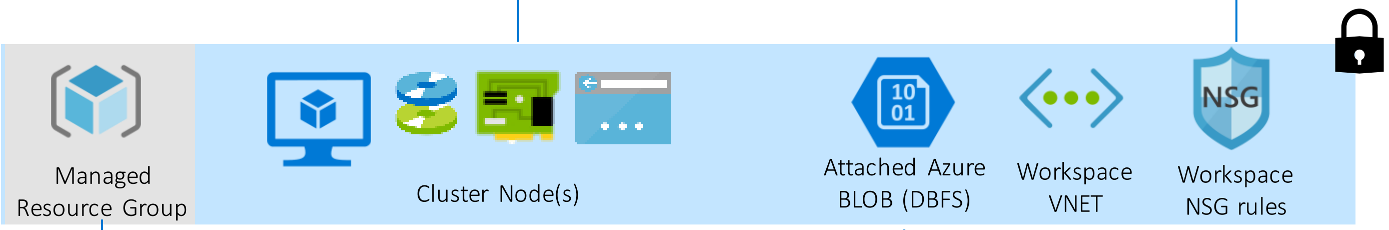
Minimum default resources that customer is billed for

a. VMs
b. DBUs
c. Public IP
d. Storage account – default and customer owned
e. Managed disk

Managed resource group

- For each driver or worker node in each cluster, a VM, SSD, Network Interface and IP address resource is created
- Each resource is tagged with
  - “Vendor : Databricks”
  - “ClusterName :” + {Cluster Name}
  - Custom Tags can be added at Cluster creation

- All resources in the RG are in a pre-configured VNET
- VNET allows communication between nodes and with the Control Plane
- NSG is locked contains the Control Plane IP addresses
- VNET & NSG are locked but customers can peer with other VNETs



- A locked RG is created in your subscription when you create the Azure Databricks Workspace
- RG Name = “databricks-rg”+{workspace} + {random chars}

- Each workspace comes with an attached blob storage, contains workspace related configuration
- This can be access from Notebooks and Jobs as DBFS
- You can mount your own Azure Storage or ADLS to this DBFS

Regional distribution of the control plane

- Available today in 24 Regions / 6 Geographies
- Every geography has a Control Plane & Backend Services
- All dependent services run in that geography
- Data never leaves the geography
- Geographies : https://azure.microsoft.com/en-us/global-infrastructure/geographies/

Disaster Recovery for Azure Databricks

- Provision two Azure Databricks workspaces in separate Azure geo regions
- Use GRS storage – Data can be accessed in secondary region
- Migrate these resources to secondary region – users, user folders, notebooks, cluster configuration, jobs configuration, libraries, init scripts, and reconfigure access control
- https://docs.microsoft.com/en-us/azure/azure-databricks/howto-regional-disaster-recovery

Who has access to Control Plane ?

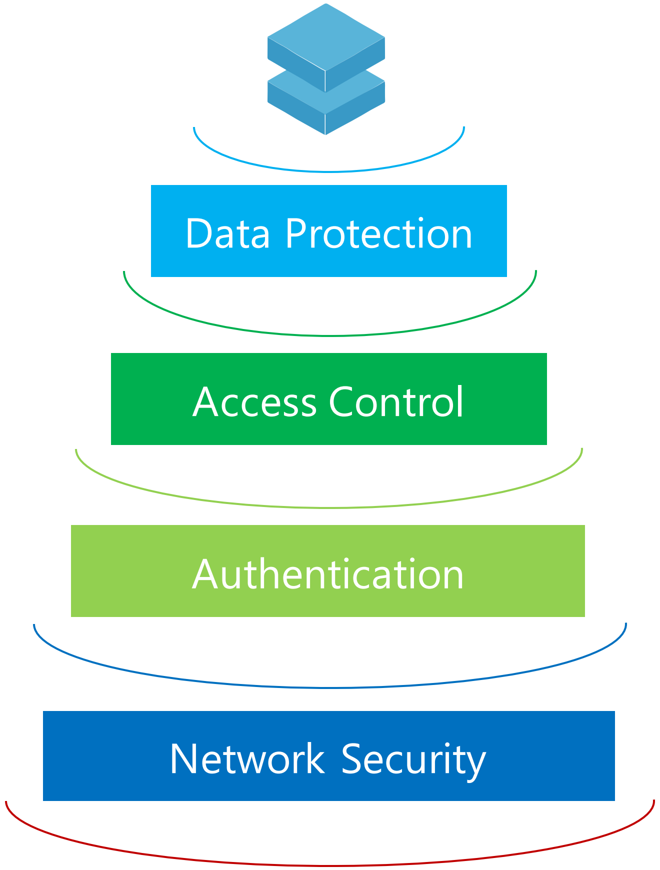
Common Scenarios – When deploying a new feature, when making a fix, when adding a new region, automated jobs to read telemetry.

Policies and Procedures

- Follows all Azure Guidelines
- Access only allowed via secure hardware & JIT
- Logged & Audited

Security and Networking

Enterprise Grade Security that is Easy-to Use



- Encryption-at-rest – Service Managed Keys, User Managed Keys
- File/Folder Level ACLs for AAD Users, Groups, Service Principals
- Encryption-in-flight (Transport Layer Security TLS)

- Role Base Access Control for Clusters, Workspaces, Notebooks
- Access Control for Tables

Azure Active Directory Authentication (w/ MFA)
Azure Active Directory Conditional Access

