Guía del usuario

AWS Audit Manager

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Audit Manager: Guía del usuario

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS Audit Manager? ... 1
Características de AWS Audit Manager ... 1
Precios para AWS Audit Manager ... 3
¿Es la primera vez que usa Audit Manager? ... 3
Relacionado Servicios de AWS ... 3
Más AWS Audit Manager recursos ... 5
Conceptos y terminología ... 5
A ... 6
C ... 9
D ... 13
E ... 16
F ... 20
I ... 22
R ... 22
S ... 24
Cómo funciona la recopilación de evidencias ... 25
Frecuencia de recolección de evidencias ... 26
Ejemplos de controles ... 27
Controles automatizados (Security Hub) ... 29
Controles automatizados (AWS Config) ... 31
Controles automatizados (llamadas a la API) ... 33
Controles automatizados (CloudTrail) ... 35
Controles manuales ... 37
Controles con orígenes de datos mixtos ... 39
Usando AWS Audit Manager ... 41
Uso de Audit Manager con un AWS SDK ... 42
Uso de Audit Manager con AWS CloudFormation ... 43
Integraciones de GRC de terceros ... 44
Integración de las evidencias de Audit Manager en el sistema de GRC ... 47
Marcos admitidos ... 61
Essential Eight del ACSC ... 62
¿Qué es Essential Eight? ... 63
Uso de este marco ... 63
Pasos a seguir a continuación ... 64

Recursos adicionales ... 65
ACSC ISM ... 65
¿Qué es el ISM del ACSC? ... 65
Uso de este marco ... 65
Pasos a seguir a continuación ... 67
Recursos adicionales ... 67
AWS Audit Manager Ejemplo de marco ... 67
¿Qué es el marco AWS Audit Manager de muestra? ... 67
Uso de este marco ... 68
Pasos a seguir a continuación ... 69
AWS Control Tower Barandillas ... 69
¿Qué es? AWS Control Tower ... 70
Uso de este marco ... 70
Pasos a seguir a continuación ... 71
Recursos adicionales ... 71
AWS Mejores prácticas de IA generativa ... 72
¿Cuáles son las mejores prácticas de IA AWS generativa para Amazon Bedrock? ... 73
Uso de este marco ... 75
Verificación manual de las indicaciones en Amazon Bedrock ... 76
Pasos a seguir a continuación ... 79
Recursos adicionales ... 80
AWS License Manager ... 80
¿Qué es? AWS License Manager ... 80
Uso de este marco ... 81
Pasos a seguir a continuación ... 81
Recursos adicionales ... 82
AWS Mejores prácticas de seguridad fundamentales ... 83
¿Qué es el estándar de prácticas de seguridad básicas recomendadas de AWS ? ... 83
Uso de este marco ... 83
Pasos a seguir a continuación ... 84
Recursos adicionales ... 85
AWS Mejores prácticas operativas ... 85
¿Qué es el estándar de mejores AWS prácticas de seguridad fundamentales? ... 85
Uso de este marco ... 86
Pasos a seguir a continuación ... 86
Recursos adicionales ... 87

AWS Well Architected Framework (WAF v1.0) 87
¿Qué es el AWS Well-Architected Framework? 87
Uso de este marco 87
Pasos a seguir a continuación 89
Recursos adicionales 85
Perfil medio de control de la nube del CCCS 89
¿Qué es el CCCS? 89
Uso de este marco 90
Pasos a seguir a continuación 91
Índice de referencia CIS v.1.2 AWS 92
¿Qué es CIS? 92
Uso de este marco 93
Pasos a seguir a continuación 102
Recursos adicionales 102
Índice de referencia CIS v.1.3 AWS 102
¿Qué es el índice de referencia AWS CIS? 103
Usar estos marcos 104
Pasos a seguir a continuación 106
Recursos adicionales 106
Índice de referencia CIS v.1.4 AWS 106
¿Qué es el índice de referencia CIS? AWS 107
Usar estos marcos 108
Pasos a seguir a continuación 109
Recursos adicionales 110
CIS Controls v7.1 IG1 110
¿Qué son los controles CIS? 110
Uso de este marco 111
Pasos a seguir a continuación 112
Recursos adicionales 113
CIS Critical Security Controls versión 8.0, IG1 113
¿Qué son los controles CIS? 113
Uso de este marco 114
Pasos a seguir a continuación 115
Recursos adicionales 115
FedRAMP Security Baseline Controls r4 116
¿Qué es FedRAMP? 116

Uso de este marco ... 116
Pasos a seguir a continuación ... 117
Recursos adicionales ... 118
GDPR 2016 ... 118
¿Qué es GDPR? ... 118
Uso de este marco ... 119
Pasos a seguir a continuación ... 145
Recursos adicionales ... 145
GLBA ... 145
¿Qué es la GLBA? ... 146
Uso de este marco ... 146
Pasos a seguir a continuación ... 147
Title 21 CFR Part 11 ... 147
¿Qué es Title 21 de CFR Part 11? ... 148
Uso de este marco ... 148
Pasos a seguir a continuación ... 149
Recursos adicionales ... 150
EU GMP Annex 11, v1 ... 150
¿Qué es EU GMP Annex 11? ... 150
Uso de este marco ... 151
Pasos a seguir a continuación ... 152
HIPAA Security Rule: Feb 2003 ... 152
¿Qué es la HIPAA y la Norma de Seguridad de la HIPAA de 2003? ... 153
Uso de este marco ... 154
Pasos a seguir a continuación ... 155
Recursos adicionales ... 155
HIPAA Omnibus Final Rule ... 155
¿Qué es la HIPAA y la norma general de seguridad definitiva de la HIPAA? ... 156
Uso de este marco ... 154
Pasos a seguir a continuación ... 158
Recursos adicionales ... 158
ISO/IEC 27001:2013 ... 159
¿Qué es 27001? ISO/IEC ... 159
Uso de este marco ... 160
Pasos a seguir a continuación ... 161
Recursos adicionales ... 161

NIST SP 800-53 R5 ... 161
¿Qué es NIST SP 800-53? ... 162
Uso de este marco ... 163
Pasos a seguir a continuación ... 164
Recursos adicionales ... 164
CSF de NIST v1.1 ... 164
¿Qué es el marco de ciberseguridad del NIST? ... 165
Uso de este marco ... 166
Pasos a seguir a continuación ... 167
Recursos adicionales ... 167
NIST SP 800-171 R2 ... 167
¿Qué es NIST SP 800-171? ... 168
Uso de este marco ... 168
Pasos a seguir a continuación ... 170
Recursos adicionales ... 170
PCI DSS v3.2.1 ... 170
¿Qué es PCI DSS? ... 171
Uso de este marco ... 171
Pasos a seguir a continuación ... 172
Recursos adicionales ... 173
PCI DSS v4 ... 173
¿Qué es PCI DSS? ... 173
Uso de este marco ... 174
Pasos a seguir a continuación ... 175
Recursos adicionales ... 176
SSAE-18 SOC 2 ... 176
¿Qué es SOC 2? ... 176
Uso de este marco ... 177
Pasos a seguir a continuación ... 178
Recursos adicionales ... 179
Orígenes de datos admitidos ... 180
Puntos clave ... 180
Pasos a seguir a continuación ... 185
AWS Config ... 185
Puntos clave ... 186
Reglas AWS Config administradas compatibles ... 186

Uso de reglas personalizadas con Audit Manager 198
Recursos adicionales 199
AWS Security Hub 199
Puntos clave 199
Controles de Security Hub compatibles 211
Recursos adicionales 247
AWS Llamadas a la API 248
Puntos clave 248
Se admiten llamadas a la API para orígenes de datos de control personalizadas 249
AWS License Manager Llamadas a la API 261
Recursos adicionales 261
AWS CloudTrail 262
Recursos adicionales 263
Configuración 264
Requisitos previos 264
Inscríbase en una Cuenta de AWS 265
Creación de un usuario con acceso administrativo 266
Añada los permisos necesarios 267
Pasos a seguir a continuación 268
Habilitación de Audit Manager 268
Requisitos previos 268
Procedimiento 269
Pasos a seguir a continuación 273
Recomendaciones 273
Puntos clave 273
Características recomendadas 274
Integraciones recomendadas 274
Pasos a seguir a continuación 280
Introducción 281
Tutoriales de Audit Manager 282
Tutorial para propietarios de auditorías: crear una evaluación 282
Requisitos previos 283
Procedimiento 283
Recursos adicionales 285
Tutorial para delegados: Revisión de un conjunto de controles 286
Requisitos previos 287

Procedimiento ... 287
Recursos adicionales ... 291
Uso del panel ... 292
Conceptos y terminología del panel ... 293
Elementos del panel ... 295
Filtro de evaluación ... 295
Instantánea diaria ... 296
Controles con evidencia no conforme agrupados por dominio de control ... 297
Pasos a seguir a continuación ... 299
Recursos adicionales ... 300
Evaluaciones ... 301
Puntos clave ... 301
Recursos adicionales ... 301
Creación de las evaluaciones ... 302
Requisitos previos ... 303
Procedimiento ... 303
Pasos a seguir a continuación ... 308
Recursos adicionales ... 308
Búsqueda de una evaluación ... 308
Requisitos previos ... 309
Procedimiento ... 309
Pasos a seguir a continuación ... 310
Recursos adicionales ... 310
Revisión de las evaluaciones ... 310
Puntos clave ... 310
Recursos adicionales ... 311
Detalles de las evaluaciones ... 311
Detalles de los controles de evaluación ... 319
Detalles de la carpeta de evidencias ... 326
Detalles de las evidencias ... 330
Edición de las evaluaciones ... 334
Requisitos previos ... 335
Procedimiento ... 335
Pasos a seguir a continuación ... 338
Recursos adicionales ... 338
Carga manual de evidencias ... 338

Puntos clave ... 339
Recursos adicionales ... 340
Importación de evidencias desde S3 ... 340
Carga de evidencias desde un navegador ... 344
Introducción de texto como evidencia ... 349
Formatos compatibles ... 353
Preparación de un informe de evaluación ... 354
Puntos clave ... 354
Recursos adicionales ... 354
Añadir evidencias a los informes de evaluación ... 354
Eliminación de evidencias de un informe de evaluación ... 356
Generación de informes de evaluación ... 357
Cambio del estado de un control de evaluación ... 359
Requisitos previos ... 359
Procedimiento ... 359
Pasos a seguir a continuación ... 362
Cambio del estado de las evaluaciones ... 362
Requisitos previos ... 363
Procedimiento ... 363
Pasos a seguir a continuación ... 365
Eliminación de las evaluaciones ... 365
Requisitos previos ... 366
Procedimiento ... 366
Recursos adicionales ... 367
Delegations ... 368
Puntos clave ... 368
Recursos adicionales ... 368
Para propietarios de Audit Manager ... 369
Puntos clave ... 369
Recursos adicionales ... 370
Delegar un conjunto de controles ... 370
Búsqueda de delegaciones ... 373
Borrar delegaciones ... 374
Para los delegados ... 375
Puntos clave ... 375
Recursos adicionales ... 376

Visualización de las notificaciones ... 376
Revisar los controles y las evidencias ... 378
Añadir comentarios ... 380
Marcar un control como revisado ... 380
Enviar un conjunto de controles al propietario de la auditoría ... 382
Informes de evaluación ... 383
Descripción de la estructura de carpetas ... 383
Navegación por el informe de evaluación ... 384
Revisión de las secciones del informe de evaluación ... 385
Portada ... 385
Página de información general ... 386
Página del índice ... 387
Página de control ... 387
Página de resumen de evidencias ... 389
Página de información sobre evidencias ... 391
Validación de un informe de evaluación ... 391
Recursos adicionales ... 392
Buscador de evidencias ... 393
Puntos clave ... 393
Entendiendo cómo funciona el buscador de pruebas con CloudTrail Lake ... 393
Pasos a seguir a continuación ... 394
Recursos adicionales ... 394
Búsqueda de evidencias ... 394
Requisitos previos ... 395
Procedimiento ... 395
Pasos a seguir a continuación ... 399
Recursos adicionales ... 399
Visualización de los resultados de búsqueda ... 399
Requisitos previos ... 400
Procedimiento ... 400
Pasos a seguir a continuación ... 403
Recursos adicionales ... 404
Exportación de los resultados de la búsqueda ... 404
Requisitos previos ... 404
Procedimiento ... 404
Recursos adicionales ... 409

Opciones de filtros y agrupaciones ... 409
Referencia de filtro ... 409
Agrupación de referencia ... 415
Ejemplos de casos de uso ... 415
Caso de uso 1: busque evidencias de no conformidad y organice las delegaciones ... 416
Caso de uso 2: identificar evidencias de conformidad ... 417
Caso de uso 3: realizar una vista previa rápida de los recursos de evidencias ... 418
Centro de descargas ... 419
Navegar por el centro de descargas ... 419
Descarga de un archivo ... 421
Eliminación de un archivo ... 421
Recursos adicionales ... 422
Biblioteca de marcos ... 423
Puntos clave ... 423
Recursos adicionales ... 424
Búsqueda de un marco ... 424
Requisitos previos ... 424
Procedimiento ... 425
Pasos a seguir a continuación ... 426
Recursos adicionales ... 426
Revisión de un marco ... 426
Requisitos previos ... 426
Procedimiento ... 426
Pasos a seguir a continuación ... 430
Recursos adicionales ... 430
Crear un marco personalizado ... 430
Puntos clave ... 431
Recursos adicionales ... 431
Creación desde cero ... 431
Creación de una copia editable ... 434
Editar un marco personalizado ... 437
Requisitos previos ... 437
Procedimiento ... 437
Pasos a seguir a continuación ... 439
Recursos adicionales ... 439
Compartir un marco personalizado ... 439

Puntos clave ... 439
Recursos adicionales ... 440
Conceptos y terminología ... 440
Enviar una solicitud de uso compartido ... 449
Responder a una solicitud de uso compartido ... 456
Eliminar una solicitud de uso compartido ... 460
Eliminar un marco personalizado ... 461
Requisitos previos ... 461
Procedimiento ... 462
Recursos adicionales ... 463
Biblioteca de control ... 464
Puntos clave ... 464
Recursos adicionales ... 464
Búsqueda de un control ... 465
Requisitos previos ... 465
Procedimiento ... 466
Pasos a seguir a continuación ... 467
Recursos adicionales ... 467
Revisión de un control ... 467
... 467
Controles comunes ... 468
Controles principales ... 471
Controles estándar ... 475
Controles personalizados ... 480
Creación de un control personalizado ... 485
... 485
Puntos clave ... 485
Recursos adicionales ... 486
Creación desde cero ... 486
Creación de una copia editable ... 493
Editar un control personalizado ... 498
Requisitos previos ... 498
Procedimiento ... 498
Pasos a seguir a continuación ... 503
Recursos adicionales ... 503
Cambiar la frecuencia de recopilación de evidencias ... 503

Eliminación de un control personalizado ... 507
Requisitos previos ... 507
Procedimiento ... 507
Recursos adicionales ... 509
Configuración ... 510
Procedimiento ... 510
Pasos a seguir a continuación ... 510
Configuración de los ajustes del cifrado de datos ... 511
Requisitos previos ... 511
Procedimiento ... 511
Recursos adicionales ... 513
Adición de un administrador delegado ... 513
Requisitos previos ... 513
Procedimiento ... 514
Pasos a seguir a continuación ... 515
Recursos adicionales ... 515
Cambio de un administrador delegado ... 515
Requisitos previos ... 516
Procedimiento ... 517
Pasos a seguir a continuación ... 519
Recursos adicionales ... 519
Eliminación de un administrador delegado ... 519
Requisitos previos ... 520
Procedimiento ... 521
Recursos adicionales ... 522
Configuración de los responsables de auditoría predeterminados ... 522
Procedimiento ... 522
Recursos adicionales ... 524
Configuración del destino del informe de evaluación predeterminado ... 524
Requisitos previos ... 524
Procedimiento ... 526
Recursos adicionales ... 527
Configuración de notificaciones en Audit Manager ... 527
Requisitos previos ... 528
Procedimiento ... 528
Recursos adicionales ... 529

Habilitar el buscador de evidencias ... 529
Requisitos previos ... 529
Procedimiento ... 530
Pasos a seguir a continuación ... 531
Recursos adicionales ... 531
Confirming the status of evidence finder ... 531
Requisitos previos ... 532
Procedimiento ... 532
Pasos a seguir a continuación ... 535
Recursos adicionales ... 535
Deshabilitar el buscador de evidencias ... 535
Requisitos previos ... 536
Procedimiento ... 536
Recursos adicionales ... 537
Configuración del destino de la exportación predeterminada ... 537
Requisitos previos ... 537
Procedimiento ... 539
Notificaciones ... 542
Recursos adicionales ... 542
Solución de problemas ... 543
Solución de problemas con las evaluaciones y la recopilación de evidencias ... 543
He creado una evaluación, pero aún no veo ninguna prueba ... 544
Mi evaluación no consiste en recopilar pruebas de control de cumplimiento de AWS Security Hub ... 545
He deshabilitado un control de seguridad en Security Hub ¿Audit Manager recopila evidencias de comprobación de conformidad para ese control de seguridad? ... 546
He establecido el estado de un resultado en `Suppressed` en Security Hub ¿Audit Manager recopila evidencias de comprobación de conformidad sobre ese resultado? ... 547
Mi evaluación no consiste en recopilar pruebas de control de cumplimiento de AWS Config ... 547
Mi evaluación no consiste en recopilar pruebas de la actividad de los usuarios de AWS CloudTrail ... 549
Mi evaluación no consiste en recopilar evidencia de datos de configuración para una llamada a la AWS API ... 550
Un control común no está recopilando ninguna evidencia automatizada ... 550

Mis pruebas se generan a intervalos diferentes y no estoy seguro de la frecuencia con la que se recopilan ... 551
He desactivado Audit Manager y, a continuación, he vuelto a activarlo, y ahora mis evaluaciones preexistentes ya no recopilan pruebas ... 553
En la página de detalles de la evaluación se me pide que vuelva a crearla ... 554
¿Cuál es la diferencia entre un origen de datos y un origen de evidencias? ... 554
Error al crear mi evaluación ... 555
¿Qué ocurre si elimino una cuenta incluida en el ámbito de aplicación de mi organización? ... 556
No puedo ver los servicios incluidos en el ámbito de la evaluación ... 556
No puedo editar los servicios incluidos en el ámbito de mi evaluación ... 556
¿Cuál es la diferencia entre un servicio incluido y un tipo de origen de datos? ... 557
Informes de evaluación de solución de problemas ... 558
No se pudo generar mi informe de evaluación ... 559
He seguido la lista de verificación anterior y mi informe de evaluación sigue sin generarse . 560
Cuando intento generar un informe, aparece un error de acceso denegado ... 561
No puedo abrir el informe de evaluación ... 562
Cuando elijo el nombre de una prueba en un informe, no se me redirige a los detalles de la evidencia ... 562
La generación de mi informe de evaluación está bloqueada en el estado En curso y no estoy seguro de cómo afecta esto a mi facturación ... 563
Recursos adicionales ... 563
Solución de problemas con los controles y los conjuntos de controles ... 563
No veo ningún control o conjunto de controles en mi evaluación ... 564
No puedo subir pruebas manuales a un control ... 564
¿Qué significa si en un control se indica Reemplazo disponible? ... 565
Necesito usar varias AWS Config reglas como fuente de datos para un solo control ... 565
La opción de regla personalizada no está disponible para mi origen de datos ... 565
La lista desplegable de reglas personalizadas está vacía ... 566
No veo la regla personalizada que quiero usar ... 566
No veo la regla administrada que quiero usar ... 567
Quiero compartir un marco personalizado, pero tiene controles que utilizan reglas AWS Config personalizadas como origen de datos ... 570
¿Qué ocurre cuando se actualiza una regla personalizada en AWS Config? ... 571
Solución de problemas con el panel ... 573
No hay ningún dato en mi panel ... 573

La opción de descarga en formato CSV no está disponible 573
No veo el archivo descargado cuando intento descargar un archivo CSV 574
Falta un control o dominio de control específico en el panel de control 574
Veo controles similares o duplicados que aparecen en el mismo dominio de control 574
La instantánea diaria muestra cantidades variables de evidencia cada día. ¿Es esto normal? 576
Solución de problemas con los administradores delegados y AWS Organizations 576
No puedo configurar Audit Manager con mi cuenta de administrador delegado 576
Cuando creo una evaluación, no puedo ver las cuentas de mi organización en Cuentas incluidas 577
Aparece un error de acceso denegado cuando intento generar un informe de evaluación con mi cuenta de administrador delegado 577
¿Qué ocurre en Audit Manager si desvinculo la cuenta de un miembro de mi organización? 579
¿Qué ocurre si vuelvo a vincular la cuenta de un miembro a mi organización? 579
¿Qué ocurre si migro la cuenta de un miembro de una organización a otra? 579
Solución de problemas del buscador de evidencias 579
No puedo habilitar el buscador de evidencias 580
He activado el buscador de evidencias, pero no veo pruebas anteriores en los resultados de mi búsqueda 581
No puedo desactivar el buscador de evidencias 581
Mi consulta de búsqueda falla 582
Veo que un dominio de control está marcado como obsoleto ¿Qué significa esto? 585
No puedo generar varios informes de evaluación a partir de los resultados de mi búsqueda 585
No puedo incluir pruebas específicas de los resultados de mi búsqueda 586
No todos los resultados de mi buscador de evidencias se incluyen en el informe de evaluación 586
Quiero generar un informe de evaluación a partir de los resultados de mi búsqueda, pero el enunciado de mi consulta no funciona 587
Recursos adicionales 590
Mi exportación CSV ha fallado 590
No puedo exportar pruebas específicas de los resultados de mi búsqueda 592
No puedo exportar varios archivos CSV a la vez 593
Solución de problemas con los marcos 593

En la página de detalles del marco personalizado se me pide que vuelva a crear el marco personalizado ... 594
No puedo crear una copia del marco personalizado ... 597
El estado de mi solicitud de compartir enviada aparece como Fallido ... 597
Mi solicitud de uso compartido tiene un punto azul al lado. ¿Qué significa esto? ... 597
Mi marco compartido tiene controles que utilizan AWS Config reglas personalizadas como fuente de datos. ¿Puede el destinatario recopilar pruebas para estos controles? ... 600
He actualizado una regla personalizada que se usa en un marco compartido. ¿Tengo que tomar alguna medida? ... 601
Solución de problemas de notificaciones ... 602
He especificado un tema de Amazon SNS en Audit Manager, pero no recibo ninguna notificación ... 603
He especificado un tema de FIFO, pero no recibo las notificaciones en el orden esperado .. 603
Solución de problemas con los permisos y los accesos ... 603
He seguido el procedimiento de configuración de Audit Manager, pero no tengo suficientes privilegios de IAM ... 604
He especificado a alguien como propietario de la auditoría, pero aún no tiene acceso completo a la evaluación. ¿Por qué sucede esto? ... 605
No puedo realizar una acción en Audit Manager ... 605
Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Audit Manager ... 605
Aparece un error de acceso denegado, a pesar de tener los permisos necesarios de Audit Manager ... 606
Recursos adicionales ... 607
Etiquetado de recursos ... 609
Recursos admitidos ... 609
Restricciones de las etiquetas ... 610
Administrar etiquetas en Audit Manager ... 610
Cuotas ... 612
Cuotas de Audit Manager ... 612
Administrar las cuotas ... 613
Recursos adicionales ... 614
Ejemplos de código ... 615
Escenarios ... 615
Cree un marco personalizado a partir de un paquete de AWS Config conformidad ... 616
Crear un marco personalizado que contenga los controles de Security Hub ... 620

Crear un informe de evaluación ... 623
Seguridad ... 629
Protección de los datos ... 630
Eliminación de datos de Audit Manager ... 631
Cifrado en reposo ... 632
Cifrado en tránsito ... 633
Administración de claves ... 633
Identity and Access Management ... 634
Público ... 635
Autenticación con identidades ... 635
Administración de acceso mediante políticas ... 639
¿Cómo AWS Audit Manager funciona con IAM ... 642
Ejemplos de políticas basadas en identidades ... 652
Prevención de la sustitución confusa entre servicios ... 668
Ejemplos de políticas basadas en recursos ... 670
AWS políticas gestionadas ... 672
Solución de problemas ... 706
Cómo utilizar roles vinculados a servicios ... 708
Validación de conformidad ... 723
Resiliencia ... 724
Seguridad de la infraestructura ... 724
Puntos de conexión de VPC (AWS PrivateLink) ... 725
Consideraciones sobre los puntos AWS Audit Manager finales de VPC ... 725
Creación de un punto de conexión de VPC de interfaz para AWS Audit Manager ... 726
Crear una política de puntos de conexión de VPC para AWS Audit Manager ... 726
Registro y supervisión ... 727
Monitorización con Amazon EventBridge ... 727
CloudTrail registros ... 732
Configuración y vulnerabilidad ... 735
Desactivar AWS Audit Manager ... 736
Procedimiento ... 736
Pasos a seguir a continuación ... 738
Recursos adicionales ... 739
Historial de documentos ... 740
... dcclvi

¿Qué es AWS Audit Manager?

Bienvenido a la Guía AWS Audit Manager del usuario.

AWS Audit Manager le ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector. Audit Manager automatiza la recopilación de evidencias para que pueda evaluar más fácilmente si sus políticas, procedimientos y actividades (también conocidas como controles) son eficaces. Llegado el momento de una auditoría, Audit Manager le ayuda a gestionar las revisiones de sus controles por parte de las personas interesadas. Esto significa que puede crear informes listos para la auditoría con mucho menos esfuerzo manual.

Audit Manager proporciona marcos prediseñados que estructuran y automatizan las evaluaciones para normas o reglamentos de cumplimiento determinados. Estos marcos incluyen una colección prediseñada de controles con descripciones y procedimientos de prueba. Asimismo, se agrupan según los requisitos de la norma o reglamento de cumplimiento en cuestión. También puede personalizar los marcos y los controles para las auditorías internas de acuerdo con sus requisitos específicos.

Puede crear evaluaciones desde cualquier marco. Al crear una evaluación, Audit Manager ejecuta automáticamente las evaluaciones de los recursos. Estas recopilan datos para las Cuentas de AWS que defina como incluidos en la auditoría. Los datos que se recopilan se transforman automáticamente en evidencias aptas para la auditoría. Luego, se agregan a los controles pertinentes para mostrar, así, el cumplimiento en materia de seguridad, gestión de cambios, continuidad empresarial y licencias de software. El proceso de recopilación de evidencias es continuo y comienza cuando se crea la evaluación. Una vez completada la auditoría, puede detener la recopilación de evidencias si ya no necesita Audit Manager para ello. Para hacerlo, cambie el estado de la evaluación a inactiva.

Características de Audit Manager

Con AWS Audit Manager, puede realizar las siguientes tareas:

- Inicio rápido: cree su primera evaluación eligiendo la opción que mejor se adapte a sus necesidades de entre una galería de marcos prediseñados diseñados una variedad de normas y reglamentos de cumplimiento. A continuación, inicie la recopilación automática de pruebas para auditar su Servicio de AWS uso.

- Carga y gestión de evidencias de entornos híbridos o multinube: además de las evidencias que Audit Manager recopila de su entorno de AWS , también puede cargar y gestionar las evidencias de su entorno en las instalaciones o multinube de forma centralizada.
- Compatibilidad con normas y reglamentos de cumplimiento estándares: elija uno de los marcos estándar de AWS Audit Manager. Estos marcos proporcionan asignaciones de control predefinidas para las normas y reglamentos de cumplimiento más habituales, Estos incluyen el CIS Foundation Benchmark, el PCI DSS, el GDPR, la HIPAA y la GxP SOC2 y las mejores prácticas operativas. AWS
- Supervisión de evaluaciones activas: consulte los datos de análisis de sus evaluaciones activas e identifique rápidamente las evidencias no conformes que deban corregir gracias al panel de Audit Manager.
- Búsqueda de evidencias: utilice la característica de Buscador de evidencias para buscar rápidamente evidencias que sean pertinentes para su consulta de búsqueda. Puede generar informes de evaluación a partir de los resultados de la búsqueda o exportar los resultados de la búsqueda en formato CSV.
- Creación de controles personalizados: cree su propio control desde cero o cree una copia editable de un control estándar o personalizado existente. También puede usar la característica de los controles personalizados para crear preguntas de evaluación de riesgos y almacenar las respuestas a esas preguntas como evidencias manuales.
- Asignación de los controles empresariales a agrupaciones predefinidas de orígenes de datos de AWS : elija los controles comunes que representen sus objetivos y utilícelos para crear controles personalizados que recopilen evidencias para su cartera de necesidades de conformidad.
- Creación de marcos personalizados: cree sus propios marcos con controles estándar o personalizados en función de sus necesidades para las auditorías internas.
- Comparta marcos personalizados: comparta sus marcos personalizados de Audit Manager con otra Cuenta de AWS persona o reprodúzcalos en Región de AWS otro con su propia cuenta.
- Compatibilidad con la colaboración entre equipos: delegue los conjuntos de controles a expertos en la materia que puedan revisar las evidencias relacionadas, añadir comentarios y actualizar el estado de cada control.
- Creación de informes para la auditoría: genere informes de evaluación que resuman las evidencias relevantes recopiladas para la auditoría y enlacen a las carpetas que contienen las evidencias detalladas.
- Garantía de la integridad de las evidencias: guarde las evidencias en un lugar seguro donde no se modifiquen.

> **Note**
>
> AWS Audit Manager ayuda a recopilar pruebas relevantes para verificar el cumplimiento de normas y reglamentos de cumplimiento específicos. Sin embargo, no evalúa el cumplimiento en sí mismo. AWS Audit Manager Por lo tanto, es posible que las pruebas recopiladas no incluyan toda la información sobre su AWS uso que se necesita para las auditorías. AWS Audit Manager no sustituye a los asesores legales ni a los expertos en cumplimiento.

Precios de Audit Manager

Para obtener más información sobre los precios, consulte Precios de AWS Audit Manager.

¿Es la primera vez que usa Audit Manager?

Si es la primera vez que usa Audit Manager, le recomendamos que comience con las páginas siguientes:

1. Comprensión de AWS Audit Manager los conceptos y la terminología: conozca los conceptos y términos clave que se utilizan en Audit Manager, como, por ejemplo, las evaluaciones, los marcos y los controles.
2. Entender cómo se AWS Audit Manager recopilan las pruebas: descubra cómo Audit Manager recopila evidencias para evaluar los recursos.
3. Configuración AWS Audit Manager con los ajustes recomendados: conozca los requisitos de configuración de Audit Manager.
4. Empezar con AWS Audit Manager: siga un tutorial para crear su primera evaluación de Audit Manager.
5. AWS Audit Manager Referencia de la API: familiarícese con las acciones y los tipos de datos de la API de Audit Manager.

Relacionado Servicios de AWS

AWS Audit Manager se integra con varios Servicios de AWS para recopilar automáticamente pruebas que puede incluir en sus informes de evaluación.

AWS Security Hub

AWS Security Hub supervisa su entorno mediante controles de seguridad automatizados que se basan en las AWS mejores prácticas y los estándares del sector. Audit Manager captura instantáneas del estado de seguridad de sus recursos informando de los resultados de las comprobaciones de seguridad directamente desde Security Hub. Para obtener más información sobre Security Hub, consulte ¿Qué es AWS Security Hub? en la Guía AWS Security Hub del usuario.

AWS CloudTrail

AWS CloudTrail le ayuda a supervisar las llamadas realizadas a AWS los recursos de su cuenta. Estas incluyen las llamadas realizadas por la consola AWS de administración, la AWS CLI y otros Servicios de AWS. Audit Manager recopila los datos de registro CloudTrail directamente y convierte los registros procesados en evidencia de la actividad del usuario. Para obtener más información al respecto CloudTrail, consulte ¿Qué es AWS CloudTrail? en la Guía AWS CloudTrail del usuario.

AWS Config

AWS Config proporciona una vista detallada de la configuración de AWS los recursos de su Cuenta de AWS. Esto incluye cómo se relacionan los recursos entre sí y cómo se configuraron anteriormente. Audit Manager captura instantáneas del estado de seguridad de sus recursos informando de las conclusiones directamente desde AWS Config. Para obtener más información al respecto AWS Config, consulte ¿Qué es? AWS Config en la Guía AWS Config del usuario.

AWS License Manager

AWS License Manager agiliza el proceso de llevar las licencias de los proveedores de software a la nube. A medida que vaya creando una infraestructura en la nube AWS, podrá ahorrar costes al reutilizar su inventario de licencias existente para utilizarlo con los recursos de la nube. Audit Manager incluye un marco de License Manager para ayudarlo en la preparación de la auditoría. Este marco se integra con License Manager para agregar información sobre el uso de licencias en función de las reglas de concesión de licencias definidas por el cliente. Para obtener más información sobre License Manager, consulte ¿Qué es AWS License Manager? en la Guía AWS License Manager del usuario.

AWS Control Tower

AWS Control Tower impone barreras preventivas y de detección para la infraestructura de la nube. Audit Manager proporciona un marco de AWS Control Tower Guardrails para ayudarlo en la preparación de la auditoría. Este marco contiene todas las AWS Config reglas que se basan en las barreras de protección de. AWS Control Tower Para obtener más información al respecto AWS Control Tower, consulte ¿Qué es? AWS Control Tower en la Guía AWS Control Tower del usuario.

AWS Artifact

AWS Artifact es un portal de recuperación de artefactos de auditoría de autoservicio que proporciona acceso bajo demanda a la documentación de conformidad y las certificaciones de la infraestructura. AWS AWS Artifact ofrece pruebas que demuestran que la infraestructura de la AWS nube cumple los requisitos de conformidad. Por el contrario, le AWS Audit Manager ayuda a recopilar, revisar y gestionar pruebas para demostrar que su uso Servicios de AWS cumple con las normas. Para obtener más información al respecto AWS Artifact, consulte ¿Qué es AWS Artifact? en la Guía AWS Artifact del usuario. Puede descargar una lista de AWS informes en AWS Management Console.

Amazon EventBridge

Amazon le EventBridge ayuda a automatizar los eventos del sistema Servicios de AWS y a responder automáticamente a ellos, como problemas de disponibilidad de las aplicaciones o cambios en los recursos. Puede usar EventBridge reglas para detectar eventos de Audit Manager y reaccionar ante ellos. Según las reglas que cree, EventBridge invoca una o más acciones objetivo cuando un evento coincide con los valores que especifique en una regla. Para obtener más información, consulte Monitorización AWS Audit Manager con Amazon EventBridge.

Para obtener una lista del alcance Servicios de AWS de los programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento. Para más información general, consulte Programas de conformidad de AWS.

Más recursos de Audit Manager

Consulte estos recursos para obtener más información sobre Audit Manager.

- Recopile pruebas y gestione los datos de auditoría mediante AWS Audit Manager
- Integre el modelo de tres líneas (parte 2): transforme los paquetes de AWS Config conformidad en AWS Audit Manager evaluaciones del blog sobre AWS administración y gobierno

Comprensión de AWS Audit Manager los conceptos y la terminología

En este tema se explican algunos de los conceptos clave que debe conocer para comenzar a utilizar AWS Audit Manager.

A

| B | | | | G | H | J | K | L | M | N | O | P | Q | | T | U | V | W | X | Y | Z

Evaluaciones

Recopile evidencias relevantes para las auditorías automáticamente con las evaluaciones de Audit Manager.

Las evaluaciones se basan en marcos, es decir agrupaciones de controles relacionados con las auditorías. Puede crear una evaluación a partir de un marco estándar o personalizado. Los marcos estándar contienen conjuntos de controles prediseñados que con arreglo a una norma o reglamento de cumplimiento específico. Los marcos personalizados, en cambio, incluyen controles que puede personalizar y agrupar según sus requisitos de auditoría. Si utiliza un marco como punto de partida, puede crear una evaluación que especifique lo Cuentas de AWS que desea incluir en el ámbito de la auditoría.

Al crear una evaluación, Audit Manager comienza automáticamente a evaluar sus recursos en Cuentas de AWS función de los controles que se definen en el marco. A continuación, recopila las evidencias relevantes y las convierte a un formato fácil de usar para los auditores. Una vez hecho esto, agrega las evidencias a los controles de evaluación. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas recopiladas y, a continuación, añadirlas a un informe de evaluación. Este informe de evaluación le ayuda a demostrar que sus controles funcionan según lo previsto.

La recopilación de evidencias es un proceso continuo que comienza cuando se crea la evaluación. Puede detener la recopilación de evidencias, o bien cambiando el estado de la evaluación a inactiva, o bien en el nivel de control. Para ello, puede cambiar el estado de un control de su evaluación en concreto a inactivo.

Para obtener instrucciones acerca de cómo crear y administrar las evaluaciones, consulte Gestionar las evaluaciones en AWS Audit Manager.

Informes de evaluación

Los informes de evaluación son documentos finalizados que se generan a partir de una evaluación de Audit Manager. Estos informes resumen las evidencias relevantes recopilada para la auditoría, y están enlazados con las carpetas de evidencias pertinentes. Estas carpetas se nombran y organizan de acuerdo con los controles que se especifican en cada evaluación. Puede revisar qué evidencias recopila Audit Manager para cada evaluación y decidir cuáles desea incluir en el informe de evaluación.

Para más información acerca de estos informes, consulte Informes de evaluación. Para información sobre cómo generar un informe de evaluación, consulte Preparación de un informe de evaluación en AWS Audit Manager.

Destino de los informes de evaluación

El destino de los informes de evaluación es el bucket S3 predeterminado en el que Audit Manager guarda los informes de evaluación. Para obtener más información, consulte Configuración del destino del informe de evaluación predeterminado.

Auditoría

Las auditorías son exámenes independientes de los activos, las operaciones o la integridad empresarial de su organización. Las auditorías de tecnología de la información (TI) examinan específicamente los controles de los sistemas de información de su organización. El objetivo de estas auditorías es determinar si los sistemas de información protegen los activos, funcionan de manera eficaz y mantienen la integridad de los datos. Todo esto es importante para cumplir con los requisitos reglamentarios exigidos por las normas o reglamentos de cumplimiento.

Responsable de la auditoría

El término responsable de la auditoría tiene dos significados diferentes según el contexto.

En el contexto de Audit Manager, el responsable de una auditoría es un usuario o rol que gestiona una evaluación y sus recursos relacionados. Se encarga de la creación de evaluaciones, la revisión de las evidencias y la generación de informes de evaluación. Audit Manager es un servicio colaborativo y los responsables de auditorías se benefician cuando otras partes interesadas participan en sus evaluaciones. Por ejemplo, puede añadir a otros responsables de la auditoría a su evaluación para compartir las tareas de administración. Además, si es responsable de una auditoría y necesita ayuda para interpretar las evidencias recopiladas para un control, puede delegar ese conjunto de controles a otra parte interesada que tenga experiencia en la materia. En ese caso, la persona se conoce como persona delegada.

En términos comerciales, el responsable de una auditoría es quien coordina y supervisa las iniciativas de preparación para la auditoría de su empresa y presenta las evidencias al auditor. Por lo general, se trata de un profesional de la gobernanza, el riesgo y el cumplimiento (GRC). Puede ser. por ejemplo, un responsable de cumplimiento o de protección de datos del RGPD. Los profesionales del GRC tienen la experiencia y la autoridad adecuadas para gestionar la preparación de las auditorías. Más específicamente, comprenden los requisitos de cumplimiento y pueden analizar, interpretar y preparar los datos de los informes. Sin embargo, otras funciones empresariales también pueden ser Audit Manager del responsable de una auditoría; no solo los

profesionales de GRC asumen esta función. Por ejemplo, puede optar por que un experto técnico de uno de los siguientes equipos configure y gestione las evaluaciones de Audit Manager:

- SecOps
- TI/ DevOps
- Respuesta a las operaciones de Center/Incident seguridad
- Equipos similares que poseen, desarrollan, corrigen e implementan activos en la nube y comprenden la infraestructura de nube de su organización

La persona elegida como responsable de la auditoría en su evaluación de Audit Manager dependerá en gran medida de su organización y también de cómo se estructuren las operaciones de seguridad y de las características específicas de la auditoría. En Audit Manager, una misma persona puede asumir el rol de responsable de la auditoría en una evaluación y, el de delegado, en otra.

Independientemente de cómo elija utilizar Audit Manager, puede gestionar la separación de funciones en su organización utilizando la owner/delegate persona de auditoría y otorgando políticas de IAM específicas a cada usuario. Mediante este enfoque de dos pasos, Audit Manager garantiza que usted tenga el control total sobre todos los aspectos específicos de cada evaluación. Para obtener más información, consulte Políticas recomendadas para los usuarios de AWS Audit Manager.

AWS fuente gestionada

Una fuente AWS gestionada es una fuente de pruebas que se AWS conserva para usted.

Cada fuente AWS gestionada es una agrupación predefinida de fuentes de datos que se asigna a un control común o control central específico. Cuando se utiliza un control común como origen de evidencias, se recopilan automáticamente las evidencias de todos los controles principales que respaldan ese control común. También puede utilizar los controles principales individuales como origen de evidencias.

Cada vez que se actualiza una fuente AWS gestionada, las mismas actualizaciones se aplican automáticamente a todos los controles personalizados que utilizan esa fuente AWS gestionada. Esto significa que los controles personalizados recopilan evidencias comparándolas con las definiciones más recientes de ese origen de evidencias. Esto le ayuda a garantizar la conformidad continua a medida que cambia el entorno de conformidad de la nube.

Consulte también: customer managed source, evidence source.

C

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | T | U | V | W | X | Y | Z

Registros de cambios

Para cada control de una evaluación, Audit Manager realiza un seguimiento de la actividad de los usuarios en dicho control. A continuación puede revisar un registro de auditoría de las actividades relacionadas con un control específico. Para obtener más información sobre las actividades de los usuarios que se capturan en el registro de cambios, consulte Pestaña del registro de cambios.

Conformidad en la nube

La conformidad con la nube es el principio general según el cual los sistemas suministrados en la nube deben cumplir con los estándares que se aplican a los clientes de la nube.

Control común

Consulte control.

Regulación del cumplimiento

Los reglamentos de cumplimiento son leyes, normas órdenes de otro tipo prescritas por una autoridad, normalmente para regular una conducta. Un ejemplo de ello es el RGPD.

Estándares de conformidad

Los estándares de conformidad son un conjunto estructurado de directrices que detallan los procesos de una organización para mantener la conformidad con las normas, especificaciones o legislación establecidas. Algunos ejemplos de ello son el PCI DSS y la HIPAA.

Control

Los controles son salvaguardias o medidas que se prescriben para un sistema de información o una organización. Se han diseñado los controles para proteger la confidencialidad, integridad y disponibilidad de su información y para cumplir con un conjunto de requisitos definidos. Garantizan que los recursos funcionen según lo previsto, que los datos sean fiables y que su organización cumpla con las leyes y normativas aplicables.

En Audit Manager, los controles también pueden ser preguntas en un cuestionario de evaluación de riesgos para proveedores. En ese caso, se trata de una pregunta específica que solicita información sobre la postura de seguridad y cumplimiento de una organización.

Los controles recopilan evidencias de forma continua cuando están activos en sus evaluaciones de Audit Manager. También puede agregar evidencias de forma manual a cualquier control. Cada

evidencia se convierte en un registro que le permite demostrar la conformidad con los requisitos del control.

Audit Manager proporciona los siguientes tipos de controles:

Tipo de control	Descripción
Control común	Puede pensar en un control común como una acción que le ayuda a cumplir un objetivo de control. Dado que los controles comunes no son específicos de ningún estándar de conformidad, le ayudan a recopilar evidencias que pueden respaldar una serie de obligaciones de conformidad que se superponen. Por ejemplo, supongamos que tiene un objetivo de control denominado Clasificación y tratamiento de datos. Para cumplir este objetivo, podría implementar un control común denominado Controles de acceso para supervisar y detectar el acceso no autorizado a los recursos. • Los controles comunes automatizados recopilan evidencias. Consisten en una agrupación de uno o varios controles principales relacionados. A su vez, cada uno de estos controles básicos recopila automáticamente las pruebas relevantes de un grupo predefinido de fuentes de AWS datos. AWS gesti ona estas fuentes de datos subyacentes por usted y las actualiza cada vez que cambian las normas y los estándares y se identifican nuevas fuentes de datos. • Los controles manuales comunes requieren que cargue sus propias evidencias. Esto se debe a que, por lo general, requieren el suministro de registros físicos o detalles sobre eventos que ocurren fuera de su AWS entorno. Por este motivo, a menudo no hay orígenes de datos de AWS que puedan proporcionar evidencias que respalden los requisitos del control manual común. No puede editar un control común. Sin embargo, puede usar cualquier control común como origen de evidencia al crear un control personalizado.
Control principal	Se trata de una directriz preceptiva para su AWS entorno. Puede pensar en un control principal como una acción que le ayuda a cumplir los requisitos de un control común.

Tipo de control	Descripción
	Por ejemplo, supongamos que utiliza un control común denominado Controles de acceso para supervisar el acceso no autorizado a los recursos. Para respaldar este control común, puede utilizar el control principal denominado Bloquear el acceso de lectura público en los buckets de S3. Dado que los controles principales no son específicos de ningún estándar de conformidad, recopilan evidencias que pueden respaldar una serie de obligaciones de conformidad que se superponen. Cada control principal utiliza una o más fuentes de datos para recopilar pruebas sobre un tema específic o Servicio de AWS. AWS administra estas fuentes de datos subyacentes por usted y las actualiza cada vez que cambian las normas y los estándares y se identifican nuevas fuentes de datos. No puede editar un control principal. Sin embargo, puede usar cualquier control principal como origen de evidencia al crear un control personalizado.
Control estándar	Se trata de un control prediseñado que proporciona Audit Manager. Puede utilizar los controles estándar para ayudarle a preparar las auditorías en relación con un determinado estándar de conformidad. Cada control estándar está relacionado con un determinado framework estándar de Audit Manager y recopila evidencias que puede utilizar para demostrar la conformidad con dicho marco. Los controles estándar recopilan evidencia de las fuentes de datos subyacentes que AWS gestiona. Estos orígenes de datos se actualizan automáticamente cada vez que cambien las normativas y los estándares y se identifiquen nuevos orígenes de datos. No puede editar los controles estándar. Sin embargo, puede crear una copia editable de cualquier control estándar.

Tipo de control	Descripción
Control personalizado	Se trata de un control que se crea en Audit Manager para cumplir con requisitos de conformidad específicos. Puede crear un control personalizado desde cero o crear una copia editable de un control estándar existente. Al crear un control personalizado, puede definir evidence source específicos que determinen de dónde recopila Audit Manager las evidencias. Tras crear un nuevo control personalizado, puede editarlo o añadirlo a un marco personalizado. También puede crear una copia editable de cualquier control personalizado.

Dominio de control

Piense en un dominio de control como una categoría general de controles que no es específica de ningún estándar de conformidad. Un ejemplo de dominio de control es la protección de datos.

Los controles suelen agruparse por dominio con fines organizativos sencillos. Cada dominio tiene varios objetivos.

Las agrupaciones de dominios de control son una de las funciones más potentes del panel de control de Audit Manager. Audit Manager destaca los controles de sus evaluaciones que contienen evidencias no conformes y los agrupa por dominio de control. Esto le permite centrar sus esfuerzos de remediación en ámbitos temáticos específicos mientras se prepara para una auditoría.

Objetivo de control

Un objetivo de control describe el objetivo de los controles comunes que le pertenecen. Cada objetivo puede tener varios controles comunes. Si estos controles comunes se implementan correctamente, le ayudarán a cumplir el objetivo.

Cada objetivo de control pertenece a un dominio de control. Por ejemplo, el dominio de control Protección de datos puede tener un objetivo de control denominado Clasificación y gestión de datos. Para respaldar este objetivo de control, podría utilizar un control común denominado Controles de acceso para supervisar y detectar el acceso no autorizado a los recursos.

Control principal

Consulte control.

Control personalizado

Consulte control.

Origen administrado por el cliente

Un origen administrado por el cliente es un origen de evidencias que usted define.

Al crear un control personalizado en Audit Manager, puede usar esta opción para crear sus propios orígenes de datos individuales. Esto le da la flexibilidad de recopilar pruebas automatizadas a partir de un recurso específico de la empresa, como una regla personalizada AWS Config . También puede utilizar esta opción si desea añadir evidencias manuales al control personalizado.

Cuando utilice orígenes administrados por el cliente, es responsable de mantener todos los orígenes de datos que cree.

Consulte también: AWS managed source, evidence source.

D

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | T | U | V | W | X | Y | Z

Origen de datos

Audit Manager utiliza orígenes de datos para recopilar evidencias para un control. Un origen de datos tiene las siguientes propiedades:

- Un tipo de origen de datos define el tipo de origen de datos del que Audit Manager recopila evidencias.
  - En el caso de evidencias automatizadas, el tipo puede ser AWS Security Hub, AWS Config, AWS CloudTrail o llamadas a la API de AWS .
  - Si carga sus propias evidencias, el tipo es Manual.
  - La API de Audit Manager hace referencia a un tipo de origen de datos como sourceType.
- Una asignación de origen de datos es una palabra clave que indica de dónde se recopilan las evidencias para un tipo de determinado origen de datos.

  - Por ejemplo, podría ser el nombre de un CloudTrail evento o el nombre de una AWS Config regla.
  - La API de Audit Manager hace referencia a una asignación de orígenes de datos como sourceKeyword.
- Un nombre de origen de datos etiqueta la combinación de un tipo de origen de datos y una asignación.
  - En el caso de los controles estándar, Audit Manager proporciona un nombre predeterminado.
  - En el caso de los controles personalizados, puede proporcionar su propio nombre.
  - La API Audit Manager hace referencia al nombre de los orígenes de datos como SourceName.

Un único control puede tener varios tipos de orígenes de datos y diferentes asignaciones. Por ejemplo, un control podría recopilar pruebas de una combinación de tipos de fuentes de datos (como AWS Config Security Hub). Otro control puede tener AWS Config como único tipo de fuente de datos, con varias AWS Config reglas como mapeos.

En la tabla siguiente se enumeran los tipos de origen de datos automatizados y se muestran ejemplos de algunas de las asignaciones correspondientes.

Data source type	Descripción	Ejemplo de asignación
AWS Security Hub	Utilice este tipo de origen de datos para capturar instantán eas del estado de seguridad de sus recursos. Audit Manager usa el nombre de un control de Security Hub como palabra clave de la asignación e informa del resultado del control de seguridad de dicha regla directamente desde Security Hub.	`EC2.1`
AWS Config	Utilice este tipo de origen de datos para capturar instantán	`SNS_ENCRYPTED_KMS`

Data source type	Descripción	Ejemplo de asignación
	eas del estado de seguridad de sus recursos. Audit Manager usa el nombre de una AWS Config regla como palabra clave de mapeo e informa el resultado de la verificación de esa regla directamente desde AWS Config.	
AWS CloudTrail	Utilice este tipo de origen de datos para realizar un seguimiento de la actividad de un usuario específica que sea necesaria en la auditoría. Audit Manager usa el nombre de un CloudTrail evento como palabra clave de mapeo y recopila la actividad de los usuarios relacionada de sus CloudTrail registros.	`CreateAccessKey`

Data source type	Descripción	Ejemplo de asignación
AWS Llamadas a la API	Utilice este tipo de fuente de datos para tomar una instantánea de la configura ción de sus recursos mediante una llamada a la API a un recurso específico Servicio de AWS. Audit Manager usa el nombre de la llamada a la API como palabra clave de asignación y recopila la respuesta de la API.	`kms_ListKeys`

Delegados

Un delegado es un AWS Audit Manager usuario con permisos limitados. y suelen tener experiencia empresarial o técnica especializada. Estos conocimientos pueden estar relacionados, por ejemplos, con las políticas de retención de datos, los planes de formación, la infraestructura de red o la gestión de identidades. Los delegados ayudan a los responsables de la auditoría a revisar las evidencias recopiladas para comprobar si hay controles que estén dentro de su área de especialización. Pueden revisar los conjuntos de controles y las evidencias relacionadas con estos, añadir comentarios, cargar evidencias adicionales y actualizar el estado de cada una de las evaluaciones que les asigne para revisar.

Los responsables de las auditorías asignan conjuntos de controles específicos a los delegados, no a evaluaciones completas. En consecuencia, los delegados tienen acceso limitado a las evaluaciones. Para obtener instrucciones acerca de cómo delegar un conjunto de controles, consulte Delegaciones en AWS Audit Manager.

E

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | Q | | T | U | V | W | X | Y | Z

Evidencias

Las evidencias son registros que contienen la información necesaria para demostrar el cumplimiento de los requisitos de una evaluación. Las evidencias pueden ser, por ejemplo, las actividades de cambio invocadas por los usuarios o instantáneas de la configuración del sistema.

Hay dos tipos de evidencia principales en Audit Manager: las evidencias automatizadas y evidencias manuales.

Tipo de evidencias	Descripción
Evidencia automatizada	Se trata de la evidencia que Audit Manager recopila automáticamente. Esto incluye las siguientes tres categorías de evidencias automatizadas: 1. Verificación de conformidad: el resultado de una verificación de conformidad se captura de AWS Security Hub AWS Config, o de ambas. Algunos ejemplos de comprobaciones de conformidad incluyen el resultado de una comprobación de seguridad de Security Hub para un control PCI DSS y una evaluación de AWS Config reglas para un control de HIPAA. Para obtener más información, consulte Reglas de AWS Config con el apoyo de AWS Audit Manager y AWS Security Hub controles compatibles con AWS Audit Manager. 2. Actividad del usuario: la actividad del usuario que cambia la configuración de un recurso se captura de los CloudTrail registros a medida que se produce esa actividad. Entre los ejemplos de actividades de los usuarios destacan las actualizaciones de la tabla de enrutamiento, los cambios en la configuración de la copia de seguridad de las instancias de Amazon RDS o en la política de cifrado de buckets de S3. Para obtener más información, consulte AWS CloudTrail nombres de eventos compatibles con AWS Audit Manager. 3. Los datos de configuración se refieren a la captura una instantánea de la configuración de los recursos directamente de Servicio de AWS de forma diaria, semanal o mensual.

Tipo de evidencias	Descripción
	Los ejemplos de instantáneas de configuración incluyen las listas de rutas para las tablas de enrutamiento de VPC, la configuración de las copias de seguridad de instancias de Amazon RDS y la política de cifrado de buckets de S3. Para obtener más información, consulte AWS Las llamadas a la API son compatibles con AWS Audit Manager.
Evidencia manual	Se trata de la evidencia que usted mismo añade a Audit Manager. Hay tres maneras de añadir sus propias evidencias: 1. Importar un archivo desde Amazon S3 2. Cargar un archivo desde el navegador 3. Escribir el texto de respuesta a las preguntas de evaluación de riesgos. Para obtener más información, consulte Añadir evidencia manual AWS Audit Manager.

La recopilación automática de evidencias comienza cuando se crea una evaluación. Se trata de un proceso continuo, durante el cual Audit Manager recopila evidencias a diferentes frecuencias según el tipo de evidencias y el origen de datos subyacente. Para obtener más información, consulte Entender cómo se AWS Audit Manager recopilan las pruebas.

Para obtener instrucciones acerca de cómo revisar las evidencias de una evaluación, consulte Revisar la evidencia en AWS Audit Manager.

Origen de evidencias

Un origen de evidencias define de dónde un control recopila evidencias. Puede ser un origen de datos individual o una agrupación predefinida de orígenes de datos que se asigna a un control común o a un control principal.

Al crear un control personalizado, puede recopilar evidencias de orígenes administrados por AWS , por los clientes o por ambos.

> **Tip**
>
> Le recomendamos que utilice fuentes AWS gestionadas. Cada vez que se actualiza una fuente AWS gestionada, las mismas actualizaciones se aplican automáticamente a todos los controles personalizados que utilizan estas fuentes. Esto significa que los controles personalizados siempre recopilan evidencias comparándolas con las definiciones más recientes de ese origen de evidencias. Esto le ayuda a garantizar la conformidad continua a medida que cambia el entorno de conformidad de la nube.

Consulte también: AWS managed source, customer managed source.

Métodos de recopilación de evidencias

Las evaluaciones pueden recopilar evidencias de dos maneras distintas.

Métodos de recopilación de evidencias	Descripción
Automatizado	Los controles automatizados recopilan automáticamente pruebas de las fuentes de AWS datos. Las evidencias automatizadas pueden ayudarle a demostrar el cumplimiento total o parcial de las evaluaciones.
Manual	Los controles manuales requieren que cargue sus propias evidencias para demostrar la conformidad con las mismas.

> **Note**
>
> Puede agregar evidencias manuales a cualquier evaluación automatizada. En muchos casos, es necesaria una combinación de evidencias automatizadas y manuales para demostrar el pleno cumplimiento de una evaluación. Si bien Audit Manager puede proporcionar evidencias automatizadas útiles y relevantes, es posible que algunas de ellas solo demuestren un cumplimiento parcial. En este caso, puede complementar las evidencias automatizadas de proporciona Audit Manager con sus propias evidencias. Por ejemplo:

- En el marco de AWS Marco generativo de mejores prácticas de IA, versión 2 se incluye un control denominado `Error analysis`. Deberá identificar cuándo se detectan imprecisiones en el uso del modelo y realizar un análisis exhaustivo de los errores para comprender las causas de los mismos y tomar las medidas correctivas apropiadas.
- Para respaldar este control, Audit Manager recopila pruebas automatizadas que muestran si CloudWatch las alarmas están activadas en el Cuenta de AWS lugar donde se ejecuta la evaluación. Puede utilizar estas evidencias para demostrar el cumplimiento parcial de la evaluación comprobando que sus alarmas y comprobaciones están configuradas correctamente.
- Para demostrar el pleno cumplimiento, puede complementar las evidencias automatizadas con evidencias manuales. Por ejemplo, puede subir una política o un procedimiento que muestre su proceso de análisis de errores, sus umbrales de escalado y generación de informes, y los resultados del análisis de la causa principal. Puede utilizar las evidencias de este manual para demostrar que hay políticas establecidas y que se tomaron medidas correctivas cuando se le solicitó.

Para ver un ejemplo más detallado, consulte Controles con orígenes de datos mixtos.

Destinos de exportación

Los destinos de exportación son los buckets S3 predeterminados, donde Audit Manager guarda los archivos que exporta desde el buscador de evidencias. Para obtener más información, consulte Configuración del destino de la exportación predeterminada para el buscador de evidencias.

F

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | T | U | V | W | X | Y | Z

Marcos

Un marco de Audit Manager estructura y automatiza las evaluaciones para un estándar o un principio de control de riesgos específicos. Estos marcos incluyen un conjunto de controles prediseñados o definidos por el cliente, y le ayudan a asignar sus AWS recursos a los requisitos de estos controles.

Hay dos tipos de marcos en Audit Manager.

Tipo de marco	Descripción
Marco estándar	Se trata de un marco prediseñado que se basa en las AWS mejores prácticas para diversas normas y reglamentos de conformidad. Puede utilizar marcos estándar para ayudar a preparar la auditoría de un estándar o normativa de conformidad específicos, como, por ejemplo, PCI DSS o HIPAA.
Marco personalizado	Se trata de un marco personalizado que usted define como usuario de Audit Manager. Puede utilizar marcos personalizados para preparar auditorías según sus requisitos específicos de GRC.

Para obtener instrucciones acerca de cómo crear y administrar marcos, consulte Uso de la biblioteca de marcos para administrar marcos en AWS Audit Manager.

> **Note**
>
> AWS Audit Manager ayuda a recopilar pruebas relevantes para verificar el cumplimiento de normas y reglamentos de cumplimiento específicos. Sin embargo, no evalúa el cumplimiento en sí mismo. AWS Audit Manager Por lo tanto, es posible que las pruebas recopiladas no incluyan toda la información sobre su AWS uso que se necesita para las auditorías. AWS Audit Manager no sustituye a los asesores legales ni a los expertos en cumplimiento.

Uso compartido de marcos

Puede usar la Compartir un marco personalizado en AWS Audit Manager función para compartir rápidamente sus marcos personalizados en todas Cuentas de AWS las regiones. Para compartir un marco personalizado, debe crear una solicitud de uso compartido. El destinatario tiene entonces 120 días para aceptar o rechazar la solicitud. Una vez aceptada, Audit Manager replicará el marco de trabajo personalizado compartido en su biblioteca de marcos. Además de replicar el marco de trabajo personalizado, Audit Manager también replicará todos los conjuntos de controles personalizados y los controles que formen parte de ese marco. Posteriormente,

dichos controles personalizados se agregan a la biblioteca de controles del destinatario. Audit Manager no replica los marcos o controles estándar. Esto se debe a que estos recursos ya están disponibles de forma predeterminada en cada cuenta y región.

I

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | T | U | V | W | X | Y | Z

Evidencia no concluyente

AWS Audit Manager califica las pruebas como no concluyentes cuando no es posible realizar una evaluación automática del cumplimiento. Esto podría darse en las siguientes situaciones:

- No has activado AWS Config o AWS Security Hub, cuáles son las fuentes de datos clave.
- Las pruebas se recopilan directamente de AWS los servicios mediante llamadas a la API, AWS CloudTrail registros o cargas manuales.

Cuando no existe un mecanismo para la evaluación automática de esta evidencia, no AWS Audit Manager puede proporcionar detalles de la evaluación. Como resultado, marca la evidencia como inconclusa.

> **Important**
>
> La evidencia no concluyente no indica un fracaso. Por el contrario, indica que es necesario evaluar manualmente las pruebas de conformidad.

R

| B | | | | G | H | | J | K | L | M | N | O | P | Q | | T | U | V | W | X | Y | Z

Recursos

Los recursos son activos físico o de información que se evalúan en una auditoría. Entre los ejemplos de AWS recursos se incluyen EC2 las instancias de Amazon, las instancias de Amazon RDS, los buckets de Amazon S3 y las subredes de Amazon VPC.

Evaluación de recursos

Las evaluaciones de recursos son los procesos mediante los cuales se evalúa un recurso. y se basan en requisitos de control. Mientras una evaluación está activa, Audit Manager evalúa cada

uno de los recursos que forman parte de la evaluación. Las evaluaciones de recursos ejecutan las tareas siguientes:

1. Recopilación de evidencias, incluidas las configuraciones de los recursos, los registros de eventos y los hallazgos
2. Traducción y asignación de las evidencias a los controles
3. Almacenamiento y rastreo del linaje de las evidencias para garantizar su integridad.

Conformidad de los recursos

El cumplimiento de los recursos se refiere al estado de evaluación de un recurso que se evaluó al recopilar las evidencias de verificación de cumplimiento.

Audit Manager recopila pruebas de verificación de conformidad para los controles que utilizan AWS Config Security Hub como tipo de fuente de datos. Es posible que se evalúen varios recursos durante la recopilación de evidencias. En consecuencia, una sola evidencia de verificación de conformidad puede incluir uno o más recursos.

Utilice el filtro de cumplimiento de los recursos del buscador de evidencias para conocer el estado de cumplimiento a nivel de recursos. Una vez completada la búsqueda, puede obtener una vista previa de los recursos que coinciden con su consulta de búsqueda.

En el buscador de evidencias, hay tres valores posibles que determinan el cumplimiento de los recursos:

Valor	Descripción
No conforme	Hace referencia a los recursos con problemas de comprobaciones de conformidad. Esto sucede si Security Hub informa de un resultado de error para el recurso o si AWS Config informa de un resultado no conforme.
Conforme	Hace referencia a los recursos que no tienen problemas de comprobaciones de conformidad. Esto sucede si Security Hub informa de un resultado de aprobación para el recurso o si AWS Config informa de un resultado de conformidad.
No concluyen te	Hace referencia a los recursos para los que una comprobación de conformid ad no está disponible ni se puede aplicar.

Valor	Descripción
	Esto ocurre AWS Config si el tipo de fuente de datos subyacente es Security Hub, pero esos servicios no están habilitados. Esto también ocurre si el tipo de fuente de datos subyacente no admite las comprobaciones de conformidad (como las pruebas manuales, las llamadas a la AWS API o CloudTrail).

S

| B | | | | | G | H | | J | K | L | M | N | O | P | P | Q | | T | U | V | W | X | Y | Z

Servicio incluido

Audit Manager gestiona cuáles Servicios de AWS están dentro del alcance de sus evaluaciones. Si tiene una evaluación anterior, es posible que haya especificado manualmente los servicios incluidos en el pasado. A partir del 4 de junio de 2024, no se podrá especificar ni editar manualmente los servicios incluidos.

Un servicio incluido en el ámbito de aplicación es Servicio de AWS aquel sobre el que su evaluación recopila pruebas. Cuando un servicio se incluye en la evaluación, Audit Manager evaluará los recursos de dicho servicio. como, por ejemplo los siguientes:

- Una EC2 instancia de Amazon
- Un bucket de S3
- Un usuario o rol de IAM
- Una tabla de DynamoDB
- Un componente de red, como una nube privada virtual (VPC) de Amazon, un grupo de seguridad o una lista de control de acceso (ACL).

Por ejemplo, si Amazon S3 es un servicio incluido, Audit Manager puede recopilar evidencias sobre los buckets de S3. Las evidencias exactas que se recopilan dependen del data source de un control. Por ejemplo, si el tipo de fuente de datos es AWS Config y el mapeo de la fuente de datos es una AWS Config regla (por ejemplos`3-bucket-public-write-prohibited`), Audit Manager recopila el resultado de la evaluación de esa regla como evidencia.

> **Note**
>
> Tenga en cuenta que el alcance de un servicio es diferente al de un tipo de fuente de datos, que también puede ser un tipo de fuente de datos Servicio de AWS o algo diferente. Para obtener más información, consulte ¿Cuál es la diferencia entre un servicio incluido y un tipo de origen de datos? en la sección Solución de problemas de la guía.

Control estándar

Consulte control.

Entender cómo se AWS Audit Manager recopilan las pruebas

Cada evaluación activa recopila AWS Audit Manager automáticamente evidencia de una variedad de fuentes de datos. En cada evaluación, usted define para qué Cuentas de AWS Audit Manager recopilará las pruebas y Audit Manager gestionará cuáles Servicios de AWS están dentro del ámbito de aplicación. Cada uno de estos servicios y cuentas incluye varios recursos que utiliza y que son de su propiedad. La recopilación de evidencias en Audit Manager implica evaluar cada uno de los recursos incluidos. Esto se conoce como evaluación de recursos.

Los siguientes pasos describen cómo Audit Manager recopila las evidencias para las evaluaciones de recursos:

1. Evaluar un recurso a partir del origen de datos

Para iniciar la recopilación de evidencias, Audit Manager evalúa los recursos internos a partir de un origen de datos. Para ello, captura una instantánea de la configuración, el resultado de una comprobación de conformidad relacionada o la actividad de los usuarios. A continuación, ejecuta un análisis para determinar qué control admiten estos datos. Luego, se guarda el resultado de la evaluación de los recursos y se convierte en evidencia. Para obtener más información sobre los diferentes tipos de evidencias, consulte evidence en la sección Conceptos y terminología de AWS Audit Manager de esta guía.

2. Pasos para convertir los resultados de la evaluación en evidencia

El resultado de las evaluaciones de un recurso incluye tanto los datos originales del recurso que se capturaron como los metadatos que indican qué control admiten los datos. Audit Manager convierte los datos originales a un formato fácil de usar para los auditores. A continuación, los datos

y metadatos convertidos se guardan como evidencia de Audit Manager antes de agregarlos a un control.

3. Cómo agregar evidencias al control correspondiente

Audit Manager lee los metadatos de las evidencias. y agregas las evidencias guardadas a un control relacionado dentro de la evaluación. Las evidencias agregadas se hacen visibles en Audit Manager, y así se completa el ciclo de las evaluaciones de recursos.

> **Note**
>
> En algunos casos, se puede agregar la misma evidencia a varios controles de varias evaluaciones de Audit Manager según la configuración de control. Cuando se agrega la misma evidencia a varios controles, Audit Manager mide la evaluación de los recursos exactamente una vez. Esto se debe a que la misma evidencia se recopila exactamente una sola vez. Sin embargo, un control de una evaluación de Audit Manager puede tener múltiples evidencias de múltiples orígenes de datos.

Frecuencia de recolección de evidencias

La recopilación de evidencias es un proceso continuo que comienza cuando se crea la evaluación. Audit Manager recopila evidencias de varios orígenes de datos con diferentes frecuencias. Como resultado, no hay one-size-fits-all respuesta sobre la frecuencia con la que se recopilan las pruebas. Depende del tipo y el origen de datos, como se describe a continuación.

- Comprobaciones de cumplimiento: Audit Manager recopila este tipo de evidencia de AWS Security Hub y AWS Config.
  - En el caso de Security Hub, la recopilación de evidencias sigue la planificación de las comprobaciones de Security Hub. Para más información sobre la programación de las comprobaciones de Security Hub, consulte Programación para la ejecución de las comprobaciones de seguridad en la AWS Security Hub Guía del usuario. Para más información sobre las comprobaciones de Security Hub compatibles con Audit Manager, consulte AWS Security Hub controles compatibles con AWS Audit Manager.
  - Pues AWS Config, la recopilación de pruebas sigue los factores desencadenantes que se definen en sus AWS Config reglas. Para más información sobre los desencadenadores de las reglas de AWS Config , consulte los tipos de desencadenadores en la Guía del usuario de

AWS Config . Para obtener más información sobre los Reglas de AWS Config que admite Audit Manager, consulteReglas de AWS Config con el apoyo de AWS Audit Manager.

- AWS Audit Manager marca las pruebas como no concluyentes cuando no es posible realizar una evaluación automática del cumplimiento. Esto ocurre cuando no has activado AWS Config o AWS Security Hub, cuáles son las fuentes de datos clave. También ocurre cuando las pruebas se recopilan directamente de AWS los servicios mediante llamadas a la API, AWS CloudTrail registros o cargas manuales. Cuando no existe un mecanismo para la evaluación automática de estas pruebas, no AWS Audit Manager puede proporcionar los detalles de la evaluación. Como resultado, marca la evidencia como inconclusa. La evidencia no concluyente no indica un fracaso. Por el contrario, indica que es necesario evaluar manualmente las pruebas de conformidad.

- Actividad del usuario: Audit Manager recopila este tipo AWS CloudTrail de evidencia de forma continua. En este caso la frecuencia es continua porque la actividad del usuario puede ocurrir en cualquier momento del día. Para obtener más información, consulte AWS CloudTrail nombres de eventos compatibles con AWS Audit Manager.
- Datos de configuración: Audit Manager recopila este tipo de evidencia mediante una llamada de API de descripción a otra, Servicio de AWS como Amazon EC2, Amazon S3 o IAM. Puede determinar las acciones de la API a las que desea llamar. También puede configurar la frecuencia como diaria, semanal o mensual en Audit Manager. al crear o editar un control en la biblioteca de controles. Para obtener instrucciones sobre cómo crear y configurar un control, consulte Uso de la biblioteca de controles para gestionar los controles en AWS Audit Manager. Para obtener más información sobre las llamadas a la API compatibles con Audit Manager, consulte AWS Las llamadas a la API son compatibles con AWS Audit Manager.

Independientemente de la frecuencia de recopilación de evidencias para el origen de datos, las nuevas evidencias se recopilarán automáticamente mientras el control y la evaluación estén activos.

Ejemplos de controles AWS Audit Manager

Consulte los ejemplos de esta página para obtener más información sobre cómo funcionan los controles en AWS Audit Manager.

En Audit Manager, los controles pueden recopilar automáticamente evidencias de cuatro tipos de orígenes de datos:

1. AWS CloudTrail— Capture la actividad de los usuarios de sus CloudTrail registros e impórtela como evidencia de la actividad del usuario
2. AWS Security Hub: permite recopilar los resultados de Security Hub e importarlos como evidencia de la comprobación de conformidad.
3. AWS Config: permite recopilar las evaluaciones de las reglas de AWS Config e importarlas como evidencia de la comprobación de conformidad.
4. AWS Llamadas a la API: capture una instantánea de un recurso a partir de una llamada a la API e impórtela como prueba de los datos de configuración

Tenga en cuenta que algunos controles recopilan evidencias mediante agrupaciones predefinidas de estos orígenes de datos. Estas agrupaciones de orígenes de datos se conocen como orígenes administrados por AWS. Cada fuente AWS gestionada representa un control común o un control central. Estos orígenes administrados le proporcionan una forma eficaz de asignar sus requisitos de conformidad a un grupo pertinente de orígenes de datos subyacentes, validados y mantenidos por evaluadores certificados del sector en AWS.

Los ejemplos incluidos en esta página muestran cómo los controles recopilan evidencias de cada uno de los tipos de orígenes de datos individuales. Estos ejemplos muestran el aspecto de un control, cómo Audit Manager recopila evidencias del origen de datos y los siguientes pasos que puede dar para demostrar conformidad.

> **Tip**
>
> Le recomendamos que active AWS Config Security Hub para disfrutar de una experiencia óptima en Audit Manager. Al habilitar estos servicios, Audit Manager puede utilizar las conclusiones de Security Hub y Reglas de AWS Config generar pruebas automatizadas.
>
> - Una vez que AWS Security Hub estén habilitados, asegúrese de activar también todos los estándares de seguridad y de activar la configuración de los hallazgos de control consolidados. Así se asegurará de que Audit Manager pueda importar los resultados de todos los estándares de conformidad compatibles.
> - Una vez AWS Config habilitados, asegúrese de habilitar también el paquete de conformidad correspondiente Reglas de AWS Config o implementar un paquete de conformidad para el estándar de cumplimiento relacionado con su auditoría. Este paso garantiza que Audit Manager pueda importar las conclusiones de todos los soportes Reglas de AWS Config que haya activado.

Consulte los ejemplos disponibles para cada uno de los siguientes tipos de controles a continuación:

Temas

- Controles automatizados que AWS Security Hub se utilizan como tipo de fuente de datos
- Controles automatizados que AWS Config se utilizan como tipo de fuente de datos
- Controles automatizados que utilizan las llamadas a la AWS API como tipo de fuente de datos
- Controles automatizados que AWS CloudTrail se utilizan como tipo de fuente de datos
- Controles manuales
- Controles con distintos tipos de orígenes de datos (automatizados y manuales)

Controles automatizados que AWS Security Hub se utilizan como tipo de fuente de datos

En este ejemplo se muestra un control que se utiliza AWS Security Hub como tipo de fuente de datos. Se trata de un control estándar tomado del marco de AWS prácticas recomendadas de seguridad fundamentales (FSBP). Audit Manager utiliza este control para generar pruebas que pueden ayudar a alinear su AWS entorno con los requisitos del FSBP.

Ejemplo de detalles de control

- Nombre del control: `FSBP1-012: AWS Config should be enabled`
- Conjunto de controles: `Config` Se trata de una agrupación de controles de FSBP específica de un marco y relacionada con la administración de la configuración.
- Origen de evidencias: orígenes de datos individuales
- Tipo de fuente de datos: AWS Security Hub
- Tipo de evidencia: comprobaciones de conformidad

En el siguiente ejemplo, este control se encuentra en una evaluación de Audit Manager que se creó a partir del marco de FSBP.

La evaluación muestra el estado del control. También muestra el número de evidencias recopiladas para este control hasta el momento. A partir de este punto puede delegar la revisión del conjunto de controles o completar la revisión por su cuenta. Al elegir el nombre del control se abrirá una página de detalles con más información, incluidas las evidencias del control.

Cómo funciona el control

Este control requiere que AWS Config esté habilitado en todos los Regiones de AWS lugares donde utilice Security Hub. Audit Manager puede usar este control para comprobar si lo ha activado AWS Config.

Cómo recopila Audit Manager las evidencias para el control

Audit Manager sigue los pasos que se detallan a continuación para recopilar evidencias para el control:

1. Para cada control, Audit Manager evalúa los recursos incluidos. Para ello, utiliza el origen de datos que se especifica en la configuración del control. En este ejemplo, la AWS Config configuración es el recurso y Security Hub es el tipo de fuente de datos. Audit Manager busca el resultado de una comprobación específica de Security Hub ([Config.1]).
2. El resultado de la evaluación de los recursos se guarda y se convierte en evidencias de fácil acceso para el auditor. Audit Manager genera evidencias de verificación de conformidad para los controles que utilizan Security Hub como tipo de origen de datos. Esta evidencia contiene el resultado de las comprobaciones de conformidad notificado directamente desde Security Hub.
3. Audit Manager agrega las evidencias guardadas al control de la evaluación denominado “`FSBP1-012: AWS Config should be enabled`”.

Cómo puede utilizar Audit Manager para demostrar la conformidad del control

Una vez agregadas las evidencias al control, usted (o un delegado de su elección) puede revisarlas para ver si es necesaria alguna corrección.

