Networkology

AZURE NIST SP 800-53
Detailed Report

Compliance Report

Created For:
Acme Corporation

Created On:
Aug 24, 2020 at 05:38 AM

Cloud Account:
c3m-azure-01

Powered by C3M

About Report

Disclaimer

The report generated for the compliance assessment is indicative and based on the assessment period, mapped controls, and does not in any way indicate complete compliance with a specific standard or regulation. C3M does not certify your compliance against any particular standard since all of them involve some level of MANUAL checks which must be completed outside of our system.

Table of contents

Brief Summary

Current Score
72%

Policies

Total Policies	Passed Policies	Failed Policies
74	54	20

Critical	3
High	14
Medium	3
Low	0

Resources

Total Resources	Passed Resources	Failed Resources
5756	5501	255

Controls Summary

Control	Compliance
AC-2 Account Management	8/9
AC-3 Access Enforcement	4/5
AC-4 Information Flow Enforcement	33/39
AC-6 Least Privilege	6/13
AC-17 Remote Access	7/10
AU-2 Audit Events	5/6
AU-3 Content of Audit Records	3/4
AU-4 Audit Storage Capacity	1/2
AU-5 Response to Audit Processing Failures	2/2
AU-10 Non-Repudiation	5/6
AU-11 Audit Record Retention	1/2
AU-12 Audit Generation	5/6
CM-5 Access Restrictions For Change	8/16
CM-6 Configuration Settings	6/14

Controls Summary

Control	Compliance
CM-7 Least Functionality	33/40
SC-7 Boundary Protection	34/39
SC-8 Transmission Confidentiality and Integrity	4/6
SC-13 Cryptographic Protection	2/4
SC-23 Session Authenticity	4/6
SC-28 Protection of Information at Rest	2/4

Evaluation Summary

AC-2 Account Management 8/9

Policy Name	Compliance	Passed	Failed
Ensure Log profile captures all the activities	✓	1	0
Ensure SQLServers configured with appropriate "AuditActionGroups"	✓	0	0
Ensure SQLServers enable "Auditing"	✓	0	0
Ensure Activity Log Alert exists for Create Policy Assignment	✓	1	0
Ensure that Azure Active Directory Admin is configured	✓	0	0
Ensure Log Profile is configured	✓	1	0
Ensure logging is enabled for Azure Key vault	✗	0	5
Enable role-based access control (RBAC) within Azure Kubernetes Services	✓	0	0
Ensure log profile captures activity logs for all regions including global	✓	1	0

Evaluation Summary

AC-3 Access Enforcement 4/5

Policy Name	Compliance	Passed	Failed
Enable role-based access control (RBAC) within Azure Kubernetes Services	✓	0	0
Ensure Cosmos DB account is not exposed to the Internet	✓	0	0
Ensure default network access rule for Storage Accounts is set to deny	✗	0	78
Ensure Storage Accounts enable access to Trusted Microsoft Services	✓	78	0
Ensure that no SQL Databases allow ingress from 0.0.0.0/0	✓	0	0

Evaluation Summary

AC-4 Information Flow Enforcement 33/39

Policy Name	Compliance	Passed	Failed
Ensure no Virtual Machine allows Public access on FTP port 20	✓	1	0
Ensure no Virtual Machine allows Public access on NetBIOS port 137	✓	1	0
Ensure no Virtual Machine allows Public access on FTP port 21	✓	1	0
Ensure no Virtual Machine allows Public access on NetBIOS port 138	✓	1	0
Ensure no Virtual Machine allows Public access on Cassandra Monitoring port 7199	✓	1	0
Ensure no Virtual Machine allows Public access on Oracle DB port 2483	✓	1	0
Ensure no Virtual Machine allows Public access on SMB port 445	✓	1	0
Ensure no Virtual Machine allows Public access on NetBIOS port 139	✓	1	0
Ensure no Virtual Machine allows Public access on LDAP SSL port 636	✓	1	0
Ensure no Virtual Machine allows Public access on SMTP port 25	✓	1	0
Ensure no Virtual Machine allows Public access on RDP port 3389	✓	1	0
Ensure no Virtual Machine allows Public access on RPC port 135	✓	1	0
Ensure no Virtual Machine allows Public access on MySQL port 3306	✓	1	0

Evaluation Summary

AC-4 Information Flow Enforcement 33/39

Policy Name	Compliance	Passed	Failed
Ensure no Virtual Machine allows Public access on Elastic search port 9300	✓	1	0
Ensure no Virtual Machine allows Public access on MSSQL port 1433	✓	1	0
Ensure no Virtual Machine allows Public access on Cassandra Internode Communication port 7000	✓	1	0
Ensure no Virtual Machine allows Public access on Redis port 6379	✓	1	0
Ensure no Network Security Groups allow Egress to 0.0.0.0/0	✗	5659	3
Ensure no Virtual Machine allows Public access on service SNMP UDP port 161	✓	1	0
Ensure no Network Security Groups allow Egress to any IPv4 address to ALL ports	✗	5660	2
Public Virtual Machines	✗	0	1
Ensure no Virtual Machine allows Public access on Mongod (with configsvr option) default port 27019	✓	1	0
Ensure no Virtual Machine allows Public access on SSH port 22	✗	0	1
Ensure no Virtual Machine allows Public access on TELNET port 23	✓	1	0
Ensure no Virtual Machine allows Public access on Postgres SQL port 5432	✓	1	0
Ensure no Virtual Machine allows Public access on mongod (with shardsvr option) default port 27018	✓	1	0