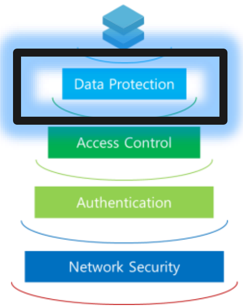
VNET – Managed & Injection*

✓

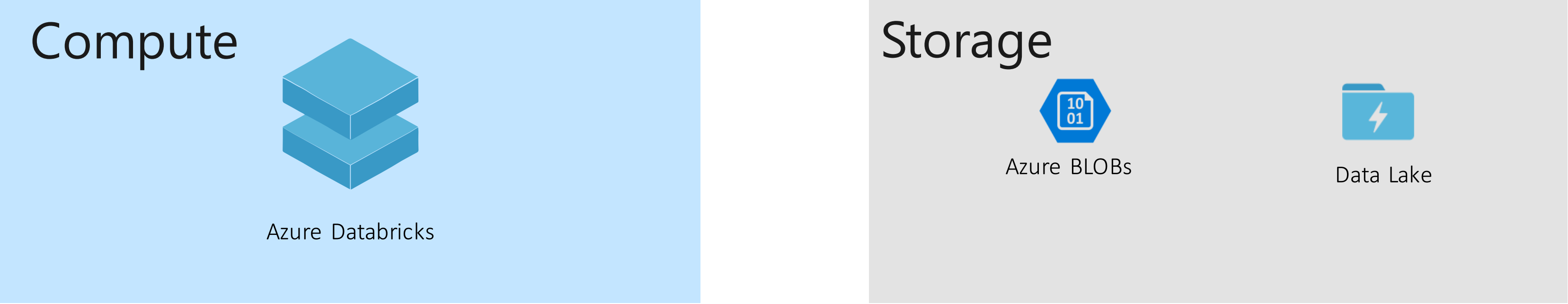
Defense in Depth

* VNET Injection support in Public Preview

Data Protection | Encryption - Data at rest

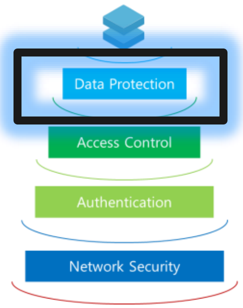


- Azure Databricks has separation of compute and storage

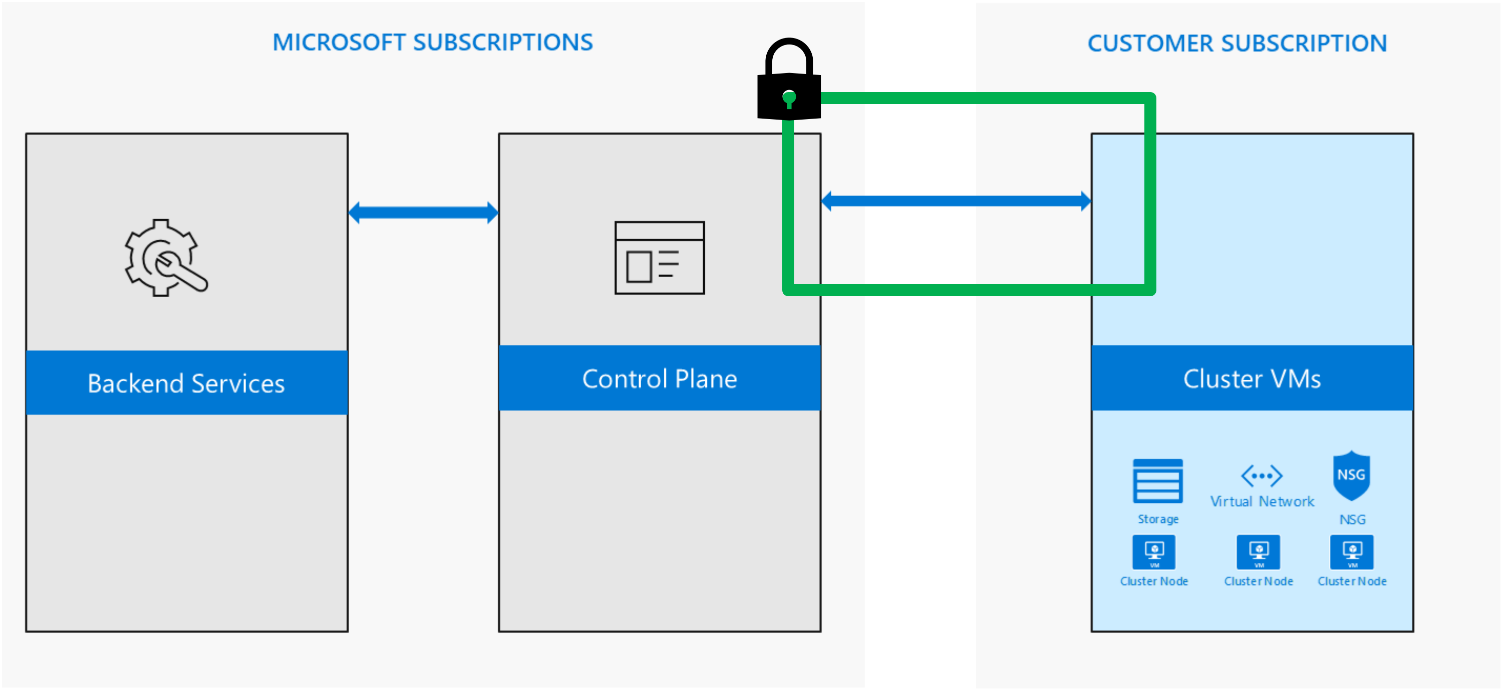


- Storage Services such as Azure Blob Store, Azure Data Lake Storage Provide
  - Encryption of Data – Remote storage and managed disk backed by blob storage using SSE
  - Customer Managed Keys or Microsoft Managed Keys
  - File/Folder Level ACLs (Azure Data Lake Storage)
- All Azure Databricks provided data stores are encrypted at rest

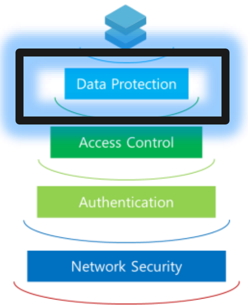
Data Protection | Encryption - Data in motion



- All the traffic from the Control Plane to the Clusters in the customer subscription is always encrypted with TLS.
- All the traffic to Data Plane is encrypted
- All the traffic to Control Plane is encrypted – Port 443 - HTTPS



Secrets in Notebooks – Understanding the need

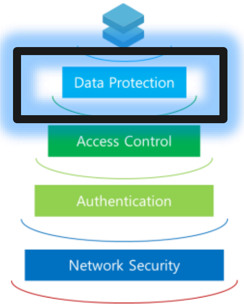


- Customer often connect to other Azure resources such as Azure BLOB Storage, Azure Data Lake, SQL DW from Azure Databricks

- A “Connection String” is required to connect to these services. This string may contain secrets.

- Customers don’t want to store Secrets in the clear

Securing secrets in Notebooks



Data Protection

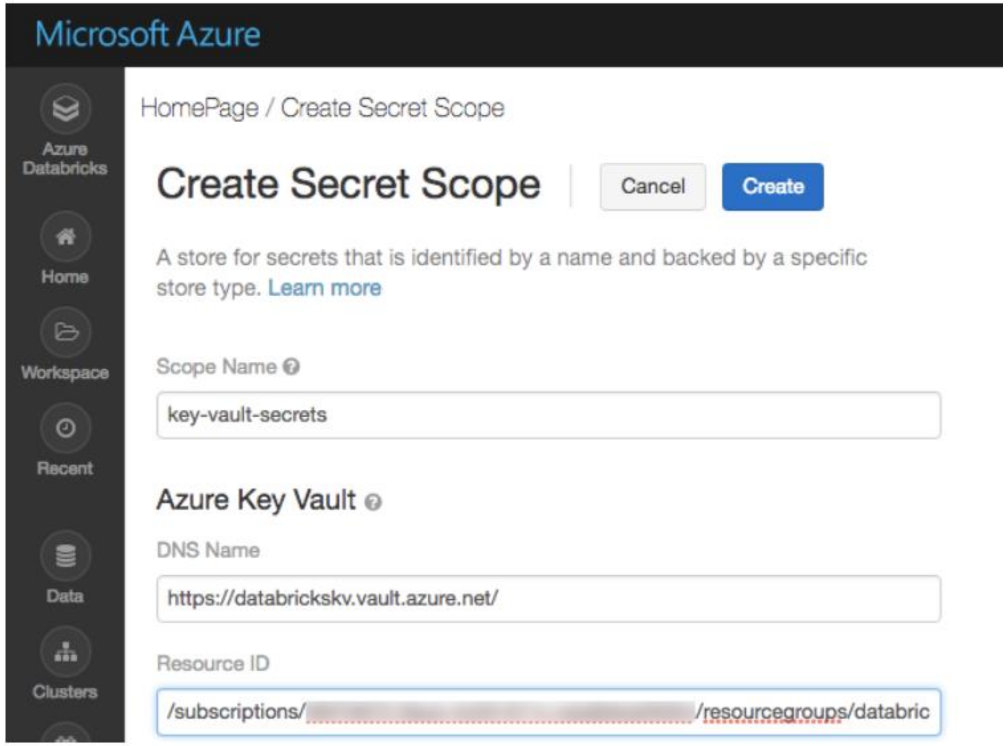
Access Control

Authentication

Network Security

- Using our Secrets APIs, Secrets can be securely stored including in a Key Vault
- Authorized users can consume the secrets to access services but cannot see them.
- Assign granular permissions with premium
- Use multiple AKV to isolate secrets

https://docs.azuredatabricks.net/user-guide/secrets/secret-scopes.html



HomePage / Create Secret Scope

Create Secret Scope

A store for secrets that is identified by a name and backed by a specific store type. Learn more

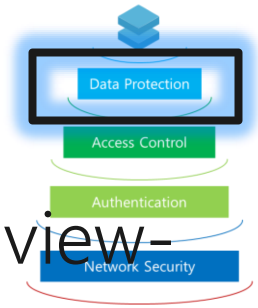
Scope Name: key-vault-secrets

Azure Key Vault

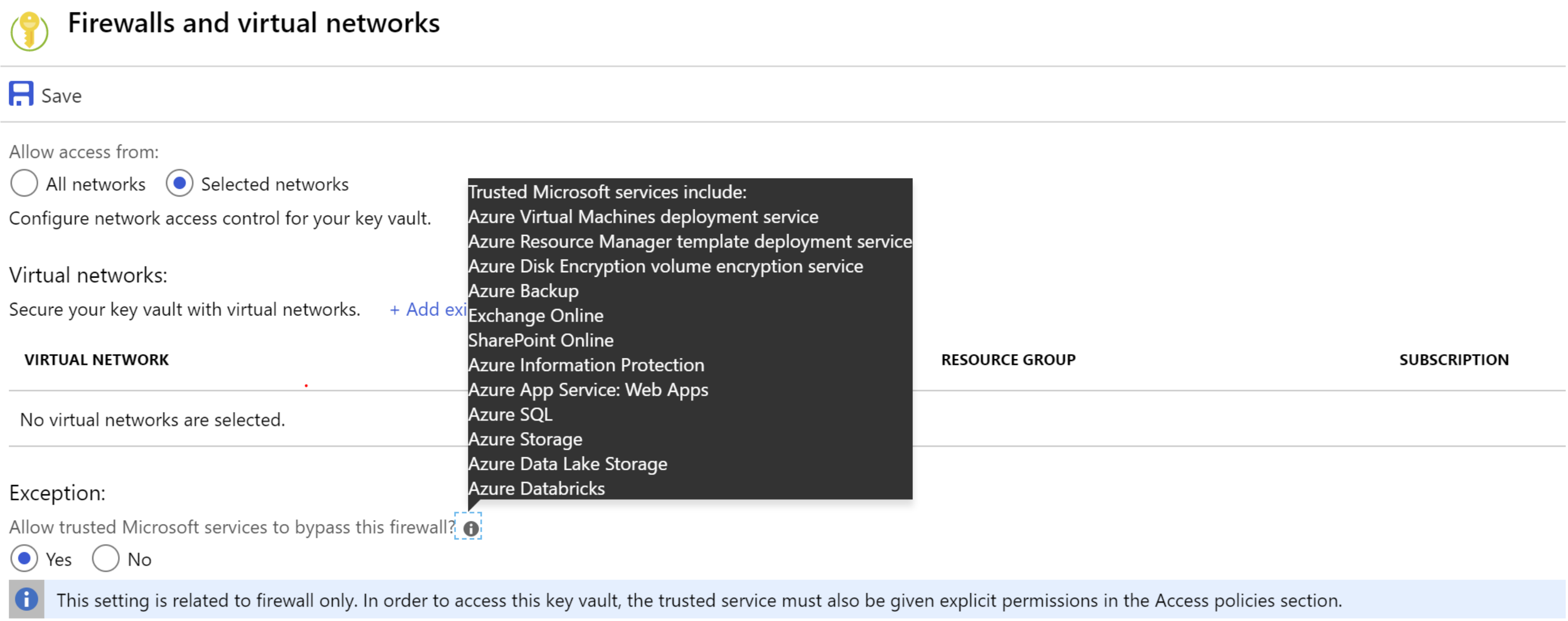
DNS Name: https://databrickskv.vault.azure.net/

Resource ID: /subscriptions/[redacted]/resourcegroups/databric

Securing secrets in Notebooks



https://docs.microsoft.com/en-us/azure/key-vault/key-vault-overview-vnet-service-endpoints



Firewalls and virtual networks

Allow access from:

○ All networks ● Selected networks

Configure network access control for your key vault.

