TABLE OF CONTENTS

EXECUTIVE SUMMARY

SUMMARY OF TESTS PERFORMED

Tests Performed	Passed	Failed
951	50.89% (484)	49.11% (467)

FAILED TESTS BY SEVERITY

Critical	High	Medium	Low	Informational
0	140	317	10	10

SUMMARY OF RULES TESTED

Rules Performed	Passed	Failed
332	58.73% (195)	41.27% (137)

Entities by type, Pass Vs Fail

Entity Type	Passed	Failed
VirtualMachine (5)	0	**5**
SQLServer (0)	0	0
RedisCache (0)	0	0
KeyVault (0)	0	0
AksCluster (2)	0	**2**
PolicyAssignment (1)	**1**	0
PostgreSQL (0)	0	0
NetworkSecurityGroup (1)	0	**1**
StorageAccount (4)	0	**4**
SQLDB (0)	0	0
List<LogProfile> (1)	0	**1**
List<NetworkWatcher> (1)	**1**	0
ContainerRegistry (1)	0	**1**
ResourceGroup (10)	0	**10**
CosmosDbAccount (0)	0	0
LogProfile (0)	0	0
ApplicationGateway (0)	0	0
VNet (4)	**1**	**3**

Regions

Name	Passed Tests	Failed Tests	Failed Entities	Failed Critical	Failed High	Failed Medium	Failed Low	Failed Informational
East US	**816**	**135**	**9**	0	**70**	**64**	**1**	0

Failed Tests Summary

Rule Name	Severity	Tested	Relevant	Non Compliant

Rule Name	Severity	Tested	Relevant	Non Compliant
Ensure default network access rule for Storage Accounts is set to deny	**High**	**4**	**4**	**4**
Ensure that a network policy is in place to secure traffic between pods	**High**	**2**	**2**	**2**
VirtualMachine with unencrypted LDAP (UDP:389) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Memcached (UDP:11211) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with service Memcached SSL (TCP:11214) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with administrative service: Remote Desktop (TCP:3389) is too exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with service NetBIOS Name Service (UDP:137) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Redis (TCP:6379) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with administrative service: CiscoSecure,websm (TCP:9090) is too exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Elastic search (TCP:9200) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with service SNMP (UDP:161) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service Prevalent known internal port (TCP:3000) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service MySQL (TCP:3306) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service SaltStack Master (TCP:4505) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service Memcached SSL (UDP:11214) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Oracle DB (TCP:1521) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with administrative service: SSH (TCP:22) is too exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Cassandra Internode Communication (TCP:7000) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Oracle DB (UDP:2483) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Mongo (TCP:27017) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with service VNC Listener (TCP:5500) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service MSSQL Debugger (TCP:135) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service Telnet (TCP:23) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service NetBios Session Service (TCP:139) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Oracle DB (TCP:2483) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with service Known internal web port (TCP:8000) is exposed to the entire internet	**High**	**5**	**2**	**2**

Rule Name	Severity	Tested	Relevant	Non Compliant
Ensure that you are using authorized IP address ranges in order to secure access to the API server	**High**	**2**	**2**	**2**
VirtualMachine with service NetBios Datagram Service (UDP:138) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service Oracle DB SSL (TCP:2484) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service Mongo Web Portal (TCP:27018) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service Postgres SQL (UDP:5432) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service CIFS / SMB (TCP:3020) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service Cassandra OpsCenter agent (TCP:61621) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service VNC Server (TCP:5900) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service POP3 (TCP:110) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Elastic search (TCP:9300) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Cassandra Thrift (TCP:9160) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with service SQL Server Analysis Services (TCP:2383) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service LDAP SSL (TCP:636) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service Cassandra (TCP:7001) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Cassandra Monitoring (TCP:7199) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with service Hadoop Name Node (TCP:9000) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service MSSQL Admin (TCP:1434) is exposed to the entire internet	**High**	**5**	**2**	**2**
Ensure that the pod security policy is enabled in your AKS cluster	**High**	**2**	**2**	**2**
VirtualMachine with service SQL Server Analysis Service browser (TCP:2382) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service Puppet Master (TCP:8140) is exposed to the entire internet	**High**	**5**	**2**	**2**
Ensure that at least one Network Security Group is attached to all VMs and subnets that are public	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted LDAP (TCP:389) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with service Known internal web port (TCP:8080) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service NetBIOS Name Service (TCP:137) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service SMTP (TCP:25) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service DNS (UDP:53) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service MSSQL Server (TCP:1433) is exposed to the entire internet	**High**	**5**	**2**	**2**