Evaluation Summary

AC-4 Information Flow Enforcement 33/39

Policy Name	Compliance	Passed	Failed
Ensure no Virtual Machine allows Public access on Cassandra Thrift port 9160	✓	1	0
Ensure no Virtual Machine allows Public access on Mongod default port 27017	✓	1	0
Ensure no Network Security Groups allow Ingress from 0.0.0.0/0	✗	5499	163
Ensure no Virtual Machine allows Public access on Elastic search port 9200	✓	1	0
Ensure no Virtual Machine allows Public access on Oracle port 1521	✓	1	0
Ensure no Virtual Machine allows Public access on MSSQL monitor port 1434	✓	1	0
Ensure no Virtual Machine allows Public access on DNS port 53	✓	1	0
Ensure that no SQL Databases allow ingress from 0.0.0.0/0	✓	0	0
Ensure no Virtual Machine allows Public access on Cassandra Client port 9042	✓	1	0
Ensure no Virtual Machine allows Public access on Memcached port 11211	✓	1	0
Ensure no Virtual Machine allows Public access on LDAP port 389	✓	1	0
Ensure no Virtual Machine allows Public access on Internal web port 8080	✓	1	0
Ensure no Network Security Groups allow Ingress from any IPv4 address to ALL ports	✗	5497	165

Evaluation Summary

AC-6 Least Privilege 6/13

Policy Name	Compliance	Passed	Failed
Ensure Activity Log Alert exists for Delete Security Solution	✗	0	1
Ensure Activity Log Alert exists for the Delete Network Security Group Rule	✗	0	1
Ensure Activity Log Alert exists for Create or Update Security Solution	✗	0	1
Ensure Activity Log Alert exists for Create or Update Network Security Group Rule	✗	0	1
Ensure Activity Log Alert exists for Update Security Policy	✗	0	1
Ensure Activity Log Alert exists for Delete SQL Server Firewall Rule	✓	1	0
Ensure SQLServers enable "Auditing"	✓	0	0
Enable role-based access control (RBAC) within Azure Kubernetes Services	✓	0	0
Ensure Activity Log Alert exists for Create/Update SQL Server Firewall Rule	✗	0	1
Ensure Activity Log Alert exists for Create or Update Network Security Group	✗	0	1
Ensure Activity Log Alert exists for Delete Network Security Group	✓	1	0
Ensure Activity Log Alert exists for Create Policy Assignment	✓	1	0
Ensure SQLServers configured with appropriate "AuditActionGroups"	✓	0	0

Evaluation Summary

AC-17 Remote Access 7/10

Policy Name	Compliance	Passed	Failed
Ensure SSL is enabled for PostgreSQL Database Server	✓	0	0
Ensure Storage Accounts enable Secure transfer	✓	78	0
Ensure the web app has Client Certificates (Incoming client certificates) set to "On"	✗	0	5
Ensure logging is enabled for Azure Key vault	✗	0	5
Ensure Log Profile is configured	✓	1	0
Ensure the web app is using the latest version of TLS encryption	✓	5	0
Ensure Log profile captures all the activities	✓	1	0
Ensure the web app in App Service redirects all HTTP traffic to HTTPS	✗	1	4
Ensure log profile captures activity logs for all regions including global	✓	1	0
Ensure SSL is enabled for MySQL Database Server	✓	0	0

Evaluation Summary

AU-2 Audit Events 5/6

Policy Name	Compliance	Passed	Failed
Ensure Log profile captures all the activities	✓	1	0
Ensure Log Profile is configured	✓	1	0
Ensure logging is enabled for Azure Key vault	✗	0	5
Ensure log profile captures activity logs for all regions including global	✓	1	0
Ensure SQLServers enable "Auditing"	✓	0	0
Ensure SQLServers configured with appropriate "AuditActionGroups"	✓	0	0

Evaluation Summary

AU-3 Content of Audit Records 3/4

Policy Name	Compliance	Passed	Failed
Ensure Log Profile is configured	✓	1	0
Ensure log profile captures activity logs for all regions including global	✓	1	0
Ensure Log profile captures all the activities	✓	1	0
Ensure logging is enabled for Azure Key vault	✗	0	5

Evaluation Summary

AU-4 Audit Storage Capacity 1/2

Policy Name	Compliance	Passed	Failed
Ensure SQLServers configured with Audit retention greater than 90 days	✓	0	0
Ensure Activity Log Retention is set as 365 days or greater	✗	0	1

Evaluation Summary

AU-5 Response to Audit Processing Failures 2/2

Policy Name	Compliance	Passed	Failed
Ensure SQLServers configured with appropriate emails to receive notifications under Advanced Data security	✓	0	0
Ensure SQLServers enable Email notification to admins and Subscription owners under Advanced Data Security	✓	0	0

Evaluation Summary

AU-10 Non-Repudiation 5/6

Policy Name	Compliance	Passed	Failed
Ensure Log profile captures all the activities	✓	1	0
Ensure Log Profile is configured	✓	1	0
Ensure logging is enabled for Azure Key vault	✗	0	5
Ensure log profile captures activity logs for all regions including global	✓	1	0
Ensure SQLServers enable "Auditing"	✓	0	0
Ensure SQLServers configured with appropriate "AuditActionGroups"	✓	0	0