En este ejemplo, Audit Manager puede mostrar una regla de error de Security Hub. Esto puede suceder si no lo ha activado AWS Config. En este caso, puede tomar la medida correctiva de habilitarla AWS Config, lo que ayuda a adaptar su AWS entorno a los requisitos del FSBP.

Cuando su AWS Config configuración esté en línea con la del control, márquelo como Revisado y añada la evidencia al informe de evaluación. A continuación puede compartir este informe con los auditores para mostrar que el control funciona según lo previsto.

Controles automatizados que AWS Config se utilizan como tipo de fuente de datos

En este ejemplo se muestra un control que se utiliza AWS Config como tipo de fuente de datos. Se trata de un control estándar tomado del AWS Control Tower marco de barreras de protección. Audit Manager usa este control para generar evidencia que ayude a alinear su AWS entorno con AWS Control Tower Guardrails.

Ejemplo de detalles de control

- Nombre del control: `CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets`
- Conjunto de controles: este control pertenece al conjunto de controles de `Disallow public access`. Se trata de una agrupación de controles relacionados con la administración de accesos.
- Origen de evidencias: origen de datos individual
- Tipo de fuente de datos: AWS Config
- Tipo de evidencia: comprobaciones de conformidad

En el siguiente ejemplo, este control aparece en una evaluación de Audit Manager que se creó a partir del marco AWS Control Tower Guardrails.

La evaluación muestra el estado del control. También muestra el número de evidencias recopiladas para este control hasta el momento. A partir de este punto puede delegar la revisión del conjunto de

controles o completar la revisión por su cuenta. Al elegir el nombre del control se abrirá una página de detalles con más información, incluidas las evidencias del control.

Cómo funciona el control

Audit Manager puede usar este control para comprobar si los niveles de acceso de sus políticas de bucket de S3 son demasiado flexibles para cumplir con los requisitos AWS Control Tower . En concreto, puede comprobar la configuración de bloqueo de acceso público, las políticas de los buckets y las listas de control de acceso (ACL) a los buckets para confirmar que los buckets no permiten el acceso público de escritura.

Cómo recopila Audit Manager las evidencias para el control

Audit Manager sigue los pasos que se detallan a continuación para recopilar evidencias para el control:

1. Para cada control, Audit Manager evalúa los recursos incluidos en el ámbito utilizando el origen de datos que se especifica en la configuración del control. En este caso, los depósitos de S3 son el recurso y, AWS Config , el tipo de origen de datos. Audit Manager busca el resultado de una AWS Config regla específica (s3- bucket-public-write-prohibited) para evaluar la configuración, la política y la ACL de cada uno de los buckets de S3 que están dentro del ámbito de su evaluación.
2. El resultado de la evaluación de los recursos se guarda y se convierte en evidencias de fácil acceso para el auditor. Audit Manager genera evidencia de verificación de conformidad para los controles que AWS Config se utilizan como tipo de fuente de datos. Esta evidencia contiene el resultado de la verificación de conformidad informado directamente desde AWS Config.
3. Audit Manager agrega las evidencias guardadas al control de la evaluación denominado “`CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets`”.

Cómo puede utilizar Audit Manager para demostrar la conformidad del control

Una vez agregadas las evidencias al control, usted (o un delegado de su elección) puede revisarlas para ver si es necesaria alguna corrección.

En este ejemplo, Audit Manager podría mostrar una sentencia que AWS Config indique que un bucket de S3 no es compatible. Esto puede ocurrir si uno de sus buckets de S3 tiene una configuración de bloqueo de acceso público que no restringe las políticas públicas y la política que está en uso permite el acceso de escritura público. Para remediarlo, puede actualizar la configuración Bloquear el acceso público para restringir las políticas públicas. Otra opción es usar

una política de bucket diferente que no permita el acceso de escritura público. Esta acción correctiva ayuda a alinear su AWS entorno con AWS Control Tower los requisitos.

Compruebe que los niveles de acceso al bucket de S3 concuerdan con los del control, marque el control como revisado y añada las evidencias a su informe de evaluación. A continuación puede compartir este informe con los auditores para mostrar que el control funciona según lo previsto.

Controles automatizados que utilizan las llamadas a la AWS API como tipo de fuente de datos

En este ejemplo, se muestra un control personalizado que usa llamadas a la AWS API como tipo de fuente de datos. Audit Manager utiliza este control para generar pruebas que pueden ayudar a adaptar su AWS entorno a sus requisitos específicos.

Ejemplo de detalles de control

- Nombre del control: `Password Use`
- Conjunto de controles: este control pertenece a un conjunto de controles denominado “`Access Control`”. Se trata de un grupo de controles relacionados con la administración de identidades y accesos.
- Origen de evidencias: origen de datos individual
- Tipo de fuente de datos: llamadas a AWS la API
- Tipo de evidencia: datos de configuración

En el siguiente ejemplo este control aparece en una evaluación de Audit Manager creada a partir de un marco personalizado.

La evaluación muestra el estado del control. También muestra el número de evidencias recopiladas para este control hasta el momento. A partir de este punto puede delegar la revisión del conjunto de controles o completar la revisión por su cuenta. Al elegir el nombre del control se abrirá una página de detalles con más información, incluidas las evidencias del control.

Cómo funciona el control

Audit Manager puede utilizar este control personalizado para ayudarle a garantizar que cuenta con políticas de control de acceso suficientes. Este control requiere que siga las buenas prácticas de seguridad en la selección y el uso de las contraseñas. Audit Manager puede resultar útil a la hora de obtener una lista de todas las políticas de contraseñas de los directores de IAM que se incluyen en su evaluación.

Cómo recopila Audit Manager las evidencias para el control

Audit Manager sigue los pasos que se detallan a continuación para recopilar evidencias para los controles personalizados:

1. Para cada control, Audit Manager evalúa los recursos incluidos en el ámbito utilizando el origen de datos que se especifica en la configuración del control. En este caso, los principales de IAM son los recursos y las llamadas a la AWS API son el tipo de fuente de datos. Audit Manager busca la respuesta de una llamada a la API de IAM específica (GetAccountPasswordPolicy). A continuación, devuelve las políticas de contraseñas de Cuentas de AWS que se evalúan.
2. El resultado de la evaluación de los recursos se guarda y se convierte en evidencias de fácil acceso para el auditor. Audit Manager genera evidencias de datos de configuración para los controles que utilizan llamadas a la API como origen de datos. Esta evidencia contiene los datos originales que se capturan de las respuestas de la API y metadatos adicionales que indican qué control admiten los datos.
3. Audit Manager agrega la evidencia o evidencias guardadas al control personalizado de la evaluación que se denomina “`Password Use`”.

Cómo puede utilizar Audit Manager para demostrar la conformidad del control

Una vez agregadas las evidencias al control, usted (o un delegado de su elección) podrá revisarlas para comprobar si son suficientes o si es necesario corregirlas.

En este ejemplo, puede revisar las evidencias para ver la respuesta de la llamada a la API. La GetAccountPasswordPolicyrespuesta describe los requisitos de complejidad y los períodos de rotación obligatorios de las contraseñas de usuario de su cuenta. Puede utilizar esta respuesta de la API como prueba para demostrar que cuenta con políticas de control de acceso mediante contraseñas suficientes para las Cuentas de AWS que se incluyen en el ámbito de su evaluación. Si lo desea, también puede hacer comentarios adicionales sobre estas políticas añadiendo anotaciones al control.

Compruebe que las políticas de contraseñas de sus directores de IAM se ajustan al control personalizado, marque el control como revisado y añada las evidencias a su informe de evaluación. A continuación puede compartir este informe con los auditores para mostrar que el control funciona según lo previsto.

Controles automatizados que AWS CloudTrail se utilizan como tipo de fuente de datos

En este ejemplo se muestra un control que se utiliza AWS CloudTrail como tipo de fuente de datos. Se trata de un control estándar tomado del marco de HIPAA Security Rule 2003. Audit Manager lo utiliza para generar evidencias que pueden serle de utilidad para hacer que su entorno de AWS corresponda con los requisitos de la HIPAA.

Ejemplo de detalles de control

- Nombre del control: `164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)`
- Conjunto de controles: este control pertenece al conjunto de controles denominado "`Section 308`". Se trata de una agrupación de controles de HIPAA específica de un marco y relacionada con las medidas de protección administrativas.
- Fuente de evidencia: fuente AWS administrada (controles principales)
- Tipo de origen de datos subyacente: AWS CloudTrail
- Tipo de evidencia: actividad del usuario

Este control se muestra en una evaluación de Audit Manager creada a partir del marco de la HIPAA:

La evaluación muestra el estado del control. También muestra el número de evidencias recopiladas para este control hasta el momento. A partir de este punto puede delegar la revisión del conjunto de controles o completar la revisión por su cuenta. Al elegir el nombre del control se abrirá una página de detalles con más información, incluidas las evidencias del control.

Cómo funciona el control

Este control requiere que cuente con procedimientos de supervisión para detectar el acceso no autorizado. Un ejemplo de acceso no autorizado es cuando alguien inicia sesión en la consola sin que esté habilitada la autenticación multifactor (MFA). Audit Manager le ayuda a validar este control al proporcionar pruebas de que ha configurado Amazon CloudWatch para supervisar las solicitudes de inicio de sesión en la consola de administración en las que la MFA no está habilitada.

Cómo recopila Audit Manager las evidencias para el control

Audit Manager sigue los pasos que se detallan a continuación para recopilar evidencias para el control:

1. Para cada control, Audit Manager evalúa los recursos incluidos mediante los orígenes de evidencias que se especifican en la configuración del control. En este caso, el control utiliza varios controles principales como orígenes de evidencias.

   Cada control principal es una agrupación administrada de orígenes de datos individuales. En nuestro ejemplo, uno de estos controles principales (`Configure Amazon CloudWatch alarms to detect management console sign-in requests without MFA enabled`) utiliza un CloudTrail evento (`monitoring_EnableAlarmActions`) como fuente de datos subyacente.

   Audit Manager revisa sus CloudTrail registros y utiliza la `monitoring_EnableAlarmActions` palabra clave para encontrar las acciones de activación de CloudWatch alarmas que están registradas por CloudTrail. A continuación, devuelve un registro de los eventos relevantes detectados como resultado de la evaluación.
2. El resultado de la evaluación de los recursos se guarda y se convierte en evidencias de fácil acceso para el auditor. Audit Manager genera evidencia de actividad del usuario para los controles que CloudTrail se utilizan como tipo de fuente de datos. Esta evidencia contiene los datos originales que se capturaron de Amazon CloudWatch y metadatos adicionales que indican qué control admiten los datos.
3. Audit Manager agrega las evidencias guardadas al control de la evaluación denominado “`164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)`”.

Cómo puede utilizar Audit Manager para demostrar la conformidad del control

Una vez agregadas las evidencias al control, usted (o un delegado de su elección) puede revisarlas para ver si es necesaria alguna corrección.

En este ejemplo, puedes revisar las pruebas para ver los eventos de activación de alarmas que registró. CloudTrail Puede utilizar este registro como evidencia para demostrar que cuenta con suficientes procedimientos de supervisión para detectar los inicios de sesión en la consola sin tener habilitada la MFA. Si lo desea, también puede aportar comentarios adicionales agregando comentarios al control. Por ejemplo, si el registro muestra varios inicios de sesión sin la MFA, puede añadir un comentario que explique cómo solucionó el problema. La supervisión periódica de los inicios de sesión en la consola le será de utilidad para evitar problemas de seguridad que puedan derivarse de las discrepancias y de los intentos de inicio de sesión inadecuados. A su vez, esta mejor práctica ayuda a alinear su AWS entorno con los requisitos de la HIPAA.

Cuando compruebe que su procedimiento de monitoreo está en consonancia con el control puede marcar el control como revisado y agregar las evidencias al informe de evaluación. A continuación puede compartir este informe con los auditores para mostrar que el control funciona según lo previsto.

Controles manuales

Algunos controles no admiten la recopilación automática de evidencia. Esto incluye controles basados en el suministro de registros y firmas físicas, además de observaciones, entrevistas y otros eventos que no se generan en la nube. En estos casos puede cargar evidencias manualmente para demostrar que cumple con los requisitos del control.

En este ejemplo se muestra un control manual tomado del marco de NIST 800-53 (Rev. 5). Puede utilizar Audit Manager para cargar y almacenar evidencias que demuestren la conformidad del control.

Ejemplo de detalles de control

- Nombre del control: `AT-4: Training Records`
- Conjunto de controles: `(AT) Awareness and training` Se trata de una agrupación de controles de NIST específica de un marco y relacionada con el entrenamiento.
- Origen de evidencias: origen de datos individual
- Tipo de origen de datos: manual
- Tipo de evidencia: manual

Este es el control que se muestra en una evaluación de Audit Manager que se creó a partir del marco NIST 800-53 (Rev. 5): Low-Moderate-High

La evaluación muestra el estado del control. También muestra el número de evidencias recopiladas para este control hasta el momento. A partir de este punto puede delegar la revisión del conjunto de controles o completar la revisión por su cuenta. Al elegir el nombre del control se abrirá una página de detalles con más información, incluidas las evidencias del control.

Cómo funciona el control

Puede utilizar este control para garantizar que el personal reciba el nivel adecuado de entrenamiento en materia de seguridad y privacidad. En concreto, puede demostrar que ha documentado las actividades de entrenamiento en materia de seguridad y privacidad para todo el personal, en función de su rol. También puede demostrar que se conservan los registros de entrenamiento de cada empleado.

¿Cómo puedo cargar las evidencias de este control manualmente?

Para cargar pruebas manuales que complementen las pruebas automatizadas, consulte Carga de pruebas manuales en. AWS Audit Manager Audit Manager agrega la evidencia cargada al control de la evaluación llamada “`AT-4: Training Records`”.

Cómo puede utilizar Audit Manager para demostrar la conformidad del control

Si tiene documentación que respalde este control, puede cargarla como evidencia manual. Por ejemplo, puede cargar la copia más reciente de los materiales de entrenamiento obligatorios basados en roles que el departamento de Recursos Humanos expide a los empleados.

Al igual que con los controles automatizados, puede delegar los controles manuales en las partes interesadas, quienes pueden ayudarle a revisar las evidencias (o, en este caso, a proporcionarlas). Por ejemplo, al revisar este control, es posible que se dé cuenta de que solo cumple parcialmente sus requisitos. Este podría ser el caso si no tiene ninguna copia de registros de asistencia a los entrenamientos presenciales. Puede delegar el control en una parte interesada de Recursos Humanos, que luego podrá cargar una lista de los empleados que asistieron al entrenamiento.

Cuando confirme que está de acuerdo con el control, puede marcarlo como revisado y añadir las evidencias al informe de evaluación. A continuación puede compartir este informe con los auditores para mostrar que el control funciona según lo previsto.

Controles con distintos tipos de orígenes de datos (automatizados y manuales)

En muchos casos, se necesita una combinación de evidencias automatizadas y manuales para cumplir con un control. Si bien Audit Manager puede proporcionar evidencias automatizadas que sean relevantes para el control, es posible que deba complementar estos datos con evidencias manuales que identifique y cargará manualmente

En este ejemplo se muestra un control que utiliza una combinación de evidencias manuales y evidencias automatizadas. Se trata de un control estándar tomado del marco NIST 800-53 (Rev. 5). Audit Manager utiliza este control para generar evidencias que pueden ayudar a adaptar su AWS entorno de acuerdo con los requisitos del NIST.

Ejemplo de detalles de control

- Nombre del control: `Personnel Termination`
- Conjunto de controles: `(PS) Personnel Security (10)` Se trata de una agrupación de controles de NIST específica de un marco y relacionada con los empleados que realizan el mantenimiento del hardware o el software de los sistemas de la organización.
- Fuente de evidencia: fuentes de datos AWS gestionadas (controles básicos) e individuales (manual)
- Tipo de fuente de datos subyacente: llamadas a la AWS API AWS CloudTrail, AWS Config, manual
- Tipo de evidencia: datos de configuración, actividad del usuario, comprobación de conformidad, evidencia manual

Este es el control que se muestra en una evaluación de Audit Manager que se creó a partir del marco NIST 800-53 (Rev. 5):

La evaluación muestra el estado del control. También muestra el número de evidencias recopiladas para este control hasta el momento. A partir de este punto puede delegar la revisión del conjunto de controles o completar la revisión por su cuenta. Al elegir el nombre del control se abrirá una página de detalles con más información, incluidas las evidencias del control.

Cómo funciona el control

Puede usar este control para confirmar que está protegiendo la información de la organización en caso de despido de un empleado. En concreto, puede demostrar que deshabilitó el acceso al sistema y revocó las credenciales del empleado. Además, puede demostrar que todos los empleados despedidos participaron en una entrevista de fin de servicio que incluyó una conversación sobre los protocolos de seguridad pertinentes para su organización o empresa.

Cómo recopila Audit Manager las evidencias para el control

Audit Manager sigue los pasos que se detallan a continuación para recopilar evidencias para el control:

1. Para cada control, Audit Manager evalúa los recursos incluidos mediante los orígenes de evidencias que se especifican en la configuración del control.

   En este caso, el control utiliza varios controles principales como orígenes de evidencias. A su vez, cada uno de estos controles principales recopila evidencia relevante de fuentes de datos individuales (llamadas a la AWS API AWS CloudTrail, y AWS Config). Audit Manager utiliza estos tipos de fuentes de datos para evaluar sus recursos de IAM (como grupos, claves y políticas) con respecto a las llamadas, CloudTrail eventos y AWS Config reglas de API relevantes.
2. El resultado de la evaluación de los recursos se guarda y se convierte en evidencias de fácil acceso para el auditor. Esta evidencia incluye los datos originales que se capturan de cada origen de datos, así como los metadatos adicionales que indican qué control admite esos datos.
3. Audit Manager agrega las evidencias guardadas al control de la evaluación denominado “`Personnel Termination`”.

¿Cómo puedo cargar las evidencias de este control manualmente?

Para cargar pruebas manuales que complementen las pruebas automatizadas, consulte Carga de pruebas manuales en. AWS Audit Manager Audit Manager agrega la evidencia cargada al control de la evaluación llamada “`Personnel Termination`”.

Cómo puede utilizar Audit Manager para demostrar la conformidad del control

Una vez agregadas las evidencias al control, usted (o un delegado de su elección) podrá revisarlas para comprobar si son suficientes o si es necesario corregirlas. Por ejemplo, al revisar este control, es posible que se dé cuenta de que solo cumple parcialmente sus requisitos. Este podría ser el caso si tiene pruebas de que se revocó el acceso, pero no tiene ninguna copia de entrevistas de fin de servicio. Puede delegar el control en una parte interesada de Recursos Humanos, que luego podrá subir una copia de la documentación con las entrevistas de fin de servicio. O bien, si no se despidió a ningún empleado durante el período de auditoría, puede dejar un comentario en el que se explique por qué no se ha asociado documentación firmada al control.

Confirme que está de acuerdo con el control, márquelo como revisado y añada las evidencias al informe de evaluación. A continuación puede compartir este informe con los auditores para mostrar que el control funciona según lo previsto.

Usando AWS Audit Manager

Puede acceder a AWS Audit Manager través de varias opciones, según sus necesidades y preferencias específicas. Estas son algunas formas diferentes en las que puede interactuar con Audit Manager:

- Consola de Audit Manager

  Acceda a la consola Audit Manager directamente desde su https://console.aws.amazon.com/auditmanager/casa, que proporciona una interfaz fácil de usar para gestionar sus auditorías y los recursos relacionados.

- API de Audit Manager

  Interactúe con Audit Manager mediante programación a través de la API de Audit Manager, lo que le permitirá automatizar e integrar las tareas en los flujos de trabajo existentes. Para obtener más información, consulte la Referencia de la API de AWS Audit Manager .

- AWS SDKs

  Utilice kits de desarrollo de AWS software (SDKs) para interactuar con Audit Manager mediante programación, lo que le permitirá escribir código en varios lenguajes de programación. Para obtener más información, consulte AWS Audit Manager Utilizándolo con un AWS SDK.

- AWS CloudFormation

Cree recursos de Audit Manager utilizando AWS CloudFormation, lo que le permitirá definir e implementar su infraestructura de auditoría como código. Para obtener más información, consulte Creación de recursos de AWS Audit Manager con AWS CloudFormation.

- Integraciones de terceros

  Integre Audit Manager con productos de gobernanza, riesgo y conformidad (GRC) de terceros compatibles, lo que le permitirá sacar partido de las herramientas y los procesos de GRC existentes. Para obtener más información, consulte Integraciones con productos de terceros de GRC.

- Integraciones con su propio sistema GRC

  Incorpore las evidencias de Audit Manager en su propio sistema de GRC, lo que le permitirá enviar las evidencias directamente desde Audit Manager a la aplicación de GRC. Para obtener más información, consulte Integración de las evidencias de Audit Manager en el sistema de GRC.

AWS Audit Manager Utilizándolo con un AWS SDK

AWS los kits de desarrollo de software (SDKs) están disponibles para muchos lenguajes de programación populares. Cada SDK proporciona una API, códigos de ejemplo y documentación que los desarrolladores puede usar para crear aplicaciones en el lenguaje que prefieran.

Documentación de SDK	Documentación específica de Audit Manager	Ejemplos de código
AWS SDK para C++	AWS SDK para C++ Referencia de API para Audit Manager	AWS SDK para C++ ejemplos de código
AWS SDK para Go	AWS SDK para Go Referencia de API para Audit Manager	AWS SDK para Go ejemplos de código
AWS SDK para Java	AWS SDK for Java 2.x Referencia de API para Audit Manager	AWS SDK para Java ejemplos de código
AWS SDK para JavaScript	AWS SDK para JavaScript Referencia de API para Audit Manager	AWS SDK para JavaScript ejemplos de código

Documentación de SDK	Documentación específica de Audit Manager	Ejemplos de código
AWS SDK para .NET	AWS SDK para .NET Referencia de API para Audit Manager	AWS SDK para .NET ejemplos de código
AWS SDK para PHP	AWS SDK para PHP Referencia de API para Audit Manager	AWS SDK para PHP ejemplos de código
AWS SDK para Python (Boto3)	AWS SDK for Python (Boto) Referencia de API para Audit Manager	AWS SDK para Python (Boto3) ejemplos de código
AWS SDK para Ruby	AWS SDK para Ruby Referencia de API para Audit Manager	AWS SDK para Ruby ejemplos de código

Para ver ejemplos específicos de Audit Manager, consulte Ejemplos de código para el uso de Audit Manager AWS SDKs.

> **Note**
>
> Audit Manager está disponible en la versión 1.19.32 de botocore y posteriores para AWS SDK para Python (Boto3). Antes de empezar a usar el SDK, asegúrese de que usa la versión botocore adecuada.

Creación de recursos de AWS Audit Manager con AWS CloudFormation

AWS Audit Manager está integrado con AWS CloudFormation un servicio que le ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Cree una plantilla que describa todos los AWS recursos que desee (como las evaluaciones) y los AWS CloudFormation aprovisione y configure automáticamente.

Cuando la utilice AWS CloudFormation, podrá reutilizar la plantilla para configurar los recursos de AWS Audit Manager de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisione los mismos recursos una y otra vez en varias AWS cuentas y regiones.

AWS Audit Manager y AWS CloudFormation plantillas

Para aprovisionar y configurar los recursos de AWS Audit Manager y sus servicios relacionados, debe entender las plantillas de AWS CloudFormation. Las plantillas son archivos de texto con formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus AWS CloudFormation pilas. Si no estás familiarizado con JSON o YAML, puedes usar AWS CloudFormation Designer para ayudarte a empezar con AWS CloudFormation las plantillas. Para obtener más información, consulte ¿Qué es Designer de AWS CloudFormation ? en la Guía del usuario de AWS CloudFormation .

AWS Audit Manager admite la creación de evaluaciones en AWS CloudFormation. Para obtener más información, incluyendo ejemplos de plantillas JSON y YAML para las evaluaciones, consulte la referencia del tipo de recurso de AWS Audit Manager en la Guía del usuario de AWS CloudFormation .

Obtenga más información sobre AWS CloudFormation

Para obtener más información AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- AWS CloudFormation Guía del usuario
- AWS CloudFormation Referencia de la API
- AWS CloudFormation Guía del usuario de la interfaz de línea de comandos

Integraciones con productos de terceros de GRC

AWS Audit Manager admite integraciones con los productos GRC de socios externos que se enumeran en esta página.

Si su empresa utiliza un modelo de nube híbrida o multinube, es probable que utilice un producto GRC para gestionar las evidencias de esos entornos. Cuando ese producto se integra con Audit Manager, puede obtener pruebas sobre su AWS uso directamente en su entorno de GRC. Esto simplifica la gestión del cumplimiento ya que le proporciona un lugar centralizado para revisar y corregir las evidencias al prepararse para las auditorías.

En esta página se describen los productos GRC de terceros que pueden capturar evidencias de Audit Manager. También encontrará una referencia de las acciones de la API de Audit Manager que puede realizar directamente en esos productos.

Temas

- Cómo funcionan las integraciones de terceros con Audit Manager
- Productos de socios GRC de terceros que se integran con Audit Manager

Cómo funcionan las integraciones de terceros con Audit Manager

Los socios de GRC pueden utilizar el Audit Manager public APIs para integrar sus productos con Audit Manager. Con esta integración, puede asignar los controles empresariales del entorno de GRC a los controles comunes que Audit Manager proporciona.

> **Tip**
>
> Puede asignar los controles empresariales a cualquier tipo de control de Audit Manager. Sin embargo, le recomendamos que utilice controles comunes. Cuando asigna un control común que representa su objetivo, Audit Manager recopila pruebas de un grupo predefinido de fuentes de datos gestionado por AWS. Esto significa que no tendrá que ser un experto en AWS para saber qué orígenes de datos recopilan las evidencias pertinentes para su objetivo.

Solo tendrá que asignar el control una vez. Después de ello podrá crear las evaluaciones de Audit Manager directamente en el producto GRC. Esta acción inicia la recopilación de pruebas sobre su AWS uso. A continuación, podrá ver estas AWS pruebas junto con las demás pruebas recopiladas en su entorno híbrido, todo ello en el mismo contexto de los controles de su empresa.

Tenga en cuenta los siguientes aspectos cuando utilice una integración de Audit Manager con un producto GRC de terceros:

- Las integraciones están disponibles para todas las Regiones de AWS donde se admite Audit Manager.
- Todos los recursos de Audit Manager que cree en el producto asociado de GRC también se reflejarán en Audit Manager.
- El uso está sujeto a los precios de AWS Audit Manager y del producto de GRC de terceros.
- Las evidencias que recopila Audit Manager son inmutables. Las evidencias se presentan exactamente de la misma manera en los productos GRC de terceros que en la consola Audit Manager. Sin embargo, si utiliza una integración de terceros, es posible que pueda mejorarlas agregando un contexto adicional en sus informes.

- Se aplican las mismas cuotas de Audit Manager al producto GRC de terceros. Por ejemplo, cada Cuenta de AWS puede tener hasta 100 evaluaciones de Audit Manager activas. Esta cuota a nivel de cuenta se aplica tanto si crea las evaluaciones en la consola Audit Manager como en el producto GRC de terceros. La mayoría de las cuotas de Audit Manager, pero no todas, aparecen en el espacio de AWS Audit Manager nombres de la consola de Service Quotas. Para más información acerca de los aumentos de cuota, consulte Administrar las cuotas de Audit Manager.

Si tiene una solución de cumplimiento y desea integrarla con Audit Manager, envíe un correo electrónico a `auditmanager-partners@amazon.com`.

Productos de socios GRC de terceros que se integran con Audit Manager

Los siguientes productos de GRC de terceros pueden capturar evidencias de Audit Manager.

MetricStream

Para utilizar esta integración, póngase en contacto con nosotros MetricStreampara acceder al software MetricStream GRC y comprarlo.

Basada en la MetricStream plataforma, la solución MetricStream Enterprise GRC permite un enfoque integral y colaborativo de las actividades y los procesos de GRC en toda la empresa. Al incorporar las pruebas de Audit Manager MetricStream, puede identificar de forma proactiva las pruebas no conformes de su AWS entorno y revisarlas junto con las pruebas de sus fuentes de datos locales u otros socios de nube. Se trata de una forma cómoda y centralizada de revisar y mejorar su postura en materia de cumplimiento y seguridad en la nube al tiempo que se prepara para las auditorías.

Con la integración de Audit Manager MetricStream y Audit Manager, puede realizar las siguientes operaciones de API.

Tarea	Operación de la API
Configuración de la integración de Audit Manager	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Revisión de los recursos de Audit Manager	• GetAssessment • GetAssessmentFramework • GetControl

Tarea	Operación de la API
	• ListAssessmentFrameworks • ListControls
Creación de recursos de Audit Manager	• CreateAssessment • CreateAssessmentFramework
Actualización de los recursos de Audit Manager	• UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
Gestión de la evidencia	• StartQuery(AWS CloudTrail API) • GetQueryResults(AWS CloudTrail API)
Eliminar recursos de Audit Manager	• DeleteAssessmentFramework

MetricStream Enlaces relacionados

- AWS Marketplace link
- Enlace al producto
- Precios del producto

Integración de las evidencias de Audit Manager en el sistema de GRC

Como cliente empresarial, es probable que tenga recursos en varios centros de datos, incluidos otros proveedores de servicios en la nube y entornos en las instalaciones. Para recopilar pruebas de estos entornos, puede utilizar soluciones de GRC (gobierno, riesgo y cumplimiento) de terceros, como MetricStream CyberGRC o RSA Archer. O bien, puede utilizar un sistema de GRC patentado que haya desarrollado a nivel interno.

Este tutorial le muestra cómo puede integrar un sistema de GRC interno o externo con Audit Manager. Esta integración permite a los proveedores recopilar pruebas sobre el AWS uso y las configuraciones de sus clientes y enviar esas pruebas directamente desde Audit Manager a la aplicación GRC. De este modo, puede centralizar los informes de conformidad en varios entornos.

Para este tutorial:

1. Un proveedor es la entidad o empresa propietaria de la aplicación de GRC que se está integrando con Audit Manager.
2. Un cliente es la entidad o empresa que utiliza AWS y que también utiliza una aplicación GRC interna o externa.

> **Note**
>
> En algunos casos, la aplicación de GRC es propiedad de la misma empresa que la utiliza. En este escenario, el proveedor es el grupo o equipo propietario de la aplicación de GRC, y el cliente es el equipo o grupo que usa la aplicación de GRC.

Este tutorial le enseña a realizar las siguientes tareas:

- Paso 1: habilitar Audit Manager
- Paso 2: configuración de permisos
- Paso 3. Asignación de los controles empresariales a los controles de Audit Manager
- Paso 4. Actualización de las asignaciones de controles
- Paso 5: crear una evaluación
- Paso 6. Comenzar a recopilar evidencias

Requisitos previos

Antes de comenzar, asegúrese de cumplir las siguientes condiciones:

- Tiene una infraestructura que se ejecuta en AWS.
- Utiliza un sistema de GRC interno o utiliza un software de GRC de terceros proporcionado por un proveedor.
- Ha completado todos los requisitos previos necesarios para configurar Audit Manager.
- Conoce Comprensión de AWS Audit Manager los conceptos y la terminología.

Algunas restricciones que hay que tener en cuenta:

- Audit Manager es regional Servicio de AWS. Debe configurar Audit Manager por separado en cada región en la que ejecute sus AWS cargas de trabajo.
- Audit Manager no permite agregar evidencias de varias regiones a una única región. Si sus recursos abarcan varios Regiones de AWS, debe agregar la evidencia dentro de su sistema GRC.
- Audit Manager tiene cuotas predeterminadas para el número de recursos que puede crear. Si es necesario, puede solicitar un aumento de estas cuotas predeterminadas. Para obtener más información, consulte Quotas and restrictions for AWS Audit Manager.

Paso 1: habilitar Audit Manager

Usuario que debe completar este paso

Cliente

Qué necesita

Comience por habilitar Audit Manager para su Cuenta de AWS. Si su cuenta forma parte de una organización, puede habilitar Audit Manager con su cuenta de administración y, a continuación, especificar un administrador delegado para Audit Manager.

Procedimiento

Habilitación de Audit Manager

Siga las instrucciones para habilitar Audit Manager. Repita el procedimiento de configuración en todas las regiones en las que desee recopilar evidencias.

> **Tip**
>
> Si lo utiliza AWS Organizations, le recomendamos encarecidamente que configure un administrador delegado durante este paso. Si utiliza una cuenta de administrador delegado en Audit Manager, puede utilizar el buscador de evidencias para buscar en todas las cuentas de miembros de la organización.

Paso 2: configuración de permisos

Usuario que debe completar este paso

Cliente

Qué necesita

En este paso, el cliente crea un rol de IAM para su cuenta. A continuación, el cliente concede al proveedor permisos para asumir el rol.

Procedimiento

Creación de un rol para la cuenta de cliente

Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.

- En el paso 8 del flujo de trabajo de creación de roles, elija Crear política e introduzca una política para el rol.

  El rol debe tener, como mínimo, los siguientes permisos:

  JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
        "Sid" : "AuditManagerAccess",
        "Effect" : "Allow",
        "Action" : [
          "auditmanager:*"
        ],
        "Resource" : "*"
      },
      {
        "Sid" : "OrganizationsAccess",
        "Effect" : "Allow",
        "Action" : [
          "organizations:ListAccountsForParent",
          "organizations:ListAccounts",
          "organizations:DescribeOrganization",
          "organizations:DescribeOrganizationalUnit",
          "organizations:DescribeAccount",
          "organizations:ListParents",
          "organizations:ListChildren"
        ],
        "Resource" : "*"
      },
      {
        "Sid" : "IAMAccess",
        "Effect" : "Allow",
        "Action" : [
          "iam:GetUser",
          "iam:ListUsers",
          "iam:ListRoles"
        ],
        "Resource" : "*"
      },
      {
        "Sid" : "S3Access",
        "Effect" : "Allow",
        "Action" : [
          "s3:ListAllMyBuckets"
        ],
        "Resource" : "*"
      },
      {
        "Sid" : "KmsAccess",
        "Effect" : "Allow",
        "Action" : [
          "kms:DescribeKey",
```

```
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "auditmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SNSAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

- En el paso 11 del flujo de trabajo de creación de roles, introduzca `vendor-auditmanager` como nombre del rol.

Autorización para que la cuenta del proveedor asuma el rol

Siga las instrucciones que se indican en Conceder a un usuario permisos para cambiar de rol en la Guía del usuario de IAM.

- La declaración de política debe incluir el efecto `Allow` en la `sts:AssumeRole action`.
- También debe incluir el nombre de recurso de Amazon (ARN) del rol en un elemento de recurso.
- A continuación, se muestra un ejemplo de declaración de política que puede utilizar.

  En esta política, sustitúyalo por el *`placeholder text`* Cuenta de AWS identificador de su proveedor.

  JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "arn:aws:iam::111122223333:role/vendor-auditmanager"
    }
}
```

Paso 3. Asignación de los controles empresariales a los controles de Audit Manager

Usuario que debe completar este paso

Cliente

Qué necesita

Los proveedores mantienen una lista seleccionada de controles empresariales que los clientes pueden utilizar en una evaluación. Para integrarse con Audit Manager, los proveedores deben crear una interfaz que permita a los clientes asignar sus controles empresariales a los controles de Audit Manager correspondientes. Puede realizar la asignación a varios common control (recomendado) o a varios standard control. Debe completar esta asignación antes de iniciar cualquier evaluación en la aplicación de GRC del proveedor.

Opción 1: asignar los controles empresariales a los controles comunes (recomendado)

Esta es la forma recomendada de asignar los controles empresariales a Audit Manager. Esto se debe a que los controles comunes están en consonancia con los estándares comunes del sector. Esto facilita su asignación a los controles empresariales.

Con este método, el proveedor crea una interfaz que permite al cliente realizar una asignación única entre sus controles empresariales y los controles comunes correspondientes que proporciona Audit Manager. Los proveedores pueden usar las operaciones de GetControlAPI y ListControlsListCommonControls, para mostrar esta información a los clientes. Una vez que el cliente complete el ejercicio de asignación, el proveedor puede usar estas asignaciones para crear controles personalizados en Audit Manager.

A continuación, se muestra un ejemplo de una asignación de controles comunes:

Supongamos que tiene un control empresarial denominado `Asset Management`. Este control empresarial se asigna a dos controles comunes en Audit Manager (`Asset performance management` y `Asset maintenance scheduling`). En este caso, debe crear un control personalizado en Audit Manager (lo denominaremos `enterprise-asset-management`). A continuación, añada `Asset performance management` y `Asset maintenance scheduling` como orígenes de evidencias al nuevo control personalizado. Estas fuentes de evidencia recopilan evidencia de apoyo de un grupo predefinido de fuentes de AWS datos. Esto le proporciona una forma eficaz de identificar las fuentes de AWS datos que se corresponden con los requisitos de control de su empresa.

Procedimiento

Búsqueda de los controles comunes disponibles a los se que pueden realizar asignaciones

Siga los pasos para buscar la lista de controles comunes disponibles en Audit Manager.

Creación de un control personalizado

1. Siga los pasos para crear un control personalizado que esté en concordancia con el control empresarial.

   Cuando especifique los orígenes de evidencias en el paso 2 del flujo de trabajo de creación de controles personalizados, haga lo siguiente:

   - Elija orígenes administrados por AWS como el origen de evidencias.
   - Seleccione Usar un control común que coincida con el objetivo de conformidad.
   - Elija hasta cinco controles comunes como orígenes de evidencias para el control empresarial.
2. Repita esta tarea para todos los controles empresariales y cree los controles personalizados correspondientes en Audit Manager para cada uno de ellos.

Opción 2: asignar controles empresariales a controles estándar

Audit Manager proporciona una gran número de controles estándar prediseñados. Puede realizar una asignación única entre los controles empresariales y estos controles estándar. Una vez que haya identificado los controles estándar que corresponden a los controles empresariales, puede añadirlos directamente a un marco personalizado. Si elige esta opción, no necesitará crear ningún control personalizado en Audit Manager.

Procedimiento

Búsqueda de los controles estándar disponibles a los que se pueden realizar asignaciones

Siga los pasos para buscar la lista de controles estándar disponibles en Audit Manager.

Creación de un marco personalizado

1. Siga los pasos para crear un marco personalizado en Audit Manager.

   Cuando especifique un conjunto de controles en el paso 2 del procedimiento de creación de marcos, incluya los controles estándar que se asignan a los controles empresariales.
2. Repita esta tarea para todos los controles empresariales hasta que haya incluido todos los controles estándar correspondientes en el marco personalizado.

Paso 4. Actualización de las asignaciones de controles

Usuario que debe completar este paso

Proveedor, cliente

Qué necesita

Audit Manager actualiza continuamente los controles comunes y los controles estándar para garantizar que utilizan las últimas fuentes de AWS datos disponibles. Esto significa que la asignación de los controles es una tarea única: no es necesario administrar los controles estándar después de añadirlos a un marco personalizado, y no es necesario administrar los controles comunes después de añadirlos como origen de evidencias en el control personalizado. Siempre que se actualice un control común, se aplicarán automáticamente las mismas actualizaciones a todos los controles personalizados que utilizan ese control común como origen de evidencias.

Sin embargo, con el tiempo, es posible que estén disponibles nuevos controles comunes y estándar para utilizarlos como orígenes de evidencias. Teniendo esto en cuenta, los proveedores y los clientes deben crear un flujo de trabajo para obtener periódicamente los controles comunes y estándar más recientes de Audit Manager. A continuación, puede revisar las asignaciones entre los controles empresariales y los controles de Audit Manager, y actualizar las asignaciones según sea necesario.

Si los controles empresariales se asignan a controles comunes

Durante el proceso de asignación, ha creado controles personalizados. Puede usar Audit Manager para editar esos controles personalizados de modo que utilicen los controles comunes más recientes disponibles como orígenes de evidencias. Una vez que se apliquen las actualizaciones de los controles personalizados, las evaluaciones existentes recopilarán automáticamente evidencias comparándolas con los controles personalizados actualizados. No es necesario crear un nuevo marco o evaluación.

Procedimiento

Búsqueda de los controles comunes más recientes a los se que pueden realizar asignaciones

Siga los pasos para buscar los controles comunes disponibles en Audit Manager.

Edición de un control personalizado

1. Siga los pasos para editar un control personalizado en Audit Manager.

Al actualizar los orígenes de evidencias en el paso 2 del flujo de trabajo de edición, haga lo siguiente:

- Elija orígenes administrados por AWS como el origen de evidencias.
- Seleccione Usar un control común que coincida con el objetivo de conformidad.
- Elija el nuevo control común que desee utilizar como origen de evidencias para el control personalizado.

2. Repita esta tarea para todos los controles empresariales que desee actualizar.

Si los controles empresariales se asignan a controles estándar

En este caso, los proveedores deben crear un nuevo marco personalizado que incluya los controles estándar más recientes disponibles y, a continuación, crear una nueva evaluación con este nuevo marco. Tras crear la nueva evaluación, puede marcar la anterior como en estado Inactivo.

Procedimiento

Búsqueda de los controles estándar más recientes a los que se pueden realizar asignaciones

Siga los pasos para buscar los controles estándar disponibles en Audit Manager.

Creación de un marco personalizado y cómo añadir los controles estándar más recientes

Siga los pasos para crear un marco personalizado en Audit Manager.

Cuando especifique un conjunto de controles en el paso 2 del flujo de trabajo de creación de marcos, incluya los nuevos controles estándar.

Creación de una evaluación

Cree una evaluación en la aplicación de GRC.

Cambio del estado de una evaluación a Inactivo

Siga los pasos para cambiar el estado de una evaluación en Audit Manager.

Paso 5: crear una evaluación

Usuario que debe completar este paso

Aplicación de GRC, con información del proveedor

Qué necesita

Como cliente, no necesita crear una evaluación directamente en Audit Manager. Al iniciar una evaluación de determinados controles en la aplicación de GRC, la aplicación de GRC crea los recursos correspondientes en Audit Manager. En primer lugar, la aplicación de GRC utiliza las asignaciones que ha creado para identificar los controles pertinentes de Audit Manager. A continuación, utiliza la información del control para crear un marco personalizado. Por último, utiliza el marco personalizado recién creado para crear una evaluación en Audit Manager.

La creación de una evaluación en Audit Manager también requiere un ámbito. Este ámbito incluye una lista de los Cuentas de AWS lugares en los que el cliente desea realizar la evaluación y recopilar las pruebas. Los clientes deben definir este ámbito directamente en la aplicación de GRC.

Como proveedor, debe almacenar el `assessmentId` asignado a la evaluación que se ha iniciado en la aplicación de GRC. Este `assessmentId` es necesario para obtener evidencias de Audit Manager.

Búsqueda de un ID de evaluación

1. Utilice la ListAssessmentsoperación para ver sus evaluaciones en Audit Manager. Puede utilizar el parámetro status para ver las evaluaciones con el estado Activo.

   ```
   aws auditmanager list-assessments --status ACTIVE
   ```

2. En la respuesta, identifique la evaluación que desea almacenar en la aplicación de GRC y tome nota del `assessmentId`.

Paso 6. Comenzar a recopilar evidencias

Usuario que debe completar este paso

AWS Audit Manager, con la información del proveedor

Qué necesita

Tras crear una evaluación, se tardan hasta 24 horas en empezar a recopilar evidencias. En este momentos, los controles empresariales están recopilando activamente evidencias para la evaluación de Audit Manager.

Le recomendamos que utilice la característica de buscador de evidencias para consultar y encontrar evidencias rápidamente en Audit Manager. Si utiliza el buscador de evidencias como administrador

delegado, puede buscar evidencias en todas las cuentas de miembros de su organización. Mediante una combinación de filtros y agrupaciones, puede reducir progresivamente el alcance de su consulta de búsqueda. Por ejemplo, si desea obtener una visión general del estado de su sistema, realice una búsqueda amplia y filtre por evaluación, intervalo de fechas y conformidad de los recursos. Si su objetivo es corregir un recurso específico, puede realizar una búsqueda restringida para encontrar evidencias que apunten a un identificador de control o recurso específico. Tras definir los filtros, puede agrupar y, a continuación, obtener una vista previa de los resultados de búsqueda coincidentes antes de crear un informe de evaluación.

Habilitación del buscador de evidencias

- Siga las instrucciones para habilitar el buscador de evidencias en la configuración de Audit Manager.

Después de habilitar el buscador de evidencias, puede decidir el ritmo con el que desea obtener las evidencias de Audit Manager para la evaluación. También puede buscar evidencias para un determinado control en una evaluación y almacenarlas en la aplicación de GRC asignada al control empresarial. Puede utilizar las siguientes operaciones de la API de Audit Manager para obtener evidencias:

- GetEvidence
- GetEvidenceByEvidenceFolder
- GetEvidenceFolder
- GetEvidenceFoldersByAssessment
- GetEvidenceFoldersByAssessmentControl

Precios

No incurrirá en ningún costo adicional por la configuración de esta integración, ya sea un proveedor o un cliente. A los clientes se les cobra por las evidencias recopiladas en Audit Manager. Para obtener más información sobre los precios, consulte Precios de AWS Audit Manager.

Recursos adicionales

Consulte los siguientes recursos para obtener más información sobre los conceptos que se presentan en este tutorial:

- Evaluaciones: obtenga información sobre los conceptos y las tareas para administrar una evaluación.
- Biblioteca de controles: obtenga información sobre los conceptos y las tareas para administrar un control personalizado.
- Biblioteca de marcos: obtenga información sobre los conceptos y las tareas para administrar un marco personalizado.
- Buscador de evidencias: obtenga información sobre cómo exportar un archivo CSV o generar un informe de evaluación a partir de los resultados de consultas.
- Centro de descargas: obtenga información sobre cómo descargar archivos de evaluación y exportaciones a archivos CSV de Audit Manager.

Marcos compatibles en AWS Audit Manager

Al explorar la biblioteca de marcos en AWS Audit Manager, encontrará una lista completa de marcos estándar prediseñados que pueden ayudarlo a optimizar sus esfuerzos de cumplimiento. Estos marcos prediseñados se basan en las AWS mejores prácticas para varios estándares y reglamentos de cumplimiento. Puede utilizar estos marcos como ayuda en la preparación de la auditoría, ya sea que necesite evaluar el entorno en función de los requisitos de HIPAA, PCI DSS, SOC 2, etc.

> **Note**
>
> Si es la primera vez que utiliza Audit Manager, comience con AWS Audit Manager Sample Framework. Este marco está diseñado con fines de aprendizaje y no admite ningún estándar de cumplimiento específico. Proporciona un entorno controlado para que explore las funciones principales de Audit Manager dentro de un ámbito manejable. Tras utilizar el marco de ejemplo para familiarizarse con Audit Manager, estará preparado para utilizar los demás marcos para realizar evaluaciones de conformidad reales.

En la siguiente lista se proporciona una descripción general de los marcos disponibles para que pueda identificar fácilmente los que se adaptan a sus requisitos específicos. Dedique un momento a revisar la lista y a familiarizarse con los marcos más pertinentes para las necesidades de su organización. Abra cualquier página para ver una descripción general de ese marco y descubra cómo puede usarlo para crear una evaluación y empezar a recopilar evidencias en Audit Manager.

Temas

- Essential Eight del ACSC
- ACSC ISM 02 March 2023
- AWS Audit Manager Ejemplo de marco
- AWS Control Tower Barandillas
- AWS Marco generativo de mejores prácticas de IA, versión 2
- AWS License Manager
- AWS Mejores prácticas de seguridad fundamentales
- AWS Mejores prácticas operativas
- AWS Well Architected Framework (WAF v1.0)

- CCCS Medium Cloud Control
- CIS AWS Benchmark v1.2.0
- Índice de referencia CIS v1.3.0 AWS
- CIS AWS Benchmark v1.4.0
- CIS Controls v7.1, IG1
- CIS Critical Security Controls versión 8.0, IG1
- FedRAMP Security Baseline Controls r4
- GDPR 2016
- Gramm-Leach-Bliley Actúa
- Title 21 CFR Part 11
- EU GMP Annex 11, v1
- HIPAA Security Rule: Feb 2003
- HIPAA Omnibus Final Rule
- Anexo A de la norma de la ISO/IEC 27001:2013
- NIST SP 800-53 Rev 5
- Marco de Ciberseguridad del NIST v1.1
- NIST SP 800-171 Rev 2
- PCI DSS V3.2.1
- PCI DSS V4.0
- SSAE-18 SOC 2

Essential Eight del ACSC

AWS Audit Manager proporciona un marco estándar prediseñado que respalda el Essential Eight del Centro Australiano de Ciberseguridad (ACSC).

Temas

- ¿Qué es ACSC Essential Eight?
- Uso de este marco

- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es ACSC Essential Eight?

El ACSC es la principal agencia del gobierno australiano en materia de ciberseguridad. Para protegerse contra las ciberamenazas, el ACSC recomienda que las organizaciones implementen ocho estrategias de mitigación esenciales tomadas de las Estrategias para mitigar los incidentes de ciberseguridad del ACSC como punto de partida. Esta base de referencia, conocida como Essential Eight, hace que sea mucho más difícil para los adversarios comprometer los sistemas.

Dado que Essential Eight describen un conjunto mínimo de medidas preventivas, su organización debe implementar medidas adicionales cuando lo justifique su entorno. Además, si bien Essential Eight puede ayudar a mitigar la mayoría de las ciberamenazas, no mitigarán todas las ciberamenazas. Por ello, es necesario considerar estrategias de mitigación y controles de seguridad adicionales, incluidos los que figuran en las Estrategias para mitigar los incidentes de ciberseguridad y el Manual de seguridad de la información (ISM).

Essential Eight, del ACSC, tiene una licencia internacional de atribución 4.0 de Creative Commons y la información sobre derechos de autor se puede encontrar en ACSC | Derechos de autor. © Mancomunidad de Australia 2022.

Uso de este marco

Puede utilizar el marco estándar Essential Eight como ayuda AWS Audit Manager para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de Essential Eight. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace basándose en los controles que se definen en el marco Essential Eight. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En

cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Australian Cyber Security Center (ACSC) Essential Eight	61	132	3

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el archivo AuditManager_ ConfigDataSourceMappings _Australian-Cyber-Security-Center - (ACSC) - Essential-Eight.zip.

Los controles de este AWS Audit Manager marco no pretenden verificar si sus sistemas cumplen con los ocho controles Essential. Además, no pueden garantizar que pases una auditoría de la ACSC. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Essential Eight del ACSC

ACSC ISM 02 March 2023

AWS Audit Manager proporciona un marco estándar prediseñado que respalda el Manual de Seguridad de la Información (ISM) del Centro Australiano de Ciberseguridad (ACSC).

Temas

- ¿Qué es el ISM del ACSC?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es el ISM del ACSC?

El ACSC es la principal agencia del gobierno australiano en materia de ciberseguridad. El ACSC elabora el ISM, que funciona como un conjunto de principios de ciberseguridad. El objetivo de estos principios es proporcionar una guía estratégica sobre cómo una organización puede proteger sus sistemas y datos de las ciberamenazas. Estos principios de ciberseguridad se agrupan en cuatro actividades clave: gobernar, proteger, detectar y responder. Una organización debe poder demostrar que se respetan los principios de ciberseguridad dentro de su organización. El ISM está dirigido a los directores de seguridad de la información, los directores de información, los profesionales de la ciberseguridad y los administradores de tecnología de la información.

El ACSC proporciona el marco de ISM en virtud de una Creative Commons Attribution 4.0 International License, y la información sobre derechos de autor se encuentra en ACSC | Copyright. © Mancomunidad de Australia 2022.

Uso de este marco

Puede utilizar el marco estándar ISM del ACSC como ayuda AWS Audit Manager para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los

requisitos de ACSC ISM. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco de ACSC ISM. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Australian Cyber Security Center (ACSC) Information Security Manual (ISM) 02 March 2023	88	789	22

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el archivo AuditManager_ ConfigDataSourceMappings _Australian-Cyber-Security-Center- (ACSC) -Information-Security-Manual- (ISM) -02-March-2023.zip.

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si sus sistemas cumplen con los controles del Manual de seguridad de la información de la ACSC. Además, no

pueden garantizar que supere una auditoría de la ACSC. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Manual de seguridad de la información del ACSC

AWS Audit Manager Ejemplo de marco

Si es la primera vez que utiliza Audit Manager, puede utilizar el AWS Audit Manager Sample Framework para conocer cómo funciona Audit Manager. Proporciona un entorno sencillo en el que puede explorar la funcionalidad de Audit Manager sin dejarse abrumar por pruebas excesivas ni sobrepasar sus capa gratuita de AWS límites. Una vez que haya probado el marco de ejemplo, estará listo para empezar a utilizar el resto de marcos que proporciona Audit Manager.

Temas

- ¿Qué es el marco AWS Audit Manager de muestra?
- Uso de este marco
- Pasos a seguir a continuación

¿Qué es el marco AWS Audit Manager de muestra?

El marco de ejemplo proporciona una forma simplificada y fácil de usar para principiantes de explorar la funcionalidad principal de Audit Manager: recopilar pruebas y adjuntarlas a los controles.

En el marco, encontrará ejemplos de controles que le muestran las diferentes fuentes de datos que Audit Manager utiliza para recopilar pruebas automáticamente. Estas fuentes de datos incluyen un AWS CloudTrail evento, una AWS Config regla, un AWS Security Hub control y una llamada a la AWS API. Al utilizar estas fuentes de datos en una evaluación de prueba, puede ver cómo Audit Manager trabaja con diferentes fuentes de datos Servicios de AWS para recopilar pruebas. Además de demostrar la recopilación automática de pruebas, el modelo de marco muestra cómo puede añadir manualmente sus propias pruebas. También tiene un control manual que le permite cargar archivos como evidencia. Al probar tanto los controles automatizados como los manuales, puede desarrollar una comprensión completa de las diferentes formas en que se pueden añadir pruebas a sus evaluaciones.

> **Note**
>
> Este marco es diferente de otros marcos estándar. El marco de muestra no está diseñado para gestionar auditorías o evaluaciones de cumplimiento reales. Su objetivo es ayudarle a aprender a utilizar Audit Manager. Proporciona un entorno controlado en el que puede recopilar pruebas suficientes para probar las capacidades de Audit Manager y, al mismo tiempo, mantener el alcance manejable para los principiantes.

Uso de este marco

El uso de AWS Audit Manager Sample Framework le permite practicar la navegación por la interfaz de Audit Manager, recopilar pruebas y ver cómo esas pruebas se adjuntan a los controles de evaluación.

Para empezar, utilice el marco de ejemplo para crear una evaluación. Esta acción inicia la recopilación continua de pruebas para cada uno de los controles automatizados del marco muestral. En función de las definiciones de control, Audit Manager evalúa sus AWS recursos, recopila las pruebas pertinentes y, a continuación, las adjunta a los controles de su evaluación. En este momento, puede explorar las pruebas que Audit Manager ha recopilado. También puede intentar añadir sus propias pruebas a los controles manuales.

Puede encontrar este marco en la pestaña Marcos estándar de la biblioteca de marcos de Audit Manager.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Marco de prueba de Amazon Web Services (AWS) Audit Manager	4	1	2

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el ConfigDataSourceMappingsarchivo AuditManager _ _AWS-Audit-Manager-Sample-Framework.zip.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

AWS Control Tower Barandillas

AWS Audit Manager proporciona un marco AWS Control Tower Guardrails prediseñado para ayudarlo en la preparación de la auditoría.

Temas

- ¿Qué es? AWS Control Tower
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es? AWS Control Tower

AWS Control Tower es un servicio de administración y gobierno que puede utilizar para analizar el proceso de configuración y los requisitos de gobierno que implica la creación de un AWS entorno de múltiples cuentas.

Con él AWS Control Tower, puede aprovisionar nuevos Cuentas de AWS productos que se ajusten a las políticas de su empresa u organización con unos pocos clics. AWS Control Tower crea una capa de organización en su nombre que combina e integra las capacidades de varias otras. Servicios de AWS Estos servicios incluyen AWS Organizations AWS IAM Identity Center, y Servicio de AWS Catalog. Esto ayuda a agilizar el proceso de configuración y administración de un entorno de AWS de cuentas múltiples que sea seguro y cumpla con las normas.

El marco AWS Control Tower Guardrails contiene todos los Reglas de AWS Config que se basan en guardrails de. AWS Control Tower

Uso de este marco

Puede utilizar el marco medidas de seguridad de AWS Control Tower como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan de acuerdo con los Reglas de AWS Config que se basan en las barandillas. AWS Control Tower También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para una AWS Control Tower auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco de AWS Control Tower Guardrails. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir

de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco de AWS Control Tower Guardrails son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
AWS Control Tower Barandillas	14	0	5

> **Important**
>
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las reglas necesarias AWS Config . Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el ConfigDataSourceMappingsarchivo AuditManager _ _AWS-Control-Tower-Guardrails.zip.

Los controles de este AWS Audit Manager marco no tienen por objeto comprobar si sus sistemas cumplen con AWS Control Tower los requisitos de Guardrails. Además, no pueden garantizar que supere una auditoría.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- AWS Control Tower página de servicio

- AWS Control Tower guía de usuario

AWS Marco generativo de mejores prácticas de IA, versión 2

> **Note**
>
> El 11 de junio de 2024, AWS Audit Manager actualizé este marco a una nueva versión, el marco de mejores prácticas de IA AWS generativa v2. Además de respaldar las prácticas recomendadas para Amazon Bedrock, la versión 2 le permite recopilar pruebas que demuestren que sigue las prácticas recomendadas en Amazon SageMaker AI.
> Ya no es compatible el Marco de prácticas recomendadas de IA generativa de AWS v1. Si ha creado anteriormente una evaluación a partir del marco v1, las evaluaciones existentes seguirán funcionando. Sin embargo, ya no podrá crear nuevas evaluaciones a partir del marco v1. Le sugerimos que utilice el marco actualizado v2.

AWS Audit Manager proporciona un marco estándar prediseñado para ayudarlo a obtener visibilidad sobre cómo su implementación de IA generativa en Amazon Bedrock y Amazon SageMaker AI funciona en comparación con las mejores prácticas AWS recomendadas.

Amazon Bedrock es un servicio totalmente gestionado que permite que los modelos de IA de Amazon y otras empresas líderes en IA estén disponibles a través de una API. Con Amazon Bedrock, puede ajustar de forma privada los modelos existentes con los datos de su organización. Esto le permite aprovechar los modelos básicos (FMs) y los modelos de lenguaje de gran tamaño (LLMs) para crear aplicaciones de forma segura, sin comprometer la privacidad de los datos. Para obtener más información, consulte ¿Qué es Amazon Bedrock? en la Guía del usuario de Amazon Bedrock.

Amazon SageMaker AI es un servicio de aprendizaje automático (ML) totalmente gestionado. Con la SageMaker IA, los científicos de datos y los desarrolladores pueden crear, entrenar e implementar modelos de aprendizaje automático para casos de uso extensos que requieren una personalización profunda y un ajuste preciso del modelo. SageMaker La IA proporciona algoritmos de aprendizaje automático gestionados para que se ejecuten de forma eficiente con datos extremadamente grandes en un entorno distribuido. Con soporte integrado para sus propios algoritmos y marcos, la SageMaker IA ofrece opciones de formación distribuidas y flexibles que se ajustan a sus flujos de

trabajo específicos. Para obtener más información, consulta ¿Qué es Amazon SageMaker AI? en la Guía del usuario de Amazon SageMaker AI.

Temas

- ¿Cuáles son las mejores prácticas de IA AWS generativa para Amazon Bedrock?
- Utilice este marco para respaldar la preparación de la auditoría
- Verificación manual de las indicaciones en Amazon Bedrock
- Pasos a seguir a continuación
- Recursos adicionales

¿Cuáles son las mejores prácticas de IA AWS generativa para Amazon Bedrock?

La IA generativa se refiere a una rama de la IA que se centra en permitir que las máquinas generen contenido. Los modelos de IA generativa están diseñados para crear resultados que se parezcan mucho a los ejemplos en los que se entrenaron. Esto crea escenarios en los que la IA puede imitar la conversación humana, generar contenido creativo, analizar grandes volúmenes de datos y automatizar procesos que normalmente realizan las personas. El rápido crecimiento de la IA generativa trae consigo nuevas y prometedoras innovaciones. Al mismo tiempo, plantea nuevos desafíos en torno a cómo utilizar la IA generativa de forma responsable y de conformidad con los requisitos de gobernanza.

AWS se compromete a proporcionarle las herramientas y la orientación necesarias para crear y gestionar las aplicaciones de forma responsable. Para ayudarlo a alcanzar este objetivo, Audit Manager se ha asociado con Amazon Bedrock y SageMaker AI para crear el marco AWS generativo de mejores prácticas de IA v2. Este marco le proporciona una herramienta especialmente diseñada para supervisar y mejorar la gobernanza de sus proyectos de IA generativa en Amazon Bedrock y Amazon AI. SageMaker Puede utilizar las prácticas recomendadas de este marco para obtener un control y una visibilidad más estrictos sobre el uso del modelo y mantenerse informado sobre el comportamiento del modelo.

Los controles de este marco se desarrollaron en colaboración con expertos en IA, profesionales del cumplimiento y especialistas en garantía de la seguridad de todo el mundo AWS, y con la colaboración de Deloitte. Cada control automatizado se asigna a una fuente de AWS datos de la que Audit Manager recopila pruebas. Puede utilizar las pruebas recopiladas para evaluar su implementación de IA generativa en función de los ocho principios siguientes:

1. Responsable: desarrolle y cumpla las directrices éticas para la implementación y el uso de modelos de IA generativa
2. Seguro: establezca parámetros y límites éticos claros para evitar la generación de resultados dañinos o problemáticos
3. Justo: considere y respete la forma en que un sistema de IA afecta a las diferentes subpoblaciones de usuarios
4. Sostenible: esfuércese por lograr una mayor eficiencia y fuentes de energía más sostenibles
5. Resiliencia: mantenga los mecanismos de integridad y disponibilidad para garantizar que un sistema de IA funcione de manera confiable
6. Privacidad: asegúrese de que los datos confidenciales estén protegidos contra el robo y la exposición
7. Precisión: cree sistemas de IA que sean precisos, fiables y robustos
8. Seguro: evite el acceso no autorizado a los sistemas de IA generativa

Ejemplo

Supongamos que su aplicación utiliza un modelo básico de terceros que está disponible en Amazon Bedrock. Puede utilizar el marco AWS generativo de mejores prácticas de IA para supervisar el uso de este modelo. Al utilizar este marco, puede recopilar pruebas que demuestren que su uso cumple con las prácticas recomendadas de IA generativa. Esto le proporciona un enfoque coherente para rastrear el uso y los permisos del modelo de seguimiento, marcar los datos confidenciales y recibir alertas sobre cualquier divulgación inadvertida. Por ejemplo, los controles específicos de este marco pueden recopilar pruebas que te ayuden a demostrar que has implementado los siguientes mecanismos:

- Documentar la fuente, la naturaleza, la calidad y el tratamiento de los nuevos datos para garantizar la transparencia y ayudar a solucionar problemas o realizar auditorías (Responsable)
- Evaluar periódicamente el modelo mediante métricas de rendimiento predefinidas para garantizar que cumpla con los puntos de referencia de precisión y seguridad (Seguro)
- Utilizar herramientas de supervisión automatizadas para detectar posibles resultados o comportamientos sesgados en tiempo real y alertar sobre ellos (Justo)
- Evaluar, identificar y documentar el uso de los modelos y los escenarios en los que se pueden reutilizar los modelos existentes, independientemente de que los haya generado o no (Sostenible)
- Configurar los procedimientos de notificación en caso de que se divulgue o divulgue inadvertidamente la PII (Privacidad)

- Establecer un monitoreo en tiempo real del sistema de IA y configurar alertas para detectar cualquier anomalía o interrupción (Resiliencia)
- Detectar imprecisiones y realizar un análisis exhaustivo de los errores para comprender las causas fundamentales (Precisión)
- Implementar el end-to-end cifrado de los datos de entrada y salida de los modelos de IA según los estándares mínimos del sector (seguro)

Utilice este marco para respaldar la preparación de la auditoría

> **Note**
>
> - Si es cliente de Amazon Bedrock o SageMaker AI, puede utilizar este marco directamente en Audit Manager. Asegúrese de utilizar el marco y de realizar evaluaciones en Cuentas de AWS y en las regiones en las que ejecuta sus modelos y aplicaciones de IA generativa.
> - Si desea cifrar los CloudWatch registros de Amazon Bedrock o SageMaker AI con su propia clave de KMS, asegúrese de que Audit Manager tenga acceso a esa clave. Para ello, puede elegir la clave administrada por el cliente en la configuración Configuración de los ajustes del cifrado de datos de Audit Manager.
> - Este marco utiliza la ListCustomModelsoperación Amazon Bedrock para generar pruebas sobre el uso del modelo personalizado. Actualmente, esta operación de API Regiones de AWS solo se admite en EE. UU. Este (Norte de Virginia) y EE. UU. Oeste (Oregón). Por este motivo, es posible que no vea pruebas sobre el uso de modelos personalizados en las regiones Asia-Pacífico (Tokio), Asia-Pacífico (Singapur) o Europa (Fráncfort).

Puede utilizar este marco para prepararse para las auditorías sobre su uso de la IA generativa en Amazon Bedrock y SageMaker la IA. Incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según las prácticas recomendadas de IA generativa. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas que le ayuden a supervisar el cumplimiento de las políticas previstas. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace basándose en los controles que se definen en el marco AWS generativo de mejores prácticas de IA. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas

que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
AWS Marco generativo de mejores prácticas de IA, versión 2	72	38	8

> **Important**
>
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos de control en este marco estándar, descargue el archivo AuditManager_ ConfigDataSourceMappings _AWS-Generative-AI-Best-Practices-Framework-v2.

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si sus sistemas cumplen con las mejores prácticas de IA generativa. Además, no pueden garantizar que pases una auditoría sobre tu uso de la IA generativa. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Verificación manual de las indicaciones en Amazon Bedrock

Es posible que tenga diferentes conjuntos de indicaciones que necesite evaluar en función de modelos específicos. En este caso, puede utilizar la operación de `InvokeModel` para evaluar cada solicitud y recopilar las respuestas como prueba manual.

Usar la operación **`InvokeModel`**

Para comenzar, cree una lista de mensajes predefinidos. Utilizará estas indicaciones para verificar las respuestas del modelo. Asegúrese de que su lista de solicitudes contenga todos los casos de uso que desee evaluar. Por ejemplo, es posible que tenga indicaciones que pueda utilizar para comprobar que las respuestas modelo no divulgan ninguna información de identificación personal (PII).

Después de crear la lista de solicitudes, pruebe cada una de ellas mediante la InvokeModeloperación que proporciona Amazon Bedrock. A continuación, puede recopilar las respuestas del modelo a estas solicitudes y cargar estos datos como evidencia manual en su evaluación de Audit Manager.

Hay tres formas diferentes de utilizar la operación de `InvokeModel`.

1. Solicitud HTTP

   Puede usar herramientas como Postman para crear una llamada de solicitud HTTP a `InvokeModel` y almacenar la respuesta.

   > **Note**
   >
   > Postman se ha desarrollado por un tercero. No está desarrollado ni respaldado por. AWS Para obtener más información sobre Postman, o para obtener ayuda en relación con problemas relacionados con Postman, consulte el Centro de soporte en el sitio web de Postman.

2. AWS CLI

   Puede usar el AWS CLI para ejecutar el comando invoke-model. Para obtener instrucciones y más información, consulte Cómo ejecutar inferencias en un modelo en la Guía del usuario de Amazon Bedrock.

   El siguiente ejemplo muestra cómo generar texto AWS CLI utilizando la línea de comandos *`"story of two dogs"`* y el *`Anthropic Claude V2`* modelo. En el ejemplo, se devuelven los *`300`* símbolos de la respuesta y se guarda la respuesta en el archivo*`invoke-model-output.txt`*:

   ```
   aws bedrock-runtime invoke-model \
   ```

```
          --model-id anthropic.claude-v2 \
          --body "{\"prompt\": \"\n\nHuman:story of two dogs\n\nAssistant:\",
 \"max_tokens_to_sample\" : 300}" \
          --cli-binary-format raw-in-base64-out \
          invoke-model-output.txt
```

3. Verificación automatizada

   Puedes usar CloudWatch Synthetics canaries para monitorear las respuestas de tu modelo. Con esta solución, puede comprobar el `InvokeModel` resultado de una lista de solicitudes predefinidas y, a continuación, utilizarla CloudWatch para supervisar el comportamiento del modelo en relación con estas solicitudes.

   Para empezar con esta solución, primero debes crear un valor controlado de Synthetics. Después de crear un valor controlado, puede usar el siguiente fragmento de código para verificar su solicitud y la respuesta del modelo.

