2023 VMware Tanzu Hub Governance Policy Release Notes

VMware Tanzu Hub 2023

vmware by Broadcom

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://docs.vmware.com/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to https://www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. Copyright and trademark information.

Contents

Introduction

1

You can review this page for about information on new additions or updates to the governance policies in VMware Tanzu Hub. Security posture policy updates also apply to VMware Aria Automation for Secure Clouds, where they are referred to as rules. If you arrived at this page from the VMware Aria Automation for Secure Clouds documentation, you can return to the landing page for that product.

November 28, 2023 Policy Release

2

Read the following topics next:

- Deprecated Compliance Frameworks

Deprecated Compliance Frameworks

The following frameworks are deprecated:

- MITRE ATT&CK Cloud, version 10.0
- MITRE ATT&CK Cloud, version 11.0
- MITRE ATT&CK Containers, version 10.0
- MITRE ATT&CK Containers, version 11.0

Per the compliance lifecycle, only the two latest versions of a compliance framework are supported at any given time. When a framework is deprecated, users can either switch to a newer version or create a custom framework to maintain the deprecated one.

November 16, 2023 Policy Release

3

Read the following topics next:

- Deprecated Compliance Framework

Deprecated Compliance Framework

The following framework is deprecated:

- CIS AWS Foundations Benchmark, version 1.4.0

Per the compliance lifecycle, only the two latest versions of a compliance framework are supported at any given time. When a framework is deprecated, users can either switch to a newer version or create a custom framework to maintain the deprecated one.

October 18, 2023 Policy Release

4

Read the following topics next:

Updated AWS Security Posture Policies

The following policies received a query change to increase the accuracy of finding results:

- Systems Manager managed instance patch should be in compliant status (RuleId: 993ece60-6a4e-497e-bf04-ad65dc9b8543) - Medium
- Systems Manager managed instance association should be in compliant status (RuleId: bc8f3ffa-09d8-4465-80b6-068ebba38a31) - Low

October 12, 2023 Policy Release

5

Read the following topics next:

- New Azure Secure Posture Policies

New Azure Secure Posture Policies

- AppService remote debugging should be turned off (RuleId: d53fcbc5-709b-449d-bb92-5692f52f6079) - Medium
- Virtual machine should have IaaSAntimalware security extension enabled (RuleId: 24a0760d-991f-4439-910a-65a4f8dfc35c) - Medium
- Virtual machine should have monitoring extension enabled (RuleId: c13a7d62-579c-478a-b500-13209eea1140) - Medium
- Virtual machine should have system identity assigned (RuleId: 5910a49f-f3bc-4da3-9226-4e3720018f64) - Medium

September 27, 2023 Policy Release

6

Read the following topics next:

Updated Compliance Framework

The following framework had a control mapping corrected from 1.18 to 1.17 for a rule (IAM role for customer support should be created):

- CIS AWS Foundations Benchmark, version 1.5.0.

September 21, 2023 Policy Release

7

Read the following topics next:

New AWS Security Posture Policy

- DocumentDB cluster should have log exports to CloudWatch enabled (RuleId: 9425b8d1-d37c-4267-95cd-146a0537ee49) - Low

New Azure AD Security Posture Policies

- Active Directory tenant should have an authorization policy that prevents users from creating new tenants (RuleId: ee476fe9-b788-4b08-8b7e-fd9cf529de09) - High
- Active Directory tenant should have an authorization policy that prevents users from creating security groups (RuleId: 16821389-8d2a-46d2-ac3c-d3e6fd9dbaa5) - High
- Active Directory tenant should have an authorization policy that prevents users from registering apps (RuleId: 90644939-fbf9-4ca0-97f0-c97d6ff7f29b) - High

New Compliance Framework

- CIS AWS Foundations Benchmark, version 2.0.0

Deprecated Compliance Frameworks

The following frameworks are deprecated:

- CIS Kubernetes V1.20 Benchmark, version 1.0.0
- CIS Kubernetes V1.23 Benchmark, version 1.0.0
- CIS Microsoft Azure Foundations Benchmark, version 1.4.0

- CIS Google Kubernetes Engine (GKE) Benchmark, version 1.0.0

Per the compliance lifecycle, only the two latest versions of a compliance framework are supported at any given time. When a framework is deprecated, users can either switch to a newer version or create a custom framework to maintain the deprecated one.