Evaluation Summary

AU-11 Audit Record Retention 1/2

Policy Name	Compliance	Passed	Failed
Ensure SQLServers configured with Audit retention greater than 90 days	✓	0	0
Ensure Activity Log Retention is set as 365 days or greater	✗	0	1

Evaluation Summary

AU-12 Audit Generation 5/6

Policy Name	Compliance	Passed	Failed
Ensure Log profile captures all the activities	✓	1	0
Ensure Log Profile is configured	✓	1	0
Ensure logging is enabled for Azure Key vault	✗	0	5
Ensure log profile captures activity logs for all regions including global	✓	1	0
Ensure SQLServers enable "Auditing"	✓	0	0
Ensure SQLServers configured with appropriate "AuditActionGroups"	✓	0	0

Evaluation Summary

CM-5 Access Restrictions For Change 8/16

Policy Name	Compliance	Passed	Failed
Ensure Activity Log Alert exists for the Delete Network Security Group Rule	✗	0	1
Ensure Activity Log Alert exists for Delete SQL Server Firewall Rule	✓	1	0
Ensure Activity Log Alert exists for Create or Update Network Security Group Rule	✗	0	1
Ensure Activity Log Alert exists for Update Security Policy	✗	0	1
Ensure Activity Log Alert exists for Create or Update Security Solution	✗	0	1
Ensure SQLServers configured with appropriate emails to receive notifications under Advanced Data security	✓	0	0
Ensure Activity Log Alert exists for Delete Security Solution	✗	0	1
Ensure Activity Log Alert exists for Create/Update SQL Server Firewall Rule	✗	0	1
Ensure Activity Log Alert exists for Create or Update Network Security Group	✗	0	1
Ensure Activity Log Alert exists for Create Policy Assignment	✓	1	0
Ensure Activity Log Alert exists for Delete Network Security Group	✓	1	0
Ensure SQLServers enable Email notification to admins and Subscription owners under Advanced Data Security	✓	0	0
Ensure default network access rule for Storage Accounts is set to deny	✗	0	78

Evaluation Summary

CM-5 Access Restrictions For Change 8/16

Policy Name	Compliance	Passed	Failed
Enable role-based access control (RBAC) within Azure Kubernetes Services	✓	0	0
Ensure SQLServers configured with appropriate "AuditActionGroups"	✓	0	0
Ensure SQLServers enable "Auditing"	✓	0	0

Evaluation Summary

CM-6 Configuration Settings 6/14

Policy Name	Compliance	Passed	Failed
Ensure Activity Log Alert exists for Delete SQL Server Firewall Rule	✓	1	0
Ensure Activity Log Alert exists for Create or Update Network Security Group Rule	✗	0	1
Ensure Activity Log Alert exists for the Delete Network Security Group Rule	✗	0	1
Ensure log profile captures activity logs for all regions including global	✓	1	0
Ensure Activity Log Alert exists for Create/Update SQL Server Firewall Rule	✗	0	1
Ensure Activity Log Alert exists for Create or Update Network Security Group	✗	0	1
Ensure Activity Log Alert exists for Delete Network Security Group	✓	1	0
Ensure Activity Log Alert exists for Create Policy Assignment	✓	1	0
Ensure Log profile captures all the activities	✓	1	0
Ensure Activity Log Alert exists for Delete Security Solution	✗	0	1
Ensure Log Profile is configured	✓	1	0
Ensure logging is enabled for Azure Key vault	✗	0	5
Ensure Activity Log Alert exists for Update Security Policy	✗	0	1

Evaluation Summary

CM-6 Configuration Settings 6/14

Policy Name	Compliance	Passed	Failed
Ensure Activity Log Alert exists for Create or Update Security Solution	✗	0	1

Evaluation Summary

CM-7 Least Functionality 33/40

Policy Name	Compliance	Passed	Failed
Ensure no Virtual Machine allows Public access on FTP port 20	✓	1	0
Ensure no Virtual Machine allows Public access on NetBIOS port 137	✓	1	0
Ensure no Virtual Machine allows Public access on FTP port 21	✓	1	0
Ensure no Virtual Machine allows Public access on NetBIOS port 138	✓	1	0
Ensure no Virtual Machine allows Public access on Cassandra Monitoring port 7199	✓	1	0
Ensure no Virtual Machine allows Public access on Oracle DB port 2483	✓	1	0
Ensure no Virtual Machine allows Public access on LDAP port 389	✓	1	0
Ensure no Virtual Machine allows Public access on RPC port 135	✓	1	0
Ensure no Virtual Machine allows Public access on SMB port 445	✓	1	0
Ensure no Virtual Machine allows Public access on NetBIOS port 139	✓	1	0
Ensure no Virtual Machine allows Public access on MySQL port 3306	✓	1	0
Ensure no Virtual Machine allows Public access on Elastic search port 9300	✓	1	0
Ensure no Virtual Machine allows Public access on MSSQL port 1433	✓	1	0