```
const invokeModel = async function () {
    log.info("Starting Bedrock::Invoke.");

    const prompt = "Hello";
    const maxTokenCount = 512;
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

    const modelId = "amazon.titan-tg1-large";

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
 "us-west-2"});
    const param = {
      body: {
        "inputText": prompt,
        "textGenerationConfig": {
            "maxTokenCount": maxTokenCount,
            "stopSequences": stopSequences,
            "temperature": temperature,
            "topP": topP
        }
      },
      modelId: modelId
    };
    const response = await bedrockRuntime.invokeModel(param);
```

```
    return "Successfully completed Bedrock::Invoke.";
};
```

> **Note**
>
> Otra opción, puede utilizar una función de Lambda para ejecutar este script. Si elige esta solución, primero tendrá que crear una función de Lambda.

Ejemplos de indicaciones

Puede utilizar estas instrucciones de ejemplo como punto de partida para probar las respuestas de su modelo. En los ejemplos siguientes, sustitúyalos *`placeholder text`* por sus propios datos para reflejar sus casos de uso específicos en las pruebas.

Para comprobar si hay contenido inadecuado en las respuestas del modelo

```
"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age,
religion, or other protected class>"
```

Para comprobar la PII en las respuestas del modelo

```
"hi, you can reach customer service at <your phone number>" -> "hi, you can reach
 customer service at {PHONE}"
```

Para comprobar si hay blasfemias en las respuestas del modelo

```
"<abusive or derogatory insult>" -> "**** *** **** **"
"Hello, <offensive name>" -> "Hello, ******"
```

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Amazon Bedrock
- Guía del usuario de Amazon Bedrock
- Amazon SageMaker AI
- Guía del usuario de Amazon SageMaker AI
- Transforma la IA responsable de la teoría a la práctica
- Proteger a los consumidores y promover la innovación: regulación de la IA y fomento de la confianza en una IA responsable
- Guía sobre el uso responsable de Machine Learning

AWS License Manager

AWS Audit Manager proporciona un AWS License Manager marco prediseñado para ayudarlo en la preparación de la auditoría.

Temas

- ¿Qué es? AWS License Manager
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es? AWS License Manager

Con AWS License Manager, puede administrar sus licencias de software de varios proveedores de software (como Microsoft, SAP, Oracle o IBM) de forma centralizada en todos AWS los entornos locales. Tener todas sus licencias de software en un solo lugar le permite tener un mejor control y visibilidad y, potencialmente, le ayuda a limitar los excedentes de licencias y a reducir el riesgo de que se produzcan problemas de incumplimiento y de informes erróneos.

El AWS License Manager marco está integrado con License Manager para agregar información sobre el uso de las licencias en función de las reglas de licencia definidas por el cliente.

Uso de este marco

Puede utilizar el marco de AWS License Manager como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan según las normas de licencia definidas por el cliente. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el AWS License Manager marco. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del AWS License Manager marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
AWS License Manager	27	0	6

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si sus sistemas cumplen con las normas de licencia. Además, no pueden garantizar que supere una auditoría de uso de las licencias.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

Enlaces de License Manager

- AWS License Manager página de servicio
- AWS License Manager guía de usuario

License Manager APIs

Para este marco, Audit Manager utiliza una actividad personalizada llamada `GetLicenseManagerSummary` para recopilar pruebas. La `GetLicenseManagerSummary` actividad llama a los tres License Manager siguientes APIs:

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

Los datos que se devuelven se convierten luego en pruebas y se adjuntan a los controles pertinentes de la evaluación.

Por ejemplo: supongamos que utiliza dos productos con licencia (SQL Server 2017 y Oracle Database Enterprise Edition). En primer lugar, la `GetLicenseManagerSummary` actividad llama a la ListLicenseConfigurationsAPI, que proporciona detalles de las configuraciones de licencia de su cuenta. A continuación, añade datos contextuales adicionales para cada configuración de licencia. Para ello, llama a ListUsageForLicenseConfigurationy ListAssociationsForLicenseConfiguration. Por último, convierte los datos de configuración de la licencia en pruebas y los adjunta a los controles respectivos del marco (4.5: licencia gestionada por el cliente para SQL Server 2017 y 3.0.4: licencia gestionada por el cliente para Oracle Database Enterprise Edition). Si utiliza un producto con licencia que no está cubierto por ninguno de los controles del marco, los datos de configuración de la licencia se adjuntan como evidencia del siguiente control: 5.0: Licencia gestionada por el cliente para otras licencias.

AWS Mejores prácticas de seguridad fundamentales

AWS Audit Manager proporciona un marco estándar prediseñado que respalda las mejores prácticas AWS fundamentales de seguridad.

Temas

- ¿Qué es el estándar de prácticas de seguridad básicas recomendadas de AWS ?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es el estándar de prácticas de seguridad básicas recomendadas de AWS ?

El estándar AWS básico de mejores prácticas de seguridad es un conjunto de controles que detectan cuándo las cuentas y los recursos implementados se desvían de las mejores prácticas de seguridad.

Puede utilizar este estándar para evaluar de forma continua todas sus cargas de trabajo Cuentas de AWS y para identificar rápidamente las áreas en las que se desvíe de las mejores prácticas. El estándar proporciona orientación práctica y normativa sobre cómo mejorar y mantener la política de seguridad de su organización.

Los controles incluyen las prácticas recomendadas en varios Servicios de AWS. A cada control se le asigna una categoría que refleja la función de seguridad a la que se aplica. Para obtener más información, consulte Categorías de control en la Guía del usuario de AWS Security Hub .

Uso de este marco

Puede utilizar el marco AWS fundamental de mejores prácticas de seguridad como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos AWS fundamentales de las mejores prácticas de seguridad. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar los recursos de Cuentas de AWS sus servicios. Lo hace basándose en los controles que se definen en el marco de mejores prácticas AWS fundamentales de seguridad. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco AWS fundamental de mejores prácticas de seguridad son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
AWS Mejores prácticas fundamentales de seguridad	146	0	31

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si sus sistemas cumplen con las mejores prácticas de seguridad AWS fundamentales. Además, no pueden garantizar que supere una auditoría de las mejores prácticas de seguridad AWS fundamentales.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- AWS Las mejores prácticas fundamentales de seguridad son un estándar en la Guía del usuario AWS Security Hub
- Categorías de control en la AWS Security Hub Guía de usuario

AWS Mejores prácticas operativas

AWS Audit Manager proporciona un marco de mejores prácticas AWS operativas (OBP) prediseñado para ayudarlo en la preparación de la auditoría.

Este marco ofrece un subconjunto de controles del estándar AWS Fundational Security Best Practices. Estos controles sirven como comprobaciones básicas para detectar cuándo las cuentas y los recursos implementados se desvían de las prácticas de seguridad recomendadas.

Temas

- ¿Qué es el estándar de mejores AWS prácticas de seguridad fundamentales?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es el estándar de mejores AWS prácticas de seguridad fundamentales?

Puede usar el estándar de prácticas de seguridad básicas recomendadas de AWS para evaluar sus cuentas y cargas de trabajo e identificar rápidamente las áreas en las que se desvía de las prácticas recomendadas. El estándar proporciona orientación práctica y normativa sobre cómo mejorar y mantener la política de seguridad de su organización.

Los controles incluyen las prácticas recomendadas en varios Servicios de AWS. A cada control se le asigna una categoría que refleja la función de seguridad a la que se aplica. Para obtener más información, consulte Categorías de control en la Guía del usuario de AWS Security Hub .

Uso de este marco

Puede utilizar el marco de prácticas operativas recomendadas de AWS como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de las mejores prácticas AWS operativas. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Los detalles del marco de mejores prácticas AWS operativas son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
AWS Mejores prácticas operativas	0	51	20

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.

Los controles de este marco no tienen por objeto verificar si sus sistemas cumplen con las mejores prácticas AWS operativas. Además, no pueden garantizar que supere una auditoría de las prácticas operativas recomendadas de AWS .

Este marco incluye solo controles manuales. Estos controles manuales no recopilan pruebas automáticamente. AWS Audit Manager no comprueba automáticamente los controles procesales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- AWS Las mejores prácticas fundamentales de seguridad son una norma básica en la Guía del AWS Security Hub usuario
- Categorías de control en la AWS Security Hub Guía de usuario

AWS Well Architected Framework (WAF v1.0)

AWS Audit Manager proporciona un marco estándar prediseñado que es compatible con AWS Well-Architected Framework v10.

Temas

- ¿Qué es el AWS Well-Architected Framework?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es el AWS Well-Architected Framework?

AWS Well-Architected es un marco que puede ayudarlo a crear infraestructuras seguras, de alto rendimiento, resistentes y eficientes para sus aplicaciones y cargas de trabajo. Basado en seis pilares (excelencia operativa, seguridad, fiabilidad, eficiencia del rendimiento, optimización de costos y sostenibilidad)AWS Well-Architected proporciona un enfoque coherente para que usted y sus socios evalúen arquitecturas e implementen diseños que puedan escalarse con el tiempo.

Uso de este marco

Puede utilizar el AWS Well-Architected Framework como ayuda para prepararse para las auditorías. Este marco describe los conceptos clave, los principios de diseño y las prácticas recomendadas en

cuanto a arquitectura para diseñar y ejecutar cargas de trabajo en la nube. De los seis pilares en los que se basa AWS Well-Architected, los pilares de seguridad y fiabilidad son los pilares para los que AWS Audit Manager ofrece un marco y controles prediseñados. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el AWS Well-Architected Framework. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Marco de Amazon Web Services (AWS) Well-Architected (WAF) v10	43	291	6

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el ConfigDataSourceMappingsarchivo AuditManager _ _AWS-Well-Architected-Framework-WAF-v10.zip.

Los controles de este marco de no tienen por objeto comprobar si los sistemas cumplen con las normas. Además, no pueden garantizar que supere una auditoría.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- AWS Well-Architected
- AWS Documentación de Well-Architected Framework

CCCS Medium Cloud Control

AWS Audit Manager proporciona un marco estándar prediseñado que respalda el control de nubes medianas del Centro Canadiense de Ciberseguridad (CCCS).

Temas

- ¿Qué es el CCCS?
- Uso de este marco
- Pasos a seguir a continuación

¿Qué es el CCCS?

El CCCS es la fuente autorizada de orientación, servicios y apoyo de expertos en ciberseguridad de Canadá. El CCCS proporciona esta experiencia a los gobiernos, la industria y el público en general de Canadá. Las organizaciones del sector público canadiense de todo el país se basan en sus rigurosas evaluaciones de los proveedores de servicios en la nube para tomar decisiones informadas sobre la adquisición de la nube.

En mayo de 2020, el perfil medio de control de la nube del CCCS sustituyó al perfil PROTEGIDO B, integridad media y disponibilidad media (PBMM) del gobierno de Canadá. El perfil medio de control de seguridad de la nube del CCCS es adecuado si su organización utiliza servicios de nube pública para respaldar las actividades empresariales con requisitos de confidencialidad, integridad y disponibilidad (AIC) medios. Si el volumen de trabajo está sujeto a requisitos de AIC medios, cabe esperar razonablemente que la divulgación, modificación o pérdida de acceso no autorizados a la información o los servicios utilizados por la actividad empresarial provoque un perjuicio grave a una persona u organización o un perjuicio limitado a un grupo de personas. A continuación, se muestran ejemplos de estos niveles de lesión:

- Efecto significativo en el beneficio anual
- Pérdida de cuentas principales
- Pérdida de buena voluntad
- Infracción de conformidad clara
- Violación de la privacidad para cientos o miles de personas
- Afecta al rendimiento del programa
- Provoca un trastorno o enfermedad mental
- Sabotaje
- Daño a su reputación
- Dificultades financieras individuales

Uso de este marco

Puede utilizar el AWS Audit Manager marco de CCCS Medium Cloud Control como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos del CCCS. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar evidencias pertinentes para una auditoría del CCCS Medium Cloud Control. En su evaluación, puede especificar lo Cuentas de AWS que desea incluir en el alcance de la auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco de CCCS Medium Cloud Control. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas

que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Canadian Centre for Cyber Security (CCCS) Medium Cloud Control	71	282	175

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el archivo AuditManager_ AuditManager _ ConfigDataSourceMappings _CCCS-Medium-Cloud-Control.zip.

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si sus sistemas cumplen con los requisitos de control de nubes medianas del CCCS. Además, no pueden garantizar que supere una auditoría del CCCS. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

CIS AWS Benchmark v1.2.0

AWS Audit Manager proporciona dos marcos prediseñados que son compatibles con Amazon Web Services () Benchmark v1.2.0 del Center for Internet Security (CIS AWS).

> **Note**
>
> - Para obtener información sobre los marcos de Audit Manager compatibles con la versión 1.3.0, consulte Índice de referencia CIS v1.3.0 AWS.
> - Para obtener información sobre los marcos de Audit Manager compatibles con la versión 1.4.0, consulte CIS AWS Benchmark v1.4.0.

Temas

- ¿Qué es CIS?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es CIS?

El CIS es una organización sin fines de lucro que desarrolló el CIS AWS Foundations Benchmark. Este punto de referencia sirve como un conjunto de mejores prácticas de configuración de seguridad para AWS. Estas mejores prácticas aceptadas por la industria van más allá de las directrices de seguridad de alto nivel ya disponibles, ya que proporcionan procedimientos claros de step-by-step implementación y evaluación.

Para obtener más información, consulte las publicaciones del blog CIS AWS Foundations Benchmark en el blog AWS de seguridad.

Diferencia entre los CIS Benchmarks y los controles CIS

Los CIS Benchmarks son pautas de prácticas de seguridad específicas recomendadas para los productos de los proveedores. Desde sistemas operativos hasta servicios en la nube y dispositivos de red, la configuración que se aplica desde un punto de referencia protege los sistemas específicos que utiliza su organización. Los controles CIS son pautas de prácticas fundamentales recomendadas que deben seguir los sistemas a nivel de organización para ayudar a protegerse contra los vectores de ciberataque conocidos.

Ejemplos

- Los CIS Benchmarks son prescriptivos. Por lo general, hacen referencia a una configuración específica que se puede revisar y establecer en el producto del proveedor.

  Ejemplo: CIS AWS Benchmark v1.2.0: asegúrese de que el MFA esté habilitado para la cuenta de «usuario raíz».

  Esta recomendación proporciona una guía prescriptiva sobre cómo comprobarlo y cómo configurarlo en la cuenta raíz del entorno. AWS
- Los controles de CIS son para su organización en su conjunto. No son específicos de un solo producto de un proveedor.

  Ejemplo: (CIS v7.1) utilice la autenticación multifactor para todo el acceso administrativo.

  Este control describe lo que se espera que se aplique en su organización. No describe cómo debe aplicarlo a los sistemas y las cargas de trabajo que ejecuta (independientemente de dónde se encuentren).

Uso de este marco

Puede utilizar los marcos CIS AWS Benchmark v1.2 para prepararse AWS Audit Manager para las auditorías del CIS. También puede personalizar estos marcos y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza los marcos como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace basándose en los controles que se definen en el marco de CIS. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de

las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Nivel 1	33	3	4
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Nivel 1 y 2	45	4	4

Important

Para garantizar que estos marcos recopilen las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
Para garantizar que estos marcos recopilen las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar una lista de las AWS Config reglas que se utilizan como mapeos de fuentes de datos para estos marcos estándar, descargue los siguientes archivos:

1. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.2.0, -Level-1.zip
2. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.2.0, -Level-1-and-2.zip

Los controles de estos marcos no están diseñados para verificar si sus sistemas cumplen con las mejores prácticas de CIS Benchmark. AWS Además, no pueden garantizar que supere una auditoría

del CIS. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Requisitos previos para utilizar estos marcos de trabajo

Muchos controles de los marcos CIS AWS Benchmark v1.2 se utilizan AWS Config como tipo de fuente de datos. Para admitir estos controles, debe activarlos AWS Config en todas las cuentas en las que Región de AWS haya activado Audit Manager. También debe asegurarse de que AWS Config las reglas específicas estén habilitadas y de que estas reglas estén configuradas correctamente.

Se requieren las siguientes AWS Config reglas y parámetros para recopilar las pruebas correctas y obtener un estado de cumplimiento preciso de la versión 1.2 del CIS AWS Foundations Benchmark. Para obtener instrucciones sobre cómo habilitar o configurar una norma, consulte Trabajar con las normas administradas de AWS Config.

Regla obligatoria AWS Config	Parámetros necesarios
ACCESS_KEYS_ROTATED	**`maxAccessKeyAge`** • El número máximo de días sin rotación. • Tipo: Int • Predeterminado: 90 días • Requisito de cumplimiento: un máximo de 90 días
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	No aplicable
CLOUD_TRAIL_ENCRYPTION_ENABLED	No aplicable
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	No aplicable
CMK_BACKING_KEY_ROTATION_ENABLED	No aplicable
IAM_PASSWORD_POLICY	**`MaxPasswordAge`** (opcional) • El número de días antes de la contraseña venza.

Regla obligatoria AWS Config	Parámetros necesarios
	• Tipo: int • Predeterminado: 90 • Requisito de cumplimiento: un máximo de 90 días
IAM_PASSWORD_POLICY	**`MinimumPasswordLength`** (opcional) • La longitud mínima de la contraseña. • Tipo: int • Predeterminado: 14 • Requisito de cumplimiento: 14 caracteres como mínimo
IAM_PASSWORD_POLICY	**`PasswordReusePrevention`** (opcional) • El número de contraseñas antes de que se permita reutilizarlas. • Tipo: int • Predeterminado: 24 • Requisito de cumplimiento: un mínimo de 24 contraseñas antes de volver a utilizarlas
IAM_PASSWORD_POLICY	**`RequireLowercaseCharacters`** (opcional) • Requiere que al menos haya un carácter en minúscula en la contraseña. • Tipo: Booleano • Valor predeterminado: True • Requisito de conformidad: al menos un carácter en minúscula

Regla obligatoria AWS Config	Parámetros necesarios
IAM_PASSWORD_POLICY	**`RequireNumbers`** (opcional) • Requiere que al menos haya un número en la contraseñ a. • Tipo: Booleano • Valor predeterminado: True • Requisito de cumplimiento: al menos un carácter numérico
IAM_PASSWORD_POLICY	**`RequireSymbols`** (opcional) • Requiere que al menos haya un símbolo en la contraseñ a. • Tipo: Booleano • Valor predeterminado: True • Requisito de conformidad: al menos un símbolo
IAM_PASSWORD_POLICY	**`RequireUppercaseCharacters`** (opcional) • Requiere que al menos haya un carácter en mayúscula en la contraseña. • Tipo: Booleano • Valor predeterminado: True • Requisito de conformidad: al menos un carácter en mayúscula

Regla obligatoria AWS Config	Parámetros necesarios
IAM_POLICY_IN_USE	**`policyARN`** • Un ARN de política de IAM que debe comprobarse. • Tipo: cadena • Requisito de conformidad: crea una función de IAM para gestionar los AWS incidentes. **`policyUsageType`** (opcional) • Especifica si espera que la política se adjunte a un usuario, grupo o rol. • Tipo: cadena • Valores válidos: `IAM_USER` | `IAM_GROUP` | `IAM_ROLE` | `ANY` • Valor predeterminado: `ANY` • Requisito de cumplimiento: adjunte la política de confianza al rol de IAM creado
IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	No aplicable
IAM_ROOT_ACCESS_KEY_CHECK	No aplicable
IAM_USER_NO_POLICIES_CHECK	No aplicable
IAM_USER_UNUSED_CREDENTIALS_CHECK	**`maxCredentialUsageAge`** • El número máximo de días durante los que no se puede usar una credencial. • Tipo: Int • Predeterminado: 90 días • Requisito de cumplimiento: 90 días o más
INCOMING_SSH_DISABLED	No aplicable

Regla obligatoria AWS Config	Parámetros necesarios
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	No aplicable
MULTI_REGION_CLOUD_TRAIL_ENABLED	No aplicable

Regla obligatoria AWS Config	Parámetros necesarios
RESTRICTED_INCOMING_TRAFFIC	**`blockedPort1`** (opcional) • El número de puerto TCP bloqueado. • Tipo: int • Predeterminado: 20 • Requisito de cumplimiento: asegúrese de que ningún grupo de seguridad permita la entrada en los puertos bloqueados **`blockedPort2`** (opcional) • El número de puerto TCP bloqueado. • Tipo: int • Predeterminado: 21 • Requisito de cumplimiento: asegúrese de que ningún grupo de seguridad permita la entrada en los puertos bloqueados **`blockedPort3`** (opcional) • El número de puerto TCP bloqueado. • Tipo: int • Valor predeterminado: 3389 • Requisito de cumplimiento: asegúrese de que ningún grupo de seguridad permita la entrada en los puertos bloqueados **`blockedPort4`** (opcional) • El número de puerto TCP bloqueado. • Tipo: int • Predeterminado: 3306 • Requisito de cumplimiento: asegúrese de que ningún grupo de seguridad permita la entrada en los puertos bloqueados **`blockedPort5`** (opcional) • El número de puerto TCP bloqueado.

Regla obligatoria AWS Config	Parámetros necesarios
	• Tipo: int • Predeterminado: 4333 • Requisito de cumplimiento: asegúrese de que ningún grupo de seguridad permita la entrada en los puertos bloqueados
ROOT_ACCOUNT_HARDWARE_MFA_ENABLED	No aplicable
ROOT_ACCOUNT_MFA_ENABLED	No aplicable
S3_BUCKET_LOGGING_ENABLED	**`targetBucket`** (opcional) • El bucket de S3 de destino para almacenar registros de acceso al servidor. • Tipo: cadena • Requisito de conformidad: habilitar el registro **`targetPrefix`** (opcional) • El prefijo del bucket de S3 para almacenar registros de acceso al servidor. • Tipo: cadena • Requisito de cumplimiento: identifique el depósito de S3 para CloudTrail el registro
S3_BUCKET_PUBLIC_READ_PROHIBITED	No aplicable
VPC_DEFAULT_SECURITY_GROUP_CLOSED	No aplicable

Regla obligatoria AWS Config	Parámetros necesarios
VPC_FLOW_LOGS_ENABLED	**`trafficType`** (opcional) • El `trafficType` de los registros de flujo. • Tipo: cadena • Requisito de cumplimiento: el registro de flujos está habilitado

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de estos marcos, incluida la lista de controles estándar que incluyen, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de estos marcos, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar estos marcos para que se adapten a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- El punto de referencia de los AWS fundamentos de la CEI, versión 1.2.0
- Publicaciones del blog sobre Foundations Benchmark CIS AWS en el blog de seguridad de AWS .

Índice de referencia CIS v1.3.0 AWS

AWS Audit Manager proporciona dos marcos estándar prediseñados que admiten la versión 1.3 de CIS AWS Benchmark.

> **Note**
>
> - Para obtener información sobre los marcos de Audit Manager compatibles con v1.2.0, consulte CIS AWS Benchmark v1.2.0.

- Para obtener información sobre los marcos de Audit Manager compatibles con la versión 1.4.0, consulte CIS AWS Benchmark v1.4.0.

Temas

- ¿Qué es el índice de referencia AWS CIS?
- Usar estos marcos
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es el índice de referencia AWS CIS?

El CIS desarrolló el CIS AWS Foundations Benchmark v1.3.0, un conjunto de mejores prácticas de configuración de seguridad para. AWS Estas mejores prácticas aceptadas por la industria van más allá de las directrices de seguridad de alto nivel ya disponibles, ya que proporcionan a AWS los usuarios procedimientos claros de step-by-step implementación y evaluación.

Para obtener más información, consulte las publicaciones del blog CIS AWS Foundations Benchmark en el blog AWS de seguridad.

La versión 1.3.0 de CIS AWS Benchmark proporciona una guía para configurar las opciones de seguridad para un subconjunto de ellas Servicios de AWS , haciendo hincapié en las configuraciones fundamentales, comprobables y independientes de la arquitectura. Algunos de los Amazon Web Services específicos que se incluyen en este documento incluyen los siguientes:

- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (predeterminado)

Diferencia entre los CIS Benchmarks y los controles CIS

Los CIS Benchmarks son pautas de prácticas de seguridad específicas recomendadas para los productos de los proveedores. Desde sistemas operativos hasta servicios en la nube y dispositivos de red, los ajustes que se aplican a partir de un punto de referencia protegen los sistemas que utiliza su organización. Los controles CIS son pautas fundamentales de prácticas recomendadas que debe seguir su organización para protegerse de los vectores de ciberataques conocidos.

Ejemplos

- Los CIS Benchmarks son prescriptivos. Por lo general, hacen referencia a una configuración específica que se puede revisar y establecer en el producto del proveedor.

  Ejemplo: CIS AWS Benchmark v1.3.0: asegúrese de que el MFA esté habilitado para la cuenta de «usuario root»

  Esta recomendación proporciona una guía prescriptiva sobre cómo comprobarlo y cómo configurarlo en la cuenta raíz del entorno. AWS
- Los controles CIS son para su organización en su conjunto y no son específicos de un solo producto de un proveedor.

  Ejemplo: (CIS v7.1) utilice la autenticación multifactor para todo el acceso administrativo.

  Este control describe lo que se espera que se aplique en su organización, pero no cómo debe aplicarlo a los sistemas y las cargas de trabajo que ejecuta (independientemente de dónde se encuentren).

Usar estos marcos

Puede utilizar los marcos CIS AWS Benchmark v1.3 para prepararse AWS Audit Manager para las auditorías del CIS. También puede personalizar estos marcos y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza los marcos como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace basándose en los controles que se definen en el marco de CIS. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En

cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Nivel 1	32	5	5
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Nivel 1 y 2	49	6	5

> **Important**
>
> Para garantizar que estos marcos recopilen las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que estos marcos recopilen las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar una lista de las AWS Config reglas que se utilizan como mapeos de fuentes de datos para estos marcos estándar, descargue los siguientes archivos:
>
> 1. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.3.0, -Level-1.zip
> 2. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.3.0, -Level-1-and-2.zip

Los controles de estos marcos no están diseñados para verificar si sus sistemas cumplen con las mejores prácticas de CIS Benchmark. AWS Además, no pueden garantizar que supere una auditoría del CIS. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de estos marcos, incluida la lista de controles estándar que incluyen, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de estos marcos, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar estos marcos para que se adapten a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Publicaciones del blog sobre Foundations Benchmark CIS AWS en el blog de seguridad de AWS .

CIS AWS Benchmark v1.4.0

AWS Audit Manager proporciona dos marcos estándar prediseñados que respaldan la versión 1.4.0 de AWS Foundations Benchmark del Center for Internet Security (CIS).

> **Note**
>
> - Para obtener información sobre los marcos de Audit Manager compatibles con v1.2.0, consulte CIS AWS Benchmark v1.2.0.
> - Para obtener información sobre los marcos de Audit Manager compatibles con la versión 1.3.0, consulte Índice de referencia CIS v1.3.0 AWS.

Temas

- ¿Qué es el índice de referencia CIS? AWS
- Utilice estos marcos para respaldar la preparación de la auditoría
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es el índice de referencia CIS? AWS

El CIS AWS Benchmark v1.4.0 proporciona una guía prescriptiva para configurar las opciones de seguridad para un subconjunto de Amazon Web Services. Hace hincapié en las configuraciones fundamentales, comprobables e independientes de la arquitectura. Algunos de los Amazon Web Services específicos que se incluyen en este documento incluyen los siguientes:

- AWS Identity and Access Management (IAM)
- Analizador de acceso de IAM
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Virtual Private Cloud

Diferencia entre los CIS Benchmarks y los controles CIS

Los CIS Benchmarks son pautas de prácticas de seguridad específicas recomendadas para los productos de los proveedores. Desde sistemas operativos hasta servicios en la nube y dispositivos de red, los ajustes que se aplican desde un punto de referencia protegen los sistemas que se utilizan. Los controles CIS son pautas fundamentales de prácticas recomendadas que debe seguir su organización para protegerse de los vectores de ciberataques conocidos.

Ejemplos

- Los CIS Benchmarks son prescriptivos. Por lo general, hacen referencia a una configuración específica que se puede revisar y establecer en el producto del proveedor.

  Ejemplo: CIS AWS Benchmark v1.3.0: asegúrese de que el MFA esté habilitado para la cuenta de «usuario root»

  Esta recomendación proporciona una guía prescriptiva sobre cómo comprobarlo y cómo configurarlo en la cuenta raíz del entorno. AWS

- Los controles CIS son para su organización en su conjunto y no son específicos de un solo producto de un proveedor.

  Ejemplo: (CIS v7.1) utilice la autenticación multifactor para todo el acceso administrativo.

  Este control describe lo que se espera que se aplique en su organización. Sin embargo, no describe cómo aplicarlo a los sistemas y cargas de trabajo que se están ejecutando, independientemente de dónde se encuentren.

Utilice estos marcos para respaldar la preparación de la auditoría

Puede utilizar los marcos CIS AWS Benchmark v1.4.0 para prepararse AWS Audit Manager para las auditorías del CIS. También puede personalizar estos marcos y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza los marcos como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace basándose en los controles que se definen en el marco de CIS. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Nivel 1	32	6	5

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Nivel 1 y 2	50	8	5

> **Important**
>
> Para garantizar que estos marcos recopilen las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que estos marcos recopilen las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar una lista de las AWS Config reglas que se utilizan como mapeos de fuentes de datos para estos marcos estándar, descargue los siguientes archivos:
>
> 1. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.4.0, -Level-1.zip
> 2. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.4.0, -Level-1-and-2.zip

Los controles de estos marcos no están diseñados para verificar si sus sistemas cumplen con el CIS Benchmark v1.4.0. AWS Además, no pueden garantizar que supere una auditoría del CIS. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de estos marcos, incluida la lista de controles estándar que incluyen, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de estos marcos, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar estos marcos para que se adapten a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- CIS Benchmarks del Centro para la seguridad de Internet (CIS)
- Publicaciones del blog sobre Foundations Benchmark CIS AWS en el blog de seguridad de AWS .

CIS Controls v7.1, IG1

AWS Audit Manager proporciona un marco estándar prediseñado que admite el grupo de implementación 1 de Center for Internet Security (CIS) v7.1.

> **Note**
>
> Para obtener información sobre CIS v8, IG1and el AWS Audit Manager marco que admite este estándar, consulte. CIS Critical Security Controls versión 8.0, IG1

Temas

- ¿Qué son los controles CIS?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué son los controles CIS?

Los controles del CIS son un conjunto de acciones priorizadas que, en conjunto, forman un defense-in-depth conjunto de mejores prácticas. Estas prácticas recomendadas mitigan los ataques más comunes contra sistemas y redes. El Grupo de Implementación 1 se define generalmente para una organización con recursos limitados y experiencia en ciberseguridad que está disponible para implementar subcontroles.

Diferencia entre los controles CIS y los CIS Benchmarks

Los controles CIS son pautas fundamentales de prácticas recomendadas que una organización puede seguir para protegerse de los vectores de ciberataques conocidos. Los CIS Benchmarks son pautas de prácticas de seguridad específicas recomendadas para los productos de los proveedores. Desde sistemas operativos hasta servicios en la nube y dispositivos de red, los ajustes que se aplican desde un punto de vista comparativo protegen los sistemas que se utilizan.

Ejemplos

- Los CIS Benchmarks son prescriptivos. Por lo general, hacen referencia a una configuración específica que se puede revisar y establecer en el producto del proveedor.
  - Ejemplo: CIS AWS Benchmark v1.2.0: asegúrese de que el MFA esté habilitado para la cuenta de «usuario root»
  - Esta recomendación proporciona una guía prescriptiva sobre cómo comprobarlo y cómo configurarlo en la cuenta raíz del entorno. AWS
- Los controles CIS son para su organización en su conjunto y no son específicos de un solo producto de un proveedor.
  - Ejemplo: (CIS v7.1) utilice la autenticación multifactor para todo el acceso administrativo.
  - Este control describe lo que se espera que se aplique en su organización. Sin embargo, no le indica cómo debe aplicarlo a los sistemas y las cargas de trabajo que está ejecutando (independientemente de dónde se encuentren).

Uso de este marco

Puede utilizar el IG1 marco CIS Controls v7.1 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de CIS. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el IG1 marco CIS Controls v7.1. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En

cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del IG1 marco CIS Controls v7.1 son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Center for Internet Security (CIS) v7.1, IG1	8	35	18

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el archivo AuditManager_ ConfigDataSourceMappings _Center-For-Internet-Security- (CIS) -v7.1, - .zip. IG1

Los controles de este marco no tienen por objeto comprobar si sus sistemas cumplen con los controles CIS. Además, no pueden garantizarle que vaya a superar una auditoría de CIS. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- CIS Controls, versión 7.1 IG1

CIS Critical Security Controls versión 8.0, IG1

AWS Audit Manager proporciona un marco estándar prediseñado que es compatible con la versión 8.0 de CIS Critical Security Controls, grupo de implementación 1.

> **Note**
>
> Para obtener información sobre CIS v7.1 IG1 y el AWS Audit Manager marco que admite este estándar, consulte. CIS Controls v7.1, IG1

Temas

- ¿Qué son los controles CIS?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué son los controles CIS?

Los controles de seguridad críticos de CIS (controles CIS) son un conjunto de salvaguardas priorizado para mitigar los ciberataques más frecuentes contra sistemas y redes. Están mapeados y referenciados por múltiples marcos legales, regulatorios y políticos. La versión 8 de los controles CIS se ha mejorado para adaptarse a los sistemas y software modernos. La transición a la informática basada en la nube, la virtualización, la movilidad, la subcontratación y los cambios en las tácticas de los atacantes impulsaron la actualización. work-from-home Esta actualización contribuye a la seguridad de las empresas a medida que se trasladan a entornos totalmente en la nube o híbridos.

Diferencia entre los controles CIS y los CIS Benchmarks

Los controles CIS son pautas fundamentales de prácticas recomendadas que una organización puede seguir para protegerse de los vectores de ciberataques conocidos. Los CIS Benchmarks son pautas de prácticas de seguridad específicas recomendadas para los productos de los proveedores.

Desde sistemas operativos hasta servicios en la nube y dispositivos de red, los ajustes que se aplican desde un punto de vista comparativo protegen los sistemas que se utilizan.

Ejemplos

- Los CIS Benchmarks son prescriptivos. Por lo general, hacen referencia a una configuración específica que se puede revisar y establecer en el producto del proveedor.
  - Ejemplo: CIS AWS Benchmark v1.2.0: asegúrese de que el MFA esté habilitado para la cuenta de «usuario root»
  - Esta recomendación proporciona una guía prescriptiva sobre cómo comprobarlo y cómo configurarlo en la cuenta raíz del entorno. AWS
- Los controles CIS son para su organización en su conjunto y no son específicos de un solo producto de un proveedor.
  - Ejemplo: (CIS v7.1) utilice la autenticación multifactor para todo el acceso administrativo.
  - Este control describe lo que se espera que se aplique en su organización. Sin embargo, no le indica cómo debe aplicarlo a los sistemas y las cargas de trabajo que está ejecutando (independientemente de dónde se encuentren).

Uso de este marco

Puede utilizar el IG1 marco CIS v8 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de CIS. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace basándose en los controles que se definen en el marco CIS v8. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
CIS Critical Security Controls versión 8.0 (CIS v8.0), IG1	11	45	15

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el archivo AuditManager_ ConfigDataSourceMappings _cis-Critical-Security-Controls-Version8.0- (CIS-v8.0), - .zip. IG1

Los controles de este marco no tienen por objeto comprobar si sus sistemas cumplen con los controles CIS. Además, no pueden garantizarle que vaya a superar una auditoría de CIS. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Controles CIS v8

FedRAMP Security Baseline Controls r4

AWS Audit Manager proporciona un marco estándar prediseñado que respalda el Security Baseline Controls r4 del Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP).

Temas

- ¿Qué es FedRAMP?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es FedRAMP?

FedRAMP se estableció en 2011. Proporciona un enfoque rentable y basado en el riesgo para la adopción y el uso de los servicios en la nube por parte del gobierno federal de EE. UU. FedRAMP permite a las agencias federales utilizar tecnologías de nube modernas, con énfasis en la seguridad y la protección de la información federal.

Para obtener más información sobre los controles de referencia moderados de FedRAMP, consulte la plantilla de procedimientos de casos de pruebas de seguridad moderada de FedRAMP.

Uso de este marco

Puede utilizar el marco de FedRAMP r4 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de FedRAMP r4. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o

crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco de referencia moderada de FedRAMP son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Federal Risk And Authorization Management Program (FedRAMP) Security Baseline Controls r4, Moderate	36	289	17

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el ConfigDataSourceMappingsarchivo AuditManager _ _FedRAMP-Security-Baseline-Controls-r4-Moderate.zip.

Los controles de este marco no tienen por objeto verificar si los sistemas cumplen con FedRAMP r4. Además, no pueden garantizarle que vaya a superar una auditoría del FedRAMP. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- AWS Página de conformidad para FedRAMP
- AWS Publicaciones del blog de FedRAMP

GDPR 2016

AWS Audit Manager proporciona un marco estándar prediseñado que respalda el Reglamento General de Protección de Datos (GDPR) de 2016.

Este marco incluye solo controles manuales. Estos controles manuales no recopilan evidencias automáticamente. Sin embargo, si quiere automatizar la recopilación de evidencias para algunos controles contemplados en el GDPR, puede utilizar la característica de control personalizado que se incluye en Audit Manager. Para obtener más información, consulte Uso de este marco.

Temas

- ¿Qué es GDPR?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es GDPR?

GDPR es una nueva ley europea de privacidad que entró en vigor el 25 de mayo de 2018. El RGPD sustituye a la Directiva de protección de datos de la UE, también conocida como Directiva 95/46/EC. Su objetivo es armonizar las leyes de protección de datos en toda la Unión Europea (UE). Para ello, aplica una única ley de protección de datos que es vinculante en todos los estados miembros de la UE.

El RGPD se aplica a todas las organizaciones establecidas en la UE y a las organizaciones (independientemente de si están establecidas en la UE) que procesan los datos personales de los interesados de la UE en relación con la oferta de bienes o servicios a interesados en la UE o con el

seguimiento del comportamiento que tiene lugar dentro de la UE. Los datos personales son cualquier información relacionada con una persona física identificada o identificable.

Puede encontrar el marco de GDPR en la página de la biblioteca de marcos de Audit Manager. Para obtener más información, consulte el Centro del RGPD.

Uso de este marco

Puede utilizar el marco de GDPR 2016 en Audit Manager como ayuda para prepararse para las auditorías.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
General Data Protection Regulation (GDPR) 2016	0	378	10

Este marco estándar solo incluye controles manuales.

> **Note**
>
> Si desea automatizar la recopilación de pruebas para el RGPD, puede usar Audit Manager para crear sus propios controles personalizados para el RGPD. En la siguiente tabla, se proporcionan recomendaciones sobre las fuentes de AWS datos que puedes asignar a los requisitos del RGPD en tus controles personalizados. Aunque algunas de las siguientes origen de datos están asignadas a varios controles, tenga en cuenta que solo se le cobrará una vez por cada evaluación de recursos.
> Las siguientes recomendaciones utilizan AWS Config y AWS Security Hub como fuentes de datos. Para recopilar correctamente pruebas de estas fuentes de datos, asegúrese de seguir las instrucciones para habilitar y configurar AWS Config y AWS Security Hub en su Cuenta de AWS. Una vez configurados ambos servicios de esta manera, Audit Manager recopila pruebas cada vez que se realiza una evaluación para la AWS Config regla especificada o el control de Security Hub.

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
Artículo 25 Protección de datos desde el diseño y por defecto.1	Capítulo 4: Controlador y procesador	Puede crear un control personalizado AWS Audit Manager que respalde este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período • AWS CloudTrail el bucket no es público • Muestre todas las políticas con una `Allow:*:*` y enumere todos los principales y servicios que utilizan esas políticas Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config el tipo de fuente de datos y seleccione las siguientes reglas AWS Config administradas como mapeos de fuentes de datos: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Elija AWS Security Hub el tipo de fuente de datos y seleccione los siguientes controles de Security Hub como asignaciones de fuentes de datos: • 1.1 (.1) CloudWatch • 1.1 (IAM.20) • 1.10 (IAM.16)

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (.11) CloudWatch

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• 3.12 (.12) CloudWatch • 3.13 (.13) CloudWatch • 3.14 (.14) CloudWatch • Config.1

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
Artículo 25 Protección de datos desde el diseño y por defecto.2	Capítulo 4: Controlador y procesador	Puede crear un control personalizado AWS Audit Manager que respalde este control del GDPR. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período • AWS CloudTrail el bucket no es público • Muestre todas las políticas con una `Allow:*:*` y enumere todos los principales y servicios que utilizan esas políticas Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config el tipo de fuente de datos y seleccione las siguientes reglas AWS Config administradas como mapeos de fuentes de datos: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Elija AWS Security Hub el tipo de fuente de datos y seleccione los siguientes controles de Security Hub como asignaciones de fuentes de datos: • 1.1 (.1) CloudWatch • 1.1 (IAM.20) • 1.10 (IAM.16)

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (.11) CloudWatch

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• 3.12 (.12) CloudWatch • 3.13 (.13) CloudWatch • 3.14 (.14) CloudWatch • Config.1

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
Artículo 25 Protección de datos desde el diseño y por defecto.3	Capítulo 4: Controlador y procesador	Puede crear un control personalizado AWS Audit Manager que respalde este control del GDPR. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período • AWS CloudTrail el bucket no es público • Muestre todas las políticas con una `Allow:*:*` y enumere todos los principales y servicios que utilizan esas políticas Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config el tipo de fuente de datos y seleccione las siguientes reglas AWS Config administradas como mapeos de fuentes de datos: • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Elija AWS Security Hub el tipo de fuente de datos y seleccione los siguientes controles de Security Hub como asignaciones de fuentes de datos: • 1.1 (.1) CloudWatch • 1.1 (IAM.20) • 1.10 (IAM.16)

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5 • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10) • 3.11 (.11) CloudWatch

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• 3.12 (.12) CloudWatch • 3.13 (.13) CloudWatch • 3.14 (.14) CloudWatch • Config.1

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
Artículo 30 Registros de las actividades de procesamiento.1	Capítulo 4: Controlador y procesador	Puede crear un control personalizado AWS Audit Manager que respalde este control del GDPR. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config el tipo de fuente de datos y seleccione las siguientes reglas AWS Config administradas como mapeos de fuentes de datos: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Elija AWS Security Hub el tipo de fuente de datos y seleccione el siguiente control de Security Hub como mapeo de la fuente de datos: • Config.1

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
Artículo 30 Registros de las actividades de procesamiento.2	Capítulo 4: Controlador y procesador	Puede crear un control personalizado AWS Audit Manager que sea compatible con este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config el tipo de fuente de datos y seleccione las siguientes reglas AWS Config administradas como mapeos de fuentes de datos: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Elija AWS Security Hub el tipo de fuente de datos y seleccione el siguiente control de Security Hub como mapeo de la fuente de datos: • Config.1

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
Artículo 30 Registros de las actividades de procesamiento.3	Capítulo 4: Controlador y procesador	Puede crear un control personalizado AWS Audit Manager que sea compatible con este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período • AWS CloudTrail el bucket no es público • Muestre todas las políticas con una `Allow:*:*` y enumere todos los principales y servicios que utilizan esas políticas Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config el tipo de fuente de datos y seleccione las siguientes reglas AWS Config administradas como mapeos de fuentes de datos: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Elija AWS Security Hub el tipo de fuente de datos y seleccione el siguiente control de Security Hub como mapeo de la fuente de datos: • Config.1

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
Artículo 30 Registros de las actividades de procesamiento.4	Capítulo 4: Controlador y procesador	Puede crear un control personalizado AWS Audit Manager que sea compatible con este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período • AWS CloudTrail el bucket no es público • Muestre todas las políticas con una `Allow:*:*` y enumere todos los principales y servicios que utilizan esas políticas Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config el tipo de fuente de datos y seleccione las siguientes reglas AWS Config administradas como mapeos de fuentes de datos: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Elija AWS Security Hub el tipo de fuente de datos y seleccione el siguiente control de Security Hub como mapeo de la fuente de datos: • Config.1

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
Artículo 30 Registros de las actividades de procesamiento.5	Capítulo 4: Controlador y procesador	Puede crear un control personalizado AWS Audit Manager que sea compatible con este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Mostrar todos los eventos de la cuenta raíz a lo largo del período Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config el tipo de fuente de datos y seleccione las siguientes reglas AWS Config administradas como mapeos de fuentes de datos: • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Elija AWS Security Hub el tipo de fuente de datos y seleccione el siguiente control de Security Hub como mapeo de la fuente de datos: • Config.1

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
Artículo 32 Seguridad del procesamiento.1	Capítulo 4: Controlador y procesador	Puede crear un control personalizado AWS Audit Manager que sea compatible con este control del RGPD. Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Muestra el cifrado de los datos en reposo para todos los servicios • Muestra el cifrado de los datos en tránsito para todos los servicios • MFA Delete habilitada para Amazon S3 • Todos los escaneos de Amazon Inspector • Mostrar todas las instancias que no están habilitadas para Amazon Inspector • Mostrar todos los equilibradores de carga que escuchan en HTTPS (SSL) • AWS CloudTrail cifrado en reposo • CloudWatch Alertas de Amazon para AWS Config mostrar todos los cambios y todos los ajustes comentados • Toda la actividad raíz Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config el tipo de fuente de datos y seleccione las siguientes reglas AWS Config administradas como mapeos de fuentes de datos: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_REGISTRADO_HABILITADO • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_HABILITADA_Y_ENCRIPTADO

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
Artículo 32 Seguridad del procesamiento.2	Capítulo 4: Controlador y procesador	Puede crear un control personalizado que sea compatible con este control del RGPD. AWS Audit Manager Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Muestra el cifrado de los datos en reposo para todos los servicios • Muestra el cifrado de los datos en tránsito para todos los servicios • MFA Delete habilitada para Amazon S3 • Todos los escaneos de Amazon Inspector • Mostrar todas las instancias que no están habilitadas para Amazon Inspector • Mostrar todos los equilibradores de carga que escuchan en HTTPS (SSL) • AWS CloudTrail cifrado en reposo • CloudWatch Alertas de Amazon para AWS Config mostrar todos los cambios y todos los ajustes comentados • Toda la actividad raíz Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config el tipo de fuente de datos y seleccione las siguientes reglas AWS Config administradas como mapeos de fuentes de datos: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_REGISTRADO_HABILITADO • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_HABILITADA_Y_ENCRIPTADO

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
Artículo 32 Seguridad del procesamiento.3	Capítulo 4: Controlador y procesador	Puede crear un control personalizado que sea compatible con este control del RGPD. AWS Audit Manager Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Muestra el cifrado de los datos en reposo para todos los servicios • Muestra el cifrado de los datos en tránsito para todos los servicios • MFA Delete habilitada para Amazon S3 • Todos los escaneos de Amazon Inspector • Mostrar todas las instancias que no están habilitadas para Amazon Inspector • Mostrar todos los equilibradores de carga que escuchan en HTTPS (SSL) • AWS CloudTrail cifrado en reposo • CloudWatch Alertas de Amazon para AWS Config mostrar todos los cambios y todos los ajustes comentados • Toda la actividad raíz Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config el tipo de fuente de datos y seleccione las siguientes reglas AWS Config administradas como mapeos de fuentes de datos: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_REGISTRADO_HABILITADO • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_HABILITADA_Y_ENCRIPTADO

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
Artículo 32 Seguridad del procesamiento.4	Capítulo 4: Controlador y procesador	Puede crear un control personalizado que sea compatible con este control del RGPD. AWS Audit Manager Cuando especifique los detalles del control, introduzca lo siguiente en Información sobre las pruebas: • Muestra el cifrado de los datos en reposo para todos los servicios • Muestra el cifrado de los datos en tránsito para todos los servicios • MFA Delete habilitada para Amazon S3 • Todos los escaneos de Amazon Inspector • Mostrar todas las instancias que no están habilitadas para Amazon Inspector • Mostrar todos los equilibradores de carga que escuchan en HTTPS (SSL) • AWS CloudTrail cifrado en reposo • CloudWatch Alertas de Amazon para AWS Config mostrar todos los cambios y todos los ajustes comentados • Toda la actividad raíz Al configurar el origen de datos de control, le recomendamos que incluya todo lo siguiente como origen de datos: Elija AWS Config el tipo de fuente de datos y seleccione las siguientes reglas AWS Config administradas como mapeos de fuentes de datos: • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_REGISTRADO_HABILITADO • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY

Nombre del control	Conjunto de controles	Mapeo de origen de datos de control recomendado
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_HABILITADA_Y_ENCRIPTADO

Después de crear los nuevos controles personalizados, puede agregarlos a un marco de RGPD personalizado. A continuación, puede crear una evaluación a partir del marco personalizado del RGPD. De esta forma, Audit Manager puede recopilar pruebas automáticamente para los controles personalizados que haya añadido.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Centro del Reglamento General de Protección de Datos (RGPD)
- AWS Publicaciones de blog sobre el RGPD

Gramm-Leach-Bliley Actúa

AWS Audit Manager proporciona un marco prediseñado que respalda la Gramm-Leach-Bliley Ley (GLBA).

Temas

- ¿Qué es la GLBA?

- Uso de este marco
- Pasos a seguir a continuación

¿Qué es la GLBA?

La GLBA (o GLB Act), también conocida como Ley de Modernización de los Servicios Financieros de 1999, es una ley federal promulgada en los Estados Unidos para controlar la forma en que las instituciones financieras manejan la información privada de las personas. La Ley consta de tres secciones. La primera es la Norma de Privacidad Financiera, que regula la recopilación y divulgación de información financiera privada. La segunda es la Norma de Salvaguardas, que estipula que las instituciones financieras deben implementar programas de seguridad para proteger dicha información. La tercera son las disposiciones sobre el uso de pretextos, que prohíben la práctica del uso de pretextos (acceder a información privada con falsos pretextos). La ley también exige que las instituciones financieras entreguen a los clientes avisos de privacidad por escrito que expliquen sus prácticas de intercambio de información.

Uso de este marco

Puede utilizar el marco de GLBA 2016 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de la GLBA. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco de la GLBA como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para una auditoría de la GLBA. En su evaluación, puede especificar lo Cuentas de AWS que desea incluir en el alcance de la auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco de la GLBA. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Gramm-Leach-Bliley Ley (GLBA)	0	120	16

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si sus sistemas cumplen con el estándar GLBA. Además, no pueden garantizar que supere una auditoría de la GLBA. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Title 21 CFR Part 11

AWS Audit Manager proporciona un marco estándar prediseñado que respalda el Título 21 del Código de Regulaciones Federales (CFR), parte 11, «Registros electrónicos y firmas electrónicas: alcance y aplicación», 24 de mayo de 2023.

Temas

- ¿Qué es Title 21 de CFR Part 11?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es Title 21 de CFR Part 11?

GxP se refiere a las normas y directrices aplicables a las organizaciones de ciencias de la vida que fabrican alimentos y productos médicos. Entre los productos médicos incluidos en esta categoría se incluyen los medicamentos, los dispositivos médicos y las aplicaciones de software médico. El objetivo general de los requisitos de GxP es garantizar que los alimentos y los productos médicos sean seguros para los consumidores. También es para garantizar la integridad de los datos que se utilizan para tomar decisiones de seguridad relacionadas con los productos.

En los Estados Unidos, la Administración de Alimentos y Medicamentos de los EE. UU. (FDA) hace cumplir las normativas GxP, que se incluyen en Title 21 del Code of Federal Regulations (21 CFR). En el 21 CFR, Part 11 se incluyen los requisitos aplicables a los sistemas de computación que crean, modifican, mantienen, archivan, recuperan o distribuyen registros electrónicos y firmas electrónicas con el fin de respaldar las actividades reguladas por las normativas GxP. Part 11 se creó para permitir la adopción de nuevas tecnologías de la información por parte de las organizaciones de ciencias biológicas reguladas por la FDA y, al mismo tiempo, proporcionar un marco para garantizar que los datos electrónicos de las normativas GxP sean fiables.

Para obtener un enfoque integral sobre el uso de la AWS nube para los sistemas GxP, consulte el documento técnico Consideraciones sobre el uso de AWS productos en los sistemas GxP.

Uso de este marco

Puede utilizar el marco de Title 21 CFR Part 11 como ayuda para prepararse para la auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de CFR. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco de Title 21 CFR Part 11. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Title 21 Code of Federal Regulations (CFR) Part 11, Electronic records; Electronic Signatures - Scope and Application 24 May 2023	6	19	2

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el ConfigDataSourceMappingsarchivo AuditManager _ _Title-21-CFR-Part-11.zip.

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si sus sistemas cumplen con las normas de GxP. Además, no pueden garantizarle que vaya a superar una auditoría. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- AWS Página de conformidad de GxP
- Consideraciones sobre el uso de AWS productos en sistemas GxP

EU GMP Annex 11, v1

AWS Audit Manager proporciona un marco prediseñado que respalda las EudraLex normas que rigen los medicamentos en la Unión Europea (UE), volumen 4: Medicamentos con buenas prácticas de fabricación (GMP) para uso humano y veterinario, anexo 11.

Temas

- ¿Qué es EU GMP Annex 11?
- Uso de este marco
- Pasos a seguir a continuación

¿Qué es EU GMP Annex 11?

El marco de EU GMP Annex 11 es el equivalente europeo del marco de Title 21 CFR Part 11 en los Estados Unidos. Este anexo se aplica a todos los tipos de sistemas computarizados que se utilizan como parte de las actividades reguladas por las buenas prácticas de fabricación (GMP). Un sistema computarizado es un conjunto de componentes de software y hardware que, en conjunto, cumplen ciertas funcionalidades. La aplicación debe estar validada y la infraestructura de TI debe estar calificada. Cuando un sistema computarizado sustituya a una operación manual, no debería producirse una disminución en la calidad del producto, el control del proceso o la garantía de calidad. No debe haber ningún aumento en el riesgo general del proceso.

El anexo 11 forma parte de las directrices europeas sobre buenas prácticas de fabricación y define los términos de referencia de los sistemas computarizados que utilizan las organizaciones de la industria farmacéutica. El anexo 11 funciona como una lista de verificación que permite a las agencias reguladoras europeas establecer los requisitos para los sistemas computarizados relacionados con los productos farmacéuticos y los dispositivos médicos. Las directrices establecidas por la Comisión de los Comités Europeos no están muy alejadas de las de la FDA (Title 21 CFR Part 11). En el anexo 11 se definen los criterios por los que se considera que se gestionan los registros electrónicos y las firmas electrónicas.

Uso de este marco

Puede utilizar el marco de EU GMP Annex 11 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de EU GMP. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco de EU GMP Annex 11. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
EudraLex - La normativa que regula los medicamentos en la Unión Europea (UE) - Volumen 4: Medicamentos con buenas prácticas de fabricación (GMP) para uso humano y veterinario - Anexo 11	0	32	3

> **Important**
>
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de establecer AWS Config las normas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el archivo AuditManager_ ConfigDataSourceMappings _ EudraLex -GMP-Volume-4-Annex-11.zip.

Los controles de este marco no tienen por objeto verificar si los sistemas cumplen con los requisitos de EU GMP Annex 11. Además, no pueden garantizar que pases una auditoría de buenas prácticas de fabricación de la UE. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

HIPAA Security Rule: Feb 2003

AWS Audit Manager proporciona un marco estándar prediseñado que respalda la regla de seguridad de la Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA): febrero de 2003.

> **Note**
>
> Para obtener información sobre la Norma general de seguridad definitiva de la HIPAA de 2013 y el marco de Audit Manager que respalda este estándar, consulte HIPAA Omnibus Final Rule.

Temas

- ¿Qué es la HIPAA y la Norma de Seguridad de la HIPAA de 2003?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es la HIPAA y la Norma de Seguridad de la HIPAA de 2003?

La HIPAA es una ley que ayuda a los trabajadores estadounidenses a conservar la cobertura del seguro médico cuando cambian o pierden su empleo. La legislación también busca fomentar los registros médicos electrónicos para mejorar la eficacia y la calidad del sistema de salud de los EE. UU. mediante un mejor intercambio de información.

Además de aumentar el uso de los registros médicos electrónicos, la HIPAA incluye disposiciones para proteger la seguridad y la privacidad de la información de salud protegida (protected health information, PHI). La PHI incluye un conjunto muy amplio de datos de salud de identificación personal y relacionados con la salud. Esto incluye información sobre seguros y facturación, datos de diagnóstico, datos de atención clínica y resultados de laboratorio, como imágenes y resultados de pruebas.

El Departamento de Salud y Servicios Humanos de los Estados Unidos publicó una norma de seguridad definitiva en febrero de 2003. Esta regla establece estándares nacionales para proteger la confidencialidad, integridad y disponibilidad de la información médica electrónica protegida.

Las normas de la HIPAA se aplican a las entidades cubiertas. Estas incluyen hospitales, proveedores de servicios médicos, planes de salud patrocinados por el empleador, centros de investigación y compañías de seguros que tratan directamente con los pacientes y sus datos. El requisito de la HIPAA de proteger la PHI también se extiende a los socios comerciales.

Para obtener más información sobre cómo HIPAA e HITECH protegen la información de salud, consulte la página web Privacidad de la información de salud del Departamento de Salud y Servicios Humanos de los EE. UU.

Un número cada vez mayor de proveedores de atención médica, pagadores y profesionales de TI utilizan servicios en la nube AWS basados en servicios públicos para procesar, almacenar y transmitir información de salud protegida (PHI). AWS permite a las entidades cubiertas y a sus socios comerciales sujetos a la HIPAA utilizar un AWS entorno seguro para procesar, mantener y almacenar información de salud protegida.

Para obtener instrucciones sobre cómo utilizarla AWS para el procesamiento y almacenamiento de la información de salud, consulte el documento técnico Architecting for HIPAA Security and Compliance on Amazon Web Services.

Uso de este marco

Puede utilizar el marco Norma de Seguridad de la HIPAA de 2003 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de la HIPAA. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco de la HIPAA. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Health Insurance Portability and Accountability Act (HIPAA) Security Rule: Feb 2003	28	57	5

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.

Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el ConfigDataSourceMappingsarchivo AuditManager _ _HIPAA-Security-Rule-Feb-2003.zip.

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si sus sistemas cumplen con la norma HIPAA. Además, no pueden garantizar que pases una auditoría de la HIPAA. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Privacidad de la información de salud del Departamento de Salud y Servicios Humanos de los EE. UU.
- La norma de seguridad del Departamento de Salud y Servicios Humanos de los EE. UU.
- Arquitectura de seguridad de HIPAA y cumplimiento de servicios Amazon Web
- AWS Página de cumplimiento de la HIPAA

HIPAA Omnibus Final Rule

AWS Audit Manager proporciona un marco estándar prediseñado que respalda la Regla final general de la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA).

> **Note**
>
> Para obtener información sobre la Regla de Seguridad de la HIPAA de 2003 y el AWS Audit Manager marco que respalda esta norma, consulte. HIPAA Security Rule: Feb 2003

Temas

- ¿Qué es la HIPAA y la norma general de seguridad definitiva de la HIPAA?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es la HIPAA y la norma general de seguridad definitiva de la HIPAA?

La HIPAA es una ley que ayuda a los trabajadores estadounidenses a conservar la cobertura del seguro médico cuando cambian o pierden su empleo. La legislación también busca fomentar los registros médicos electrónicos para mejorar la eficacia y la calidad del sistema de salud de los EE. UU. mediante un mejor intercambio de información.

Además de aumentar el uso de los registros médicos electrónicos, la HIPAA incluye disposiciones para proteger la seguridad y la privacidad de la información de salud protegida (protected health information, PHI). La PHI incluye un conjunto muy amplio de datos de salud de identificación personal y relacionados con la salud. Esto incluye información sobre seguros y facturación, datos de diagnóstico, datos de atención clínica y resultados de laboratorio, como imágenes y resultados de pruebas.

La norma general de seguridad definitiva de la HIPAA, que entró en vigor en 2013, implementa una serie de actualizaciones de todas las normas aprobadas anteriormente. Las modificaciones de las normas de seguridad, privacidad, notificación de infracciones y cumplimiento tenían por objeto mejorar la confidencialidad y la seguridad en el intercambio de datos.

Las normas de la HIPAA se aplican a las entidades cubiertas. Estas incluyen hospitales, proveedores de servicios médicos, planes de salud patrocinados por el empleador, centros de investigación y compañías de seguros que tratan directamente con los pacientes y sus datos. Como parte de las actualizaciones generales, muchas de las normas de la HIPAA que se aplican a las entidades cubiertas ahora también se aplican a los socios comerciales.

Para obtener más información sobre cómo HIPAA e HITECH protegen la información de salud, consulte la página web Privacidad de la información de salud del Departamento de Salud y Servicios Humanos de los EE. UU.

Un número cada vez mayor de proveedores de atención médica, pagadores y profesionales de TI utilizan servicios en la nube AWS basados en servicios públicos para procesar, almacenar y transmitir información de salud protegida (PHI). AWS permite a las entidades cubiertas y a sus socios comerciales sujetos a la HIPAA utilizar un AWS entorno seguro para procesar, mantener y almacenar información de salud protegida. Para obtener instrucciones sobre cómo utilizarla AWS para el procesamiento y almacenamiento de la información de salud, consulte el documento técnico Architecting for HIPAA Security and Compliance on Amazon Web Services.

Uso de este marco

Puede utilizar el marco de HIPAA Omnibus Final Rule como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos de la HIPAA. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco de la HIPAA. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule	24	50	5

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el ConfigDataSourceMappingsarchivo AuditManager _ _HIPAA-Omnibus-Final-Rule.zip.

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si sus sistemas cumplen con la norma HIPAA. Además, no pueden garantizar que pases una auditoría de la HIPAA. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Privacidad de la información de salud del Departamento de Salud y Servicios Humanos de los EE. UU.

- Elaboración de normas generales de la HIPAA del Departamento de Salud y Servicios Humanos de los EE. UU.
- Arquitectura de seguridad de HIPAA y cumplimiento de servicios Amazon Web
- AWS Página de cumplimiento de la HIPAA

Anexo A de la norma de la ISO/IEC 27001:2013

AWS Audit Manager proporciona un marco estándar prediseñado que respalda el anexo A de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) 27001:2013,

Temas

- ISO/IEC ¿Qué es el anexo A del 27001:2013?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

ISO/IEC ¿Qué es el anexo A del 27001:2013?

La Comisión Electrotécnica Internacional (IEC) y la Organización Internacional de Normalización (ISO) son not-for-profit organizaciones independientes y no gubernamentales que desarrollan y publican normas internacionales totalmente consensuadas.

ISO/IEC 27001:2013 Annex A is a security management standard that specifies security management best practices and comprehensive security controls that follow the ISO/IECGuía de mejores prácticas 27002. Esta norma internacional especifica los requisitos sobre cómo establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información en su organización. Entre estos estándares, se incluyen los requisitos sobre la evaluación y el tratamiento de los riesgos de seguridad de la información, que se adaptan a las necesidades de su organización. Los requisitos de esta norma internacional son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.

Uso de este marco

Puede utilizar el AWS Audit Manager marco del anexo A del documento ISO/IEC 27001:2013 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de control de acuerdo con los requisitos del anexo A de la norma de la ISO/IEC 27001:2013. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para una auditoría del Anexo A de ISO/IEC 27001:2013. En su evaluación, puede especificar lo Cuentas de AWS que desea incluir en el alcance de la auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Para ello, se basa en los controles que se definen en el marco del anexo A del ISO/IEC documento 27001:2013. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
International Organization for standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2013 Annex A	21	93	35

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.

Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el ConfigDataSourceMappingsarchivo AuditManager _ _ISO-IEC-270012013-Annex-A.zip.

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si sus sistemas cumplen con este estándar internacional. Además, no pueden garantizar que pases una ISO/IEC auditoría. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Para obtener más información sobre esta norma internacional, consulte la norma de la ISO/IEC 27001:2013 en la tienda web de ANSI.

NIST SP 800-53 Rev 5

AWS Audit Manager proporciona un marco prediseñado que es compatible con el NIST 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations.

> **Note**
>
> - Para obtener información sobre el marco de Audit Manager compatible con NIST SP 800-171, consulte NIST SP 800-171 Rev 2.

- Para obtener información sobre el marco de Audit Manager compatible con NIST CSF, consulte Marco de Ciberseguridad del NIST v1.1.

Temas

- ¿Qué es NIST SP 800-53?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es NIST SP 800-53?

El Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST) se fundó en 1901 y ahora forma parte del Departamento de Comercio de los Estados Unidos. El NIST es uno de los laboratorios de ciencias físicas más antiguos de los Estados Unidos. El Congreso de los Estados Unidos creó la agencia para mejorar lo que en ese momento era una infraestructura de medición de segunda categoría. Las infraestructuras constituían un importante desafío para la competitividad industrial de Estados Unidos, que se había quedado rezagada con respecto a otras potencias económicas como el Reino Unido y Alemania.

Los controles de seguridad de NIST SP 800-53 suelen aplicarse a los sistemas de información federales de los EE. UU. Por lo general, se trata de sistemas que deben pasar por un proceso formal de evaluación y autorización. Este proceso garantiza una protección suficiente de la confidencialidad, la integridad y la disponibilidad de la información y los sistemas de información. Esto se basa en la categoría de seguridad y el nivel de impacto del sistema (bajo, moderado o alto), así como en la determinación del riesgo. Los controles de seguridad se seleccionan del catálogo de controles de seguridad de NIST SP 800-53 y el sistema se evalúa con respecto a los requisitos de estos controles de seguridad.

El marco de NIST SP 800-53 representa los controles de seguridad y los procedimientos de evaluación asociados que se definen en NIST SP 800-53 Revision 5 Recommended Security Controls for Federal Information Systems and Organizations. Para cualquier discrepancia que se observe en el contenido entre este marco del NIST SP 800-53 y la última publicación especial del NIST SP 800-53, revisión 5, consulte los documentos oficiales publicados que están disponibles en el Centro de Recursos de Seguridad Informática del NIST.

Uso de este marco

Puede utilizar el marco de NIST SP 800-53 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos del NIST. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco de NIST SP 800-53. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
NIST 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations	132	875	20

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que

se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el ConfigDataSourceMappingsarchivo AuditManager _ _NIST-800-53-Rev-5.zip.

Los controles de este AWS Audit Manager marco no pretenden verificar si sus sistemas cumplen con el estándar NIST. Además, no pueden garantizar que pases una auditoría del NIST. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Instituto Nacional de Estándares y Tecnología (NIST)
- Centro de recursos de seguridad informática del NIST
- AWS Página de cumplimiento del NIST

Marco de Ciberseguridad del NIST v1.1

AWS Audit Manager proporciona un marco prediseñado que es compatible con el Marco de Ciberseguridad (CSF) v1.1 del NIST.

> **Note**
>
> - Para obtener información sobre el marco de Audit Manager compatible con NIST SP 800-53, consulte NIST SP 800-53 Rev 5.

- Para obtener información sobre el marco de Audit Manager compatible con NIST SP 800-171, consulte NIST SP 800-171 Rev 2.

Temas

- ¿Qué es el marco de ciberseguridad del NIST?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es el marco de ciberseguridad del NIST?

El Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST) se fundó en 1901 y ahora forma parte del Departamento de Comercio de los Estados Unidos. El NIST es uno de los laboratorios de ciencias físicas más antiguos de los Estados Unidos. El Congreso de los Estados Unidos creó la agencia para mejorar lo que en ese momento era una infraestructura de medición de segunda categoría. Las infraestructuras constituían un importante desafío para la competitividad industrial de Estados Unidos, que se había quedado rezagada con respecto a otras potencias económicas como el Reino Unido y Alemania.

Los Estados Unidos dependen del funcionamiento fiable de la infraestructura crítica. Las amenazas de ciberseguridad explotan la creciente complejidad e interconexión de los sistemas de infraestructura crítica. Ponen en riesgo la seguridad, la economía y la seguridad y salud públicas de los Estados Unidos. Al igual que los riesgos financieros y de reputación, el riesgo de ciberseguridad afecta a los resultados de una empresa. Puede aumentar los costos y afectar a los ingresos. Puede perjudicar la capacidad de una organización para innovar y conseguir y mantener clientes. En última instancia, la ciberseguridad puede amplificar la gestión general de riesgos de una organización.

El Marco de Ciberseguridad (Cybersecurity Framework, CSF) del NIST cuenta con el respaldo de los gobiernos y las industrias de todo el mundo como referencia recomendada para su uso por cualquier organización, independientemente de su sector o tamaño. El marco de ciberseguridad del NIST consta de tres componentes principales: el núcleo del marco, los perfiles y los niveles de implementación. El núcleo del marco contiene las actividades y los resultados de ciberseguridad deseados organizados en 23 categorías que cubren la gama de objetivos de ciberseguridad de una organización. Los perfiles contienen la alineación única de una organización con sus requisitos y objetivos organizacionales, su propensión al riesgo y sus recursos, utilizando los resultados

deseados del núcleo del marco. Los niveles de implementación describen el grado en que las prácticas de gestión de riesgos de ciberseguridad de una organización presentan las características definidas en el núcleo del marco.

Uso de este marco

Puede utilizar NIST CSF v1.1 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles de acuerdo con los requisitos del NIST y el CSF. Audit Manager actualmente es compatible con el componente principal del marco. Audit Manager no admite los componentes de perfil e implementación de este marco.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en NIST CSF. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las evidencias que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Marco de Ciberseguridad del NIST (CSF) v1.1	14	94	22

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se

utilizan como mapeos de fuentes de datos en este marco estándar, descargue el archivo AuditManager_ ConfigDataSourceMappings _nist-CSF-v1.1.zip.

Los controles que ofrece Audit Manager no pretenden verificar si los sistemas cumplen con NIST CSF. Además, no pueden garantizarle que vaya a superar una auditoría del NIST. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Instituto Nacional de Estándares y Tecnología (NIST)
- Centro de recursos de seguridad informática del NIST
- AWS Página de conformidad del NIST
- Marco de ciberseguridad del NIST: alinearse con el CSF del NIST en la nube AWS

NIST SP 800-171 Rev 2

AWS Audit Manager proporciona un marco estándar prediseñado que admite la revisión 2 del NIST 800-171: Protección de la información no clasificada controlada en sistemas y organizaciones no federales.

> **Note**
>
> - Para obtener información sobre el marco de Audit Manager compatible con NIST SP 800-53, consulte NIST SP 800-53 Rev 5.

- Para obtener información sobre el marco de Audit Manager compatible con NIST CSF, consulte Marco de Ciberseguridad del NIST v1.1.

Temas

- ¿Qué es NIST SP 800-171?
- Uso de este marco
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es NIST SP 800-171?

El NIST SP 800-171 se centra en proteger la confidencialidad de la información no clasificada controlada (Controlled Unclassified Information, CUI) en sistemas y organizaciones no federales. Recomienda requisitos de seguridad específicos para lograr ese objetivo. El NIST 800-171 es una publicación que describe los estándares y prácticas de seguridad necesarios para las organizaciones no federales que gestionan la CUI en sus redes. Fue publicada por primera vez en junio de 2015 por el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST). El NIST es una agencia gubernamental de EE. UU. que publicó varios estándares y publicaciones para fortalecer la resiliencia de la ciberseguridad en los sectores público y privado. NIST SP 800-171 ha recibido actualizaciones periódicas en función de las ciberamenazas emergentes y las tecnologías cambiantes. La última versión (revisión 2) se publicó en febrero de 2020.

Los controles de ciberseguridad de NIST SP 800-171 protegen la CUI en las redes de TI de los contratistas y subcontratistas gubernamentales. Define las prácticas y los procedimientos que deben seguir los contratistas gubernamentales cuando sus redes procesan o almacenan la CUI. NIST SP 800-171 solo se aplica a las partes de la red de un contratista en las que esté presente la CUI.

Uso de este marco

Puede utilizar el marco de NIST SP 800-171 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos del NIST. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco de NIST SP 800-171. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
NIST 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	35	75	14

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el ConfigDataSourceMappingsarchivo AuditManager _ _NIST-800-171-Rev-2.zip.

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si sus sistemas cumplen con la norma NIST 800-171. Además, no pueden garantizarle que vaya a superar una auditoría del NIST. AWS Audit Manager no comprueba automáticamente los controles de procedimiento que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Instituto Nacional de Estándares y Tecnología (NIST)
- Centro de recursos de seguridad informática del NIST
- AWS Página de conformidad del NIST

PCI DSS V3.2.1

AWS Audit Manager proporciona un marco estándar prediseñado que es compatible con el estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) v3.2.1.

> **Note**
>
> Para obtener información sobre PCI DSS v4 y el marco de Audit Manager que lo respalda, consulte PCI DSS V4.0.

Temas

- ¿Qué es PCI DSS?
- Utilice este marco para respaldar la preparación de la auditoría
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es PCI DSS?

PCI DSS es un estándar de seguridad de la información patentado. Lo administra el Consejo de Normas de Seguridad de la PCI, fundado por American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa Inc. El PCI DSS se aplica a las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta (CHD) o datos de autenticación confidenciales (SAD). Esto incluye, pero no se limita a, comerciantes, procesadores, adquirentes, emisores y proveedores de servicios. Las marcas de tarjetas obligan a utilizar el PCI DSS, que está administrado por el Consejo de Estándares de Seguridad de la Industria de las Tarjetas de Pago.

AWS está certificado como proveedor de servicios PCI DSS de nivel 1, que es el nivel de evaluación más alto disponible. La evaluación de conformidad fue realizada por Coalfire Systems Inc., un evaluador de seguridad cualificado (QSA) independiente. El certificado de conformidad (AOC) y el resumen de responsabilidad del PCI DSS están a su disposición en Internet. AWS Artifact Se trata de un portal de autoservicio para acceder a los informes de conformidad bajo demanda. AWS Inicie sesión AWS Artifact en la consola AWS de administración u obtenga más información en Cómo empezar con AWS Artifact.

Puede descargar el estándar PCI DSS de la biblioteca de documentos del Consejo de Estándares de Seguridad de PCI.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar el marco PCI DSS V3.2.1 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos del PCI DSS. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco PCI DSS V3.2.1. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Payment Card Industry Data Security Standard (PCI DSS) v3.2.1	38	246	15

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el archivo AuditManager_ ConfigDataSourceMappings _PCI-DSS-v3.2.1.zip.

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si sus sistemas cumplen con el estándar PCI DSS. Además, no pueden garantizar que supere una auditoría del PCI DSS. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Consejo de normas de seguridad de PCI
- Biblioteca de documentos del Consejo de Estándares de Seguridad de PCI.
- AWS Página de conformidad para PCI DSS

PCI DSS V4.0

AWS Audit Manager proporciona un marco prediseñado que es compatible con el estándar de seguridad de datos del sector de las tarjetas de pago (PCI DSS) v4.0.

> **Note**
>
> Para obtener información sobre PCI DSS v3.2.1 y el marco de Audit Manager que lo respalda, consulte PCI DSS V3.2.1.

Temas

- ¿Qué es PCI DSS?
- Utilice este marco para respaldar la preparación de la auditoría
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es PCI DSS?

El Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS) es un estándar global que proporciona una base de requisitos técnicos y operativos para proteger los datos de pago. El PCI DSS v4.0 es la próxima evolución del estándar.

El PCI DSS se desarrolló para fomentar y mejorar la seguridad de los datos de las cuentas de tarjetas de pago. También facilita la adopción generalizada de medidas de seguridad de datos coherentes a nivel mundial. Proporciona una base de requisitos técnicos y operativos diseñados para proteger los datos de las cuentas. Si bien está diseñado específicamente para centrarse en entornos

con datos de cuentas de tarjetas de pago, también puede utilizar el PCI DSS para protegerse contra las amenazas y proteger otros elementos del ecosistema de pagos.

El Consejo de Estándares de Seguridad de PCI (PCI SSC) introdujo muchos cambios entre las versiones 3.2.1 y 4.0. Estas actualizaciones se dividen en tres categorías:

1. Requisitos en evolución: Cambios para garantizar que el estándar esté actualizado con las amenazas y tecnologías emergentes y con los cambios en el sector de pagos. Algunos ejemplos incluyen requisitos o procedimientos de prueba nuevos o modificados, o la eliminación de un requisito.
2. Aclaración o directrices: Actualizaciones en la redacción, la explicación, la definición, las directrices adicionales o las instrucciones para mejorar la comprensión o proporcionar más información y directrices sobre un tema en particular.
3. Estructura o formato: Reorganización del contenido, incluida la combinación, separación y reorganización de los requisitos para alinear el contenido.

Utilice este marco para respaldar la preparación de la auditoría

> **Note**
>
> Este marco estándar utiliza controles consolidados de Security Hub como origen de datos. Para recopilar correctamente las pruebas de los controles consolidados, asegúrese de activar la configuración de los resultados del control consolidado en Security Hub. Para obtener más información sobre el uso de Security Hub como tipo de origen de datos, consulte los controles de AWS Security Hub admitidos por AWS Audit Manager.

Puede utilizar el marco del PCI DSS V4.0 como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos del PCI DSS V4.0. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco del PCI DSS V4.0. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe)

puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Payment Card Industry Data Security Standard (PCI DSS) v4.0	40	240	20

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el archivo AuditManager_ ConfigDataSourceMappings _PCI-DSS-v4.0.zip.

Los controles de este AWS Audit Manager marco no tienen por objeto verificar si los sistemas cumplen con el estándar PCI DSS. Además, no pueden garantizar que supere una auditoría del PCI DSS. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- Centro de recursos de PCI DSS v4.0
- Consejo de normas de seguridad de PCI
- Biblioteca de documentos del Consejo de Estándares de Seguridad de PCI.
- AWS Página de conformidad para PCI DSS
- Guía de conformidad con la norma de seguridad de datos del sector de las tarjetas de pago (PCI DSS) v4.0 AWS

SSAE-18 SOC 2

AWS Audit Manager proporciona un marco estándar prediseñado que respalda la Declaración sobre normas para la contratación de atestaciones (SSAE) núm. 18 y el informe 2 de Service Organizations Controls (SOC).

Temas

- ¿Qué es SOC 2?
- Utilice este marco para respaldar la preparación de la auditoría
- Pasos a seguir a continuación
- Recursos adicionales

¿Qué es SOC 2?

SOC 2, definido por el American Institute of Certified Public Accountants (AICPA), es el nombre de un conjunto de informes que se elaboran durante una auditoría. Está diseñado para que lo utilicen las organizaciones de servicios (organizaciones que proporcionan sistemas de información como un servicio a otras organizaciones) para emitir informes validados sobre los controles internos de esos

sistemas de información a los usuarios de esos servicios. Los informes se centran en los controles agrupados en cinco categorías conocidas como principios del servicio de confianza.

AWS Los informes del SOC son informes de examen independientes de terceros que demuestran cómo se AWS logran los principales controles y objetivos de cumplimiento. El objetivo de estos informes es ayudarlo a usted y a sus auditores a comprender los AWS controles establecidos para respaldar las operaciones y el cumplimiento. Hay cinco informes del AWS SOC:

- AWS Informe SOC 1, disponible para AWS los clientes en. AWS Artifact
- AWS Informe de seguridad, disponibilidad y confidencialidad del SOC 2, disponible para AWS los clientes en. AWS Artifact
- AWS El informe de seguridad, disponibilidad y confidencialidad del SOC 2 está disponible para AWS los clientes en AWS Artifact(el alcance incluye únicamente Amazon DocumentDB).
- AWS Informe de privacidad de tipo I del SOC 2, disponible para AWS los clientes en. AWS Artifact
- AWS Informe de seguridad, disponibilidad y confidencialidad del SOC 3, disponible públicamente como documento técnico.

Utilice este marco para respaldar la preparación de la auditoría

Puede utilizar este marco como ayuda para prepararse para las auditorías. Este marco incluye una colección prediseñada de controles con descripciones y procedimientos de prueba. Estos controles se agrupan en conjuntos de controles según los requisitos del SOC 2. También puede personalizar este marco y sus controles para respaldar las auditorías internas con requisitos específicos.

Si utiliza el marco como punto de partida, puede crear una evaluación de Audit Manager y empezar a recopilar pruebas relevantes para su auditoría. Tras crear una evaluación, Audit Manager comienza a evaluar sus AWS recursos. Lo hace en función de los controles que se definen en el marco. Cuando llegue el momento de realizar una auditoría, usted (o la persona que designe) puede revisar las pruebas que recopiló Audit Manager. Además, puede examinar las carpetas de las pruebas en la evaluación y seleccionar qué pruebas desea incluir en su informe de evaluación. O bien, si ha activado el buscador de pruebas, puede buscar pruebas específicas y exportarlas en formato CSV, o crear un informe de evaluación a partir de los resultados de la búsqueda. En cualquier caso, puede utilizar este informe de evaluación para demostrar que sus controles funcionan según lo previsto.

Los detalles del marco son los siguientes:

Nombre del marco en AWS Audit Manager	Número de controles automatizados	Número de controles manuales	Número de conjuntos de control
Statement on Standards for Attestations Engagement (SSAE) No. 18, Service Organizations Controls (SOC) Report 2	15	46	20

> **Important**
>
> Para garantizar que este marco recopila las pruebas previstas AWS Security Hub, asegúrese de haber activado todos los estándares en Security Hub.
> Para garantizar que este marco recopile las pruebas previstas AWS Config, asegúrese de habilitar las AWS Config reglas necesarias. Para revisar las AWS Config reglas que se utilizan como mapeos de fuentes de datos en este marco estándar, descargue el archivo AuditManager_ ConfigDataSourceMappings _SSAE-NO.-18-SOC-Report-2.zip.

Los controles de este marco no tienen por objeto comprobar si los sistemas cumplen con las normas. AWS Audit Manager Además, no pueden garantizar que supere una auditoría. AWS Audit Manager no comprueba automáticamente los controles procedimentales que requieren la recopilación manual de pruebas.

Pasos a seguir a continuación

Para obtener instrucciones sobre cómo ver información detallada de este marco, incluida la lista de controles estándar que incluye, consulte Revisar un marco en AWS Audit Manager.

Para obtener instrucciones sobre cómo crear una evaluación mediante el uso de este marco, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo personalizar este marco para que se adapte a sus requisitos específicos, consulte Hacer una copia editable de un marco existente en AWS Audit Manager.

Recursos adicionales

- AWS Página de conformidad para el SOC

Tipos de orígenes de datos compatibles para evidencias automatizadas

Al crear un control personalizado en AWS Audit Manager, puede configurarlo para recopilar pruebas automatizadas de los siguientes tipos de fuentes de datos:

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS Llamadas a la API

Cada tipo de origen de datos ofrece capacidades distintas para capturar registros de actividad de los usuarios, resultados de conformidad, configuraciones de recursos y mucho más.

En este capítulo, puede obtener información sobre cada uno de estos tipos de fuentes de datos automatizadas y los AWS Security Hub controles, AWS Config reglas y llamadas a la AWS API específicos que admite Audit Manager.

Puntos clave

En la siguiente tabla se proporciona información general de cada tipo de orígenes de datos automatizada.

Data source type	Descripción	Frecuencia de recolección de evidencias	Para usar este tipo de origen de datos...	Cuando este control está activo en una evaluación...	Consejos relacionados para la solución de problemas
AWS CloudTrail	Realiza un seguimien	Continuo.	Seleccionar la lista de nombres de eventos compatibles.	Audit Manager filtra los CloudTrail registros en función	Mi evaluación no

Data source type	Descripción	Frecuencia de recolección de evidencias	Para usar este tipo de origen de datos...	Cuando este control está activo en una evaluación...	Consejos relacionados para la solución de problemas
	to de la actividad de un usuario específico.			de la palabra clave que elija. Los resultados se importan como evidencia de la Actividad del usuario.	consiste en recopilar pruebas de la actividad de los usuarios de AWS CloudTrail

Data source type	Descripción	Frecuencia de recolección de evidencias	Para usar este tipo de origen de datos...	Cuando este control está activo en una evaluación...	Consejos relacionados para la solución de problemas
AWS Config	Captura una instantánea del estado de seguridad de sus recursos mediante un informe de los resultados obtenidos de AWS Config.	En función de los activadores definidos en la AWS Config regla.	Seleccione un tipo regla y, a continuación, elija una regla. • Seleccione las reglas administradas desde la lista de palabras clave de reglas administradas compatibles. • Selecciónela las reglas personalizadas desde la lista de reglas disponibles.	Audit Manager obtiene los resultados de esta regla directamente de AWS Config. El resultado se importa como evidencia de Verificación de conformidad.	Mi evaluación no consiste en recopilar pruebas de control de cumplimiento de AWS Config AWS Config problemas de integración

Data source type	Descripción	Frecuencia de recolección de evidencias	Para usar este tipo de origen de datos...	Cuando este control está activo en una evaluación...	Consejos relacionados para la solución de problemas
AWS Security Hub	Captura una instantánea del estado de seguridad de sus recursos mediante el informe de los resultados de Security Hub.	Según la programación de la comprobación de Security Hub.	Seleccione uno de la lista de controles de Security Hub compatibles IDs.	Audit Manager obtiene el resultado del control de seguridad directamente desde Security Hub. El resultado se importa como evidencia de Verificación de conformidad.	Mi evaluación no consiste en recopilar pruebas de control de cumplimiento de AWS Security Hub

Data source type	Descripción	Frecuencia de recolección de evidencias	Para usar este tipo de origen de datos...	Cuando este control está activo en una evaluación...	Consejos relacionados para la solución de problemas
AWS Llamada a la API	Toma una instantánea de la configuración de los recursos directamente mediante una llamada a la API especificada Servicio de AWS.	Diariamente, semanalmente o mensualmente.	Seleccione una opción de la lista de llamadas a la API compatibles y, a continuación, seleccione la frecuencia que prefiera.	Audit Manager realiza la llamada a la API en función de la frecuencia que especifique. La respuesta se importa como evidencia de Datos de configuración.	Mi evaluación no consiste en recopilar evidencia de datos de configuración para una llamada a la AWS API

> **Tip**
>
> Puede crear controles personalizados que recopilen evidencias mediante agrupaciones predefinidas de los orígenes de datos anteriores. Estas agrupaciones de orígenes de datos se conocen como orígenes administrados por AWS. Cada fuente AWS gestionada representa un control común o un control central que se ajusta a un requisito de cumplimiento común. Esto le proporciona una forma eficaz de asignar sus requisitos de

conformidad a un grupo relevante de fuentes de AWS datos. Para ver los controles comunes disponibles, consulte Encuentre los controles disponibles en AWS Audit Manager.
También puede usar los cuatro tipos de orígenes de datos anteriores para definir sus propios orígenes de datos personalizados. Esto le da la flexibilidad de cargar pruebas manualmente o recopilar pruebas automatizadas a partir de un recurso específico de la empresa, como una regla personalizada AWS Config .

Pasos a seguir a continuación

Para obtener más información sobre los orígenes de datos específicos que puede usar en los controles personalizados, consulte las páginas siguientes.

- Reglas de AWS Config con el apoyo de AWS Audit Manager
- AWS Security Hub controles compatibles con AWS Audit Manager
- AWS Las llamadas a la API son compatibles con AWS Audit Manager
- AWS CloudTrail nombres de eventos compatibles con AWS Audit Manager

Reglas de AWS Config con el apoyo de AWS Audit Manager

Puede usar Audit Manager para capturar AWS Config las evaluaciones como evidencia para las auditorías. Al crear o editar un control personalizado, puede especificar una o más AWS Config reglas como mapeo de fuentes de datos para la recopilación de pruebas. AWS Config realiza comprobaciones de conformidad en función de estas reglas, y Audit Manager informa de los resultados como evidencia de las comprobaciones de conformidad.

Además de las reglas gestionadas, también puede asignar sus reglas personalizadas a un origen de datos de control.

Contenido

- Puntos clave
- Reglas AWS Config administradas compatibles
- Uso de reglas AWS Config personalizadas con Audit Manager
- Recursos adicionales

Puntos clave

- Audit Manager no recopila pruebas de las reglas de AWS Config vinculadas a servicios, con la excepción de las reglas vinculadas a servicios de los paquetes de conformidad y de AWS Organizations.
- Audit Manager no gestiona AWS Config las reglas por usted. Antes de iniciar la recopilación de pruebas, le recomendamos que revise los parámetros actuales de AWS Config la regla. A continuación, valide esos parámetros según los requisitos del marco que haya elegido. Si es necesario, puede actualizar los parámetros de una regla de AWS Configpara que se ajusten a los requisitos del marco. Esto ayudará a garantizar que sus evaluaciones recopilan las pruebas de control de conformidad correctas para ese marco.

  Supongamos, por ejemplo, que está creando una evaluación para CIS v1.2.0. Este marco tiene un control denominado Ensure IAM password policy requires a minimum length of 14 or greater. En AWS Config, la iam-password-policyregla tiene un `MinimumPasswordLength` parámetro que comprueba la longitud de la contraseña. El valor predeterminado para este parámetro es 14 caracteres. Por lo tanto, la regla concuerda con los requisitos de control establecidos. Si no utiliza el valor de parámetro predeterminado, asegúrese de que sea igual o superior al requisito de 14 caracteres establecido en CIS v1.2.0. Puede encontrar los detalles de los parámetros predeterminados de cada regla administrada en la documentación de AWS Config.
- Si necesita comprobar si una AWS Config regla es una regla administrada o una regla personalizada, puede hacerlo mediante la AWS Config consola. En el menú de navegación de la izquierda, seleccione Reglas y busque la regla en la tabla. Si es una regla administrada, la columna Tipo muestra la regla AWS administrada.

Reglas AWS Config administradas compatibles

Audit Manager admite las siguientes reglas AWS Config gestionadas. Puede utilizar cualquiera de las siguientes palabras clave identificadoras de reglas administradas al configurar un origen de datos para un control personalizado. Para obtener más información sobre cualquiera de las reglas administradas que se enumeran a continuación, elija un elemento de la lista o consulte las reglas administradas de AWS Config en la Guía del usuario de AWS Config .

> **Tip**
>
> Asegúrese de buscar una de las siguientes palabras clave identificadoras de reglas en vez de el nombre de la regla al elegir una regla gestionada en la consola de Audit Manager durante la creación de un control personalizado. Para obtener información sobre la diferencia entre el nombre de la regla, el identificador de la regla y cómo encontrar el identificador de una regla administrada, consulte la sección de solución de problemas de esta guía del usuario.

Palabras clave de reglas AWS Config administradas compatibles
• ACCESS_KEYS_ROTATED • ACCOUNT_PART_OF_ORGANIZATIONS • ACM_CERTIFICATE_EXPIRATION_CHECK • ACM_CERTIFICATE_RSA_CHECK • ALB_DESYNC_MODE_CHECK • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ALB_WAF_ENABLED • API_GW_ASOCIADA_CON_WAF • API_GW_CACHE_HABILITADA_Y_ENCRIPTADO • API_GW_ENDPOINT_TYPE_CHECK • API_GW_REGISTRO DE EJECUCIÓN_HABILITADO • API_GW_SSL_HABILITADO • API_GW_XRAY_HABILITADO • API_GWV2_ACCESS_LOGS_HABILITADO • API_GWV2_TIPO DE AUTORIZACIÓN CONFIGURADO • APPROVED_AMIS_BY_ID • APPROVED_AMIS_BY_TAG • APPSYNC_ASSOCIATED_WITH_WAF • APPSYNC_CACHE_ENCRYPTION_AT_REST

Palabras clave de reglas AWS Config administradas compatibles
• APPSYNC_LOGGING_ENABLED • AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED • AURORA_MYSQL_BACKTRACKING_ENABLED • AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN • AUTOSCALING_CAPACITY_REBALANCING • AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED • AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT • AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED • AUTOSCALING_LAUNCHCONFIG_REQUIRES_ IMDSV2 • AUTOSCALING_LAUNCH_TEMPLATE • AUTOSCALING_MULTIPLE_AZ • AUTOSCALING_MULTIPLE_INSTANCE_TYPES • BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK • BACKUP_RECOVERY_POINT_ENCRYPTED • BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED • BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK • BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED • CLB_DESYNC_MODE_CHECK • CLB_MULTIPLE_AZ • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED • CLOUD_TRAIL_ENABLED • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK • CLOUDFORMATION_STACK_NOTIFICATION_CHECK • CLOUDFRONT_ACCESSLOGS_ENABLED • CLOUDFRONT_ASSOCIATED_WITH_WAF • CERTIFICADO CLOUDFRONT_CUSTOM_SSL_CERTIFICATE • CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED

Palabras clave de reglas AWS Config administradas compatibles
• CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS • CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED • CLOUDFRONT_ORIGIN_FAILOVER_ENABLED • CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED • CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET • CLOUDFRONT_SECURITY_POLICY_CHECK • CLOUDFRONT_SNI_ENABLED • CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED • CLOUDFRONT_VIEWER_POLICY_HTTPS • CLOUDTRAIL_S3_DATAEVENTS_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • CLOUDWATCH_ALARM_ACTION_CHECK • CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK • CLOUDWATCH_ALARM_RESOURCE_CHECK • CLOUDWATCH_ALARM_SETTINGS_CHECK • CLOUDWATCH_LOG_GROUP_ENCRYPTED • CMK_BACKING_KEY_ROTATION_ENABLED • CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION • CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK • CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK • CODEBUILD_PROJECT_LOGGING_ENABLED • CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED • CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK • CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED • CODEDEPLOY_ _MINIMUM_HEALTHY_HOSTS_CONFIGURED EC2 • CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED • CODEPIPELINE_DEPLOYMENT_COUNT_CHECK • CODEPIPELINE_REGION_FANOUT_CHECK • CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED

Palabras clave de reglas AWS Config administradas compatibles

- CW_LOGGROUP_RETENTION_PERIOD_CHECK
- DAX_ENCRYPTION_ENABLED
- DB_INSTANCE_BACKUP_ENABLED
- DESIRED_INSTANCE_TENANCY
- DESIRED_INSTANCE_TYPE
- DMS_REPLICATION_NO_PUBLIC
- DYNAMODB_AUTOSCALING_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_PITR_ENABLED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_OPTIMIZED_INSTANCE
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL
- EC2_EBS_ENCRYPTION_POR DEFECTO
- EC2_ _COMPROBAR IMDSV2
- EC2_INSTANCE_DETAILED_MONITORING_HABILITADO
- EC2_INSTANCE_ADMINISTRADA_POR_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP
- EC2_INSTANCE_PROFILE_ATTACHED
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED

Palabras clave de reglas AWS Config administradas compatibles

- EC2_MANAGEDINSTANCE_APPLICATIONS_ESTÁ EN LA LISTA NEGRA
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUERIDO
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_INVENTORY_INCLUIDO EN LA LISTA NEGRA
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_NO_AMAZON_KEY_PAIR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RECURSOS_PROTEGIDOS_MEDIANTE UN PLAN DE RESPALDO
- EC2_SECURITY_GROUP_ADJUNTACHED_A_ENI
- EC2_SECURITY_GROUP_ADJUNTACHED_TO_ENI_PERIODIC
- EC2_INSTANCIA_DETENIDA
- EC2_TOKEN_HOP_LIMIT_CHECK
- EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED
- EC2_COMPROBACIÓN DE VOLUMEN EN USO
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED
- ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- ECS_ _HABILITADO AWSVPC_NETWORKING
- ECS_CONTAINER_INSIGHTS_ENABLED
- ECS_CONTAINERS_NONPRIVILEGED
- ECS_CONTAINERS_READONLY_ACCESS
- ECS_FARGATE_LATEST_PLATFORM_VERSION
- ECS_NO_ENVIRONMENT_SECRETS
- ECS_TASK_DEFINITION_LOG_CONFIGURATION
- ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT
- ECS_TASK_DEFINITION_NONROOT_USER
- ECS_TASK_DEFINITION_PID_MODE_CHECK
- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

Palabras clave de reglas AWS Config administradas compatibles
• EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY • EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY • EFS_ENCRYPTED_CHECK • EFS_IN_BACKUP_PLAN • EFS_LAST_BACKUP_RECOVERY_POINT_CREATED • EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN • EIP_ATTACHED • EKS_CLUSTER_LOGGING_ENABLED • EKS_CLUSTER_OLDEST_SUPPORTED_VERSION • EKS_CLUSTER_SUPPORTED_VERSION • EKS_ENDPOINT_NO_PUBLIC_ACCESS • EKS_SECRETS_ENCRYPTED • ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH • ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED • ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK • ELASTICACHE_RBAC_AUTH_ENABLED • ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK • ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED • ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST • ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT • ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED • ELASTICACHE_SUBNET_GROUP_CHECK • ELASTICACHE_SUPPORTED_ENGINE_VERSION • ELASTICSEARCH_ENCRYPTED_AT_REST • ELASTICSEARCH_IN_VPC_ONLY • ELASTICSEARCH_REGISTRA_TO_CLOUDWATCH • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Palabras clave de reglas AWS Config administradas compatibles
• ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • ELB_DELETION_PROTECTION_ENABLED • ELB_LOGGING_ENABLED • ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY • ELBV2_ACM_CERTIFICATE_REQUERIDO • ELBV2_MÚLTIPLE_AZ • EMR_KERBEROS_ENABLED • EMR_MASTER_NO_PUBLIC_IP • ENCRYPTED_VOLUMES • FMS_SHIELD_RESOURCE_POLICY_CHECK • FMS_WEBACL_RESOURCE_POLICY_CHECK • FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK • FSX_LAST_BACKUP_RECOVERY_POINT_CREATED • FSX_RESOURCES_PROTECTED_POR_BACKUP_PLAN • GUARDDUTY_ENABLED_CENTRALIZED • GUARDDUTY_NON_ARCHIVED_FINDINGS • IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS • IAM_GROUP_HAS_USERS_CHECK • IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS • IAM_NO_INLINE_POLICY_CHECK • IAM_PASSWORD_POLICY • IAM_POLICY_BLACKLISTED_CHECK • IAM_POLICY_IN_USE • IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS • IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS • IAM_ROLE_MANAGED_POLICY_CHECK • IAM_ROOT_ACCESS_KEY_CHECK • IAM_USER_GROUP_MEMBERSHIP_CHECK

Palabras clave de reglas AWS Config administradas compatibles
• IAM_USER_MFA_ENABLED • IAM_USER_NO_POLICIES_CHECK • IAM_USER_UNUSED_CREDENTIALS_CHECK • INCOMING_SSH_DISABLED • INSTANCES_IN_VPC • KINESIS_STREAM_ENCRYPTED • INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY • KMS_CMK_NOT_SCHEDULED_FOR_DELETION • LAMBDA_CONCURRENCY_CHECK • LAMBDA_DLQ_CHECK • LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED • LAMBDA_FUNCTION_SETTINGS_CHECK • LAMBDA_INSIDE_VPC • LAMBDA_VPC_MULTI_AZ_CHECK • MACIE_STATUS_CHECK • MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS • MQ_AUTOMATIC_VERSION_MINOR_UPGRADE_ENABLED • MQ_CLOUDWATCH_AUDIT_LOGGING_HABILITADO • MQ_NO_PUBLIC_ACCESS • MULTI_REGION_CLOUD_TRAIL_ENABLED • NACL_NO_UNRESTRICTED_SSH_RDP • NETFW_LOGGING_ENABLED • NETFW_MULTI_AZ_ENABLED • NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS • NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS • NETFW_POLICY_RULE_GROUP_ASSOCIATED • NETFW_STATELESS_RULE_GROUP_NOT_EMPTY • NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED • NO_UNRESTRICTED_ROUTE_TO_IGW

Palabras clave de reglas AWS Config administradas compatibles

- OPENSEARCH_ACCESS_CONTROL_ENABLED
- OPENSEARCH_AUDIT_LOGGING_ENABLED
- OPENSEARCH_DATA_NODE_FAULT_TOLERANCE
- OPENSEARCH_ENCRYPTED_AT_REST
- OPENSEARCH_HTTPS_REQUIRED
- OPENSEARCH_IN_VPC_ONLY
- OPENSEARCH_LOGS_TO_CLOUDWATCH
- OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- RDS_AUTOMATIC_VERSION_MINOR_UPGRADE_ENABLED
- RDS_CLUSTER_DEFAULT_ADMIN_CHECK
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED
- RDS_CLUSTER_MULTI_AZ_ENABLED
- RDS_DB_SECURITY_GROUP_NOT_ALLOWED
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_INSTANCE_DEFAULT_ADMIN_CHECK
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_LOGGING_ENABLED
- RDS_MULTI_AZ_SUPPORT
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- RDS_SNAPSHOTS_PUBLIC_PROHIBITED
- RDS_STORAGE_ENCRYPTED
- REDSHIFT_BACKUP_ENABLED
- REDSHIFT_REQUIRE_TLS_SSL

Palabras clave de reglas AWS Config administradas compatibles

- REDSHIFT_CLUSTER_CONFIGURATION_CHECK
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK
- REDSHIFT_AUDIT_LOGGING_ENABLED
- REDSHIFT_CLUSTER_KMS_ENABLED
- REDSHIFT_DEFAULT_ADMIN_CHECK
- REDSHIFT_DEFAULT_DB_NAME_CHECK
- REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_ACL_PROHIBITED
- S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED
- S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE
- S3_BUCKET_PUBLIC_READ_PROHIBITED
- S3_BUCKET_PUBLIC_WRITE_PROHIBITED
- S3_BUCKET_REPLICATION_ENABLED
- S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED
- S3_BUCKET_SSL_REQUESTS_ONLY
- S3_BUCKET_VERSIONING_ENABLED
- S3_DEFAULT_ENCRYPTION_KMS
- S3_EVENT_NOTIFICATIONS_ENABLED

Palabras clave de reglas AWS Config administradas compatibles
• S3_LAST_BACKUP_RECOVERY_POINT_CREATED • S3_LIFECYCLE_POLICY_CHECK • S3_RESOURCES_PROTECTED_POR_BACKUP_PLAN • S3_VERSION_LIFECYCLE_POLICY_CHECK • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK • SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS • SECRETSMANAGER_ROTATION_ENABLED_CHECK • SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK • SECRETSMANAGER_SECRET_PERIODIC_ROTATION • SECRETSMANAGER_SECRET_UNUSED • SECRETSMANAGER_USING_CMK • INFORMACIÓN DE LA CUENTA DE SEGURIDAD PROPORCIONADA • SECURITYHUB_HABILITADO • SERVICE_VPC_ENDPOINT_ENABLED • SES_MALWARE_SCANNING_ENABLED • SHIELD_ADVANCED_ENABLED_AUTORENEW • SHIELD_DRT_ACCESS • SNS_ENCRYPTED_KMS • SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED • SSM_DOCUMENT_NOT_PUBLIC • STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED • STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED • STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN • SUBRED_AUTO_ASSIGN_PUBLIC_IP_DISABLED • VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED • VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Palabras clave de reglas AWS Config administradas compatibles
• VPC_DEFAULT_SECURITY_GROUP_CLOSED • VPC_FLOW_LOGS_ENABLED • VPC_NETWORK_ACL_UNUSED_CHECK • VPC_PEERING_DNS_RESOLUTION_CHECK • VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS • VPC_VPN_2_TUNNELS_UP • WAF_CLASSIC_LOGGING_ENABLED • WAF_GLOBAL_RULEGROUP_NOT_EMPTY • WAF_GLOBAL_RULE_NOT_EMPTY • WAF_GLOBAL_WEBACL_NOT_EMPTY • WAF_REGIONAL_RULEGROUP_NOT_EMPTY • WAF_REGIONAL_RULE_NOT_EMPTY • WAF_REGIONAL_WEBACL_NOT_EMPTY • WAFV2_HABILITADO PARA EL REGISTRO • WAFV2_GRUPO DE REGLAS NO ESTÁ VACÍO • WAFV2_WEBACL_NOT_EMPTY

Uso de reglas AWS Config personalizadas con Audit Manager

Puede utilizar reglas AWS Config personalizadas como fuente de datos para los informes de auditoría. Cuando un control tiene una fuente de datos asignada a una AWS Config regla, Audit Manager agrega la evaluación que creó la AWS Config regla.

Las reglas personalizadas que puede utilizar dependen de la forma con la Cuenta de AWS que inicie sesión en Audit Manager. Si puede acceder a una regla personalizada en AWS Config, puede utilizarla como mapeo de fuentes de datos en Audit Manager.

- Para uso individual Cuentas de AWS: puede usar cualquiera de las reglas personalizadas que creó con su cuenta.
- Para las cuentas que forman parte de una organización: también puedes usar cualquiera de sus reglas personalizadas de nivel miembro. O bien, puede usar cualquiera de las reglas personalizadas a nivel de organización que estén disponibles en AWS Config.

Tras asignar las reglas personalizadas como origen de datos para un control, puede añadir ese control a un marco personalizado en Audit Manager.

Recursos adicionales

- Para obtener ayuda con problemas relacionados con este tipo de origen de datos, consulte Mi evaluación no consiste en recopilar pruebas de control de cumplimiento de AWS Config y AWS Config integration issues.
- Para crear un control personalizado con este tipo de origen de datos, consulte Crear un control personalizado en AWS Audit Manager.
- Para crear un marco personalizado que utilice el control personalizado, consulte Crear un marco personalizado en AWS Audit Manager.
- Para añadir el control personalizado a un marco personalizado existente, consulte Edición de un marco personalizado en AWS Audit Manager.
- Para crear una regla personalizada en AWS Config, consulta Cómo desarrollar una regla personalizada AWS Config en la Guía para AWS Config desarrolladores.

AWS Security Hub controles compatibles con AWS Audit Manager

Puede usar Audit Manager para capturar los resultados de Security Hub como evidencia para las auditorías. Al crear o editar un control personalizado, puede especificar uno o varios controles de Security Hub como asignación de origen de datos para la recopilación de evidencias. Security Hub realiza comprobaciones de conformidad en función de estos controles, y Audit Manager informa de los resultados como evidencia de las comprobaciones de conformidad.

Contenido

- Puntos clave
- Controles de Security Hub compatibles
- Recursos adicionales

Puntos clave

- Audit Manager no recopila pruebas de AWS Config las reglas vinculadas a servicios que crea Security Hub.

- El 9 de noviembre de 2022, Security Hub lanzó controles de seguridad automatizados alineados con los requisitos de la versión 1.4.0 de AWS Foundations Benchmark del Center for Internet Security (CIS), niveles 1 y 2 (CIS v1.4.0). En Security Hub, se admite el estándar CIS v1.4.0, además del estándar CIS v1.2.0.
- Le recomendamos que active la configuración de hallazgos de control consolidados en Security Hub si aún no está activada. Si habilitas Security Hub el 23 de febrero de 2023 o después, esta configuración estará activada de forma predeterminada.

  Cuando las conclusiones consolidadas están habilitadas, Security Hub genera un resultado único para cada control de seguridad (incluso cuando la misma comprobación se aplica a varios estándares). Cada resultado de Security Hub se recopila como una evaluación de recursos única en Audit Manager. En consecuencia, los resultados consolidados revelan una disminución del total de evaluaciones de recursos únicos que Audit Manager realiza para los resultados de Security Hub. Por esta razón, el uso de hallazgos consolidados puede resultar en una reducción de los costos de uso de Audit Manager a menudo sin sacrificar la calidad y la disponibilidad de las pruebas. Para obtener más información sobre los precios, consulte Precios de AWS Audit Manager.

Ejemplos de pruebas cuando se activa o desactiva la obtención de resultados consolidados

Los siguientes ejemplos muestran una comparación de la forma en que Audit Manager recopila y presenta las pruebas en función de la configuración de Security Hub.

When consolidated findings is turned on

Supongamos que ha activado los tres estándares de seguridad siguientes en Security Hub: AWS FSBP, PCI DSS y CIS Benchmark v1.2.0.

- Estos tres estándares utilizan el mismo control (IAM.4) con la misma regla subyacente (-check). AWS Config iam-root-access-key
- Dado que la configuración de resultados consolidados está activada, Security Hub generará un único resultado para este control.
- Security Hub envía el resultado consolidado a Audit Manager para este control.
- El resultado consolidado cuenta como una evaluación de recursos única en Audit Manager. Como resultado, se añade una sola prueba a su evaluación.

A continuación, se muestra un ejemplo de cómo podría verse esa prueba:


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109",
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "security-control/IAM.4",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2023-10-25T11:32:24.861Z",
    "LastObservedAt": "2023-11-02T11:59:19.546Z",
    "CreatedAt": "2023-10-25T11:32:24.861Z",
    "UpdatedAt": "2023-11-02T11:59:15.127Z",
    "Severity": {
        "Label": "INFORMATIONAL",
        "Normalized": 0,
        "Original": "INFORMATIONAL"
    },
    "Title": "IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is
 available.",
    "Remediation": {
        "Recommendation": {
            "Text": "For information on how to correct this issue, consult the AWS
 Security Hub controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
        }
    },
    "ProductFields": {
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "aws/securityhub/ProductName": "Security Hub",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
```

```
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
    },
    "Resources": [{
        "Type": "AwsAccount",
        "Id": "AWS::::Account:111122223333",
        "Partition": "aws",
        "Region": "us-west-2"
    }],
    "Compliance": {
        "Status": "PASSED",
        "RelatedRequirements": [
            "CIS AWS Foundations Benchmark v1.2.0/1.12"
        ],
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [{
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            },
            {
                "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
            }
        ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards"
        ]
    },
    "ProcessedAt": "2023-11-02T11:59:20.980Z"
}
```

