APPENDIX A FULL LIST OF THE SELECTED AND CATEGORIZED AWS POLICIES WITH RESULTS

Table A.1 AWS: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
Admin by default	Ensure IAM policies that allow full ""-"" administrative privileges are not created	2172	2163	9	99.58
	Ensure KMS key policy does not contain wildcard (*) principal	243	239	4	98.35
	Ensure no IAM policies documents allow ""*"" as a statement's actions	2172	2158	14	99.35
	Ensure IAM policies that allow full ""-"" administrative privileges are not created	2639	2597	42	98.40
	Ensure no IAM policies documents allow ""*"" as a statement's actions	2640	2596	44	98.33
	Ensure SQS policy does not allow ALL (*) actions.	48	48	0	100.0
Encryption in transit	Ensure ALB protocol is HTTPS	359	223	136	62.11
	Ensure all Elasticsearch has node-to-node encryption enabled	38	30	8	78.94
	Ensure all data stored in the Elasticache Replication Group is securely encrypted at transit	39	13	26	33.33
	Ensure all data stored in the Elasticache Replication Group is securely encrypted at transit and has auth token	39	6	33	15.38
	Ensure cloudfront distribution ViewerProtocolPolicy is set to HTTPS	188	147	41	78.19

continued on the next page

Table A.1 AWS: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	Policies	Nb of checks	Nb pass	Nb fail	Pass Rate%
Encryption in transit	Ensure Elasticsearch Domain enforces HTTPS	40	39	1	97.5
	Ensure Encryption in transit is enabled for EFS volumes in ECS Task definitions	293	289	4	98.63
	Ensure that load balancer is using TLS 1.2	281	160	121	56.93
	Ensure Redshift uses SSL	7	2	5	28.57
	Ensure Session Manager data is encrypted in transit	6	4	2	66.66
	Ensure that ALB drops HTTP headers	204	20	184	9.803
	Ensure MemoryDB data is encrypted in transit	1	1	0	100.0
	Ensure ELB Policy uses only secure protocols	5	5	0	100.0
	Ensure Appsync API Cache is encrypted in transit	0	0	0	
	Ensure that ALB redirects HTTP requests into HTTPS ones	216	144	72	66.66
Encryption at rest	Ensure all data stored in the EBS is securely encrypted	165	83	82	50.30
	Ensure all data stored in the Elasticsearch is securely encrypted at rest	40	8	32	20.0
	Ensure all data stored in the Launch configuration or instance Elastic Blocks Store is securely encrypted	850	43	807	5.058
	Ensure all data stored in the RDS is securely encrypted at rest	202	55	147	27.22
	Ensure all data stored in the S3 bucket is securely encrypted at rest	1441	310	1131	21.51
	Ensure SageMaker Notebook is encrypted at rest using KMS CMK	3	1	2	33.33
	Ensure all data stored in the SNS topic is encrypted	216	40	176	18.51
	Ensure all data stored in the SQS queue is encrypted	212	42	170	19.81
	Ensure all data stored in the Elasticache Replication Group is securely encrypted at rest	39	13	26	33.33
	Ensure CloudTrail logs are encrypted at rest using KMS CMKs	54	15	39	27.77