Virtual networks:

Secure your key vault with virtual networks. + Add exi

VIRTUAL NETWORK	RESOURCE GROUP	SUBSCRIPTION
No virtual networks are selected.		

Trusted Microsoft services include:
Azure Virtual Machines deployment service
Azure Resource Manager template deployment service
Azure Disk Encryption volume encryption service
Azure Backup
Exchange Online
SharePoint Online
Azure Information Protection
Azure App Service: Web Apps
Azure SQL
Azure Storage
Azure Data Lake Storage
Azure Databricks

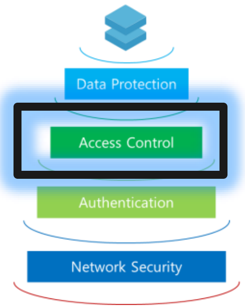
Exception:

Allow trusted Microsoft services to bypass this firewall? ⓘ

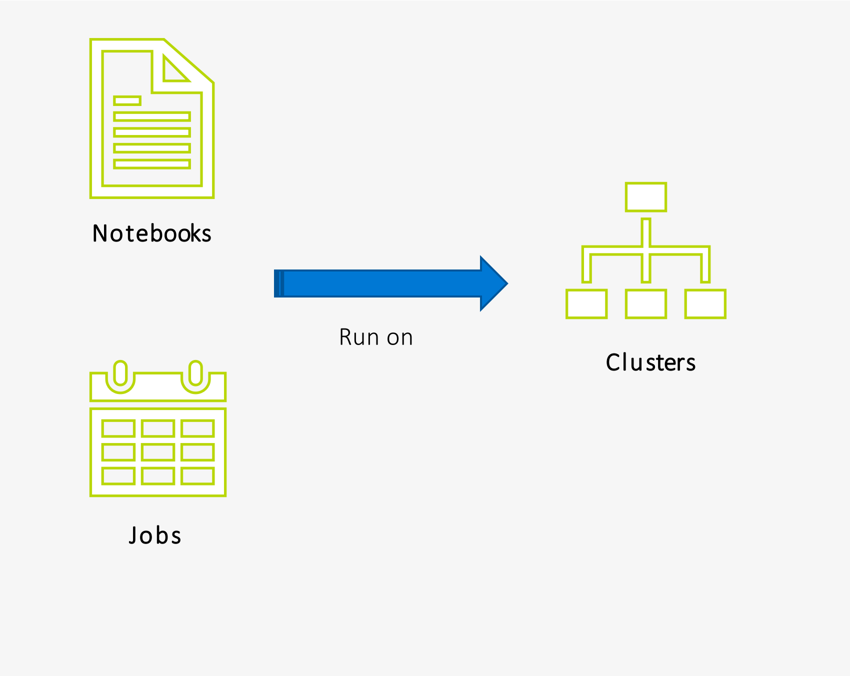
● Yes ○ No

ⓘ This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions in the Access policies section.

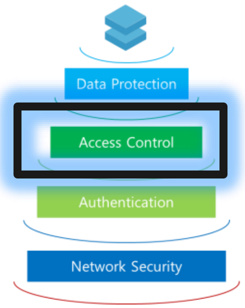
Access Control



- Many users in the customers organization can use the Service
- Different users have different roles – Admin, Data Scientist, Engineers
- Access Controls lets you limit what users can do

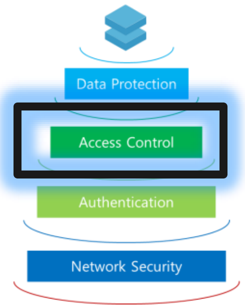


Access Control | Folders

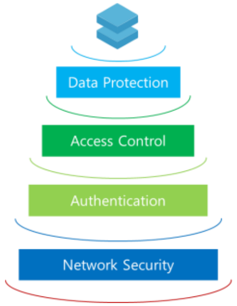


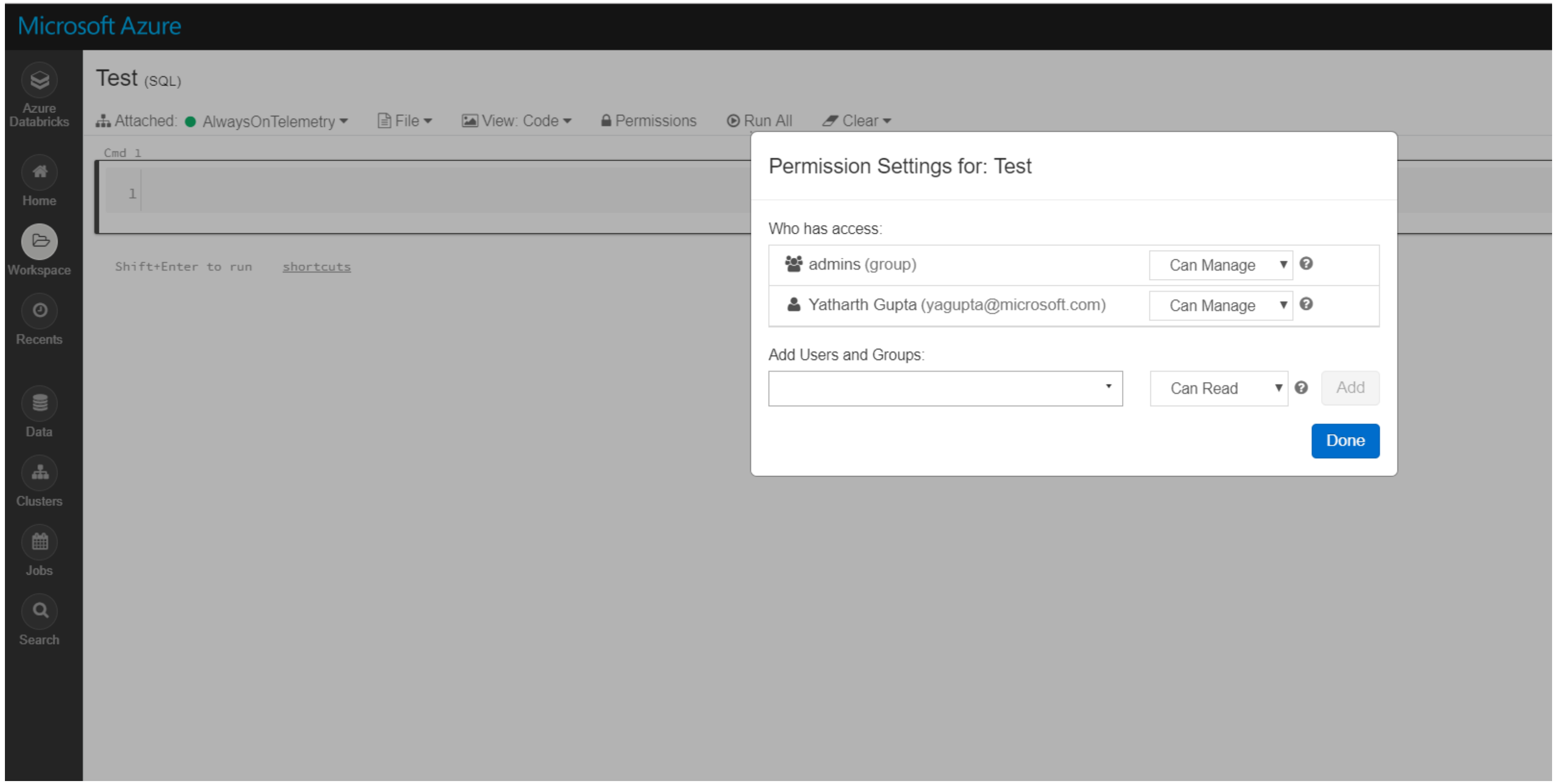
Ability	No Permissions	Read	Run	Edit	Manage
View items		x	x	x	x
Create, clone, import, export items		x	x	x	x
Run commands on notebooks			x	x	x
Attach/detach notebooks			x	x	x
Delete items				x	x
Move/rename items				x	x
Change permissions					x

Access Control | Notebooks



Ability	No Permissions	Read	Run	Edit	Manage
View cells		x	x	x	x
Comment		x	x	x	x
Run commands			x	x	x
Attach/detach notebooks			x	x	x
Edit cells				x	x
Change permissions					x





Permission Settings for: Test

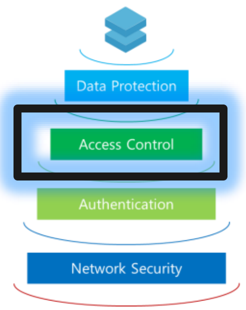
Who has access:

admins (group)	Can Manage
Yatharth Gupta (yagupta@microsoft.com)	Can Manage

Add Users and Groups:

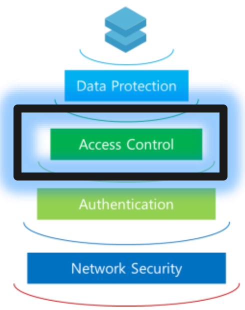
Can Read

Access Control | Jobs



Ability	No Permissions	Can View	Can Manage Run	Is Owner	Can Manage (admin)
View job details and settings	x	x	x	x	x
View results, Spark UI, logs of a job run		x	x	x	x
Run now			x	x	x
Cancel run			x	x	x
Edit job settings				x	x
Modify permissions				x	x

Access Control | Clusters



Data Protection

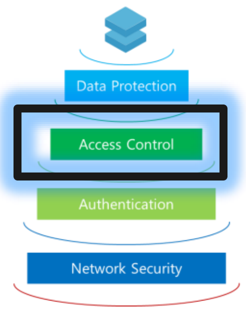
Access Control

Authentication

Network Security

Ability	No Permissions	Can Attach To	Can Restart	Can Manage
Attach notebook to cluster		x	x	x
View Spark UI		x	x	x
View cluster metrics		x	x	x
Terminate cluster			x	x
Start cluster			x	x
Restart cluster			x	x
Edit cluster				x
Attach library to cluster				x
Resize cluster				x
Modify permissions				x

Access Control | Tables



Objects

CATALOG | DATABASE | TABLE | VIEW | FUNCTION | ANONYMOUS FUNCTION | ANY FILE

Privileges

SELECT - read access to an object

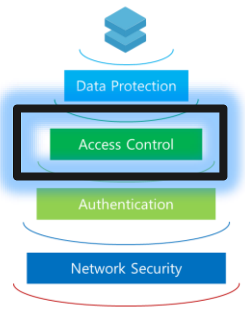
CREATE - ability to create an object (eg. Table in a Database)

MODIFY - ability to add/delete/modify data in an Object

READ_METADATA - ability to read Meta data about an object

ALL_PRIVELEGES - all of the above

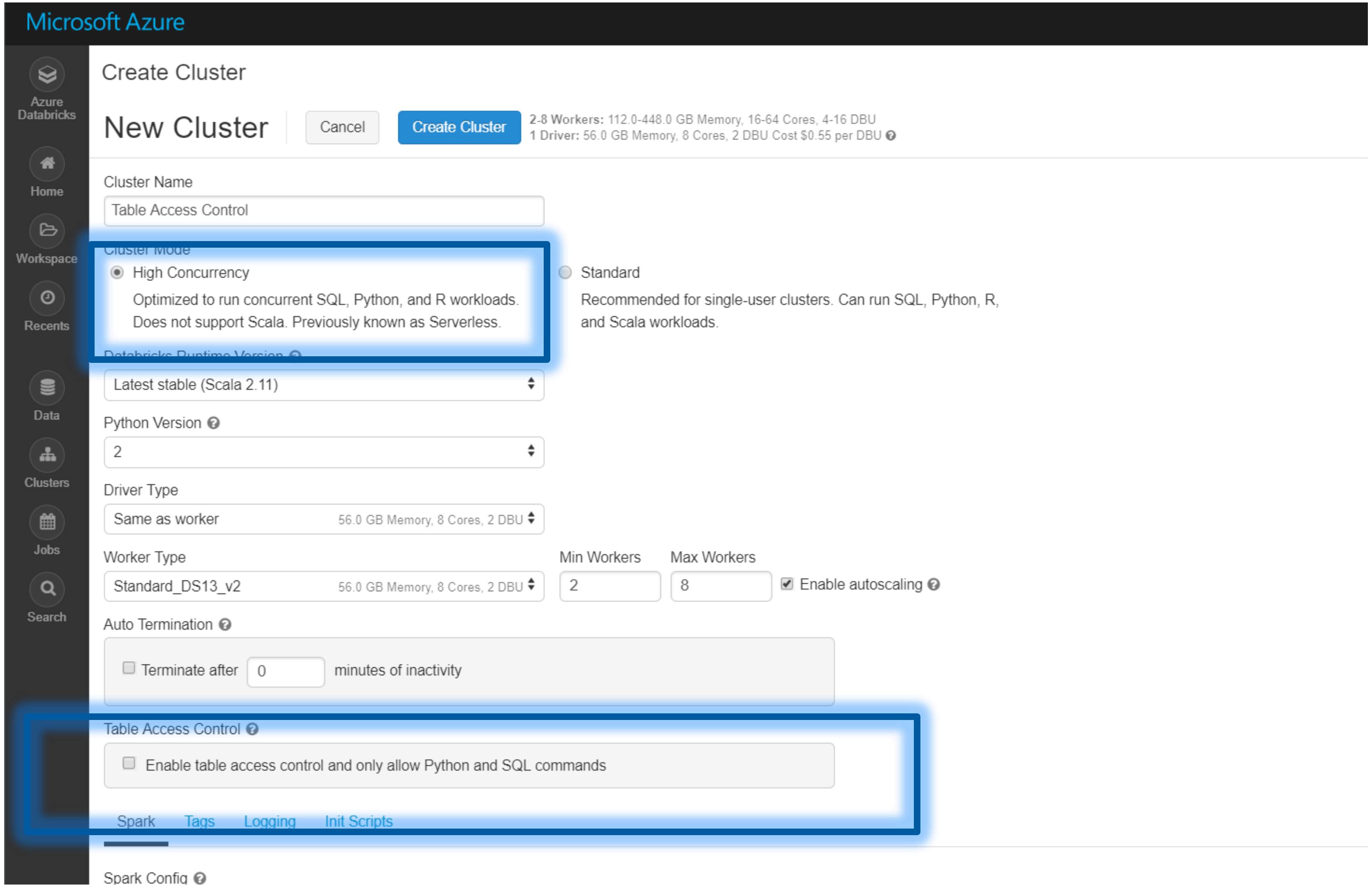
Access Control | Tables



```
[GRANT  |  DENY]
     ON  [OBJECT]
          TO  [USER]
               [PRIVELEGE_TYPE]
```

- Access Control on Tables limits to SQL and Python only. This ensures that low level commands cannot be used to bypass these restrictions.
- High concurrence clusters provide isolation between users.

Access Control | Tables



Create Cluster

New Cluster Cancel Create Cluster

2-8 Workers: 112.0-448.0 GB Memory, 16-64 Cores, 4-16 DBU
1 Driver: 56.0 GB Memory, 8 Cores, 2 DBU Cost $0.55 per DBU

Cluster Name: Table Access Control

Cluster Mode

● High Concurrency
Optimized to run concurrent SQL, Python, and R workloads. Does not support Scala. Previously known as Serverless.

○ Standard
Recommended for single-user clusters. Can run SQL, Python, R, and Scala workloads.

Databricks Runtime Version: Latest stable (Scala 2.11)

Python Version: 2

Driver Type: Same as worker 56.0 GB Memory, 8 Cores, 2 DBU

Worker Type: Standard_DS13_v2 56.0 GB Memory, 8 Cores, 2 DBU

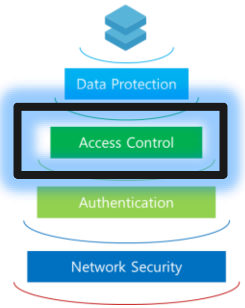
Min Workers: 2 Max Workers: 8 ☑ Enable autoscaling

Auto Termination
□ Terminate after 0 minutes of inactivity

Table Access Control
□ Enable table access control and only allow Python and SQL commands

Spark Tags Logging Init Scripts

Spark Config



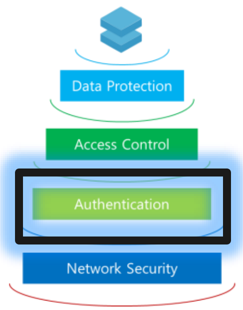
Data Protection

Access Control

Authentication

Network Security

Authentication



- Azure Databricks support Azure Active Directory as an Authentication provider.

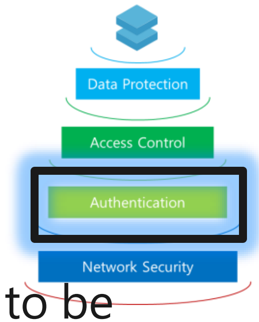
- This is pre-configured with zero setup needed. It includes the ability for the organization to enable multi-factor authentication.

- Support for conditional access has been added for additional policies – restrict access to set of network locations

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

https://docs.azuredatabricks.net/administration-guide/cloud-configurations/azure/conditional-access.html#id1

Credential pass-through for ADLS Gen1



1. Data admins configure the File/Folder ACLs on Storage (ADLS) and would want those permissions to be honored wherever the storage is accessed from.

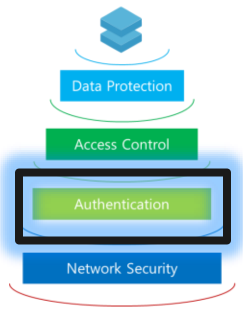
2. Credential Service Principal is pain and not every user has the right to do it as it require specific permission. This creates friction.