Evaluation Summary

CM-7 Least Functionality 33/40

Policy Name	Compliance	Passed	Failed
Ensure no Virtual Machine allows Public access on Cassandra Internode Communication port 7000	✓	1	0
Ensure no Virtual Machine allows Public access on Redis port 6379	✓	1	0
Ensure no Network Security Groups allow Egress to 0.0.0.0/0	✗	5659	3
Ensure no Virtual Machine allows Public access on service SNMP UDP port 161	✓	1	0
Ensure no Network Security Groups allow Egress to any IPv4 address to ALL ports	✗	5660	2
Public Virtual Machines	✗	0	1
Ensure no Virtual Machine allows Public access on Mongod (with configsvr option) default port 27019	✓	1	0
Ensure no Virtual Machine allows Public access on SSH port 22	✗	0	1
Ensure no Virtual Machine allows Public access on TELNET port 23	✓	1	0
Ensure no Virtual Machine allows Public access on Postgres SQL port 5432	✓	1	0
Ensure no Virtual Machine allows Public access on mongod (with shardsvr option) default port 27018	✓	1	0
Ensure no Virtual Machine allows Public access on Cassandra Thrift port 9160	✓	1	0
Ensure no Virtual Machine allows Public access on Mongod default port 27017	✓	1	0

Evaluation Summary

CM-7 Least Functionality 33/40

Policy Name	Compliance	Passed	Failed
Ensure no Network Security Groups allow Ingress from 0.0.0.0/0	✗	5499	163
Ensure no Virtual Machine allows Public access on Elastic search port 9200	✓	1	0
Ensure no Virtual Machine allows Public access on Oracle port 1521	✓	1	0
Ensure no Virtual Machine allows Public access on MSSQL monitor port 1434	✓	1	0
Ensure no Virtual Machine allows Public access on DNS port 53	✓	1	0
Ensure no Virtual Machine allows Public access on LDAP SSL port 636	✓	1	0
Ensure no Virtual Machine allows Public access on RDP port 3389	✓	1	0
Ensure default network access rule for Storage Accounts is set to deny	✗	0	78
Ensure no Virtual Machine allows Public access on SMTP port 25	✓	1	0
Ensure no Virtual Machine allows Public access on Internal web port 8080	✓	1	0
Ensure no Virtual Machine allows Public access on Memcached port 11211	✓	1	0
Ensure no Virtual Machine allows Public access on Cassandra Client port 9042	✓	1	0
Ensure that no SQL Databases allow ingress from 0.0.0.0/0	✓	0	0

Evaluation Summary

CM-7 Least Functionality 33/40

Policy Name	Compliance	Passed	Failed
Ensure no Network Security Groups allow Ingress from any IPv4 address to ALL ports	✗	5497	165

Evaluation Summary

SC-7 Boundary Protection 34/39

Policy Name	Compliance	Passed	Failed
Ensure no Virtual Machine allows Public access on FTP port 20	✓	1	0
Ensure no Virtual Machine allows Public access on NetBIOS port 137	✓	1	0
Ensure no Virtual Machine allows Public access on FTP port 21	✓	1	0
Ensure no Virtual Machine allows Public access on NetBIOS port 138	✓	1	0
Ensure no Virtual Machine allows Public access on Cassandra Monitoring port 7199	✓	1	0
Ensure no Virtual Machine allows Public access on Oracle DB port 2483	✓	1	0
Ensure no Virtual Machine allows Public access on LDAP port 389	✓	1	0
Ensure no Virtual Machine allows Public access on RPC port 135	✓	1	0
Ensure no Virtual Machine allows Public access on SMB port 445	✓	1	0
Ensure no Virtual Machine allows Public access on Mongod (with configsvr option) default port 27019	✓	1	0
Ensure no Virtual Machine allows Public access on SSH port 22	✗	0	1
Ensure no Virtual Machine allows Public access on TELNET port 23	✓	1	0
Ensure no Virtual Machine allows Public access on Postgres SQL port 5432	✓	1	0

Evaluation Summary

SC-7 Boundary Protection — 34/39

Policy Name	Compliance	Passed	Failed
Ensure no Virtual Machine allows Public access on mongod (with shardsvr option) default port 27018	✓	1	0
Ensure no Virtual Machine allows Public access on Cassandra Thrift port 9160	✓	1	0
Ensure no Virtual Machine allows Public access on Mongod default port 27017	✓	1	0
Ensure Cosmos DB account is not exposed to the Internet	✓	0	0
Ensure no Virtual Machine allows Public access on MySQL port 3306	✓	1	0
Ensure no Virtual Machine allows Public access on Elastic search port 9300	✓	1	0
Ensure no Virtual Machine allows Public access on MSSQL port 1433	✓	1	0
Public Virtual Machines	✗	0	1
Ensure no Network Security Groups allow Egress to 0.0.0.0/0	✗	5659	3
Ensure no Virtual Machine allows Public access on Cassandra Internode Communication port 7000	✓	1	0
Ensure no Virtual Machine allows Public access on Redis port 6379	✓	1	0
Ensure no Virtual Machine allows Public access on service SNMP UDP port 161	✓	1	0
Ensure no Network Security Groups allow Egress to any IPv4 address to ALL ports	✗	5660	2