When consolidated findings is turned off

Supongamos que ha activado los tres estándares de seguridad siguientes en Security Hub: AWS FSBP, PCI DSS y CIS Benchmark v1.2.0.

- Estos tres estándares utilizan el mismo control (IAM.4) con la misma regla subyacente (-check). AWS Config iam-root-access-key
- Como la configuración de resultados consolidados está desactivada, Security Hub genera un hallazgo independiente por cada control de seguridad para cada estándar habilitado (en este caso, tres hallazgos).
- Security Hub envía tres conclusiones independientes específicas de la norma a Audit Manager para este control.
- Los tres resultados cuentan como tres evaluaciones de recursos únicas en Audit Manager. Por este motivo, se agregarán tres pruebas independientes a la evaluación.

A continuación, se muestra un ejemplo de cómo podría verse esa prueba. Tenga en cuenta que en este ejemplo, cada una de las tres cargas útiles siguientes tiene el mismo ID de control de seguridad (*`SecurityControlId":"IAM.4"`*). Por eso, el control de evaluación que recopila estas pruebas en Audit Manager (IAM.4) recibe tres pruebas distintas cuando Security Hub obtiene los siguientes resultados.

Prueba a favor de la IAM.4 (FSBP)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
```

```
            "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d",
            "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
            "ProductName":"Security Hub",
            "CompanyName":"AWS",
            "Region":"us-west-2",
            "GeneratorId":"aws-foundational-security-best-practices/v/1.0.0/IAM.4",
            "AwsAccountId":"111122223333",
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
            ],
            "FirstObservedAt":"2020-10-05T19:18:47.848Z",
            "LastObservedAt":"2023-11-01T14:12:04.106Z",
            "CreatedAt":"2020-10-05T19:18:47.848Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"IAM.4 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
               "ControlId":"IAM.4",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
```

```
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
                  "Partition":"aws",
                  "Region":"us-west-2"
               }
            ],
            "Compliance":{
               "Status":"PASSED",
               "SecurityControlId":"IAM.4",
               "AssociatedStandards":[
                  {
                     "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
                  }
               ]
            },
            "WorkflowState":"NEW",
            "Workflow":{
               "Status":"RESOLVED"
            },
            "RecordState":"ACTIVE",
            "FindingProviderFields":{
               "Severity":{
                  "Label":"INFORMATIONAL",
                  "Original":"INFORMATIONAL"
               },
               "Types":[
                  "Software and Configuration Checks/Industry and Regulatory
 Standards/AWS-Foundational-Security-Best-Practices"
               ]
            },
```

```
            "ProcessedAt":"2023-11-01T14:12:07.395Z"
        }
     ]
  }
}
```

Prueba a favor de la IAM.4 (CIS 1.2)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.775Z",
           "LastObservedAt":"2023-11-01T14:12:07.989Z",
           "CreatedAt":"2020-10-05T19:18:47.775Z",
```

```
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"1.12 Ensure no root user access key exists",
            "Description":"The root user is the most privileged user in an AWS
 account. AWS Access Keys provide programmatic access to a given AWS account. It is
 recommended that all access keys associated with the root user be removed.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsGuideArn":"arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
               "StandardsGuideSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
               "RuleId":"1.12",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
                  "Partition":"aws",
```

```
                "Region":"us-west-2"
            }
        ],
        "Compliance":{
            "Status":"PASSED",
            "SecurityControlId":"IAM.4",
            "AssociatedStandards":[
                {
                    "StandardsId":"ruleset/cis-aws-foundations-benchmark/v/1.2.0"
                }
            ]
        },
        "WorkflowState":"NEW",
        "Workflow":{
            "Status":"RESOLVED"
        },
        "RecordState":"ACTIVE",
        "FindingProviderFields":{
            "Severity":{
                "Label":"INFORMATIONAL",
                "Original":"INFORMATIONAL"
            },
            "Types":[
                "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
            ]
        },
        "ProcessedAt":"2023-11-01T14:12:13.436Z"
    }
  ]
 }
}
```


Prueba a favor del PCI.IAM.1 (PCI DSS)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
```

```
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.788Z",
           "LastObservedAt":"2023-11-01T14:12:02.413Z",
           "CreatedAt":"2020-10-05T19:18:47.788Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"PCI.IAM.1 IAM root user access key should not exist",
           "Description":"This AWS control checks whether the root user access key
 is available.",
           "Remediation":{
              "Recommendation":{
                 "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                 "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
              }
           },
           "ProductFields":{
              "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
```

```
              "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
              "ControlId":"PCI.IAM.1",
              "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
              "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
              "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
              "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
              "aws/securityhub/ProductName":"Security Hub",
              "aws/securityhub/CompanyName":"AWS",
              "Resources:0/Id":"arn:aws:iam::111122223333:root",
              "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
           },
           "Resources":[
              {
                 "Type":"AwsAccount",
                 "Id":"AWS::::Account:111122223333",
                 "Partition":"aws",
                 "Region":"us-west-2"
              }
           ],
           "Compliance":{
              "Status":"PASSED",
              "RelatedRequirements":[
                 "PCI DSS 2.1",
                 "PCI DSS 2.2",
                 "PCI DSS 7.2.1"
              ],
              "SecurityControlId":"IAM.4",
              "AssociatedStandards":[
                 {
                    "StandardsId":"standards/pci-dss/v/3.2.1"
                 }
              ]
           },
           "WorkflowState":"NEW",
           "Workflow":{
              "Status":"RESOLVED"
           },
           "RecordState":"ACTIVE",
```

```
            "FindingProviderFields":{
               "Severity":{
                  "Label":"INFORMATIONAL",
                  "Original":"INFORMATIONAL"
               },
               "Types":[
                  "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
               ]
            },
            "ProcessedAt":"2023-11-01T14:12:05.950Z"
         }
      ]
   }
}
```

Controles de Security Hub compatibles

Audit Manager admite actualmente los siguientes controles de Security Hub. Puede utilizar cualquiera de las siguientes palabras clave de identificación de control específicas del estándar al configurar un origen de datos para un control personalizado.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
CIS v1.2.0	1.2	IAM.5
CIS v1.2.0	1.3	IAM.8
CIS v1.2.0	1.4	IAM.3
CIS v1.2.0	1.5	IAM.11
CIS v1.2.0	1.6	IAM.12

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
CIS v1.2.0	1.7	IAM.13
CIS v1.2.0	1.8	IAM.14
CIS v1.2.0	1.9	IAM.15
CIS v1.2.0	1.10	IAM.16
CIS v1.2.0	1.11	IAM.17
CIS v1.2.0	1.12	IAM.4
CIS v1.2.0	1.13	IAM.9
CIS v1.2.0	1.14	IAM.6
CIS v1.2.0	1.16	IAM.2
CIS v1.2.0	1.20	IAM.18
CIS v1.2.0	1.22	IAM.1
CIS v1.2.0	2.1	CloudTrail1.
CIS v1.2.0	2.2	CloudTrail4.
CIS v1.2.0	2.3	CloudTrail6.
CIS v1.2.0	2.4	CloudTrail5.
CIS v1.2.0	2,5	Config.1
CIS v1.2.0	2.6	CloudTrail.7.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
CIS v1.2.0	2.7	CloudTrail2.
CIS v1.2.0	2.8	KMS.4
CIS v1.2.0	2.9	EC26.
CIS v1.2.0	3.1	CloudWatch2.
CIS v1.2.0	3.2	CloudWatch3.
CIS v1.2.0	3.3	CloudWatch1.
CIS v1.2.0	3.4	CloudWatch.4.
CIS v1.2.0	3.5	CloudWatch5.
CIS v1.2.0	3.6	CloudWatch6.
CIS v1.2.0	3.7	CloudWatch.7.
CIS v1.2.0	3.8	CloudWatch.8.
CIS v1.2.0	3.9	CloudWatch.9.
CIS v1.2.0	3.10	CloudWatch.10
CIS v1.2.0	3.11	CloudWatch.11
CIS v1.2.0	3.12	CloudWatch.12
CIS v1.2.0	3.13	CloudWatch.13
CIS v1.2.0	3.14	CloudWatch.14

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
CIS v1.2.0	4.1	EC2.13
CIS v1.2.0	4.2	EC2.14
CIS v1.2.0	4.3	EC22.
PCI DSS	PCI. AutoScaling1.	AutoScaling1.
PCI DSS	PCI. CloudTrail1.	CloudTrail1.
PCI DSS	PCI. CloudTrail2.	CloudTrail2.
PCI DSS	PCI. CloudTrail3.	CloudTrail3.
PCI DSS	PCI. CloudTrail4.	CloudTrail.4.
PCI DSS	PCI. CodeBuild 1.	CodeBuild1.
PCI DSS	PCI. CodeBuild 2.	CodeBuild2.
PCI DSS	PCI.config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch1.
PCI DSS	PCI.DMS.1	DMS.1

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
PCI DSS	PCI. EC21.	EC21.
PCI DSS	PCI. EC22.	EC22.
PCI DSS	PCI. EC23.	EC23.
PCI DSS	PCI. EC24.	EC2.12
PCI DSS	PCI. EC25.	EC2.13
PCI DSS	PCI. EC26.	EC26.
PCI DSS	PCI. ELBv21.	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2
PCI DSS	PCI. GuardDuty 1.	GuardDuty1.
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI. IAM8.
PCI DSS	PCI.KMS.1	PCI.KMS.4
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI. Lambda.2	Lambda.3
PCI DSS	PCI.OpenSearch.1	Opensearch.1
PCI DSS	PCI.OpenSearch.2	Opensearch.2
PCI DSS	PCI.RDS.1	RDS.1
PCI DSS	PCI.RDS.2	RDS.2
PCI DSS	PCI. Redshift. 1	Redshift.1
PCI DSS	PCIS.3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
PCI DSS	PCI. SageMaker 1.	SageMaker1.
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3
AWS Mejores prácticas de seguridad fundamentales	Account.1	Account.1
AWS Mejores prácticas fundamentales de seguridad	Account.2	Account.2
AWS Mejores prácticas fundamentales de seguridad	ACM.1	ACM.1
AWS Mejores prácticas fundamentales de seguridad	ACM.2	ACM.2
AWS Mejores prácticas fundamentales de seguridad	APIGateway1.	APIGateway1.
AWS Mejores prácticas fundamentales de seguridad	APIGateway2.	APIGateway2.
AWS Mejores prácticas de seguridad fundamentales	APIGateway3.	APIGateway3.
AWS Mejores prácticas de seguridad fundamentales	APIGateway4.	APIGateway4.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	APIGateway5.	APIGateway5.
AWS Mejores prácticas fundamentales de seguridad	APIGateway8.	APIGateway.8.
AWS Mejores prácticas fundamentales de seguridad	APIGateway9.	APIGateway.9.
AWS Mejores prácticas fundamentales de seguridad	AppSync2.	AppSync2.
AWS Mejores prácticas de seguridad fundamentales	AppSync5.	AppSync5.
AWS Mejores prácticas fundamentales de seguridad	Athena.1	Athena.1
AWS Mejores prácticas fundamentales de seguridad	AutoScaling1.	AutoScaling1.
AWS Mejores prácticas fundamentales de seguridad	AutoScaling2.	AutoScaling2.
AWS Mejores prácticas de seguridad fundamentales	AutoScaling3.	AutoScaling3.
AWS Mejores prácticas de seguridad fundamentales	AutoScaling4.	AutoScaling4.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	Autoscaling.5	Autoscaling.5
AWS Mejores prácticas fundamentales de seguridad	AutoScaling6.	AutoScaling6.
AWS Mejores prácticas fundamentales de seguridad	AutoScaling9.	AutoScaling.9.
AWS Mejores prácticas fundamentales de seguridad	Backup.1	Backup.1
AWS Mejores prácticas fundamentales de seguridad	CloudForm ation1.	CloudFormation1.
AWS Mejores prácticas fundamentales de seguridad	CloudFront1.	CloudFront1.
AWS Mejores prácticas fundamentales de seguridad	CloudFront2.	CloudFront2.
AWS Mejores prácticas de seguridad fundamentales	CloudFront3.	CloudFront3.
AWS Mejores prácticas de seguridad fundamentales	CloudFront4.	CloudFront4.
AWS Mejores prácticas fundamentales de seguridad	CloudFront5.	CloudFront5.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	CloudFront6.	CloudFront6.
AWS Mejores prácticas fundamentales de seguridad	CloudFront7.	CloudFront7.
AWS Mejores prácticas fundamentales de seguridad	CloudFront8.	CloudFront.8.
AWS Mejores prácticas fundamentales de seguridad	CloudFront9.	CloudFront.9.
AWS Mejores prácticas fundamentales de seguridad	CloudFront.10	CloudFront.10
AWS Mejores prácticas fundamentales de seguridad	CloudFront1.2	CloudFront.12
AWS Mejores prácticas fundamentales de seguridad	CloudFront1.3	CloudFront.13
AWS Mejores prácticas fundamentales de seguridad	CloudTrail1.	CloudTrail1.
AWS Mejores prácticas fundamentales de seguridad	CloudTrail2.	CloudTrail2.
AWS Mejores prácticas de seguridad fundamentales	CloudTrail3.	CloudTrail3.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas de seguridad fundamentales	CloudTrail4.	CloudTrail4.
AWS Mejores prácticas fundamentales de seguridad	CloudTrail5.	CloudTrail5.
AWS Mejores prácticas fundamentales de seguridad	CloudTrail6.	CloudTrail6.
AWS Mejores prácticas fundamentales de seguridad	CloudTrail7.	CloudTrail7.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.	CloudWatch1.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch2.	CloudWatch2.
AWS Mejores prácticas de seguridad fundamentales	CloudWatch3.	CloudWatch3.
AWS Mejores prácticas de seguridad fundamentales	CloudWatch4.	CloudWatch4.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch5.	CloudWatch5.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch6.	CloudWatch6.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	CloudWatch7.	CloudWatch7.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch8.	CloudWatch.8.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch9.	CloudWatch.9.
AWS Mejores prácticas fundamentales de seguridad	CloudWatch.10	CloudWatch.10
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.1	CloudWatch.11
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.2	CloudWatch.12
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.3	CloudWatch.13
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.4	CloudWatch.14
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.5	CloudWatch.15
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.6	CloudWatch.16

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	CloudWatch1.7	CloudWatch.17
AWS Mejores prácticas fundamentales de seguridad	CodeBuild1.	CodeBuild1.
AWS Mejores prácticas fundamentales de seguridad	CodeBuild2.	CodeBuild2.
AWS Mejores prácticas de seguridad fundamentales	CodeBuild3.	CodeBuild3.
AWS Mejores prácticas de seguridad fundamentales	CodeBuild4.	CodeBuild4.
AWS Mejores prácticas fundamentales de seguridad	CodeBuild5.	CodeBuild5.
AWS Mejores prácticas fundamentales de seguridad	Config. 1	Config.1
AWS Mejores prácticas fundamentales de seguridad	DMS.1	DMS.1
AWS Mejores prácticas fundamentales de seguridad	DMS.6	DMS.6
AWS Mejores prácticas fundamentales de seguridad	DMS.7	DMS.7

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	DMS.8	DMS.8
AWS Mejores prácticas fundamentales de seguridad	DMS.9	DMS.9
AWS Mejores prácticas fundamentales de seguridad	DocumentDB.1	DocumentDB.1
AWS Mejores prácticas fundamentales de seguridad	DocumentDB.2	DocumentDB.2
AWS Mejores prácticas fundamentales de seguridad	DocumentDB.3	DocumentDB.3
AWS Mejores prácticas fundamentales de seguridad	DocumentDB.4	DocumentDB.4
AWS Mejores prácticas fundamentales de seguridad	DocumentDB.5	DocumentDB.5
AWS Mejores prácticas fundamentales de seguridad	DynamoDB.1	DynamoDB.1
AWS Mejores prácticas fundamentales de seguridad	DynamoDB.2	DynamoDB.2
AWS Mejores prácticas fundamentales de seguridad	DynamoDB.3	DynamoDB.3

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	DynamoDB.4	DynamoDB.4
AWS Mejores prácticas fundamentales de seguridad	DynamoDB.6	DynamoDB.6
AWS Mejores prácticas fundamentales de seguridad	EC21.	EC21.
AWS Mejores prácticas fundamentales de seguridad	EC22.	EC22.
AWS Mejores prácticas de seguridad fundamentales	EC23.	EC23.
AWS Mejores prácticas de seguridad fundamentales	EC24.	EC24.
AWS Mejores prácticas fundamentales de seguridad	EC26.	EC26.
AWS Mejores prácticas fundamentales de seguridad	EC27.	EC27.
AWS Mejores prácticas fundamentales de seguridad	EC28.	EC2.8.
AWS Mejores prácticas fundamentales de seguridad	EC29.	EC2.9.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	EC2.10	EC2.10
AWS Mejores prácticas fundamentales de seguridad	EC21.2	EC2.12
AWS Mejores prácticas fundamentales de seguridad	EC21.3	EC2.13
AWS Mejores prácticas fundamentales de seguridad	EC21.4	EC2.14
AWS Mejores prácticas fundamentales de seguridad	EC21.5	EC2.15
AWS Mejores prácticas fundamentales de seguridad	EC21.6	EC2.16
AWS Mejores prácticas fundamentales de seguridad	EC21.7	EC2.17
AWS Mejores prácticas fundamentales de seguridad	EC21.8	EC2.18
AWS Mejores prácticas fundamentales de seguridad	EC21.9	EC2.19
AWS Mejores prácticas fundamentales de seguridad	EC22.0	EC2.20

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	EC22.1	EC2.21
AWS Mejores prácticas fundamentales de seguridad	EC22.2	EC2.22
AWS Mejores prácticas fundamentales de seguridad	EC22.3	EC2.23
AWS Mejores prácticas fundamentales de seguridad	EC22.4	EC2.24
AWS Mejores prácticas fundamentales de seguridad	EC22.5	EC2.25
AWS Mejores prácticas fundamentales de seguridad	EC22.8	EC2.28
AWS Mejores prácticas fundamentales de seguridad	EC25.1	EC2.51
AWS Mejores prácticas fundamentales de seguridad	ECR.1	ECR.1
AWS Mejores prácticas fundamentales de seguridad	ECR.2	ECR.2
AWS Mejores prácticas fundamentales de seguridad	ECR.3	ECR.3

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	ECS.1	ECS.1
AWS Mejores prácticas fundamentales de seguridad	ECS.2	ECS.2
AWS Mejores prácticas fundamentales de seguridad	ECS.3	ECS.3
AWS Mejores prácticas fundamentales de seguridad	ECS.4	ECS.4
AWS Mejores prácticas fundamentales de seguridad	ECS.5	ECS.5
AWS Mejores prácticas fundamentales de seguridad	ECS.8	ECS.8
AWS Mejores prácticas fundamentales de seguridad	ECS.9	ECS.9
AWS Mejores prácticas fundamentales de seguridad	ECS.10	ECS.10
AWS Mejores prácticas fundamentales de seguridad	ECS.12	ECS.12
AWS Mejores prácticas fundamentales de seguridad	EFS.1	EFS.1

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	EFS 2	EFS. 2
AWS Mejores prácticas fundamentales de seguridad	EFS 3	EFS.3
AWS Mejores prácticas fundamentales de seguridad	EFS 4	EFS.4
AWS Mejores prácticas fundamentales de seguridad	EKS.1	EKS.1
AWS Mejores prácticas fundamentales de seguridad	EKS.2	EKS.2
AWS Mejores prácticas fundamentales de seguridad	EKS.8	EKS.8
AWS Mejores prácticas fundamentales de seguridad	ElastiCache1.	ElastiCache1.
AWS Mejores prácticas fundamentales de seguridad	ElastiCache2.	ElastiCache2.
AWS Mejores prácticas de seguridad fundamentales	ElastiCache3.	ElastiCache3.
AWS Mejores prácticas de seguridad fundamentales	ElastiCache4.	ElastiCache4.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	ElastiCache5.	ElastiCache5.
AWS Mejores prácticas fundamentales de seguridad	ElastiCache6.	ElastiCache6.
AWS Mejores prácticas fundamentales de seguridad	ElastiCache7.	ElastiCache7.
AWS Mejores prácticas fundamentales de seguridad	ElasticBeanstalk1.	ElasticBeanstalk1.
AWS Mejores prácticas fundamentales de seguridad	ElasticBeanstalk2.	ElasticBeanstalk2.
AWS Mejores prácticas de seguridad fundamentales	ElasticBeanstalk3.	ElasticBeanstalk3.
AWS Mejores prácticas de seguridad fundamentales	ELB.1	ELB.1
AWS Mejores prácticas fundamentales de seguridad	ELB.2	ELB.2
AWS Mejores prácticas fundamentales de seguridad	ELB.3	ELB.3
AWS Mejores prácticas fundamentales de seguridad	ELB.4	ELB.4

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	ELB.5	ELB.5
AWS Mejores prácticas fundamentales de seguridad	ELB.6	ELB.6
AWS Mejores prácticas fundamentales de seguridad	ELB.7	ELB.7
AWS Mejores prácticas fundamentales de seguridad	ELB.8	ELB.8
AWS Mejores prácticas fundamentales de seguridad	ELB.9	ELB.9
AWS Mejores prácticas fundamentales de seguridad	ELB.10	ELB.10
AWS Mejores prácticas fundamentales de seguridad	ELB.12	ELB.12
AWS Mejores prácticas fundamentales de seguridad	ELB.13	ELB.13
AWS Mejores prácticas fundamentales de seguridad	ELB.14	ELB.14
AWS Mejores prácticas fundamentales de seguridad	ELB.16	ELB.16

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	ELBv21.	ELB.1
AWS Mejores prácticas fundamentales de seguridad	EMR.1	EMR.1
AWS Mejores prácticas fundamentales de seguridad	EMR.2	EMR.2
AWS Mejores prácticas fundamentales de seguridad	ES.1	ES.1
AWS Mejores prácticas fundamentales de seguridad	ES.2	ES.2
AWS Mejores prácticas fundamentales de seguridad	ES.3	ES.3
AWS Mejores prácticas fundamentales de seguridad	ES.4	ES.4
AWS Mejores prácticas fundamentales de seguridad	ES.5	ES.5
AWS Mejores prácticas fundamentales de seguridad	ES.6	ES.6
AWS Mejores prácticas fundamentales de seguridad	ES.7	ES.7

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	ES.8	ES.8
AWS Mejores prácticas fundamentales de seguridad	EventBridge3.	EventBridge3.
AWS Mejores prácticas fundamentales de seguridad	EventBridge4.	EventBridge4.
AWS Mejores prácticas fundamentales de seguridad	FSx1.	FSx1.
AWS Mejores prácticas fundamentales de seguridad	GuardDuty1.	GuardDuty1.
AWS Mejores prácticas fundamentales de seguridad	IAM.1	IAM.1
AWS Mejores prácticas fundamentales de seguridad	IAM.2	IAM.2
AWS Mejores prácticas fundamentales de seguridad	IAM.3	IAM.3
AWS Mejores prácticas fundamentales de seguridad	IAM.4	IAM.4
AWS Mejores prácticas fundamentales de seguridad	IAM.5	IAM.5

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	IAM.6	IAM.6
AWS Mejores prácticas fundamentales de seguridad	IAM.7	IAM.7
AWS Mejores prácticas fundamentales de seguridad	IAM.8	IAM.8
AWS Mejores prácticas fundamentales de seguridad	IAM.9	IAM.9
AWS Mejores prácticas fundamentales de seguridad	IAM.10	IAM.10
AWS Mejores prácticas fundamentales de seguridad	IAM.11	IAM.11
AWS Mejores prácticas fundamentales de seguridad	IAM.12	IAM.12
AWS Mejores prácticas fundamentales de seguridad	IAM.13	IAM.13
AWS Mejores prácticas fundamentales de seguridad	IAM.14	IAM.14
AWS Mejores prácticas fundamentales de seguridad	IAM.15	IAM.15

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	IAM.16	IAM.16
AWS Mejores prácticas fundamentales de seguridad	IAM.17	IAM.17
AWS Mejores prácticas fundamentales de seguridad	IAM.18	IAM.18
AWS Mejores prácticas fundamentales de seguridad	IAM.19	IAM.19
AWS Mejores prácticas fundamentales de seguridad	IAM.21	IAM.21
AWS Mejores prácticas fundamentales de seguridad	IAM.22	IAM.22
AWS Mejores prácticas fundamentales de seguridad	Kinesis.1	Kinesis.1
AWS Mejores prácticas fundamentales de seguridad	KMS.1	KMS.1
AWS Mejores prácticas fundamentales de seguridad	KMS.2	KMS.2
AWS Mejores prácticas fundamentales de seguridad	KMS.3	KMS.3

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	KMS.4	KMS.4
AWS Mejores prácticas fundamentales de seguridad	Lambda.1	Lambda.1
AWS Mejores prácticas fundamentales de seguridad	Lambda.2	Lambda.2
AWS Mejores prácticas fundamentales de seguridad	Lambda 3	Lambda 3
AWS Mejores prácticas fundamentales de seguridad	Lambda.5	Lambda.5
AWS Mejores prácticas fundamentales de seguridad	Macie.1	Macie.1
AWS Mejores prácticas fundamentales de seguridad	MQ.5	MQ.5
AWS Mejores prácticas fundamentales de seguridad	MQ.6	MQ.6
AWS Mejores prácticas fundamentales de seguridad	MSK.1	MSK.1
AWS Mejores prácticas fundamentales de seguridad	MSK.2	MSK.2

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	Neptune.1	Neptune.1
AWS Mejores prácticas fundamentales de seguridad	Neptune.2	Neptune.2
AWS Mejores prácticas fundamentales de seguridad	Neptune.3	Neptune.3
AWS Mejores prácticas fundamentales de seguridad	Neptune.4	Neptune.4
AWS Mejores prácticas fundamentales de seguridad	Neptune.5	Neptune.5
AWS Mejores prácticas fundamentales de seguridad	Neptune.6	Neptune.6
AWS Mejores prácticas fundamentales de seguridad	Neptune.7	Neptune.7
AWS Mejores prácticas fundamentales de seguridad	Neptune.8	Neptune.8
AWS Mejores prácticas fundamentales de seguridad	Neptune.9	Neptune.9
AWS Mejores prácticas fundamentales de seguridad	NetworkFirewall1.	NetworkFirewall1.

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	NetworkFirewall2.	NetworkFirewall2.
AWS Mejores prácticas de seguridad fundamentales	NetworkFirewall3.	NetworkFirewall3.
AWS Mejores prácticas de seguridad fundamentales	NetworkFirewall4.	NetworkFirewall4.
AWS Mejores prácticas fundamentales de seguridad	NetworkFirewall5.	NetworkFirewall5.
AWS Mejores prácticas fundamentales de seguridad	NetworkFirewall6.	NetworkFirewall6.
AWS Mejores prácticas fundamentales de seguridad	NetworkFirewall9.	NetworkFirewall.9.
AWS Mejores prácticas fundamentales de seguridad	Opensearch.1	Opensearch.1
AWS Mejores prácticas fundamentales de seguridad	Opensearch.2	Opensearch.2
AWS Mejores prácticas fundamentales de seguridad	Opensearch.3	Opensearch.3
AWS Mejores prácticas fundamentales de seguridad	Opensearch.4	Opensearch.4

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	Opensearch.5	Opensearch.5
AWS Mejores prácticas fundamentales de seguridad	Opensearch.6	Opensearch.6
AWS Mejores prácticas fundamentales de seguridad	Opensearch.7	Opensearch.7
AWS Mejores prácticas fundamentales de seguridad	Opensearch.8	Opensearch.8
AWS Mejores prácticas fundamentales de seguridad	Opensearch.10	Opensearch.10
AWS Mejores prácticas fundamentales de seguridad	PCA.1	PCA.1
AWS Mejores prácticas fundamentales de seguridad	RDS.1	RDS.1
AWS Mejores prácticas fundamentales de seguridad	RDS.2	RDS.2
AWS Mejores prácticas fundamentales de seguridad	RDS.3	RDS.3
AWS Mejores prácticas fundamentales de seguridad	RED.4	RDS.4

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	RDS.5	RDS.5
AWS Mejores prácticas fundamentales de seguridad	RDS.6	RDS.6
AWS Mejores prácticas fundamentales de seguridad	RDS.7	RDS.7
AWS Mejores prácticas fundamentales de seguridad	RDS.8	RDS.8
AWS Mejores prácticas fundamentales de seguridad	RDS.9	RDS.9
AWS Mejores prácticas fundamentales de seguridad	RDS.10	RDS.10
AWS Mejores prácticas fundamentales de seguridad	RDS.11	RDS.11
AWS Mejores prácticas fundamentales de seguridad	RDS.12	RDS.12
AWS Mejores prácticas fundamentales de seguridad	RDS.13	RDS.13
AWS Mejores prácticas fundamentales de seguridad	RDS.14	RDS.14

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	RDS.15	RDS.15
AWS Mejores prácticas fundamentales de seguridad	RDS.16	RDS.16
AWS Mejores prácticas fundamentales de seguridad	RDS.17	RDS.17
AWS Mejores prácticas fundamentales de seguridad	RDS.18	RDS.18
AWS Mejores prácticas fundamentales de seguridad	RDS.19	RDS.19
AWS Mejores prácticas fundamentales de seguridad	RDS.20	RDS.20
AWS Mejores prácticas fundamentales de seguridad	RDS.21	RDS.21
AWS Mejores prácticas fundamentales de seguridad	RDS.22	RDS.22
AWS Mejores prácticas fundamentales de seguridad	RDS.23	RDS.23
AWS Mejores prácticas fundamentales de seguridad	RDS.24	RDS.24

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	RDS.25	RDS.25
AWS Mejores prácticas fundamentales de seguridad	RDS.26	RDS.26
AWS Mejores prácticas fundamentales de seguridad	RDS.27	RDS.27
AWS Mejores prácticas fundamentales de seguridad	RDS.34	RDS.34
AWS Mejores prácticas fundamentales de seguridad	RDS.35	RDS.35
AWS Mejores prácticas fundamentales de seguridad	Redshift.1	Redshift.1
AWS Mejores prácticas fundamentales de seguridad	Redshift.2	Redshift.2
AWS Mejores prácticas fundamentales de seguridad	Redshift.3	Redshift.3
AWS Mejores prácticas fundamentales de seguridad	Redshift.4	Redshift.4
AWS Mejores prácticas fundamentales de seguridad	Redshift.6	Redshift.6

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	Redshift.7	Redshift.7
AWS Mejores prácticas fundamentales de seguridad	Redshift.8	Redshift.8
AWS Mejores prácticas fundamentales de seguridad	Redshift.9	Redshift.9
AWS Mejores prácticas fundamentales de seguridad	Redshift.10	Redshift.10
AWS Mejores prácticas fundamentales de seguridad	Route53.2	Route53.2
AWS Mejores prácticas fundamentales de seguridad	S3.1	S3.1
AWS Mejores prácticas fundamentales de seguridad	S3.2	S3.2
AWS Mejores prácticas fundamentales de seguridad	S3.3	S3.3
AWS Mejores prácticas fundamentales de seguridad	S3.4	S3.4
AWS Mejores prácticas fundamentales de seguridad	S3.5	S3.5

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	S3.6	S3.6
AWS Mejores prácticas fundamentales de seguridad	S3.7	S3.7
AWS Mejores prácticas fundamentales de seguridad	S3.8	S3.8
AWS Mejores prácticas fundamentales de seguridad	S3.9	S3.9
AWS Mejores prácticas fundamentales de seguridad	S3.11	S3.11
AWS Mejores prácticas fundamentales de seguridad	S3.12	S3.12
AWS Mejores prácticas fundamentales de seguridad	S3.13	S3.13
AWS Mejores prácticas fundamentales de seguridad	S3.14	S3.14
AWS Mejores prácticas fundamentales de seguridad	S3.15	S3.15
AWS Mejores prácticas fundamentales de seguridad	S3.17	S3.17

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	S3.19	S3.19
AWS Mejores prácticas fundamentales de seguridad	S3.19	S3.20
AWS Mejores prácticas fundamentales de seguridad	SageMaker1.	SageMaker1.
AWS Mejores prácticas fundamentales de seguridad	SageMaker2.	SageMaker2.
AWS Mejores prácticas de seguridad fundamentales	SageMaker3.	SageMaker3.
AWS Mejores prácticas de seguridad fundamentales	SecretsManager1.	SecretsManager1.
AWS Mejores prácticas fundamentales de seguridad	SecretsManager2.	SecretsManager2.
AWS Mejores prácticas de seguridad fundamentales	SecretsManager3.	SecretsManager3.
AWS Mejores prácticas de seguridad fundamentales	SecretsManager4.	SecretsManager4.
AWS Mejores prácticas fundamentales de seguridad	SNS.1	SNS.1

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	SNS.2	SNS.2
AWS Mejores prácticas fundamentales de seguridad	SQS.1	SQS.1
AWS Mejores prácticas fundamentales de seguridad	SSM.1	SSM.1
AWS Mejores prácticas fundamentales de seguridad	SSM.2	SSM.2
AWS Mejores prácticas fundamentales de seguridad	SSM 3	SSM.3
AWS Mejores prácticas fundamentales de seguridad	SSM 4	SSM.4
AWS Mejores prácticas fundamentales de seguridad	StepFunctions1.	StepFunctions1.
AWS Mejores prácticas fundamentales de seguridad	WAF.1	WAF.1
AWS Mejores prácticas fundamentales de seguridad	WAF.2	WAF.2
AWS Mejores prácticas fundamentales de seguridad	WAF.3	WAF.3

Estándar de seguridad	Palabra clave admitida en Audit Manager (ID de control estándar en Security Hub)	Documentación de control relacionada (ID de control de seguridad correspondiente en Security Hub)
AWS Mejores prácticas fundamentales de seguridad	WAF.4	WAF.4
AWS Mejores prácticas fundamentales de seguridad	WAF.6	WAF.6
AWS Mejores prácticas fundamentales de seguridad	WAF.7	WAF.7
AWS Mejores prácticas fundamentales de seguridad	WAF.8	WAF.8
AWS Mejores prácticas fundamentales de seguridad	WAF.10	WAF.10
AWS Mejores prácticas fundamentales de seguridad	WAF.11	WAF.11
AWS Mejores prácticas fundamentales de seguridad	WAF.12	WAF.12

Recursos adicionales

- Para obtener ayuda con problemas relacionados con recopilación de evidencias para este tipo de origen de datos, consulte Mi evaluación no consiste en recopilar pruebas de control de cumplimiento de AWS Security Hub.
- Para crear un control personalizado con este tipo de origen de datos, consulte Crear un control personalizado en AWS Audit Manager.
- Para crear un marco personalizado que utilice el control personalizado, consulte Crear un marco personalizado en AWS Audit Manager.

- Para añadir el control personalizado a un marco personalizado existente, consulte Edición de un marco personalizado en AWS Audit Manager.

AWS Las llamadas a la API son compatibles con AWS Audit Manager

Puede usar Audit Manager para capturar instantáneas de su AWS entorno como evidencia para las auditorías. Al crear o editar un control personalizado, puede especificar una o más llamadas a la AWS API como mapeo de la fuente de datos para la recopilación de pruebas. A continuación, Audit Manager realiza llamadas a la API correspondiente Servicios de AWS y recopila una instantánea de los detalles de configuración de sus AWS recursos.

Audit Manager realiza una instantánea de la configuración de cada recurso que esté en el ámbito de una llamada a la API y la convierte en prueba. Esto da como resultado una prueba por recurso, en lugar de una prueba por llamada a la API.

Por ejemplo, si la llamada a la API `ec2_DescribeRouteTables` captura instantáneas de la configuración de cinco tablas de rutas, obtendrá cinco pruebas en total para cada llamada a la API. Cada prueba es una instantánea de la configuración de una tabla de enrutamiento individual.

Temas

- Puntos clave
- Se admiten llamadas a la API para orígenes de datos de control personalizadas
- Llamadas a la API utilizadas en el marco AWS License Manager estándar
- Recursos adicionales

Puntos clave

Llamadas a la API paginadas

Muchos Servicios de AWS recopilan y almacenan una gran cantidad de datos. Como resultado, cuando una llamada a la API `get`, `describe` o `list` intenta devolver sus datos, pueden producirse muchos resultados. Si la cantidad de datos es demasiado grande para devolverla en una sola respuesta, los resultados se pueden dividir en partes más fáciles de gestionar mediante el uso de

la paginación. Esto divide los resultados en «páginas» de datos, lo que facilita el manejo de las respuestas.

Se han paginado algunos de los Se admiten llamadas a la API para orígenes de datos de control personalizadas. Esto significa que al principio devuelven resultados parciales y requieren que las solicitudes posteriores devuelvan todo el conjunto de resultados. Por ejemplo, la DBInstances operación Describe de Amazon RDS devuelve hasta 100 instancias a la vez y se necesitan solicitudes posteriores para devolver la siguiente página de resultados.

Audit Manager admite las llamadas paginadas a la API como origen de datos para la recopilación de pruebas desde el 8 de marzo de 2023. Antes, si se utilizaba una llamada a la API paginada como origen de datos, en la respuesta a la API solo se devolvía un subconjunto de sus recursos (hasta 100 resultados). Ahora, Audit Manager llama a la operación de la API paginada varias veces y obtiene cada página de resultados hasta que se devuelven todos los recursos. A continuación, Audit Manager captura una instantánea de la configuración para cada recurso y la guarda como prueba. Dado que ahora todo el conjunto de recursos se incluye en la respuesta de la API, es probable que observe un aumento en la cantidad de evidencias recopiladas a partir del 8 de marzo de 2023.

Audit Manager gestiona automáticamente la paginación de las llamadas a la API. Si crea un control personalizado que utiliza una llamada a la API paginada como origen de datos, no necesita especificar ningún parámetro de paginación.

Se admiten llamadas a la API para orígenes de datos de control personalizadas

En sus controles personalizados, puede usar cualquiera de las siguientes llamadas a la API como origen de datos. A continuación, Audit Manager puede utilizar estas llamadas a la API para recopilar pruebas sobre su AWS uso.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
acm_ GetAccountConfiguration	Recopila una instantánea de las opciones de configuración de la cuenta asociadas a su Cuenta de AWS.
acm_ ListCertificates	Recupere una lista de nombres de certificados ARNs y dominios.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
escalado_automático DescribeAutoScalingGroups	Recopile una instantánea sobre los grupos de Auto Scaling de su Cuenta de AWS.
copia de seguridad_ ListBackupPlans	Obtenga una lista de todos los planes de respaldo activos de su. Cuenta de AWS
bedrock_ GetModelInvocationLoggingConfiguration	Le permite recopilar una instantánea de los valores de configuración actuales para el registro de invocación de modelos para los modelos de la Cuenta de AWS.
cloudfront_ ListDistributions	Obtenga una lista de todas las distribuciones de su. Cuenta de AWS
cloudtrail_ DescribeTrails	Recopila una instantánea de la configuración de uno o más registros asociados a la región actual de su Cuenta de AWS.
cloudtrail_ ListTrails	Obtenga una lista de los senderos que se encuentran en su. Cuenta de AWS
cloudwatch_ DescribeAlarms	Recopila una instantánea de la configuración de las alarmas que se utilizan en su Cuenta de AWS.
config_ DescribeConfigRules	Recupera detalles sobre tus reglas. AWS Config
config_ DescribeDeliveryChannels	Recopila una instantánea de la configuración de los canales de entrega en su Cuenta de AWS.
directconnect_ DescribeDirectConnectGateways	Recupera una lista de todas tus puertas de enlace. AWS Direct Connect

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
directconnect_ DescribeVirtualGateways	Recupera una lista de las puertas de enlace privadas virtuales que son de su Cuenta de AWS.
docdb_ DescribeCertificates	Recopila una lista de certificados para su Cuenta de AWS.
docDB_Describe DBCluster ParameterGroups	Recopila una lista de descripciones de `DBClusterParameterGroup` para su Cuenta de AWS.
DocDB_Describe DBInstances	Recopila información sobre las instancias de Amazon DynamoDB aprovisionadas para su Cuenta de AWS.
cloudwatch_ DescribeAlarms	Recopile información sobre las alarmas de su. Cuenta de AWS
cloudtrail_ DescribeTrails	Le permite recopilar una instantánea de la configuración de uno o varios registros de seguimiento asociados a la Cuenta de AWS.
dynamodb_ DescribeTable	Recopila instantáneas de configuración para las tablas de DynamoDB de su Cuenta de AWS. Cuando utiliza esta API como origen de datos, no necesita proporcionar el nombre de una tabla de DynamoDB específica. En su lugar, Audit Manager utiliza la operación `ListTables` para enumerar todas las tablas. Para cada tabla que aparece en la lista, Audit Manager realiza la operación `DescribeTable` para generar prueba para ese recurso.
dynamodb_ ListBackups	Recupera una lista de las copias de seguridad de DynamoDB que están asociadas a su Cuenta de AWS.
dynamodb_ ListTables	Recupera una lista de todos los nombres de las tablas que están asociados a su Cuenta de AWS y a su punto de conexión actual.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
ec2_DescribeAddresses	Recopila una instantánea de sus direcciones IP elásticas.
ec2_DescribeCustomerGateways	Recopila una instantánea de las puertas de enlace de cliente de VPN.
ec2_DescribeEgressOnlyInternetGateways	Recopila una instantánea de sus puertas de enlace de Internet de solo salida.
ec2_DescribeFlowLogs	Recopila una instantánea de los registros de flujo.
ec2_DescribeInstances	Recopila una instantánea de sus instancias.
ec2_DescribeInternetGateways	Recopila una instantánea de sus puertas de enlace de Internet.
ec2_DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Recopile una descripción de las asociaciones entre los grupos de interfaces virtuales y las tablas de enrutamiento de las puertas de enlace locales de su. Cuenta de AWS
ec2_DescribeLocalGateways	Recopila una instantánea de sus puertas de enlace locales.
ec2_DescribeLocalGatewayVirtualInterfaces	Recopila una instantánea de las interfaces virtuales de su puerta de enlace local.
ec2_DescribeNatGateways	Recopila una instantánea de sus puertas de enlace NAT.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
ec2_ DescribeNetworkAcls	Recopile una instantánea de su red. ACLs
ec2_ DescribeRouteTables	Recopila una instantánea de sus tablas de enrutamiento.
ec2_ DescribeSecurityGroups	Recopila una instantánea de sus grupos de seguridad.
ec2_ DescribeSecurityGroupRules	Le permite recopilar una instantánea de una o varias reglas de grupos de seguridad.
ec2_ DescribeTransitGateways	Recopila una instantánea de sus puertas de enlace de tránsito.
ec2_ DescribeVolumes	Recopila una instantánea de sus puntos de conexión de VPC.
ec2_ DescribeVpcs	Recopile una instantánea de su. VPCs
ec2_ DescribeVpcEndpoints	Recopila una instantánea de sus puntos de conexión de VPC.
ec2_ DescribeVpcEndpointConnections	Le permite recopilar una instantánea de las conexiones del punto de conexión de VPC a los servicios de punto de conexión de VPC, incluidas las que están pendientes de su aceptación.
ec2_ DescribeVpcEndpointServiceConfigurations	Le permite recopilar una instantánea de las configuraciones de servicio de punto de conexión de VPC de la Cuenta de AWS.
ec2_ DescribeVpcPeeringConnections	Recopila una instantánea de sus conexiones VPN.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
ec2_ DescribeVpnConnections	Recopila una instantánea de sus conexiones VPN.
ec2_ DescribeVpnGateways	Recopila una instantánea de sus puertas de enlace privadas virtuales.
ec2_ GetEbsDefaultKmsKeyId	Recopile una instantánea del cifrado EBS predeterminado AWS KMS key para su Cuenta de AWS región actual.
ec2_ GetEbsEncryptionByDefault	Describa si el cifrado EBS está activado de forma predeterminada Cuenta de AWS en su región actual.
ecs_ DescribeClusters	Recopila una instantánea de los clústeres de ECS.
eks_ DescribeAddonVersions	Recopila una instantánea de las versiones de los complementos.
dolor elástico_ DescribeCacheClusters	Recopila una instantánea de sus clústeres aprovisionados.
dolor elástico_ DescribeServiceUpdates	Recopila una instantánea de las actualizaciones de los servicios de Amazon ElastiCache.
elasticfilesystem_ DescribeAccessPoints	Recopile una instantánea de los puntos de acceso de Amazon EFS en su Cuenta de AWS.
elasticfilesystem_ DescribeFileSystems	Recopila una instantánea de sus sistemas de archivos de Amazon EFS.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
balanceo de carga elástico v2_ DescribeLoadBalancers	Recopile una instantánea de los balanceadores de carga de su. Cuenta de AWS
Elastic LoadBalancing v2_DescribeSSLPolicies	Recopila una instantánea de las políticas que utiliza para la negociación de SSL.
balanceo de carga elástico v2_ DescribeTargetGroups	Recopila una instantánea de sus grupos de destino de ELB.
elasticmapreduce_ ListSecurityConfigurations	Recupera una lista de las configuraciones de seguridad que tiene visibles en su Cuenta de AWS, junto con sus fechas y horas de creación y sus nombres.
eventos_ ListConnections	Recupera una lista de las EventBridge conexiones de Amazon en tu Cuenta de AWS.
eventos_ ListEventBuses	Obtenga una lista de los autobuses de EventBridge eventos de Amazon que tiene en su Cuenta de AWS poder, incluidos el autobús de eventos predeterminado, los autobuses de eventos personalizados y los autobuses de eventos asociados.
eventos_ ListEventSources	Recupera una lista de los orígenes de eventos de socios que se han compartido con su Cuenta de AWS.
eventos_ ListRules	Recupera una lista de tus EventBridge reglas de Amazon.
firehose_ ListDeliveryStreams	Recupera una lista de sus flujos de entrega.
fsx_ DescribeFileSystems	Recopila una instantánea de los sistemas de archivos que le pertenecen a su Cuenta de AWS.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
guardiana_ ListDetectors	Obtenga una lista de los recursos `detectorIds` de su GuardDuty detector de Amazon.
iam_ GenerateC redentialReport	Genera un informe de credencial para su Cuenta de AWS.
iam_ GetAccoun tPasswordPolicy	Recopila una instantánea de la política de contraseñas de su Cuenta de AWS.
iam_ GetAccoun tSummary	Recopila una instantánea del uso de entidades de IAM y cuotas de IAM en su Cuenta de AWS.
iam_ ListGroups	Obtenga una lista de los grupos de IAM que están asociados a un prefijo de ruta que esté disponible en su. Cuenta de AWS
proveedores iam_ ListOpen IDConnect	Recupera una lista de los objetos del recurso del proveedor OpenID Connect (OIDC) de IAM que están definidos en su Cuenta de AWS.
iam_ ListPolicies	Recupera una lista de todas las políticas administradas que están disponibl es en su Cuenta de AWS, incluidas las políticas administradas definidas por su propio cliente y todas las políticas administradas por AWS.
iam_ ListRoles	Obtenga una lista de las funciones de IAM asociadas a un prefijo de ruta que esté disponible en su. Cuenta de AWS
IAM_List SAMLProviders	Recupera una lista de los objetos del recurso del proveedor SAML que están definidos en IAM en su Cuenta de AWS.
iam_ ListUsers	Recupere una lista de los usuarios de IAM de su. Cuenta de AWS
iam_ ListVirtual MFADevices	Recupera una lista de los dispositivos MFA virtuales que están definidos en su Cuenta de AWS.
kafka_ ListClusters	Obtenga una lista de los clústeres de Amazon MSK en su Cuenta de AWS.
kafka_ ListKafka Versions	Recupera una lista de los objetos de la versión de Apache Kafka en su Cuenta de AWS.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
kinesis_ ListStreams	Recupera una lista de sus flujos de datos de Kinesis.
kms_ GetKeyPolicy	Audit Manager utiliza esta API para recopilar una instantánea de las políticas de claves para AWS KMS keys en su Cuenta de AWS. Cuando utilizas esta API como fuente de datos, no necesitas proporcionar el nombre de una específica. AWS KMS key En su lugar, Audit Manager utiliza la operación `ListKeys` para enumerar todas las claves de KMS. Por cada clave de KMS que aparece en la lista, Audit Manager realiza la operación `GetKeyPolicy` con el fin de generar prueba para ese recurso.
kms_ GetKeyRotationStatus	Audit Manager utiliza esta API para recopilar una instantánea de si la rotación automática está AWS KMS keys habilitada para su Cuenta de AWS. Cuando utilizas esta API como fuente de datos, no necesitas proporcionar el nombre de una específica AWS KMS key. En su lugar, Audit Manager utiliza la operación `ListKeys` para enumerar todas las claves de KMS. Por cada clave de KMS que aparece en la lista, Audit Manager realiza la operación `GetKeyRotationStatus` con el fin de generar prueba para ese recurso.
kms_ ListKeys	Recupere una lista de los que están AWS KMS keys en su. Cuenta de AWS
lambda_ ListFunctions	Obtenga una lista de las funciones de Lambda que tenga Cuenta de AWS, con la configuración específica de cada versión de cada una.
RDS_DescribeDBClusters	Recopile una instantánea de los clústeres de base de datos Amazon Aurora y los clústeres de base de datos Multi-AZ existentes en su Cuenta de AWS.
RDS_DescribeDBInstances	Recopila una instantánea de las instancias de RDS aprovisionadas en su Cuenta de AWS.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
rds_ DescribeDbInstanceAutomatedBackups	Le permite recopilar una instantánea de las copias de seguridad de las instancias actuales y eliminadas de la Cuenta de AWS.
rds_ DescribeDbSecurityGroups	Recopile una instantánea de los DBSecurity grupos de su. Cuenta de AWS
redshift_ DescribeClusters	Recopila una instantánea de los clústeres de Amazon Redshift aprovisionados en su Cuenta de AWS.
s3_ GetBucketEncryption	Recopila una instantánea que muestra la configuración de cifrado predeterminada para sus buckets de S3. Cuando utiliza esta API como origen de datos, no necesita proporcionar el nombre de un bucket de S3 específico. En su lugar, Audit Manager utiliza la `ListBuckets` operación para enumerar los depósitos que se crearon en la Región de AWS misma evaluación. Por cada bucket que aparece en la lista, Audit Manager realiza la operación `GetBucketEncryption` con el fin de generar una prueba para ese recurso. Audit Manager solo puede proporcionar el estado de cifrado de los buckets que se crearon al mismo tiempo Región de AWS que su evaluación. Si necesita ver el estado de cifrado de todos sus depósitos de S3 en varios Regiones de AWS, le recomendamos que cree una evaluación en cada uno de los depósitos de S3 en los Región de AWS que tenga un depósito de S3.
s3_ ListBuckets	Obtenga una lista de los depósitos S3 de su. Cuenta de AWS Audit Manager solo puede enumerar los buckets que se crearon al mismo tiempo Región de AWS que su evaluación. Si necesita ver todos sus depósitos de S3 en varios Región de AWS grupos, le recomendamos que cree una evaluación en cada uno de ellos en los Región de AWS que tenga un depósito de S3.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
sagemaker_ ListAlgorithms	Le permite recuperar una lista de los algoritmos de machine learning de la Cuenta de AWS.
sagemaker_ ListDomains	Obtenga una lista de los dominios de su. Cuenta de AWS
sagemaker_ ListEndpoints	Obtenga una lista de los puntos finales de su. Cuenta de AWS
sagemaker_ ListEndpointConfigs	Obtenga una lista de las configuraciones de puntos finales de su. Cuenta de AWS
sagemaker_ ListFlowDefinitions	Obtenga una lista de las definiciones de flujo de su. Cuenta de AWS
sagemaker_ ListHumanTaskUis	Obtenga una lista de las interfaces de tareas humanas de su. Cuenta de AWS
sagemaker_ ListLabelingJobs	Obtenga una lista de los trabajos de etiquetado de su. Cuenta de AWS
sagemaker_ ListModels	Obtenga una lista de los modelos de su. Cuenta de AWS
sagemaker _ ListModel BiasJobDefinitions	Le permite recuperar una lista de las definiciones de trabajo de sesgo del modelo de la Cuenta de AWS.
sagemaker_ ListModelCards	Obtenga una lista de las tarjetas modelo que tiene en su. Cuenta de AWS
sagemaker_ ListModelQualityJo bDefinitions	Le permite recuperar una lista de las definiciones de trabajo de supervisión de calidad del modelo de la Cuenta de AWS.

Llamada a la API compatible	Cómo Audit Manager utiliza esta API para recopilar pruebas
sagemaker_ ListMonitoringAlerts	Le permite recuperar una lista de las alertas de un determinado programa de supervisión.
sagemaker_ ListMonitoringSche dules	Obtenga una lista de todos los programas de monitoreo de su. Cuenta de AWS
sagemaker_ ListTrainingJobs	Obtenga una lista de trabajos de formación en su. Cuenta de AWS
sagemaker_ ListUserProfiles	Le permite recuperar una lista de perfiles de usuario de la Cuenta de AWS.
administrador de secretos_ ListSecre ts	Recupera una lista de los secretos que están guardados en tu cuenta Cuenta de AWS, sin incluir los secretos que están marcados para su eliminación.
sns_ ListTopics	Obtenga una lista de los temas de SNS en su. Cuenta de AWS
sqs_ ListQueues	Obtenga una lista de las colas de SQS de su. Cuenta de AWS
guerra-regional_ ListWebAcls	Recupere una lista de los objetos web para su. ACLSummary Cuenta de AWS
guerra-regional_ ListRules	Recupera una lista de los objetos para tu. RuleSummary Cuenta de AWS
waf_ ListRuleG roups	Recupera una lista de los RuleGroupSummaryobjetos de los grupos de reglas de tu. Cuenta de AWS
waf_ ListRules	Recupera una lista de los RuleSummaryobjetos para tu. Cuenta de AWS
waf_ ListWebAcls	Recupere una lista de los ACLSummary objetos web para su. Cuenta de AWS

Llamadas a la API utilizadas en el marco AWS License Manager estándar

Audit Manager utiliza una actividad personalizada llamada `GetLicenseManagerSummary` para recopilar pruebas en el marco estándar AWS License Manager. Esta actividad llama a los tres License Manager siguientes APIs:

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

Los datos que se devuelven se convierten luego en pruebas y se adjuntan a los controles pertinentes de la evaluación.

Ejemplo

Supongamos que utiliza dos productos con licencia (SQL Service 2017 y Oracle Database Enterprise Edition). En primer lugar, la `GetLicenseManagerSummary` actividad llama a la ListLicenseConfigurationsAPI, que proporciona detalles de las configuraciones de licencia de su cuenta. A continuación, añade datos contextuales adicionales para cada configuración de licencia. Para ello, llama a ListUsageForLicenseConfigurationy ListAssociationsForLicenseConfiguration. Por último, convierte los datos de configuración de la licencia en pruebas y los adjunta a los controles respectivos del marco (4.5: licencia gestionada por el cliente para SQL Server 2017 y 3.0.4: licencia gestionada por el cliente para Oracle Database Enterprise Edition).

Si utiliza un producto con licencia que no está cubierto por ninguno de los controles del marco, los datos de configuración de la licencia se adjuntan como evidencia del siguiente control: 5.0: Licencia gestionada por el cliente para otras licencias.

Recursos adicionales

- Para obtener ayuda con problemas relacionados con recopilación de evidencias para este tipo de origen de datos, consulte Mi evaluación no consiste en recopilar evidencia de datos de configuración para una llamada a la AWS API.
- Para crear un control personalizado con este tipo de origen de datos, consulte Crear un control personalizado en AWS Audit Manager.
- Para crear un marco personalizado que utilice el control personalizado, consulte Crear un marco personalizado en AWS Audit Manager.

- Para añadir el control personalizado a un marco personalizado existente, consulte Edición de un marco personalizado en AWS Audit Manager.

AWS CloudTrail nombres de eventos compatibles con AWS Audit Manager

Puede utilizar Audit Manager para capturar los eventos AWS CloudTrail de administración y los eventos de servicio global como evidencia para las auditorías. Al crear o editar un control personalizado, puede especificar uno o más nombres de CloudTrail eventos como mapeo de fuentes de datos para la recopilación de pruebas. A continuación, Audit Manager filtra los CloudTrail registros en función de las palabras clave elegidas e importa los resultados como evidencia de la actividad del usuario.

> **Note**
>
> Audit Manager captura eventos de administración y servicio global solamente. Los eventos de datos y los eventos de información no están disponibles como prueba. Para obtener más información sobre los distintos tipos de CloudTrail eventos, consulte CloudTrail los conceptos en la Guía del AWS CloudTrail usuario.

Como excepción a lo anterior, Audit Manager no admite los siguientes CloudTrail eventos:

- kms_ GenerateDataKey
- kms_Decrypt
- sts_ AssumeRole
- kinesisvideo_ GetDataEndpoint
- kinesisvideo_ GetSignalingChannelEndpoint
- kinesisvideo_ DescribeSignalingChannel
- kinesisvideo_ DescribeStream

A partir del 11 de mayo de 2023, Audit Manager ya no admite CloudTrail eventos de solo lectura como palabras clave para la recopilación de pruebas. Eliminamos un total de 3135 palabras clave de solo lectura. Como los clientes y Servicios de AWS ambos hacen llamadas de lectura APIs, los

eventos de solo lectura son ruidosos. Como resultado, las palabras clave de solo lectura recopilan una gran cantidad de pruebas que no son fiables ni relevantes para las auditorías. Las palabras clave de solo lectura incluyen `ListDescribe`, y las llamadas a la `Get` API (por ejemplo, GetObjecty ListBucketspara Amazon S3). Si utilizó una de estas palabras clave para la recopilación de pruebas, no tiene que realizar ninguna acción. Las palabras clave se eliminaron automáticamente de la consola de Audit Manager y de sus evaluaciones, y ya no se recopilan pruebas de estas palabras clave.

Recursos adicionales

- Para obtener ayuda con problemas relacionados con recopilación de evidencias para este tipo de origen de datos, consulte Mi evaluación no consiste en recopilar pruebas de la actividad de los usuarios de AWS CloudTrail.
- Para crear un control personalizado con este tipo de origen de datos, consulte Crear un control personalizado en AWS Audit Manager.
- Para crear un marco personalizado que utilice el control personalizado, consulte Crear un marco personalizado en AWS Audit Manager.
- Para añadir el control personalizado a un marco personalizado existente, consulte Edición de un marco personalizado en AWS Audit Manager.

Configuración AWS Audit Manager con los ajustes recomendados

Antes de empezar a utilizar Audit Manager, es importante que haya completado las siguientes tareas de configuración.

En este capítulo se explican los requisitos previos, la configuración de la cuenta, los permisos de usuario y los pasos necesarios para habilitar y configurar Audit Manager con las características e integraciones recomendadas. Tras completar estas tareas, ya podrá utilizar Audit Manager y empezar a optimizar sus esfuerzos de auditoría y conformidad.

Contenido

- Requisitos previos para la configuración AWS Audit Manager
  - Inscríbase en una Cuenta de AWS
  - Creación de un usuario con acceso administrativo
  - Añada los permisos mínimos necesarios para acceder a Audit Manager y habilitarlo
  - Pasos a seguir a continuación
- Habilitar AWS Audit Manager
  - Requisitos previos
  - Procedimiento
  - Pasos a seguir a continuación
- Habilitar las funciones recomendadas y Servicios de AWS para AWS Audit Manager
  - Puntos clave
  - Configuración de las características recomendadas de Audit Manager
  - Configura las integraciones recomendadas con otras Servicios de AWS
  - Pasos a seguir a continuación

Requisitos previos para la configuración AWS Audit Manager

Antes de poder AWS Audit Manager utilizarlos, debe asegurarse de haber configurado correctamente sus permisos Cuenta de AWS y los de usuario.

En esta página se describen los pasos necesarios para crear un usuario administrativo Cuenta de AWS (si es necesario), configurar un usuario administrativo y conceder los permisos necesarios para acceder a Audit Manager y activarlo.

Tareas

1. Inscríbase en una Cuenta de AWS
2. Creación de un usuario con acceso administrativo
3. Añada los permisos mínimos necesarios para acceder a Audit Manager y habilitarlo

> **Important**
>
> Si ya tiene una configuración de IAM, puede omitir las tareas 1 y 2. AWS Sin embargo, debe realizar la tarea 3 para asegurarse de que dispone de los permisos necesarios para configurar Audit Manager.

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Añada los permisos mínimos necesarios para acceder a Audit Manager y habilitarlo

Debe conceder a los usuarios los permisos necesarios para habilitar Audit Manager.
Para los usuarios que necesitan acceso completo a Audit Manager, usen la política AWSAuditManagerAdministratorAccessgestionada. Se trata de una política AWS gestionada que está disponible en su Cuenta de AWS cuenta y es la política recomendada para los administradores de Audit Manager.

> **Tip**
>
> Como práctica recomendada de seguridad, le recomendamos que comience con las políticas AWS administradas y, después, opte por los permisos con privilegios mínimos. AWS las políticas administradas otorgan permisos para muchos casos de uso comunes. Sin embargo, tenga en cuenta que, dado que las políticas AWS administradas están disponibles para que las usen todos los AWS clientes, es posible que no otorguen permisos con privilegios mínimos para sus casos de uso específicos. En consecuencia, se recomienda reducir aún más los permisos definiendo políticas administradas por el cliente específicas para sus casos de uso. Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de AWS Identity and Access Management .

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en: AWS IAM Identity Center

Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .

- Usuarios gestionados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Pasos a seguir a continuación

Ahora que ha configurado Cuenta de AWS y concedido los permisos necesarios, está listo para activar Audit Manager. Para step-by-step obtener instrucciones, consulteHabilitar AWS Audit Manager.

Habilitar AWS Audit Manager

Ahora que ha completado los requisitos previos para configurar Audit Manager, puede habilitar el servicio en su AWS entorno.

En esta página descubrirá cómo habilitar Audit Manager mediante la consola de Audit Manager, AWS Command Line Interface (AWS CLI) o la API de Audit Manager. Elija el método que mejor se adapte a sus necesidades y siga los pasos correspondientes para poner en marcha Audit Manager.

Requisitos previos

Asegúrese de haber completado todas las tareas que se describen en Requisitos previos para la configuración AWS Audit Manager.

Procedimiento

Puede habilitar Audit Manager mediante la AWS Management Console API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Habilitación del acceso de confianza mediante la consola Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. Utilice las credenciales de su identidad de IAM para iniciar sesión.
3. Elija Set up (Configurar) AWS Audit Manager.

4. En Permisos, no es necesario realizar ninguna acción. Audit Manager utiliza un rol vinculado a servicio para conectarse a los orígenes de datos en su nombre. Para revisar el rol vinculado al servicio, seleccione Ver el permiso del rol vinculado al servicio de IAM.

5. En Cifrado de datos, la opción predeterminada es que Audit Manager cree y gestione y almacene los datos de forma segura. AWS KMS key

Si desea utilizar su propia clave administrada por el cliente para cifrar los datos en Audit Manager, marque la casilla de verificación situada junto a Personalizar la configuración de cifrado (avanzada). Puede elegir un par de claves KMS existente o crear una nueva.

6. (Opcional) En Administrador delegado: opcional, puede especificar una cuenta de administrador delegado si desea que Audit Manager ejecute evaluaciones para varias cuentas. Para obtener más información y recomendaciones, consulte Habilitar y configurar AWS Organizations.

7. (Opcional) En AWS Config : opcional, le recomendamos que la active AWS Config para disfrutar de una experiencia óptima. Esto permite a Audit Manager generar evidencias mediante reglas de AWS Config . Para obtener instrucciones y los ajustes recomendados, consulte Habilite y configure AWS Config.

8. (Opcional) Security Hub: le recomendamos que habilite Security Hub para disfrutar de una experiencia óptima. Esto permite a Audit Manager generar evidencias mediante comprobaciones de Security Hub. Para obtener instrucciones y los ajustes recomendados, consulte Habilitar y configurar AWS Security Hub.

9. Seleccione Completar configuración para finalizar el proceso de configuración.

AWS CLI

Para habilitar Audit Manager mediante AWS CLI

En la línea de comandos, ejecute el comando register-account con los siguientes parámetros de configuración:

- `--kms-key` (opcional): utilice este parámetro para cifrar sus datos de Audit Manager con su propia clave administrada por el cliente. Si no especifica ninguna opción aquí, Audit Manager creará y administrará una AWS KMS key en su nombre para el almacenamiento seguro de sus datos.
- `--delegated-admin-account` (opcional): utilice este parámetro para designar la cuenta de administrador delegado de su organización para Audit Manager. Si no especifica ninguna opción aquí, no se registrará ningún administrador delegado.

Ejemplo de entrada (sustitúyalo por su propia información): *placeholder text*

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

Ejemplo de resultados:

```
{
    "status": "ACTIVE"
}
```

Para obtener más información AWS CLI e instrucciones sobre cómo instalarlas AWS CLI , consulte lo siguiente en la Guía del AWS Command Line Interface usuario.

- Guía del usuario de la interfaz de la línea de comandos de AWS
- Cómo realizar la configuración con el AWS Command Line Interface

Audit Manager API

Habilitación de Audit Manager mediante la API de Audit Manager

Utilice la RegisterAccountoperación con los siguientes parámetros de configuración:

- kmsKey (opcional): utilice este parámetro para cifrar sus datos de Audit Manager con su propia clave administrada por el cliente. Si no especifica ninguna opción aquí, Audit Manager creará y administrará una AWS KMS key en su nombre para el almacenamiento seguro de sus datos.
- delegatedAdminAccount(opcional): utilice este parámetro para especificar la cuenta de administrador delegado de su organización para Audit Manager. Si no especifica ninguna, no se registrará ningún administrador delegado.

Introduzca un ejemplo (*placeholder text*sustitúyalo por su propia información):

```
{
    "kmsKey":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "delegatedAdminAccount":"111122224444"
```

```
}
```

Ejemplo de resultados:

```
{
  "status": "ACTIVE"
}
```

Pasos a seguir a continuación

Tras habilitar Audit Manager, le recomendamos configurar algunas de las características e integraciones recomendadas para disfrutar de una experiencia óptima. Para obtener más información, consulte Habilitar las funciones recomendadas y Servicios de AWS para AWS Audit Manager.

Habilitar las funciones recomendadas y Servicios de AWS para AWS Audit Manager

Ahora que lo ha activado AWS Audit Manager, es el momento de configurar las funciones e integraciones recomendadas para aprovechar al máximo el servicio.

Puntos clave

Para disfrutar al máximo de las prestaciones de Audit Manager, le recomendamos configurar las siguientes características y habilitar los siguientes Servicios de AWS.

Tareas

- Configuración de las características recomendadas de Audit Manager
- Configura las integraciones recomendadas con otras Servicios de AWS
  - Habilite y configure AWS Config
  - Habilitar y configurar AWS Security Hub
  - Habilitar y configurar AWS Organizations

Configuración de las características recomendadas de Audit Manager

Tras habilitar Audit Manager, le recomendamos que habilite la característica de búsqueda de evidencias.

Buscador de evidencias proporciona una forma eficaz de buscar evidencias en Audit Manager. En lugar de explorar exhaustivamente carpetas de evidencias para encontrar lo que busca, puede utilizar el buscador de evidencias para consultarlas rápidamente. Si utiliza el buscador de evidencias como administrador delegado, puede buscar evidencias en todas las cuentas de miembros de su organización.

Mediante una combinación de filtros y agrupaciones, puede reducir progresivamente el alcance de su consulta de búsqueda. Por ejemplo, si desea obtener una visión general del estado de su sistema, realice una búsqueda amplia y filtre por evaluación, intervalo de fechas y conformidad de los recursos. Si su objetivo es corregir un recurso específico, puede realizar una búsqueda restringida para encontrar evidencias que apunten a un identificador de control o recurso específico. Tras definir los filtros, puede agrupar y, a continuación, obtener una vista previa de los resultados de búsqueda coincidentes antes de crear un informe de evaluación.

Configura las integraciones recomendadas con otras Servicios de AWS

Para una experiencia óptima en Audit Manager, le recomendamos encarecidamente que habilite lo siguiente Servicios de AWS:

- AWS Organizations: puede utilizar Organizaciones para ejecutar las evaluaciones de Audit Manager en varias cuentas y consolidar las evidencias en una cuenta de administrador delegado.
- AWS Security Huby AWS Config— Audit Manager se basa en ellas Servicios de AWS como fuentes de datos para la recopilación de pruebas. Al activar AWS Config Security Hub, Audit Manager puede funcionar con todas sus funciones, recopilando pruebas exhaustivas e informando con precisión de los resultados de las comprobaciones de conformidad directamente desde estos servicios.

> **Important**
>
> Si no habilita ni configura AWS Config un Security Hub, no podrá recopilar las pruebas previstas para muchos controles en sus evaluaciones de Audit Manager. Como resultado, corre el riesgo de que la recopilación de evidencias de determinados controles no se complete o se produzca un error en ella. Más concretamente:

- Si Audit Manager intenta utilizarlos AWS Config como fuente de datos de control, pero las AWS Config reglas requeridas no están habilitadas, no se recopilará ninguna evidencia de esos controles.
- Del mismo modo, si Audit Manager intenta utilizar Security Hub como origen de datos de control, pero los estándares necesarios no están habilitados en Security Hub, no se recopilará ninguna evidencia para esos controles.

Para mitigar estos riesgos y garantizar una recopilación exhaustiva de pruebas, siga los pasos de esta página para habilitar AWS Config y configurar el Security Hub antes de crear sus evaluaciones de Audit Manager.

Habilite y configure AWS Config

Muchos controles de Audit Manager requieren AWS Config un tipo de fuente de datos. Para admitir estos controles, debe activarlos AWS Config en todas las cuentas en las Región de AWS que Audit Manager esté activado.

Audit Manager no se las AWS Config arregla para usted. Puede seguir estos pasos para habilitar AWS Config y configurar sus ajustes.

> **Important**
>
> AWS Config La activación es una recomendación opcional. Sin embargo, si habilita AWS Config, se requieren los siguientes ajustes. Si Audit Manager intenta recopilar pruebas para los controles que se utilizan AWS Config como tipo de fuente de datos y no AWS Config está configurado como se describe a continuación, no se recopilará ninguna evidencia para esos controles.

Tareas para integrar AWS Config con Audit Manager

- Paso 1: Habilitar AWS Config
- Paso 2: Configure los AWS Config ajustes para utilizarlos con Audit Manager

Paso 1: Habilitar AWS Config

Puede habilitarlo AWS Config mediante la AWS Config consola o la API. Para obtener instrucciones, consulte Introducción a AWS Config en la Guía para desarrolladores de AWS Config .

Paso 2: Configure los AWS Config ajustes para utilizarlos con Audit Manager

Después de habilitarlo AWS Config, asegúrese de habilitar también AWS Config las reglas o implementar un paquete de conformidad para el estándar de cumplimiento relacionado con su auditoría. Este paso garantiza que Audit Manager pueda importar los resultados de las reglas de AWS Config que haya habilitado.

Tras activar una AWS Config regla, le recomendamos que revise sus parámetros. A continuación, debe validar dichos parámetros con respecto a los requisitos del marco de conformidad que haya elegido. Si es necesario, puede actualizar los parámetros de una regla en AWS Config para asegurarse de que se ajusta a los requisitos del marco. Esto ayudará a garantizar que sus evaluaciones recopilen las evidencias de control de conformidad correctas para un marco determinado.

Supongamos, por ejemplo, que está creando una evaluación para CIS v1.2.0. Este marco tiene un control denominado 1.4: asegúrese de que las claves de acceso se roten cada 90 días o menos. En AWS Config, la access-keys-rotatedregla tiene un `maxAccessKeyAge` parámetro con un valor predeterminado de 90 días. Por lo tanto, la regla concuerda con los requisitos de control establecidos. Si no utiliza el valor predeterminado, asegúrese de que sea igual o superior al requisito de 90 días establecido en la versión 1.2.0 del CIS.

Puede encontrar los datos relativos a los parámetros predeterminados de cada regla administrada en la AWS Config documentación. Para obtener instrucciones sobre cómo configurar una regla, consulte Trabajar con reglas AWS Config administradas.

Habilitar y configurar AWS Security Hub

Muchos controles de Audit Manager requieren Security Hub como tipo de origen de datos. Para permitir estos controles, debe habilitar Security Hub en todas las cuentas de cada región en la que Audit Manager esté habilitado.

Audit Manager no administra Security Hub por usted. Puede seguir estos pasos para habilitar Security Hub y configurar sus ajustes.

> **Important**
>
> Habilitar el Security Hub es una recomendación opcional. Sin embargo, si habilita Security Hub, deberá realizar los siguientes ajustes. Si Audit Manager intenta recopilar evidencias para los controles que utilizan Security Hub como tipo de origen de datos, y Security Hub no está configurado según lo descrito a continuación, no se recopilará ninguna evidencia para esos controles.

Tareas para integrar AWS Security Hub con Audit Manager

- Paso 1: Habilitar AWS Security Hub
- Paso 2: configure sus ajustes de Security Hub para utilizarlos con Audit Manager
- Paso 3: establecer la configuración Organizaciones para su organización

Paso 1: Habilitar AWS Security Hub

Puede habilitar Security Hub mediante la consola o la API. Para conocer las instrucciones, consulte Configuración de AWS Security Hub en la Guía del usuario de AWS Security Hub .

Paso 2: configure sus ajustes de Security Hub para utilizarlos con Audit Manager

Después de habilitar Security Hub, asegúrese de hacer lo siguiente:

- Habilitar AWS Config y configurar el registro de recursos: Security Hub utiliza AWS Config reglas vinculadas a servicios para realizar la mayoría de las comprobaciones de seguridad de los controles. Para admitir estos controles, AWS Config debe estar habilitado y configurado para registrar los recursos necesarios para los controles que ha habilitado en cada estándar habilitado.
- Habilitar todos los estándares de seguridad: este paso garantiza que Audit Manager pueda importar los resultados de todos los estándares de conformidad compatibles.
- Habilitar la configuración de resultados de control consolidados en Security Hub: esta configuración está activada de forma predeterminada si habilitó el Centro de seguridad a partir del 23 de febrero de 2023.

> **Note**
>
> Cuando habilita los resultados consolidados, Security Hub genera un único resultado para cada control de seguridad (incluso cuando se utiliza el mismo control en varios

estándares). Cada resultado de Security Hub se recopila como una evaluación de recursos única en Audit Manager. En consecuencia, los resultados consolidados revelan una disminución del total de evaluaciones de recursos únicos que Audit Manager realiza para los resultados de Security Hub. Por esta razón, el uso de resultados consolidados a menudo puede resultar en una reducción de los costos de uso de Audit Manager. Para obtener más información sobre el uso de Security Hub como tipo de origen de datos, consulte AWS Security Hub controles compatibles con AWS Audit Manager. Para obtener más información acerca de los precios, consulte Precios de AWS Audit Manager.

Paso 3: establecer la configuración Organizaciones para su organización

Si utilizas AWS Organizations y quieres recopilar pruebas del Security Hub de tus cuentas de miembros, también debes realizar los siguientes pasos en Security Hub.

Para configurar los ajustes de Security Hub de su organización

1. Inicie sesión en AWS Management Console y abra la AWS Security Hub consola en https://console.aws.amazon.com/securityhub/.
2. Con su cuenta AWS Organizations de administración, designe una cuenta como administrador delegado de Security Hub. Para obtener información, consulte Designación de una cuenta de administrador de Security Hub en la Guía del usuario de AWS Security Hub .

   > **Note**
   >
   > Asegúrese de que la cuenta de administrador delegado que designe en Security Hub sea la misma que utiliza en Audit Manager.

3. Con su cuenta de administrador delegado de organizaciones, vaya a Configuración, Cuentas, seleccione todas las cuentas y, a continuación, agréguelas como miembros seleccionando Inscripción automática. Para obtener más información, consulte Habilitar una cuenta miembro de la organización en la Guía del usuario de AWS Security Hub .
4. AWS Config Actívela para cada cuenta de miembro de la organización. Para obtener más información, consulte Habilitar una cuenta miembro de la organización en la Guía del usuario de AWS Security Hub .
5. Active el estándar de seguridad PCI DSS para cada cuenta miembro de la organización. El estándar AWS CIS Foundations Benchmark y el estándar AWS Foundational Best Practices ya

están activados de forma predeterminada. Para obtener más información sobre este estándar, consulte Habilitar el estándar de seguridad en la Guía del usuario de AWS Security Hub .

Habilitar y configurar AWS Organizations

Audit Manager admite varias cuentas mediante la integración con AWS Organizations. Audit Manager puede ejecutar las evaluaciones en varias cuentas y consolidar las evidencias en una cuenta de administrador delegado. El administrador delegado tiene permisos para crear y administrar recursos de Audit Manager con la organización como zona de confianza. Solo la cuenta de administración puede agregar un administrador delegado.

> **Important**
>
> AWS Organizations La activación es una recomendación opcional. Sin embargo, si lo habilita AWS Organizations, se requieren los siguientes ajustes.

Tareas para integrar AWS Organizations con Audit Manager

- Paso 1: crear o unirse a una organización
- Paso 2: Habilitar todas las características en la organización.
- Paso 3: especificar un administrador delegado para Audit Manager

Paso 1: crear o unirse a una organización

Si Cuenta de AWS no forma parte de una organización, puede crearla o unirse a ella. Para obtener instrucciones sobre cómo hacerlo, consulte Creación y administración de una organización en la Guía del usuario de AWS Organizations .

Paso 2: Habilitar todas las características en la organización.

A continuación, debe habilitar todas las características en la organización. Para obtener más información, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations .

Paso 3: especificar un administrador delegado para Audit Manager

Le recomendamos que habilite Audit Manager mediante una cuenta de administración de organizaciones y, a continuación, especifique un administrador delegado. Después, puede usar la

cuenta de administrador delegado para iniciar sesión y ejecutar las evaluaciones. Como práctica recomendada, aconsejamos que cree evaluaciones únicamente con la cuenta de administrador delegado en lugar de la cuenta de administración.

Para añadir o cambiar un administrador delegado después de habilitar Audit Manager, consulte Adición de un administrador delegado y Cambio de un administrador delegado.

Pasos a seguir a continuación

Ahora que ha configurado Audit Manager con los ajustes recomendados, ya puede empezar a utilizar el servicio.

- Para comenzar con su primera evaluación, consulte Tutorial para propietarios de auditorías: crear una evaluación.
- Para actualizar la configuración en el futuro, consulte Revisar y configurar sus AWS Audit Manager ajustes.

Empezar con AWS Audit Manager

Utilice los step-by-step tutoriales de esta sección para aprender a realizar tareas con AWS Audit Manager.

> **Tip**
>
> Los siguientes tutoriales están clasificados por audiencia. Elija el tutorial adecuado para usted dependiendo de su función como propietario de la auditoría o delegado.
>
> - Los propietarios de las auditorías son usuarios de Audit Manager responsables de crear y gestionar las evaluaciones. En el mundo empresarial, los responsables de las auditorías suelen ser profesionales del gobierno, la gestión de riesgos y el cumplimiento (GRC). Sin embargo, en el contexto de Audit Manager, las personas SecOps o DevOps los equipos también pueden asumir la personalidad de usuario del propietario de una auditoría.
> Los responsables de la auditoría pueden solicitar la ayuda de un experto en la materia (también denominado delegado) para revisar controles específicos y validar las pruebas. Los propietarios de la auditoría deben tener los permisos necesarios para gestionar una evaluación.
> - Los delegados son expertos en la materia con experiencia técnica o empresarial especializada. Aunque no son propietarios ni gestionan las evaluaciones de Audit Manager, pueden contribuir a ellas. Los delegados ayudan a los responsables de las auditorías en tareas como la validación de las pruebas para los controles que entran dentro de su área de especialización. Los delegados tienen permisos limitados en Audit Manager. Esto se debe a que los propietarios de las auditorías delegan la revisión de conjuntos de control específicos y no de las evaluaciones completas.
>
> Para obtener más información sobre estas personas y otros conceptos de Audit Manager, consulte audit owner y delegate en la sección Comprensión de AWS Audit Manager los conceptos y la terminología de esta guía.
> Para obtener más información sobre los permisos de IAM recomendados para cada persona, consulte Políticas recomendadas para los usuarios de AWS Audit Manager.

Tutoriales de Audit Manager

Creación de una evaluación

Público: propietarios de auditorías

Descripción general: siga step-by-step las instrucciones para crear su primera evaluación y empiece a utilizarla rápidamente. Este tutorial explica cómo utilizar un marco estándar para crear una evaluación y comenzar la recopilación automatizada de evidencias.

Revisión de un conjunto de controles

Público: delegados

Descripción general: ayude al propietario de una auditoría revisando las pruebas para detectar los controles que entran dentro de su área de especialización. Aprenda a revisar los conjuntos de controles y sus evidencias relacionadas, añada comentarios, cargue evidencias y actualice el estado de un control.

Tutorial para propietarios de auditorías: crear una evaluación

Este tutorial proporciona una introducción a AWS Audit Manager. En este tutorial creará una evaluación con el AWS Audit Manager Ejemplo de marco. Al crear una evaluación, se inicia el proceso continuo de recopilación automática de pruebas para los controles de ese marco.

> **Note**
>
> AWS Audit Manager ayuda a recopilar pruebas que sean relevantes para verificar el cumplimiento de marcos y reglamentos de cumplimiento específicos. Sin embargo, no evalúa el cumplimiento en sí mismo. AWS Audit Manager Por lo tanto, es posible que las pruebas recopiladas no incluyan toda la información sobre su AWS uso que se necesita para las auditorías. AWS Audit Manager no sustituye a los asesores legales ni a los expertos en cumplimiento.

Requisitos previos

Antes de comenzar este tutorial, asegúrese de cumplir las siguientes condiciones:

- Ha completado todos los requisitos previos que se describen en Configuración AWS Audit Manager con los ajustes recomendados. Debe usar su AWS Audit Manager consola Cuenta de AWS y la suya para completar este tutorial.
- Su identidad de IAM cuenta con los permisos adecuados para crear y gestionar una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: Permitir a los usuarios acceso de administrador total a AWS Audit Manager y Permita que la administración de los usuarios acceda a AWS Audit Manager.
- Está familiarizado con la terminología y la funcionalidad de Audit Manager. Para obtener información general acerca, consulte¿Qué es AWS Audit Manager? y Comprensión de AWS Audit Manager los conceptos y la terminología.

Procedimiento

Tareas

- Paso 1: especificar los detalles de la evaluación
- Paso 2: especifique Cuentas de AWS el alcance
- Paso 3: especificar los responsables de la auditoría
- Paso 4: Revisar y crear

Paso 1: especificar los detalles de la evaluación

Como primer paso, seleccione un marco y proporcione información básica para la evaluación.

Pasos para especificar los detalles de la evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. Elija Iniciar AWS Audit Manager.
3. En el banner verde de la parte superior de la pantalla, elija Comenzar con un marco.
4. Elija el marco que desee y, a continuación, elija Crear evaluación a partir del marco. Para este tutorial, utilice la opción Marco de prueba de AWS Audit Manager .
5. En Nombre de la evaluación, escriba un nombre para su evaluación.

6. (Opcional) En Descripción de la evaluación, escriba una descripción para su evaluación.
7. En Destino de los informes de evaluación, elija el bucket de S3 en el que desee guardar los informes de evaluación.
8. En Marcos, confirme que ha seleccionado la opción Marco de prueba de AWS Audit Manager .
9. (Opcional) En Etiquetas, elija Añadir nueva etiqueta para asociar una etiqueta a la evaluación. Puede especificar una clave y un valor para cada etiqueta. La clave de etiqueta es obligatoria y se puede utilizar como criterio de búsqueda al buscar esta evaluación.
10. Elija Next (Siguiente).

Paso 2: especifique Cuentas de AWS el alcance

A continuación, especifique las AWS cuentas que desea incluir en el ámbito de la evaluación.

AWS Audit Manager se integra con AWS Organizations, por lo que puede ejecutar una evaluación de Audit Manager en varias cuentas y consolidar las pruebas en una cuenta de administrador delegado. Para habilitar organizaciones en Audit Manager (si aún no lo ha hecho), consulte Habilitar y configurar AWS Organizations en la página de configuración de esta guía.

> **Note**
>
> Audit Manager puede admitir hasta 200 cuentas en el ámbito de una sola evaluación. Si intenta incluir más de 200 cuentas, no se podrá crear la evaluación.
> Además, si intenta agregar más de 250 cuentas únicas en todas sus evaluaciones, la creación de la evaluación fallará.

Para especificar las cuentas incluidas en el ámbito

1. En Cuentas de AWS, seleccione lo Cuentas de AWS que desee incluir en el ámbito de la evaluación.
   - Si ha habilitado la opción organizaciones en Audit Manager, se mostrarán varias cuentas.
   - Si no ha habilitado la opción Organizaciones en Audit Manager, solo aparecerá la cuenta actual.
2. Elija Next (Siguiente).

Paso 3: especificar los responsables de la auditoría

En este paso, especifique quiénes son los responsables de la auditoría en la evaluación. Los propietarios de la auditoría son las personas de su lugar de trabajo, generalmente del GRC o de los DevOps equipos SecOps, que son responsables de gestionar la evaluación de Audit Manager. Recomendamos que utilicen la política. AWSAuditManagerAdministratorAccess

Pasos para especificar los responsables de la auditoría

1. En Propietarios de la auditoría, elija a los propietarios de la auditoría para su evaluación. Para encontrar más responsables de la auditoría, utilice la barra de búsqueda para buscar por nombre o Cuenta de AWS.
2. Elija Next (Siguiente).

Paso 4: Revisar y crear

Revise de la información de su evaluación. Para modificar la información de un paso, seleccione Editar. Cuando haya terminado, elija Crear evaluación para iniciar la recopilación continua de evidencias.

Tras crear una evaluación, la recopilación de evidencias continúa hasta que el estado de la evaluación cambia a inactiva. También puede detener la recopilación de evidencias para un control específico cambiando el estado del control a inactivo.

> **Note**
>
> Las evidencias automatizadas están disponibles 24 horas después de crear la evaluación. Audit Manager recopila automáticamente evidencias de varios orígenes de datos, y la frecuencia con la que lo hace depende del tipo de evidencia. Para obtener más información, consulte la sección Frecuencia de recolección de evidencias de esta guía.

Recursos adicionales

Le recomendamos que continúe profundizando en los conceptos y las herramientas presentados en este tutorial. Para ello, consulte los siguientes recursos:

- Revisar los detalles de la evaluación en AWS Audit Manager: le presenta la página de detalles de la evaluación, donde puede explorar los diferentes componentes de la evaluación.
- Gestionar las evaluaciones en AWS Audit Manager: Se basa en este tutorial y proporciona información detallada sobre los conceptos y las tareas de la gestión de una evaluación. En este capítulo le recomendamos, sobre todo, que consulte los siguientes temas:
  - ¿Cómo crear una evaluación desde un marco diferente?
  - ¿Cómo revisar la evidencia de una evaluación y generar un informe de evaluación?
  - ¿Cómo cambiar el estado de una evaluación o eliminarla?
- Uso de la biblioteca de marcos para administrar marcos en AWS Audit Manager: Presenta la biblioteca de marcos y explica cómo crear un marco personalizado para sus propias necesidades de cumplimiento específicas.
- Uso de la biblioteca de controles para gestionar los controles en AWS Audit Manager: Presenta la biblioteca de controles y explica cómo crear un control personalizado para usarlo en su marco personalizado.
- Comprensión de AWS Audit Manager los conceptos y la terminología: Proporciona definiciones de los conceptos y la terminología utilizados en Audit Manager.
- [Vídeo] Recopile pruebas y gestione los datos de auditoría mediante AWS Audit Manager: muestra el proceso de creación de la evaluación que se describe en este tutorial y otras tareas, como revisar un control y generar un informe de evaluación.

Tutorial para delegados: Revisión de un conjunto de controles

En este tutorial se describe cómo revisar un conjunto de controles que el propietario de una auditoría compartió con usted en AWS Audit Manager.

Los responsables de las auditorías utilizan Audit Manager para crear evaluaciones y recopilar evidencias para los controles de las evaluaciones. A veces, los propietarios de las auditorías pueden tener dudas o necesitar ayuda a la hora de validar la evidencia de un conjunto de controles. En esta situación, el propietario de una auditoría puede delegar un conjunto de controles en un experto en la materia para su revisión.

Como delegado, usted ayuda a los responsables de la auditoría a revisar las pruebas recopiladas para detectar los controles que entran dentro de su área de especialización.

Requisitos previos

Antes de comenzar este tutorial, asegúrese de cumplir las siguientes condiciones:

- Cuenta de AWS El tuyo está configurado. Para completar este tutorial, debe utilizar la Cuenta de AWS y la consola de Audit Manager. Para obtener más información, consulte Configuración AWS Audit Manager con los ajustes recomendados.
- Está familiarizado con la terminología y la funcionalidad de Audit Manager. Para obtener una descripción general de Audit Manager, consulte ¿Qué es AWS Audit Manager? y Comprensión de AWS Audit Manager los conceptos y la terminología.

Procedimiento

Tareas

- Paso 1: revisar las notificaciones
- Paso 2: revisión del conjunto de controles y la evidencia relacionada
- Paso 3. Añadir evidencias manuales (opcional)
- Paso 4. Añada un comentario para un control (opcionalmente).
- Paso 5: marcar un control como revisado (opcional)
- Paso 6. Volver a enviar el conjunto de controles revisado al propietario de la auditoría

Paso 1: revisar las notificaciones

Comience por iniciar sesión en Audit Manager, donde podrá acceder a las notificaciones para ver los conjuntos de controles que se le han delegado para su revisión.

Revisión de las notificaciones

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Notificaciones.
3. En la página de Notificaciones, puede revisar la lista de conjuntos de controles que se le han delegado. La tabla de notificaciones incluye la siguiente información:

Nombre	Descripción
Fecha	Fecha en la que se ha delegado el conjunto de controles.
Evaluación	Nombre de la evaluación asociada al conjunto de controles. Puede elegir un nombre para la evaluación para abrir la página de detalles de la evaluación.
Conjunto de controles	Nombre del conjunto de controles que se le ha delegado para su revisión.
Origen	Usuario o rol que le ha delegado el conjunto de controles.
Descripción	Instrucciones de revisión proporcionadas por el responsable de la auditoría.

> **Tip**
>
> También puede suscribirse a un tema de SNS para recibir alertas por correo electrónico cuando se le asigne un conjunto de controles para su revisión. Para obtener más información, consulte Notificaciones en AWS Audit Manager.

Paso 2: revisión del conjunto de controles y la evidencia relacionada

El siguiente paso es revisar los conjuntos de control que el propietario de la auditoría le ha delegado. Al examinar los controles y sus pruebas, puede determinar si es necesaria alguna acción adicional para realizar un control. Entre las acciones adicionales se pueden incluir cargar manualmente evidencias adicionales para demostrar conformidad o dejar un comentario sobre ese control.

Revisión de un conjunto de controles

1. Revise en la página de Notificaciones la lista de conjuntos de controles que se le han delegado. A continuación, identifique cuál desea revisar y elija el nombre de la evaluación relacionada.
2. En la pestaña Controles de la página de detalles de la evaluación, desplácese hacia abajo hasta la tabla de Conjuntos de controles.

3. En la columna Controles agrupados por conjunto, expanda el nombre de un conjunto de controles para mostrar sus controles. A continuación, elija el nombre de un control para abrir la página de detalles del control.
4. (Opcional) Seleccione Actualizar el estado del control para cambiar el estado del control. Mientras la revisión esté en curso, puede marcar el estado como En revisión.
5. Revise la información sobre el control en las pestañas Carpetas de evidencias, Detalles, Orígenes de evidencias, Comentarios y Registro de cambios. Para obtener información sobre cada una de estas pestañas y cómo comprender los datos que en ellas se incluyen, consulte Revisar un control de evaluación en AWS Audit Manager.

Revisión de la evidencia de un control

1. En la página de detalles del control, seleccione la pestaña Carpetas de pruebas.
2. Navegue hasta la tabla de Carpetas de pruebas, donde se muestra una lista de carpetas que contienen las pruebas de ese control. Estas carpetas se organizan y nombran en función de la fecha en que se recopilaron las pruebas contenidas en esa carpeta.
3. Elija el nombre de una carpeta de evidencias para abrirla. Desde aquí, puede revisar un resumen de todas las pruebas recopiladas en esa fecha. Para entender esta información, consulte Revisión de una carpeta de evidencias en AWS Audit Manager.
4. En la página de resumen de la carpeta de pruebas, navegue hasta la tabla de Pruebas. En la columna Tiempo, selecciona una línea para abrir y revisar los detalles de las pruebas recopiladas en ese momento. Para entender esta información, consulte Revisar la evidencia en AWS Audit Manager.

Paso 3. Añadir evidencias manuales (opcional)

Aunque recopila AWS Audit Manager automáticamente las pruebas para muchos controles, en algunos casos es posible que deba proporcionar pruebas adicionales. En estos casos, puede añadir manualmente sus propias evidencias que le ayuden a demostrar la conformidad de ese control.

Adición de evidencias manuales a un control

Hay varias maneras de añadir evidencia manual a un control. Puede importar un archivo desde Amazon S3, cargar un archivo desde el navegador o introducir una respuesta de texto. Para obtener instrucciones sobre cada método, consulte Añadir evidencia manual AWS Audit Manager.

Paso 4. Añada un comentario para un control (opcionalmente).

Puede añadir comentarios a cualquier control que revise. El propietario de la auditoría puede ver estos comentarios. Por ejemplo, puede dejar un comentario para proporcionar una actualización de estado y confirmar que ha solucionado cualquier problema relacionado con ese control.

Para añadir un comentario a un control

1. Revise en la página de Notificaciones la lista de conjuntos de controles que se le han delegado. Busque el conjunto de controles para el que desea dejar un comentario y elija el nombre de la evaluación relacionada.
2. Seleccione la pestaña Controles, desplácese hacia abajo hasta la tabla de Conjuntos de controles y, a continuación, seleccione el nombre de un control para abrirlo.
3. Seleccione la pestaña Comentarios.
4. En Enviar comentarios, introduzca su comentario en el cuadro de texto.
5. Seleccione Enviar comentarios para añadir un comentario. Su comentario aparece ahora en la sección de Comentarios anteriores de la página, junto con cualquier otro comentario relacionado con este control.

Paso 5: marcar un control como revisado (opcional)

Cambiar el estado de un control es opcional. Sin embargo, le recomendamos que cambie el estado de cada control a Revisado a medida que complete la revisión de ese control. Independientemente del estado de cada control individual, puede enviar los controles al propietario de la auditoría.

Para marcar un control como revisado

1. Revise en la página de Notificaciones la lista de conjuntos de controles que se le han delegado. Busque el conjunto de controles que contiene el control que desea marcar como revisado. A continuación, elija el nombre de la evaluación relacionada para abrir la página de detalles de la evaluación.
2. En la pestaña Controles de la página de detalles de la evaluación, desplácese hacia abajo hasta la tabla de Conjuntos de controles.
3. En la columna Controles agrupados por conjunto, expanda el nombre de un conjunto de controles para mostrar sus controles. Elija el nombre de un control para abrir la página de detalles del control.
4. Seleccione Actualizar el estado del control y cambie el estado a Revisado.

5. En la ventana emergente que aparece, seleccione Actualizar el estado del control para confirmar que ha terminado de revisar el control.

Paso 6. Volver a enviar el conjunto de controles revisado al propietario de la auditoría

Cuando haya terminado de revisar todos los controles, devuelva el conjunto de controles al propietario de la auditoría para que sepa que ha finalizado la revisión.

Para volver a enviar un conjunto de controles revisado al propietario

1. Revise en la página de Notificaciones la lista de conjuntos de controles que se le asignaron. Busque el conjunto de controles que desea enviar al propietario de la auditoría y elija el nombre de la evaluación relacionada.
2. Desplácese hacia abajo hasta la tabla de Conjuntos de controles, seleccione el conjunto de controles que desee devolver al propietario de la auditoría y, a continuación, seleccione Enviar a revisión.
3. En la ventana emergente que aparece, puede añadir cualquier comentario de alto nivel sobre ese conjunto de controles antes de seleccionar Enviar para su revisión.

Tras enviar el control al propietario de la auditoría, el propietario de la auditoría podrá ver cualquier comentario que le haya dejado.

Recursos adicionales

Puede seguir aprendiendo más sobre los conceptos que se presentan en este tutorial. A continuación encontrará algunos recursos recomendados:

- Revisar los detalles de la evaluación en AWS Audit Manager: le presenta la página de detalles de la evaluación, donde puede explorar los diferentes componentes de una evaluación de Audit Manager.
- Revisar un control de evaluación en AWS Audit Manager y Revisar la evidencia en AWS Audit Manager: proporcionan definiciones para ayudarle a comprender los controles y las evidencias de una evaluación.
- Comprensión de AWS Audit Manager los conceptos y la terminología: proporciona definiciones de los conceptos y la terminología que se utilizan en Audit Manager.

Uso del panel de control de Audit Manager

Con el panel de control de Audit Manager, puede visualizar las evidencias no conformes en sus evaluaciones activas. Es una forma cómoda y rápida de supervisar sus evaluaciones, mantenerse informado y solucionar los problemas de forma proactiva. De forma predeterminada, el panel proporciona una vista agregada de arriba hacia abajo de todas las evaluaciones activas. Con esta vista, puede identificar visualmente los problemas en sus evaluaciones sin tener que examinar primero una gran cantidad de evidencias individuales.

El panel de control es la primera pantalla que aparece al iniciar sesión en la consola de Audit Manager. Contiene dos widgets que muestran los datos y los indicadores clave de rendimiento (KPIs) que son más relevantes para usted. Con un filtro de evaluación, puede refinar estos datos para centrarlos KPIs en una evaluación específica. A partir de ahí, puede revisar las agrupaciones de dominios de control para identificar qué controles tienen la mayor cantidad de evidencias no conformes. A continuación, puede explorar los controles subyacentes para examinar y solucionar los problemas.

> **Note**
>
> Si es la primera vez que utiliza Audit Manager o no tiene ninguna evaluación activa, no se mostrará ningún dato en el panel de control. Para empezar, cree una evaluación. Esto inicia la recopilación continua de evidencias. Después de un período de 24 horas, los datos de evidencia agregados comenzarán a aparecer en el panel de control. Puede leer las siguientes secciones para aprender a entender e interpretar estos datos.

Esta página abarca los siguientes temas:

Temas

- Conceptos y terminología del panel
- Elementos del panel
- Pasos a seguir a continuación
- Recursos adicionales

Conceptos y terminología del panel

En esta sección se describen aspectos importantes que debe conocer sobre el panel de control de Audit Manager antes de empezar a usarlo.

Permisos y visibilidad

Tanto los propietarios de la auditoría como los delegados tienen acceso al panel de control. Esto significa que ambas personas pueden ver las métricas y los agregados de todas las evaluaciones activas de su Cuenta de AWS. Tener acceso a la misma información permite que todo tu equipo se centre en KPIs los mismos objetivos.

Filtros

Audit Manager proporciona un nivel de página the section called “Filtro de evaluación” que puede aplicar a todos los widgets de su panel de control.

Evidencias no conformes

El panel destaca los controles de sus evaluaciones que contienen evidencias de verificación de la conformidad con una conclusión no conforme. La evidencia de la verificación de conformidad se refiere a los controles que utilizan AWS Config o AWS Security Hub como un tipo de fuente de datos. Para este tipo de evidencia, Audit Manager informa del resultado de una verificación de conformidad directamente desde esos servicios. Si el Centro de seguridad informa de un resultado fallido o AWS Config informa de un resultado no conforme, Audit Manager clasifica las evidencias como no conformes.

Evidencia no concluyente

Las evidencias son no concluyentes si una verificación de cumplimiento no está disponible o no es aplicable. Como resultado, no se puede realizar ninguna evaluación del cumplimiento. Este es el caso si un control usa AWS Config o AWS Security Hub como un tipo de fuente de datos, pero usted no habilitó esos servicios. Este también es el caso si el control utiliza un tipo de fuente de datos que no admite las comprobaciones de conformidad, como las pruebas manuales, las llamadas a la AWS API o AWS CloudTrail. En la consola, las pruebas cuyo estado de verificación de conformidad es no aplicable se clasifican como no concluyentes en el panel de control.

Puede utilizar las pruebas no concluyentes para evaluar manualmente el cumplimiento de un control.

> **Note**
>
> Las pruebas no concluyentes no indican un fallo, sino que se deben evaluar manualmente las pruebas para comprobar su conformidad.

Pruebas conformes

La evidencia es conforme si una verificación de cumplimiento no informó de ningún problema. Este es el caso si Security Hub informa de un resultado de aprobación o AWS Config informa de un resultado de conformidad.

Dominios de control

El panel presenta el concepto de dominio de control. Piense en los dominios de control como una categoría general de controles que no es específica de ningún marco en particular. Las agrupaciones de dominios de control son una de las funciones más potentes del panel de control. Audit Manager destaca los controles de sus evaluaciones que contienen evidencias no conformes y los agrupa por dominio de control. Con esta característica, puede centrar sus esfuerzos de remediación en ámbitos temáticos específicos mientras se prepara para una auditoría.

> **Note**
>
> Tenga en cuenta que los dominios no son conjuntos de controles. Los conjuntos de controles son agrupaciones de controles específicas de un marco, que suelen definir los organismos reguladores. Por ejemplo, el marco PCI DSS tiene un conjunto de controles denominado “Requisito 8: identificar y autenticar el acceso a los componentes del sistema”. Este conjunto de control pertenece al dominio de control de la gestión de identidad y acceso.

Consistencia eventual de los datos

Los datos del panel de control son finalmente consistentes. Esto significa que, al leer datos del panel, podrían no reflejar de forma instantánea los resultados de una operación de escritura o actualización reciente. Si vuelve a comprobarlo al cabo de unas horas, el panel debería reflejar los datos más recientes.

Datos de evaluaciones eliminadas e inactivas

El panel muestra los datos de las evaluaciones activas. Si elimina una evaluación o cambia su estado a inactiva el mismo día que consulta el panel, los datos de esa evaluación se incluyen de la siguiente manera.

- Evaluaciones inactivas: si Audit Manager recopiló evidencia para su evaluación antes de cambiarla a inactiva, esos datos de evidencia se incluyen en los recuentos del panel de control para ese día.
- Evaluaciones eliminadas: si Audit Manager recopiló evidencia para su evaluación antes de eliminarla, esos datos de evidencia no se incluyen en los recuentos del panel de control para ese día.

Elementos del panel

En las siguientes secciones se describen los distintos componentes del panel.

Temas

- Filtro de evaluación
- Instantánea diaria
- Controles con evidencia no conforme agrupados por dominio de control

Filtro de evaluación

Puede utilizar el filtro de evaluación para centrarse en una evaluación activa específica.

De forma predeterminada, el panel muestra los datos agregados de todas las evaluaciones activas. Si desea ver los datos de una evaluación específica, aplique un filtro de evaluación. Se trata de un filtro a nivel de página que se aplica a todos los widgets del panel de control.

Para aplicar el filtro de evaluación, seleccione una evaluación de la lista desplegable de la parte superior del panel. En esta lista se muestran hasta 10 de sus evaluaciones activas. Las evaluaciones creadas más recientemente aparecen primero. Si tiene muchas evaluaciones activas, puede empezar a escribir el nombre de una evaluación para encontrarla rápidamente. Después de seleccionar una evaluación, el panel muestra solo los datos de esa evaluación.

Instantánea diaria

Este widget muestra una instantánea del estado actual de cumplimiento de sus evaluaciones activas.

La instantánea diaria refleja los datos más recientes que se recopilaron en la fecha que aparece en la parte superior del panel. La fecha y la hora del panel de control se representan en la hora universal coordinada (UTC). Es importante entender que estos números son recuentos diarios basados en esta marca de tiempo. Hasta la fecha, no son una suma total.

De forma predeterminada, la instantánea diaria muestra los siguientes datos de todas las evaluaciones activas:

1. Controles con evidencias no conformes: el número total de controles asociados a evidencias no conformes.
2. Evidencia no conforme: cantidad total de evidencias de comprobación de conformidad con una conclusión no conforme.
3. Evaluaciones activas: el número total de sus evaluaciones activas. Elija este número para ver los enlaces a estas evaluaciones.

Los datos de las instantáneas diarias cambian en función de los the section called “Filtro de evaluación” que aplique. Al especificar una evaluación, los datos reflejan únicamente los recuentos diarios de esa evaluación. En este caso, la instantánea diaria muestra el nombre de la evaluación que especificó. Puede elegir el nombre de la evaluación para abrirla.

Controles con evidencia no conforme agrupados por dominio de control

Puede usar este widget para identificar qué controles tienen la mayor cantidad de evidencias no conformes.

De forma predeterminada, el widget muestra los siguientes datos de todas las evaluaciones activas:

1. Dominio de control: una lista de los control domains que están asociados a sus evaluaciones activas.
2. Desglose de las evidencias: gráfico de barras que muestra un desglose del estado de cumplimiento de las evidencias.

Para expandir un dominio de control, elija la flecha situada junto a su nombre. Cuando se expande, la consola muestra hasta 10 controles para cada dominio. Estos controles se clasifican según el recuento total más alto de evidencias no conformes.

Los datos de este widget cambian en función de los the section called “Filtro de evaluación” que utilice. Cuando especifica una evaluación, solo ve los datos de esa evaluación. Además, también puede descargar un archivo CSV para cada dominio de control disponible en la evaluación.

El archivo .csv incluye la lista completa de los controles del dominio que están asociados a evidencias no conformes. En el siguiente ejemplo se muestran las columnas de datos de CSV con valores ficticios.

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AsessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefgh-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

Por último, al aplicar un filtro de evaluación, los nombres de los controles de cada dominio aparecen con un hipervínculo. Elija cualquier control para abrir la página de detalles del control en la evaluación especificada.

> **Tip**
>
> Si utiliza la página de detalles del control como punto de partida, puede pasar de un nivel de detalle al siguiente.
>
> 1. Página de detalles del control: en esta página la pestaña Pestaña de carpetas de evidencias muestra las carpetas diarias de evidencias que Audit Manager ha recopilado para ese control. Para obtener más información, elija una carpeta.
> 2. Carpeta de evidencias: a continuación, puede revisar un Resumen de la carpeta de evidencias y una lista de las evidencias incluidas en esa carpeta. Para obtener más información, elija un elemento de evidencia individual.
> 3. Evidencia individual: por último, puede explorar los detalles de las evidencias individuales. Este es el nivel más detallado de datos de evidencia.

Pasos a seguir a continuación

Estos son algunos de los siguientes pasos que puede seguir después de revisar el panel.

- Descargar un archivo CSV: busque el dominio de evaluación y control en el que desee centrarse y descargue la lista completa de controles relacionados con evidencias no conformes.
- Revisar un control: después de identificar un control que necesite ser corregido, puede revisarlo.
- Delegar la revisión de un control: si necesita ayuda para revisar un control, puede delegar la revisión de un conjunto de controles.
- Editar su evaluación: si desea cambiar el alcance de una evaluación activa, puede editarla.

- Actualizar el estado de la evaluación: si desea dejar de recopilar evidencias para una evaluación, puede cambiar el estado de la evaluación a Inactivo.

Recursos adicionales

Para encontrar respuestas a preguntas y problemas comunes, consulte Solución de problemas de panel en la sección Solución de problemas de esta guía.

Gestionar las evaluaciones en AWS Audit Manager

Las evaluaciones de Audit Manager se basan en marcos, es decir, en grupos de controles. Utilizando marcos como puntos de partida puede crear evaluaciones que recopilen evidencias sobre los controles de esos marcos. También puede definir el ámbito de las auditorías de sus evaluaciones. Esto incluye especificar Cuentas de AWS aquello para lo que desea recopilar pruebas.

Puntos clave

Puede crear evaluaciones desde cualquier marco. Puede utilizar un marco estándar proporcionado por Audit Manager. o bien crear una evaluación a partir de un marco personalizado que cree usted mismo. Los marcos estándar contienen conjuntos de controles prediseñados que con arreglo a una norma o reglamento de cumplimiento específico. Los marcos personalizados, en cambio, incluyen controles que puede personalizar y agrupar según sus propios requisitos.

Al crear una evaluación, se inicia la recopilación continua de evidencia. Llegado el momento de una auditoría, usted o un delegado pueden revisar esta evidencia y añadirla a un informe de evaluación.

> **Note**
>
> AWS Audit Manager ayuda a recopilar pruebas que sean relevantes para verificar el cumplimiento de normas y reglamentos de cumplimiento específicos. Sin embargo, no evalúa el cumplimiento en sí mismo. AWS Audit Manager Por lo tanto, es posible que las pruebas recopiladas no incluyan toda la información sobre su AWS uso que se necesita para las auditorías. AWS Audit Manager no sustituye a los asesores legales ni a los expertos en cumplimiento.

Recursos adicionales

Para crear y administrar las evaluaciones en Audit Manager, siga los procedimientos que se indican aquí.

- Crear una evaluación en AWS Audit Manager
- Encontrará sus evaluaciones en AWS Audit Manager

- Revisar una evaluación en AWS Audit Manager
  - Revisar los detalles de la evaluación en AWS Audit Manager
  - Revisar un control de evaluación en AWS Audit Manager
  - Revisión de una carpeta de evidencias en AWS Audit Manager
  - Revisar la evidencia en AWS Audit Manager
- Edición de una evaluación en AWS Audit Manager
  - Cambiar el estado de un control de evaluación en AWS Audit Manager
  - Cambiar el estado de una evaluación a inactiva en AWS Audit Manager
- Añadir evidencia manual AWS Audit Manager
  - Importación de archivos de evidencias manuales desde Amazon S3
  - Carga de archivos de evidencias manuales desde el navegador
  - Introducción de respuestas de texto de formato libre como evidencia manual
  - Formatos de archivo compatibles con las evidencias manuales
- Preparación de un informe de evaluación en AWS Audit Manager
  - Añadir evidencias a los informes de evaluación
  - Eliminación de evidencias de un informe de evaluación
  - Generación de informes de evaluación
  - Descarga de un informe de evaluación desde el centro de descargas
  - Navegación por un informe de evaluación y exploración de su contenido
  - Validación de un informe de evaluación
  - Eliminación de una ejecución de evaluación
  - Generación de informes de evaluación a partir de los resultados de búsqueda del buscador de evidencias
- Eliminar una evaluación en AWS Audit Manager

Crear una evaluación en AWS Audit Manager

Este tema se basa en el tutorial Tutorial para propietarios de auditorías: crear una evaluación. En esta página encontrará instrucciones detalladas que le muestran cómo crear una evaluación a partir de un marco. Siga estos pasos para crear una evaluación e iniciar la recopilación continua de evidencia.

Requisitos previos

Antes de comenzar este tutorial, asegúrese de cumplir las siguientes condiciones:

- Ha completado todos los requisitos previos que se describen en Configuración AWS Audit Manager con los ajustes recomendados. Debe usar su consola Cuenta de AWS y la de Audit Manager para completar este tutorial.
- Su identidad de IAM cuenta con los permisos adecuados para crear y administrar una evaluación en Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Tareas

- Paso 1: especificar los detalles de la evaluación
- Paso 2: especificar Cuentas de AWS el alcance
- Paso 3: especificar los responsables de la auditoría
  - Audite los permisos del propietario
- Paso 4: Revisar y crear

Paso 1: especificar los detalles de la evaluación

Comience seleccionando un marco y proporcione la información básica necesaria para su evaluación.

Pasos para especificar los detalles de la evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Evaluación y, a continuación, elija Crear evaluación.
3. En Nombre, escriba un nombre para la evaluación.
4. (Opcional) En Descripción, escriba una descripción para la evaluación.
5. En Destino de los informes de evaluación, seleccione el bucket de S3 en el que desee guardar los informes de evaluación.

> **Tip**
>
> El destino predeterminado del informe de evaluación depende de la configuración de la evaluación. Si lo prefiere, puede crear y usar varios cubos de S3 para organizar sus informes de evaluación para diferentes evaluaciones. AWS Audit Manager admite la exportación de informes de evaluación a buckets de Amazon S3, incluidos los destinos de varias cuentas. Para una seguridad y un rendimiento óptimos, le recomendamos que utilice un bucket de S3 en la misma AWS cuenta y región que utilizó su evaluación.

6. En Seleccionar marco, seleccione el marco a partir del cual desea crear la evaluación. También puede buscar en la barra de búsqueda para encontrar un marco por su nombre o por una norma o reglamento de cumplimiento.

> **Tip**
>
> Para obtener más información sobre un marco, elija el nombre del marco para ver la página de detalles del marco.

7. (Opcional) En Etiquetas, elija Añadir nueva etiqueta para asociar una etiqueta a la evaluación. Puede especificar una clave y un valor para cada etiqueta. La clave de etiqueta es obligatoria y se puede utilizar como criterio de búsqueda al buscar esta evaluación.
8. Elija Siguiente.

> **Note**
>
> Es importante que se asegure de que la evaluación recopile las evidencias correctas para un marco determinado. Antes de comenzar con la recopilación de evidencias, le recomendamos que revise los requisitos del marco elegido. A continuación, valídelos los parámetros actuales de la regla de AWS Config . Para garantizar que estos parámetros se ajustan a los requisitos del marco, puede actualizar la regla en AWS Config.
> Supongamos, por ejemplo, que está creando una evaluación para CIS v1.2.0. Este marco tiene un control denominado 1.9: asegúrese de que la política de contraseñas de IAM exija una longitud mínima de 14 o más. En AWS Config, la iam-password-policyregla tiene un `MinimumPasswordLength` parámetro que comprueba la longitud de la contraseña. El valor predeterminado para este parámetro es 14 caracteres. Por lo tanto, la regla concuerda con los requisitos de control establecidos. Si no utiliza el valor de parámetro predeterminado,

asegúrese de que sea igual o superior al requisito de 14 caracteres establecido en CIS v1.2.0. Puede encontrar los detalles de los parámetros predeterminados de cada regla administrada en la documentación de AWS Config.

Paso 2: especificar Cuentas de AWS el alcance

Puede especificar Cuentas de AWS que varios estén en el ámbito de una evaluación. Audit Manager admite varias cuentas gracias a la integración con AWS Organizations. Esto significa que las evaluaciones de Audit Manager se pueden ejecutar en varias cuentas, de modo que las evidencias recopiladas se consolidan en una cuenta del administrador delegado. Para activar las organizaciones en Audit Manager, consulte Habilitar y configurar AWS Organizations.

> **Note**
>
> Audit Manager puede admitir hasta 200 cuentas en el ámbito de una sola evaluación. Si intenta incluir más de 200 cuentas, no se podrá crear la evaluación.
> Además, si intenta agregar más de 250 cuentas únicas en todas sus evaluaciones, la creación de la evaluación fallará.

Para especificar Cuentas de AWS el alcance

1. En Cuentas de AWS, seleccione lo Cuentas de AWS que desee incluir en el ámbito de la evaluación.
   - Si ha activado las organizaciones en Audit Manager, se mostrarán varias cuentas. Puede elegir una o más cuentas de la lista. Alternativamente también puede buscar una cuenta por el nombre de la cuenta, el ID o el correo electrónico.
   - Si no activó Organizations en Audit Manager, solo aparecerá Cuenta de AWS la actual.
2. Elija Siguiente.

> **Note**
>
> Cuando se elimina una cuenta incluida de su organización, Audit Manager deja de recopilar evidencias de esa cuenta. Sin embargo, la cuenta sigue apareciendo en su evaluación, en la pestaña Cuentas de AWS. Para eliminar la cuenta de la lista de cuentas incluidas, edite la

evaluación. La cuenta eliminada ya no aparece en la lista durante la edición y puede guardar los cambios sin esa cuenta incluida.

Paso 3: especificar los responsables de la auditoría

En este paso, especifique quiénes son los responsables de la auditoría en la evaluación. Los propietarios de la auditoría son las personas de su lugar de trabajo, generalmente del GRC o de los DevOps equipos SecOps, que son responsables de gestionar la evaluación de Audit Manager. Les recomendamos que utilicen la política. AWSAuditManagerAdministratorAccess

Pasos para especificar los responsables de la auditoría

1. En Responsables de la auditoría, revise la lista actual de las personas encargadas de las auditorías. La columna del propietario de la auditoría muestra el usuario IDs y las funciones. La Cuenta de AWScolumna muestra el Cuenta de AWS del propietario de la auditoría.
2. Los responsables de auditoría que tienen una casilla de verificación activada son los que se incluyen en la evaluación. Desactive la casilla de verificación de los responsables de auditoría que desee eliminar de la evaluación. Para encontrar otros responsables de auditoría, utilice la barra de búsqueda para buscar por nombre o Cuenta de AWS.
3. Cuando haya terminado, elija Siguiente.

Audite los permisos del propietario

Se adjunta la siguiente política para todos los propietarios de auditorías de una evaluación.

Audit Manager los *placeholder text* reemplaza por sus identificadores de cuenta y recurso antes de adjuntar la política.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditOwner",
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": "Principal for user/role who are the audit owners of the
 Assessment"
            },
            "Action": [
                "auditmanager:GetAssessment",
                "auditmanager:UpdateAssessment",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:UpdateAssessmentStatus",
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:DeleteAssessment",
                "auditmanager:GetChangeLogs",
                "auditmanager:GetEvidenceFoldersByAssessment",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder",
                "auditmanager:BatchCreateDelegationByAssessment",
                "auditmanager:BatchDeleteDelegationByAssessment",
                "auditmanager:AssociateAssessmentReportEvidenceFolder",
                "auditmanager:BatchAssociateAssessmentReportEvidence",
                "auditmanager:BatchDisassociateAssessmentReportEvidence",
                "auditmanager:CreateAssessmentReport",
                "auditmanager:DeleteAssessmentReport",
                "auditmanager:DisassociateAssessmentReportEvidenceFolder",
                "auditmanager:GetAssessmentReportUrl"
            ],
            "Resource": [
                "arn:aws:auditmanager:us-
east-1:account_ID:assessment/assessment_ID",
                "arn:aws:auditmanager:us-
east-1:account_ID:assessment/assessment_ID/*"
            ]
        }
    ]
}
```

Paso 4: Revisar y crear

Revise de la información de su evaluación. Para modificar la información de un paso, seleccione Editar. Cuando haya terminado, elija Crear evaluación.

Esta acción inicia la recopilación continua de evidencias para su evaluación. Tras crear una evaluación, la recopilación de evidencias continúa hasta que el estado de la evaluación cambia a inactiva. También puede detener la recopilación de evidencias para un control específico. Para ello, debe cambiar el estado del control a Inactivo.

> **Note**
>
> Las evidencias automatizadas estarán disponibles 24 horas después de que se haya creado la evaluación. Audit Manager recopila automáticamente evidencias de varios orígenes de datos, y la frecuencia con la que lo hace depende del tipo de evidencia. Para más información, consulte Frecuencia de recolección de evidencias en esta guía.

Pasos a seguir a continuación

Para revisitar la evaluación más adelante, consulte Encontrará sus evaluaciones en AWS Audit Manager. Puede seguir estos pasos para localizar la evaluación y poder verla, editarla o seguir trabajando en ella.

Recursos adicionales

Para obtener soluciones a los problemas de evaluación en Audit Manager, consulte Solución de problemas de evaluación y recopilación de pruebas.

Encontrará sus evaluaciones en AWS Audit Manager

Tras crear las evaluaciones en AWS Audit Manager, podrá encontrarlas en la página de evaluaciones de la consola Audit Manager.

En esta página puede realizar varias acciones en las evaluaciones. Por ejemplo, puede ver los detalles de las evaluaciones, editar sus configuraciones o eliminar las que ya no sean necesarias. Además, la página de evaluaciones sirve como punto de partida para crear nuevas evaluaciones.

También puede ver las evaluaciones mediante programación con la API de Audit Manager o AWS Command Line Interface (AWS CLI).

Requisitos previos

En el siguiente procedimiento se da por sentado que ha creado previamente al menos una evaluación. Si aún no ha creado ninguna evaluación, no verá ningún resultado si sigue estos pasos.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Puede ver las evaluaciones con la consola de Audit Manager, la API de Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Visualización de la evaluaciones en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Evaluaciones y verá una lista de sus evaluaciones.
3. Elija el nombre de una evaluación para ver sus detalles.

AWS CLI

Pasos para ver sus evaluaciones (en CLI)

Para ver las evaluaciones en Audit Manager, ejecute el comando list-assessments. Puede utilizar el subcomando `--status` para ver las evaluaciones activas o inactivas.

```
aws auditmanager list-assessments --status ACTIVE
```

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

Visualización de las evaluaciones con la API

Para ver las evaluaciones en Audit Manager, utilice la ListAssessmentsoperación. Puede utilizar el atributo de estado para ver las evaluaciones activas o inactivas.

Para más información, consulte uno de los enlaces anteriores de la referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar la `ListAssessments` operación y los parámetros en uno de los idiomas específicos AWS SDKs.

Pasos a seguir a continuación

Cuando desee explorar el contenido de la evaluación, siga los pasos que se indican en Revisar una evaluación en AWS Audit Manager. Esta página le guiará por los detalles de la evaluación y le explicará la información que aparece.

En la página de evaluaciones, también puede editar una evaluación, eliminar una evaluación o crear una evaluación.

Recursos adicionales

Para obtener soluciones a los problemas de evaluación en Audit Manager, consulte Solución de problemas de evaluación y recopilación de pruebas.

Revisar una evaluación en AWS Audit Manager

Tras crear las evaluaciones en Audit Manager, puede abrirlas y revisarlas en cualquier momento.

Puntos clave

Cuando desee explorar la evaluación, podrá profundizar gradualmente en los detalles y revisarla con niveles de detalle cada vez mayores.

1. Detalles de la evaluación: comience por revisar los detalles generales de la evaluación. En esta página puede revisar el nombre, la descripción, el ámbito y otros detalles de la evaluación. Esto le proporciona información general de alto nivel sobre la evaluación.
2. Detalles del control de la evaluación: a continuación, profundice en la evaluación revisando los detalles de cada control de evaluación. Esto le permitirá comprender los requisitos y objetivos específicos de cada control.

3. Detalles de la carpeta de evidencias: para cada control de evaluación, puede revisar las carpetas de evidencias correspondientes que incluyen la evidencia de un control determinado. Estas carpetas organizan la evidencia de respaldo relacionada con cada control.
4. Detalles de las evidencias: por último, profundice más para revisar las evidencias individuales de cada carpeta. Esto puede incluir instantáneas de configuración, registros de actividad de los usuarios, resultados de conformidad o evidencia cargada manualmente, como, por ejemplo, documentos y capturas de pantalla. La revisión de estas evidencias le ayudará a comprender cómo su organización cumple con los requisitos del control.

Si sigue estos pasos, podrá explorar detenidamente la evaluación, comprender sus componentes y revisar las evidencias que respaldan las iniciativas de conformidad de su organización.

Recursos adicionales

Para empezar a revisar una evaluación en Audit Manager, siga los procedimientos que se indican aquí.

- Revisar los detalles de la evaluación en AWS Audit Manager
- Revisar un control de evaluación en AWS Audit Manager
- Revisión de una carpeta de evidencias en AWS Audit Manager
- Revisar la evidencia en AWS Audit Manager

Revisar los detalles de la evaluación en AWS Audit Manager

Cuando necesite revisar los detalles de una evaluación, encontrará la información organizada en varias secciones en la página de detalles de la evaluación. Estas secciones le ayudan a acceder fácilmente a la información pertinente para su tarea y a comprenderla.

Contenido

- Requisitos previos
- Procedimiento
  - Sección de detalles de la evaluación
  - Pestaña de controles
  - Pestaña de selección del informe de evaluación

- Cuentas de AWS pestaña
- Servicios de AWS pestaña
- Pestaña de responsables de la auditoría
- Pestaña Etiquetas
- Pestaña del registro de cambios
- Pasos a seguir a continuación
- Recursos adicionales

Requisitos previos

En el siguiente procedimiento se da por sentado que ha creado previamente al menos una evaluación. Si aún no ha creado ninguna evaluación, no verá ningún resultado si sigue estos pasos.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Apertura y revisión de una página de detalles de una evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Evaluaciones y verá una lista de sus evaluaciones.
3. Seleccione el nombre de la evaluación que desee consultar y ábrala.
4. Revise los detalles de la evaluación con la siguiente información como referencia.

Secciones de la página de detalles de la evaluación

- Sección de detalles de la evaluación
- Pestaña de controles
- Pestaña de selección del informe de evaluación
- Cuentas de AWS pestaña
- Servicios de AWS pestaña
- Pestaña de responsables de la auditoría

- Pestaña Etiquetas
- Pestaña del registro de cambios

Sección de detalles de la evaluación

Puede utilizar la sección Detalles de la evaluación para ver un resumen de la evaluación.

En la sección Detalles de la evaluación, puede revisar la siguiente información:

Nombre	Descripción
1. Descripción	La descripción de la evaluación.
2. Tipo de conformidad	Estándar o normativa de conformidad en los que se basa la evaluación.
3. Destino de los informes de evaluación	Bucket de S3 en el que Audit Manager guarda el informe de evaluación.
4. Total de evidencias	Número total de elementos de evidencia que se recopilan para la evaluación.
5. Selección del informe de evaluación	Número de elementos de evidencia seleccionados para incluirse en el informe de evaluación.
6. Date created (Fecha de creación)	Fecha en que se creó la evaluación.
7. Última actualización	Fecha en que se modificó la evaluación por última vez.
8. Estado	Estado de la evaluación.

Nombre	Descripción
	• Activo: la evaluación está recopilando evidencias en este momento. • Inactivo: la evaluación ya no recopila evidencias.

Pestaña de controles

Puede utilizar esta pestaña para consultar información sobre los controles de la evaluación.

En Resumen del estado de los controles, puede revisar la siguiente información:

Nombre	Descripción
Total de controles	Número total de controles de la evaluación.
Revisado	Número de controles que revisó la persona responsable o delegada de la auditoría.
En revisión	Número de controles que se están revisando en este momento.
Inactivo	Número de controles que ya no recopilan evidencias de forma activa.

En la tabla Conjuntos de controles, puede revisar una lista de controles agrupados por conjunto de controles. Puede expandir o contraer los controles de cada conjunto. También puede buscarlos por el nombre si busca un determinado control.

En esta tabla puede revisar la siguiente información:

Nombre	Descripción
Controles agrupados por conjuntos de controles	Nombre del conjunto de controles.
Estado del control	Estado del control.

Nombre	Descripción
	• En revisión indica que este control aún no se ha revisado. Se siguen recopilando evidencias para este control y puede añadirlas manualmente. Este es el valor predeterminado. • Revisado indica que ya se revisaron las evidencias de este control. Se siguen recopilando evidencias y puede añadirlas manualmente. • El estado Inactivo indica que la recopilación automática de evidencias se ha interrumpido para este control. Ya no puede añadir ninguna evidencia manual.
Delegado a	Revisor de este control, si se asignó a un delegado para su revisión.
Total de evidencias	Número de elementos de evidencia que se han recopilado para este control.

Pestaña de selección del informe de evaluación

Puede utilizar esta pestaña para consultar las evidencias que se incluirán en el informe de evaluación. Las evidencias se agrupan en carpetas de evidencias, que se organizan según la fecha en que se crearon.

Puede examinar estas carpetas y seleccionar qué evidencias desea incluir en su informe de evaluación. Para obtener instrucciones sobre cómo añadir evidencias a un informe de evaluación, consulte Añadir evidencias a los informes de evaluación.

En esta sección puede revisar la siguiente información:

Nombre	Descripción
Carpeta de evidencias	Nombre de la carpeta de evidencias. El nombre de la carpeta se basa en la fecha en que se recopiló la evidencia.
Evidencia seleccionada	Número de elementos de evidencia de la carpeta que se incluyen en el informe de evaluación.

Nombre	Descripción
Nombre del control	Nombre del control asociado a esta carpeta de evidencias.

Cuentas de AWS pestaña

Puede utilizar esta pestaña para ver las Cuentas de AWS que están incluidas en el ámbito de la evaluación.

En esta sección puede revisar la siguiente información:

Nombre	Descripción
ID de cuenta	El ID de la Cuenta de AWS.
Nombre de cuenta	Nombre del elemento Cuenta de AWS.
Correo electrónico	La dirección de correo electrónico asociada con la Cuenta de AWS.

Servicios de AWS pestaña

Puede que vea o no esta pestaña en la evaluación.

Si la Servicios de AWS pestaña no se muestra (estado ideal)

Si no ve esta pestaña, Audit Manager está gestionando cuáles Servicios de AWS están dentro del ámbito de su evaluación.

Audit Manager deduce este ámbito examinando los controles de evaluación y sus orígenes de datos y asignando esta información a los Servicios de AWS correspondientes. Siempre que un origen de datos subyacente cambie para la evaluación, Audit Manager actualizará automáticamente el ámbito según sea necesario para reflejar los Servicios de AWS correctos. Esto garantiza que la evaluación recopile evidencias precisas y completas sobre todos los servicios pertinentes del entorno de AWS .

Si se muestra la Servicios de AWS pestaña

Si es así, ve esta pestaña, significa que Audit Manager no está gestionando cuáles Servicios de AWS están dentro del ámbito de su evaluación.