continued on the next page

Table A.1 AWS: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	Policies	Nb of checks	Nb pass	Nb fail	Pass Rate%
Encryption at rest	Ensure EFS is securely encrypted	51	22	29	43.13
	Ensure Kinesis Stream is securely encrypted	24	5	19	20.83
	Ensure Neptune storage is securely encrypted	12	0	12	0.0
	Ensure DAX is encrypted at rest (default is unencrypted)	2	1	1	50.0
	Ensure all data stored in the Redshift cluster is securely encrypted at rest	19	2	17	10.52
	Ensure Athena Database is encrypted at rest (default is unencrypted)	7	2	5	28.57
	Ensure Glue Data Catalog Encryption is enabled	2	2	0	100.0
	Ensure all data stored in Aurora is securely encrypted at rest	53	24	29	45.28
	Ensure all data stored in the Sagemaker Endpoint is securely encrypted at rest	2	1	1	50.0
	Ensure Glue Security Configuration Encryption is enabled	4	1	3	25.0
	Ensure EBS default encryption is enabled	11	9	2	81.81
	Ensure DynamoDB Tables are encrypted using a KMS Customer Managed CMK	161	9	152	5.590
	Ensure that ECR repositories are encrypted using KMS	159	3	156	1.886
	Ensure that RDS global clusters are encrypted	4	1	3	25.0
	Ensure that Redshift cluster is encrypted by KMS	19	1	18	5.263
	Ensure that Workspace user volumes are encrypted	0	0	0	
	Ensure that Workspace root volumes are encrypted	0	0	0	
	Check encryption settings for Lambda environmental variable	383	96	287	25.06
	Ensure MemoryDB is encrypted at rest using KMS CMKs	1	0	1	0.0

continued on the next page

Table A.1 AWS: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	Policies	Nb of checks	Nb pass	Nb fail	Pass Rate%
Encryption at rest	Ensure AMIs are encrypted using KMS CMKs	11	9	2	81.81
	Ensure MQ broker encrypted by KMS using a customer managed Key (CMK)	18	2	16	11.11
	Ensure EBS Volume is encrypted by KMS using a customer managed Key (CMK)	8	2	6	25.0
	Ensure Appsync API Cache is encrypted at rest	0	0	0	
	Ensure KMS key is enabled	243	242	1	99.58
	Ensure that only encrypted EBS volumes are attached to EC2 instances	159	141	18	88.67
Access policy	Ensure all data stored in RDS is not publicly accessible	238	215	23	90.33
	S3 Bucket has an ACL defined which allows public READ access.	1439	1249	190	86.79
	Ensure ECR policy is not set to public	24	22	2	91.66
	Ensure Amazon EKS public endpoint disabled	42	4	38	9.523
	Ensure IAM policies are attached only to groups or roles (Reducing access management complexity may in-turn reduce opportunity for a principal to inadvertently receive or retain excessive privileges.)	387	166	221	42.89
	Ensure S3 bucket has block public ACLS enabled	303	287	16	94.71
	Ensure S3 bucket has block public policy enabled	303	291	12	96.03
	Ensure S3 bucket has ignore public ACLs enabled	304	280	24	92.10
	Ensure S3 bucket has ’restrict_public_bucket’ enabled	303	268	35	88.44
	S3 Bucket has an ACL defined which allows public WRITE access.	1436	1383	53	96.30
	Ensure there is no open access to back-end resources through API	158	74	84	46.83
	Ensure IAM role allows only specific services or principals to assume it	1911	1910	1	99.94

continued on the next page

Table A.1 AWS: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	Policies	Nb of checks	Nb pass	Nb fail	Pass Rate%
Access policy	Ensure AWS IAM policy does not allow assume role permission across all services	1911	1910	1	99.94
	CloudFront Distribution should have WAF enabled	188	12	176	6.382
	Ensure MQ Broker is not publicly exposed	18	16	2	88.88
	Redshift cluster should not be publicly accessible	19	2	17	10.52
	Ensure Neptune Cluster instance is not publicly available	3	3	0	100.0
	Ensure IAM policies does not allow credentials exposure	2161	2133	28	98.70
	Ensure IAM policies does not allow data exfiltration	2161	2124	37	98.28
	Ensure IAM policies does not allow privilege escalation	2162	2142	20	99.07
	Ensure IAM policies does not allow write access without constraints	2141	1780	361	83.13
	Ensure that AWS Lambda function is configured inside a VPC	613	159	454	25.93
	Ensure SQS queue policy is not public by only allowing specific services or principals to access it	228	223	5	97.80
	Ensure SNS topic policy is not public by only allowing specific services or principals to access it	3	2	1	66.66
	Ensure that S3 bucket has a Public Access block	1428	224	1204	15.68
	Ensure that Amazon EMR clusters' security groups are not open to the world	6	4	2	66.66
	Ensure the default security group of every VPC restricts all traffic	440	3	437	0.681
	Ensure public facing ALB are protected by WAF	206	102	104	49.51
	Ensure public API gateway are protected by WAF	34	5	29	14.70