Evaluation Summary

SC-7 Boundary Protection 34/39

Policy Name	Compliance	Passed	Failed
Ensure no Virtual Machine allows Public access on Elastic search port 9200	✓	1	0
Ensure no Virtual Machine allows Public access on Oracle port 1521	✓	1	0
Ensure no Virtual Machine allows Public access on MSSQL monitor port 1434	✓	1	0
Ensure no Virtual Machine allows Public access on DNS port 53	✓	1	0
Ensure no Virtual Machine allows Public access on LDAP SSL port 636	✓	1	0
Ensure no Virtual Machine allows Public access on RDP port 3389	✓	1	0
Ensure default network access rule for Storage Accounts is set to deny	✗	0	78
Ensure no Virtual Machine allows Public access on SMTP port 25	✓	1	0
Ensure no Virtual Machine allows Public access on Internal web port 8080	✓	1	0
Ensure no Virtual Machine allows Public access on Memcached port 11211	✓	1	0
Ensure no Virtual Machine allows Public access on Cassandra Client port 9042	✓	1	0
Ensure that no SQL Databases allow ingress from 0.0.0.0/0	✓	0	0
Ensure no Virtual Machine allows Public access on NetBIOS port 139	✓	1	0

Evaluation Summary

SC-8 Transmission Confidentiality and Integrity 4/6

Policy Name	Compliance	Passed	Failed
Ensure the web app in App Service redirects all HTTP traffic to HTTPS	✗	1	4
Ensure the web app is using the latest version of TLS encryption	✓	5	0
Ensure the web app has Client Certificates (Incoming client certificates) set to "On"	✗	0	5
Ensure Storage Accounts enable Secure transfer	✓	78	0
Ensure SSL is enabled for MySQL Database Server	✓	0	0
Ensure SSL is enabled for PostgreSQL Database Server	✓	0	0

Evaluation Summary

SC-13 Cryptographic Protection 2/4

Policy Name	Compliance	Passed	Failed
Ensure Virtual Machines have OS Disk Encrypted	✗	0	1
Ensure Virtual Machines have all Data Disks Encrypted	✓	1	0
Ensure SQL server TDE protector is encrypted with BYOK (Use your own key)	✓	0	0
Ensure Unattached Disks are Encrypted or Deleted	✗	0	3

Evaluation Summary

SC-23 Session Authenticity 4/6

Policy Name	Compliance	Passed	Failed
Ensure the web app in App Service redirects all HTTP traffic to HTTPS	✗	1	4
Ensure the web app is using the latest version of TLS encryption	✓	5	0
Ensure the web app has Client Certificates (Incoming client certificates) set to "On"	✗	0	5
Ensure Storage Accounts enable Secure transfer	✓	78	0
Ensure SSL is enabled for MySQL Database Server	✓	0	0
Ensure SSL is enabled for PostgreSQL Database Server	✓	0	0

Evaluation Summary

SC-28 Protection of Information at Rest 2/4

Policy Name	Compliance	Passed	Failed
Ensure Virtual Machines have OS Disk Encrypted	✗	0	1
Ensure Virtual Machines have all Data Disks Encrypted	✓	1	0
Ensure SQL server TDE protector is encrypted with BYOK (Use your own key)	✓	0	0
Ensure Unattached Disks are Encrypted or Deleted	✗	0	3

Policy Details

Ensure logging is enabled for Azure Key vault

Resource(s) Evaluated : 5

Non-Compliant Resource(s) : 5

Description

It is a security best practice to enable AuditEvent logging for Key Vault instances to ensure all interactions with key vaults are logged and available.

For more information visit
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-logging

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Key vaults".
3. Select each Key vault and click on "Diagnostic settings".
4. Click "Add diagnostic setting" or Click "Edit setting" if diagnostic setting already created.
5. Enable "Archive to a storage account".
6. Set "AuditEvent" with Retention as 180 days or as appropriate.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/anilresourcegroup/providers/Microsoft.KeyVault/vaults/arc1, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/anilresourcegroup/providers/Microsoft.KeyVault/vaults/arc1, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/anilresourcegroup/providers/Microsoft.KeyVault/vaults/arc1, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/anilresourcegroup/providers/Microsoft.KeyVault/vaults/arc1, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/anilresourcegroup/providers/Microsoft.KeyVault/vaults/arc1

Policy Details

Ensure Activity Log Alert exists for Delete Security Solution

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Activity log alerts are the alerts that get activated when a new activity log event occurs that matches the conditions specified in the alert. It is recommended to monitor the Delete Security Solution events to detect any security solution changes.

For more information visit
https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Monitor > Alerts".
3. Click "+ New alert rule"
4. Under RESOURCE, select the Subscription.
5. Under CONDITION, select "Delete Security Solutions (Microsoft.Security/securitySolutions)", and Alert logic as Event Level: "All", Status: "All", Event initiated by: "" or empty.
6. Under ACTIONS, select an appropriate action group.
7. Under ALERT DETAILS provide rule name, description, resource group and enable the rule upon creation.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21

Policy Details

Ensure Activity Log Alert exists for the Delete Network Security Group Rule

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Activity log alerts are the alerts that get activated when a new activity log event occurs that matches the conditions specified in the alert. It is recommended to monitor the Network Security Group Rule events to detect any network access changes.