Rule Name	Severity	Tested	Relevant	Non Compliant
VirtualMachine with service SaltStack Master (TCP:4506) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Cassandra OpsCenter Website (TCP:8888) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with service Memcached SSL (UDP:11215) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service Microsoft-DS (TCP:445) is exposed to the entire internet	**High**	**5**	**2**	**2**
Ensure that 'Secure transfer required' is enabled for Storage Accounts	**High**	**4**	**4**	**2**
VirtualMachine with service MSSQL Browser Service (UDP:1434) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service Memcached SSL (TCP:11215) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with service Postgres SQL (TCP:5432) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Cassandra OpsCenter Monitoring (TCP:61620) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with service NetBios Datagram Service (TCP:138) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Cassandra Client (TCP:9042) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with service NetBios Session Service (UDP:139) is exposed to the entire internet	**High**	**5**	**2**	**2**
VirtualMachine with unencrypted Memcached (TCP:11211) is exposed to the public internet	**High**	**5**	**2**	**2**
VirtualMachine with service Oracle DB SSL (UDP:2484) is exposed to the entire internet	**High**	**5**	**2**	**2**
Ensure that inbound traffic is restricted to only that which is necessary, and all other traffic denied	**High**	**1**	**1**	**1**
Ensure that SSH access is restricted from the internet	**High**	**1**	**1**	**1**
Ensure Container Registry has locks	**High**	**1**	**1**	**1**
Ensure that a Log Profile exists	**High**	**1**	**1**	**1**
VirtualMachine with unencrypted Cassandra Client (TCP:9042) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service NetBios Datagram Service (TCP:138) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Cassandra Internode Communication (TCP:7000) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Memcached SSL (UDP:11214) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service SNMP (UDP:161) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service NetBios Session Service (TCP:139) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Known internal web port (TCP:8000) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service NetBIOS Name Service (TCP:137) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service VNC Listener (TCP:5500) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**

Rule Name	Severity	Tested	Relevant	Non Compliant
VirtualMachine with service Cassandra (TCP:7001) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted LDAP (TCP:389) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service NetBIOS Name Service (UDP:137) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service SQL Server Analysis Service browser (TCP:2382) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Oracle DB (UDP:2483) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Mongo (TCP:27017) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Cassandra Monitoring (TCP:7199) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service MSSQL Server (TCP:1433) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted LDAP (UDP:389) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service NetBios Datagram Service (UDP:138) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Cassandra OpsCenter Monitoring (TCP:61620) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Puppet Master (TCP:8140) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Microsoft-DS (TCP:445) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Postgres SQL (UDP:5432) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Oracle DB (TCP:1521) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service MSSQL Browser Service (UDP:1434) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Memcached SSL (UDP:11215) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Postgres SQL (TCP:5432) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service SMTP (TCP:25) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Memcached SSL (TCP:11215) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service POP3 (TCP:110) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Memcached SSL (TCP:11214) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Elastic search (TCP:9200) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service SaltStack Master (TCP:4506) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Memcached (TCP:11211) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with administrative service: SSH (TCP:22) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**

Rule Name	Severity	Tested	Relevant	Non Compliant
VirtualMachine with service NetBios Session Service (UDP:139) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service VNC Server (TCP:5900) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with administrative service: CiscoSecure,websm (TCP:9090) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Elastic search (TCP:9300) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service MySQL (TCP:3306) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service LDAP SSL (TCP:636) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Mongo Web Portal (TCP:27018) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with administrative service: Remote Desktop (TCP:3389) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Telnet (TCP:23) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Cassandra Thrift (TCP:9160) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Oracle DB (TCP:2483) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service CIFS / SMB (TCP:3020) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service SaltStack Master (TCP:4505) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Hadoop Name Node (TCP:9000) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Cassandra OpsCenter agent (TCP:61621) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Redis (TCP:6379) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Known internal web port (TCP:8080) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Oracle DB SSL (UDP:2484) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Oracle DB SSL (TCP:2484) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service SQL Server Analysis Services (TCP:2383) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
Ensure that 'OS disk' are encrypted	**Medium**	**5**	**5**	**5**
VirtualMachine with service MSSQL Debugger (TCP:135) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service Prevalent known internal port (TCP:3000) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Cassandra OpsCenter Website (TCP:8888) is exposed to a large network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service DNS (UDP:53) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with service MSSQL Admin (TCP:1434) is exposed to a wide network scope	**Medium**	**5**	**5**	**5**
VirtualMachine with unencrypted Memcached (UDP:11211) is exposed to a large network scope	**Medium**	**5**	**5**	**5**

