

Last updated by | Lisa Liu | Nov 6, 2020 at 10:35 AM PST

Database will be in inaccessible state

[More events in the activity log](#) →

[Dismiss all](#) ✓

## ! Key validation failed

The server 'byoktestpostgre' requires following Azure Key Vault permissions: 'Get, WrapKey, UnwrapKey'. Please grant any missing permissions to the service principal with ID 'https://myprettylittlevault.vault.azure.net/keys/Myenabledbutnopermissionkey/97

a few seconds ago

The key vault administrator can also [enable logging of Key Vault](#) audit events, so they can be audited later.

Home > Log Analytics workspaces > byoktestanalytics | Solutions > KeyVaultAnalytics(byoktestanalytics) > KeyVaultAnalytics(byoktestanalytics) > Logs

**Logs**  
byoktestanalytics

New Query 1\* +

Example queries Query explorer Settings Bookmarks

Select Scope Run Time range: Custom Save Copy link New alert rule Export Pin to dashboard Prettify query

Tables Filter

Search

Group by: Solution Filters: not selected

**Favorites**  
You can add favorites by clicking on the ☆ icon

**LogManagement**

- AADDomainServicesAcc...
- AADDomainServicesAcc...
- AADDomainServicesDir...
- AADDomainServicesLog...
- AADDomainServicesPoli...

Provider == "MICROSOFT.KEYVAULT" and Category == "AuditEvent" and ResultSignature == "Forbidden" | sort by TimeGenerated desc

Results Chart Columns Display time (UTC+00:00)

Completed. Showing results from the custom time range. 00:00:02.185 331 records

Drag a column header and drop it here to group by that column

TimeGenerated [UTC]	Stable	ResultDescription	Category	OperationName	ResultType
3/16/2020, 10:00:44.051 AM	AzureDiagnostics	Operation unwrapKey is not permitted on this key.	AuditEvent	KeyUnwrap	Success
3/16/2020, 9:50:42.741 AM	AzureDiagnostics	Operation unwrapKey is not permitted on this key.	AuditEvent	KeyUnwrap	Success
3/16/2020, 9:40:40.552 AM	AzureDiagnostics	Operation unwrapKey is not permitted on this key.	AuditEvent	KeyUnwrap	Success

**Logs**  
byoktestanalytics

New Query 1\* +

Example queries Query explorer Settings Bookmarks

Select Scope Run Time range: Custom Save Copy link New alert rule Export Pin to dashboard Prettify query

Search

Group by: Solution Filters: not selected

**Favorites**  
You can add favorites by clicking on the ☆ icon

**LogManagement**

- AADDomainServicesAcc...
- AADDomainServicesAcc...
- AADDomainServicesDir...
- AADDomainServicesLog...
- AADDomainServicesPoli...

search in (AzureDiagnostics) ResourceProvider == "MICROSOFT.KEYVAULT" and Category == "AuditEvent" and OperationName == "KeyDelete"


Results Chart Columns Display time (UTC+00:00)



Completed. Showing results from the custom time range. 00:00:06.125 1 records


Drag a column header and drop it here to group by that column

TimeGenerated [UTC]	Stable	identity_claim_http_schemas_microsoft_com_identity_claims_scope_s	identity_claim_ipaddr_s	identity_claim...
Category		AuditEvent		
OperationName		KeyDelete		
ResultType		Success		


Home > [REDACTED] > Keys > Myenabledbutnopermissionkey > 97af5151902f4240bb448f1fb6526717

 **97af5151902f4240bb448f1fb6526717**  
Key Version


 Save  Discard

Set activation date? 

**Activation Date**

03/12/2020  9:50:33 PM

(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Set expiration date?  ☐

**Enabled?** Yes No

---

**Tags**

0 tags

---

**Permitted operations**

<input checked="" type="checkbox"/> Encrypt	<input checked="" type="checkbox"/> Sign	<input type="checkbox"/> Wrap Key
<input checked="" type="checkbox"/> Decrypt	<input checked="" type="checkbox"/> Verify	<input type="checkbox"/> Unwrap Key

To check since when the database was not accessible

`MonAnalyticsElasticServersSnapshot`

```
| where name == "{REPLACE_HERE}"
| summarize min(TIMESTAMP), max(TIMESTAMP) by ['state'], bin(TIMESTAMP, 1h)
```

For any failed operation from the customer side to enable this feature, we are going to use the normal troubleshooting steps once we get the tracking ID from the customer side of that failed operation from the activity Log: Example:

`HttpIncomingRequests`

```
| where subscriptionId == "13ef485e-ff37-448c-ad35-7b06b9bd6eb9" | where serviceRequestId == "93452b9c-ec8d-4a96-a523-40588e8cfc2e"
```

We can see that the request\_id = 083621aa-2fe1-4d43-aea6-0df87ffc1a9f

`MonManagement`

```
| where request_id == toupper("083621aa-2fe1-4d43-aea6-0df87ffc1a9f")
| project originalEventTimestamp, NodeName, event, ['state'], fsm_event, caller_state_machine_type,
state_machine_type, exception_type, old_state, new_state, error_message, operation_type,
exception, error, error_classification, error_code, error_message_format, error_number,
stack_trace, elastic_server_name, operation_parameters
```

and engage the product group based on the above results.

## Key Vault Outage

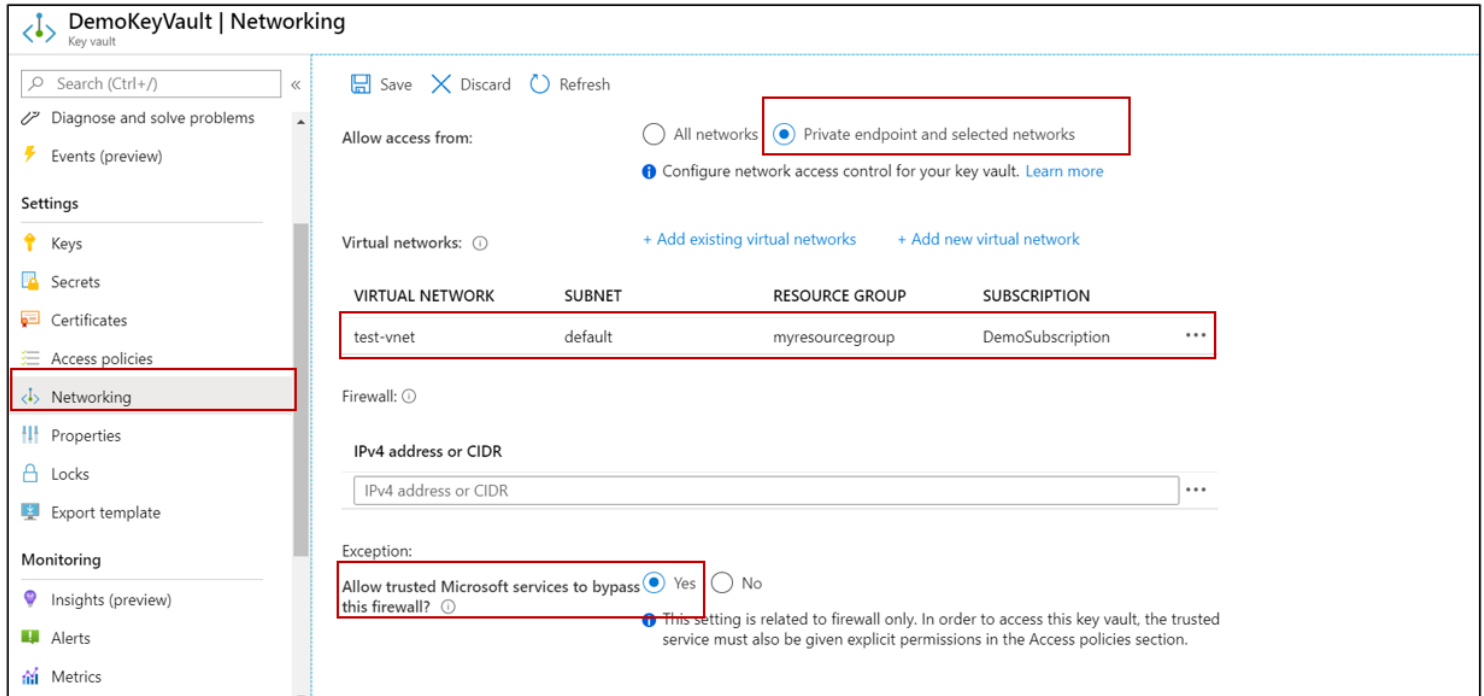
AKV service supports high availability out of the box providing both the local and Geo redundancy.

**Note:** Azure Key Vault Service provides local and Geo redundancy requiring no explicit action or configuration from customers.