3. Every time user (or environment) changes one has to re-think or redo the mount point for isolation.

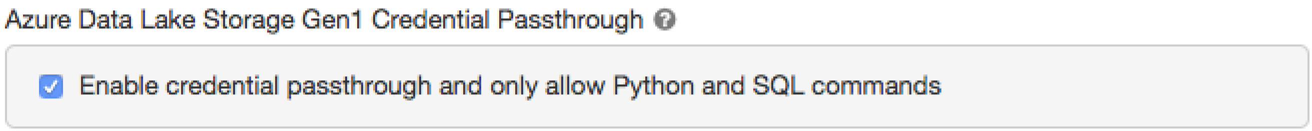
Requirements:

1. Azure Databricks Premium Plan
2. Databricks runtime 5.1 or above
3. High Concurrency clusters, which support Python and SQL
4. An Azure Active Directory administrator must properly configure the lifetime of Azure AD token

Credential pass-through for ADLS Gen1



- When you create the cluster, set the Cluster Mode to High Concurrency.
- Use Databricks Runtime 5.1 or above. Premium plan
- Select Enable credential passthrough and only allow Python and SQL commands.



Azure Data Lake Storage Gen1 Credential Passthrough

☑ Enable credential passthrough and only allow Python and SQL commands

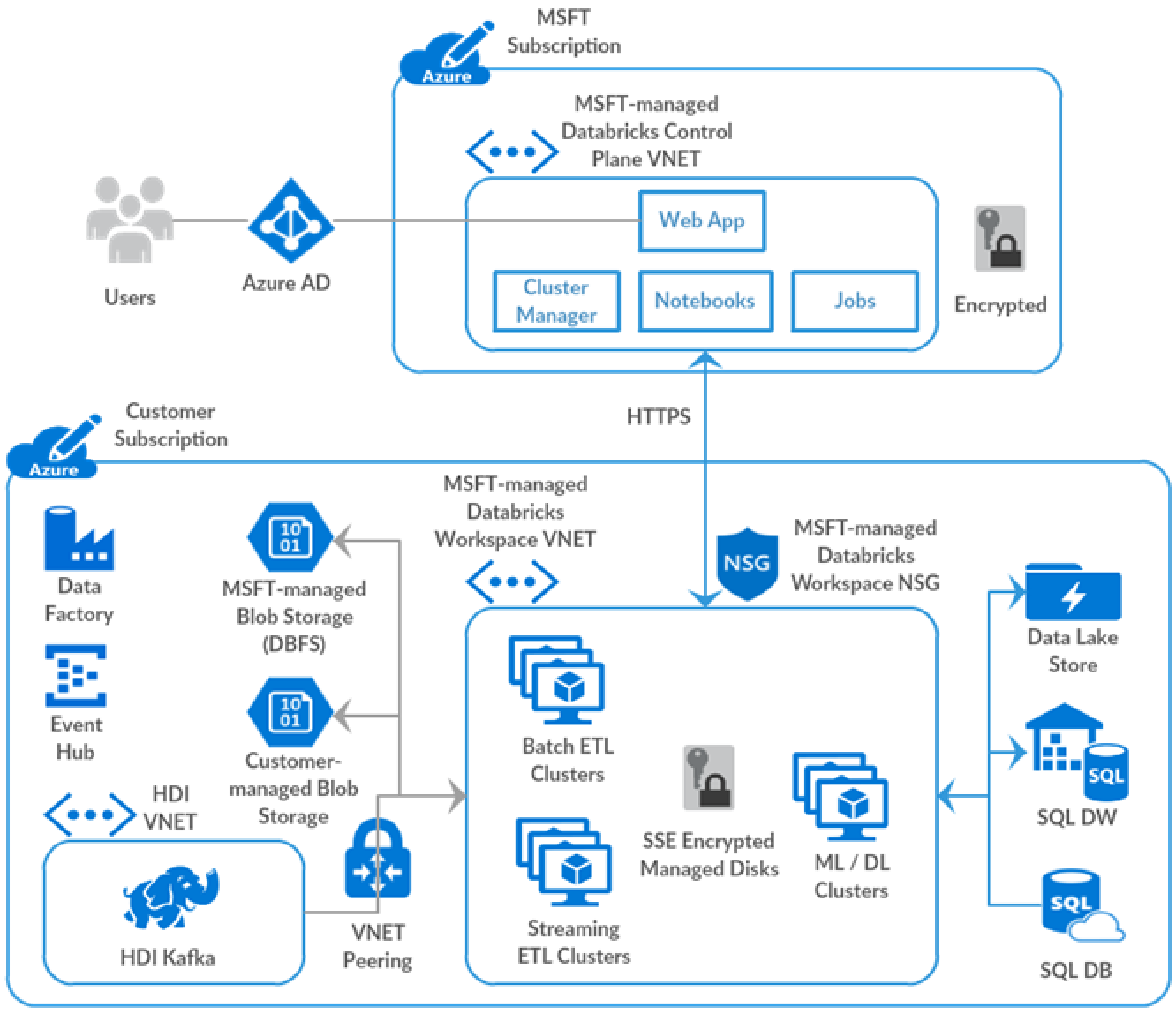
Important

1. Working to support this on ADLS Gen 2 – Q2 CY19
2. Known issue – Doesn't work if you do VNet Injection and enable Service Endpoint for ADLS Gen 1

https://docs.azuredatabricks.net/spark/latest/data-sources/azure/azure-datalake.html#adls1-aad-credentials

Virtual Network for Azure Databricks

Default Deployment with Managed VNet



- Clusters (VMs) are always deployed in the customer's subscription. We deploy these in a VNET we create for the Customer.

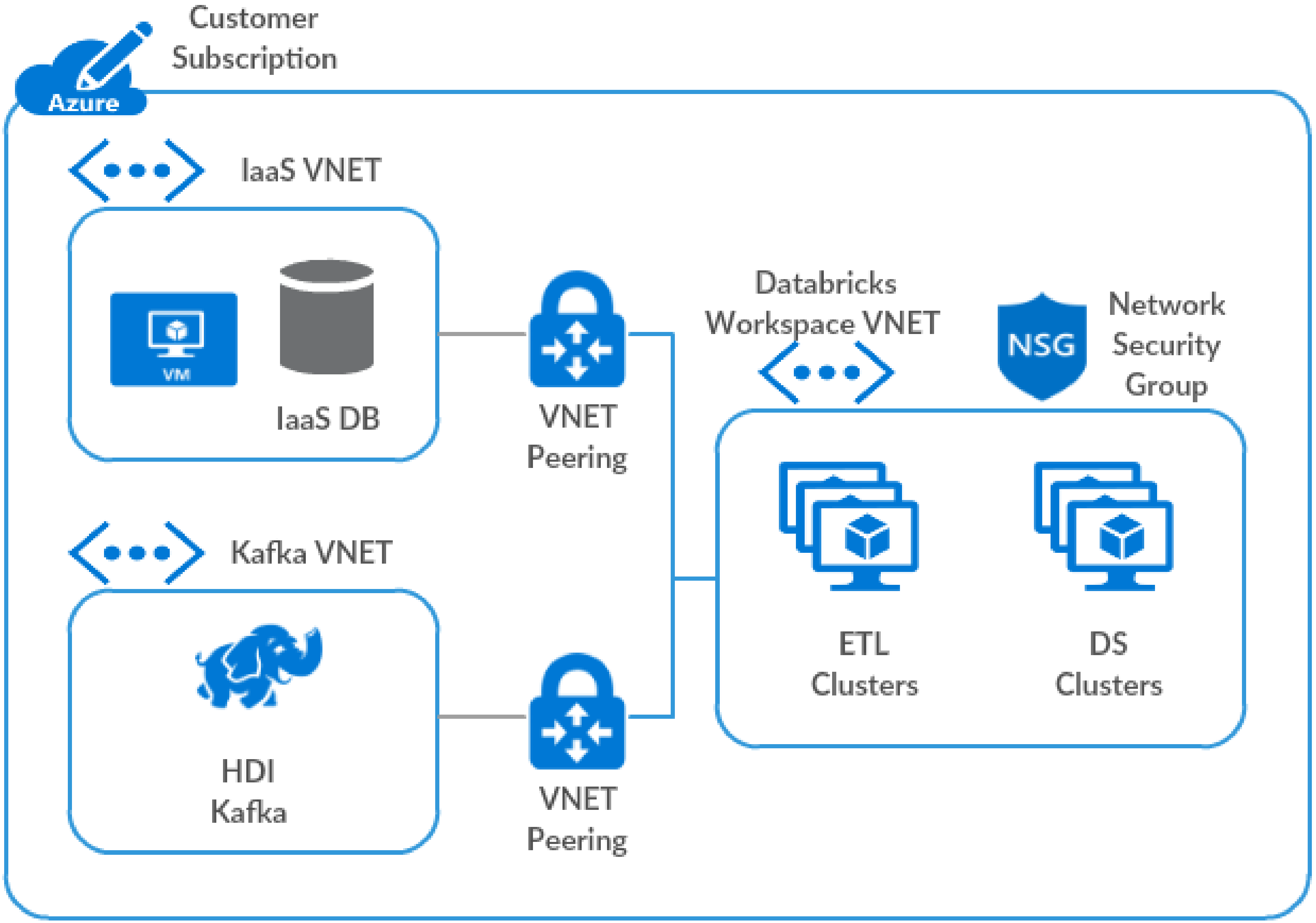
- In this mode, the VNET and accompanying NSG rules are managed by us.