continued on the next page

Table A.1 AWS: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
Logging/Monitoring	Ensure the S3 bucket has access logging enabled	1435	176	1259	12.26
	Ensure MQ Broker logging is enabled	19	4	15	21.05
	X-ray tracing is enabled for Lambda	613	108	505	17.61
	Ensure CloudTrail is enabled in all Regions	54	22	32	40.74
	Ensure Redshift Cluster logging is enabled	19	3	16	15.78
	Ensure API Gateway has X-Ray Tracing enabled	35	8	27	22.85
	Ensure API Gateway has Access Logging enabled	64	16	48	25.0
	Ensure Elasticsearch Domain Logging is enabled	40	13	27	32.5
	Ensure the ELBv2 (Application/Network) has access logging enabled	252	74	178	29.36
	Ensure the ELB has access logging enabled	174	69	105	39.65
	Ensure Neptune logging is enabled	12	1	11	8.333
	Ensure Session Manager logs are enabled and encrypted	3	1	2	33.33
	Ensure that enhanced monitoring is enabled for Amazon RDS instances	235	27	208	11.48
	Ensure that detailed monitoring is enabled for EC2 instances	659	40	619	6.069
	Ensure CloudTrail logging is enabled	54	54	0	100.0
	Ensure VPC flow logging is enabled in all VPCs	439	15	424	3.416
IP Address binding	Ensure no security groups allow ingress from 0.0.0.0:0 to port 22	3338	3007	331	90.08
	Ensure no security groups allow ingress from 0.0.0.0:0 to port 3389	3339	3251	88	97.36
	Ensure Amazon EKS public endpoint not accessible to 0.0.0.0/0	42	3	39	7.142
	EC2 instance should not have public IP.	768	605	163	78.77
	Ensure AWS EKS node group does not have implicit SSH access from 0.0.0.0/0	41	39	2	95.12

continued on the next page

Table A.1 AWS: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
IP Address binding	Ensure VPC subnets do not assign public IP by default	934	688	246	73.66
	Ensure no NACL allow ingress from 0.0.0.0:0 to port 21	224	151	73	67.41
	Ensure no NACL allow ingress from 0.0.0.0:0 to port 20	224	151	73	67.41
	Ensure no NACL allow ingress from 0.0.0.0:0 to port 3389	224	151	73	67.41
	Ensure no NACL allow ingress from 0.0.0.0:0 to port 22	224	148	76	66.07
	Ensure no security groups allow ingress from 0.0.0.0:0 to port 80	3339	3048	291	91.28
	Ensure that all NACL are attached to subnets	69	21	48	30.43
Hard-coded secret	Ensure no hard coded AWS access key and secret key exists in provider	2825	2810	15	99.46
	Ensure no hard-coded secrets exist in lambda environment	616	615	1	99.83
	Ensure no hard-coded secrets exist in EC2 user data	660	659	1	99.84
	Ensure EKS Cluster has Secrets Encryption Enabled	42	2	40	4.761
Outdated feature	Ensure Instance Metadata Service Version 1 is not enabled	963	48	915	4.984
	Ensure MQBroker version is current	24	6	18	25.0
	Ensure DB instance gets all minor upgrades automatically	236	65	171	27.54
	Ensure that RDS PostgreSQL instances use a non vulnerable version with the log_fdw extension	31	10	21	32.25