For more information visit
https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Monitor > Alerts".
3. Click "+ New alert rule"
4. Under RESOURCE, select the Subscription.
5. Under CONDITION, select "Delete Security Rule (Microsoft.Network/networkSecurityGroups/securityRules)", and Alert logic as Event Level: "All", Status: "All", Event initiated by: "" or empty.
6. Under ACTIONS, select an appropriate action group.
7. Under ALERT DETAILS provide rule name, description, resource group and enable the rule upon creation.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21

Policy Details

Ensure Activity Log Alert exists for Create or Update Security Solution

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Activity log alerts are the alerts that get activated when a new activity log event occurs that matches the conditions specified in the alert. It is recommended to monitor the Create or Update Security Solution events to detect any active security solution changes.

For more information visit
https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Monitor > Alerts".
3. Click "+ New alert rule"
4. Under RESOURCE, select the Subscription.
5. Under CONDITION, select "Create or Update Security Solutions (Microsoft.Security/securitySolutions)", and Alert logic as Event Level: "All", Status: "All", Event initiated by: "" or empty.
6. Under ACTIONS, select an appropriate action group.
7. Under ALERT DETAILS provide rule name, description, resource group and enable the rule upon creation.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21

Policy Details

Ensure Activity Log Alert exists for Create or Update Network Security Group Rule

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Activity log alerts are the alerts that get activated when a new activity log event occurs that matches the conditions specified in the alert. It is recommended to monitor the Network Security Group Rule events to detect any network access changes.

For more information visit
https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Monitor > Alerts".
3. Click "+ New alert rule"
4. Under RESOURCE, select the Subscription.
5. Under CONDITION, select "Create or Update Security Rule (Microsoft.Network/networkSecurityGroups/securityRules)", and Alert logic as Event Level: "All", Status: "All", Event initiated by: "" or empty.
6. Under ACTIONS, select an appropriate action group.
7. Under ALERT DETAILS provide rule name, description, resource group and enable the rule upon creation.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21

Policy Details

Ensure Activity Log Alert exists for Update Security Policy

Resource(s) Evaluated : 1	Non-Compliant Resource(s) : 1

Description

Activity log alerts are the alerts that get activated when a new activity log event occurs that matches the conditions specified in the alert. It is recommended to monitor the Update Security Policy events to detect any security policy changes.

For more information visit
https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Monitor > Alerts".
3. Click "+ New alert rule"
4. Under RESOURCE, select the Subscription.
5. Under CONDITION, select "Update security policy (Microsoft.Security/policies)", and Alert logic as Event Level: "All", Status: "All", Event initiated by: "" or empty.
6. Under ACTIONS, select an appropriate action group.
7. Under ALERT DETAILS provide rule name, description, resource group and enable the rule upon creation.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21

Policy Details

Ensure Activity Log Alert exists for Create/Update SQL Server Firewall Rule

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Activity log alerts are the alerts that get activated when a new activity log event occurs that matches the conditions specified in the alert. It is recommended to monitor the Create/Update SQL Server Firewall Rule events to detect any network access changes to the database.

For more information visit
https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Monitor > Alerts".
3. Click "+ New alert rule"
4. Under RESOURCE, select the Subscription.
5. Under CONDITION, select "Create/Update server firewall rule (Microsoft.Sql/servers/firewallRules)", and Alert logic as Event Level: "All", Status: "All", Event initiated by: "" or empty.
6. Under ACTIONS, select an appropriate action group.
7. Under ALERT DETAILS provide rule name, description, resource group and enable the rule upon creation.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21

Policy Details

Ensure Activity Log Alert exists for Create or Update Network Security Group

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Activity log alerts are the alerts that get activated when a new activity log event occurs that matches the conditions specified in the alert. It is recommended to monitor the Network Security Group events to detect any network access changes.

For more information visit
https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Monitor > Alerts".
3. Click "+ New alert rule"
4. Under RESOURCE, select the Subscription.
5. Under CONDITION, select "Create or Update Network Security Group (Microsoft.Network/networkSecurityGroups)", and Alert logic as Event Level: "All", Status: "All", Event initiated by: "" or empty.
6. Under ACTIONS, select an appropriate action group.
7. Under ALERT DETAILS provide rule name, description, resource group and enable the rule upon creation.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21

Policy Details

Ensure the web app in App Service redirects all HTTP traffic to HTTPS

Resource(s) Evaluated : 5

Non-Compliant Resource(s) : 4

Description

Allowing only HTTPS traffic ensures the connection between clients and web apps is secure, and avoid any man-in-the-middle attacks.

For more information visit https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-ssl#enforce-https

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "App Services".
3. Select each App, and click on "TLS/SSL settings".
4. Under Protocol Settings, Set "HTTPS Only" to "On".

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Web/sites/testsoni1, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Web/sites/looseupagain, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/dopaminesoni/providers/Microsoft.Web/sites/dopaminesoni, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/vasutest01/providers/Microsoft.Web/sites/vasutest01

Policy Details

Ensure the web app has Client Certificates (Incoming client certificates) set to "On"

Resource(s) Evaluated : 5

Non-Compliant Resource(s) : 5

Description

It is recommended to enable client certificates to ensure only an authenticated client with valid certificates can access the web app.

For more information visit

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "App Services".
3. Select each App, and click on "TLS/SSL settings".
4. Under Protocol Settings, Set "Incoming client certificates" to "On".