Rule Name	Severity	Tested	Relevant	Non Compliant
Ensure that Azure Virtual Network subnet is configured with a Network Security Group	**Medium**	**4**	**4**	**3**
Ensure that Azure Virtual Machine is assigned to an availability set	**Medium**	**5**	**5**	**3**
Ensure audit profile captures all the activities	**Medium**	**1**	**1**	**1**
Ensure that Azure Resource Group has resource lock enabled	**Low**	**10**	**10**	**10**

FAILED TESTS

FAILED

Ensure default network access rule for Storage Accounts is set to deny

High

Description:

Restricting default network access helps to provide a new layer of security, since storage accounts accept connections from clients on any network. To limit access to selected networks, the default action must be changed.

4 TESTED **4** RELEVANT 4 NON COMPLIANT

Network Security

Remediation:

1. Go to Storage Accounts
2. For each storage account, Click on the settings menu called Firewalls and virtual networks.
3. Ensure that you have elected to allow access from Selected networks.
4. Add rules to allow traffic from specific network.
5. Click Save to apply your changes.

Azure Command Line Interface 2.0 Use the below command to update default-action to Deny.

References:

https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security (https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security)

Failed Entities

ID	Name	Region	VNET
/subscriptions/a08c11fe-96c2-4f3a-92a9-8825a1323e86/resourceGroups/MC_KubernetesContainer01_accessitdemo_eastus/providers/Microsoft.Storage/storageAccounts/fleastus1591714933701	fleastus1591714933701	East US	-
/subscriptions/a08c11fe-96c2-4f3a-92a9-8825a1323e86/resourceGroups/R80dot40Mgmt/providers/Microsoft.Storage/storageAccounts/diagef25306c4b15024f	diagef25306c4b15024f	East US	-

ID	Name	Region	VNET
/subscriptions/a08c11fe-96c2-4f3a-92a9-8825a1323e86/resourceGroups/aitgvmssrg/providers/Microsoft.Storage/storageAccounts/diagebf39e219d600da7	diagebf39e219d600da7	East US	-
/subscriptions/a08c11fe-96c2-4f3a-92a9-8825a1323e86/resourceGroups/cloud-shell-storage-eastus/providers/Microsoft.Storage/storageAccounts/cs21003200097cd55da	cs21003200097cd55da	East US	-

FAILED

Ensure that a network policy is in place to secure traffic between pods

High

Description:

In Kubernetes when you run modern, microservices-based applications, you often want to control which components can communicate with each other. The principle of least privilege should be applied to how traffic can flow between pods in an Azure Kubernetes Service (AKS) cluster. The Network Policy feature in Kubernetes lets you define rules for ingress and egress traffic between pods in a cluster.

2 TESTED 2 RELEVANT 2 NON COMPLIANT

Azure Kubernetes Services

Remediation:

In an AKS cluster, all pods can send and receive traffic without limitations, by default. To improve security, you can define rules that control the flow of traffic.
Network Policy is a Kubernetes specification that defines access policies for communication between Pods. These network policy rules are defined as YAML manifests.

The network policy feature can only be enabled when the cluster is created. You can't enable network policy on an existing AKS cluster. To create AKS cluster that supports network policy, please refer - https://docs.microsoft.com/en-us/azure/aks/use-network-policies?ocid=AID754288&wt.mc_id=CFID0471#create-an-aks-cluster-and-enable-network-policy (https://docs.microsoft.com/en-us/azure/aks/use-network-policies?ocid=AID754288&wt.mc_id=CFID0471#create-an-aks-cluster-and-enable-network-policy)

Failed Entities

ID	Name	Region	VNET
/subscriptions/a08c11fe-96c2-4f3a-92a9-8825a1323e86/resourcegroups/KubernetesCluster1/providers/Microsoft.ContainerService/managedClusters/AITGKubernetesCluster01	AITGKubernetesCluster01	East US	-
/subscriptions/a08c11fe-96c2-4f3a-92a9-8825a1323e86/resourcegroups/KubernetesContainer01/providers/Microsoft.ContainerService/managedClusters/accessitdemo	accessitdemo	East US	-

FAILED

High