September 7, 2023 Policy Release

8

Read the following topics next:

- New AWS Security Posture Policies
- Updated AWS Security Posture Policy

New AWS Security Posture Policies

- CloudWatch log group retention period should be greater than 30 days (RuleId: a9fb2106-4e45-4dd0-80d2-22e890afc3ad) - High
- S3 bucket should have object lock enabled (RuleId: 26904364-7d42-4547-bda6-2714ec830168) - High
- EC2 instance should be managed by SSM agent (RuleId: 6a0c61e6-f839-4ac3-84c8-5c66fd164288) - Medium
- ECS container in task definition should be limited to read-only access for root filesystems (RuleId: 89ab3c33-943b-47e2-b1b2-ba0455faaa4d) - Medium
- ElastiCache automatic backup should be enabled (RuleId: ecae40d7-d66a-4586-a002-097f33d49316) - Medium
- RDS DB instance should have CloudWatch enabled (RuleId:28460d18-93eb-4279-9d60-2b4cb062cac8) - Medium
- EBS volume should be attached to EC2 instance (RuleId: 5f675da4-9665-4fa8-83e2-7f9ee3db08fc) - Low
- EC2 Elastic IP address should be attached (RuleId: 54e320d0-dc3e-4961-a408-aeac87e3c6cc) - Low
- EC2 instance should have EBS volume optimization enabled (RuleId: 2dd99cae-2d81-4ae7-b802-819ef024c6a9) - Low

Updated AWS Security Posture Policy

The following policy received a query change to increase the accuracy of finding results:

- Redshift engine automatic upgrades should be enabled (RuleId: 5c8c264f7a550e1fb6560c54) - Low

August 31, 2023 Policy Release

9

Read the following topics next:

Updated AWS Security Posture Policy

The following policy received a SSQL conversion:

- Secrets Manager secret should be rotated within a specified number of days (RuleId-3d7322ca-c748-4106-bdfa-0ee89de73914) - Medium

Changing policy queries from Gremlin to SSQL provides greater transparency into what a policy is specifically checking for and also enables customers to more easily use queries to create explore searches and custom policies. SSQL queries will eventually be added to the policies page, but in meantime you can review them in the change log for a specific policy.

August 21, 2023 Policy Release

10

Read the following topics next:

- Updated Azure Security Posture Policies
- New Compliance Frameworks

Updated Azure Security Posture Policies

The following rules received query updates to align with ongoing changes to how the region for an Azure entity is checked on system scan, ensuring they continue to report findings correctly:

- Activity log should generate an alert for delete policy assignment events (RuleId: e26607e4-2b03-49d2-bfc2-f0412dee3b22) - Medium
- Create or Update Network Security Group event should generate an alert (RuleId: 5c8c26697a550e1fb6560c74) - Medium
- Create or Update Security Solution event should generate an alert (RuleId: 5c8c266b7a550e1fb6560c78) - Medium
- Create or Update SQL Server Firewall Rule event should generate an alert (RuleId: 5c8c266b7a550e1fb6560c7a) - Medium
- Create Policy Assignment event should generate an alert (RuleId: 5c8c266c7a550e1fb6560c7b) - Medium
- Delete Network Security Group event should generate an alert (RuleId: 5c8c266d7a550e1fb6560c7d) - Medium
- Delete Network Security Group Rule event should generate an alert (RuleId: 5c8c266e7a550e1fb6560c7f) - Medium
- Delete Security Solution event should generate an alert (RuleId: 5c8c266e7a550e1fb6560c81) - Medium
- Delete SQL Firewall Rule event should generate an alert (RuleId: 5c8c26717a550e1fb6560c83) - Medium
- Update Network Security Group Rule event should generate an alert (RuleId: 5c8c266a7a550e1fb6560c76) - Medium

- Update Security Policy event should generate an alert (RuleId: 5c8c26717a550e1fb6560c85) - Medium

New Compliance Frameworks

The following frameworks were mapped to controls for AWS, Azure,GCP, and Kubernetes policies for the first time:

- MITRE ATT&CK Cloud, version 12
- MITRE ATT&CK Cloud, version 13
- MITRE ATT&CK Containers, version 12
- MITRE ATT&CK Containers, version 13

Per the compliance lifecycle, only the two latest versions of a compliance framework are supported at any given time. When a framework is deprecated, users can either switch to a newer version or create a custom framework to maintain the deprecated one.