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Web/sites/testsoni1, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Web/sites/looseupagain, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Web/sites/SoniToasted, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/dopaminesoni/providers/Microsoft.Web/sites/dopaminesoni, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/vasutest01/providers/Microsoft.Web/sites/vasutest01

Policy Details

Ensure no Virtual Machine allows Public access on SSH port 22

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

SSH (Secure Shell) port - 22 is used to get CLI access to Linux Instances. Allowing Inbound traffic from all the external IP addresses to SSH port is vulnerable to â€œbanner grabbingâ€ and â€œbrute force attack.â€ It is a best practice to restrict access from specific IP addresses to port 22.

For more information visit
https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Virtual machines".
3. For each virtual machine, Click on "Networking".
4. Ensure there are no Inbound port rules from 0.0.0.0/0 to port 22.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/anilresourcegroup/providers/Microsoft.Compute/virtualMachines/test-resource-enrichment

Policy Details

Public Virtual Machines

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Allowing access from all IP addresses on the Internet to Virtual Machines is risky as it can lead to Brute Force or DoS attacks. It is a best practice to follow the principle of least privilege, and allow access to only required ports.

For more information visit
https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Virtual machines".
3. For each virtual machine, Click on "Networking".
4. Ensure there are no Inbound port rules from 0.0.0.0/0 to port 0-65535.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/anilresourcegroup/providers/Microsoft.Compute/virtualMachines/test-resource-enrichment

Policy Details

Ensure no Network Security Groups allow Egress to 0.0.0.0/0

Resource(s) Evaluated : 5662

Non-Compliant Resource(s) : 3

Description

Allowing Outbound traffic to any IP address can lead to internal resources accessing unwanted and untrusted resources. If a system is compromised, an attacker can use it to exfiltrate data or conduct spam or phishing campaigns. It is a best practice to restrict outbound traffic to only required IP address(es).

For more information visit
https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Network Security Groups" and select the network security group.
3. For each network security group, Click on "Outbound security rules".
4. Ensure there are no outbound rule with source as "Any".

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Network/networkSecurityGroups/nsg-1, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Network/networkSecurityGroups/nsg-3, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Network/networkSecurityGroups/nsg-4

Policy Details

Ensure no Network Security Groups allow Egress to any IPv4 address to ALL ports

Resource(s) Evaluated : 5662

Non-Compliant Resource(s) : 2

Description

Allowing Outbound traffic to ALL ports can lead to internal resources accessing unwanted and untrusted resources. It is a best practice to follow the principle of least privilege, and allow access to only required ports.

For more information visit
https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Network Security Groups" and select the network security group.
3. For each network security group, Click on "Outbound security rules".
4. Ensure there is no rule granting access to port range 0-65535.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Network/networkSecurityGroups/nsg-1, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Network/networkSecurityGroups/nsg-4

Policy Details

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

Resource(s) Evaluated : 78

Non-Compliant Resource(s) : 78

Description

It is recommended to restrict access to storage accounts from specific virtual networks. It helps in building a secure network boundary for your applications.

For more information visit
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security#grant-access-from-a-virtual-network

Recommendation

1. Login in to Azure Portal https://portal.azure.com.
2. Navigate to "Storage accounts" and select the storage account.
3. Click on the "Firewalls and virtual networks."
4. Ensure "Allow access from" is set for "Selected networks."

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Storage/storageAccounts/storageaccountsonit9c90, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Storage/storageAccounts/storageaccountsonitb129, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/soni-test/providers/Microsoft.Storage/storageAccounts/storageaccountsonit8ffa, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-eastasia-c3mauto-0/providers/Microsoft.Storage/storageAccounts/stgaccc3mautoqhs0, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-eastasia-c3mauto-0/providers/Microsoft.Storage/storageAccounts/stgaccc3mautorhs0, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-eastasia-c3mauto-0/providers/Microsoft.Storage/storageAccounts/stgaccc3mautolhs0, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-eastasia-c3mauto-2/providers/Microsoft.Storage/storageAccounts/stgaccc3mautolhs2, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-eastasia-c3mauto-2/providers/Microsoft.Storage/storageAccounts/stgaccc3mautorhs2, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-eastasia-c3mauto-2/providers/Microsoft.Storage/storageAccounts/stgaccc3mautoqhs2, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-eastasia-c3mauto-1/providers/Microsoft.Storage/storageAccounts/stgaccc3mautoqhs1, ...68 more

Policy Details

Ensure no Network Security Groups allow Ingress from 0.0.0.0/0

Resource(s) Evaluated : 5662

Non-Compliant Resource(s) : 163

Description

Allowing Inbound traffic from any IP address can lead to attacks like DoS, Brute Force, Smurf, and reconnaissance. It is a best practice to restrict inbound traffic from the required source IP address(es).

For more information visit
https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Network Security Groups" and select the network security group.
3. For each network security group, Click on "Inbound security rules".
4. Ensure there are no Inbound rule with source as "Any".