- We allow for Customer's to be able to Peer this with other VNETs

VNET Peering with CIDR Conflicts

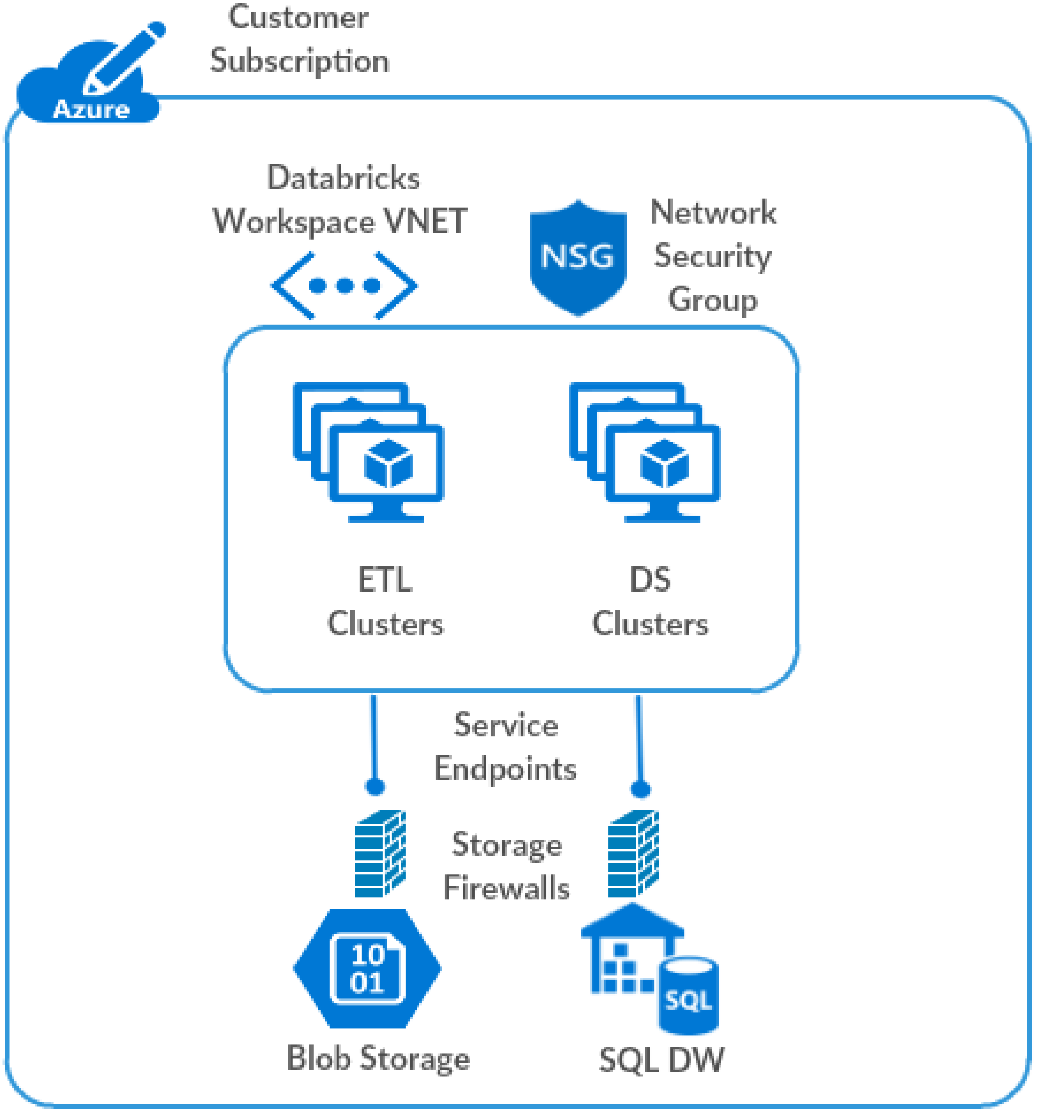
VNET Peering is supported out of the box.

But what if there's CIDR conflict with other VNETs?



Service Endpoints to Azure Data Services

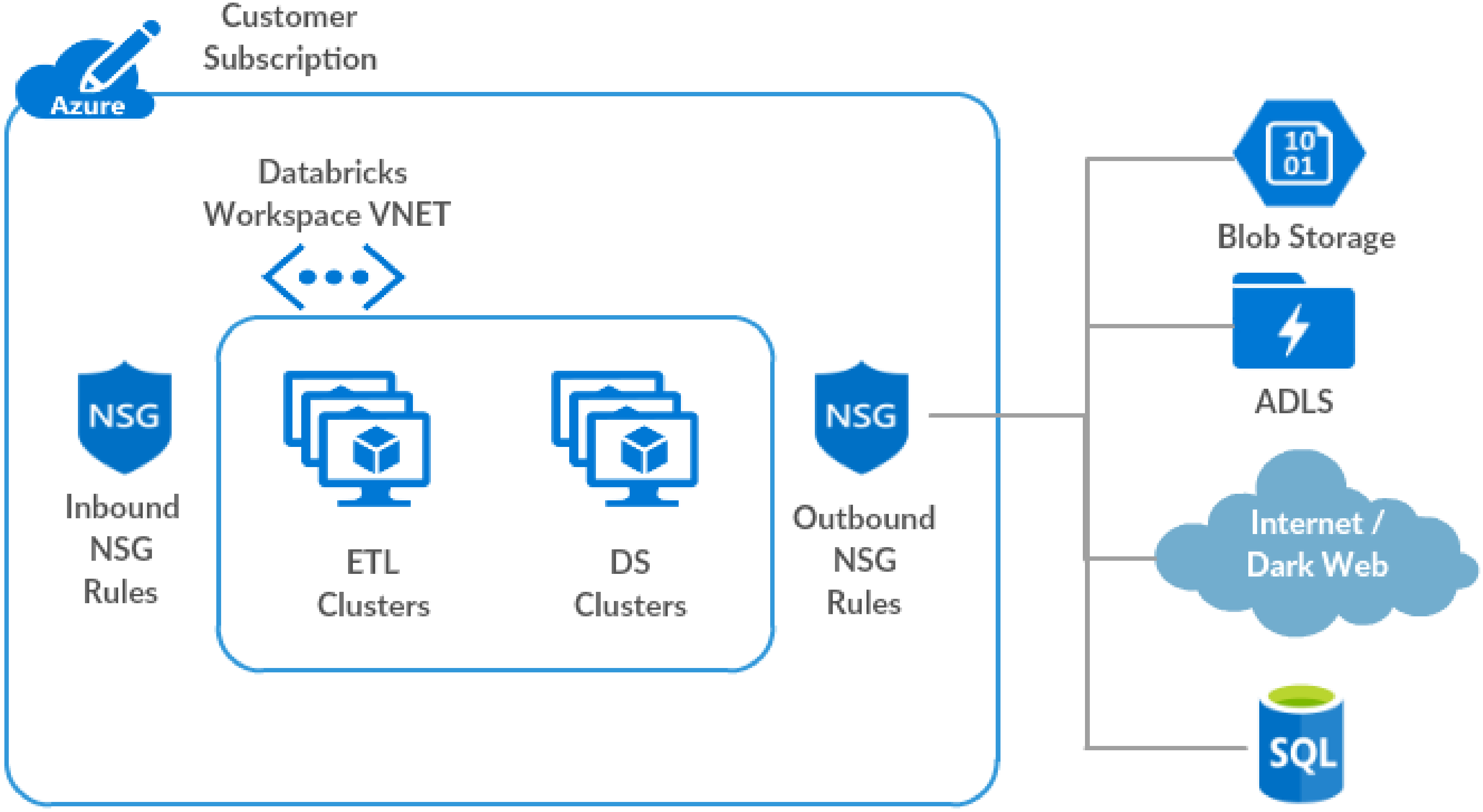
- Service Endpoints allow traffic over Azure backbone rather than public network.
- One could configure service-level built-in firewall with service endpoints
- Available for most Azure data services, with continuous improvements