August 10, 2023 Policy Release

11

Read the following topics next:

- Updated Azure Security Posture Policy
- New Azure Security Posture Policy
- New Azure AD Security Posture Policies

Updated Azure Security Posture Policy

The following policy received a KB change:

- Custom role should not grant permissions equal to owner role (RuleId: 4c6b3141-3f25-4247-8540-8214326f9b19) - Low

New Azure Security Posture Policy

- Custom role should be created to have full resource lock permissions (RuleId: 802cef95-daad-4706-8228-5b4528c45ead) - Medium

New Azure AD Security Posture Policies

- Azure Active Directory user should have MFA enabled (RuleId: ae98266b-658b-4b35-a921-ef217451e4e7) - High
- Azure AD Conditional Access policy should include an exclusionary geographic access policy (RuleId: 12520f19-8e08-4965-a4d6-6d68c7ead51c) - High
- Azure AD tenant should have authorization policy that enforces strict guest permission restrictions (RuleId: 04782266-d857-4767-8b94-a8a828376bc3) - High
- Azure AD tenant should have authorization policy that limits the permission to invite guest users (RuleId: 68d992e8-6ece-4a64-b53e-bcc1fca7997b) - High
- Azure AD tenant should have conditional access policy requiring MFA for all risky sign-ins (RuleId: 55015749-1301-41ef-99ae-03592798e208) - High
- Azure AD tenant should have security defaults enabled (RuleId: a78813dd-ab5a-452b-b532-d69878cb6d1e) - High

- Azure AD Conditional Access policy should list Trusted Locations (RuleId: 469196f2-c61b-46d9-9673-e27641be679c) - Medium
- Azure AD tenant should have conditional access policy requiring MFA (RuleId: 260a4845-9b28-481d-8f50-03f93b908a13) - Medium

July 27, 2023 Policy Release

12

Read the following topics next:

- New AWS Security Posture Policies

New AWS Security Posture Policies

- FSx file system should be encrypted with a customer managed key (RuleId: 5082c609-e763-4ae3-86fd-26f98feee05b) - Medium
- FSx file system should have automatic backups enabled (RuleId: b02d28a2-894e-4ce0-9259-1f681ca95363) - Medium
- FSx for Lustre file system should have logging enabled (RulelD: 6e1ed4f4-85a1-44dd-aaa0-b581c9225820) - Low
- FSx for Windows File Server file system should have audit logging enabled (RuleId: d0e431ea-7c5b-4892-9d00-7405bbec1017) - Low

July 21, 2023 Policy Release

13

Read the following topics next:

- New AWS Security Posture Policies
- New Azure Security Posture Policy
- Updated AWS Security Posture Policy
- New Compliance Frameworks

New AWS Security Posture Policies

- DocumentDB cluster should be encrypted using customer managed key (RuleId: 71a34b4b-984c-4a86-810c-57016e36bebc) - High
- DocumentDB cluster should have encryption enabled (RuleId: 11390bea-0b54-4997-9831-96c3da024923) – High
- DocumentDB snapshot should have encryption enabled (RuleId: ad20b451-d780-4cd8-a5d3-361529c463ac) – High
- DocumentDB cluster backup retention period should be greater than or equal to 30 days (RuleId: 1d336634-43c4-43bd-8b91-282d6a4c142e) - Low
- DocumentDB cluster should not have deletion protection disabled (RuleId: 89f1e1b0-bb33-42ff-8ecf-68146c13d8cd) - Low
- DocumentDB cluster should not use a database engine default port (RuleId: f5f42879-f5f6-4658-b457-d2d0c25550fb) - Low
- DocumentDB event notifications subscription should be configured for critical cluster events (RuleId: beb0af93-7836-4efc-843a-183c41d570cd) - Low
- DocumentDB event notifications subscription should be configured for critical database instance events (RuleId: ee5f739e-a663-49b8-b962-125d42cb0922) - Low
- DocumentDB event notifications subscription should be configured for critical database parameter group events (RuleId: 39b494cd-bb7c-4f4d-89dd-2e1c96f5cb73) - Low
- DocumentDB event notifications subscription should be configured for critical database security group events (RuleId: 61293976-e499-4c15-90cb-58d9d939fd74) – Low