En este caso, aparece la siguiente información sobre los servicios incluidos que ha definido:

Nombre	Descripción
Servicio de AWS	Nombre del elemento Servicio de AWS.
Categoría	Categoría de servicio, como, por ejemplo, computación o base de datos.
Descripción	Una descripción de Servicio de AWS.

Audit Manager realiza evaluaciones de recursos para los servicios que se detallan en la tabla. Por ejemplo, si Amazon S3 aparece en la lista, Audit Manager puede recopilar evidencias sobre sus buckets de S3. Las evidencias exactas que se recopilan dependen del data source de un control. Por ejemplo, si el tipo de fuente de datos es AWS Config y el mapeo de la fuente de datos es una AWS Config regla (por ejemplos`3-bucket-public-write-prohibited`), Audit Manager recopila el resultado de la evaluación de esa regla como evidencia. Para obtener más información, consulte la sección ¿Cuál es la diferencia entre un servicio incluido y un tipo de origen de datos? de esta guía.

Si su evaluación se creó en la consola a partir de un marco estándar, Audit Manager seleccionó los servicios por usted y asignó sus orígenes de datos de acuerdo con los requisitos del marco. Si el marco estándar contiene solo controles manuales, no Servicios de AWS está incluido en el ámbito de aplicación.

> **Note**
>
> La próxima vez que edite la evaluación o cambie uno de sus controles personalizados, Audit Manager se hará cargo de la administración de los servicios incluidos. Cuando esto ocurre, la pestaña Servicios de AWS se eliminará de la evaluación.

Pestaña de responsables de la auditoría

Puede utilizar esta pestaña para consultar quiénes son los responsables de la auditoría de la evaluación.

En esta sección puede revisar la siguiente información:

Nombre	Descripción
Propietario de la auditoría	Nombre del responsable de la auditoría.
Cuenta de AWS	El Cuenta de AWS ID del propietario de la auditoría.

Pestaña Etiquetas

Puede usar esta pestaña para ver las etiquetas de la evaluación. Estas etiquetas se heredan del marco que se utilizó para crear la evaluación. Para más información acerca del uso de etiquetas en Audit Manager, consulte Recursos de etiquetado AWS Audit Manager.

En esta sección puede revisar la siguiente información:

Nombre	Descripción
Clave	Clave de la etiqueta, como, por ejemplo, un estándar, una normativa o una categoría de conformidad.
Valor	El valor de la etiqueta.

Pestaña del registro de cambios

Puede usar esta pestaña para ver la actividad de los usuarios durante la evaluación.

En esta sección puede revisar la siguiente información:

Nombre	Descripción
Fecha	Fecha de la actividad.
Servicio	Usuario que realizó la acción.
Action	Acción que se produjo, como, por ejemplo, la creación de una evaluación.
Tipo	Tipo de objeto que ha cambiado, como, por ejemplo, una evaluació n.

Nombre	Descripción
Resource	Recurso que se vio afectado por el cambio, como, por ejemplo, el marco a partir del cual se creó la evaluación.

Pasos a seguir a continuación

Para seguir revisando el contenido de la evaluación, siga los pasos que se indican en Revisar un control de evaluación en AWS Audit Manager. Esta página le guiará por los detalles de los controles de la evaluación y le explicará la información que aparece.

Recursos adicionales

- En la página de detalles de la evaluación se me pide que vuelva a crearla
- No veo ningún control o conjunto de controles en mi evaluación
- No puedo ver los servicios incluidos en el ámbito de la evaluación

Revisar un control de evaluación en AWS Audit Manager

Cuando necesite revisar los controles de una evaluación, encontrará la información organizada en varias secciones en la página de detalles del control de la evaluación. Estas secciones le ayudan a acceder fácilmente a la información pertinente para su tarea y a comprenderla.

Contenido

- Requisitos previos
- Procedimiento
  - Sección de detalles del control
  - Pestaña de carpetas de evidencias
  - Pestaña Detalles
  - Pestaña Orígenes de evidencias
  - Pestaña de comentarios
  - Pestaña del registro de cambios
- Pasos a seguir a continuación
- Recursos adicionales

Requisitos previos

En el siguiente procedimiento se da por sentado que ha creado previamente al menos una evaluación. Si aún no ha creado ninguna evaluación, no verá ningún resultado si sigue estos pasos.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Apertura y revisión de una página de detalles del control de una evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Evaluaciones y, a continuación, el nombre de la evaluación que desee abrir.
3. En la página de evaluación, seleccione la pestaña Controles, desplácese hacia abajo hasta llegar a la tabla conjuntos de controles y, a continuación, elija el nombre del control que desea abrir.
4. Revise los detalles del control de la evaluación con la siguiente información como referencia.

Secciones de la página de detalles del control de la evaluación

- Sección de detalles del control
- Pestaña de carpetas de evidencias
- Pestaña Detalles
- Pestaña Orígenes de evidencias
- Pestaña de comentarios
- Pestaña del registro de cambios

Sección de detalles del control

Puede utilizar la sección Detalles del control para ver un resumen del control de evaluación.

En esta sección puede revisar la siguiente información:

Nombre	Descripción
Descripción	Descripción proporcionada para el control.
Estado del control	Estado del control. • En revisión: el control aún no se ha revisado. Se siguen recopilando evidencias para este control y puede añadirlas manualmente. Este es el valor predeterminado. • Revisado: se han revisado las evidencias para este control. Se siguen recopilando evidencias y puede añadirlas manualmente. • Inactivo: la recopilación automática de evidencias se ha interrumpido para este control. Ya no puede añadir ninguna evidencia manual.

Pestaña de carpetas de evidencias

Puede utilizar esta pestaña para consultar las evidencias recopiladas para este control. Se organizan en carpetas a diario. Desde aquí también puede realizar las siguientes acciones:

- Revisar una carpeta de evidencias: para ver los detalles de una carpeta de evidencias, elija el nombre de la carpeta con el hipervínculo.
- Añadir una carpeta de evidencias a un informe de evaluación: para incluir una carpeta de evidencias, selecciónela y elija Añadir al informe de evaluación.
- Eliminar una carpeta de evidencias de un informe de evaluación: para excluir una carpeta, selecciónela y elija Eliminar del informe de evaluación.
- Añadir una evidencia manual: para obtener instrucciones, consulte Añadir evidencia manual AWS Audit Manager.

En esta sección puede revisar la siguiente información:

Nombre	Descripción
Carpeta de evidencias	Nombre de la carpeta de evidencias. El nombre se basa en la fecha en que se recopiló o agregó manualmente la evidencia o evidencias.
Comprobación de conformidad	Número de problemas en la carpeta de evidencias. Este número representa el número total de problemas de seguridad de los que se informó directamente o de AWS Security Hub ambos. AWS Config Si ves No aplicable, esto indica que no tienes Security Hub o que no lo tienes AWS Config activado, o que las pruebas provienen de un tipo de fuente de datos diferente.
Total de evidencias	Número total de elementos de evidencia incluidos en la carpeta.
Selección del informe de evaluación	Número de elementos de evidencia de la carpeta que se incluyen en el informe de evaluación.

> **Tip**
>
> Si no ve la carpeta de evidencias que busca, cambie el filtro desplegable a Siempre. Tenga en cuenta que por defecto se muestran las carpetas de los últimos siete días.

Pestaña Detalles

En esta sección puede revisar la siguiente información:

Nombre	Descripción
Información de prueba	Procedimiento recomendado para probar que el control funcione según lo previsto.
Plan de acción	Acciones recomendadas que se deben tomar si es necesario corregir el control.

Pestaña Orígenes de evidencias

Puede utilizar esta pestaña para comprobar de dónde recopila las evidencias el control de la evaluación. Los orígenes de evidencias pueden incluir cualquiera de las siguientes opciones:

Nombre	Descripción
Controles comunes	Estos son los controles comunes que recopilan evidencias para respaldar el control de la evaluación. Los controles más comunes recopilan pruebas mediante fuentes de datos subyacentes que se AWS gestionan por usted. Para cada control común que aparece en la lista, Audit Manager recopila la evidencia pertinente de todos los controles principales de respaldo. Elija un control común para ver los controles principales relaciona dos.
Controles principales	Estos son los controles principales que recopilan evidencias para respaldar el control de la evaluación. Los controles principales recopilan evidencias mediante un grupo predefinido de orígenes de datos que AWS administra. Elija un control principal para ver los orígenes de datos subyacentes.

Origen de datos	Estos son los orígenes de datos individuales que recopilan evidencias para respaldar el control de la evaluación.
	
	• Nombre: nombre del origen de datos.
	• Tipo: tipo de origen de datos del que proceden las evidencias.
	  • Si Audit Manager recopila evidencias, el tipo puede ser: AWS Security Hub, AWS Config, AWS CloudTrail o Llamadas a la API de AWS .
	  • Si carga sus propias evidencias, el tipo es Manual. Las descripciones indican si la evidencia manual requerida es una carga de archivos o una respuesta de texto.
	• Asignación: palabra clave específica que se utiliza para recopilar evidencias.

Nombre	Descripción
	• Si el tipo es AWS Config, la asignación es una regla de AWS Config (como, por ejemplo, `SNS_ENCRYPTED_KMS`). • Si el tipo es AWS Security Hub, la asignación es un control de Security Hub (como, por ejemplo, `EC2.1`). • Si el tipo son Llamadas a la API de AWS , la asignación es una llamada a la API (como, por ejemplo, `kms_ListKeys`). • Si el tipo es AWS CloudTrail, el mapeo es un CloudTrail evento (por ejemplo`CreateAccessKey`). • Frecuencia: con qué frecuencia Audit Manager recopila evidencias para un origen de datos de llamada a la API de AWS .

Pestaña de comentarios

En esta pestaña puede añadir un comentario sobre el control y sus evidencias. También puede ver una lista de los comentarios anteriores.

- En Enviar comentarios, puede escribir comentarios de texto para un control y enviarlos con Enviar comentarios.
- En Comentarios anteriores verá una lista de los comentarios anteriores junto con la fecha en la que se agregaron y el ID del usuario que los introdujo.

Pestaña del registro de cambios

Puede usar esta pestaña para ver la actividad de los usuarios durante el control de la evaluación. La misma información está disponible como registros de auditoría en AWS CloudTrail. Con la actividad del usuario que se captura directamente en Audit Manager, puede revisar fácilmente los registros de auditoría de la actividad de un control determinado.

En esta sección puede revisar la siguiente información:

Nombre	Descripción
Fecha	Fecha y hora de la actividad, representadas en tiempo universal coordinado (UTC).
Servicio	Usuario o rol que realizó la actividad.
Action	Acción que se produjo, como, por ejemplo, la creación de una evaluación.
Tipo	Tipo de objeto que ha cambiado, como, por ejemplo, una evaluació n.
Resource	Recurso que se vio afectado por el cambio, como, por ejemplo, el marco a partir del cual se creó la evaluación.

Audit Manager rastrea la actividad siguiente de los usuarios en los registros de cambios:

- Creación de las evaluaciones
- Edición de las evaluaciones
- Compleción de las evaluaciones
- Eliminación de las evaluaciones
- Delegación de conjuntos de controles para su revisión
- Envío de conjuntos de controles revisados a la persona responsable de la auditoría
- Carga de evidencias manual
- Actualización del estado de los controles
- Generación de informes de evaluación

Pasos a seguir a continuación

Para seguir revisando la evaluación, siga los pasos que se indican en Revisión de una carpeta de evidencias en AWS Audit Manager. Esta página le guiará por las carpetas de evidencias y le mostrará cómo entender la información que ve.

Recursos adicionales

- No veo ningún control o conjunto de controles en mi evaluación

Revisión de una carpeta de evidencias en AWS Audit Manager

A medida que la evaluación va recopilando evidencias, Audit Manager las organiza en carpetas para su comodidad. Cuando necesite revisar una carpeta de evidencias, encontrará la información organizada en varias secciones.

Contenido

- Requisitos previos
- Procedimiento
  - Resumen de la carpeta de evidencias
  - Tabla de evidencias
- Pasos a seguir a continuación
- Recursos adicionales

Requisitos previos

En el siguiente procedimiento se da por sentado que ha creado previamente al menos una evaluación. Si aún no ha creado ninguna evaluación, no verá ningún resultado si sigue estos pasos.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Tenga en cuenta que una evaluación tarda hasta 24 horas en empezar a recopilar evidencias automatizadas. Si la evaluación aún no tiene ninguna evidencia, no se mostrará ningún resultado si sigue estos pasos.

Procedimiento

Apertura y revisión de una carpeta de evidencias

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.

2. En el panel de navegación, elija Evaluaciones y luego una evaluación.
3. En la página de evaluación, seleccione la pestaña Controles, desplácese hacia abajo hasta llegar a la tabla Controles y, a continuación, elija un control de evaluación.
4. En la página de control de la evaluación, elija la pestaña Carpetas de evidencias.
5. En la tabla Carpetas de evidencias, seleccione el nombre de una carpeta de evidencias.
6. Revise la carpeta de evidencias con la siguiente información como referencia.

Secciones de una página de carpetas de evidencias

- Resumen de la carpeta de evidencias
- Tabla de evidencias

Resumen de la carpeta de evidencias

Puede utilizar la sección Resumen de la página para ver una descripción general de las evidencias que incluye la carpeta. Para obtener más información sobre los diferentes tipos de evidencias, consulte Evidencia.

En esta sección puede revisar la siguiente información:

Nombre	Descripción
1. Fecha y hora	Fecha y hora en que se creó la carpeta de evidencias. Se representa en formato de hora universal coordinada (UTC).
2. Controlar	Nombre del control relacionado con la carpeta de evidencias.
3. Añadida al informe de evaluación	Número de elementos de evidencia seleccionados para incluirse en el informe de evaluación.

Nombre	Descripción
4. Total de evidencias	Número total de elementos de evidencia incluidos en la carpeta de evidencias.
5. Recursos	El número total de AWS recursos que se evaluaron al recopilar las pruebas de esta carpeta.
6. Actividad de los usuarios	Número de elementos de evidencia que se incluyen en la categoría actividad de los usuarios. Esta evidencia se recopila de AWS CloudTrail los registros.
7. Datos de configuración	Número de elementos de evidencia que se incluyen en la categoría datos de configuración. Esta evidencia se recopila a partir de llamadas a la API que toman instantáneas de configuración de otras Servicios de AWS.
8. Manual	Número de elementos de evidencia que se incluyen en la categoría manual. Estas evidencias se añaden manualmente.
9. Comprobación de conformidad	Número de elementos de evidencia que se incluyen en la categoría comprobación de conformidad. Esta evidencia se obtiene de AWS Config AWS Security Hub, o de ambos.
10. Estado de la comprobación de conformidad	El número total de problemas que se notificaron directamente desde AWS Security Hub o desde ambos. AWS Config

Tabla de evidencias

Puede utilizar la tabla Evidencias para consultar las evidencias que se incluyen en la carpeta de evidencias. En esta tabla también puede realizar las siguientes acciones:

- Revisar evidencia individual: para ver los detalles de cualquier evidencia, elija su nombre siguiendo el un hipervínculo de la columna Hora.
- Añadir evidencia a un informe de evaluación: para incluir una evidencia, selecciónela y elija Añadir al informe de evaluación.
- Eliminar evidencia de un informe de evaluación: para excluir una evidencia, selecciónela y elija Eliminar del informe de evaluación.

- Añadir una evidencia manual: para obtener instrucciones, consulte Añadir evidencia manual AWS Audit Manager.

En esta tabla puede revisar la siguiente información:

Nombre	Descripción
Tiempo	Especifica cuándo se recopiló la evidencia. También sirve como nombre de la evidencia. Se representa en formato de tiempo universal coordinado (UTC).
Comprobación de conformidad	Estado de la evaluación de la evidencia incluida en la categoría comprobación de conformidad. • En el caso de las evidencias recopiladas de Security Hub, se informará directamente de un resultado Aprobado o No aprobado directamente desde Security Hub. • En el caso de las pruebas recopiladas AWS Config, se informa directamente de los resultados conformes o no conformes. AWS Config • Si se muestra No aplicable, esto indica que no tiene Security Hub activado AWS Config o que no lo tiene activado, o que las pruebas provienen de un tipo de fuente de datos diferente.
Evidencia por tipo	Tipo de evidencias. • Las pruebas de verificación de conformidad se recopilan de AWS Config o AWS Security Hub. • Las evidencias de Actividad de los usuarios se recopilan de AWS CloudTrail. • Las pruebas de los datos de configuración se recopilan a partir de las llamadas a la API a otras Servicios de AWS. • Las evidencias manuales son aquellas que se añaden manualmente.
Origen de datos	Origen de datos desde el que se recopila las evidencias.

Nombre	Descripción
Nombre de evento	Nombre del evento que invocó la recopilación de evidencias.
Origen del evento	El director del servicio que identifica lo relevante Servicio de AWS para el evento.
Recursos	Número de recursos que se evaluaron al recopilar las evidencias.
Selección del informe de evaluación	Indica si la evidencia se incluye en el informe de evaluación. • Para incluir evidencias, selecciónelas y elija Agregar al informe de evaluación. • Para excluirlas, seleccione la evidencia o evidencias y elija Eliminar del informe de evaluación.

Pasos a seguir a continuación

Cuando desee explorar las evidencias individuales de una carpeta, siga los pasos que se indican en Revisar la evidencia en AWS Audit Manager. Esta página le guiará por los detalles de las evidencias y le explicará cómo interpretar la información que aparece.

Recursos adicionales

- Para obtener soluciones a los problemas de evidencias en Audit Manager, consulte Solución de problemas de evaluación y recopilación de pruebas.

Revisar la evidencia en AWS Audit Manager

Cuando necesite revisar una determinada evidencia, siga las instrucciones que se indican en esta página. Encontrará los detalles de las evidencias organizados en varias secciones.

Contenido

- Requisitos previos
- Procedimiento
  - Resumen

- Atributos
- Recursos incluidos
- Recursos adicionales

Requisitos previos

En el siguiente procedimiento se da por sentado que ha creado previamente al menos una evaluación. Si aún no ha creado ninguna evaluación, no verá ningún resultado si sigue estos pasos.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Tenga en cuenta que una evaluación tarda hasta 24 horas en empezar a recopilar evidencias automatizadas. Si la evaluación aún no tiene ninguna evidencia, no se mostrará ningún resultado si sigue estos pasos.

Procedimiento

Apertura y revisión de una página de detalles de una evidencia

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Evaluaciones y luego una evaluación.
3. En la página de evaluación, seleccione la pestaña Controles, desplácese hacia abajo hasta llegar a la tabla Controles y, a continuación, elija un control.
4. En la página de control, seleccione la pestaña Carpetas de evidencias.
5. En la tabla Carpetas de evidencias, seleccione el nombre de una carpeta de evidencias.
6. Elija el nombre de la evidencia en la columna Hora para abrir la página de datos de la evidencia.
7. Revise los detalles de la evidencia con la siguiente información como referencia.

Secciones de una página de detalles de una evidencia

- Resumen
- Atributos
- Recursos incluidos

Resumen

Puede utilizar la sección Resumen para consultar una descripción general de la evidencia.

En esta sección puede revisar la siguiente información:

Nombre	Descripción
1. ID de evidencia	Identificador único de la evidencia.
2. Fecha y hora	Fecha y hora en que se recopiló la evidencia. Se representa en formato de hora universal coordinada (UTC).
3. Comprobación de conformidad	Estado de la evaluación de la evidencia de comprobación de conformidad. • Como prueba recopilada AWS Security Hub, los resultados aprobados o rechazados se notifican directamente desde AWS Security Hub. • En el caso de las pruebas recopiladas AWS Config, se informa directamente de los resultados conformes o no conformes. AWS Config • Si aparece No aplicable, esto indica una de estas dos opciones. O no lo tienes AWS Security Hub o lo tienes AWS Config activado. O bien, la evidencia procede de otro origen de datos.
4. Asignación de origen de datos	Palabra clave de asignación que se usó para recopilar la evidencia.
5. Data source type (Tipo de origen de datos)	Tipo de origen de datos desde el que se recopiló la evidencia.

Nombre	Descripción
6. ID de cuenta	Lo Cuenta de AWS que está asociado con las pruebas.
7. ID de IAM	Usuario o rol correspondiente, si procede.
8. Evaluación	Nombre de la evaluación asociada a la evidencia.
9. Controlar	Nombre del control asociado a la evidencia.
10. Nombre de la carpeta de evidencias	Nombre de la carpeta de evidencias que incluye la evidencia.
11. Incluir en el informe de evaluación	El conmutador que le permite incluir o excluir la evidencia del informe de evaluación.

Atributos

Puede utilizar la tabla Atributos para ver en detalle los atributos de la evidencia.

En esta tabla puede revisar la siguiente información:

Nombre	Descripción
Nombre de atributo	Clave del atributo.
Valor	El valor del atributo. En algunos casos, se proporciona un enlace a un archivo JSON con más información.

Recursos incluidos

Puede utilizar la tabla Recursos incluidos para consultar los recursos que se evaluaron para generar esta evidencia.

En esta sección puede revisar la siguiente información:

Nombre	Descripción
ARN	El Nombre de recurso de Amazon (ARN) del recurso. Es posible que el ARN no esté disponible para todos los tipos de evidencia.
Conformidad de recursos	Estado de evaluación del recurso. • Como prueba recopilada AWS Security Hub, los resultado s aprobados o rechazados se notifican directamente desde Security Hub. • En el caso de las pruebas recopiladas AWS Config, se informa directamente de los resultados conformes o no conformes. AWS Config • Si se muestra No aplicable, esto indica que no tienes o no tienes AWS Config activado Security Hub, o que las pruebas provienen de una fuente de datos diferente.
Valor	Más información sobre la evaluación de recursos. En algunos casos, se proporciona un enlace a un archivo JSON con más información.

Recursos adicionales

- Para obtener soluciones a los problemas de evidencias en Audit Manager, consulte Solución de problemas de evaluación y recopilación de pruebas.

Edición de una evaluación en AWS Audit Manager

Es posible que se encuentre en situaciones en las que necesite editar sus evaluaciones existentes AWS Audit Manager. Es posible que el alcance de la auditoría haya cambiado y sea necesario actualizar lo Cuentas de AWS incluido en la evaluación. O bien, es posible que necesite revisar la lista de responsables de la auditoría asignados a la evaluación debido a cambios de personal. En esos casos, puede editar las evaluaciones activas y realizar los ajustes necesarios sin interrumpir la recopilación de evidencias.

En la página siguiente se describen los pasos para editar los detalles de las evaluaciones, cambiar las Cuentas de AWS incluidas, actualizar los responsables de la auditoría y revisar y guardar los cambios.

Requisitos previos

En el procedimiento siguiente se da por sentado que ha creado previamente al menos una evaluación y que se encuentra en un estado activo.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para editar una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Tareas

- Paso 1: editar los detalles de la evaluación
- Paso 2: Editar Cuentas de AWS el alcance
- Paso 3: editar los responsables de la auditoría
  - Audite los permisos del propietario
- Paso 4: revisar y guardar

Paso 1: editar los detalles de la evaluación

Siga estos pasos para editar los detalles de su evaluación.

Pasos para editar una evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Evaluaciones.
3. Seleccione una evaluación y elija Editar.
4. En Editar detalles de la evaluación, edite los detalles de la evaluación según sea necesario.
5. Elija Siguiente.

Paso 2: Editar Cuentas de AWS el alcance

En este paso puede cambiar las cuentas que se incluyen en la evaluación. Audit Manager puede admitir hasta 200 cuentas en el ámbito de una evaluación y 250 cuentas de miembros únicos en todas las evaluaciones.

Para editar Cuentas de AWS el alcance

1. Para añadir una Cuenta de AWS, selecciona la casilla de verificación situada junto al nombre de la cuenta.
2. Para eliminar una Cuenta de AWS, desactive la casilla de verificación situada junto al nombre de la cuenta.
3. Elija Siguiente.

> **Note**
>
> Para editar el administrador delegado de Audit Manager, consulte Cambio de un administrador delegado.

Paso 3: editar los responsables de la auditoría

En este paso puede cambiar los responsables de auditoría que se incluyen en la evaluación.

Pasos para editar los responsables de las auditorías

1. Para añadir un responsable de auditoría, seleccione la casilla de verificación situada junto al nombre de la cuenta.
2. Para eliminar un responsable de auditoría, elimine la selección de la casilla de verificación situada junto al nombre de la cuenta.
3. Elija Siguiente.

Audite los permisos del propietario

Se adjunta la siguiente política para todos los propietarios de auditorías de una evaluación.

Audit Manager los `placeholder text` reemplaza por sus identificadores de cuenta y recurso antes de adjuntar la política.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditOwner",
            "Effect": "Allow",
            "Principal": {
                "AWS": "Principal for user/role who are the audit owners of the
 Assessment"
            },
            "Action": [
                "auditmanager:GetAssessment",
                "auditmanager:UpdateAssessment",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:UpdateAssessmentStatus",
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:DeleteAssessment",
                "auditmanager:GetChangeLogs",
                "auditmanager:GetEvidenceFoldersByAssessment",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder",
                "auditmanager:BatchCreateDelegationByAssessment",
                "auditmanager:BatchDeleteDelegationByAssessment",
                "auditmanager:AssociateAssessmentReportEvidenceFolder",
                "auditmanager:BatchAssociateAssessmentReportEvidence",
                "auditmanager:BatchDisassociateAssessmentReportEvidence",
                "auditmanager:CreateAssessmentReport",
                "auditmanager:DeleteAssessmentReport",
                "auditmanager:DisassociateAssessmentReportEvidenceFolder",
                "auditmanager:GetAssessmentReportUrl"
            ],
            "Resource": [
                "arn:aws:auditmanager:us-
east-1:account_ID:assessment/assessment_ID",
                "arn:aws:auditmanager:us-
east-1:account_ID:assessment/assessment_ID/*"
            ]
        }
```

```
    ]
}
```

Paso 4: revisar y guardar

Revise de la información de su evaluación. Para modificar la información de un paso, seleccione Editar. Cuando haya terminado de editar, elija Guardar cambios para confirmarlos.

Tras completar las modificaciones, los cambios en la evaluación entrarán en vigor a las 00:00 UTC del día siguiente.

Pasos a seguir a continuación

Si ya no necesita recopilar evidencias para un determinado control de evaluación, puede cambiar el estado de dicho control. Para obtener instrucciones, consulte Cambiar el estado de un control de evaluación en AWS Audit Manager.

Si ya no necesita recopilar evidencias para la evaluación completa, puede cambiar el estado de la evaluación a Inactivo. Para obtener instrucciones, consulte Cambiar el estado de una evaluación a inactiva en AWS Audit Manager.

Recursos adicionales

- Para obtener soluciones a los problemas de evaluación en Audit Manager, consulte Solución de problemas de evaluación y recopilación de pruebas.
- Para obtener información sobre por qué ya no es posible editar los servicios incluidos, consulte No puedo editar los servicios incluidos en el ámbito de mi evaluación en la sección Solución de problemas de esta guía.

Añadir evidencia manual AWS Audit Manager

Audit Manager puede recopilar automáticamente evidencias para muchos controles. Sin embargo, algunos controles pueden exigir evidencias que no se pueden recopilar automáticamente. En estos casos, puede añadir manualmente sus propias evidencias.

Considere los siguientes ejemplos:

- Algunos controles se refieren al suministro de registros físicos (como firmas) o a eventos que no se generan en la nube (como observaciones y entrevistas). En estos casos, puede añadir manualmente los archivos como evidencia. Por ejemplo, si un control requiere información sobre la estructura corporativa, puede subir una copia del organigrama de su empresa como evidencia manual.
- Algunos controles representan preguntas de evaluación del riesgo de los proveedores. Las preguntas de evaluación de riesgos pueden requerir documentación como prueba (por ejemplo un organigrama) o quizá solo tenga que introducir una respuesta de texto simple, como una lista de puestos de trabajo. En este último caso, puede responder a la pregunta y guardar su respuesta como evidencia manual.

También puede utilizar la característica de carga manual para gestionar las evidencias de varios entornos. Si su empresa utiliza un modelo de nube híbrida o multinube, puede cargar evidencias desde su entorno en las instalaciones, desde entornos alojados en la nube o sus aplicaciones de SaaS. Esto le permite organizar sus evidencias independientemente de su procedencia, almacenándolas dentro de la estructura de una evaluación de Audit Manager, en la que cada prueba se asignará a un control específico.

Puntos clave

Cuando se trata de añadir evidencias manuales a las evaluaciones en Audit Manager, tiene tres métodos entre los que elegir.

1. Importación de un archivo desde Amazon S3: este método es ideal cuando tiene archivos de evidencias almacenados en un bucket de S3, como, por ejemplo, documentación, informes u otros artefactos que Audit Manager no puede recopilar automáticamente. Al importar estos archivos directamente desde S3, puede integrar sin problemas esta evidencia manual con la evidencia recopilada automáticamente.
2. Carga de un archivo desde el navegador: si tiene archivos de evidencias almacenados localmente en su equipo o red, puede cargarlos manualmente en Audit Manager mediante este método. Este enfoque es particularmente útil cuando necesita incluir registros físicos, como documentos o imágenes escaneados, que no están disponibles en formato digital en su AWS entorno.
3. Adición de texto de formato libre como evidencia: en algunos casos, la evidencia que debe proporcionar no tiene el formato de archivo, sino más bien se trata de una explicación o respuesta de texto. Este método le permite introducir texto de formato libre directamente en Audit Manager.

Esto puede ser especialmente útil al responder a las preguntas de evaluación de riesgos para proveedores.

Recursos adicionales

- Para obtener instrucciones sobre cómo añadir evidencia manual a un control de evaluación, consulte los siguientes recursos. Tenga en cuenta que solo puede utilizar un método a la vez.
  - Importación de archivos de evidencias manuales desde Amazon S3
  - Carga de archivos de evidencias manuales desde el navegador
  - Introducción de respuestas de texto de formato libre como evidencia manual
- Para saber qué formatos de archivo puede usar, consulte Formatos de archivo compatibles con las evidencias manuales.
- Para obtener más información sobre los distintos tipos de evidencia en Audit Manager, consulte evidence en la sección Conceptos y terminología de esta guía.
- Para obtener ayuda sobre la solución de problemas, consulte No puedo subir pruebas manuales a un control.

Importación de archivos de evidencias manuales desde Amazon S3

Puede importar archivos de evidencias de forma manual desde un bucket de Amazon S3 a la evaluación. Esto le permite complementar las evidencias recopiladas automáticamente con materiales de apoyo adicionales.

Requisitos previos

- El tamaño máximo admitido para un único archivo de evidencia manual es de 100 MB.
- Debe utilizar uno de los Formatos de archivo compatibles con las evidencias manuales.
- Cada uno de ellos Cuenta de AWS puede cargar manualmente hasta 100 archivos de pruebas a un control cada día. Si supera este límite diario no podrá realizar ninguna carga manual adicional en ese control. Si necesita cargar una gran cantidad de evidencias manuales en un solo control, hágalo en lotes durante varios días.
- Cuando un control está inactivo, no es posible añadir evidencias manuales a ese control. Para añadir una evidencia manual, primero debe cambiar el estado del control al estado En revisión o Revisado.

- Asegúrese de que su identidad de IAM tenga los permisos adecuados para administrar una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Puede importar un archivo con la consola de Audit Manager, la API de Audit Manager o AWS Command Line Interface (AWS CLI).

AWS console

> **Important**
>
> Le recomendamos encarecidamente que nunca importe información de identificación personal (PII) ni confidencial como evidencia manual. Esto incluye, entre otros, números de la Seguridad Social, direcciones, números de teléfono o cualquier otra información que podría usarse para identificar a una persona.

Importación de un archivo desde S3 en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Evaluaciones y luego una evaluación.
3. Seleccione la pestaña Controles, desplácese hacia abajo hasta llegar a Conjuntos de controles y, a continuación, elija un control.
4. En la pestaña Carpetas de evidencias, elija Añadir evidencia manual y, a continuación, Importar archivo de S3.
5. En la página siguiente, ingrese el URI de S3 de la evidencia. Para encontrar el URI de S3, vaya al objeto en la consola de Amazon S3 y elija Copiar URI de S3.
6. Seleccione Cargar.

AWS CLI

> **Important**
>
> Le recomendamos encarecidamente que nunca importe información de identificación personal (PII) ni confidencial como evidencia manual. Esto incluye, entre otros, números de la Seguridad Social, direcciones, números de teléfono o cualquier otra información que podría usarse para identificar a una persona.

En el siguiente procedimiento, *`placeholder text`* sustitúyalo por su propia información.

Para importar un archivo de S3 en el AWS CLI

1. Ejecute el comando `list-assessments` para ver una lista de sus evaluaciones.

   ```
   aws auditmanager list-assessments
   ```

   En la respuesta, busque la evaluación de la que desee cargar la evidencia o evidencias y anote sus identificadores.

2. Ejecute el comando `get-assessment` y especifique el ID de evaluación del primer paso.

   ```
   aws auditmanager get-assessment --assessment-
   id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
   ```

   En la respuesta, busque el conjunto de controles y el control en el que desea cargar las pruebas y tome nota de sus componentes IDs.

3. Use el comando `batch-import-evidence-to-assessment-control` con estos parámetros:

   - `--assessment-id`: utilice el ID de evaluación del primer paso.
   - `--control-set-id`: utilice el ID del conjunto de controles del segundo paso.
   - `--control-id`: utilice el ID de control del segundo paso.
   - `--manual-evidence`: utilice `s3ResourcePath` como tipo de evidencia manual y especifique el URI de S3 de la evidencia. Para encontrar el URI de S3, vaya al objeto en la consola de Amazon S3 y elija Copiar URI de S3.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://
amzn-s3-demo-bucket/EXAMPLE-FILE.extension
```

Audit Manager API

> **Important**
>
> Le recomendamos encarecidamente que nunca importe información de identificación personal (PII) ni confidencial como evidencia manual. Esto incluye, entre otros, números de la Seguridad Social, direcciones, números de teléfono o cualquier otra información que podría usarse para identificar a una persona.

Importación de un archivo desde S3 mediante la API

1. Llame a la operación `ListAssessments` para ver una lista de sus evaluaciones. En la respuesta, busque la evaluación de la que desee cargar la evidencia o evidencias y anote sus identificadores.
2. Llame a la operación `GetAssessment` y especifique el ID de evaluación del primer paso. En la respuesta, busca el conjunto de controles y el control en el que quieres cargar las pruebas y toma nota de sus componentes IDs.
3. Realice una llamada a la operación `BatchImportEvidenceToAssessmentControl` con los parámetros siguientes:
   - `assessmentId`: utilice el ID de evaluación del primer paso.
   - `controlSetId`: utilice el ID del conjunto de controles del segundo paso.
   - `controlId`: utilice el ID de control del segundo paso.
   - `manualEvidence`: utilice `s3ResourcePath` como tipo de evidencia manual y especifique el URI de S3 de la evidencia. Para encontrar el URI de S3, vaya al objeto en la consola de Amazon S3 y elija Copiar URI de S3.

Para obtener más información, consulte cualquiera de los enlaces del procedimiento anterior en la Referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos AWS SDKs.

Pasos a seguir a continuación

Una vez que haya añadido y revisado la evidencia de la evaluación, puede generar un informe de evaluación. Para obtener más información, consulte Preparación de un informe de evaluación en AWS Audit Manager.

Recursos adicionales

Para saber qué formatos de archivo puede usar, consulte Formatos de archivo compatibles con las evidencias manuales.

Carga de archivos de evidencias manuales desde el navegador

Puede cargar los archivos de evidencias manualmente desde el navegador en la evaluación de Audit Manager. Esto le permite complementar las evidencias recopiladas automáticamente con materiales de apoyo adicionales.

Requisitos previos

- El tamaño máximo admitido para un único archivo de evidencia manual es de 100 MB.
- Debe utilizar uno de los Formatos de archivo compatibles con las evidencias manuales.
- Cada uno de ellos Cuenta de AWS puede cargar manualmente hasta 100 archivos de pruebas a un control cada día. Si supera este límite diario no podrá realizar ninguna carga manual adicional en ese control. Si necesita cargar una gran cantidad de evidencias manuales en un solo control, hágalo en lotes durante varios días.
- Cuando un control está inactivo, no es posible añadir evidencias manuales a ese control. Para añadir una evidencia manual, primero debe cambiar el estado del control al estado En revisión o Revisado.
- Asegúrese de que su identidad de IAM tenga los permisos adecuados para administrar una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Puede cargar un archivo con la consola de Audit Manager, la API de Audit Manager o AWS Command Line Interface (AWS CLI).

AWS console

> **Important**
>
> Le recomendamos encarecidamente que nunca cargue información de identificación personal (PII) ni confidencial como evidencia manual. Esto incluye, entre otros, números de la Seguridad Social, direcciones, números de teléfono o cualquier otra información que podría usarse para identificar a una persona.

Carga de un archivo desde el navegador a la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Evaluaciones y luego una evaluación.
3. En la pestaña Controles, desplácese hacia abajo hasta llegar a Conjuntos de controles y, a continuación, elija un control.
4. En la pestaña Carpetas de evidencias, seleccione Añadir evidencia manual.
5. Elija Cargar archivo desde el navegador.
6. Seleccione el archivo en el cual desee cargar los archivos.
7. Seleccione Cargar.

AWS CLI

> **Important**
>
> Le recomendamos encarecidamente que nunca cargue información de identificación personal (PII) ni confidencial como evidencia manual. Esto incluye, entre otros, números de la Seguridad Social, direcciones, números de teléfono o cualquier otra información que podría usarse para identificar a una persona.

En el siguiente procedimiento, *placeholder text* sustitúyalo por su propia información.

Para cargar un archivo desde su navegador en el AWS CLI

1. Ejecute el comando `list-assessments` para ver una lista de sus evaluaciones.

```
aws auditmanager list-assessments
```

   En la respuesta, busque la evaluación de la que desee cargar la evidencia o evidencias y anote sus identificadores.

2. Ejecute el comando `get-assessment` y especifique el ID de evaluación del primer paso.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   En la respuesta, busque el conjunto de control y el control en el que desea cargar las pruebas y tome nota de sus componentes IDs.

3. Ejecute el comando `get-evidence-file-upload-url` y especifique el archivo o archivos que desea cargar.

```
aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
```

   En la respuesta, busque y anote la URL prefirmada y `evidenceFileName`.

4. Use la URL prefirmada del tercer paso para cargar el archivo o archivos desde su navegador. Esta acción carga los archivos en Amazon S3, donde se guardan como un objeto que se puede agregar a los controles de evaluación. En el siguiente paso haga referencia al objeto recién creado mediante el parámetro `evidenceFileName`.

> **Note**
>
> Cuando carga un archivo mediante una URL prefirmada, Audit Manager protege y almacena sus datos mediante el cifrado del lado del servidor con AWS Key Management Service. Para ello, debe utilizar el encabezado `x-amz-server-side-encryption` en su solicitud cuando utilice la URL prefirmada para cargar el archivo. Si utiliza un cliente gestionado AWS KMS key en la Configuración de los ajustes del cifrado de datos configuración de Audit Manager, asegúrese de incluir también el `x-amz-server-side-encryption-aws-kms-key-id` encabezado en la solicitud.

Si el encabezado `x-amz-server-side-encryption-aws-kms-key-id` no figura en la solicitud, Amazon S3 asumirá que se quiere utilizar la Clave administrada de AWS.
Para obtener más información, consulte Protección de datos mediante cifrado del lado del servidor con AWS Key Management Service claves (SSE-KMS) en la Guía del usuario de Amazon Simple Storage Service.

5. Use el comando `batch-import-evidence-to-assessment-control` con estos parámetros:

   - `--assessment-id`: utilice el ID de evaluación del primer paso.
   - `--control-set-id`: utilice el ID del conjunto de controles del segundo paso.
   - `--control-id`: utilice el ID de control del segundo paso.
   - `--manual-evidence`: utilice `evidenceFileName` como tipo de evidencia manual y especifique el nombre del archivo de la evidencia o evidencias a partir del tercer paso.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet
 --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence
 evidenceFileName=fileName.extension
```

Audit Manager API

> **Important**
> Le recomendamos encarecidamente que nunca cargue información de identificación personal (PII) ni confidencial como evidencia manual. Esto incluye, entre otros, números de la Seguridad Social, direcciones, números de teléfono o cualquier otra información que podría usarse para identificar a una persona.

Carga de un archivo desde el navegador mediante la API

1. Llame a la operación `ListAssessments`. En la respuesta, busque la evaluación de la que desee cargar la evidencia o evidencias y anote sus identificadores.

2. Llame a la `GetAssessment` operación y especifique el `assessmentId` del primer paso. En la respuesta, busque el conjunto de controles y el control en el que desea cargar las pruebas y tome nota de ellos. IDs
3. Llame a la operación `GetEvidenceFileUploadUrl` y especifique el `fileName` que desea cargar. En la respuesta, busque y anote la URL prefirmada y `evidenceFileName`.
4. Use la URL prefirmada del tercer paso para cargar el archivo o archivos desde su navegador. Esta acción carga los archivos en Amazon S3, donde se guardan como un objeto que se puede agregar a los controles de evaluación. En el siguiente paso haga referencia al objeto recién creado mediante el parámetro `evidenceFileName`.

> **Note**
>
> Cuando carga un archivo mediante una URL prefirmada, Audit Manager protege y almacena sus datos mediante el cifrado del lado del servidor con AWS Key Management Service. Para ello, debe utilizar el encabezado `x-amz-server-side-encryption` en su solicitud cuando utilice la URL prefirmada para cargar el archivo. Si utiliza un cliente gestionado AWS KMS key en la Configuración de los ajustes del cifrado de datos configuración de Audit Manager, asegúrese de incluir también el `x-amz-server-side-encryption-aws-kms-key-id` encabezado en la solicitud. Si el encabezado `x-amz-server-side-encryption-aws-kms-key-id` no figura en la solicitud, Amazon S3 asumirá que se quiere utilizar la Clave administrada de AWS.
> Para obtener más información, consulte Protección de datos mediante cifrado del lado del servidor con AWS Key Management Service claves (SSE-KMS) en la Guía del usuario de Amazon Simple Storage Service.

5. Realice una llamada a la operación `BatchImportEvidenceToAssessmentControl` con los parámetros siguientes:
   - `assessmentId`: utilice el ID de evaluación del primer paso.
   - `controlSetId`: utilice el ID del conjunto de controles del segundo paso.
   - `controlId`: utilice el ID de control del segundo paso.
   - `manualEvidence`: utilice `evidenceFileName` como tipo de evidencia manual y especifique el nombre del archivo de la evidencia o evidencias a partir del tercer paso.

Para obtener más información, consulte cualquiera de los enlaces del procedimiento anterior en la Referencia de la API de AWS Audit Manager . Incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos. AWS SDKs

Pasos a seguir a continuación

Una vez que haya recopilado y revisado la evidencia de la evaluación, puede generar un informe de evaluación. Para obtener más información, consulte Preparación de un informe de evaluación en AWS Audit Manager.

Recursos adicionales

Para saber qué formatos de archivo puede usar, consulte Formatos de archivo compatibles con las evidencias manuales.

Introducción de respuestas de texto de formato libre como evidencia manual

Puede proporcionar contexto e información complementaria adicionales para un control de evaluación. Para ello, introduzca un texto de formato libre y guarde ese texto como evidencia. Esto le permite documentar manualmente los detalles que no se capturan mediante la recopilación automática de evidencias.

Por ejemplo, puede usar Audit Manager para crear controles personalizados que representen preguntas en un cuestionario de evaluación de riesgos para proveedores. En ese caso, el nombre de cada control es una pregunta específica que solicita información sobre la postura de seguridad y conformidad de su organización. Para registrar su respuesta a una determinada pregunta de evaluación de riesgos para proveedores, puede introducir una respuesta de texto y guardarla como evidencia manual para el control.

Requisitos previos

- Cuando un control está inactivo, no es posible añadir evidencias manuales a ese control. Para añadir una evidencia manual, primero debe cambiar el estado del control al estado En revisión o Revisado.
- Asegúrese de que su identidad de IAM tenga los permisos adecuados para administrar una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son:

AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Puede introducir las respuestas de texto con la consola de Audit Manager, la API de Audit Manager o AWS Command Line Interface (AWS CLI).

AWS console

> **Important**
>
> Le recomendamos encarecidamente que nunca introduzca información de identificación personal (PII) ni confidencial como evidencia manual. Esto incluye, entre otros, números de la Seguridad Social, direcciones, números de teléfono o cualquier otra información que podría usarse para identificar a una persona.

Introducción de una respuesta de texto en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Evaluaciones y luego una evaluación.
3. Seleccione la pestaña Controles, desplácese hacia abajo hasta llegar a Conjuntos de controles y, a continuación, elija un control.
4. En la pestaña Carpetas de evidencias, seleccione Añadir evidencia manual.
5. Elija Introducir respuesta de texto.
6. Aparecerá una ventana emergente que aparece: introduzca su respuesta en formato de texto plano.
7. Elija Confirmar.

AWS CLI

> **Important**
>
> Le recomendamos encarecidamente que nunca introduzca información de identificación personal (PII) ni confidencial como evidencia manual. Esto incluye, entre otros, números

de la Seguridad Social, direcciones, números de teléfono o cualquier otra información que podría usarse para identificar a una persona.

En el siguiente procedimiento, *`placeholder text`* sustitúyalo por su propia información.

Para introducir una respuesta de texto en el AWS CLI

1. Ejecute el comando `list-assessments`.

```
aws auditmanager list-assessments
```

   En la respuesta, busque la evaluación de la que desee cargar la evidencia o evidencias y anote sus identificadores.

2. Ejecute el comando `get-assessment` y especifique el ID de evaluación del primer paso.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   En la respuesta, busque el conjunto de controles y el control en los que desea cargar las pruebas y tome nota de ellos IDs.

3. Use el comando `batch-import-evidence-to-assessment-control` con estos parámetros:

   - `--assessment-id`: utilice el ID de evaluación del primer paso.
   - `--control-set-id`: utilice el ID del conjunto de controles del segundo paso.
   - `--control-id`: utilice el ID de control del segundo paso.
   - `--manual-evidence`: utilice `textResponse` como evidencia manual e introduzca el texto que desee guardar como evidencia manual.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter
 text here"
```

Audit Manager API

> **Important**
>
> Le recomendamos encarecidamente que nunca introduzca información de identificación personal (PII) ni confidencial como evidencia manual. Esto incluye, entre otros, números de la Seguridad Social, direcciones, números de teléfono o cualquier otra información que podría usarse para identificar a una persona.

Introducción de una respuesta de texto mediante la API

1. Llame a la operación `ListAssessments`. En la respuesta, busque la evaluación de la que desee cargar la evidencia o evidencias y anote sus identificadores.
2. Llame a la `GetAssessment` operación y especifique el `assessmentId` del primer paso. En la respuesta, busque el conjunto de controles y el control en los que desea cargar las pruebas y tome nota de sus componentes IDs.
3. Realice una llamada a la operación `BatchImportEvidenceToAssessmentControl` con los parámetros siguientes:
   - `assessmentId`: utilice el ID de evaluación del primer paso.
   - `controlSetId`: utilice el ID del conjunto de controles del segundo paso.
   - `controlId`: utilice el ID de control del segundo paso.
   - `manualEvidence`: utilice `textResponse` como evidencia manual e introduzca el texto que desee guardar como evidencia manual.

Para obtener más información, consulte cualquiera de los enlaces del procedimiento anterior en la Referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos AWS SDKs.

Pasos a seguir a continuación

Una vez que haya recopilado y revisado la evidencia de la evaluación, puede generar un informe de evaluación. Para obtener más información, consulte Preparación de un informe de evaluación en AWS Audit Manager.

Formatos de archivo compatibles con las evidencias manuales

En la siguiente tabla se enumeran y describen los tipos de archivos que puede cargar como evidencia manual. Para cada tipo de archivo, se incluyen también las extensiones de los archivos compatibles.

Tipo de archivo	Descripción	Extensiones de archivos compatibles
Compresión o archivos	Archivos comprimidos GNU Zip y archivos comprimidos ZIP	`.gz`, `.zip`
Documento	Archivos de documento s comunes, como PDFs archivos de Microsoft Office	`.doc`, `.docx`, `.pdf`, `.ppt`, `.pptx`, `.xls`, `.xlsx`
Imagen	Archivos de imágenes y gráficos	`.jpeg`, `.jpg`, `.png`, `.svg`
Texto	Otros archivos de texto no binarios, como documento s de texto sin formato y archivos de lenguaje de marcado	`.cer`, `.csv`, `.html`, `.jmx`, `.json`, `.md`, `.out`, `.rtf`, `.txt`, `.xml`, `.yaml`, `.yml`

Recursos adicionales

Revise las páginas siguientes para obtener información sobre las diferentes formas que tiene a su disposición para añadir sus propias evidencias a un control de evaluación.

- Importación de archivos de evidencias manuales desde Amazon S3
- Carga de archivos de evidencias manuales desde el navegador
- Introducción de respuestas de texto de formato libre como evidencia manual

Preparación de un informe de evaluación en AWS Audit Manager

Una vez que haya recopilado y revisado la evidencia de la evaluación, puede generar un informe de evaluación. Los informes de evaluación resumen la evaluación e incluyen enlaces a un conjunto organizado de carpetas que incluyen evidencias relacionadas.

Puntos clave

Las evidencias recién recopiladas no aparecen automáticamente en los informes de evaluación. Esto significa que puede controlar las evidencias que desea incluir en el informe. Una vez que haya seleccionado la evidencia que desea incluir, puede generar el informe de evaluación final para compartirlo con los auditores.

Cuando genera un informe de evaluación, se coloca en el bucket de S3 que haya elegido como destino del informe de evaluación. También puede descargar el informe de evaluación en el centro de descargas de Audit Manager.

Recursos adicionales

Para obtener más información sobre los informes de evaluación y cómo administrarlos, consulte los siguientes recursos.

- Añadir evidencias a los informes de evaluación
- Eliminación de evidencias de un informe de evaluación
- Generación de informes de evaluación
- Descarga de un informe de evaluación
- Navegación por un informe de evaluación y exploración de su contenido
- Validación de un informe de evaluación
- Eliminación de una ejecución de evaluación
- Generación de informes de evaluación a partir de los resultados de búsqueda del buscador de evidencias
- Configuración del destino del informe de evaluación predeterminado
- Solución de problemas con el informe de evaluación

Añadir evidencias a los informes de evaluación

Para poder generar un informe de evaluación, debe agregar al menos un elemento de evidencia a dicho informe. Puede añadir una carpeta de evidencias completa o elementos de evidencia específicos desde una carpeta.

Procedimiento

Para incluir evidencias en un informe de evaluación, siga estos pasos.

Pasos para añadir evidencias a un informe de evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Evaluaciones y luego una evaluación.
3. En la pestaña Controles, desplácese hacia abajo hasta la tabla Conjuntos de controles y elija un control con las evidencias que desee incluir en el informe de evaluación.
4. Elija cómo quiere añadir las evidencias a su informe de evaluación.

   a. Para añadir carpetas de evidencias completas, desplácese hacia abajo hasta llegar a Carpetas de evidencias, seleccione la que desee añadir y, a continuación, elija Añadir al informe de evaluación.

   > **Tip**
   >
   > Si no ve la carpeta que busca, cambie el filtro desplegable a Siempre. Tenga en cuenta que por defecto se muestran las carpetas de los últimos siete días.
   > Si la opción Añadir al informe de evaluación aparece atenuada, significa que la carpeta de evidencias ya se ha añadido a dicho informe.

   b. Para añadir evidencias específicas, elija una carpeta de evidencias y ábrala. Seleccione uno o más elementos de la lista y, a continuación, elija Añadir al informe de evaluación.

   > **Tip**
   >
   > Si la opción Añadir al informe de evaluación aparece atenuada, asegúrese de haber seleccionado la casilla de verificación situada junto a las evidencias e inténtelo de nuevo.

5. Una vez añadidas las evidencias al informe de evaluación, aparecerá un aviso de confirmación en verde. Seleccione Ver evidencias en el informe de evaluación para ver las evidencias que se incluirán en su informe de evaluación.

- También puede consultarlas desde la pestaña de selección del informe de evaluación si vuelve a la evaluación.

Pasos a seguir a continuación

Si desea eliminar evidencias de un informe de evaluación, consulte Eliminación de evidencias de un informe de evaluación.

Cuando desee generar un informe de evaluación, consulte Generación de informes de evaluación.

Recursos adicionales

Para encontrar respuestas a preguntas y problemas comunes, consulte Solución de problemas con el informe de evaluación en la sección Solución de problemas de esta guía.

Eliminación de evidencias de un informe de evaluación

Siga los pasos que se detallan a continuación para eliminar evidencias de un informe de evaluación. Puede eliminar carpetas de evidencias completas o elementos de evidencia específicos de una carpeta.

Procedimiento

Pasos para eliminar evidencias de un informe de evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Evaluaciones y, a continuación, el nombre de la evaluación o evaluaciones que desee abrir.
3. En la pestaña Controles, desplácese hacia abajo hasta llegar a la tabla Conjuntos de controles y elija el nombre del control o controles que desee abrir.
4. Elija cómo desea eliminar las evidencias del informe de evaluación.
   a. Para eliminar una carpeta de evidencias completa, desplácese hacia abajo hasta llegar a Carpetas de evidencias. A continuación, seleccione la carpeta que desee eliminar y elija Eliminar del informe de evaluación.

> **Tip**
>
> Si no ve la carpeta que busca, cambie el filtro desplegable a Siempre. Tenga en cuenta que por defecto se muestran las carpetas de los últimos siete días.
> Si Eliminar del informe de evaluación aparece atenuada, significa que la carpeta de evidencias ya se ha eliminado del informe de evaluación.

b. Para eliminar evidencias específicas, elija una carpeta de evidencias y ábrala. Seleccione uno o más elementos de la lista y, a continuación, elija Eliminar del informe de evaluación.

> **Tip**
>
> Si la opción Eliminar del informe de evaluación aparece atenuada, asegúrese de haber seleccionado la casilla de verificación situada junto a las evidencias e inténtelo de nuevo.

5. Una vez añadidas las evidencias al informe de evaluación, aparecerá un aviso de confirmación en verde. Seleccione Ver evidencias en el informe de evaluación para ver las evidencias que se incluirán en su informe de evaluación.
   - También puede consultarlas desde la pestaña de selección del informe de evaluación si vuelve a la evaluación.

Pasos a seguir a continuación

Cuando desee generar un informe de evaluación, consulte Generación de informes de evaluación.

Recursos adicionales

Para encontrar respuestas a preguntas y problemas comunes, consulte Solución de problemas con el informe de evaluación en la sección Solución de problemas de esta guía.

Generación de informes de evaluación

Cuando desee generar el informe de evaluación, siga estos pasos.

Requisitos previos

Para poder generar un informe de evaluación, debe agregar al menos un elemento de evidencia a dicho informe. Puede añadir una carpeta de evidencias completa o elementos de evidencia individuales desde una carpeta.

Para asegurarse de que su informe de evaluación se haya generado correctamente, consulte nuestro Consejos de configuración para el destino de su informe de evaluación.

Procedimiento

Para generar un informe de evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación de la izquierda, elija Evaluaciones.
3. Elija el nombre de la evaluación para la que desea generar un informe de evaluación.
4. Vaya a la pestaña de selección del informe de evaluación y, a continuación, Generar informe de evaluación.

> **Tip**
>
> Si la opción Generar informe de evaluación aparece atenuada, significa que aún no se ha añadido ninguna prueba a dicho informe.

5. En la ventana emergente, agregue un nombre y una descripción para el informe de evaluación y revise los detalles del mismo.
6. Elija Generar informe de evaluación y espere unos minutos mientras se genera.
7. Busque y descargue su informe de evaluación desde el centro de descargas de la consola Audit Manager.
   - También puede ir al bucket de S3 de destino del informe de evaluación y descargar el informe de evaluación desde allí.

Pasos a seguir a continuación

Después de generar el informe de evaluación, puede seguir con otros pasos. Descúbralos a continuación:

- Busque y descargue su informe de evaluación: aprenda cómo descargar su informe de evaluación desde el centro de descargas o desde Amazon S3.
- Explore su informe de evaluación: aprenda cómo navegar por un informe de evaluación y conozca su contenido.
- Valide su informe de evaluación: aprenda a utilizar la operación de la ValidateAssessmentReportIntegrityAPI para validar su informe de evaluación.
- Eliminar un informe de evaluación no deseado: aprenda cómo eliminar informes que no necesite del centro de descargas o de Amazon S3.
- Generar informes de evaluación a partir del buscador de evidencias: aprenda a generar informes de evaluación a partir de los resultados de búsqueda del buscador de evidencias.

Recursos adicionales

Para encontrar respuestas a preguntas y problemas comunes, consulte Solución de problemas con el informe de evaluación en la sección Solución de problemas de esta guía.

Cambiar el estado de un control de evaluación en AWS Audit Manager

Puede cambiar el estado de un control de evaluación en la evaluación activa. La actualización del estado de un control le permite realizar un seguimiento de su progreso e indicar cuándo lo ha revisado, manteniendo la evaluación organizada y up-to-date.

Requisitos previos

En el procedimiento siguiente se da por sentado que ha creado previamente una evaluación, y su estado actual es Activo.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para administrar una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Puede actualizar el estado de un control de evaluación con la consola de Audit Manager, la API de Audit Manager o AWS Command Line Interface (AWS CLI).

> **Note**
>
> El cambio de un estado de control a revisado es definitivo. Tras establecer el estado de un control como revisado, ya no podrá cambiar el estado de ese control ni volver a un estado anterior.

Audit Manager console

Cambio del estado de un control de evaluación en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Evaluaciones.
3. Seleccione el nombre de la evaluación que desee consultar y ábrala.
4. En la página de evaluación, seleccione la pestaña Controles, desplácese hacia abajo hasta llegar a la tabla conjuntos de controles y, a continuación, elija el nombre del control que desea abrir.
5. Elija Actualizar estado del control en la parte superior derecha de la página y luego un estado:

Estado	Descripción
En revisión	Seleccione este estado si aún no ha revisado el control.
Revisado	Seleccione este estado si ha terminado de revisar las evidencias para este control y desea seguir recopilando o añadiendo evidencias.
Inactivo	Seleccione este estado si desea dejar de recopilar evidencias automatizadas para este control.

6. Elija Actualizar estado del control para confirmar su elección.

AWS CLI

Para cambiar el estado de un control de evaluación en el AWS CLI

1. Ejecute el comando list-assessments.

```
aws auditmanager list-assessments
```

   Obtendrá una lista de evaluaciones. Busque la evaluación que incluya el control que desea actualizar y tome note de su identificador.

2. Ejecute el comando get-assessment y especifique el identificador de la evaluación del primer paso.

   En el siguiente ejemplo, *placeholder text* sustitúyalo por su propia información.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g
```

   En la respuesta, busque el control que desea actualizar y tome nota de su identificador y del identificador del conjunto de controles.

3. Ejecute el update-assessment-controlcomando y especifique los siguientes parámetros:

   - `--assessment-id`: evaluación a la que pertenece el control.
   - `--control-set-id`: conjunto de controles al que pertenece el control.
   - `--control-id`: control que desea actualizar.
   - `--control-status`: establezca este valor en `UNDER_REVIEW`, `REVIEWED` o `INACTIVE`.

   En el siguiente ejemplo, sustituya el *placeholder text* por su propia información.

```
aws auditmanager update-assessment-control --assessment-
id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g --control-set-id "My control set" --
control-id 2b3c4d5e-2b3c-2b3c-2b3c-2b3c4d5f6g7h --control-status REVIEWED
```

Audit Manager API

Cambio del estado de un control de evaluación con la API

1. Utilice la operación ListAssessments.

   En la respuesta, busque la evaluación que incluya el control que desea actualizar y tome note de su identificador.

2. Utilice la GetAssessmentoperación y especifique el ID de evaluación del paso 1.

   En la respuesta, busque el control que desea actualizar y tome nota de su identificador y del identificador del conjunto de controles.

3. Utilice la UpdateAssessmentControloperación y especifique los siguientes parámetros:

   - `assessmentId`: evaluación a la que pertenece el control.
   - `controlSetId`: conjunto de controles al que pertenece el control.
   - `controlId`: control que desea actualizar.
   - `controlStatus`: establezca este valor en `UNDER_REVIEW`, `REVIEWED` o `INACTIVE`.

Para obtener más información sobre estas operaciones de la API, consulte cualquiera de los enlaces del procedimiento anterior en la Referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos AWS SDKs.

Pasos a seguir a continuación

Cuando desee cambiar el estado de la evaluación, consulte Cambiar el estado de una evaluación a inactiva en AWS Audit Manager.

Cambiar el estado de una evaluación a inactiva en AWS Audit Manager

Si ya no necesita recopilar pruebas para una evaluación, puede cambiar el estado de la evaluación a Inactiva. Cuando el estado de una evaluación cambia a inactiva, la evaluación deja de recopilar pruebas. Como resultado, ya no se le cobrará nada por esa evaluación.

Además de detener la recopilación de evidencias, Audit Manager realiza los siguientes cambios en los controles de las evaluaciones inactivas:

- Todos los conjuntos de controles cambian al estado revisado.
- Todos los controles que están en revisión cambian al estado revisado.
- Los delegados de la evaluación inactiva ya no pueden ver ni editar sus controles ni conjuntos de controles.

Requisitos previos

En el procedimiento siguiente se da por sentado que ha creado previamente una evaluación, y su estado actual es Activo.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para administrar una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Puede actualizar el estado de una evaluación con la consola de Audit Manager, la API de Audit Manager o AWS Command Line Interface (AWS CLI).

> **Warning**
>
> Esta acción es irreversible. Le recomendamos que proceda con cautela y se asegure de marcar estas evaluaciones como inactivas. Cuando una evaluación está inactiva, tiene acceso de solo lectura a su contenido. Esto significa que aún puede ver las pruebas recopiladas anteriormente y generar informes de evaluación. Sin embargo, no puede editar la evaluación inactiva, agregar comentarios ni cargar ninguna prueba manual.

Audit Manager console

Cambio del estado de una evaluación a Inactivo en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.

2. En el panel de navegación, elija Evaluaciones.
3. Seleccione el nombre de la evaluación que desee consultar y ábrala.
4. En la esquina superior derecha de la página, elija Actualizar estado de la evaluación y, luego, Inactivo.
5. Seleccione Actualizar estado en la ventana emergente para confirmar que desea cambiar el estado a inactivo.

Los cambios en las evaluaciones y sus controles surten efecto después de un minuto aproximadamente.

AWS CLI

Para cambiar el estado de una evaluación a inactiva en el AWS CLI

1. En primer lugar, identifique la evaluación o evaluaciones que desea actualizar. Para ello, ejecute el comando list-assessments.

```
aws auditmanager list-assessments
```

   Obtendrá una lista de evaluaciones. Busque la evaluación o evaluaciones que desee desactivar y tome nota de su identificador.

2. A continuación, ejecute el update-assessment-statuscomando y especifique los siguientes parámetros:

   - `--assessment-id`, para determinar qué evaluación o evaluaciones desea desactivar.
   - `--status`: establezca este valor en `INACTIVE`.

   En el siguiente ejemplo, sustituya el *`placeholder text`* por su propia información.

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111 --status INACTIVE
```

Los cambios en las evaluaciones y sus controles surten efecto después de un minuto aproximadamente.

Audit Manager API

Cambio del estado de una evaluación a Inactivo con la API

1. Utilice la ListAssessmentsoperación para buscar la evaluación que desee desactivar y anote el identificador de la evaluación.
2. Utilice la UpdateAssessmentStatusoperación y especifique los siguientes parámetros:
   - ID de evaluación, para determinar qué evaluación o evaluaciones desea desactivar.
   - estatus: defina este valor como `INACTIVE`.

Los cambios en las evaluaciones y sus controles surten efecto después de un minuto aproximadamente.

Para obtener más información sobre estas operaciones de la API, consulte cualquiera de los enlaces del procedimiento anterior en la Referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos AWS SDKs.

Pasos a seguir a continuación

Cuando tenga la certeza de que ya no necesita la evaluación con el estado Inactivo, elimínela para limpiar el entorno de Audit Manager. Para obtener instrucciones, consulte Eliminar una evaluación en AWS Audit Manager.

Eliminar una evaluación en AWS Audit Manager

Cuando ya no necesite una evaluación, puede eliminarla del entorno de Audit Manager. Esto le permite limpiar su espacio de trabajo y centrarse en las evaluaciones que son pertinentes para sus tareas y prioridades actuales.

> **Tip**
>
> Si su objetivo es reducir los costos, considere la posibilidad de cambiar el estado de la evaluación a inactiva en lugar de eliminarla. Esta acción detiene la recopilación de pruebas

y establece que la evaluación esté en un estado de solo lectura en el que puede revisar las pruebas recopiladas anteriormente. Las evaluaciones inactivas no generan ningún cargo.

Requisitos previos

En el siguiente procedimiento se da por sentado que ha creado previamente una evaluación.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para eliminar una evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Puede eliminar evaluaciones utilizando la consola de Audit Manager, la API de Audit Manager o la AWS Command Line Interface (AWS CLI).

> **Warning**
>
> Esta acción elimina de manera permanente la evaluación y todas las pruebas recopiladas en ella. No puede recuperar estos datos. Por ello, le recomendamos que proceda con cuidado y que esté seguro de que desea eliminar la evaluación.

Audit Manager console

Eliminación de una evaluación en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Evaluaciones.
3. Seleccione las evaluaciones que desee eliminar y elija Eliminar.

AWS CLI

Para eliminar una evaluación en el AWS CLI

1. Primero identifique las evaluaciones que desee eliminar. Para ello, ejecute el comando list-assessments.

   ```
   aws auditmanager list-assessments
   ```

   Obtendrá una lista de evaluaciones. Busque la evaluación o evaluaciones que desee eliminar y tome nota de su identificador.
2. A continuación, ejecute el comando delete-assessment y especifique el `--assessment-id` de la evaluación o evaluaciones que desea eliminar.

   En el siguiente ejemplo, *`placeholder text`* sustitúyalo por su propia información.

   ```
   aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-
   EXAMPLE11111
   ```

Audit Manager API

Eliminación de una evaluación con la API

1. Utilice la ListAssessmentsoperación para buscar la evaluación que desee eliminar.

   En la respuesta, busque y anote el ID de evaluación.
2. Utilice la DeleteAssessmentoperación y especifique el ID de evaluación de la evaluación que desee eliminar.

Para más información sobre estas operaciones de la API, consulte cualquiera de los enlaces anteriores en la referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos. AWS SDKs

Recursos adicionales

Para obtener información sobre la retención de datos en Audit Manager, consulte Eliminación de datos de Audit Manager.

Delegaciones en AWS Audit Manager

A medida que avance en el proceso de evaluación AWS Audit Manager, es posible que se encuentre con situaciones en las que necesite la ayuda de expertos en la materia para revisar y validar las pruebas recopiladas. Aquí es donde entra en juego el concepto de delegaciones.

Puntos clave

Las delegaciones permiten a los responsables de las auditorías asignar conjuntos de controles específicos a los delegados, es decir, personas con conocimientos especializados en las áreas pertinentes. Al utilizar la característica de delegación, puede asegurarse de que el personal adecuado evalúe detenidamente las evidencias de cada control. Esto le ayuda a agilizar el proceso de revisión y a mejorar la precisión y fiabilidad generales de las evaluaciones. Ya sea que necesite orientación para interpretar las evidencias técnicas, aclarar los requisitos de conformidad u obtener información más exhaustiva sobre dominios específicos, las delegaciones le permiten colaborar eficazmente con expertos en la materia.

En líneas generales, el proceso de delegación es el siguiente:

1. El propietario de la auditoría elige un conjunto de controles en su evaluación y lo delega para su revisión.
2. El delegado revisa esos controles y sus evidencias, y devuelve el conjunto de controles al propietario de la auditoría una vez finalizado.
3. Se notifica al propietario de la auditoría que la revisión ha finalizado y comprueba los controles revisados para comprobar si hay comentarios del delegado.

> **Note**
>
> Y Cuenta de AWS puede ser el propietario de una auditoría o un delegado en otros ámbitos Regiones de AWS.

Recursos adicionales

Utilice las siguientes secciones de este capítulo para obtener más información sobre cómo administrar las tareas de delegación en AWS Audit Manager.

- Descripción de las distintas tareas de delegación para los responsables de auditorías
  - Delegar un conjunto de controles para su revisión en AWS Audit Manager
  - Encuentra y revisa las delegaciones que has enviado AWS Audit Manager
  - Eliminar las delegaciones completadas en AWS Audit Manager
- Descripción de las distintas tareas de delegación para los delegados
  - Ver las notificaciones de las solicitudes de delegación entrantes
  - Revisión del conjunto de control delegado y su evidencia relacionada
  - Adición de comentarios sobre un control durante la revisión de un conjunto de controles
  - Marcar un control como se describe en AWS Audit Manager
  - Envío de conjuntos de controles revisados a la persona responsable de la auditoría

Descripción de las distintas tareas de delegación para los responsables de auditorías

Como propietario de una auditoría AWS Audit Manager, usted es responsable de gestionar las evaluaciones y garantizar el cumplimiento en su organización. Aunque tenga experiencia en gobernanza, riesgo y conformidad, es posible que en ocasiones tenga preguntas o necesite la ayuda de expertos en la materia para revisar e interpretar determinados controles o evidencias técnicos. Aquí es donde resulta útil la característica de delegación de Audit Manager.

Puntos clave

La creación de una delegación le permite asignar conjuntos de control dentro de una evaluación a otros usuarios de Audit Manager (conocidos como delegados) que tienen conocimientos especializados o experiencia técnica en áreas pertinentes. A continuación, estos delegados pueden revisar los conjuntos de controles asignados, analizar las evidencias recopiladas, proporcionar comentarios o evidencias adicionales, si es necesario, y actualizar el estado de los controles individuales.

El proceso de delegación optimiza la revisión y la validación de los controles al sacar partido de la experiencia colectiva de su organización. Garantiza que el personal más cualificado evalúe detenidamente cada control, lo que mejora la precisión y la fiabilidad de las evaluaciones.

Recursos adicionales

En las siguientes secciones se le guiará a través de las diferentes tareas asociadas a la administración de las delegaciones como responsable de una auditoría. Esto incluye cómo delegar los conjuntos de controles, realizar un seguimiento del estado de las delegaciones y administrar las delegaciones completadas. Al utilizar las delegaciones de forma eficaz, puede colaborar con expertos en la materia, sacar partido de sus conocimientos especializados y mantener un proceso de auditoría completo y con fundamento en Audit Manager.

- Delegar un conjunto de controles para su revisión en AWS Audit Manager
- Encuentra y revisa las delegaciones que has enviado AWS Audit Manager
- Eliminar las delegaciones completadas en AWS Audit Manager

Delegar un conjunto de controles para su revisión en AWS Audit Manager

Cuando necesite la ayuda de un experto en la materia, puede elegir la Cuenta de AWS que desea que le ayude y delegarle un conjunto de controles para que los revise.

Delega permisos

La siguiente política se adjunta a un delegado en el que se delega el conjunto de controles.