APPENDIX B FULL LIST OF THE SELECTED AND CATEGORIZED AZURE POLICIES WITH RESULTS

Table B.1 Azure: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
Access policy	Ensure Azure Instance does not use basic authentication(Use SSH Key Instead)	121	74	47	61.15
	Ensure that RDP access is restricted from the internet	445	426	19	95.73
	Ensure that SSH access is restricted from the internet	447	399	48	89.26
	Ensure that 'Public access level' is set to Private for blob containers	113	94	19	83.18
	Ensure 'public network access enabled' is set to 'False' for MariaDB servers	4	1	3	25.0
	Ensure Azure linux scale set does not use basic authentication(Use SSH Key Instead)	20	0	20	0.0
	Ensure 'public network access enabled' is set to 'False' for mySQL servers	7	4	3	57.14
	Ensure that Storage accounts disallow public access	236	1	235	0.423
	Ensure that PostgreSQL server disables public network access	8	3	5	37.5
	Ensure that UDP Services are restricted from the Internet	447	446	1	99.77
	Ensure that Azure Cache for Redis disables public network access	24	3	21	12.5

continued on the next page

Table B.1 Azure: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	Policies	Nb of checks	Nb pass	Nb fail	Pass Rate%
Access policy	Ensure that Azure Cosmos DB disables public network access	18	4	14	22.22
	Ensure that Azure Data factory public network access is disabled	7	5	2	71.42
	Ensure that Azure Event Grid Domain public network access is disabled	2	1	1	50.0
	Ensure that Azure IoT Hub disables public network access	2	2	0	100.0
	Ensure that SQL server disables public network access	20	2	18	10.0
	Ensure that Application Gateway enables WAF	29	11	18	37.93
	Ensure that Azure Front Door enables WAF	5	4	1	80.0
	Ensure that Azure Cognitive Search disables public network access	1	1	0	100.0
	Ensure ACR set to disable public networking	40	6	34	15.0
	Ensure that HTTP (port 80) access is restricted from the internet	445	416	29	93.48
	Ensures Spring Cloud API Portal Public Access Is Disabled	0	0	0	
	Ensure 'public network access enabled' is set to 'False' for Azure Service Bus	10	2	8	20.0
	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled	3	3	0	100.0
	Ensure the storage container storing the activity logs is not publicly accessible	115	113	2	98.26
Admin by default	Ensure ACR admin account is disabled	40	21	19	52.5
	Ensure AKS local admin account is disabled	56	10	46	17.85
Encryption at rest	Ensure Azure managed disk has encryption enabled	37	35	2	94.59
	Ensure that Automation account variables are encrypted	0	0	0	
	Ensure that Azure Data Explorer (Kusto) uses disk encryption	3	0	3	0.0

continued on the next page

Table B.1 Azure: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
Encryption at rest	Ensure that managed disks use a specific set of disk encryption sets for the customer-managed key encryption	37	2	35	5.405
	Ensure that MySQL server enables infrastructure encryption	8	1	7	12.5
	Ensure that Virtual machine scale sets have encryption at host enabled	22	0	22	0.0
	Ensure that Data Lake Store accounts enables encryption	0	0	0	
	Ensure that AKS uses disk encryption set	57	1	56	1.754
	Ensure that PostgreSQL server enables infrastructure encryption	9	0	9	0.0
	Ensure Windows VM enables encryption	45	0	45	0.0
	Ensure storage for critical data are encrypted with Customer Managed Key	241	0	241	0.0
	Ensure that Unattached disks are encrypted	51	51	0	100.0
	Ensure that Azure data factories are encrypted with a customer-managed key	8	0	8	0.0
	Ensure that MySQL server enables customer-managed key for encryption	9	0	9	0.0
	Ensure that PostgreSQL server enables customer-managed key for encryption	0	0	0	
	Ensure that Storage Accounts use customer-managed key for encryption	241	0	241	0.0
Encryption in transit	Ensure that 'enable_https_traffic_only' is enabled	234	232	2	99.14
	Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service	72	23	49	31.94
	Ensure 'Enforce SSL connection' is set to 'ENABLED' for MySQL Database Server	8	6	2	75.0