New Azure Security Posture Policy

- Network resources should not have basic SKUs in production environments (RuleId: 250612e1-9f02-41fc-968d-cd77bb327a07) - High

Updated AWS Security Posture Policy

The following policy received changes in query:

- RDS DB instance should not have password authentication enabled (RuleId: 5d488bda-4f6f-4f0d-a37b-935941641130) - Medium

New Compliance Frameworks

The following compliance frameworks were added for the first time:

- CIS Azure Kubernetes Service (AKS) Benchmark, version 1.3.0
- CIS Amazon Elastic Kubernetes Service (EKS) Benchmark, version 1.3.0
- CIS Google Kubernetes Engine (GKE) Benchmark, version 1.4.0
- CIS Kubernetes V1.24 Benchmark, version 1.0.0
- CIS Kubernetes V1.25 Benchmark, version 1.7.1
- CIS Azure Foundations Benchmark, version 2.0.0

Per the compliance lifecycle, only the two latest versions of a compliance framework are supported at any given time. When a framework is deprecated, users can either switch to a newer version or create a custom framework to maintain the deprecated one.

July 6, 2023 Policy Release

14

Read the following topics next:

- Updated AWS Security Posture Policy

Updated AWS Security Posture Policy

Improved policy to account for undocumented RDS Domain Membership states. The update will reduce false positive findings.

- RDS DB instance should not have password authentication enabled (RuleId: 5d488bda-4f6f-4f0d-a37b-935941641130) - Medium

June 22, 2023 Policy Release

15

Read the following topics next:

Updated AWS Security Posture Policy

The following policy received changes in remediation steps:

- Organization service control policy should restrict access to all services when attached to other resources (RuleId: ea804e4b-edd3-4282-9e40-173ac9267b19) - Medium

June 16, 2023 Policy Release

16

Read the following topics next:

- New AWS Security Posture Policies
- Updated AWS Security Posture Policies
- Updated GCP Security Posture Policy
- New Compliance Framework

New AWS Security Posture Policies

- IAM role used by VMware Aria should not have extraneous permissions or limitations in the attached IAM policies (RuleId: e8c3b12f-082f-4a56-add3-cd10ef83a67e) - High
- IAM role used by VMware Aria should not have extraneous policy statements in the associated trust policy (RuleId: f42b12fe-c0e3-4c23-9932-83e6247cc966) - High

Updated AWS Security Posture Policies

The following policies received changes in query:

- S3 bucket should allow only HTTPS requests (RuleId: 688d093c-3b8d-11eb-adc1-0242ac120002) - High
- KMS should have automated key rotation enabled (RuleId: 5c8c26217a550e1fb6560c12) - Medium
- RDS database cluster should use a custom administrator username (RuleId: ddd1ffc2-938d-440b-bf10-d09c641c3ce7) - Medium
- S3 bucket should have object level logging enabled for read events (RuleId: dc981b20-3ea6-11eb-b378-0242ac130002) - Low
- S3 bucket should have object level logging enabled for write events (RuleId: 45a4ef9e-3eac-11eb-b378-0242ac130002) - Low

The following policy received changes in query and trigger:

- RDS DB instance should not have password authentication enabled (RuleId: 5d488bda-4f6f-4f0d-a37b-935941641130) - Medium

Updated GCP Security Posture Policy

The following policy received changes in display name, description, and query:

- VM instance should not use a default service account with unrestricted Cloud API access (RuleId: f03bd4a2-f1e7-11ea-adc1-0242ac120002) - High