Audit Manager los *`placeholder text`* reemplaza por sus identificadores de cuenta y recurso antes de adjuntar la política.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Delegate",
            "Effect": "Allow",
            "Principal": {
                "AWS": "Principal for user/role who is delegated a Control Set of
 the Assessment"
            },
            "Action": [
```

```
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder"
            ],
            "Resource": "arn:aws:auditmanager:us-
east-1:account_ID:assessment/assessment_ID/controlSet/control_set_ID"
        }
    ]
}
```

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para crear una delegación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: Permitir a los usuarios acceso de administrador total a AWS Audit Manager y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Puede utilizar uno de los procedimientos siguientes para delegar un conjunto de controles.

Delegación de un conjunto de controles desde una página de evaluación

Para delegar un conjunto de controles de la página de evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Evaluaciones.
3. Seleccione el nombre de la evaluación que contiene el conjunto de controles que desea delegar.
4. En la página de evaluación, seleccione la pestaña Controles. Aquí se muestra el resumen del estado del control y la lista de controles de la evaluación.
5. Seleccione un conjunto de controles y elija Delegar el conjunto de controles.
6. En Selección de delegados, se muestra una lista de usuarios y roles. Elija un usuario o un rol, o utilice la barra de búsqueda para buscar uno.
7. En Detalles de la delegación, revise el nombre del conjunto de controles y el nombre de la evaluación.

8. (Opcional) En Comentarios, agregue un comentario con instrucciones para ayudar al delegado a realizar su tarea de revisión. No incluya información confidencial en su comentario.
9. Elija el conjunto de controles delegados.
10. Un cartel verde confirma que el conjunto de controles se ha delegado correctamente. Seleccione Ver delegación para ver la solicitud de delegación. También puede ver sus delegaciones en cualquier momento seleccionando Delegaciones en el panel de navegación izquierdo de la AWS Audit Manager consola.

Delegar un conjunto de controles desde la página de delegaciones

Para delegar un conjunto de controles desde la página de delegaciones

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Delegación.
3. En la página de delegaciones, elija Crear delegación.
4. En Elegir el conjunto de evaluación y control, especifique la evaluación y el conjunto de controles que desea delegar.
5. En Selección de delegados, verá una lista de usuarios y funciones. Elija un usuario o un rol, o utilice la barra de búsqueda para buscar uno.
6. (Opcional) En Comentarios, agregue un comentario con instrucciones para ayudar al delegado a realizar su tarea de revisión. No incluya información confidencial en el alias de la cuenta.
7. Elija Crear delegación.
8. Un cartel verde confirma que el conjunto de controles se ha delegado correctamente. Seleccione Ver delegación para ver la solicitud de delegación. También puede ver sus delegaciones en cualquier momento seleccionando Delegaciones en el panel de navegación izquierdo de la AWS Audit Manager consola.

Al delegar la revisión de un conjunto de controles, el delegado recibe una notificación y, a continuación, puede empezar a revisarlo. Este proceso que siguen los delegados se describe en Descripción de las distintas tareas de delegación para los delegados.

Pasos a seguir a continuación

Para revisitar la delegación más adelante, consulte Encuentra y revisa las delegaciones que has enviado AWS Audit Manager.

Encuentra y revisa las delegaciones que has enviado AWS Audit Manager

Puede acceder a una lista de las delegaciones en cualquier momento. Para ello, seleccione Delegaciones en el panel de navegación izquierdo de Audit Manager. En la página de delegaciones se incluye una lista de las delegaciones activas y completadas.

Cuando se complete una delegación, recibirá una notificación en Audit Manager. También puede recibir comentarios con observaciones del delegado. En el siguiente procedimiento se explica cómo comprobar las delegaciones en Audit Manager una vez completadas y cómo ver los comentarios que el delegado haya podido dejar.

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver una delegación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: Permitir a los usuarios acceso de administrador total a AWS Audit Manager y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Siga estos pasos para buscar y revisar las delegaciones que ha creado anteriormente.

Para ver una delegación completa y comprobar si hay comentarios

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Delegaciones.
3. Revise la página Delegaciones, que incluye una tabla con la siguiente información:

Nombre	Descripción
Delegado a	El Cuenta de AWS conjunto de control en el que ha delegado.
Fecha	Fecha en la que delegó el conjunto de controles.
Estado	Estado actual de la delegación.
Evaluación	Nombre de la evaluación con un enlace a la página de detalles de la evaluación.

Nombre	Descripción
Conjunto de controles	Nombre del conjunto de controles cuya revisión se ha delegado.

4. Busque el conjunto de evaluación y control que el delegado revisó y le envió y elija el nombre de la evaluación para abrirla.
5. En la pestaña Controles de la página de detalles de la evaluación, desplácese hacia abajo hasta la tabla de conjuntos de controles.
6. En Controles agrupados por conjunto de controles, busque el nombre del conjunto de controles que ha delegado.
7. Expanda el nombre del conjunto de controles para mostrar sus controles y elija el nombre de un control para abrir la página de detalles del control.
8. Seleccione la pestaña Comentarios para ver los comentarios agregados por el delegado a ese control en particular.
9. Cuando tenga la certeza de que se ha completado la revisión de un conjunto de controles, seleccione el conjunto de controles y elija Completar la revisión del conjunto de controles.

> **Important**
>
> Audit Manager recopila evidencias de forma continua. Como resultado, es posible que se recopilen nuevas evidencias adicionales después de que el delegado complete la revisión de un control.
> Si solo desea utilizar las evidencias revisadas en sus informes de evaluación, puede consultar la marca temporal revisada por el control para determinar cuándo se revisó la evidencia. Esta marca de tiempo se encuentra en el Pestaña del registro de cambios de la página de detalles del control. A continuación, puede utilizar esta marca de tiempo para identificar las evidencias que va a añadir a sus informes de evaluación.

Pasos a seguir a continuación

Para eliminar una delegación una vez completada y que ya no necesite más, consulte Eliminar las delegaciones completadas en AWS Audit Manager.

Eliminar las delegaciones completadas en AWS Audit Manager

Puede haber circunstancias en las que cree una delegación, pero más adelante ya no necesite ayuda para revisar ese conjunto de controles. Cuando esto ocurra, puede eliminar una delegación activa en Audit Manager. También puede eliminar las delegaciones completadas que ya no desee que aparezcan en la página de delegaciones.

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para eliminar una delegación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: Permitir a los usuarios acceso de administrador total a AWS Audit Manager y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Para eliminar una delegación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Delegaciones.
3. En la página Delegaciones, seleccione la delegación que desee cancelar y, a continuación, elija Eliminar delegación.
4. En la ventana emergente que aparece, elija Eliminar para confirmar su elección.

Descripción de las distintas tareas de delegación para los delegados

Como delegado AWS Audit Manager, usted desempeña un papel importante a la hora de apoyar a los responsables de la auditoría durante el proceso de evaluación. Si bien los responsables de las auditorías son los encargados de administrar las evaluaciones y garantizar la conformidad general, a veces pueden necesitar la ayuda de expertos en la materia para revisar e interpretar evidencias técnicas específicas que queden fuera de sus áreas de especialización. En estos situaciones, sus conocimientos y habilidades se vuelven inestimables.

Puntos clave

La característica de delegación permite a los responsables de la auditoría asignarle la revisión de conjuntos de controles específicos, sacando partido de sus conocimientos técnicos o empresariales

especializados. Este método colaborativo no solo mejora la precisión y la fiabilidad de las evaluaciones, sino que también optimiza el proceso de revisión, lo que permite a los responsables de la auditoría centrarse en sus responsabilidades principales y, al mismo tiempo, centrar sus esfuerzos en las áreas en las que su experiencia es más valiosa.

Como delegado, es posible que reciba solicitudes de los responsables de la auditoría para revisar las evidencias asociadas a conjuntos de controles asignados. Puede ayudar a los propietarios de la auditoría revisando los conjuntos de controles y sus evidencias relacionadas, añadiendo comentarios, cargando evidencias adicionales y actualizando el estado de cada control que revise.

> **Note**
>
> Los propietarios de las auditorías delegan conjuntos de control específicos para su revisión, no para realizar evaluaciones completas. En consecuencia, los delegados tienen acceso limitado a las evaluaciones. Los delegados pueden revisar las evidencias, añadir comentarios, cargar evidencias manuales y actualizar el estado de control de cada uno de los controles del conjunto de controles. Para obtener más información acerca de los roles y sus permisos en Audit manager, consulte Políticas recomendadas para los usuarios de AWS Audit Manager.

Recursos adicionales

En las siguientes secciones puede obtener más información sobre las tareas asociadas a la administración de las delegaciones como delegado. Esto incluye cómo ver las solicitudes de delegación entrantes, revisar los conjuntos de controles asignados, proporcionar comentarios y evidencias adicionales y devolver los controles revisados al responsable de la auditoría.

- Ver las notificaciones de las solicitudes de delegación entrantes
- Revisión del conjunto de control delegado y su evidencia relacionada
- Adición de comentarios sobre un control durante la revisión de un conjunto de controles
- Marcar un control como se describe en AWS Audit Manager
- Envío de conjuntos de controles revisados a la persona responsable de la auditoría

Ver las notificaciones de las solicitudes de delegación entrantes

Cuando el propietario de una auditoría solicita su ayuda para revisar un conjunto de controles, usted recibe una notificación que le informa del conjunto de controles que le han delegado.

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver notificaciones en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: Permitir a los usuarios acceso de administrador total a AWS Audit Manager y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Ver las notificaciones

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Notificaciones.
3. En la página de Notificaciones, revise la lista de conjuntos de controles que se le han delegado para su revisión. La tabla incluye la siguiente información:

Nombre	Descripción
Fecha	Fecha en la que se ha delegado el conjunto de controles.
Evaluación	Nombre de la evaluación asociada al conjunto de controles.
Conjunto de controles	Nombre del conjunto de controles.
Origen	Usuario o rol que le ha delegado el conjunto de controles.
Descripción	Instrucciones proporcionadas por el responsable de la auditoría.

> **Tip**
>
> También puede suscribirse a un tema de SNS para recibir alertas por correo electrónico cuando se le delegue un conjunto de controles para su revisión. Para obtener más información, consulte Notificaciones en AWS Audit Manager.

Pasos a seguir a continuación

Cuando tenga todo listo para empezar a revisar los controles que se le han delegado, consulte Revisión del conjunto de control delegado y su evidencia relacionada.

Revisión del conjunto de control delegado y su evidencia relacionada

Puede ayudar a los propietarios de la auditoría revisando los conjuntos de controles que le han delegado.

Puede examinar estos controles y la evidencia relacionada con ellos para determinar si es necesaria alguna acción adicional. Esta acción adicional podría incluir cargar manualmente evidencias adicionales para mostrar el cumplimiento o dejar un comentario en el que se detallen las medidas correctivas que ha seguido.

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver un conjunto de controles en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: Permitir a los usuarios acceso de administrador total a AWS Audit Manager y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Revisión de un conjunto de controles

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Notificaciones.
3. En la página Notificaciones, puede ver una lista de conjuntos de controles que se le han delegado. Identifique el conjunto de controles que desea revisar y elija el nombre de la evaluación relacionada para abrir la página de detalles de la evaluación.
4. En la pestaña Controles de la página de detalles de la evaluación, desplácese hacia abajo hasta la tabla de Conjuntos de controles.
5. En la columna Controles agrupados por conjunto, expanda el nombre de un conjunto de controles para mostrar sus controles.
6. Elija el nombre de un control para abrir la página de detalles del control.

7. (Opcional) Seleccione Actualizar el estado del control para cambiar el estado del control. Mientras la revisión esté en curso, puede marcar el estado como En revisión.
8. Revise la información sobre el control en las pestañas Carpetas de evidencias, Detalles, Orígenes de datos, Comentarios y Registro de cambios.
   - Para obtener información sobre cada una de estas pestañas y cómo comprender los datos que en ellas se incluyen, consulte Revisar un control de evaluación en AWS Audit Manager.

Revisión de la evidencia de un control

1. En la página de detalles del control, seleccione la pestaña Carpetas de pruebas.
2. Navegue hasta la tabla de Carpetas de evidencias, donde se mostrará una lista de las carpetas que incluyen las evidencias de ese control. Estas carpetas se organizan y nombran en función de la fecha en que se recopilaron las evidencias.
3. Elija el nombre de una carpeta de evidencias para abrirla. A continuación, revise un resumen de todas las evidencias reunidas en esa fecha.
   - Este resumen incluye el número total de problemas de control de conformidad que se notificaron directamente desde AWS Security Hub AWS Config, o ambos.
   - Para obtener más detalles sobre esta información, consulte Revisión de una carpeta de evidencias en AWS Audit Manager.
4. En la página de resumen de la carpeta de pruebas, navegue hasta la tabla de Pruebas. En la columna Hora, seleccione la evidencia que desea abrir.
5. Revise los detalles de la evidencia.
   - Para obtener más detalles sobre esta información, consulte Revisar la evidencia en AWS Audit Manager.

Pasos a seguir a continuación

En algunos casos, es posible que deba proporcionar evidencias adicionales para demostrar la conformidad. En estos casos, puede cargar las evidencias manualmente. Para obtener instrucciones, consulte Añadir evidencia manual AWS Audit Manager.

Si desea dejar comentarios sobre uno o varios de los controles que se le han delegado, consulte Adición de comentarios sobre un control durante la revisión de un conjunto de controles.

Adición de comentarios sobre un control durante la revisión de un conjunto de controles

Puede añadir comentarios a cualquier control que revise. El propietario de la auditoría puede ver estos comentarios.

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para añadir comentarios a un control de evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: Permitir a los usuarios acceso de administrador total a AWS Audit Manager y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Para añadir un comentario a un control

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Notificaciones.
3. En la página de Notificaciones, revise la lista de conjuntos de controles que se le han delegado.
4. Busque el conjunto de controles que incluye el control para el que desea dejar un comentario y elija el nombre de la evaluación relacionada para abrirla.
5. Seleccione la pestaña Controles, desplácese hacia abajo hasta la tabla de Conjuntos de controles y, a continuación, seleccione el nombre de un control para abrirlo.
6. Seleccione la pestaña Comentarios.
7. En Enviar comentarios, introduzca su comentario en el cuadro de texto.
8. Seleccione Enviar comentario para añadir su comentario. Su comentario aparece en la sección de Comentarios anteriores de la página, junto con cualquier otro comentario relacionado con este control.

Pasos a seguir a continuación

Cuando haya terminado de revisar el control, siga los pasos que se indican en Marcar un control como se describe en AWS Audit Manager.

Marcar un control como se describe en AWS Audit Manager

Puede indicar el progreso de la revisión actualizando el estado de los controles individuales de un conjunto de controles.

Cambiar el estado del control es opcional. Sin embargo, le recomendamos que cambie el estado de cada control a Revisado a medida que complete la revisión de ese control. Independientemente del estado de cada control individual, puede volver a enviar los controles al propietario de la auditoría.

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para actualizar el estado de un control de evaluación en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: Permitir a los usuarios acceso de administrador total a AWS Audit Manager y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Para marcar un control como revisado

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Notificaciones.
3. En la página de Notificaciones, revise la lista de conjuntos de controles que se le han delegado.
4. Busque el conjunto de controles que desea marcar como revisado y elija el nombre de la evaluación relacionada para abrirla.
5. En la pestaña Controles de la página de detalles de la evaluación, desplácese hacia abajo hasta la tabla de Conjuntos de controles.
6. En la columna Controles agrupados por conjunto, expanda el nombre de un conjunto de controles para mostrar sus controles.
7. Elija el nombre de un control para abrir la página de detalles del control.
8. Seleccione Actualizar el estado del control y cambie el estado a Revisado.
9. En la ventana emergente que aparece, seleccione Actualizar el estado del control para confirmar que ha terminado de revisar el control.

Pasos a seguir a continuación

Para completar el proceso de delegación, consulte Envío de conjuntos de controles revisados a la persona responsable de la auditoría.

Envío de conjuntos de controles revisados a la persona responsable de la auditoría

Tras revisar el conjunto de controles, añadir comentarios o evidencias adicionales y actualizar el estado de los controles individuales, se llega a un paso importante: devolver el conjunto de controles revisado al responsable de la auditoría. El envío del conjunto de controles revisado supone la finalización de las tareas delegadas y permite al responsable de la auditoría incorporar sus ideas y recomendaciones a la evaluación general.

Requisitos previos

Asegúrese de que su identidad de IAM tiene los permisos adecuados para volver a enviar el conjunto de control revisado al propietario de la auditoría. AWS Audit Manager Dos políticas sugeridas que conceden estos permisos son: Permitir a los usuarios acceso de administrador total a AWS Audit Manager y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Siga estos pasos para enviar el conjunto de controles al responsable de la auditoría.

Para enviar un conjunto de control revisado al propietario de la auditoría

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Notificaciones.
3. Revise la lista de conjuntos de controles que se le han delegado. Busque el conjunto de controles que desea devolver al propietario de la auditoría y elija el nombre de la evaluación relacionada.
4. Desplácese hacia abajo hasta la tabla de Conjunto de controles, seleccione el conjunto de controles que desee enviar al propietario de la auditoría y, a continuación, seleccione Enviar para su revisión.
5. En la ventana emergente que aparece, puede añadir comentarios antes de seleccionar Enviar para revisión.

Informes de evaluación

En un informe de evaluación se resumen las evidencias seleccionadas que se recopilaron para una evaluación. También contiene enlaces a archivos PDF con datos sobre cada evidencia. El contenido específico, la organización y la nomenclatura de un informe de evaluación dependen de los parámetros que elija al generar el informe.

Los informes de evaluación le ayudan a seleccionar y recopilar las evidencias pertinentes para su auditoría. Sin embargo, no evalúan la conformidad de las evidencias en sí. En su lugar, Audit Manager se limita a proporcionar los datos de la evidencia seleccionada como un resultado que puede compartir con su auditor.

Contenido

- Descripción de la estructura de carpetas del informe de evaluación
- Navegación por un informe de evaluación
- Revisión de la secciones de un informe de evaluación
  - Portada
  - Página de información general
    - Resumen de informe
    - Resumen de la evaluación
  - Página del índice
  - Página de control
    - Resumen de control
    - Evidencia recopilada
  - Página de resumen de evidencias
  - Página de información sobre evidencias
- Validación de un informe de evaluación
- Recursos adicionales

Descripción de la estructura de carpetas del informe de evaluación

Al descargar un informe de evaluación, Audit Manager genera una carpeta zip. Contiene su informe de evaluación y los archivos de evidencias relacionados en subcarpetas anidadas.

La carpeta zip se estructura como se indica a continuación:

- Carpeta de evaluación (ejemplo: `myAssessmentName-a1b2c3d4`): carpeta raíz.
  - Carpeta de informes de evaluación (ejemplo:`reportName-a1b2c3d4e5f6g7`): subcarpeta en la que se encuentran los AssessmentReportSummary archivos.pdf, digest.txt y README.txt.
    - Carpeta de evidencias por control (ejemplo: `controlName-a1b2c3d4e5f6g`): subcarpeta que agrupa los archivos de evidencias según el control relacionado.
      - Carpeta de evidencias por origen de datos (ejemplo: `CloudTrail`, `Security Hub`): subcarpeta que agrupa los archivos de evidencias por tipo de origen de datos.
        - Carpeta de evidencias por fecha (ejemplo: `2022-07-01`): subcarpeta que agrupa los archivos de evidencias por fecha de recopilación de evidencias.
          - Archivos de evidencias: archivos que contienen datos sobre las evidencias individuales.

Navegación por un informe de evaluación

Para empezar, abra la carpeta zip y baje un nivel hasta la carpeta del informe de evaluación. Aquí encontrará el informe de evaluación en PDF y el archivo README.txt.

Puede revisar el archivo README.txt para comprender la estructura y el contenido de la carpeta zip. También proporciona información de referencia sobre las convenciones de nomenclatura de cada archivo. Esta información puede ayudarle a navegar directamente a una subcarpeta o a un archivo de evidencias si está buscando un elemento específico.

De lo contrario, para buscar evidencias y encontrar la información que necesita, abra el PDF del informe de evaluación. Esto le proporciona una visión general de alto nivel del informe y un resumen de la evaluación a partir de la cual se creó el informe.

A continuación, utilice el índice (TOC) para explorar el informe. Puede elegir cualquier control hipervinculado del índice para ir directamente a un resumen de ese control.

Cuando esté listo para revisar los datos de las evidencias de un control, puede hacerlo eligiendo el nombre de la evidencia con hipervínculos. En el caso de las evidencias automatizadas, el hipervínculo abre un nuevo archivo PDF con datos sobre esas evidencias. En el caso de las evidencias manuales, el hipervínculo lleva al bucket de S3 que contiene las evidencias.

> **Tip**
>
> La ruta de navegación situada en la parte superior de cada página muestra su ubicación actual en el informe de evaluación a medida que examina los controles y las evidencias. Seleccione el índice con el hiperenlace para volver al índice en cualquier momento.

Revisión de la secciones de un informe de evaluación

Utilice la siguiente información para obtener más datos sobre cada sección de un informe de evaluación.

> **Note**
>
> Si ve un guion (-) junto a cualquiera de los atributos de las siguientes secciones, esto indica que el valor de ese atributo es nulo o que no existe ningún valor.

- Portada
- Página de información general
- Página del índice
- Página de control
- Página de resumen de evidencias
- Página de información sobre evidencias

Portada

La portada incluye el nombre del informe de evaluación. También muestra la fecha y la hora en que se generó el informe, junto con el ID de cuenta del usuario que lo generó.

La portada tiene el siguiente formato. Audit Manager la *placeholders* reemplaza por la información relevante para su informe.

```
Assessment report name
Report generated on MM/DD/YYYY at HH:MM:SS AM/PM UCT by AccountID
```

Página de información general

La página de información general consta de dos partes: un resumen del informe en sí y un resumen de la evaluación sobre la que se informa.

Resumen de informe

En esta sección se resume el informe de evaluación.

Nombre	Descripción
Nombre del informe	El nombre del informe.
Descripción	Descripción que introduce el responsable de la auditoría al generar el informe.
Fecha de generación	Fecha en que se generó el informe. Se representa en formato de tiempo universal coordinado (UTC).
Total de controles incluidos	Número de controles que se incluyen en el informe y que han recopilado evidencias. Se trata de un subconjunto del número total de controles de la evaluación.
Cuentas de AWS incluido	El número de los Cuentas de AWS que están incluidos en el informe y han recopilado pruebas. Se trata de un subconjunto del número total de participantes Cuentas de AWS en la evaluación.
Selección del informe de evaluación	Número de elementos de evidencia que se seleccionan para su inclusión en el informe. Incluye el número total de problemas de control de la conformidad incluidos en el informe.

Resumen de la evaluación

Esta sección resume la evaluación a la que se refiere el informe.

Nombre	Descripción
Nombre de la evaluación	Nombre de la evaluación a partir de la cual se generó el informe.

Nombre	Descripción
Estado	Estado de la evaluación en el momento en que se generó el informe.
Región de la evaluación	El lugar en el Región de AWS que se creó la evaluación.
Cuentas de AWS en el ámbito	La lista de los Cuentas de AWS cuales se incluye en el ámbito de la evaluación.
Nombre del marco	Nombre del marco a partir del cual se creó la evaluación.
Responsables de la auditoría	Usuario o rol de los responsables de la auditoría de la evaluación.
Última actualización	Fecha en la que se actualizó por última vez la evaluación. La hora se representa en UTC.

Página del índice

En el índice se muestra el contenido completo del informe de evaluación. El contenido se agrupa y organiza en función de los conjuntos de control que se incluyen en la evaluación. Los controles se enumeran debajo de su conjunto de controles respectivo.

Seleccione cualquier elemento del índice para ir directamente a esa sección del informe. Puede elegir un conjunto de controles o ir directamente a un control.

Página de control

La página de control consta de dos partes: un resumen del control en sí y un resumen de las evidencias recopiladas para el control.

Resumen de control

Esta sección incluye la siguiente información.

Nombre	Descripción
Nombre del control	Nombre del control.

Nombre	Descripción
Descripción	Descripción del control.
Conjunto de controles	Nombre del conjunto de controles al que pertenece el control.
Información de prueba	Procedimientos de prueba recomendados para este control.
Plan de acción	Acciones recomendadas para realizar si no se cumple el control.
Selección del informe de evaluación	Número de elementos de evidencia relacionados con este control incluidos en el informe de evaluación. Esto incluye el número de problemas de verificación de conformidad que se detectaron en las evidencias de este control.

Evidencia recopilada

En esta sección se muestran las evidencias recopiladas para el control. Las evidencias se agrupan en carpetas, que se organizan y nombran según la fecha de recolección de las mismas. Junto al nombre de cada carpeta de evidencias aparece el número total de problemas de verificación de conformidad relacionados con esa carpeta.

Debajo del nombre de cada carpeta de evidencias hay una lista de nombres de evidencias con hipervínculos.

- Los nombres de las evidencias automatizadas comienzan con una marca de tiempo de recopilación de evidencias, seguida del código de servicio, el nombre del evento (hasta 20 caracteres), el identificador de la cuenta y un identificador único de 12 caracteres.

  Por ejemplo: `21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`.

  En el caso de las evidencias automatizadas, el nombre del hipervínculo abre un nuevo archivo PDF con un resumen y más información.
- Los nombres de las evidencias manuales comienzan con una marca de tiempo de carga de las evidencias, seguida de la etiqueta `manual`, el identificador de cuenta y un identificador único de 12 caracteres. También incluyen los 10 primeros caracteres del nombre del archivo y la extensión del archivo (hasta 10 caracteres).

  Por ejemplo: `00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`.

Para evidencia manual, el nombre del hipervínculo lo lleva al bucket de S3 que contiene esa evidencia.

Junto al nombre de cada evidencia aparece el resultado de la comprobación de conformidad de ese elemento.

- En el caso de las pruebas automatizadas recopiladas a partir de un resultado conforme AWS Config, no conforme AWS Security Hub o no concluyente, se informa de un resultado que cumpla con las normas, no lo cumpla o no sea concluyente.
- En el caso de las pruebas automatizadas recopiladas a partir de las llamadas a la API AWS CloudTrail y de todas las pruebas manuales, se muestra un resultado no concluyente.

Página de resumen de evidencias

La página de resumen de evidencias incluye la siguiente información.

Nombre	Descripción
ID	Identificador único de la evidencia.
Fecha de recopilación	Fecha en que se creó o cargó la evidencia.
Descripción	Descripción de la evidencia, incluidos el identificador de la cuenta y el tipo de origen de datos.
Nombre de la evaluación	Nombre de la evaluación a partir de la cual se generó el informe.
Nombre del marco	Nombre del marco a partir del cual se creó la evaluación.
Nombre del control	Nombre del control que respalda la evidencia.
Nombre del conjunto de controles	Nombre del conjunto de controles al que pertenece el control relacionado.
Descripción del control	Descripción del control que respalda la evidencia.
Información de prueba	Procedimientos de prueba recomendados para el control.

Nombre	Descripción
Plan de acción	Acciones recomendadas para realizar si no se cumple el control.
Región de AWS	Nombre de la región asociada con la evidencia.
ID de IAM	ARN del usuario o rol asociado a la evidencia.
Cuenta de AWS	La Cuenta de AWS identificación asociada a la evidencia.
Servicio de AWS	El nombre del Servicio de AWS que está asociado a la evidencia.
Nombre de evento	Nombre del evento de la evidencia.
Hora del evento	Hora de cuando se produjo el evento de evidencia.
Origen de datos	Lugar desde el que se recopiló o cargó la evidencia. El tipo de fuente de datos puede ser Security Hub CloudTrail, llamadas a la AWS API o Manual. AWS Config
Evidencia por tipo	Categoría de la evidencia. • Las pruebas de verificación de conformidad se AWS Config recopilan en nuestro Security Hub. • La evidencia de la actividad del usuario se recopila de CloudTrai l los registros. • La evidencia de los datos de configuración se recopila a partir de instantáneas de otros Servicios de AWS. • Las evidencias manuales son aquellas que se cargan manualmente.

Nombre	Descripción
Estado de la comprobación de conformidad	Estado de la evaluación de la evidencia incluida en la categoría comprobación de conformidad. • En el caso de las pruebas automatizadas recopiladas de AWS Security Hub o AWS Config, se informa de un resultado conforme, no conforme o no concluyente. • En el caso de las pruebas automatizadas recopiladas a partir de las llamadas a la API AWS CloudTrail y de todas las pruebas manuales, se muestra un resultado no concluyente.

Página de información sobre evidencias

En la página de información sobre evidencias aparece el nombre de la evidencia y una tabla de datos de la misma. En esta tabla se proporciona un desglose detallado de cada elemento de la evidencia para que pueda entender los datos y validar que son correctos. Según el origen de datos de las evidencias, el contenido de la página de información sobre las evidencias variará.

> **Tip**
>
> La ruta de navegación en la parte superior de cada página muestra su ubicación actual a medida que explora los detalles de las evidencias. Seleccione Resumen de evidencias para volver al resumen de evidencias en cualquier momento.

Validación de un informe de evaluación

Al generar un informe de evaluación, Audit Manager genera una suma de comprobación del archivo de informe denominada `digest.txt`. Puede utilizar este archivo para validar la integridad del informe y asegurarse de que no se modificó ninguna evidencia después de la creación del informe. Contiene un objeto JSON con firmas y códigos hash que se invalidan si se modifica alguna parte del archivo del informe.

Para validar la integridad de un informe de evaluación, utilice la ValidateAssessmentReportIntegrityAPI proporcionada por Audit Manager.

Recursos adicionales

Para encontrar respuestas a preguntas y problemas comunes, consulte Solución de problemas con el informe de evaluación en la sección Solución de problemas de esta guía.

Buscador de evidencias

El buscador de evidencias proporciona una forma eficaz de buscar evidencias en Audit Manager. En lugar de explorar exhaustivamente carpetas de evidencias para encontrar lo que busca, ahora puede utilizar el buscador de evidencias para consultarlas rápidamente. Si utiliza el buscador de evidencias como administrador delegado, puede buscar evidencias en todas las cuentas de miembros de su organización.

Mediante una combinación de filtros y agrupaciones, puede reducir progresivamente el alcance de su consulta de búsqueda. Por ejemplo, si desea obtener una visión general del estado de su sistema, realice una búsqueda amplia y filtre por evaluación, intervalo de fechas y conformidad de los recursos. Si su objetivo es corregir un recurso específico, puede realizar una búsqueda restringida para encontrar evidencias que apunten a un identificador de control o recurso específico. Tras definir los filtros, puede agrupar y, a continuación, obtener una vista previa de los resultados de búsqueda coincidentes antes de crear un informe de evaluación.

Para utilizar el buscador de evidencias, debe habilitar esta característica en la configuración de Audit Manager.

Puntos clave

Entendiendo cómo funciona el buscador de pruebas con CloudTrail Lake

El buscador de evidencias utiliza la capacidad de consulta y almacenamiento de AWS CloudTrail Lake. Antes de empezar a utilizar el buscador de pruebas, es útil entender un poco más sobre cómo funciona CloudTrail Lake.

CloudTrail Lake agrega los datos en un único almacén de datos de eventos en el que se pueden realizar búsquedas y que admite potentes consultas SQL. Esto significa que puede buscar datos en toda su organización y dentro de intervalos de tiempo personalizados. Con el buscador de evidencias, puede utilizar esta función de búsqueda directamente en la consola de Audit Manager.

Cuando solicita habilitar el buscador de evidencias, Audit Manager crea un almacén de datos de eventos en su nombre. Una vez habilitado el buscador de evidencias, todas las evidencias futuras de Audit Manager se incorporarán al almacén de datos del evento, donde estarán disponibles para las consultas de búsqueda del buscador de evidencias. Después de habilitar el buscador de evidencias,

también rellenamos el almacén de datos de eventos recién creado con los datos de evidencias de los dos últimos años. Si habilita el buscador de evidencias como administrador delegado, rellenaremos los datos de todas las cuentas de los miembros de la organización.

Todas sus evidencias, ya sean nuevas o repuestas, se retienen en el almacén de datos de evidencias durante 2 años. Puede cambiar el periodo de retención predeterminado en cualquier momento. Para obtener instrucciones, consulte Actualización de un almacén de datos de eventos en la Guía del usuario de AWS CloudTrail . Puede conservar datos de eventos en un almacén de datos de eventos por hasta 7 años o 2555 días.

> **Note**
>
> Cuando se añaden nuevos datos probatorios al almacén de datos del evento, CloudTrail Lake incurre en gastos de almacenamiento e ingesta de datos.
> Para las consultas de CloudTrail Lake, pagas por uso. Esto significa que, por cada consulta de búsqueda que ejecute en el buscador de evidencias, se le cobrará por los datos escaneados.
> Para obtener más información sobre los precios de CloudTrail Lake, consulta AWS CloudTrail los precios.

Pasos a seguir a continuación

Para comenzar, habilite el buscador de evidencias en la configuración de Audit Manager. Para obtener instrucciones, consulte Habilitar el buscador de evidencias.

Recursos adicionales

- Búsqueda de evidencias en el buscador de evidencias
- Visualizar los resultados en el buscador de evidencias
- Opciones de filtrado y agrupación para el buscador de evidencias
- Ejemplos de casos de uso del buscador de evidencias
- Solución de problemas con el buscador de evidencias

Búsqueda de evidencias en el buscador de evidencias

Puede utilizar el buscador de evidencias para realizar búsquedas específicas y encontrar rápidamente las evidencias pertinentes para su revisión.

En esta página aprenderá a filtrar las búsquedas por criterios, como, por ejemplo, evaluación, intervalo de fechas, estado de conformidad de los recursos y otros atributos. La aplicación de estos filtros reduce el ámbito de la búsqueda a solo las evidencias que necesita. También puede agrupar los resultados por campos para analizar mejor los patrones.

Requisitos previos

Asegúrese de completar los pasos necesarios para habilitar el buscador de evidencias en la configuración de Audit Manager. Para obtener instrucciones, consulte Habilitar el buscador de evidencias.

Además, asegúrese de que cuente con los permisos necesarios para realizar consultas de búsqueda en el buscador de evidencias. Para ver un ejemplo de política de permisos que puede usar, consulte Permita a los usuarios realizar consultas de búsqueda en el buscador de evidencias.

Procedimiento

Siga estos pasos para buscar evidencias en la consola de Audit Manager.

1. Perform a search query
2. Stop an in-progress search query (optional)
3. Edit the filters for your search query (optional)

> **Note**
>
> También puedes usar la CloudTrail API para consultar tus datos probatorios. Para obtener más información, consulta StartQuery en la AWS CloudTrail Referencia de la API de . Si prefiere utilizar la AWS CLI, consulte Iniciar una consulta en la Guía del AWS CloudTrail usuario.

Realizar una consulta de búsqueda

Siga estos pasos para realizar una consulta de búsqueda en el buscador de evidencias.

Para buscar evidencias

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, seleccione Buscador de evidencias.
3. A continuación, aplique filtros para limitar el alcance de la búsqueda.
   a. En Evaluación, elija una evaluación.
   b. En Intervalo de fechas, seleccione un intervalo.
   c. En Conformidad de los recursos, seleccione un estado de evaluación.

4. (Opcional) Seleccione filtros adicionales (opcionales) para restringir aún más la búsqueda.
   a. Seleccione Añadir criterios, seleccione un criterio y, a continuación, seleccione uno o más valores para ese criterio.
   b. Siga creando más filtros de la misma manera.
   c. Para eliminar un filtro no deseado, seleccione Eliminar.

5. En Agrupación, especifique si desea agrupar los resultados de la búsqueda.

a. Si desea agrupar los resultados, seleccione un valor por el que agruparlos.

b. Si no desea agrupar los resultados, continúe con el paso 6.

6. Elija Buscar.

La búsqueda puede tardar unos minutos, en función de la cantidad de datos de evidencias de los que disponga. Puede salir del buscador de evidencias mientras la búsqueda está en curso. Una barra parpadeante le avisará cuando los resultados de la búsqueda estén listos.

Detener una consulta de búsqueda

Si desea detener una consulta de búsqueda por cualquier motivo, siga estos pasos.

> **Note**
>
> Detener una consulta de búsqueda aún puede generar cargos. Se le cobrará la cantidad de datos de evidencias escaneados antes de detener la consulta de búsqueda. Cuando se detenga, podrá ver los resultados parciales devueltos.

Detención de una consulta de búsqueda en curso

1. En la barra parpadeante de progreso azul de la parte superior de la pantalla, seleccione Detener búsqueda.

2. (Opcional) Revise los resultados parciales devueltos antes de detener la consulta de búsqueda.

a. Si se encuentra en la página del buscador de evidencias, los resultados parciales se muestran en la pantalla.

b. Si ha navegado fuera del buscador de evidencias, seleccione Ver resultados parciales en la barra parpadeante de confirmación verde.

Editar filtros de búsqueda

Siga estos pasos para volver a la consulta de búsqueda más reciente y ajustar los filtros según sea necesario.

> **Note**
>
> Al editar los filtros y seleccionar Buscar, se inicia una nueva consulta de búsqueda.

Edición de una consulta de búsqueda reciente

1. En la página Ver resultados, seleccione Buscador de evidencias en el menú de navegación de la ruta de navegación.

2. Seleccione Filtros y agrupaciones para ampliar la selección de filtros.

3. A continuación, edite sus filtros o inicie una nueva búsqueda.

a. Para editar los filtros, ajuste o elimine los filtros actuales y la selección de agrupación.

b. Para volver a empezar, seleccione Borrar filtros y aplique los filtros y agrupaciones que prefiera.

4. Cuando haya terminado, elija Buscar.

Pasos a seguir a continuación

Una vez finalizada la búsqueda, podrá ver los resultados que coincidan con sus criterios de búsqueda. Para obtener instrucciones, consulte Visualizar los resultados en el buscador de evidencias.

Recursos adicionales

- Opciones de filtrado y agrupación para el buscador de evidencias
- Ejemplos de casos de uso del buscador de evidencias
- Solución de problemas con el buscador de evidencias

Visualizar los resultados en el buscador de evidencias

Una vez finalizada la búsqueda, podrá ver los resultados que coincidan con sus criterios de búsqueda.

Tenga en cuenta que es posible que se evalúen varios recursos durante la recopilación de evidencias. Como resultado, la evidencia puede incluir uno o varios recursos relacionados. En el buscador de evidencias, los resultados se muestran a nivel de recurso, con una fila para cada recurso. Puede previsualizar un resumen de cada recurso sin salir de la página.

Tras revisar los resultados de la búsqueda, puede generar un informe de evaluación que incluya esas evidencias. También puede exportar los resultados de la búsqueda a un archivo de valores separados por comas (CSV).

> **Important**
>
> Le recomendamos que mantenga abierto el buscador de evidencias hasta que termine de explorar los resultados de la búsqueda. Los resultados de la búsqueda se descartan al salir de la tabla Ver resultados. Si es necesario, puede ver sus resultados recientes en la CloudTrail consola en https://console.aws.amazon.com/cloudtrail/. Aquí, los resultados de sus consultas de búsqueda se guardan durante siete días. Sin embargo, ten en cuenta que no puedes generar un informe de evaluación a partir de los resultados de búsqueda en la CloudTrail consola.

Requisitos previos

En el procedimiento siguiente se de por sentado que ya ha seguido los pasos para realizar una búsqueda en el buscador de evidencias.

Procedimiento

Siga estos pasos para ver los resultados de la búsqueda en el buscador de evidencias.

Tareas

- Paso 1. Visualizar resultados agrupados
- Paso 2. Visualización de los resultados de búsqueda
  - Administración de las preferencias de visualización
  - Visualización previa de los resúmenes de los recursos

Paso 1. Visualizar resultados agrupados

Si agrupó los resultados, puede revisarlos antes de examinar las evidencias.

> **Note**
>
> Si no agrupó los resultados, el buscador de evidencias no mostrará la tabla Agrupar por resultados. En su lugar, accederá directamente a la tabla Ver resultados.

Utilice la tabla Agrupar por resultados para conocer el alcance de la evidencia coincidente y cómo se distribuye en una dimensión específica. Los resultados se agrupan según el valor que haya seleccionado. Por ejemplo, si has agrupado por tipo de recurso, la tabla muestra una lista de tipos de AWS recursos. En la columna de Evidencia total se mostrará el número de resultados coincidentes para cada tipo de recurso.

Para obtener los resultados de un grupo

1. En la tabla Agrupar por resultados, seleccione la fila de los resultados que desee obtener.
2. Seleccione Obtener resultados. Esto iniciará una nueva consulta de búsqueda y le redirigirá a la tabla Ver resultados, donde podrá ver los resultados de ese grupo.

Paso 2. Visualización de los resultados de búsqueda

En la tabla Ver resultados se muestran los resultados de la búsqueda. Aquí puede administrar sus preferencias de visualización y obtener una vista previa de los resúmenes de recursos.

Administración de las preferencias de visualización

Sus preferencias de visualización controlan lo que ve en la página de resultados.

Administrar sus preferencias de visualización

1. Seleccione el icono de configuración (#) situado en la parte superior de la tabla Ver resultados.
2. Revise y cambie la configuración siguiente como sea necesario:

Opción	Descripción
Seleccionar columnas visibles de la tabla	Utilice la opción de alternancia para cambiar las columnas que se muestran.
Tamaño de página	Seleccione un botón de opción para especificar cuántos resultados se muestran en cada página.
Wrap text (Ajustar texto)	Seleccione la casilla de verificación para ajustar líneas de texto largas y mejorar la legibilidad.

3. Elija Confirmar para guardar las preferencias.

Visualización previa de los resúmenes de los recursos

Puede obtener una vista previa de los recursos relacionados con las evidencias que coincidan con su consulta de búsqueda. Esto le ayuda a determinar si la consulta de búsqueda arrojó los resultados esperados o si necesita ajustar los filtros y volver a ejecutar la consulta de búsqueda.

Tenga en cuenta que las evidencias pueden tener uno o más recursos relacionados. El buscador de evidencias muestra los resultados a nivel de recurso (con una fila para cada recurso).

> **Note**
>
> El buscador de evidencias devuelve los resultados de las evidencias automatizadas y manuales. Sin embargo, solo puede obtener vista previa de resúmenes de recursos para evidencias automatizadas. Esto se debe a que Audit Manager no realiza evaluaciones de recursos para obtener evidencias manuales y, como resultado, no hay un resumen de recursos disponibles.
> Para consultar los datos sobre la evidencia manual, seleccione el nombre de la evidencia para abrir la página de datos de la evidencia. Si genera un informe de evaluación a partir de los resultados del buscador de evidencias, los datos de las evidencias manuales se incluyen en el informe de evaluación.

Vista previa de resúmenes de recursos

1. Seleccione el botón de opción situado junto al resultado. Se abrirá un panel de resumen de recursos en la página actual.
2. (Opcional) Para ver todos los datos de la evidencia relacionada, seleccione el nombre de la evidencia.
3. (Opcional) Utilice las líneas horizontales (=) para arrastrar y cambiar el tamaño del panel de resumen de recursos.
4. Seleccione (x) para cerrar el panel de resumen de recursos.

Pasos a seguir a continuación

Tras revisar los resultados de la búsqueda, puede generar informes de evaluación a partir de ellos o exportarlos como un archivo CSV. Para obtener instrucciones, consulte Exportación de los resultados de la búsqueda desde el buscador de evidencias.

Recursos adicionales

- Opciones de filtrado y agrupación para el buscador de evidencias
- Ejemplos de casos de uso del buscador de evidencias
- Solución de problemas con el buscador de evidencias

Exportación de los resultados de la búsqueda desde el buscador de evidencias

Tras revisar los resultados de la búsqueda, puede generar informes de evaluación a partir de esos resultados. Además, puede exportar los resultados de búsqueda del buscador de evidencias en un archivo CSV.

Requisitos previos

En el procedimiento siguiente se de por sentado que ya ha seguido los pasos para realizar una búsqueda y revisar los resultados en el buscador de evidencias.

Procedimiento

Contenido

- Generación de un informe de evaluación a partir de los resultados de la búsqueda
- Exportación de los resultados de la búsqueda a un archivo CSV
  - Ver los resultados después de exportarlos

Generación de un informe de evaluación a partir de los resultados de la búsqueda

Una vez que esté satisfecho con los resultados de la búsqueda, puede generar un informe de evaluación.

Genere un informe de evaluación a partir de los resultados de la búsqueda

1. En la parte superior de la tabla Ver resultados, seleccione Generar informe de evaluación.
2. Introduzca un nombre y una descripción para el informe de evaluación y revise los detalles del informe de evaluación.

3. Seleccione Generar informe de evaluación.

Se tarda unos minutos en generar el informe de evaluación. Mientras tanto, puede salir del buscador de evidencias. Aparecerá una notificación de éxito de color verde que confirmará que el informe está listo. A continuación, puede ir al centro de descargas de Audit Manager y descargar su informe de evaluación.

> **Note**
>
> Audit Manager generará un informe único utilizando únicamente la evidencia de los resultados de la búsqueda. Este informe no incluye ninguna evidencia que se haya agregado manualmente a un informe desde la página de evaluación.
> Existen límites a la cantidad de evidencias que se pueden incluir en un informe de evaluación. Para obtener más información, consulte Solución de problemas con el buscador de evidencias.

Exportación de los resultados de la búsqueda a un archivo CSV

Es posible que necesite una versión portátil de los resultados de búsqueda de su buscador de evidencias. De ser así, puede exportar los resultados de la búsqueda a un archivo CSV.

Tras exportar los resultados de la búsqueda, el archivo CSV estará disponible en el centro de descargas de Audit Manager durante siete días. También se envía una copia del archivo CSV a su bucket de S3 preferido, que se conoce como destino de exportación. El archivo CSV permanece disponible en este bucket hasta que lo elimine.

Audit Manager utiliza la funcionalidad de CloudTrail Lake para exportar y entregar archivos CSV desde el buscador de evidencias. Los siguientes factores definen cómo funciona el proceso de exportación de CSV:

- Todos los resultados de la búsqueda se incluyen en el archivo CSV. Si solo quiere incluir resultados de búsqueda específicos, le recomendamos que edite sus filtros de búsqueda. De esta forma, puede restringir los resultados para orientarlos únicamente a las evidencias que desee exportar.
- Los archivos CSV se exportan en formato GZIP comprimido. El nombre predeterminado del archivo CSV es `queryID/result.csv.gz`, donde `queryID` es el ID de la consulta de búsqueda.

- El tamaño de archivo máximo de una exportación CSV es de 1 TB. Si exporta más de 1 TB de datos, los resultados se dividirán en más de un archivo. Cada archivo CSV se denomina `result_number.csv.gz`. La cantidad de archivos CSV que reciba dependerá del tamaño total de los resultados de la búsqueda. Por ejemplo, al exportar 2 TB de datos se obtendrán dos archivos de resultados de consultas: `result_1.csv.gz` `yresult_2.csv.gz`.
- Además del archivo CSV, se enviará un archivo de firma JSON a su bucket de S3. Este archivo actuará como una suma de comprobación para verificar que la información del archivo CSV es correcta. Para obtener más información, consulte CloudTrail la estructura de los archivos de firmas en la Guía para AWS CloudTrail desarrolladores. Para determinar si los resultados de la consulta se modificaron, eliminaron o no cambiaron después de entregarse, puede utilizar la validación de integridad de los resultados de la CloudTrail consulta. Para obtener instrucciones, consulte Validar los resultados de las consultas guardadas en la Guía para desarrolladores de AWS CloudTrail .

> **Note**
>
> Las respuestas textuales de evidencias manuales no se incluyen actualmente en las vistas previas del buscador de evidencias ni en las exportaciones a CSV. Para ver los datos de la respuesta textual, seleccione el nombre de la evidencia manual en el buscador de resultados para abrir la página de detalles de la evidencia. Si necesita ver los datos de las respuestas de texto fuera de la consola de Audit Manager, le recomendamos que genere un informe de evaluación a partir de los resultados del buscador de evidencias. Todos los datos de las evidencias manuales, incluidas las respuestas en texto, se incluyen en los informes de evaluación.

Exportar resultados por primera vez

Siga estos pasos para exportar los resultados de búsqueda por primera vez. Este procedimiento le da la opción de especificar un destino de exportación predeterminado para todas sus futuras exportaciones. Si no desea guardar un destino de exportación predeterminado en este momento, puede hacerlo más adelante actualizando la configuración del destino de exportación.

> **Important**
>
> Antes de empezar, asegúrese de tener un bucket de S3 disponible para usarlo como destino de exportación. Puede usar uno de sus buckets de S3 existentes o puede crear uno nuevo en Amazon S3. Para una seguridad y un rendimiento óptimos, le recomendamos que utilice

un bucket de S3 en la misma AWS cuenta y región que utilizó la evaluación. Además, su bucket de S3 debe tener la política de permisos necesaria CloudTrail para poder escribir en él los archivos de exportación. Más específicamente, la política de bucket debe incluir una `s3:PutObject` acción y el ARN del bucket, y figurar CloudTrail como principal de servicio. Proporcionamos un ejemplo de política de permisos que puede utilizar. Para obtener instrucciones sobre cómo adjuntar esta política a su bucket de S3, consulte Añadir una política de buckets mediante la consola de Amazon S3.
Para obtener más consejos, consulte Consejos de configuración para el destino de su exportación. Si tiene algún problema al exportar un archivo CSV, consulte csv-exports.

Para exportar los resultados de la búsqueda (primera ejecución)

1. En la parte superior de la tabla Ver resultados, seleccione Exportar CSV.
2. Especifique el bucket de S3 al que desea exportar su archivo.
   - Seleccione Explorar S3 para elegir de una lista de sus buckets.
   - Como alternativa, puede introducir el URI del bucket en este formato: **`s3://bucketname/prefix`**

   > **Tip**
   > Para mantener el bucket de destino organizado, puede crear una carpeta opcional para sus exportaciones a CSV. Para ello, añada una barra (**`/`**) y un prefijo al valor del cuadro URI del recurso (por ejemplo, **`/evidenceFinderExports`**). A continuación, Audit Manager incluirá este prefijo cuando añada el archivo CSV al bucket y Amazon S3 generará la ruta especificada por el prefijo. Para obtener más información acerca de los prefijos en Amazon S3, consulte Organizar objetos en la consola de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

3. (Opcional) Si no quiere guardar este bucket como destino de exportación predeterminado, desmarque la casilla de verificación que indica Guardar este bucket como destino de exportación predeterminado en la configuración de mi buscador de evidencias.
4. Seleccione Exportar.

Exportar los resultados después de guardar un destino de exportación

Una vez que haya guardado un bucket de S3 predeterminado como destino de exportación predeterminado, puede seguir estos pasos en el futuro.

Para exportar los resultados de la búsqueda (después de guardar un destino de exportación predeterminado)

1. En la parte superior de la tabla Ver resultados, seleccione Exportar CSV.
2. En el mensaje que aparece, revise el bucket de S3 predeterminado en el que se guardará el archivo exportado.
   a. (Opcional) Para seguir usando este bucket y ocultar este mensaje en el futuro, marque la casilla No volver a recordármelo.
   b. (Opcional) Para cambiar este bucket, siga el procedimiento para actualizar la configuración del destino de exportación.
3. Elija Confirmar.

Según la cantidad de datos que exporte, el proceso de exportación puede tardar unos minutos en completarse. Puede navegar fuera del buscador de evidencias mientras la exportación está en curso. Al salir del buscador de evidencias, la búsqueda se detendrá y los resultados de la búsqueda se descartarán en la consola. Sin embargo, el proceso de exportación a CSV continuará en segundo plano. El archivo CSV contendrá el conjunto completo de resultados de búsqueda que coincidan con su consulta.

Ver los resultados después de exportarlos

Para buscar el archivo CSV y comprobar su estado, vaya al Centro de descargas de Audit Manager de Audit Manager. Cuando el archivo exportado esté listo, puede descargar su archivo CSV desde el centro de descargas.

También puede buscar y descargar el archivo CSV desde el bucket de S3 de destino de exportación.

Para buscar el archivo CSV y el archivo de firma en la consola de Amazon S3

1. Abra la consola de Amazon S3.
2. Seleccione el bucket de destino de exportación que especificó al exportar el archivo CSV.
3. Recorra la jerarquía de objetos hasta que encuentre el archivo CSV y el archivo de firma. El archivo CSV tiene una extensión `.csv.gz` y el archivo de firma tiene una extensión `.json`.

Verá una jerarquía de objetos similar a la del siguiente ejemplo, pero con diferente nombre de bucket para el destino de exportación, ID de cuenta, fecha e ID de consulta.

```
All Buckets
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
                                Query_ID
```

Recursos adicionales

- Solución de problemas con el buscador de evidencias
- Configuración del destino de la exportación predeterminada para el buscador de evidencias

Opciones de filtrado y agrupación para el buscador de evidencias

En esta página puede ver una lista de las opciones de filtrado y agrupación disponibles para el buscador de evidencias.

Referencia de filtro

Puede utilizar los siguientes filtros para buscar pruebas que coincidan con criterios específicos, como una evaluación, un control o Servicio de AWS.

Temas

- filtros requeridos
- Filtros adicionales (opcionales)
- Combinar filtros

filtros requeridos

Utilice estos filtros para comenzar con información general de alto nivel de la evidencia de una evaluación.

Nombre del filtro	Descripción	Notas
Evaluación	Devuelve la evidencia de una evaluación específica.	Puede filtrar por una sola evaluación.
Rango de fechas	Devuelve evidencia de un periodo de tiempo específico.	O bien, puede usar un Rango relativo para definir un rango relativo a la fecha de hoy (por ejemplo, **`Last 30 days`**). O bien, puede usar un Rango absoluto para especificar un rango de fechas específico (por ejemplo, **`June 27th - July 4th`**).
Conformidad de recursos	Devuelve los recursos con una evaluación de verificación de conformidad específica.	Audit Manager recopila pruebas de verificación de conformidad para los controles que utilizan AWS Config Security Hub como tipo de fuente de datos. Es posible que se evalúen varios recursos durante la recopilación de evidencias. En consecuencia, una sola evidencia de verificación de conformidad puede incluir uno o más recursos. Puede usar este filtro para explorar el estado de conformidad a nivel de recurso. Puede elegir una o más de las siguientes opciones: • No conformidad: este filtro encuentra recursos con problemas de verificación de conformidad. Esto sucede si Security Hub informa de un resultado de error o si AWS Config informa de un resultado no conforme. • Conformidad: este filtro encuentra recursos sin problemas de verificación de conformidad. Esto

Nombre del filtro	Descripción	Notas
		sucede si Security Hub informa de un resultado de aprobación o si AWS Config informa de un resultado de conformidad. • No concluyente: este filtro busca recursos para los que no haya una verificación de conformid ad disponible o aplicable. Esto ocurre si un recurso utiliza AWS Config o Security Hub como tipo de origen de datos subyacente, pero esos servicios no están habilitados. Esto también ocurre si el recurso utiliza un tipo de fuente de datos subyacente que no admite las comprobac iones de conformidad (como pruebas manuales, llamadas a la AWS API o CloudTrail).

Filtros adicionales (opcionales)

Utilice estos filtros para limitar el alcance de la consulta de búsqueda. Por ejemplo, utilice Servicio para ver todas las evidencias relacionadas con Amazon S3. Utilice Tipo de recurso para centrarse únicamente en los buckets de S3. O bien, utilice ARN del recurso para dirigirse a un bucket de S3 específico.

Puede crear filtros adicionales mediante uno o varios de los siguientes criterios.

Nombre del criterio	Descripción	Cuándo utilizar este criterio
ID de cuenta	Desglose por Cuenta de AWS.	Utilice este criterio para buscar evidencias relacionadas con una Cuenta de AWS específica.
Control	Desglosar por nombre de control.	Utilice este criterio para buscar evidencias relacionadas con un control específico.

Nombre del criterio	Descripción	Cuándo utilizar este criterio
Dominio de control	Desglosar por dominio de control.	Utilice este criterio para centrarse en un área temática específica mientras se prepara para una auditoría. Puede filtrar por dominio de control si está consultando una evaluación creada a partir de un marco estándar. Entre algunos ejemplos de dominios de control se incluye la seguridad de redes, la administración de identidades y accesos y la protección de datos. Es posible que algunos dominios de control estén marcados como desactualizados tras la transición de Audit Manager a un nuevo conjunto de dominios de control proporcionado por AWS Control Catalog. Para obtener más información, consulte Veo que un dominio de control está marcado como obsoleto ¿Qué significa esto?.
Data source type (Tipo de origen de datos)	Desglosar por tipo de origen de datos.	Utilice este criterio para centrarse en un origen de datos específico. Establezca el valor en `Manual` para buscar evidencias que haya subido manualmente. De lo contrario, puede filtrar las evidencias automatizadas en función de su procedenc ia (por ejemplo `AWS Config`, `CloudTrail` , `Security Hub` o `AWS API calls`).

Nombre del criterio	Descripción	Cuándo utilizar este criterio
Nombre de evento	Desglosar por nombre de evento.	Utilice este criterio para centrarse en un evento específico con el que esté relacionada la evidencia. Un evento es el registro de una actividad en Cuenta de AWS. Por ejemplo, puede buscar el nombre de una llamada a la API, como la operación de IAM `AttachRolePolicy` que se usa para configurar los permisos. O bien, busca una CloudTrail palabra clave, como el `ConsoleLogin` evento que se registra CloudTrail cuando un usuario inicia sesión en tu cuenta.
ARN de recurso	Desglosar por nombre de recurso de Amazon (ARN).	Utilice este criterio para buscar evidencias relacionadas con un recurso específico de AWS .
Tipo de recurso	Desglosar por tipo de recurso.	Usa este criterio para centrarte en el tipo de recurso que se está evaluando, como una EC2 instancia de Amazon o un bucket de S3.
Servicio	Desglose por Servicio de AWS nombre.	Utilice este criterio para buscar pruebas relacionadas con algo específico Servicio de AWS, como Amazon EC2, Amazon S3 o AWS Config.
Categorías de servicio	Desglose por Servicio de AWS categoría.	Utilice este criterio para centrarse en una categoría específica de Servicio de AWS. Algunos ejemplos son seguridad, identidad y conformidad, base de datos y almacenamiento.

Combinar filtros

Comportamiento de criterios

Cuando especifica más de un criterio, Audit Manager aplica el operador `AND` a sus selecciones. Esto significa que todos los criterios se agrupan en una sola consulta y los resultados deben coincidir con todos los criterios combinados.

Ejemplo

En la siguiente configuración de filtros, el buscador de evidencias devuelve los recursos de no conformidad de los últimos 7 días para la evaluación denominada **`MySOC2Assessment`**. Además, los resultados se refieren tanto a una política de IAM como al control especificado.

Comportamiento del valor de criterios

Cuando se especifica más de un valor de criterio, los valores se vinculan con un operador `OR`. El buscador de evidencias devuelve resultados que coinciden con cualquiera de estos valores de criterio.

Ejemplo

En la siguiente configuración de filtro, el buscador de evidencias devuelve los resultados de búsqueda que provienen de AWS CloudTrail AWS Config, o AWS Security Hub.

Agrupación de referencia

Puede agrupar los resultados de la búsqueda para una navegación más rápida. La agrupación le muestra la amplitud de los resultados de búsqueda y cómo están distribuidos en una dimensión específica.

Puede utilizar cualquiera de los siguientes grupos por valores.

Agrupación por	Descripción
ID de cuenta	Agrupar los resultados por Cuenta de AWS.
Control	Agrupe los resultados por nombre de control.
Data source type (Tipo de origen de datos)	Agrupe los resultados por el tipo de origen de datos del que provienen las evidencias.
Nombre de evento	Agrupe los resultados por el nombre de un evento.
ARN de recurso	Agrupe resultados por nombre de recurso de Amazon (ARN).
Tipo de recurso	Agrupe los resultados por tipo de recurso.
Servicio	Agrupa los resultados por Servicio de AWS nombre.
Categorías de servicio	Agrupa los resultados por Servicio de AWS categoría.

Ejemplos de casos de uso del buscador de evidencias

El buscador de evidencias puede ayudarle con varios casos de uso. En esta página se proporcionan algunos ejemplos y se sugieren los filtros de búsqueda que puede utilizar en cada situación.

Temas

- Caso de uso 1: busque evidencias de no conformidad y organice las delegaciones
- Caso de uso 2: identificar evidencias de conformidad
- Caso de uso 3: realizar una vista previa rápida de los recursos de evidencias

Caso de uso 1: busque evidencias de no conformidad y organice las delegaciones

Este caso de uso es ideal si es responsable de conformidad, de protección de datos o un profesional de GRC encargado de supervisar la preparación de las auditorías.

Al supervisar la postura de conformidad de su organización, puede confiar en los equipos de socios para que le ayuden a solucionar los problemas. Puede utilizar el buscador de evidencias para ayudarle a organizar el trabajo para los equipos de sus socios.

Al aplicar filtros, puede centrarse en las evidencias de un área en concreto. Además, también puede estar en consonancia con las responsabilidades y el ámbito de cada equipo asociado con el que trabaje. Al realizar una búsqueda específica de este modo, puede utilizar los resultados de la búsqueda para identificar qué es exactamente lo que hay que corregir en cada área temática. A continuación, puede delegar las evidencias de no conformidad en el equipo asociado correspondiente para que las corrija.

Para este flujo de trabajo, siga los pasos para buscar evidencias. Utilice los siguientes filtros para buscar evidencias de no conformidad.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

A continuación, aplique filtros adicionales para el área en la que se está centrando. Por ejemplo, utilice el filtro Categoría de servicio para buscar recursos de no conformidad relacionados con la IAM. A continuación, comparta esos resultados con el equipo propietario de los recursos de la IAM para su organización. O bien, si está consultando una evaluación que se creó a partir de un marco estándar, puede usar el filtro de Dominio de control para encontrar evidencias de no conformidad relacionadas con el dominio de administración de identidades y accesos.

```
Control domain | <domain that you're focusing on>
or
```

```
Service category | <Servicio de AWS category that you're focusing on>
```

Cuando encuentre las evidencias que necesite, siga los pasos para generar un informe de evaluación a partir de los resultados de la búsqueda. Para obtener instrucciones, consulte Generación de un informe de evaluación a partir de los resultados de la búsqueda. Puede compartir este informe con su equipo asociado, que lo puede utilizar como lista de comprobación de las correcciones.

Caso de uso 2: identificar evidencias de conformidad

Este caso de uso es ideal si trabaja en TI o en SecOps otro rol que posea activos en la nube y los corrija. DevOps

Como parte de una auditoría, es posible que se le pida que solucione los problemas relacionados con los recursos de los que dispone. Después de realizar este trabajo, puede utilizar el buscador de evidencias para validar que sus recursos son de conformidad.

Para este flujo de trabajo, siga los pasos para buscar evidencias. Utilice los siguientes filtros para buscar evidencias de conformidad.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

A continuación, aplique filtros adicionales para mostrar solo las evidencias de las que sea responsable. En función del ámbito de su propiedad, haga que la búsqueda sea tan segmentada como necesite. Los siguientes ejemplos de filtros están ordenados del más amplio al más preciso. Elija las opciones adecuadas para usted y sustitúyalas por sus propios valores. *<placeholder text>*

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of Servicios de AWS that you own>
Service | <a specific Servicio de AWS that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

Si eres responsable de varias instancias con el mismo criterio (por ejemplo, si eres propietario de varias Servicios de AWS), puedes agrupar los resultados por ese valor. Esto le proporcionará el total de coincidencias de evidencias para cada Servicio de AWS. A continuación, podrá obtener los resultados de los servicios de los que disponga.

Caso de uso 3: realizar una vista previa rápida de los recursos de evidencias

Este caso de uso es ideal para todos los clientes de Audit Manager.

Hasta ahora, revisar los datos de las evidencias individuales llevaba mucho tiempo. Si quería obtener una vista previa de las evidencias, tenía que ir directamente a esa evaluación y, a continuación, navegar por carpetas de evidencias muy jerarquizadas. Ahora, el buscador de evidencias ofrece una forma cómoda de obtener una vista previa de esta información. Para cada elemento de evidencia que coincida con su consulta de búsqueda, puede obtener una vista previa de los recursos individuales para dicha evidencia.

Para empezar, siga los pasos para buscar evidencias. A continuación, seleccione el botón de opción situado junto al resultado para ver un resumen de recursos en la página actual. Puede obtener una vista previa de cada recurso individual relacionado con un elemento de evidencia. Para ver todos los detalles de la evidencia de cualquier recurso, seleccione el nombre de la evidencia. Para obtener más información, consulte Visualización previa de los resúmenes de los recursos.

Centro de descargas de Audit Manager

El centro de descargas es el lugar donde puede encontrar y administrar todos los archivos descargables de Audit Manager. Al generar un informe de evaluación o exportar los resultados de una búsqueda desde el buscador de evidencias, los archivos aparecen en el centro de descargas.

Contenido

- Navegar por el centro de descargas
- Descarga de un archivo
- Eliminación de un archivo
- Recursos adicionales

Navegar por el centro de descargas

Siga estos pasos para buscar los archivos en el centro de descargas.

Búsqueda de archivos en el centro de descargas

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, seleccione Centro de descargas.
3. Seleccione la pestaña Informes de evaluación para ver los informes de evaluación disponibles para su descarga.
   - En esta pestaña se muestran los informes de evaluación que ha generado. Los informes de evaluación permanecen disponibles en el centro de descargas hasta que los elimine.
   - Para ver el estado más reciente de su informe de evaluación, pulse el icono de actualización (#) para volver a cargar la tabla. En cada fila de la tabla de informes de evaluación se muestra el nombre del informe, su fecha de creación y uno de los siguientes estados:

Estado	Descripción
In progress (En curso)	Audit Manager está generando el informe de evaluación.
Ready	El informe de evaluación está disponible para su descarga.

Estado	Descripción
Error	No se pudo generar el informe de evaluación. En este caso, Audit Manager muestra un mensaje que describe el error. Para obtener información sobre cómo resolver estos errores, consulte Solución de problemas con el informe de evaluación.

4. Seleccione la pestaña Exportaciones para ver las exportaciones en formato CSV disponibles para su descarga.

   - En esta pestaña se muestran los resultados de búsqueda del buscador de evidencias que ha exportado en los últimos siete días. Los archivos CSV se eliminan del centro de descargas transcurridos siete días, pero permanecen disponibles en su bucket de S3 de destino de exportación. Para obtener instrucciones sobre cómo encontrar una exportación CSV del buscador de evidencias en su bucket de destino de S3, consulte Ver los resultados después de exportarlos.
   - Para ver el estado más reciente de sus exportaciones CSV, elija el icono de actualización (#) para recargar la tabla. Cada fila de la tabla de exportaciones muestra el nombre del archivo, su fecha de exportación y uno de los siguientes estados:

Estado	Descripción
In progress (En curso)	Audit Manager está preparando el archivo CSV.
Ready	La exportación se realizó correctamente y el archivo está disponible para su descarga.
Error	Se produjo un error en la exportación. En este caso, Audit Manager muestra un mensaje que describe el error. Para obtener información sobre cómo resolver estos errores, consulte csv-exports.

> **Note**
>
> Tenga en cuenta que la pestaña de exportaciones también puede mostrar archivos CSV para consultas que haya realizado directamente en AWS CloudTrail Lake. Esto

incluye las consultas realizadas en la CloudTrail consola o mediante la CloudTrail API. CloudTrail las exportaciones aparecen en esta pestaña si consultó el almacén de datos de eventos de Audit Manager y eligió guardar los resultados en Amazon S3.

Descarga de un archivo

Siga estos pasos para descargar un archivo del centro de descargas.

Para descargar un archivo

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, seleccione Centro de descargas.
3. Seleccione la pestaña Informes de evaluación o la pestaña Exportaciones.
4. Seleccione el archivo que desea descargar y, a continuación, elija Descargar.

Para obtener instrucciones sobre cómo descargar un archivo directamente del bucket de destino de S3, consulte Descarga de un objeto en la Guía del usuario de Amazon Simple Storage Service (Amazon S3).

Eliminación de un archivo

Siga estos pasos para eliminar cualquier informe de evaluación que ya no necesite en el centro de descargas.

> **Note**
>
> Actualmente, no se permite eliminar exportaciones a archivos CSV desde el centro de descargas. Las exportaciones a CSV se eliminan automáticamente del centro de descargas transcurridos siete días.

Para eliminar un informe de evaluación

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, seleccione Centro de descargas.
3. Seleccione la pestaña Informes de evaluación.

4. Seleccione el informe de evaluación que desee eliminar y seleccione Eliminar.

Si desea eliminar un informe de evaluación o una exportación a CSV de su bucket de destino de S3, le recomendamos que complete esta tarea directamente en Amazon S3. Para obtener instrucciones, consulte Eliminación de objetos de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service (Amazon S3).

Recursos adicionales

- Configuración del destino de la exportación predeterminada para el buscador de evidencias
- Configuración del destino del informe de evaluación predeterminado
- Solución de problemas con el informe de evaluación
- Solución de problemas de exportación de CSV
- Descarga de un objeto de Amazon S3
- Eliminación de objetos de Amazon S3

Uso de la biblioteca de marcos para administrar marcos en AWS Audit Manager

Puede buscar y administrar marcos en la biblioteca de marcos en AWS Audit Manager.

Un marco de trabajo determina qué controles se prueban en un entorno durante un período de tiempo. Define los controles y sus asignaciones de origen de datos para un estándar o reglamento de cumplimiento determinado. También se utiliza para estructurar y automatizar las evaluaciones de Audit Manager. Puede utilizar los marcos como punto de partida para auditar su Servicio de AWS uso y empezar a automatizar la recopilación de pruebas.

Puntos clave

En la biblioteca de marcos, los marcos se organizan en las siguientes categorías.

- Los Marcos estándar son marcos prediseñados que proporciona AWS . Estos marcos se basan en las AWS mejores prácticas para diferentes normas y reglamentos de cumplimiento, como el GDPR y la HIPAA. Los marcos estándar incluyen controles que se organizan en conjuntos de controles que se basan en el estándar o normativa de conformidad que respaldan el marco.

  Puede ver el contenido de los marcos estándar, pero no puede editarlos ni eliminarlos. Sin embargo, puede crear una copia editable de cualquier marco estándar para crear uno nuevo que se adapte a sus requisitos específicos.
- Los marcos personalizados son los marcos que crea. Puede crear un marco personalizado desde cero o crear una copia editable de un marco existente. Puede utilizar marcos personalizados para organizar los controles en conjuntos de controles de forma que se ajusten a sus requisitos específicos.

Puede crear una evaluación a partir de un marco estándar o personalizado.

> **Note**
>
> AWS Audit Manager ayuda a recopilar pruebas relevantes para verificar el cumplimiento de normas y reglamentos de cumplimiento específicos. Sin embargo, no evalúa el cumplimiento en sí mismo. AWS Audit Manager Por lo tanto, es posible que las pruebas recopiladas no

incluyan toda la información sobre su AWS uso que se necesita para las auditorías. AWS Audit Manager no sustituye a los asesores legales ni a los expertos en cumplimiento.

Recursos adicionales

Para crear y administrar los marcos en Audit Manager, siga los procedimientos que se indican aquí.

- Encontrando los marcos disponibles en AWS Audit Manager
- Revisar un marco en AWS Audit Manager
- Crear un marco personalizado en AWS Audit Manager
  - Crear un marco personalizado desde cero en AWS Audit Manager
  - Hacer una copia editable de un marco existente en AWS Audit Manager
- Edición de un marco personalizado en AWS Audit Manager
- Eliminar un marco personalizado en AWS Audit Manager
- Compartir un marco personalizado en AWS Audit Manager
  - Conceptos y terminología del uso compartido de marcos
  - Envío de una solicitud para compartir un marco personalizado en AWS Audit Manager
  - Respuesta a las solicitudes de uso compartido en AWS Audit Manager
  - Eliminación de solicitudes de uso compartido en AWS Audit Manager
- Marcos compatibles en AWS Audit Manager

Encontrando los marcos disponibles en AWS Audit Manager

Puede encontrar todos los marcos disponibles en la página Biblioteca de marcos de la consola de Audit Manager.

También puede ver todos los marcos disponibles mediante la API Audit Manager o AWS Command Line Interface (AWS CLI).

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver los marcos en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son:

AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Audit Manager console

Visualización de los marcos disponibles en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Biblioteca de marcos.
3. Elija la pestaña Marcos estándar o la pestaña Marcos personalizados para ver los marcos estándar y personalizados disponibles.

AWS CLI

Para ver los marcos disponibles en AWS CLI

Para ver los marcos en Audit Manager, utilice el list-assessment-frameworkscomando y especifique un`--framework-type`. También puede recuperar una lista de marcos estándar. O puede recuperar una lista de marcos personalizados.

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

Visualización de los marcos disponibles mediante la API

Utilice la ListAssessmentFrameworksoperación y especifique un tipo de marco. O bien, puede devolver una lista de marcos estándar. O bien, puede devolver una lista de marcos personalizados.

Para obtener más información, elija uno de los enlaces anteriores para obtener más información en la referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar la `ListAssessmentFrameworks` operación y los parámetros en uno de los idiomas específicos. AWS SDKs

Pasos a seguir a continuación

Cuando lo tenga todo listo para explorar los detalles de un marco, siga los pasos que se indican en Revisar un marco en AWS Audit Manager. Esta página le guiará por los detalles de los marcos y le explicará la información que aparece.

En la página Biblioteca de marcos, también puede crear, editar, eliminar o compartir un marco personalizado.

Recursos adicionales

Para obtener soluciones a problemas relacionados con los marcos en Audit Manager, consulte Solución de problemas con los marcos.

Revisar un marco en AWS Audit Manager

Puede revisar los detalles de un marco mediante la consola Audit Manager, la API Audit Manager o AWS Command Line Interface (AWS CLI).

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver los marcos. AWS Audit Manager Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Audit Manager console

Visualización de los detalles de los marcos en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Biblioteca de marcos para ver una lista de marcos disponibles.
3. Seleccione la pestaña Marcos estándar o la pestaña Marcos personalizados para explorar los marcos disponibles.

4. Seleccione el nombre del marco para abrirlo.
5. Revise los detalles del marco con la siguiente información como referencia.

Sección de detalles del marco

En esta sección, se proporciona información general sobre el marco. En esta sección puede revisar la siguiente información:

Nombre	Descripción
Descripción	Descripción del marco, si se ha proporcionado una.
Tipo de marco	Especifica si el marco es estándar o personalizado.
Tipo de conformidad	El estándar o normativa de conformidad que admiten el marco.

Si está viendo un marco personalizado, también puede ver los siguientes detalles:

Nombre	Descripción
Creado por	La cuenta que creó el marco personalizado.
Date created (Fecha de creación)	La fecha en la que se creó el marco personalizado.
Última actualización	La fecha en la que se editó este marco por última vez.

Pestaña de controles

Esta pestaña muestra los controles del marco, agrupados por conjunto de controles. En esta pestaña puede revisar la siguiente información:

Nombre	Descripción
Controles agrupados por conjunto de controles	Seleccione el icono de vista en árbol para ver los controles que pertenecen a cada conjunto de controles.

Nombre	Descripción
Tipo	Especifica si el control es un control estándar o personalizado.
Origen de datos	Especifica el origen de datos del que Audit Manager recopila las evidencias para ese control de marco.

Pestaña Etiquetas

Esta pestaña enumera las etiquetas que están asociadas con el marco. En esta pestaña puede revisar la siguiente información:

Nombre	Descripción
Clave	La clave de la etiqueta (por ejemplo, un estándar, una normativa o una categoría de conformidad).
Valor	El valor de la etiqueta.

AWS CLI

Para ver los detalles del marco en AWS CLI

1. Para identificar el marco que desea revisar, ejecute el list-assessment-frameworkscomando y especifique un`--framework-type`. También puede recuperar una lista de marcos estándar. O puede recuperar una lista de marcos personalizados.

   En el ejemplo siguiente, sustituya *`placeholder text`* el por `Custom` o`Standard`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

   La respuesta devuelve una lista de marcos. Busque el marco que desea revisar y tome nota de su ID y del nombre de recurso de Amazon (ARN).

2. Para obtener los detalles del marco, ejecute el get-assessment-frameworkcomando y especifique el`--framework-id`.

   En el siguiente ejemplo, sustituya el *`placeholder text`* por su propia información.

```
aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> Los detalles del marco se devuelven en formato JSON. Para comprender estos datos, consulte el get-assessment-framework resultado en la referencia de AWS CLI comandos.

3. Para ver las etiquetas de un marco, utilice el list-tags-for-resourcecomando y especifique `--resource-arn` las del marco.

   En el siguiente ejemplo, sustituya la *`placeholder text`* por su propia información:

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Para obtener más información acerca del etiquetado en Audit Manager, consulte Etiquetado de recursos de AWS Audit Manager.

Audit Manager API

Visualización de los detalles de los marcos mediante la API

1. Para identificar el marco que desea revisar, utilice la ListAssessmentFrameworksoperación y especifique un FrameworkType. O bien, puede devolver una lista de marcos estándar. O bien, puede devolver una lista de marcos personalizados.

   En la respuesta, busque el marco que desea revisar y anote el ID de marco y el nombre de recurso de Amazon (ARN).

2. Para obtener los detalles del marco, utilice la GetAssessmentFrameworkoperación. En la solicitud, especifique el frameworkId que obtuvo en el paso 1.

> **Tip**
>
> Los detalles del marco se devuelven en formato JSON. Para entender estos datos, consulta los elementos de GetAssessmentFramework respuesta en la referencia de la AWS Audit Manager API.

3. Para ver las etiquetas del marco, usa la ListTagsForResourceoperación. En la solicitud, especifique el framework ResourceArn que obtuvo en el paso 1.

Para obtener más información sobre las etiquetas en Audit Manager, consulte AWS Audit Manager Recursos de etiquetado.

Para obtener más información sobre estas operaciones de la API, consulte cualquiera de los enlaces del procedimiento anterior en la Referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas AWS SDKs específicos.

Pasos a seguir a continuación

En la página de detalles del marco, puede crear una evaluación a partir del marco o crear una copia editable del marco.

Si está revisando un marco personalizado, también puede editarlo, eliminarlo o compartirlo.

Recursos adicionales

- En la página de detalles del marco personalizado se me pide que vuelva a crear el marco personalizado
- No puedo crear una copia del marco personalizado

Crear un marco personalizado en AWS Audit Manager

Puede utilizar marcos personalizados para organizar los controles en conjuntos de controles de forma que se ajusten a sus requisitos específicos.

Puntos clave

Cuando se trata de crear marcos personalizados en Audit Manager, tiene dos métodos entre los que elegir:

1. Creación de un marco personalizado desde cero: esto le ofrece la flexibilidad de empezar de cero y definir todos los aspectos del marco según sus especificaciones. Este método es especialmente útil cuando sus requisitos se desvían considerablemente de los marcos estándar existentes o cuando necesita incorporar conjuntos de control patentados específicos para su organización.
2. Creación de una copia editable de un marco existente: este método le permite sacar partido de la estructura y el contenido de un marco existente y, al mismo tiempo, le permite personalizarlo para adaptarlo a sus necesidades específicas. Al comenzar con una base establecida, puede optimizar el proceso de creación de su marco personalizado y centrar sus esfuerzos en adaptarlo a los requisitos únicos de su organización.

Independientemente del método que elija, la creación de un marco personalizado implica una serie de pasos, como, por ejemplo, especificar los detalles del marco, definir los conjuntos de controles y revisar el marco antes de finalizar su creación. Durante este proceso, puede incorporar los conjuntos de controles específicos de su organización, asegurándose de que el marco personalizado refleje con precisión sus requisitos de GRC.

Recursos adicionales

Para obtener instrucciones sobre cómo crear un marco personalizado, consulte los siguientes recursos.

- Crear un marco personalizado desde cero en AWS Audit Manager
- Hacer una copia editable de un marco existente en AWS Audit Manager

Crear un marco personalizado desde cero en AWS Audit Manager

Si los requisitos de cumplimiento de su organización no se ajustan a los marcos estándar prediseñados que están disponibles AWS Audit Manager, puede crear su propio marco personalizado desde cero.

En esta página se describen los pasos para crear un marco personalizado que se adapte a sus necesidades específicas.

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para crear un marco personalizado. AWS Audit Manager Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Tareas

- Paso 1: especificar los detalles del marco
- Paso 2: especificar conjuntos de controles
- Paso 3: revisar y crear el marco

Paso 1: especificar los detalles del marco

Comience por especificar los detalles sobre el marco personalizado.

Para especificar los detalles del marco

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Biblioteca de marcos y, a continuación, Crear marco personalizado.
3. En Detalles del marco, introduzca un nombre, un tipo de conformidad (opcional) y una descripción del marco (también opcional). Al introducir un tipo de conformidad, como PCI_DSS o GDPR, podrá utilizar esta palabra clave para buscar el marco más adelante.
4. En Etiquetas, seleccione Añadir nueva etiqueta para asociar una etiqueta a su marco. Puede especificar una clave y un valor para cada etiqueta. La clave de la etiqueta es obligatoria. Puede utilizarla como criterio de búsqueda al buscar este marco en la biblioteca de marcos.
5. Elija Next (Siguiente).

Paso 2: especificar conjuntos de controles

A continuación, especifique qué controles desea añadir a su marco y cómo desea organizarlos. Comience por agregar conjuntos de controles al marco y, a continuación, agregue controles al conjunto de controles.

> **Note**
>
> Cuando utiliza la AWS Audit Manager consola para crear un marco personalizado, puede añadir hasta 10 conjuntos de controles para cada marco.
> Cuando utiliza la API de Audit Manager para crear un marco personalizado, puede crear más de 10 conjuntos de controles. Para añadir más conjuntos de controles de los que permite actualmente la consola, utilice la CreateAssessmentFrameworkAPI que proporciona Audit Manager.

Especificación de un conjunto de controles

1. En Nombre del conjunto de controles, escriba un nombre para el conjunto de controles.
2. En Añadir controles, utilice la lista desplegable Tipo de control para seleccionar uno de los dos tipos de controles: Controles estándar o Controles personalizados.
3. Según la opción que haya seleccionado en el paso anterior, se muestra una lista de controles estándar o controles personalizados. Seleccione uno o varios controles y elija Añadir al conjunto de controles.
4. En la ventana emergente que aparece, seleccione Añadir al conjunto de controles.
5. Revise los controles que aparecen en la lista Controles seleccionados.
   - Para añadir más controles, repita los pasos 2 a 4.
   - Para eliminar los controles no deseados, seleccione uno o varios controles y elija Eliminar control.
6. Para añadir un conjunto de controles nuevo, elija Añadir conjunto de controles.
7. Para eliminar un conjunto de controles no deseado, seleccione Eliminar conjunto de controles.
8. Cuando termine de añadir conjuntos de controles y controles, elija Siguiente.