Customizing NSG outbound rules

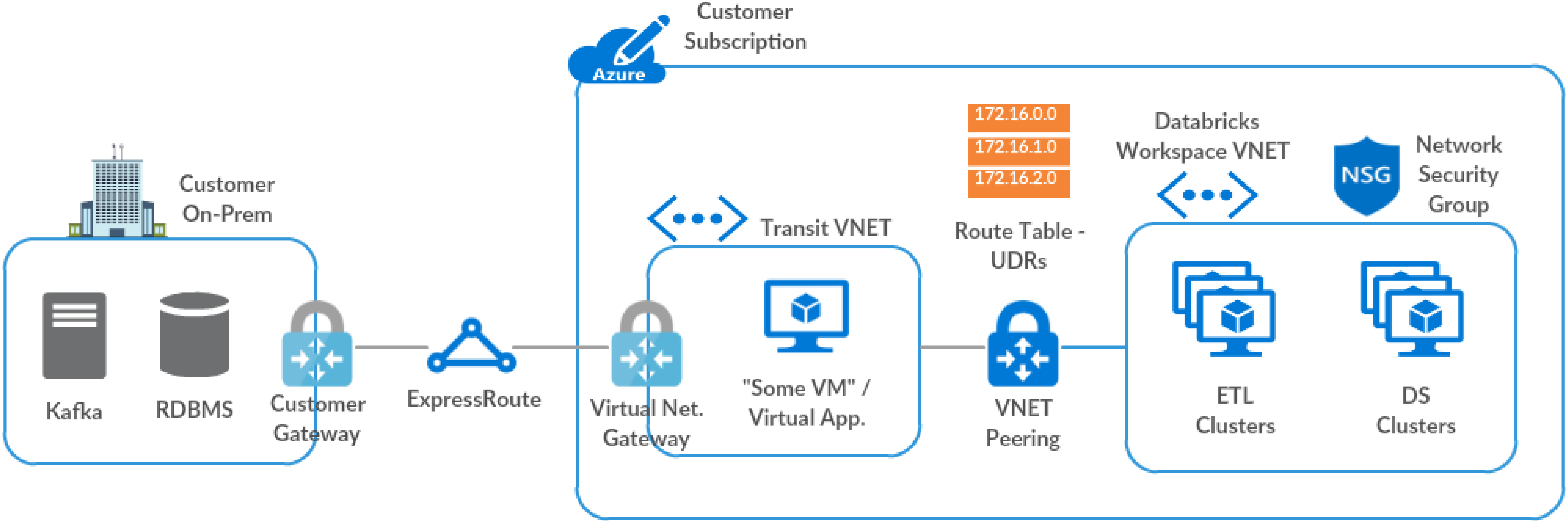
Default NSG outbound rules allow access to Internet.

What if customers want to restrict access to required Databricks services and Azure data services only?



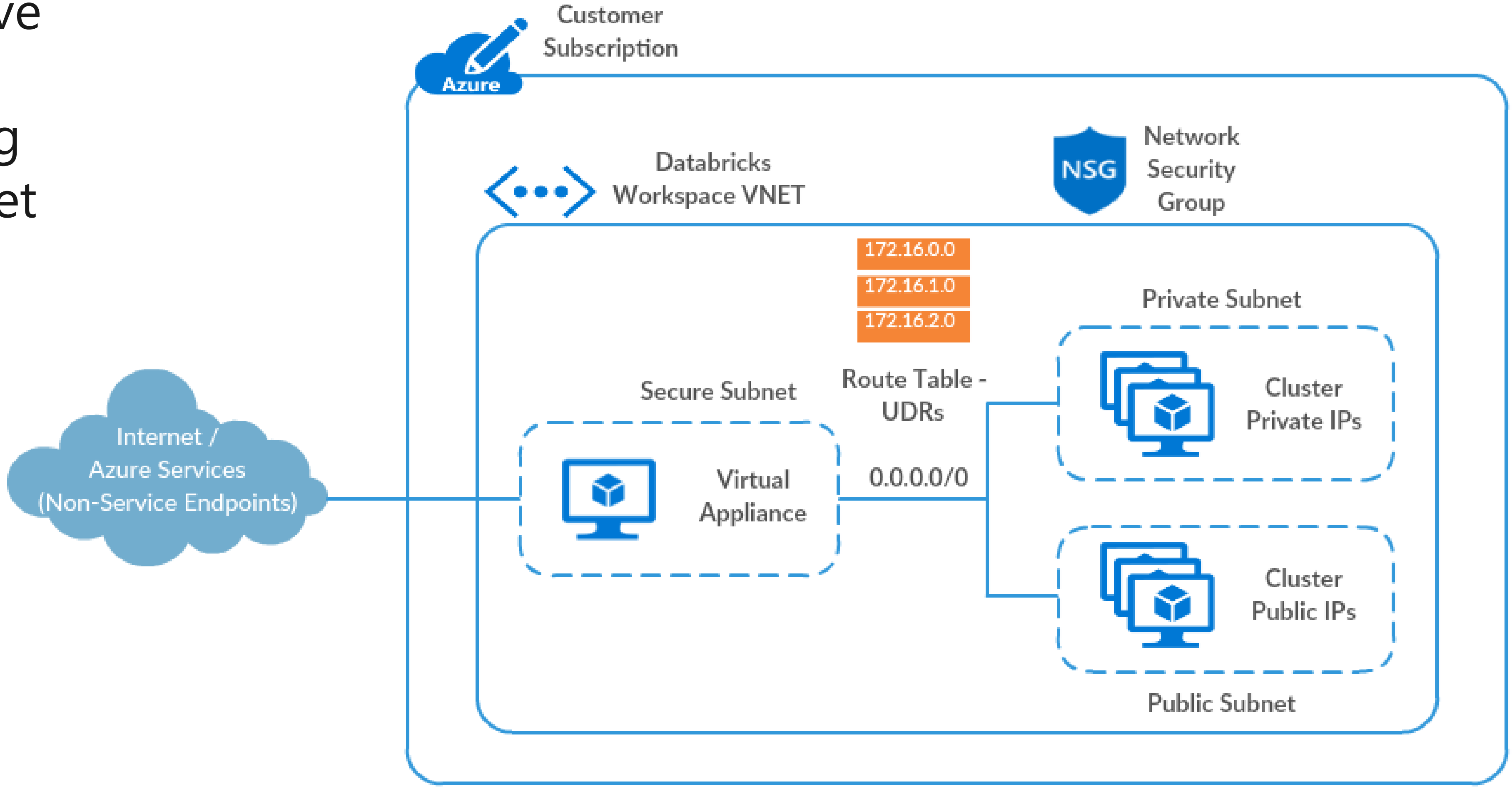
Connectivity to On-Prem Network

To enable connectivity to on-prem network, one needs to route traffic via ExpressRoute or Virtual Network Gateway, which could lead to asymmetric routing. To avoid that, one needs to add custom routes / UDRs for Databricks control plane services.

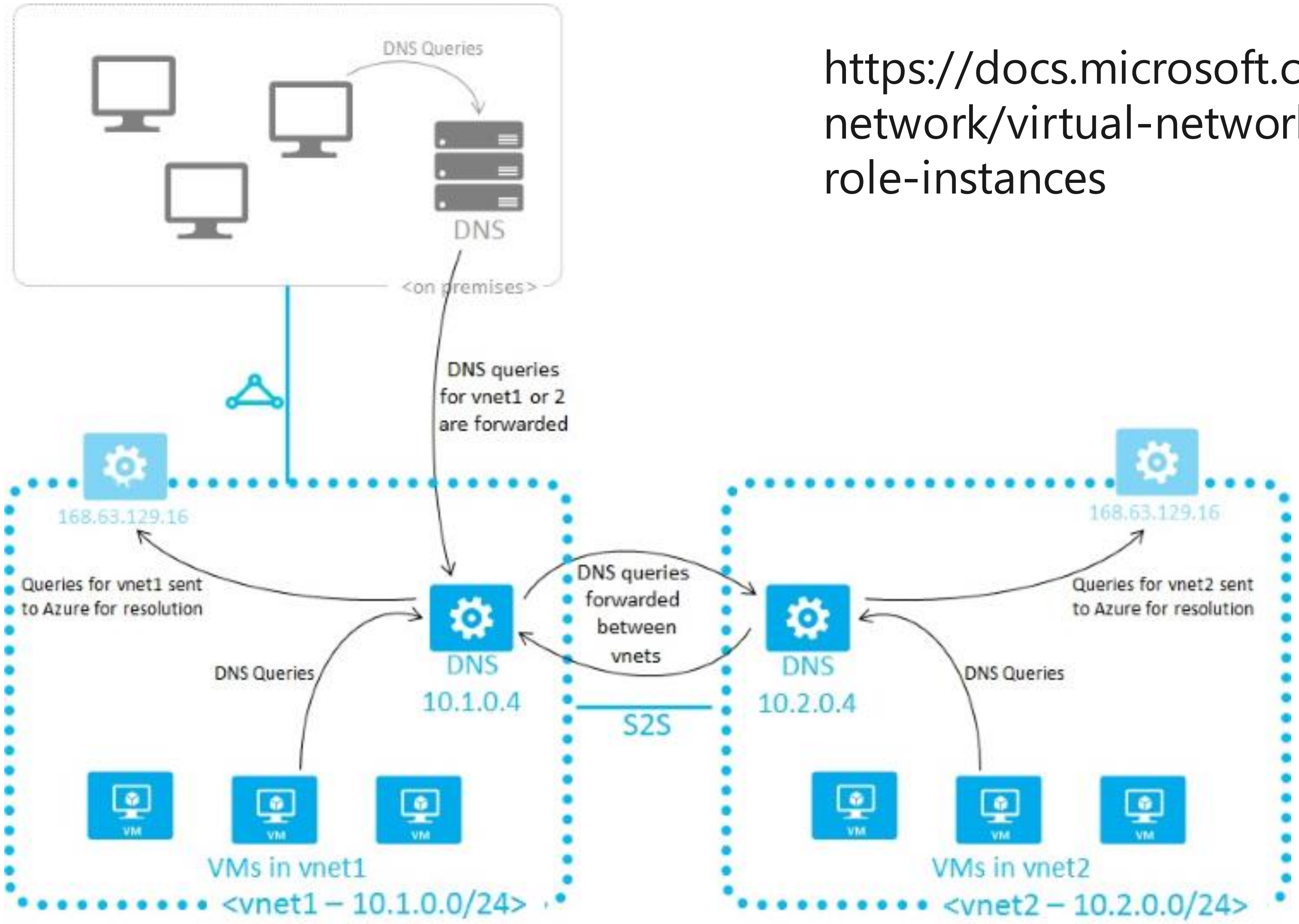


Proxy traffic via Virtual appliance (Firewall)