continued on the next page

Table B.1 Azure: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
Encryption in transit	Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server	9	7	2	77.77
	Ensure 'Enforce SSL connection' is set to 'ENABLED' for MariaDB servers	3	2	1	66.66
	Ensure that Function apps is only accessible over HTTPS	2	1	1	50.0
	Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service Slot	1	1	0	100.0
	Ensures Spring Cloud API Portal is enabled on for HTTPS	0	0	0	
	Ensure linux VM enables SSH with keys for secure communication	94	72	22	76.59
	Ensure the Azure CDN disables the HTTP endpoint	7	5	2	71.42
	Ensure the Azure CDN enables the HTTPS endpoint	7	7	0	100.0
	Ensure web app is using the latest version of TLS encryption	72	71	1	98.61
	Ensure Storage Account is using the latest version of TLS encryption	236	61	175	25.84
	Ensure MSSQL is using the latest version of TLS encryption	23	6	17	26.08
	Ensure MySQL is using the latest version of TLS encryption	8	6	2	75.0
	Ensure Function app is using the latest version of TLS encryption	2	2	0	100.0
	Ensure PostgreSQL is using the latest version of TLS encryption	9	5	4	55.55
	Ensure Redis Cache is using the latest version of TLS encryption	23	11	12	47.82
	Ensure the App service slot is using the latest version of TLS encryption	1	1	0	100.0
	Ensure the Azure CDN endpoint is using the latest version of TLS encryption	3	3	0	100.0
	Ensure Azure Service Bus is using the latest version of TLS encryption	10	0	10	0.0

continued on the next page

Table B.1 Azure: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
Hard-coded secret	Ensure that no sensitive credentials are exposed in VM custom_data	47	47	0	100.0
IP Address binding	Ensure no SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	10	10	0	100.0
	Ensure that Network Interfaces disable IP forwarding	180	157	23	87.22
	Ensure that Network Interfaces don't use public IPs	181	78	103	43.09
	Ensure AKS cluster nodes do not have public IP addresses	57	57	0	100.0
Logging/Monitoring	Ensure AKS logging to Azure Monitoring is Configured	57	26	31	45.61
	Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server	7	7	0	100.0
	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server	7	7	0	100.0
	Ensure Storage logging is enabled for Queue service for read write and delete requests	229	23	206	10.04
	Ensure server parameter 'log_retention' is set to 'ON' for PostgreSQL Database Server	7	7	0	100.0
	Ensure default Auditing policy for a SQL Server is configured to capture and retain the activity logs	4	1	3	25.0
	Ensure function app builtin logging is enabled	4	2	2	50.0
	Ensure Storage logging is enabled for Table service for read requests	20	0	20	0.0
	Ensure Storage logging is enabled for Blob service for read requests	117	0	117	0.0

continued on the next page

Table B.1 Azure: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
Outdated feature	Ensure that 'HTTP Version' is the latest if used to run the web app	72	11	61	15.27
	Ensure that 'Net Framework' version is the latest if used as a part of the web app	20	0	20	0.0
	Ensure that 'PHP version' is the latest if used to run the web app	20	19	1	95.0
	Ensure that 'Python version' is the latest if used to run the web app	20	19	1	95.0
	Ensure that 'Java version' is the latest if used to run the web app	20	19	1	95.0
	Ensure Windows VM enables automatic updates	49	5	44	10.20

APPENDIX C FULL LIST OF THE SELECTED AND CATEGORIZED GCP POLICIES WITH RESULTS

Table C.1 GCP: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
Logging/Monitoring	Ensure Stackdriver Logging is set to Enabled on Kubernetes Engine Clusters	310	305	5	98.38
	Ensure Stackdriver Monitoring is set to Enabled on Kubernetes Engine Clusters	310	307	3	99.03
	Ensure that VPC Flow Logs is enabled for every subnet in a VPC Network	585	93	492	15.89
	Ensure PostgreSQL database ’log_checkpoints’ flag is set to ’on’	105	10	95	9.523
	Ensure PostgreSQL database ’log_connections’ flag is set to ’on’	105	15	90	14.28
	Ensure PostgreSQL database ’log_disconnections’ flag is set to ’on’	105	13	92	12.38
	Ensure PostgreSQL database ’log_lock_waits’ flag is set to ’on’	105	15	90	14.28
	Ensure PostgreSQL database ’log_min_messages’ flag is set to a valid value	105	89	16	84.76
	Ensure PostgreSQL database ’log_temp_files flag is set to ’0’	105	88	17	83.80
	Ensure PostgreSQL database ’log_min_duration_statement’ flag is set to ’-1’	105	84	21	80.0