For details, please refer to <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-disaster-recovery-guidance> 

## Firewall Issue

When using firewall with AKV, you must enable option Allow trusted Microsoft services to bypass the firewall.



**DemoKeyVault | Networking**

Search (Ctrl+/) << Save Discard Refresh

Diagnose and solve problems  
Events (preview)


**Settings**

- Keys
- Secrets
- Certificates
- Access policies
- Networking**
- Properties
- Locks
- Export template


**Monitoring**

- Insights (preview)
- Alerts
- Metrics


Allow access from: ☐ All networks ☒ Private endpoint and selected networks  
Configure network access control for your key vault. [Learn more](#)

Virtual networks:  [+ Add existing virtual networks](#) [+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	RESOURCE GROUP	SUBSCRIPTION	
test-vnet	default	myresourcegroup	DemoSubscription	...

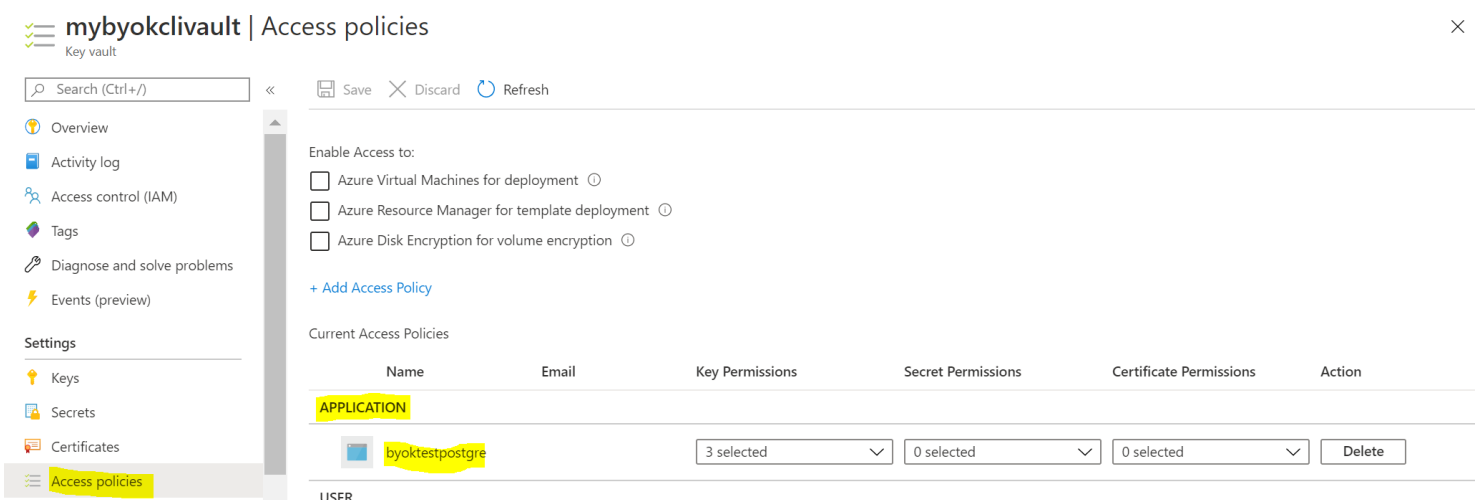
Firewall: 

IPv4 address or CIDR  
IPv4 address or CIDR ...

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.

## Deleting the managed identity of the server in Azure AD

If this is deleted, we will see database in Inaccessible state



**mybyokclivault | Access policies**




Search (Ctrl+/) << Save Discard Refresh

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Events (preview)

**Settings**


- Keys
- Secrets
- Certificates
- Access policies**

Enable Access to:

- ☐ Azure Virtual Machines for deployment 
- ☐ Azure Resource Manager for template deployment 
- ☐ Azure Disk Encryption for volume encryption 

[+ Add Access Policy](#)

Current Access Policies

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions	Action
<b>APPLICATION</b>					
 byoktestpostgre		3 selected	0 selected	0 selected	Delete

USER

## RCA (optional)

Activity log: When access to the customer key in the customer-managed Key Vault fails, entries are added to the activity log. You can reinstate access as soon as possible, if you create alerts for these events.

## More Information (optional)

[Monitor access to Customer Managed Key](#). 

## Public Doc Reference (optional)

See Above

## Root Cause Classification

Cases resolved by this TSG should be coded to the following root cause: Azure Open Source DB  
V2\Security\User Issue/Error\Data Encryption\Issues with Key Vault/Key Vault Outage

**How good have you found this content?**