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-westeurope-c3mauto-0/providers/Microsoft.Network/networkSecurityGroups/vm-0-c3mauto-0NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-westeurope-c3mauto-0/providers/Microsoft.Network/networkSecurityGroups/vm-1-c3mauto-0NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-westeurope-c3mauto-1/providers/Microsoft.Network/networkSecurityGroups/vm-0-c3mauto-1NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-westeurope-c3mauto-1/providers/Microsoft.Network/networkSecurityGroups/vm-1-c3mauto-1NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-westeurope-c3mauto-2/providers/Microsoft.Network/networkSecurityGroups/vm-0-c3mauto-2NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-westeurope-c3mauto-2/providers/Microsoft.Network/networkSecurityGroups/vm-1-c3mauto-2NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-ukwest-c3mauto-1/providers/Microsoft.Network/networkSecurityGroups/vm-0-c3mauto-1NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-ukwest-c3mauto-1/providers/Microsoft.Network/networkSecurityGroups/vm-1-c3mauto-1NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-ukwest-c3mauto-2/providers/Microsoft.Network/networkSecurityGroups/vm-1-c3mauto-2NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-ukwest-c3mauto-2/providers/Microsoft.Network/networkSecurityGroups/vm-0-c3mauto-2NSG, ...153 more

Policy Details

Ensure no Network Security Groups allow Ingress from any IPv4 address to ALL ports

Resource(s) Evaluated : 5662

Non-Compliant Resource(s) : 165

Description

Allowing Inbound traffic to ALL ports increases the attack surface of your environment. It is a best practice to follow the principle of least privilege, and allow access to only required ports.

For more information visit
https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Network Security Groups" and select the network security group.
3. For each network security group, Click on "Inbound security rules".
4. Ensure there is no rule granting access to port range 0-65535.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-westeurope-c3mauto-0/providers/Microsoft.Network/networkSecurityGroups/vm-0-c3mauto-0NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-westeurope-c3mauto-0/providers/Microsoft.Network/networkSecurityGroups/vm-1-c3mauto-0NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-westeurope-c3mauto-1/providers/Microsoft.Network/networkSecurityGroups/vm-0-c3mauto-1NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-westeurope-c3mauto-1/providers/Microsoft.Network/networkSecurityGroups/vm-1-c3mauto-1NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-westeurope-c3mauto-2/providers/Microsoft.Network/networkSecurityGroups/vm-0-c3mauto-2NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-westeurope-c3mauto-2/providers/Microsoft.Network/networkSecurityGroups/vm-1-c3mauto-2NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-ukwest-c3mauto-1/providers/Microsoft.Network/networkSecurityGroups/vm-0-c3mauto-1NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-ukwest-c3mauto-1/providers/Microsoft.Network/networkSecurityGroups/vm-1-c3mauto-1NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-ukwest-c3mauto-2/providers/Microsoft.Network/networkSecurityGroups/vm-1-c3mauto-2NSG, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/rg-ukwest-c3mauto-2/providers/Microsoft.Network/networkSecurityGroups/vm-0-c3mauto-2NSG, ...155 more

Policy Details

Ensure Virtual Machines have OS Disk Encrypted

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

It is a security best practice to encrypt Virtual machines OS disk (boot volume) to ensure data at rest is always protected.

For more information visit
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

Recommendation

1. Disk encryption at Azure requires the KeyVault to be set up as a prerequisite. Follow the link to set up key vault if not done already https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites#prerequisite-workflow-for-key-vault.
2. Follow the instructions below to encrypt Linux IaaS VMs https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-linux
3. Follow the instructions below to encrypt Windows IaaS VMs https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-windows

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/anilresourcegroup/providers/Microsoft.Compute/virtualMachines/test-resource-enrichment

Policy Details

Ensure Unattached Disks are Encrypted or Deleted

Resource(s) Evaluated : 3

Non-Compliant Resource(s) : 3

Description

In order to avoid any sensitive information leaks, it is recommended to have the unattached disks encrypted, or deleted.

For more information visit
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

Recommendation

1. Please go through the links below to either encrypt or delete the unattached disks
2. https://docs.microsoft.com/en-us/rest/api/compute/disks/delete
3. https://docs.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest#az-disk-delete
4. https://docs.microsoft.com/en-us/rest/api/compute/disks/update#encryptionsettings
5. https://docs.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest#az-disk-update.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/anilresourcegroup/providers/Microsoft.Compute/disks/test-resource-enrichment_OsDisk_1_55cc1ee6031d4865a3f9ca5d1969ba9d, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/testVasu/providers/Microsoft.Compute/disks/myVm_OsDisk_1_57ac1a122136432c86ce4e3501e33f1c, /subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/resourceGroups/myvm01/providers/Microsoft.Compute/disks/vasumyvm01_OsDisk_1_da1520de2cce4f639400d93828f0203b

Policy Details

Ensure Activity Log Retention is set as 365 days or greater

Resource(s) Evaluated : 1

Non-Compliant Resource(s) : 1

Description

Log profile provides a mechanism to export the activity log and store the same for a more extended period. To identify any security incidents, it is a best practice to set a retention period as 365 days or more for log profiles.

For more information visit
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-export

Recommendation

1. Login into Azure Portal https://portal.azure.com.
2. Navigate to "Activity Log".
3. Click on "Export to Event Hub".
4. Select all regions, and configure export to the storage account.
5. Set Retention(days) as 365, or 0 and click Save.

Non-Compliant Resource(s)

/subscriptions/37cca1be-d0e3-42c7-ae26-908535a0ed21/providers/microsoft.insights/logprofiles/default