continued on the next page

Table C.1 GCP: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
Logging/Monitoring	Enable VPC Flow Logs and Intranode Visibility	310	2	308	0.645
	Bucket should log access	586	69	517	11.77
	Bucket should not log to itself	69	69	0	100.0
	Ensure Datafusion has stack driver logging enabled	15	5	10	33.33
	Ensure Datafusion has stack driver monitoring enabled	15	5	10	33.33
	Ensure hostnames are logged for GCP PostgreSQL databases	105	0	105	0.0
	Ensure the GCP PostgreSQL database log levels are set to ERROR or lower	105	1	104	0.952
	Ensure GCP PostgreSQL logs SQL statements	105	0	105	0.0
	Ensure PostgreSQL database flag 'log_duration' is set to 'on'	235	128	107	54.46
	Ensure PostgreSQL database flag 'log_executor_stats' is set to 'off'	243	243	0	100.0
	Ensure PostgreSQL database flag 'log_parser_stats' is set to 'off'	243	243	0	100.0
	Ensure PostgreSQL database flag 'log_planner_stats' is set to 'off'	243	243	0	100.0
	Ensure PostgreSQL database flag 'log_statement_stats' is set to 'off'	243	243	0	100.0
Access policy	Ensure Google compute firewall ingress does not allow unrestricted ssh access	1018	913	105	89.68
	Ensure Google compute firewall ingress does not allow unrestricted rdp access	1018	990	28	97.24
	Ensure that Cloud SQL database Instances are not open to the world	239	235	4	98.32
	Ensure that BigQuery datasets are not anonymously or publicly accessible	141	136	5	96.45
	Ensure that DNSSEC is enabled for Cloud DNS	55	11	44	20.0
	Ensure GKE Control Plane is not public	310	304	6	98.06
	Ensure GKE basic auth is disabled	310	305	5	98.38

continued on the next page

Table C.1 GCP: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
Access policy	Ensure Kubernetes Cluster is created with Private cluster enabled	310	71	239	22.90
	Ensure that Cloud Storage bucket is not anonymously or publicly accessible	729	696	33	95.47
	Ensure that Cloud Storage buckets have uniform bucket-level access enabled	583	291	292	49.91
	Ensure clusters are created with Private Nodes	310	71	239	22.90
	Ensure Google compute firewall ingress does not allow unrestricted FTP access	1018	1005	13	98.72
	🟥 Ensure that Private google access is enabled for IPV6	593	2	591	0.337
	Ensure Cloud build workers are private	6	2	4	33.33
	Ensure Data fusion instances are private	15	4	11	26.66
	Ensure Google compute firewall ingress does not allow unrestricted mysql access	1018	999	19	98.13
	Ensure Vertex AI instances are private	23	4	19	17.39
	Ensure Dataflow jobs are private	10	1	9	10.0
	Ensure that Dataproc clusters are not anonymously or publicly accessible	14	8	6	57.14
	Ensure that Pub/Sub Topics are not anonymously or publicly accessible	298	292	6	97.98
	Ensure that BigQuery Tables are not anonymously or publicly accessible	12	6	6	50.0
	Ensure that Artifact Registry repositories are not anonymously or publicly accessible	51	43	8	84.31
	Ensure that GCP Cloud Run services are not anonymously or publicly accessible	65	30	35	46.15
	Cloud functions should not be public	19	9	10	47.36