- Solution for comprehensive outbound traffic filtering
- Solution to get a SNAT IP for Databricks clusters

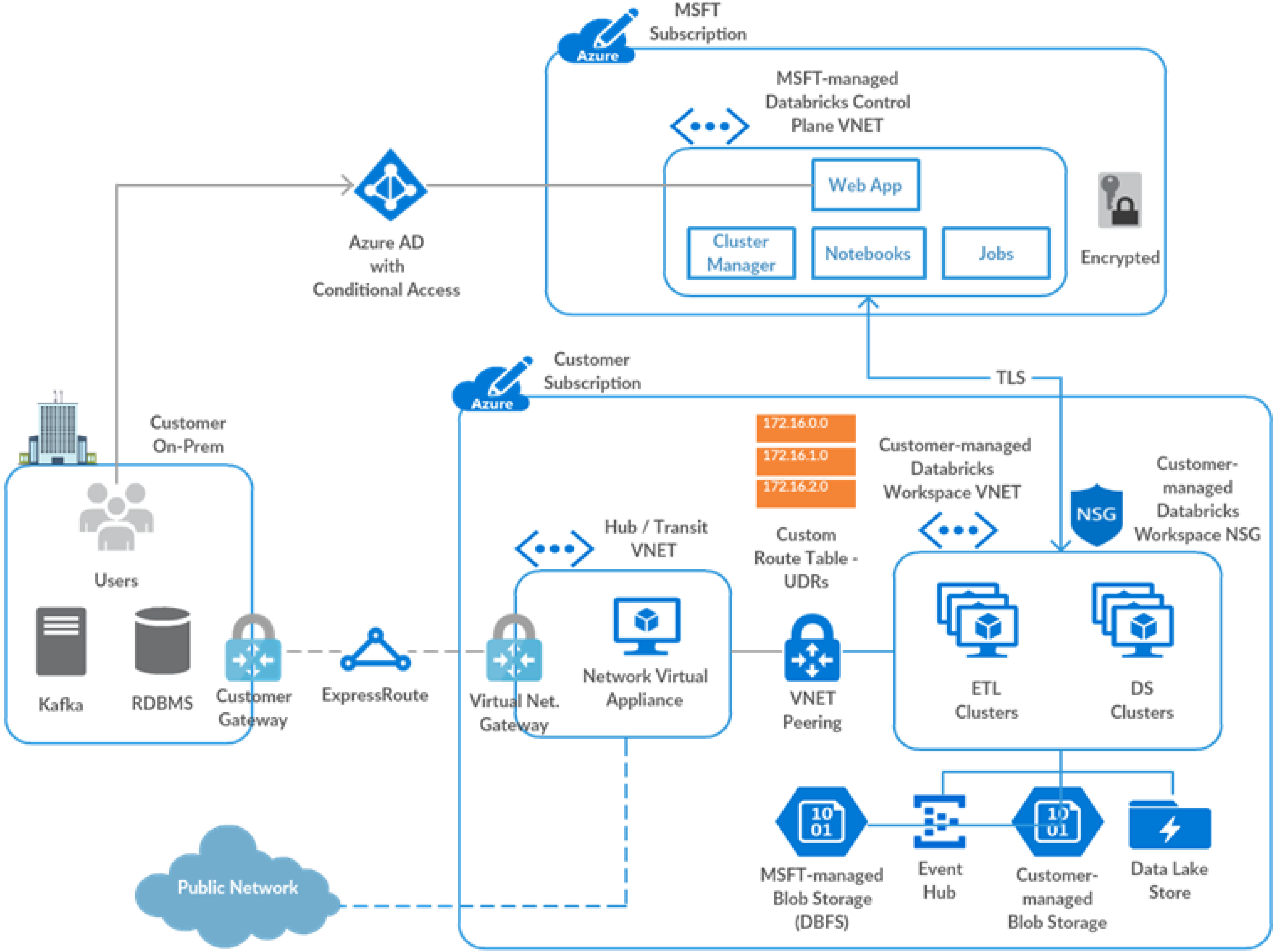


Custom DNS



https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances

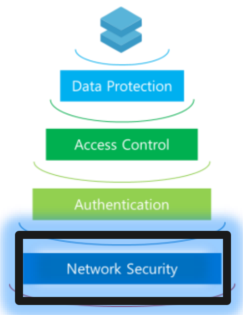
Deployment with customer managed VNet

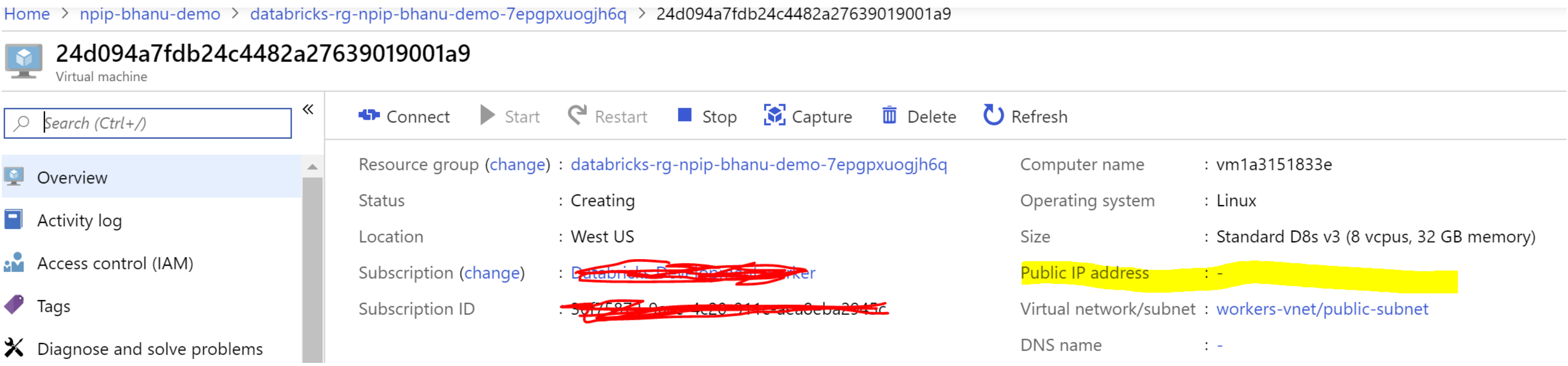


Mandatory NSG rules – IBPv1

Direction	Protocol	Source	Source Port	Destination	Destination Port
Inbound	•	VirtualNetwork	•	•	•
Inbound	•	Control Plane NAT IP	•	•	22
Inbound	•	Control Plane NAT IP	•	•	5557
Outbound	•	•	•	Webapp IP	•
Outbound	•	•	•	SQL (service tag)	•
Outbound	•	•	•	Storage (service tag)	•
Outbound	•	•	•	VirtualNetwork	•

Network Security | No Public IP




Home > npip-bhanu-demo > databricks-rg-npip-bhanu-demo-7epgpxuogjh6q > 24d094a7fdb24c4482a27639019001a9

24d094a7fdb24c4482a27639019001a9
Virtual machine

Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Start
Restart
Stop
Capture
Delete
Refresh

Resource group (change)	: databricks-rg-npip-bhanu-demo-7epgpxuogjh6q	Computer name	: vm1a3151833e
Status	: Creating	Operating system	: Linux
Location	: West US	Size	: Standard D8s v3 (8 vcpus, 32 GB memory)
Subscription (change)	: [redacted]	Public IP address	: -
Subscription ID	: [redacted]	Virtual network/subnet	: workers-vnet/public-subnet
		DNS name	: -

Compliance

- ISO 27001
- ISO 27018
- HIPAA
- SOC2, Type 2

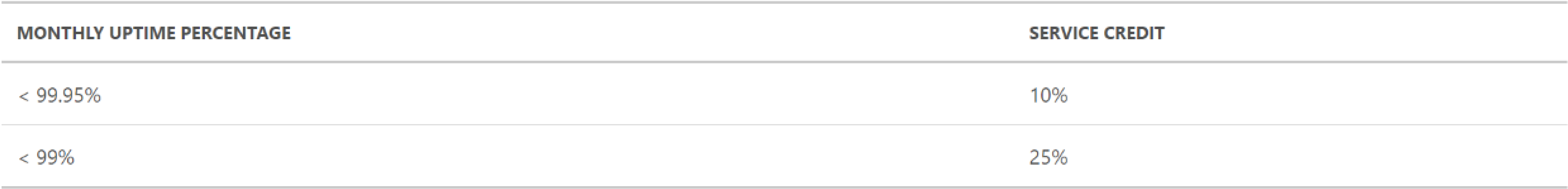
ISO

AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports

HIPAA

Service Level Agreement

99.95% uptime SLA



MONTHLY UPTIME PERCENTAGE	SERVICE CREDIT
< 99.95%	10%
< 99%	25%

https://azure.microsoft.com/en-us/support/legal/sla/databricks/v1_0/