NSC42 LTD

When you are cybersafe
We are Cyberhappy

Nimble Cloud Security

get in touch with us for a free
www.nsc42.co.uk/nimblecloud

AWS GDPR Readiness

Jun 2, 2020 5:07 PM

Automated GDPR Assessment for AWS.
For additional reference:
https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf (https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf)

Cloud Account

AWS Stage (726853184812) , All Regions

EXECUTIVE SUMMARY

SUMMARY OF TESTS PERFORMED

Tests Performed	Passed	Failed
498	33.73% (168)	66.27% (330)

FAILED TESTS BY SEVERITY

Critical	High	Medium	Low	Informational
0	261	66	3	3

SUMMARY OF RULES TESTED

Rules Performed	Passed	Failed
140	52.14% (73)	47.86% (67)

Entities by type, Pass Vs Fail

Entity Type	Passed	Failed
ELB (3)	0	**3**
List<CloudTrail> (1)	0	**1**
Instance (28)	0	**28**
Kinesis (0)	0	0
S3Bucket (20)	0	**20**
NetworkLoadBalancer (0)	0	0
IamUser (17)	**1**	**16**
Iam (1)	0	**1**
ApplicationLoadBalancer (1)	0	**1**
CloudTrail (1)	0	**1**
Region (16)	0	**16**
Lambda (7)	**3**	**4**
RDS (2)	0	**2**
IamPolicy (680)	**679**	**1**
KMS (4)	**4**	0
EFS (1)	0	**1**
EcsCluster (2)	**2**	0

Regions

Name	Passed Tests	Failed Tests	Failed Entities	Failed Critical	Failed High	Failed Medium	Failed Low	Failed Informational
N. Virginia	**460**	**38**	**14**	0	**36**	**2**	0	0
Ohio	**488**	**10**	**3**	0	**9**	**1**	0	0
Oregon	**479**	**19**	**9**	0	**16**	**3**	0	0
N. California	**491**	**7**	**2**	0	**6**	**1**	0	0
Ireland	**497**	**1**	**1**	0	**1**	0	0	0
Frankfurt	**497**	**1**	**1**	0	**1**	0	0	0
Singapore	**497**	**1**	**1**	0	**1**	0	0	0
Sydney	**497**	**1**	**1**	0	**1**	0	0	0

Name	Passed Tests	Failed Tests	Failed Entities	Failed Critical	Failed High	Failed Medium	Failed Low	Failed Informational
Tokyo	**497**	**1**	**1**	0	**1**	0	0	0
Seoul	**497**	**1**	**1**	0	**1**	0	0	0
São Paulo	**497**	**1**	**1**	0	**1**	0	0	0
Mumbai	**497**	**1**	**1**	0	**1**	0	0	0
Canada Central	**497**	**1**	**1**	0	**1**	0	0	0
London	**497**	**1**	**1**	0	**1**	0	0	0
Paris	**497**	**1**	**1**	0	**1**	0	0	0
Stockholm	**496**	**2**	**1**	0	**2**	0	0	0

Failed Tests Summary

Rule Name	Severity	Tested	Relevant	Non Compliant
Instances without Inspector runs in the last 30 days	**High**	**28**	**28**	**28**
Instances outside of Europe	**High**	**28**	**28**	**28**
Use encryption for S3 Bucket write actions	**High**	**20**	**20**	**20**
S3 Buckets Secure Transport (SSL)	**High**	**20**	**20**	**20**
S3 Buckets outside of Europe	**High**	**20**	**20**	**20**
S3 bucket should have versioning MFA delete enabled	**High**	**20**	**20**	**20**
S3 Buckets Server Side Encryption At Rest	**High**	**20**	**20**	**17**
Ensure AWS Config is enabled in all regions	**High**	**16**	**16**	**16**
Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	**High**	**17**	**15**	**15**
Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket	**High**	**20**	**7**	**7**
Instance with unencrypted Oracle DB (TCP:2483) is potentially exposed to the public internet	**High**	**28**	**8**	**4**
Instance with unencrypted Mongo (TCP:27017) is potentially exposed to the public internet	**High**	**28**	**8**	**4**
Use encrypted storage for instances that might host a database.	**High**	**28**	**4**	**4**
Lambda Functions with Admin Privileges are not created	**High**	**7**	**7**	**4**
EC2 Instance - there shouldn't be any High level findings in Inspector Scans	**High**	**28**	**28**	**4**
Instance with administrative service: Remote Desktop (TCP:3389) is too exposed to the public internet	**High**	**28**	**13**	**4**
Instance with administrative service: SSH (TCP:22) is too exposed to the public internet	**High**	**28**	**16**	**3**
ELB is setup with SSL for secure communication	**High**	**3**	**3**	**3**
Instance with unencrypted Oracle DB (TCP:1521) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Instance with unencrypted Oracle DB (UDP:2483) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Instance with unencrypted Cassandra Thrift (TCP:9160) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Use Encrypted RDS storage	**High**	**2**	**2**	**2**
Instance with unencrypted Cassandra Monitoring (TCP:7199) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Instance with unencrypted Cassandra Client (TCP:9042) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Instance with unencrypted Cassandra OpsCenter Monitoring (TCP:61620) is potentially exposed to the public internet	**High**	**28**	**5**	**2**