continued on the next page

Table C.1 GCP: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	Policies	Nb of checks	Nb pass	Nb fail	Pass Rate%
Access policy	Esnure KMS policy should not allow public access	161	161	0	100.0
	Ensure IAM policy should not define public access	140	101	39	72.14
	Ensure public access prevention is enforced on Cloud Storage bucket	586	7	579	1.194
	Ensure that Cloud KMS cryptokeys are not anonymously or publicly accessible	36	34	2	94.44
	Ensure that Cloud KMS Key Rings are not anonymously or publicly accessible	34	28	6	82.35
	Ensure that Container Registry repositories are not anonymously or publicly accessible	12	12	0	100.0
	Ensure GCP network defines a firewall and does not use the default firewall	460	178	282	38.69
Encryption in transit	Ensure all Cloud SQL database instance requires all incoming connections to use SSL	239	9	230	3.765
	Ensure 'Block Project-wide SSH keys' is enabled for VM instances	535	17	518	3.177
	Ensure Memorystore for Redis uses intransit encryption	18	2	16	11.11
IP Address binding	Ensure Kubernetes Cluster is created with Alias IP ranges enabled	310	125	185	40.32
	Ensure that IP forwarding is not enabled on Instances	530	471	59	88.86
	Ensure that Compute instances do not have public IP addresses	543	200	343	36.83
	Ensure Cloud SQL database does not have public IP	239	196	43	82.00
	Ensure that private_ip_google_access is enabled for Subnet	597	93	504	15.57
	Ensure Dataproc Clusters do not have public IPs	19	4	15	21.05
	Ensure Google compute firewall ingress does not allow unrestricted http port 80 access	1018	938	80	92.14

continued on the next page

Table C.1 GCP: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
Admin by default	Ensure that instances are not configured to use the default service account with full access to all Cloud APIs	517	512	5	99.03
	Ensure that Service Account has no Admin privileges	2043	2032	11	99.46
	Ensure no roles that enable to impersonate and manage all service accounts are used at a folder level	280	268	12	95.71
	Ensure no roles that enable to impersonate and manage all service accounts are used at an organization level	217	207	10	95.39
	Ensure that a MySQL database instance does not allow anyone to connect with administrative privileges	218	216	2	99.08
Encryption at rest	Ensure VM disks for critical VMs are encrypted with Customer Supplied Encryption Keys (CSEK)	185	64	121	34.59
	Ensure VM disks for critical VMs are encrypted with Customer Supplied Encryption Keys (CSEK)	425	65	360	15.29
	Ensure Big Query Tables are encrypted with Customer Supplied Encryption Keys (CSEK)	464	25	439	5.387
	Ensure Big Query Datasets are encrypted with Customer Supplied Encryption Keys (CSEK)	141	28	113	19.85
	Ensure PubSub Topics are encrypted with Customer Supplied Encryption Keys (CSEK)	183	14	169	7.650
	Ensure Artifact Registry Repositories are encrypted with Customer Supplied Encryption Keys (CSEK)	63	2	61	3.174
	Ensure Big Table Instances are encrypted with Customer Supplied Encryption Keys (CSEK)	10	1	9	10.0

continued on the next page

Table C.1 GCP: Full list of the selected and categorized policies, 5 Best/Worst Performing Policies With Over 50 Checks Highlighted in Green/Red – continued from previous page

Category	**Policies**	**Nb of checks**	**Nb pass**	**Nb fail**	**Pass Rate%**
Encryption at rest	Ensure data flow jobs are encrypted with Customer Supplied Encryption Keys (CSEK)	10	1	9	10.0
	Ensure Dataproc cluster is encrypted with Customer Supplied Encryption Keys (CSEK)	19	3	16	15.78
	Ensure Vertex AI datasets uses a CMK (Customer Manager Key)	8	1	7	12.5
	Ensure Spanner Database is encrypted with Customer Supplied Encryption Keys (CSEK)	7	2	5	28.57
	Ensure Vertex AI Metadata Store uses a CMK (Customer Manager Key)	7	4	3	57.14
Outdated feature	Ensure SQL database is using latest Major version	231	102	129	44.15