New Compliance Framework

The following framework received mappings for the first time to AWS, Azure, GCP, and Kubernetes policies:

- FedRAMP

April 27, 2023 Policy Release 17

Read the following topics next:

- Updated AWS Security Posture Policies
- Deprecated Compliance Framework

Updated AWS Security Posture Policies

The following policies received query updates:

- Redshift cluster should require SSL connections (RuleId: 5c8c264c7a550e1fb6560c51) - High
- S3 bucket should have object level logging enabled for read events (RuleId: dc981b20-3ea6-11eb-b378-0242ac130002) - Low
- S3 bucket should have object level logging enabled for write events (RuleId: 45a4ef9e-3eac-11eb-b378-0242ac130002) - Low

The following policy received query and KB updates:

- Redshift cluster should have user activity logging enabled (RuleId: 5c8c264d7a550e1fb6560c53) - Low

Deprecated Compliance Framework

The following framework is deprecated:

- CIS GCP Foundations Benchmark, version 1.2.0

Per the compliance lifecycle, only the two latest versions of a compliance framework are supported at any given time. When a framework is deprecated, users can either switch to a newer version or create a custom framework to maintain the deprecated one.

April 20, 2023 Policy Release

18

Read the following topics next:

- Updated AWS Security Posture Policy

Updated AWS Security Posture Policy

The following policy received KB updates:

- CloudTrail event for network access control list changes should have alarm configured (RuleId: 5c8c262e7a550e1fb6560c25) - High

April 6, 2023 Policy Release

19

Read the following topics next:

- Updated AWS Security Posture Policies

Updated AWS Security Posture Policies

The following policy received changes in query:

- Unused network access control lists should be removed (RuleId: 9b6fdd1a-1b2a-4180-8e01-b75a658ef77d) - Low

The following policy received changes in description:

- EC2 VPC default security group should restrict all access (RuleId: 5c8c25f37a550e1fb6560bca) - Medium

March 24, 2023 Policy Release 20

Read the following topics next:

- New GCP Security Posture Policies
- Updated AWS Security Posture Policies
- Updated GCP Security Posture Policies
- New Compliance Framework

New GCP Security Posture Policies

- IAM user should not have Service Account Admin and Service Account User roles assigned together (RuleId: fed8c3d8-6828-445f-ae35-e14ead6b69da) - High
- IAM user should not have the Cloud KMS Admin role assigned together with the Cloud KMS CryptoKey Encrypter/Decrypter, Cloud KMS CryptoKey Encrypter, or Cloud KMS CryptoKey Decrypter roles (RuleId:2f05cfc2-3559-4a5d-9e07-8472f5065315) - High
- API key should be rotated every 90 days (RuleId: 02124bf7-03ee-4b9d-8c93-749fc3d7a6b4) - Medium
- API key usage should be restricted to APIs the application needs to access (RuleId: 804c9d6b-c7c0-4ff0-a120-9706a137d4f2) - Medium
- API key usage should be restricted to specific hosts and applications (RuleId: cc0ea365-10b1-40ca-ae0d-bb63fd01a50a) - Medium
- BigQuery data set should be encrypted with customer managed encryption key (RuleId:70cb49d2-35ee-4e2c-851a-0b06d5c310e8) - Medium
- Dataproc cluster should be encrypted using customer-managed encryption key (RuleId:1d164e3a-814e-484f-b56e-32be96b4f959) - Medium
- API key should be used only on active service (RuleId: c740729c-4d23-4a29-811c-86fe9e5be264) - Low

Updated AWS Security Posture Policies

The following policy received changes in display name:

- EC2 instance malicious domain/IP requests detected (RuleId: b56b41de-ceb7-4a66-8f4e-42a1de5daa83) - Critical

The following policies received changes in query:

- CloudTrail event for AWS Console logins without MFA should have alarm configured" (RuleId: 5c8c262a7a550e1fb6560c21) – Medium
- CloudTrail event for CloudTrail configuration changes should have alarm configured (RuleId: 5c8c26237a550e1fb6560c16) – Medium
- CloudTrail event for customer master key deletion events should have alarm configured (RuleId: 5c8c26287a550e1fb6560c1d) - Medium
- CloudTrail event for failed AWS Console login attempts should have alarm configured (RuleId: 5c8c26287a550e1fb6560c1f) – Medium
- CloudTrail event for security group configuration changes should have alarm configured (RuleId: 5c8c26367a550e1fb6560c2f) - Medium
- CloudTrail event for unauthorized API access attempts should have alarm configured (RuleId: 5c8c26377a550e1fb6560c30) - Medium
- CloudWatch monitoring should be configured for any changes in AWS Config settings (RuleId: 64334788-3bc0-11eb-adc1-0242ac120002) - Low
- CloudWatch monitoring should be configured for any changes in AWS organizations (RuleId: ba73fb7e-3bc5-11eb-adc1-0242ac120002) – Low
- VPC flow logs should be enabled (RuleId: 5c8c25f97a550e1fb6560bd4) - Low

Updated GCP Security Posture Policies

The following policy received changes in display name, description, and suggested action:

- BigQuery Table should be encrypted with customer managed encryption key (RuleId: 8779a3b1-4012-44c6-a8de-50d79f89021c) - Medium

The following policies received changes in rule name, display name, suggested action, query and remediation steps:

- Container scanning should be enabled (RuleId: b11f699a-f1fc-4717-b375-7b8be52ba6f5) - Medium
- Cloud asset inventory should be enabled (RuleId: f7fd5738-991b-4697-b0a3-d5731608415c) - Low

New Compliance Framework

The following framework received mappings for the first time to GCP policies:

- CIS GCP Foundations Benchmark, version 2.0.0

March 16, 2023 Policy Release 21

Read the following topics next:

- Updated AWS Security Posture Policies
- Updated Azure Security Posture Policies
- Updated GCP Security Posture Policies

Updated AWS Security Posture Policies

The following policy queries have SSQL conversion updates:

- Classic Load Balancer should use a current SSL policy (RuleId: 5c8c25fa7a550e1fb6560bd7) - High
- API Gateway REST API stages should be configured to use SSL certificates (RuleId: 17d1bb39-dd77-4768-a161-880b4015fa84) - Medium
- ECS Cluster execute command logging encryption should be enabled (RuleId: 6f743c71-0fbc-4710-805b-61044a204e6a) - Medium
- ECS Services should not have public IP addresses assigned to them (RuleId: 4dde3a86-0582-43ac-bca6-8fd6267c27f2) - Medium
- Elastic Beanstalk environment with Elastic Load Balancer should be configured with a secure SSL policy (RuleId: cb662c12-b017-4ce7-97fb-943f05923e28) - Medium
- Elastic Load Balancer should have access logs enabled (RuleId: 09905d97-4075-4820-afc6-ec5ada60db46) - Medium
- Elastic Load Balancer should have cross-zone load balancing enabled (RuleId: 62506173-0c0d-4772-a212-2ed1e431df93) - Medium
- Elastic Load Balancer should have delete protection enabled (RuleId: 4f9b64a1-494f-40ee-b1b5-eb4a9c13bf31) - Medium
- Elastic Load Balancer should not have invalid HTTP headers (RuleId: df70d6b1-fdca-4589-88d6-f9d08df4db0d) - Medium
- Route53 hosted zone records should be configured with health check (RuleId:3861c363-849f-4c5f-a4a3-e48465e08e81) - Medium

- API Gateway HTTP and WebSocket API stage access logging should be enabled (RuleId: 22a611c3-d1d7-48ab-8fe9-e0ced2cce14e) - Low
- API Gateway REST API execution logging should be enabled (RuleId: d95441b3-7888-4a68-87cf-63ddb8075c25) - Low
- API Gateway REST API stage access logging should be enabled (RuleId: 1873082b-e6a7-45d4-ad11-aa5ec5e9389b) - Low
- API Gateway REST API stages should have AWS X-Ray tracing enabled (RuleId: bce5cb84-0771-4ed3-bf50-abb03435e22e) - Low
- API Gateway WebSocket API stage execution logging should be enabled (RuleId: 674de938-8e6d-4557-9d96-43e1ab2b809a) - Low
- IAM users should not have policies attached (RuleId: 5c8c261b7a550e1fb6560c0c) - Low