Rule Name	Severity	Tested	Relevant	Non Compliant
Instance with unencrypted LDAP (UDP:389) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Instance with unencrypted Elastic search (TCP:9300) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Instance with unencrypted Elastic search (TCP:9200) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Instance with unencrypted Memcached (UDP:11211) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Instance with unencrypted Cassandra OpsCenter Website (TCP:8888) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Instance with unencrypted LDAP (TCP:389) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Instance with unencrypted Memcached (TCP:11211) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Instance with unencrypted Cassandra Internode Communication (TCP:7000) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Instance with unencrypted Redis (TCP:6379) is potentially exposed to the public internet	**High**	**28**	**5**	**2**
Ensure CloudTrail logs are encrypted at rest using KMS CMKs	**High**	**1**	**1**	**1**
ELB with unencrypted Oracle DB (TCP:2483) is potentially exposed to the public internet	**High**	**3**	**1**	**1**
Ensure VPC Flow Logging is Enabled in all Applicable Regions	**High**	**16**	**16**	**1**
Ensure HARDWARE MFA is enabled for the 'root' account	**High**	**17**	**1**	**1**
Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible	**High**	**20**	**7**	**1**
ApplicationLoadBalancer with administrative service: Remote Desktop (TCP:3389) is too exposed to the public internet	**High**	**1**	**1**	**1**
Ensure that your Amazon EFS file systems are encrypted	**High**	**1**	**1**	**1**
Ensure VIRTUAL MFA is enabled for the "root" account	**High**	**17**	**1**	**1**
S3 bucket should have server access logging enabled	**Medium**	**20**	**20**	**17**
Credentials (with password enabled) unused for 90 days or more should be disabled	**Medium**	**17**	**15**	**14**
Ensure IAM policies are attached only to groups or roles	**Medium**	**17**	**16**	**8**
Credentials (with first activated accessKey) unused for 90 days or more should be disabled	**Medium**	**17**	**4**	**4**
Ensure first access key is rotated every 90 days or less	**Medium**	**17**	**4**	**4**
ELB is created with Access logs enabled	**Medium**	**3**	**3**	**3**
Ensure a log metric filter and alarm exist for AWS Config configuration changes	**Medium**	**1**	**1**	**1**
Ensure a log metric filter and alarm exist for changes to network gateways	**Medium**	**1**	**1**	**1**
Ensure a log metric filter and alarm exist for AWS Management Console authentication failures	**Medium**	**1**	**1**	**1**
Ensure a log metric filter and alarm exist for IAM policy changes	**Medium**	**1**	**1**	**1**
Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs	**Medium**	**1**	**1**	**1**
Ensure CloudTrail trails are integrated with CloudWatch	**Medium**	**1**	**1**	**1**
Ensure a log metric filter and alarm exist for Management Console sign-in without MFA	**Medium**	**1**	**1**	**1**
Ensure a log metric filter and alarm exist for route table changes	**Medium**	**1**	**1**	**1**

Rule Name	Severity	Tested	Relevant	Non Compliant
Ensure second access key is rotated every 90 days or less	**Medium**	**17**	**1**	**1**
Ensure a log metric filter and alarm exist for unauthorized API calls	**Medium**	**1**	**1**	**1**
Ensure a log metric filter and alarm exist for VPC changes	**Medium**	**1**	**1**	**1**
Ensure a log metric filter and alarm exist for security group changes	**Medium**	**1**	**1**	**1**
Ensure a log metric filter and alarm exist for usage of 'root' account	**Medium**	**1**	**1**	**1**
Ensure a log metric filter and alarm exist for S3 bucket policy changes	**Medium**	**1**	**1**	**1**
Credentials (with second activated accessKey) unused for 90 days or more should be disabled	**Medium**	**17**	**1**	**1**
Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)	**Medium**	**1**	**1**	**1**
Ensure IAM password policy expires passwords within 90 days or less	**Low**	**1**	**1**	**1**
Ensure a support role has been created to manage incidents with AWS Support	**Low**	**680**	**1**	**1**
Ensure a log metric filter and alarm exist for CloudTrail configuration changes	**Low**	**1**	**1**	**1**