Updated Azure Security Posture Policies

The following policy queries have SSQL conversion updates:

- Blob container should not have public read access enabled (RuleId: 5c8c26997a550e1fb6560cd9) - High
- CDN endpoint should require HTTPS connections (RuleId: fce9c690-4155-4b32-8f0c-b2599004955d) - High
- Front Door custom domain should be configured with HTTPS protocol (RuleId: 3e775bcb-b132-48be-af09-952daa1c77dd) - High
- SQL data encryption should be enabled (RuleId: 5c8c268d7a550e1fb6560cc0) - High
- Virtual machine data disk should be encrypted (RuleId: 5c8c26767a550e1fb6560c91) - High
- AKS cluster should have private node (RuleId: b500ea29-935e-4476-9318-ed7994c04854) - High
- App Service should use the latest TLS version (RuleId: b596ed28-0218-11eb-adc1-0242ac120002) - Medium
- Application Gateway should be configured with predefined TLS policy (RuleId: 58e588bd-2e29-412f-89ce-9ea66c29ffdd) - Medium
- Front Door health probe setting should be enabled (RuleId: b35eee6a-c4dc-47ec-bc1f-b31448bf22a2) - Medium
- Key Vault should be recoverable (RuleId: e2090e34-3580-4088-a815-2ead6a72700f) - Medium
- MySQL Flexible server should have the latest TLS version (RuleId: f7e6fa0f-f59b-465a-b297-b5ad3e9cefab) - Medium
- Storage account blob service should be configured with soft delete (RuleId: 643eb5fc-7747-4df4-b217-41c4e97e0c07) - Medium

- Traffic Manager endpoint status should be enabled (RuleId: a00bca8a-f41e-11ea-adc1-0242ac120002) - Medium
- PostgreSQL server should retain logs for more than 3 days (RuleId: 500b6663-2eba-4760-a0dd-6446bc2c0dac) - Low
- SQL database should have Advanced Threat Protections configured to send email notifications to admins and subscription owners (RuleId: 5c8c268e7a550e1fb6560cc2) - Low
- SQL database should retain Advanced Threat Protection logs for more than 90 days (RuleId: 5c8c26957a550e1fb6560cd0) - Low
- SQL database should have Azure Defender for SQL enabled (RuleId: 5c8c26937a550e1fb6560ccc) - Low
- SQL server should have Advanced Threat Protection configured to send email notification to admins and subscription owners (RuleId5c8c268e7a550e1fb6560cc4) - Low
- SQL server should have Azure Defender vulnerability assessments configured with an email destination for scan reports (RuleId: f039f2e4-f960-4904-83a6-7cc6c420bf8e) - Low
- WAF Application Gateway should have prevention mode enabled (RuleId: b90ede49-14ea-4b40-a3ec-bf6f7ece2b3e) - Low

Updated GCP Security Posture Policies

The following policy queries have SSQL conversion updates:

- Cloud DNS policy should log for all VPC networks (RuleId: 9d5f1432-a3e8-4b66-80dd-eab114e14c7c) - Medium
- GKE cluster container scanning should be enabled (RuleId: e3fe88da-6d0f-11eb-9439-0242ac130002) - Medium
- GKE legacy compute engine instance metadata APIs should be disabled (RuleId: ccb3d090-5c0c-11eb-ae93-0242ac130002) - Medium
- GKE cluster cloud asset inventory should be enabled (RuleId: 1ce93959-934c-4e66-a1f2-dc4498990646) - Low

Changing policy queries from Gremlin to SSQL provides greater transparency into what a policy is specifically checking for and also enables customers to more easily use queries to create explore searches and custom policies. SSQL queries will eventually be added to the policies page, but in meantime you can review them in the change log for a specific policy.

March 9, 2023 Policy Release 22

Read the following topics next:

- Updated AWS Security Posture Policies

Updated AWS Security Posture Policies

The following policies received changes in logic to use advanced event selectors instead of the default event selectors made in AWS:

- CloudTrail event for AWS Console root login attempts should have alarm configured (RuleId: 5c8c26317a550e1fb6560c29) - High
- CloudTrail event for IAM policy changes should have alarm configured (RuleId: 5c8c262c7a550e1fb6560c23) - High
- CloudTrail event for network access control list changes should have alarm configured (RuleId: 5c8c262e7a550e1fb6560c25) - High
- CloudTrail event for network gateway configuration changes should have alarm configured (RuleId: 5c8c262f7a550e1fb6560c27) - High
- CloudTrail event for routing table configuration changes should have alarm configured (RuleId: 5c8c26337a550e1fb6560c2b) - High
- CloudTrail event for S3 bucket policy changes should have alarm configured (RuleId: 5c8c26357a550e1fb6560c2d) - High
- CloudTrail event for VPC configuration changes should have alarm configured (Rule Id: 5c8c26397a550e1fb6560c32) - High

March 3, 2023 Policy Release 23

Read the following topics next:

- Deprecated Compliance Framework

Deprecated Compliance Framework

The following compliance framework is deprecated:

- MITRE ATT&CK Cloud, version 8

Per the compliance lifecycle, only the two latest versions of a compliance framework are supported at any given time. When a framework is deprecated, users can either switch to a newer version or create a custom framework to maintain the deprecated one.

February 16, 2023 Policy Release 24

Read the following topics next:

- Updated AWS Security Posture Policy

Updated AWS Security Posture Policy

The following policy had its service category corrected from "ACM" to "IAM":

- IAM user, group, or role should not have permission to pass all roles (RuleId: cdc3cf89-bef5-4a9c-846a-e308864b3845) - High

February 7, 2023 Policy Release 25

Read the following topics next:

- New Compliance Framework

New Compliance Framework

The following framework received mappings for the first time to AWS, Azure, GCP, and Kubernetes policies:

- PCI DSS 4.0

January 27, 2023 Policy Release 26

Read the following topics next:

- Updated AWS Security Posture Policy

Updated AWS Security Posture Policy

The following policy received changes in rule name, query, display name, description, suggested action, and trigger to support IAM and RBAC authentication checks:

- ElastiCache cluster should not have authentication disabled (RuleId: d817b2e7-f506-43b4-97e2-5e503bd2d1fd) - Medium

January 19, 2023 Policy Release 27

Read the following topics next:

- Updated AWS Security Posture Policy

Updated AWS Security Posture Policy

The following policyreceived a KB article update to fix an incorrect policy statement field:

- IAM user, group, or role should not have permission to assume all roles (RuleId: 9b5f60bb-1a84-400f-b9c8-620a5124b044) - High

January 12, 2023 Policy Release

28

Read the following topics next:

- Deprecated Compliance Framework

Deprecated Compliance Framework

The following framework is deprecated:

- CIS Azure Foundations Benchmark 1.3.0

January 9, 2023 Policy Release 29

Read the following topics next:

- New AWS Security Posture Policies
- New Compliance Frameworks

New AWS Security Posture Policies

- IAM user, group, or role should not have permission to assume all roles (RuleId: 9b5f60bb-1a84-400f-b9c8-620a5124b044) - High
- IAM user, group, or role should not have permission to pass all roles (RuleId: cdc3cf89-bef5-4a9c-846a-e308864b3845) - High
- IAM managed policy should not use the NotAction field to grant access (RuleId: 33b53a22-9610-4cb9-9ca8-66bd527cf083) - Medium

New Compliance Frameworks

The following frameworks were mapped to controls for AWS, Azure, GCP, and Kubernetes policies for the first time:

- MITRE ATT&CK Cloud, version 11.0
- MITRE ATT&CK Containers, version 11.0

These updates were part of the overall upgrade to MITRE ATT&CK Enterprise version 11.0, and include the following changes:

- Several controls received updated descriptions.
- In MITRE ATT&CK Containers, the control **Scheduled Task/Job (T1053.001)** was replaced with **Scheduled Task/Job-At (T1053.002)** to better reflect adversary behavior.