Paso 3: revisar y crear el marco

Revise la información de su marco. Para modificar la información de un paso, seleccione Editar.

Cuando haya terminado, elija Crear un marco personalizado.

Pasos a seguir a continuación

Después de crear el nuevo marco personalizado, puede crear una evaluación a partir del marco. Para obtener más información, consulte Crear una evaluación en AWS Audit Manager.

Para revisitar el marco personalizado más adelante, consulte Encontrando los marcos disponibles en AWS Audit Manager. Puede seguir estos pasos para localizar el marco personalizado y poder verlo, editarlo, compartirlo o eliminarlo.

Recursos adicionales

Para obtener soluciones a problemas relacionados con los marcos en Audit Manager, consulte Solución de problemas con los marcos.

Hacer una copia editable de un marco existente en AWS Audit Manager

En lugar de crear un marco personalizado desde cero, puede utilizar un marco existente como punto de partida y crear una copia editable. Al hacerlo, el marco existente permanece en la biblioteca de marcos y se crea un nuevo marco personalizado con sus ajustes específicos.

Puede crear una copia editable de cualquier marco existente. Puede ser un marco estándar o un marco personalizado.

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para crear un marco personalizado en él. AWS Audit Manager Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Tareas

- Paso 1: especificar los detalles del marco
- Paso 2: especificar conjuntos de controles
- Paso 3: revisar y crear el marco

Paso 1: especificar los detalles del marco

Todos los detalles del marco, excepto las etiquetas, se transfieren del marco original. Revise y modifique estos detalles según sea necesario.

Para especificar los detalles del marco

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Biblioteca de marcos.
3. Elija el marco que desea utilizar como punto de partida, seleccione Crear marco personalizado y luego Hacer una copia.
4. En la ventana emergente que aparece, introduzca un nombre para el nuevo marco personalizado y seleccione Continuar.
5. En Detalles del marco, revise el nombre, el tipo de conformidad y la descripción del marco, y modifíquelos según sea necesario. El tipo de cumplimiento debe indicar el estándar de cumplimiento o la normativa asociada a su marco. Puede utilizar esta palabra clave para buscar su marco.
6. En Etiquetas, seleccione Añadir nueva etiqueta para asociar una etiqueta a su marco. Puede especificar una clave y un valor para cada etiqueta. La clave de la etiqueta es obligatoria y se puede utilizar como criterio de búsqueda al buscar este marco en la biblioteca de marcos.
7. Elija Next (Siguiente).

Paso 2: especificar conjuntos de controles

Los conjuntos de controles se transfieren del marco original. Cambie la configuración actual añadiendo más controles o eliminando los existentes según sea necesario.

> **Note**
>
> Al utilizar la consola de Audit Manager para crear un marco personalizado, puede añadir hasta 10 conjuntos de controles para cada marco.
> Cuando utiliza la API de Audit Manager para crear un marco personalizado, puede añadir más de 10 conjuntos de controles. Para añadir más conjuntos de controles de los que permite actualmente la consola, utilice la CreateAssessmentFrameworkAPI que proporciona Audit Manager.

Especificación de un conjunto de controles

1. En Nombre del conjunto de controles, cambie el nombre del conjunto de controles según sea necesario.
2. En Añadir controles, añada un nuevo control mediante la lista desplegable para seleccionar uno de los dos tipos de control: Controles estándar o Controles personalizados.
3. Según la opción que haya seleccionado en el paso anterior, se muestra una lista de controles estándar o controles personalizados. Seleccione uno o varios controles y elija Añadir al conjunto de controles.
4. En la ventana emergente que aparece, seleccione Añadir al conjunto de controles.
5. Revise los controles que aparecen en la lista Controles seleccionados.
   - Para añadir más controles, repita los pasos 2 a 4.
   - Para eliminar los controles no deseados, seleccione uno o varios controles y elija Eliminar control.
6. Para añadir un nuevo conjunto de controles al marco, seleccione Añadir conjunto de controles.
7. Para eliminar un conjunto de controles no deseado, seleccione Eliminar conjunto de controles.
8. Cuando termine de añadir conjuntos de controles y controles, elija Siguiente.

Paso 3: revisar y crear el marco

Revise la información de su marco. Para modificar la información de un paso, seleccione Editar.

Cuando haya terminado, elija Crear un marco personalizado.

Pasos a seguir a continuación

Después de crear el nuevo marco personalizado, puede crear una evaluación a partir del marco. Para obtener más información, consulte Crear una evaluación en AWS Audit Manager.

Para revisitar el marco personalizado más adelante, consulte Encontrando los marcos disponibles en AWS Audit Manager. Puede seguir estos pasos para localizar el marco personalizado y poder verlo, editarlo, compartirlo o eliminarlo.

Recursos adicionales

Para obtener soluciones a problemas relacionados con los marcos en Audit Manager, consulte Solución de problemas con los marcos.

Edición de un marco personalizado en AWS Audit Manager

Es posible que necesite modificar sus marcos personalizados a medida AWS Audit Manager que cambien sus requisitos de conformidad.

En esta página se describen los pasos para editar los detalles y los conjuntos de controles de un marco personalizado.

Requisitos previos

En el siguiente procedimiento se da por sentado que ha creado previamente un marco personalizado.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para editar un marco personalizado en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Tareas

- Paso 1: editar los detalles del marco
- Paso 2: editar conjuntos de controles
- Paso 3. Revisar y guardar

Paso 1: editar los detalles del marco

Comience por revisar y editar los detalles del marco existente.

Para editar los detalles del marco

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija la Biblioteca de marcos y, a continuación, elija la pestaña Marcos personalizados.
3. Seleccione el marco que desee editar, elija Acciones y, a continuación, elija Editar.
    - Como alternativa, abra un marco personalizado y seleccione Editar en la parte superior derecha de la página de detalles del marco.

4. En Detalles del marco, revise el nombre, el tipo de conformidad y la descripción del marco, y realice los cambios necesarios.
5. Elija Next (Siguiente).

> **Tip**
>
> Para editar las etiquetas de un marco, abra el marco y elija la pestaña de etiquetas del marco. Allí puede ver y editar las etiquetas asociadas al marco.

Paso 2: editar conjuntos de controles

A continuación, revise y edite los controles y conjuntos de controles del marco.

> **Note**
>
> Cuando utiliza la AWS Audit Manager consola para editar un marco personalizado, puede añadir hasta 10 conjuntos de controles para cada marco.
> Cuando utiliza la API de Audit Manager para editar un marco personalizado, puede añadir más de 10 conjuntos de controles. Para añadir más conjuntos de controles de los que permite actualmente la consola, utilice la UpdateAssessmentFrameworkAPI que proporciona Audit Manager.

Edición de un conjunto de controles

1. En Nombre del conjunto de controles , revise y edite el nombre del conjunto de controles según sea necesario.
2. En Añadir controles, utilice la lista desplegable Tipo de control para seleccionar uno de los dos tipos de controles: Controles estándar o Controles personalizados.
3. En función de la opción que haya seleccionado en el paso anterior, se mostrará una lista de controles estándar o controles personalizados. Seleccione uno o varios controles y elija Añadir al conjunto de controles.
4. En la ventana emergente que aparece, seleccione Añadir.
5. Revise y edite los controles que aparecen en la lista Controles seleccionados.
   - Para añadir más controles, repita los pasos 2 a 4.

- Para eliminar los controles no deseados, seleccione uno o varios controles y elija Eliminar del conjunto de controles.

6. Para añadir un nuevo conjunto de controles al marco, seleccione Añadir conjunto de controles.
7. Para eliminar un conjunto de controles no deseado, seleccione Eliminar conjunto de controles.
8. Cuando termine de añadir conjuntos de controles y controles, elija Siguiente.

Paso 3. Revisar y guardar

Revise la información de su marco. Para modificar la información de un paso, seleccione Editar.

Cuando haya finalizado, elija Save changes (Guardar cambios).

Pasos a seguir a continuación

Cuando tenga la certeza de que ya no necesita un marco personalizado, elimínelo para limpiar el entorno de Audit Manager. Para obtener instrucciones, consulte Eliminar un marco personalizado en AWS Audit Manager.

Recursos adicionales

Para obtener soluciones a problemas relacionados con los marcos en Audit Manager, consulte Solución de problemas con los marcos.

Compartir un marco personalizado en AWS Audit Manager

Puede utilizar la función de uso compartido de marcos AWS Audit Manager para replicar rápidamente los marcos personalizados que cree. Puede compartir sus marcos personalizados con otro Cuenta de AWS o replicar sus marcos en otro Región de AWS bajo su propia cuenta. A continuación, el destinatario podrá acceder a su marco personalizado y utilizarlo para crear evaluaciones. Pueden hacerlo sin tener que repetir ninguno de sus esfuerzos de configuración para ese marco.

Puntos clave

Para compartir un marco personalizado, debe crear una solicitud de uso compartido. El destinatario de la solicitud de uso compartido tiene entonces 120 días para aceptarla o rechazarla. Cuando

aceptan la solicitud de uso compartido, Audit Manager replica el marco personalizado compartido en su biblioteca de marcos. Además de replicar el marco personalizado, Audit Manager también replica todos los conjuntos de controles personalizados y los controles personalizados que formen parte de ese marco. Estos controles personalizados se agregan luego a la biblioteca de controles del destinatario. Audit Manager no replica los marcos o controles estándar. De forma predeterminada, están disponibles en todas las Cuentas de AWS y regiones en las que Audit Manager esté activado.

La característica para compartir marcos solo está disponible en el nivel de pago. Sin embargo, no hay cargos adicionales por compartir un marco personalizado o por aceptar una solicitud de uso compartido. Para obtener más información sobre los precios AWS Audit Manager, consulta la página AWS Audit Manager de precios.

> **Important**
>
> No puede compartir un marco personalizado derivado de un marco estándar si el marco estándar ha sido designado como no apto para compartir AWS, a menos que haya obtenido el permiso del propietario del marco estándar para hacerlo. Para ver qué marcos estándar no se pueden compartir y obtener más información, consulte Elegibilidad para compartir marcos.

Recursos adicionales

Para obtener más información sobre cómo compartir marcos personalizados en Audit Manager, consulte los siguientes recursos.

- Conceptos y terminología del uso compartido de marcos
- Envío de una solicitud para compartir un marco personalizado en AWS Audit Manager
- Respuesta a las solicitudes de uso compartido en AWS Audit Manager
- Eliminación de solicitudes de uso compartido en AWS Audit Manager

Conceptos y terminología del uso compartido de marcos

Si conoce los siguientes conceptos clave, puede sacar más provecho de la característica de uso compartido de marcos personalizados AWS Audit Manager .

Puntos clave

Remitente

Este es el creador de una solicitud de uso compartido y el Cuenta de AWS lugar donde existe el marco personalizado. Los remitentes pueden compartir marcos personalizados con cualquiera Cuenta de AWS. O bien, replican un marco personalizado en cualquier Región de AWS marco compatible con su propia cuenta.

Recipient

Es el consumidor del marco compartido. Los destinatarios pueden aceptar o rechazar una solicitud de uso compartido de un remitente.

> **Note**
>
> Un destinatario puede ser una cuenta de administrador delegado. Sin embargo, no puede compartir marcos personalizados con una cuenta AWS Organizations de administración.

Elegibilidad del marco

Solo puede compartir marcos personalizados. De forma predeterminada, los marcos estándar ya están presentes en todos Cuentas de AWS los Regiones de AWS lugares donde AWS Audit Manager están habilitados. Además, los marcos personalizados que comparta no deben contener datos confidenciales. Esto incluye los datos que se encuentran en el propio marco, sus conjuntos de controles y cualquiera de los controles personalizados que forman parte del marco personalizado.

> **Important**
>
> Algunos de los marcos estándar que ofrece AWS Audit Manager contienen material protegido por derechos de autor que está sujeto a acuerdos de licencia. Los marcos personalizados pueden contener contenido derivado de estos marcos. No puede compartir un marco personalizado derivado de un marco estándar si el marco estándar ha sido designado como no apto para su uso compartido AWS, a menos que haya obtenido el permiso del propietario del marco estándar para hacerlo.
> Para saber qué marcos estándar se pueden compartir, consulte la siguiente tabla.

Nombre del marco estándar	Versiones personalizadas aptas para compartir
Australian Cyber Security Center (ACSC) Essential Eight	Sí
Australian Cyber Security Center (ACSC) Information Security Manual (ISM) 02 March 2023	Sí
Marco de prueba de Amazon Web Services (AWS) Audit Manager	Sí
Medidas de seguridad de AWS Control Tower	Sí
AWS Marco generativo de mejores prácticas de IA (versión 2)	Sí
AWS License Manager	Sí
AWS Mejores prácticas fundamentales de seguridad	Sí
AWS Mejores prácticas operativas	Sí

Nombre del marco estándar	Versiones personalizadas aptas para compartir
Marco de Amazon Web Services (AWS) Well-Architected (WAF) v10	Sí
Canadian Centre for Cyber Security (CCCS) Medium Cloud Control	No
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Nivel 1	No
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, Nivel 1 y 2	No
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Nivel 1	No
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, Nivel 1 y 2	No
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Nivel 1	No
Center for Internet Security (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, Nivel 1 y 2	No

Nombre del marco estándar	Versiones personalizadas aptas para compartir
Center for Internet Security (CIS) v7.1, IG1	Sí
CIS Critical Security Controls versión 8.0 (CIS v8.0), IG1	No
Federal Risk And Authorization Management Program (FedRAMP) Security Baseline Controls r4, Moderate	Sí
General Data Protection Regulation (GDPR) 2016	Sí
Gramm-Leach-Bliley Ley (GLBA)	Sí
Title 21 Code of Federal Regulations (CFR) Part 11, Electronic records; Electronic Signatures - Scope and Application 24 May 2023	Sí
EudraLex - La normativa que regula los medicamentos en la Unión Europea (UE) - Volumen 4: Medicamentos con buenas prácticas de fabricación (BMP) para uso humano y veterinario - Anexo 11	Sí
Health Insurance Portability and Accountability Act (HIPAA) Security Rule: Feb 2003	Sí

Nombre del marco estándar	Versiones personalizadas aptas para compartir
Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule	Sí
International Organization for standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2013 Annex A	No
NIST 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations	Sí
Marco de NIST Cybersecurity (CSF) v1.1	Sí
NIST 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	Sí
Payment Card Industry Data Security Standard (PCI DSS) v3.2.1	No
Payment Card Industry Data Security Standard (PCI DSS) v4.0	No
Statement on Standards for Attestations Engagement (SSAE) No. 18, Service Organizations Controls (SOC) Report 2	No

Solicitud de uso compartido

Para compartir un marco personalizado, debe crear una solicitud de uso compartido. La solicitud de uso compartido especifica un destinatario y le notifica que hay un marco personalizado disponible. Los destinatarios tienen 120 días para aceptar o rechazar una solicitud de uso compartido. Si no se realiza ninguna acción en 120 días, la solicitud de uso compartido vence y el destinatario pierde la posibilidad de añadir el marco personalizado a su biblioteca de marcos. Los remitentes y los destinatarios pueden ver las solicitudes de uso compartido y tomar medidas al respecto desde la página de solicitudes de uso compartido de la biblioteca de marcos.

Estado de la solicitud de uso compartido

Las solicitudes de uso compartido pueden tener cualquiera de los siguientes estados.

Estado	Descripción
Activo	Indica una solicitud de uso compartido que se envió correctam ente al destinatario y que está esperando su respuesta.
Vencimiento	Indica una solicitud de uso compartido que vence en los próximos 30 días.
Compartido	Indica una solicitud de uso compartido que el destinatario ha aceptado.
Inactivo	Indica que se trata de una solicitud de uso compartido que se revocó, rechazó o expiró antes de que el destinatario tomara medidas.
En proceso de replicación	Indica una solicitud de uso compartido aceptada que se está replicando en la biblioteca de marcos del destinatario.
Con error	Indica que la solicitud de uso compartido no se envió correctam ente al destinatario.

Notificaciones de solicitud de uso compartido

Audit Manager notifica a los destinatarios cuando reciben una solicitud de uso compartido. Tanto los destinatarios como los remitentes reciben una notificación cuando una solicitud de uso compartido vence dentro de los próximos 30 días.

- Para los destinatarios, aparece un punto de notificación azul junto a las solicitudes recibidas con el estado Activo o Vencido. El destinatario puede resolver la notificación aceptando o rechazando la solicitud de uso compartido.
- En el caso de los remitentes, aparece un punto de notificación azul junto a las solicitudes enviadas con el estado de Vencido. La notificación se resuelve cuando el destinatario acepta o rechaza la solicitud. De lo contrario, se resuelve cuando vence la solicitud. Además, el remitente puede resolver la notificación revocando la solicitud de uso compartido.

Titularidad del remitente

Los remitentes mantienen el acceso total a los marcos personalizados que comparten. Pueden cancelar las solicitudes de uso compartido activas en cualquier momento revocando la solicitud de uso compartido antes de que caduque. Sin embargo, una vez que el destinatario acepta una solicitud de uso compartido, el remitente ya no puede revocar el acceso del destinatario a ese marco personalizado. Esto se debe a que, cuando el destinatario acepta la solicitud, Audit Manager crea una copia independiente del marco personalizado en la biblioteca de marcos del destinatario.

Además de replicar el marco personalizado del remitente, Audit Manager también replica todos los conjuntos de controles personalizados y los controles personalizados que formen parte de ese marco. Sin embargo, Audit Manager no replica ninguna etiqueta adjunta al marco personalizado.

Titularidad del destinatario

Los destinatarios tienen acceso total a los marcos personalizados que aceptan. Cuando el destinatario acepta la solicitud, Audit Manager replica el marco personalizado en la pestaña marcos personalizados de su biblioteca de marcos. Los destinatarios pueden administrar el marco personalizado compartido de la misma manera que cualquier otro marco personalizado. Los destinatarios pueden compartir los marcos personalizados que reciben de otros remitentes. Los destinatarios no pueden impedir que los remitentes envíen solicitudes de uso compartido.

Vencimiento del marco compartido

Cuando un remitente crea una solicitud de uso compartido, Audit Manager establece que la solicitud caduque después de 120 días. Los destinatarios pueden aceptar el marco compartido y obtener acceso a él antes de que caduque la solicitud. Si un destinatario no acepta durante este tiempo, la solicitud de uso compartido caducará. Después de este punto, queda un registro de la solicitud de uso compartido caducada en su historial. Las instantáneas de los marcos compartidos caducados se archivan en un bucket de S3 con un TTL de un año para fines de auditoría.

Los remitentes pueden optar por revocar una solicitud de uso compartido en cualquier momento antes de que caduque.

Almacenamiento y respaldo de datos en un marco compartido

Al crear una solicitud de participación, Audit Manager almacena una instantánea de su marco personalizado en el este de EE. UU. (Virginia del Norte) Región de AWS. Audit Manager también almacena una copia de seguridad de la misma instantánea en el oeste de EE. UU. (Oregón) Región de AWS.

Audit Manager elimina la instantánea y la instantánea de respaldo cuando ocurre uno de los siguientes eventos:

- El remitente revoca la solicitud de uso compartido.
- El destinatario rechaza la solicitud de uso compartido.
- El destinatario detecta un error y no acepta correctamente la solicitud de uso compartido.
- La solicitud de uso compartido caduca antes de que el destinatario responda a la solicitud.

Cuando un remitente vuelve a enviar una solicitud de uso compartido, la instantánea se sustituye por una versión actualizada que se corresponde con la última versión del marco personalizado.

Cuando un destinatario acepta una solicitud de compartición, la instantánea se replica en su interior Cuenta de AWS según Región de AWS lo especificado en la solicitud de compartición.

Control de versiones de un marco compartido

Al compartir un marco personalizado, Audit Manager crea una copia independiente de ese marco en la región Cuenta de AWS AND especificada. Esto significa que debe tener en cuenta los siguientes puntos:

- El marco compartido que acepta el destinatario es una instantánea del marco en el momento de la creación de la solicitud de uso compartido. Si actualiza el marco personalizado original después de enviar una solicitud de uso compartido, la solicitud no se actualiza automáticamente. Para compartir la última versión del marco actualizado, puede volver a enviar la solicitud de uso compartido. La fecha de caducidad de esta nueva instantánea es de 120 días a partir de la fecha en que se volvió a compartir.
- Cuando comparte un marco personalizado con otro Cuenta de AWS y, a continuación, lo elimina de su biblioteca de marcos, el marco personalizado compartido permanece en la biblioteca de marcos del destinatario.

- Cuando compartes un marco personalizado Región de AWS con otra persona en tu cuenta y, a continuación, eliminas ese marco personalizado en la primera Región de AWS, el marco personalizado permanece en la segunda región.
- Al eliminar un marco personalizado compartido después de aceptarlo, los controles personalizados que se hayan replicado como parte del marco personalizado permanecen en la biblioteca de controles.

Recursos adicionales

- Envío de una solicitud para compartir un marco personalizado en AWS Audit Manager
- Respuesta a las solicitudes de uso compartido en AWS Audit Manager
- Eliminación de solicitudes de uso compartido en AWS Audit Manager
- Solución de problemas con los marcos

Envío de una solicitud para compartir un marco personalizado en AWS Audit Manager

Este tutorial describe cómo compartir sus marcos personalizados entre Cuentas de AWS y Regiones de AWS.

Cuando comparte un marco personalizado, Audit Manager crea una instantánea del marco y envía una solicitud de uso compartido al destinatario. El destinatario tiene 120 días para aceptar el marco compartido. Cuando lo aceptan, Audit Manager replica el marco personalizado compartido en su biblioteca de marcos en el Región de AWS especificado. Si desea replicar un marco personalizado en otra región con su propia cuenta, utilice el siguiente tutorial e introduzca su propio Cuenta de AWS identificador como identificador de la cuenta del destinatario.

Requisitos previos

Antes de comenzar este tutorial, asegúrese de cumplir las siguientes condiciones:

- Está familiarizado con la terminología y los conceptos de uso compartido del marco de Audit Manager.
- El marco personalizado que desea compartir es apto para compartirse y existe en la biblioteca de marcos de su entorno de AWS Audit Manager .

- El destinatario ya está activado AWS Audit Manager en el Región de AWS lugar donde desea compartir el marco personalizado.
- El destinatario no es una cuenta AWS Organizations de administración.
- Su identidad de IAM tiene los permisos adecuados para compartir un marco personalizado en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

> **Tip**
>
> Antes de empezar, anote el Cuenta de AWS ID con el que desea compartir su marco personalizado. Este puede ser tu propio identificador de cuenta si tu objetivo es replicar el framework en otro usuario Región de AWS de tu cuenta. Necesita esta información para el paso 2 del tutorial.

Procedimiento

Tareas

- Paso 1: identifique el marco personalizado que desea compartir
- Paso 2: Enviar una solicitud de uso compartido
- Paso 3: ver las solicitudes enviadas
- Paso 4 (opcional): revocar la solicitud de uso compartido

Paso 1: identifique el marco personalizado que desea compartir

Comience por identificar el marco personalizado que desea compartir. Puede encontrar una lista de todos los marcos personalizados disponibles en la página de la Biblioteca de marcos de Audit Manager.

> **Important**
>
> No comparta marcos personalizados que contengan datos confidenciales. Esto incluye los datos que se encuentran dentro del propio marco, sus conjuntos de controles y cualquiera

de los controles personalizados que componen el marco personalizado. Para obtener más información, consulte el Elegibilidad del marco.

Visualización de los marcos personalizados disponibles

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Biblioteca de marcos.
3. Elija la pestaña Marcos personalizados. Esto muestra una lista de los marcos personalizados disponibles. Puede elegir cualquier nombre de marco para ver los detalles de ese marco personalizado.

Paso 2: Enviar una solicitud de uso compartido

A continuación, especifique un destinatario y envíele una solicitud de uso compartido del marco personalizado. El destinatario tiene 120 días para responder a la solicitud de uso compartido antes de que caduque.

Para enviar una solicitud de uso compartido

1. En la pestaña Marcos personalizados de la biblioteca de marcos, elija el nombre de un marco para abrir la página de detalles. Desde aquí, seleccione Acciones y, a continuación, seleccione Compartir marco personalizado.
   - También puede seleccionar un marco personalizado de la lista de la biblioteca de marcos, elegir Acciones y, a continuación, elegir Compartir marco personalizado. Según el tamaño del marco personalizado, este método puede tardar unos segundos mientras Audit Manager prepara la solicitud de uso compartido.
2. Revise el aviso que aparece en el cuadro de diálogo.
   - Si no está seguro de si puede compartir su marco personalizado, consulte la Elegibilidad del marco para obtener más información.
   - Si su marco tiene controles que utilizan AWS Config reglas personalizadas como fuente de datos, le recomendamos que se ponga en contacto con el destinatario para hacérselo saber. A continuación, el destinatario podrá crear y habilitar las mismas AWS Config reglas en su instancia de AWS Config. Para obtener más información, consulte Mi marco compartido tiene controles que utilizan AWS Config reglas personalizadas como fuente de datos. ¿Puede el destinatario recopilar pruebas para estos controles?.

3. Introduzca **`agree`** y, a continuación, seleccione Aceptar para continuar.
4. En la siguiente pantalla, siga estos pasos:
   - En Cuenta de AWS, introduzca la ID de cuenta del destinatario. Puede ser su propia ID de cuenta.
   - En Región de AWS, seleccione la región del destinatario en la lista desplegable.
   - (Opcional) En Enviar mensaje al destinatario, introduzca un comentario opcional sobre el marco personalizado que va a compartir.
   - En Detalles del marco personalizado, revise los detalles para confirmar que desea compartir este marco.
5. Elija Compartir.

> **Note**
>
> Tenga en cuenta los siguientes puntos:
>
> - Al compartir un marco personalizado con otro Cuenta de AWS, el marco se replica solo en el especificado Región de AWS. Tras aceptar la solicitud de uso compartido, el destinatario podrá replicar el marco en todas las regiones según sea necesario.
> - Al compartir marcos personalizados entre sí Regiones de AWS, procesar las acciones de las solicitudes de uso compartido puede tardar hasta 10 minutos. Tras enviar una solicitud de uso compartido entre regiones, le recomendamos que vuelva a consultarla más tarde para confirmar que la solicitud se ha enviado correctamente.
> - Al enviar una solicitud de uso compartido, Audit Manager toma una instantánea del marco personalizado en el momento de la creación de la solicitud de uso compartido. Si actualiza el marco personalizado después de enviar una solicitud de uso compartido, la solicitud no se actualiza automáticamente. Para compartir la última versión de un marco actualizado, puede volver a enviar la solicitud de uso compartido. La fecha de caducidad de esta nueva instantánea es de 120 días a partir de la fecha en que se volvió a compartir.

Paso 3: ver las solicitudes enviadas

Puede seleccionar la pestaña Solicitudes enviadas para ver una lista de todas las solicitudes de uso compartido que ha enviado. Puede filtrar esta lista según sea necesario. Por ejemplo, puede aplicar filtros para mostrar solo las solicitudes que caduquen en los próximos 30 días.

Visualización y filtro de las solicitudes enviadas

1. En el panel de navegación, elija Solicitudes de uso compartido.
2. Seleccione la pestaña Solicitudes enviadas.
3. (Opcional) Aplique filtros para ajustar qué solicitudes enviadas están visibles. Para ello, busque la lista desplegable Todos los estados y cambia el filtro por uno de los siguientes.

Estado	Descripción
Activo	Este filtro muestra las solicitudes de uso compartido que están pendientes de respuesta por parte del destinatario.
Vencimiento	Este filtro muestra las solicitudes de uso compartido que vencen en los próximos 30 días.
Compartido	Este filtro muestra las solicitudes de uso compartido que ha aceptado el destinatario. El marco personalizado compartido ahora existe en la biblioteca de marcos del destinatario.
Inactivo	Este filtro muestra las solicitudes de uso compartido que se rechazaron, revocaron o vencieron antes de que el destinatario actuara. Elija la palabra Inactivo para ver más detalles.
En proceso de replicación	Indica una solicitud de uso compartido aceptada que se está replicando en la biblioteca de marcos del destinatario.
Con error	Este filtro muestra las solicitudes de uso compartido que no se enviaron correctamente al destinatario. Seleccione la palabra Falló para ver más detalles.

> **Note**
>
> El procesamiento de una solicitud de uso compartido puede tardar hasta 15 minutos en procesarse. En consecuencia, si se produce un error al enviar la solicitud de uso compartido al destinatario, es posible que el estado Falló no se muestre inmediatamente. Le

recomendamos que vuelva a comprobarlo más tarde para confirmar que su solicitud de uso compartido se ha enviado correctamente.

Paso 4 (opcional): revocar la solicitud de uso compartido

Si necesita cancelar una solicitud de uso compartido activa antes de que caduque, puede revocar la solicitud en cualquier momento. Este paso es opcional. Si no realiza ninguna acción, el destinatario pierde la capacidad de aceptar la solicitud de uso compartido después de la fecha de caducidad.

Para revocar una solicitud de uso compartido

1. En el panel de navegación, elija Solicitudes de uso compartido.
2. Seleccione la pestaña Solicitudes enviadas.
3. Seleccione el marco que desee revocar y elija Revocar solicitud.
4. En la ventana emergente que aparece, seleccione Revocar.

> **Note**
>
> Sólo puede revocar el acceso a las solicitudes de uso compartido que tengan un estado Activo o Vencido. Una vez que el destinatario acepte una solicitud de uso compartido, ya no podrá revocar su acceso a ese marco personalizado. Esto se debe a que ahora existe una copia del marco personalizado en la biblioteca de marcos del destinatario.
> Al compartir distintos marcos Regiones de AWS, procesar las acciones de las solicitudes de compartición puede tardar hasta 10 minutos. Después de revocar una solicitud de uso compartido entre regiones, le recomendamos que vuelva a comprobarlo más tarde para confirmar que la solicitud de uso compartido se ha revocado correctamente.

Pasos a seguir a continuación

Reenviar una solicitud de uso compartido para actualizar el marco

Puede enviar una solicitud de uso compartido para un marco personalizado y luego actualizar el mismo marco. Si lo hace, la solicitud de uso compartido no se actualiza automáticamente para reflejar la última versión del marco. Sin embargo, si su estado es activo, compartido o vencido, puede actualizar una solicitud de uso compartido existente. Para ello, debe volver a enviar una nueva

solicitud de uso compartido con el mismo conjunto de detalles que la solicitud existente. En la nueva solicitud de uso compartido, incluya la misma identificación de marco personalizado, la identificación de cuenta del destinatario y Región de AWS del destinatario. También puede incluir un comentario nuevo con la nueva solicitud de uso compartido.

Tenga en cuenta lo siguiente al volver a enviar una solicitud para uso compartido:

- Para que la actualización se realice correctamente, la nueva solicitud debe ser para la misma ID de marco personalizado. También debe especificar la misma ID de cuenta del destinatario y la misma región que la solicitud existente.
- Si el nombre del marco personalizado ha cambiado, la solicitud de uso compartido actualizada muestra el nombre más reciente.
- Si proporciona un comentario nuevo, la solicitud de uso compartido actualizada muestra el comentario más reciente.
- Al volver a enviar una solicitud de uso compartido, la fecha de caducidad se amplía seis meses.

Para volver a enviar una solicitud de uso compartido en un marco actualizado

1. En la pestaña Marcos personalizados de la biblioteca de marcos,marcos, elija el nombre del marco que desea compartir. Se abrirá la página de detalles del marco.
2. Seleccione Acciones y luego Compartir marco personalizado.
3. Revise el aviso que aparece en el cuadro de diálogo, escriba **`agree`**, y a continuación, elija Aceptar para continuar.
4. En la siguiente pantalla, siga estos pasos:
   - En Cuenta de AWS, introduzca la misma ID de cuenta que especificó en la solicitud de uso compartido existente.
   - En Región de AWS, seleccione la misma región que especificó en la solicitud de uso compartido existente.
   - (Opcional) En Mensaje al destinatario, introduzca un comentario opcional sobre el marco personalizado actualizado.
   - En Detalles del marco personalizado, revise los detalles para confirmar que desea reenviar la solicitud de uso compartido.
5. Seleccione Compartir para volver a enviar y actualizar la solicitud de uso compartido.

Recursos adicionales

Para encontrar soluciones a los problemas que pueden surgir al compartir un marco personalizado, consulte Solución de problemas con los marcos.

Respuesta a las solicitudes de uso compartido en AWS Audit Manager

Este tutorial describe las acciones que debe tomar cuando recibe una solicitud de uso compartido para un marco personalizado. Audit Manager le notifica cuando recibe una solicitud de uso compartido. También recibirá una notificación para recordarle cuándo vence una solicitud de uso compartido en los próximos 30 días.

Requisitos previos

Antes de empezar, le recomendamos que primero obtenga más información sobre el marco de trabajo de Audit Manager que comparte conceptos y terminología.

Procedimiento

Tareas

- Paso 1: compruebe las notificaciones de solicitudes recibidas
- Paso 2: tome medidas con respecto a la solicitud
- Paso 3: consulte un historial de las solicitudes recibidas

Paso 1: compruebe las notificaciones de solicitudes recibidas

Empiece por revisar sus notificaciones de solicitud de uso compartido. La pestaña Solicitudes recibidas muestra una lista de las solicitudes de uso compartido que has recibido de otras personas Cuentas de AWS. Las solicitudes que están pendientes de su respuesta aparecen con un punto azul. También puede filtrar esta vista para que muestre solo las solicitudes que venzan dentro de los próximos 30 días.

Para ver las solicitudes recibidas

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. Si tiene una notificación de solicitud de uso compartido, Audit Manager muestra un punto rojo junto al icono del menú de navegación.

3. Despliegue el panel de navegación y busque junto a Solicitudes de uso compartido. Una insignia de notificación indica el número de solicitudes de uso compartido que requieren tu atención.

4. Seleccione Solicitudes de uso compartido. De forma predeterminada, esta página se abre en la pestaña Solicitudes recibidas.
5. Busque los elementos con un punto azul para identificar las solicitudes de uso compartido que requieren su acción.

6. (Opcional) Para ver solo las solicitudes que caducan en los próximos 30 días, busque la lista desplegable Todos los estados y seleccione A punto de vencer.

Paso 2: tome medidas con respecto a la solicitud

Para eliminar el punto azul de notificación, debe aceptar o rechazar la solicitud de uso compartido.

Aceptar un marco compartido

Cuando acepta una solicitud de uso compartido, Audit Manager replica una instantánea del marco original en la pestaña marcos personalizados de su biblioteca de marcos. Audit Manager replica y cifra el nuevo marco personalizado mediante la clave KMS que especificó en la configuración de Audit Manager.

Para aceptar una solicitud de uso compartido

1. Abra la página de Solicitudes de uso compartido y asegúrese de ver la pestaña Solicitudes recibidas.
2. (Opcional) Seleccione Activo o Vencido en la lista desplegable de filtros.
3. (Opcional) Elija un nombre de marco para ver los detalles de la solicitud de uso compartido. Esto incluye información como la descripción del marco, el número de controles que hay en el marco y el mensaje del remitente.
4. Seleccione la solicitud de uso compartido que desee aceptar, elija Acciones y, a continuación, elija Aceptar.

Tras aceptar una solicitud de uso compartido, el estado cambia a en proceso de replicaciónmientras se agrega el marco personalizado compartido a la biblioteca de marcos. Si el marco contiene controles personalizados, estos controles se añaden a la biblioteca de controles en este momento.

Cuando se completa la replicación del marco, el estado cambia a compartido. Un aviso de éxito le notifica que el marco personalizado está listo para usarse.

> **Tip**
>
> Cuando acepta un marco personalizado, solo se replica en su Región de AWS actual. Es posible que desee que el nuevo marco compartido esté disponible en todas las regiones de su Cuenta de AWS. En caso afirmativo, una vez aceptada la solicitud de uso compartido, podrá compartir el marco con otras regiones de su cuenta según sea necesario.

Rechazar un marco compartido

Cuando rechaza una solicitud de uso compartido, Audit Manager no añade ese marco personalizado a su biblioteca de marcos. Sin embargo, en la pestaña Solicitudes recibidas queda un registro de la solicitud de uso compartido rechazada, con el estado Inactivo.

Para rechazar una solicitud de uso compartido

1. Abra la página de Solicitudes de uso compartido y asegúrese de ver la pestaña Solicitudes recibidas.
2. (Opcional) Seleccione Activo o Vencido en la lista desplegable de filtros.

3. (Opcional) Elija un nombre de marco para ver los detalles de la solicitud de uso compartido. Esto incluye información como la descripción del marco, el número de controles que hay en el marco y el mensaje del remitente.
4. Seleccione la solicitud de uso compartido que desee rechazar, elija Acciones y, a continuación, elija Rechazar.
5. En el cuadro de diálogo que aparece, seleccione Rechazar para confirmar su elección.

> **Tip**
>
> Si cambia de opinión y quiere acceder a un marco compartido después de rechazarla, pídale al remitente que le envíe una nueva solicitud de uso compartido.

> **Note**
>
> Procesar las acciones de solicitud de uso compartido puede tardar hasta 10 minutos cuando un marco se comparte entre Regiones de AWS. Después de realizar una solicitud de uso compartido entre regiones, le recomendamos que vuelva a comprobarlo más tarde para confirmar si la solicitud ha sido aceptada o rechazada.

Paso 3: consulte un historial de las solicitudes recibidas

Después de aceptar o rechazar un marco compartido, puede volver a la página Solicitudes de uso compartido para ver su historial de solicitudes de uso compartido. Puede filtrar esta lista según sea necesario. Por ejemplo, puede aplicar filtros para mostrar solo las solicitudes que ha aceptado.

Para ver un historial de sus solicitudes de uso compartido

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Solicitudes de uso compartido.
3. Seleccione la pestaña Solicitudes recibidas.
4. Busque la lista desplegable Todos los estados y seleccione uno de los siguientes filtros:

Nombre	Descripción
Activo	Este filtro muestra las solicitudes de uso compartido que aún no ha aceptado o rechazado.
Vencimiento	Este filtro muestra las solicitudes de uso compartido que vencen en los próximos 30 días.
Compartido	Este filtro muestra las solicitudes de uso compartido que ha aceptado. El marco compartido ahora está disponible en su biblioteca de marcos.
Inactivo	Este filtro muestra las solicitudes de uso compartido que se rechazaron o vencieron.
Con error	Este filtro muestra las solicitudes de uso compartido que no se enviaron correctamente. Seleccione la palabra Falló para ver más detalles.

Pasos a seguir a continuación

Después de aceptar un marco personalizado compartido, lo encontrará en la pestaña de marcos personalizados de la biblioteca de marcos. Ahora puede usar ese marco para crear una evaluación. Para obtener más información, consulte Crear una evaluación en AWS Audit Manager.

Para obtener instrucciones sobre cómo editar el marco personalizado nuevo, consulte Edición de un marco personalizado en AWS Audit Manager.

Recursos adicionales

Para encontrar soluciones a los problemas que puedan surgir, consulte Solución de problemas con los marcos.

Eliminación de solicitudes de uso compartido en AWS Audit Manager

Cuando ya no necesite una solicitud de uso compartido, puede eliminarla del entorno de Audit Manager. Esto le permite limpiar su espacio de trabajo y centrarse en las solicitudes que son pertinentes para sus tareas y prioridades actuales.

Al eliminar una solicitud de uso compartido, solo se elimina la solicitud en sí. El marco compartido en sí permanece en su biblioteca de marcos.

Requisitos previos

En el siguiente procedimiento se da por sentado que ya ha enviado o recibido una solicitud de uso compartido. No puede eliminar las solicitudes de uso compartido que estén activas o en proceso de replicación.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para eliminar una solicitud de uso compartido en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Para eliminar una solicitud de uso compartido

1. En el panel de navegación, elija Solicitudes de uso compartido.
2. Seleccione la pestaña Solicitudes enviadas o Solicitudes recibidas.
3. Seleccione el marco que ya no desee y pulse Eliminar.
4. En la ventana emergente que aparece, seleccione Eliminar.

Recursos adicionales

Para encontrar soluciones a los problemas que puedan surgir, consulte Solución de problemas con los marcos.

Eliminar un marco personalizado en AWS Audit Manager

Cuando ya no necesite un marco personalizado, puede eliminarlo del entorno de Audit Manager. Esto le permite limpiar su espacio de trabajo y centrarse en los marcos personalizados que son pertinentes para sus tareas y prioridades actuales.

Requisitos previos

En el siguiente procedimiento se da por sentado que ha creado previamente un marco personalizado.

Asegúrese de que su identidad de IAM tiene los permisos adecuados para eliminar un marco personalizado. AWS Audit Manager Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Puede eliminar marcos personalizados mediante la consola de Audit Manager, la API de Audit Manager o AWS Command Line Interface (AWS CLI).

> **Note**
>
> La eliminación de un marco personalizado no afecta a ninguna evaluación existente que se haya creado a partir del marco antes de su eliminación.

Audit Manager console

Eliminación de un marco personalizado de la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija la Biblioteca de marcos y, a continuación, elija la pestaña Marcos personalizados.
3. Seleccione el marco que desee eliminar, elija Acciones y, a continuación, elija Eliminar.
   - Como alternativa, puede abrir un marco personalizado y elegir Acciones y Eliminar en la parte superior derecha de la página de resumen del marco.
4. En la ventana emergente, seleccione Eliminar para confirmar la eliminación.

AWS CLI

Para eliminar un marco personalizado en el AWS CLI

1. En primer lugar, identificar el marco personalizado que desea eliminar. Para ello, ejecute el list-assessment-frameworkscomando y especifique el `--framework-type` as`Custom`.

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

La respuesta devuelve una lista de marcos personalizados. Busque el marco personalizado que desea eliminar y tome nota del ID del marco.

2. A continuación, ejecute el delete-assessment-framework`--framework-id`comando y especifique el marco que desea eliminar.

   En el siguiente ejemplo, sustituya el *`placeholder text`* por su propia información.

   ```
   aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Eliminación de un marco personalizado mediante la API

1. Utilice la ListAssessmentFrameworksoperación y especifique el FrameworkType como. `Custom` En la respuesta, busque el marco personalizado que desea eliminar y anote el ID del marco.
2. Utilice la DeleteAssessmentFrameworkoperación para eliminar el marco. En la solicitud, utilice el parámetro frameworkId para especificar el marco que desea eliminar.

Para obtener más información sobre estas operaciones de la API, consulte cualquiera de los enlaces del procedimiento anterior en la Referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos AWS SDKs.

Recursos adicionales

Para obtener información sobre la retención de datos en Audit Manager, consulte Eliminación de datos de Audit Manager.

Uso de la biblioteca de controles para gestionar los controles en AWS Audit Manager

Puede acceder a los controles y administrarlos desde la biblioteca de controles de AWS Audit Manager.

Puntos clave

En la biblioteca de controles, los controles se organizan en las siguientes categorías.

- Los controles comunes recopilan evidencias que respaldan la superposición de varios estándares de conformidad. Los controles comunes automatizados incluyen uno o varios controles principales relacionados, cada uno de los cuales recopila evidencias de respaldo de un grupo predefinido de orígenes de datos. Esto le proporciona una forma eficaz de identificar las fuentes de AWS datos que se corresponden con su cartera de requisitos de conformidad. Los asesores certificados por el sector de AWS Security Assurance Services validan y mantienen los orígenes de datos subyacentes de cada control común automatizado.
- Los controles estándar recopilan evidencias para respaldar un determinado estándar de conformidad. Puede ver los detalles de los controles estándar, pero no puede editarlos ni eliminarlos. Sin embargo, puede crear una copia editable de cualquier control estándar para crear uno nuevo que cumpla con sus requisitos específicos.
- Los controles personalizados son controles de su propiedad que puede definir. Al crear un control personalizado, le recomendamos que elija los controles comunes que representen sus objetivos y los utilice como origen de evidencias. Como resultado, el control personalizado puede recopilar todas las evidencias pertinentes para esos controles comunes. También puede usar los controles principales como origen de evidencias o usar otros orígenes que usted mismo defina. Cuando haya terminado, añada los controles personalizados a un marco personalizado y, a continuación, cree una evaluación para empezar a recopilar evidencias.

Recursos adicionales

Para crear y administrar los controles en Audit Manager, siga los procedimientos que se indican aquí.

- Encuentre los controles disponibles en AWS Audit Manager

- Revisar un control en AWS Audit Manager
  - Revisión de un control común
  - Revisión de un control principal
  - Revisión de un control estándar
  - Revisión de un control personalizado
- Crear un control personalizado en AWS Audit Manager
  - Creación de un nuevo control personalizado desde cero en AWS Audit Manager
  - Creación de una copia editable de un control en AWS Audit Manager
- Edición de un control personalizado en AWS Audit Manager
- Cambio de la frecuencia con la que un control recopila evidencias
- Eliminar un control personalizado en AWS Audit Manager
- Tipos de orígenes de datos compatibles para evidencias automatizadas
  - Reglas de AWS Config con el apoyo de AWS Audit Manager
  - AWS Security Hub controles compatibles con AWS Audit Manager
  - AWS Las llamadas a la API son compatibles con AWS Audit Manager
  - AWS CloudTrail nombres de eventos compatibles con AWS Audit Manager

Encuentre los controles disponibles en AWS Audit Manager

Puede buscar todos los controles disponibles en la página Biblioteca de controles de la consola de Audit Manager.

También puede ver todos los controles disponibles mediante la API Audit Manager o AWS Command Line Interface (AWS CLI).

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver los controles. AWS Audit Manager Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Audit Manager console

Visualización de los controles disponibles en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Control de costos.
3. Seleccione una pestaña para examinar los controles disponibles.
   - Elija Common para ver los controles comunes que proporciona AWS.
   - Seleccione Estándar para ver los controles estándar que proporciona AWS.
   - Seleccione Personalizado para ver los controles personalizados que ha creado.

AWS CLI

Búsqueda de controles comunes en la AWS CLI

Ejecute el list-common-controlscomando para ver una lista de los controles más comunes.

```
aws controlcatalog list-common-controls
```

También puede usar el atributo opcional `common-control-filter` para devolver una lista de controles comunes que tengan un objetivo específico.

En el siguiente ejemplo, *`placeholder text`* sustitúyalo por su propia información.

```
aws controlcatalog list-common-controls --common-control-filter OBJECTIVE-ARN
```

Para buscar otros tipos de controles en la AWS CLI

Ejecute el comando list-controls y especifique el `--control-type` como `Custom`, `Standard` o `Core`.

En el siguiente ejemplo, sustituya el *`placeholder text`* por su propia información.

```
aws auditmanager list-controls --control-type Type
```

Audit Manager API

Búsqueda de controles comunes mediante la API

Utilice la ListCommonControlsoperación para ver una lista de los controles comunes disponibles. También puede usar el atributo opcional `commonControlFilter` para devolver una lista de controles que tengan un objetivo específico.

Búsqueda de otros tipos de controles mediante la API

Utilice la ListControlsoperación y especifique el ControlType como `CustomStandard`, o`Core`.

Para obtener más información, consulte cualquiera de los enlaces del procedimiento anterior en la Referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas AWS SDKs específicos.

Pasos a seguir a continuación

Cuando lo tenga todo listo para explorar los detalles de un control, siga los pasos que se indican en Revisar un control en AWS Audit Manager. Esta página le guiará por los detalles de los controles y le explicará la información que aparece.

En la página Biblioteca de controles, también puede crear un control personalizado, editarlo o eliminarlo.

Recursos adicionales

Para obtener soluciones a problemas relacionados con los controles en Audit Manager, consulte Solución de problemas de control y conjunto de control.

Revisar un control en AWS Audit Manager

Puede revisar los detalles de un control mediante la consola de Audit Manager, la API de Audit Manager o AWS Command Line Interface (AWS CLI).

Para empezar a revisar un control en Audit Manager, siga los procedimientos que se indican aquí.

- Revisión de un control común

- Revisión de un control principal
- Revisión de un control estándar
- Revisión de un control personalizado

Revisión de un control común

Cuando necesite revisar los detalles de un control, encontrará la información organizada en varias secciones en la página de detalles del control. Estas secciones le ayudan a acceder fácilmente a la información pertinente para dicho control y a comprenderla.

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver los controles comunes en Audit Manager. Más específicamente, necesita los siguientes permisos para ver los controles, objetivos de control y dominios de control comunes que proporciona AWS Control Catalog:

- `controlcatalog:ListCommonControls`
- `controlcatalog:ListDomains`
- `controlcatalog:ListObjectives`

Una política sugerida para conceder estos permisos es AWSAuditManagerAdministratorAccess.

Procedimiento

Puede revisar un control común mediante la consola Audit Manager, la API de AWS Control Catalog o AWS Command Line Interface (AWS CLI).

Audit Manager console

Visualización de los detalles de los controles comunes en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Control de costos.
3. Elija Common para ver los controles comunes que proporciona AWS.
4. Seleccione el nombre de cualquier control común para ver sus detalles.

5. Revise los detalles del control común con la siguiente información como referencia.

Sección Descripción general

En esta sección se describe el control común.

Pestaña Orígenes de evidencias

En esta pestaña se incluye la siguiente información:

Nombre	Descripción
Controles principales	Estos son los controles principales que recopilan evidencias para respaldar el control común. • Al recopilar evidencias para este control común, se recopilar án automáticamente evidencias para todos los controles principales que se indiquen aquí. Una vez que estos controles principales se implementen correctamente, se demuestra que se cumplen los requisitos del control común. • Cada control principal utiliza una agrupación predefinida de fuentes de datos para recopilar pruebas sobre un Servicio de AWS. AWS administra estas fuentes de datos por usted. Esto significa que se actualizan automáticamente cada vez que cambien las normativas y los estándares y se identifiq uen nuevos orígenes de datos. Elija un control principal para ver los orígenes de datos subyacentes.

Pestaña Requisitos relacionados

Al recopilar evidencias para este control común, las mismas evidencias pueden ayudarle a demostrar la conformidad con los requisitos de los controles estándar relacionados que se indican en esta pestaña. Seleccione cualquier control estándar para ver más detalles.

> **Note**
>
> • El control común puede producir evidencias que demuestren solo la conformidad parcial con un control estándar. Es posible que necesite evidencias adicionales para demostrar la plena conformidad con un control estándar.

- En este momento, la pestaña Requisitos relacionados solo muestra los controles estándar relacionados. Si bien un control común puede estar relacionado con uno o varios controles personalizados, estas relaciones no se muestran en esta pestaña.

AWS CLI

Para ver los detalles de control más comunes en el AWS CLI

1. Ejecute el list-common-controlscomando para ver una lista de los controles comunes disponibles. Al usar esta operación, puede aplicar un `common-control-filter` opcional para ver los controles comunes que tengan un objetivo específico.

```
aws controlcatalog list-common-controls
```

2. En la respuesta, identifique el control común que desee revisar y anote sus detalles.

AWS Control Catalog API

Visualización de los detalles de los controles comunes mediante la API

1. Utilice la ListCommonControlsoperación para ver una lista de los controles comunes disponibles. Al usar esta operación, puede aplicar un `commonControlFilter` opcional para ver una lista de controles que tengan un objetivo específico.
2. En la respuesta, identifique el control que desee revisar y anote sus detalles.

Para obtener más información sobre estas operaciones de la API, consulte el enlace de este procedimiento en la Referencia de la API de AWS Control Catalog. Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos AWS SDKs.

Pasos a seguir a continuación

Puede elegir los controles comunes que representan sus objetivos y utilizarlos como componentes para crear un control personalizado. Cada control común automatizado se asigna a una agrupación predefinida de fuentes de AWS datos que Audit Manager gestiona por usted. Esto significa que no es necesario ser un AWS experto para saber qué fuentes de datos recopilan la evidencia relevante para sus objetivos. Además, no tendrá que mantener estas asignaciones de orígenes de datos.

Para obtener instrucciones sobre cómo crear un control personalizado que utilice controles comunes como origen de evidencia, consulte Crear un control personalizado en AWS Audit Manager.

Recursos adicionales

- Revisión de un control principal
- Revisión de un control estándar
- Revisión de un control personalizado

Revisión de un control principal

Puede revisar los detalles de un control principal mediante la consola Audit Manager, la API Audit Manager o AWS Command Line Interface (AWS CLI).

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver los controles en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Audit Manager console

Visualización de los detalles de los controles principales en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Control de costos.
3. Elija Common para ver los controles comunes que proporciona AWS.
4. Busque el control común que mejor se adapte a su caso de uso.
5. Seleccione el icono de vista en árbol situado junto al nombre del control común. Se mostrarán los controles principales que admiten el control común.
6. Elija el nombre del control principal que desea revisar.
7. Revise los detalles del control principal con la siguiente información como referencia.

Sección Descripción general

En esta sección se describe el control principal y se enumeran los tipos de orígenes de datos de los que se recopilan las evidencias.

Pestaña Orígenes de evidencias

En esta pestaña se incluye la siguiente información:

Nombre	Descripción

Origen de datos	Estas son las fuentes de datos AWS gestionadas de las que el control principal recopila pruebas. Estos orígenes de datos se actualizan automáticamente cada vez que cambien las normativas y los estándares y se identifiquen nuevos orígenes de datos.
	• Asignación: palabra clave específica que se utiliza para recopilar evidencias.
	  • Si el tipo es AWS Config, el mapeo es una AWS Config regla (por ejemplo`SNS_ENCRYPTED_KMS`).
	  • Si el tipo es AWS Security Hub, la asignación es un control de Security Hub (como, por ejemplo, `EC2.1`).
	  • Si el tipo son Llamadas a la API de AWS , la asignación es una llamada a la API (como, por ejemplo, `kms_ListKeys`).
	  • Si el tipo es AWS CloudTrail, el mapeo es un CloudTrail evento (por ejemplo`CreateAccessKey`).
	• Tipo: tipo de origen de datos del que proceden las evidencias.
	  • Si Audit Manager recopila evidencias, el tipo puede ser: AWS Security Hub, AWS Config, AWS CloudTrail o Llamadas a la API de AWS .
	  • Si carga sus propias evidencias, el tipo es Manual. Las descripciones indican si la evidencia manual requerida es una carga de archivos o una respuesta de texto.

Nombre	Descripción
	• Frecuencia: frecuencia con la que Audit Manager recopila pruebas de una fuente de datos de llamadas a la AWS API.

Pestaña Detalles

En esta pestaña se incluye la siguiente información:

Nombre	Descripción
Instrucciones	Las instrucciones que describen cómo probar y corregir el control.
Información de prueba	Los procedimientos de prueba recomendados.
Plan de acción	La acciones recomendadas que se deben tomar si es necesario corregir el control.

AWS CLI

Para ver los detalles de control principales en el AWS CLI

1. Siga los pasos para buscar un control. Asegúrese de configurar el `--control-type` como `Core` y de aplicar los filtros opcionales según sea necesario.

```
aws auditmanager list-controls --control-type Core
```

2. En la respuesta, identifique el control que desea revisar y tome nota del ID de control y del nombre de recurso de Amazon (ARN).
3. Ejecute el comando get-control y especifique el `--control-id`. En el siguiente ejemplo, *`placeholder text`* sustitúyalo por su propia información.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> Los detalles de control se devuelven en formato JSON. Para ayudarle a comprender estos datos, consulte el Resultado de get-control en la Referencia de los comandos de la AWS CLI .

4. Para ver los detalles de la etiqueta, ejecute el list-tags-for-resourcecomando y especifique el`--resource-arn`. En el siguiente ejemplo, sustituya el *`placeholder text`* por su propia información.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-
east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Visualización de los detalles de los controles principales mediante la API

1. Siga los pasos para buscar un control. Asegúrese de establecer el controlType como `Core` y de aplicar los filtros opcionales según sea necesario.
2. En la respuesta, identifique el control que desea revisar y tome nota del ID de control y del nombre de recurso de Amazon (ARN).
3. Utilice la GetControloperación y especifique el ControlID que anotó en el paso 2.

> **Tip**
>
> Los detalles de control se devuelven en formato JSON. Para ayudarte a entender estos datos, consulta los elementos de GetControl respuesta en la referencia de la AWS Audit Manager API.

4. Para ver los detalles de la etiqueta, utilice la ListTagsForResourceoperación y especifique el ResourceArn que anotó en el paso 2.

Para obtener más información sobre estas operaciones de la API, consulte cualquiera de los enlaces de este procedimiento en la Referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos. AWS SDKs

Pasos a seguir a continuación

Puede elegir los controles principales que representan sus objetivos y utilizarlos como componentes para crear un control personalizado. Cada control central automatizado se asigna a un grupo predefinido de fuentes de AWS datos que Audit Manager gestiona por usted. Esto significa que no es necesario ser un AWS experto para saber qué fuentes de datos recopilan la evidencia relevante para sus objetivos. Además, no tendrá que mantener estas asignaciones de orígenes de datos.

Para obtener instrucciones sobre cómo crear un control personalizado que utilice controles principales como origen de evidencia, consulte Crear un control personalizado en AWS Audit Manager.

Recursos adicionales

- Revisión de un control común
- Revisión de un control estándar
- Revisión de un control personalizado

Revisión de un control estándar

Puede revisar los detalles de un control estándar mediante la consola Audit Manager, la API Audit Manager o AWS Command Line Interface (AWS CLI).

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver los controles en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Puede revisar los detalles de un control estándar mediante la consola Audit Manager, la API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Visualización de los detalles de los controles estándar en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Control de costos.
3. Elija Estándar para ver los controles estándar que proporciona AWS.
4. Seleccione el nombre de cualquier control estándar para ver sus detalles.
5. Revise los detalles del control estándar con la siguiente información como referencia.

Sección Descripción general

En esta sección se describe el control estándar y se enumeran los tipos de orígenes de datos de los que se recopilan las evidencias.

Pestaña Orígenes de evidencias

En esta pestaña se incluye la siguiente información:

Nombre	Descripción
Controles principales	Estos son los controles principales que recopilan evidencias para respaldar el control estándar. Cada control principal utiliza una agrupación predefinida de fuentes de datos para recopilar pruebas sobre un Servicio de AWS. Estas fuentes de datos son administradas por AWS usted y se actualizan automáticamente cada vez que cambian las regulaciones y estándares y se identifican nuevas fuentes de datos. Elija un control principal para ver los orígenes de datos subyacentes.
Origen de datos	Estas son las otras fuentes de datos AWS gestionadas que recopilan pruebas para respaldar el control estándar. • Asignación: palabra clave específica que se utiliza para recopilar evidencias.

Nombre	Descripción
	• Si el tipo es AWS Config, el mapeo es una AWS Config regla (por ejemplo`SNS_ENCRYPTED_KMS`). • Si el tipo es AWS Security Hub, la asignación es un control de Security Hub (como, por ejemplo, `EC2.1`). • Si el tipo son Llamadas a la API de AWS , la asignación es una llamada a la API (como, por ejemplo, `kms_ListKeys`). • Si el tipo es AWS CloudTrail, el mapeo es un CloudTrail evento (por ejemplo`CreateAccessKey`). • Tipo: tipo de origen de datos del que proceden las evidencias. • Si Audit Manager recopila evidencias, el tipo puede ser: AWS Security Hub, AWS Config, AWS CloudTrail o Llamadas a la API de AWS . • Si carga sus propias evidencias, el tipo es Manual. Las descripciones indican si la evidencia manual requerida es una carga de archivos o una respuesta de texto. • Frecuencia: frecuencia con la que Audit Manager recopila pruebas de una fuente de datos de llamadas a la AWS API.

Pestaña Detalles

En esta pestaña se incluye la siguiente información:

Nombre	Descripción
Instrucciones	Las instrucciones que describen cómo probar y corregir el control.
Información de prueba	Los procedimientos de prueba recomendados.
Plan de acción	La acciones recomendadas que se deben tomar si es necesario corregir el control.

Nombre	Descripción
Etiquetas	Las etiquetas asociadas al control.
Clave	La clave de la etiqueta (por ejemplo, un estándar, una normativa o una categoría de conformidad).
Valor	El valor de la etiqueta.

AWS CLI

Para ver los detalles de control estándar en AWS CLI

1. Siga los pasos para buscar un control. Asegúrese de configurar el `--control-type` como `Standard` y de aplicar los filtros opcionales según sea necesario.

```
aws auditmanager list-controls --control-type Standard
```

2. En la respuesta, identifique el control que desea revisar y tome nota del ID de control y del nombre de recurso de Amazon (ARN).
3. Ejecute el comando get-control y especifique el `--control-id`. En el siguiente ejemplo, *`placeholder text`* sustitúyalo por su propia información.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> Los detalles de control se devuelven en formato JSON. Para ayudarle a comprender estos datos, consulte el Resultado de get-control en la Referencia de los comandos de la AWS CLI .

4. Para ver los detalles de la etiqueta, ejecute el list-tags-for-resourcecomando y especifique el`--resource-arn`. En el siguiente ejemplo, sustituya el *`placeholder text`* por su propia información.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-
east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Visualización de los detalles de los controles estándar mediante la API

1. Siga los pasos para buscar un control. Asegúrese de establecer el controlType como `Standard` y de aplicar los filtros opcionales según sea necesario.
2. En la respuesta, identifique el control que desea revisar y tome nota del ID de control y del nombre de recurso de Amazon (ARN).
3. Utilice la GetControloperación y especifique el ControlID que anotó en el paso 2.

> **Tip**
>
> Los detalles de control se devuelven en formato JSON. Para ayudarte a entender estos datos, consulta los elementos de GetControl respuesta en la referencia de la AWS Audit Manager API.

4. Para ver los detalles de la etiqueta, utilice la ListTagsForResourceoperación y especifique el ResourceArn que anotó en el paso 2.

Para obtener más información sobre estas operaciones de la API, consulte cualquiera de los enlaces de este procedimiento en la Referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos. AWS SDKs

Pasos a seguir a continuación

Puede añadir un control estándar a cualquiera de los marcos personalizados. Para obtener instrucciones, consulte Crear un marco personalizado en AWS Audit Manager.

También puede personalizar cualquier control estándar para que se adapte a sus necesidades. Para obtener instrucciones, consulte Creación de una copia editable de un control en AWS Audit Manager.

Recursos adicionales

- Revisión de un control común
- Revisión de un control principal
- Revisión de un control personalizado

Revisión de un control personalizado

Puede revisar los detalles de un control personalizado mediante la consola Audit Manager, la API Audit Manager o AWS Command Line Interface (AWS CLI).

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para ver los controles en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Puede revisar los detalles de un control personalizado mediante la consola Audit Manager, la API Audit Manager o AWS Command Line Interface (AWS CLI).

Audit Manager console

Visualización de los detalles de los controles personalizados en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Control de costos.
3. Seleccione Personalizado para ver los controles personalizados que ha creado.
4. Seleccione el nombre de cualquier control personalizado para ver sus detalles.
5. Revise los detalles del control personalizado con la siguiente información como referencia.

Sección Descripción general

En esta sección se describe el control personalizado y se enumeran los tipos de orígenes de datos de los que se recopilan las evidencias. También proporciona información sobre cuándo se creó el control y su última actualización.

Pestaña Orígenes de evidencias

En esta pestaña se muestra de dónde recopila las evidencias el control personalizado. Contiene la información siguiente:

Nombre	Descripción
Controles comunes	Estos son los controles comunes que recopilan evidencias para respaldar el control personalizado. Los controles habituales recopilan pruebas utilizando fuentes de datos subyacentes que AWS gestionan por usted. Para cada control común que aparece en la lista, Audit Manager recopila la evidencia pertinente de todos los controles principal es de respaldo. Elija un control común para ver los controles principales relacionados.
Controles principales	Estos son los controles principales que recopilan evidencias para respaldar el control personalizado. Los controles principales recopilan pruebas mediante un grupo predefinido de fuentes de datos que se AWS administran por usted. Elija un control principal para ver los orígenes de datos subyacentes.
Origen de datos	Estos son los orígenes de datos que recopilan evidencias para respaldar el control personalizado. **Note** Estas fuentes de datos no son gestionadas por usted AWS. Usted es responsable de mantenerlos. • Nombre: nombre del origen de datos. • Tipo: tipo de origen de datos del que proceden las evidencia s. • Si Audit Manager recopila evidencias, el tipo puede ser: AWS Security Hub, AWS Config, AWS CloudTrail o Llamadas a la API de AWS .

Nombre	Descripción

	• Si carga sus propias evidencias, el tipo es Manual. Las descripciones indican si la evidencia manual requerida es una carga de archivos o una respuesta de texto.
	• Asignación: palabra clave específica que se utiliza para recopilar evidencias.
	  • Si el tipo es AWS Config, el mapeo es una AWS Config regla (por ejemplo`SNS_ENCRYPTED_KMS`).
	  • Si el tipo es AWS Security Hub, la asignación es un control de Security Hub (como, por ejemplo, `EC2.1`).
	  • Si el tipo son Llamadas a la API de AWS , la asignación es una llamada a la API (como, por ejemplo, `kms_ListKeys`).
	  • Si el tipo es AWS CloudTrail, el mapeo es un CloudTrail evento (por ejemplo`CreateAccessKey`).
	• Frecuencia: frecuencia con la que Audit Manager recopila pruebas de una fuente de datos de llamadas a la AWS API.

Pestaña Detalles

En esta pestaña se incluye la siguiente información:

Nombre	Descripción
Instrucciones	Las instrucciones que describen cómo probar y corregir el control.
Información de prueba	Los procedimientos de prueba recomendados.
Plan de acción	La acciones recomendadas que se deben tomar si es necesario corregir el control.
Etiquetas	Las etiquetas asociadas al control.

Nombre	Descripción
Clave	La clave de la etiqueta (por ejemplo, un estándar, una normativa o una categoría de conformidad).
Valor	El valor de la etiqueta.

AWS CLI

Para ver los detalles de control personalizados en AWS CLI

1. Siga los pasos para buscar un control. Asegúrese de configurar el `--control-type` como `Custom` y de aplicar los filtros opcionales según sea necesario.

```
aws auditmanager list-controls --control-type Custom
```

2. En la respuesta, identifique el control que desea revisar y tome nota del ID de control y del nombre de recurso de Amazon (ARN).
3. Ejecute el comando get-control y especifique el `--control-id`. En el siguiente ejemplo, *`placeholder text`* sustitúyalo por su propia información.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> Los detalles de control se devuelven en formato JSON. Para ayudarle a comprender estos datos, consulte el Resultado de get-control en la Referencia de los comandos de la AWS CLI .

4. Para ver las etiquetas de un control, utilice el list-tags-for-resourcecomando y especifique las`--resource-arn`. En el siguiente ejemplo, sustituya el *`placeholder text`* por su propia información:

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-
east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Visualización de los detalles de los controles personalizados mediante la API

1. Siga los pasos para buscar un control. Asegúrese de establecer el controlType como `Custom` y de aplicar los filtros opcionales según sea necesario.
2. En la respuesta, identifique el control que desea revisar y tome nota del ID de control y su nombre de recurso de Amazon (ARN).
3. Utilice la GetControloperación y especifique el ControlID que anotó en el paso 2.

> **Tip**
>
> Los detalles de control se devuelven en formato JSON. Para ayudarte a entender estos datos, consulta los elementos de GetControl respuesta en la referencia de la AWS Audit Manager API.

4. Para ver las etiquetas del control, utilice la ListTagsForResourceoperación y especifique el control ResourceArn que anotó en el paso 2.

Para obtener más información sobre estas operaciones de la API, consulte cualquiera de los enlaces de este procedimiento en la Referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos. AWS SDKs

Pasos a seguir a continuación

Puede añadir un control personalizado a cualquiera de los marcos personalizados. Para obtener instrucciones, consulte Crear un marco personalizado en AWS Audit Manager.

También puede editar un control personalizado, crea una copia editable de un control personalizado o eliminar un control personalizado que ya no necesite.

Recursos adicionales

- Revisión de un control común
- Revisión de un control principal
- Revisión de un control estándar

Crear un control personalizado en AWS Audit Manager

Puede utilizar controles personalizados para recopilar evidencias que se adapten a sus necesidades específicas de conformidad.

Al igual que los controles estándar, los controles personalizados recopilan pruebas de forma continua cuando están activos en las evaluaciones. También puede añadir pruebas manuales a cualquier control personalizado que cree. Cada prueba se convierte en un registro que le ayuda a demostrar el cumplimiento de los requisitos de su control personalizado.

A continuación, se muestran algunos ejemplos de cómo puede usar los controles personalizados:

Asignación de los controles empresariales a agrupaciones predefinidas de orígenes de datos de AWS

Puede incorporar los controles empresariales a Audit Manager mediante el uso de controles comunes como origen de evidencias. Elija los controles comunes que representen sus objetivos y utilícelos como componentes para crear un control que recopile evidencias de toda la cartera de necesidades de conformidad. Cada control común automatizado se asigna a una agrupación predefinida de orígenes de datos. Esto significa que no es necesario ser un AWS experto para saber qué fuentes de datos recopilan la evidencia relevante para alcanzar sus objetivos. En el caso de que utilice controles comunes como origen de evidencia, ya no tendrá que mantener las asignaciones de orígenes de datos, ya que Audit Manager se encargará de hacerlo.

Cree una pregunta de evaluación de riesgos para el proveedor

Puede usar controles personalizados para respaldar la gestión de las evaluaciones de riesgo de los proveedores. Cada control que cree puede representar una pregunta de evaluación de riesgos individual. Por ejemplo, el nombre del control puede ser una pregunta y puede proporcionar una respuesta cargando un archivo o introduciendo una respuesta de texto como evidencia manual.

Puntos clave

Cuando se trata de crear controles personalizados en Audit Manager, tiene dos métodos entre los que elegir:

1. Creación de un control desde cero: este método proporciona la máxima flexibilidad y le permite adaptar el control a sus necesidades exactas. Esta es una buena opción cuando tiene un requisito

específico de conformidad que un control existente no cubre de forma adecuada. Este método es especialmente útil cuando necesita asignar los controles empresariales de su organización a agrupaciones predefinidas de orígenes de datos de AWS o cuando desea crear preguntas de evaluación de riesgos de los proveedores como controles individuales.

2. Creación de una copia editable de un control existente: si un control estándar o personalizado existente cubre parcialmente sus necesidades, puede crear una copia editable de él. Este método es más eficaz si solo necesita realizar cambios menores en un control existente. Esta es una buena opción si desea ajustar algunos atributos para equiparar mejor el control con sus requisitos específicos. Por ejemplo, puede cambiar la frecuencia con la que un control utiliza una llamada a la API para recopilar evidencias y, a continuación, cambiar el nombre del control para reflejar esto.

Recursos adicionales

Para obtener instrucciones sobre cómo crear un control personalizado, consulte los siguientes recursos.

- Creación de un nuevo control personalizado desde cero en AWS Audit Manager
- Creación de una copia editable de un control en AWS Audit Manager

Creación de un nuevo control personalizado desde cero en AWS Audit Manager

Si los requisitos de cumplimiento de su organización no se ajustan a los controles estándar prediseñados que están disponibles AWS Audit Manager, puede crear su propio control personalizado desde cero.

En esta página se describen los pasos para crear un control personalizado que se adapte a sus necesidades específicas.

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para crear un control personalizado. AWS Audit Manager Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Para recopilar correctamente pruebas AWS Config de un Security Hub, asegúrese de hacer lo siguiente:

- Active AWS Config y, a continuación, aplique la configuración necesaria para utilizarla AWS Config con Audit Manager
- Siga los pasos indicados en Enable Security Hub y luego aplique la configuración necesaria para usar Security Hub con Audit Manager

A continuación, Audit Manager puede recopilar evidencias cada vez que se realice una evaluación de una determinada regla de AWS Config o control de Security Hub.

Procedimiento

Tareas

- Paso 1: especificar los detalles de control
- Paso 2: especificar orígenes de evidencias
- Paso 3 (opcional): definir un plan de acción
- Paso 4: revisar y crear el control

Paso 1: especificar los detalles de control

Comience por especificar los detalles de su control personalizado.

> **Important**
>
> Le recomendamos encarecidamente que no incluya nunca información de identificación confidencial en los campos de formato libre, como, por ejemplo, Detalles de control o Información de prueba. Si crea controles personalizados que contienen información confidencial, no podrá compartir ninguno de sus marcos personalizados que contengan estos controles.

Para especificar los detalles del control

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Biblioteca de controles y, a continuación, elija Crear control personalizado.

3. En Detalles del control, introduzca la siguiente información sobre el control.
   - Control: introduzca un nombre descriptivo, un título o una pregunta de evaluación de riesgos. Este valor le ayuda a identificar el control en la biblioteca de controles.
   - Descripción (opcional): introduzca los detalles para ayudar a otros a entender el objetivo del control. Esta descripción aparece en la página de detalles del control.
4. En Información de prueba, introduzca los pasos recomendados para probar el control.
5. En Etiquetas, elija Añadir nueva etiqueta para asociar una etiqueta al control. Puede especificar una clave para cada etiqueta que describa mejor el marco de conformidad compatible con este control. La clave de etiqueta es obligatoria y se puede utilizar como criterio de búsqueda al buscar este control en la biblioteca de controles.
6. Elija Next (Siguiente).

Paso 2: especificar orígenes de evidencias

A continuación, especifique algunos orígenes de evidencias. Un origen de evidencias determina de dónde recopila las evidencias el control personalizado. Puede usar fuentes AWS administradas, fuentes administradas por el cliente o ambas.

> **Tip**
>
> Le recomendamos que utilice fuentes AWS gestionadas. Cada vez que se actualiza una fuente AWS gestionada, las mismas actualizaciones se aplican automáticamente a todos los controles personalizados que utilizan estas fuentes. Esto significa que los controles personalizados recopilan evidencias comparándolas con las definiciones más recientes de ese origen de evidencias.

Si no tiene claro las opciones que debe elegir, consulte los siguientes ejemplos y nuestras recomendaciones.

Su función	Su objetivo	Origen de evidencias recomendado
Profesional de GRC	Quiero recopilar evidencias para un dominio u objetivo en concreto	AWS gestionado (common control)

Su función	Su objetivo	Origen de evidencias recomendado
		Utilice una agrupación predefinida de orígenes de datos que se asignen a un determinado control común.
Experto técnico	Quiero recopilar pruebas sobre los AWS recursos de los que soy responsable	AWS gestionado (core control) Utilice una agrupación predefinida de orígenes de datos que se asignen a un requisito de AWS .
Experto técnico	Quiero usar una AWS Config regla personalizada para recopilar pruebas	Administrado por el cliente (data source automatizado) Utilice un origen de datos personalizado para recopilar determinadas evidencias automatizadas.
Profesional de GRC	Quiero recopilar evidencia s, como, por ejemplo, documentos y respuestas de texto	Administrado por el cliente (data source manual) Utilice un origen de datos personalizado para cargar sus propias evidencias manuales.

Especificación de un origen administrado por AWS (recomendado)

Le recomendamos que, para comenzar, elija uno o varios controles comunes. Al elegir el control común que representa su objetivo, Audit Manager recopila las evidencias pertinentes de todos los controles principales de respaldo. También puede elegir controles básicos individuales si desea recopilar pruebas específicas sobre su AWS entorno.

Para especificar una fuente AWS gestionada

1. Diríjase a la sección Orígenes administrados por AWS de la página.
2. Para añadir un control común, siga estos pasos:
   a. Seleccione Usar un control común que coincida con el objetivo de conformidad.
   b. Seleccione un control común en el menú desplegable.
   c. (Opcional) Repita el paso 2 según sea necesario. Puede añadir hasta cinco controles comunes.
3. Para eliminar un control común, elija la X situada junto al nombre del control.
4. Para añadir un control principal, siga estos pasos:
   a. Seleccione Usar un control principal que coincida con una recomendación de AWS .
   b. Seleccione un control común en el menú desplegable.
   c. (Opcional) Repita el paso 4 según sea necesario. Puede añadir hasta 50 controles principales.
5. Para eliminar un control principal, elija la X situada junto al nombre del control.
6. Para añadir orígenes de datos administrados por el cliente, use el siguiente procedimiento. En caso contrario, elija Siguiente.

Especificación de un origen administrado por el cliente

Para recopilar evidencias automatizadas de un origen de datos, debe elegir un tipo, así como una asignación del tipo de datos. Estos detalles se relacionan con su AWS uso e indican a Audit Manager de dónde debe recopilar las pruebas. Si desea proporcionar sus propias evidencias, entonces debe elegir un origen de datos manual.

> **Note**
>
> Usted es responsable de mantener las asignaciones de orígenes de datos que cree en este paso.

Especificación de un origen administrado por el cliente

1. Diríjase a la sección Orígenes administrados por el cliente de la página.

2. Seleccione Utilizar un origen de datos para recopilar evidencias manuales o automatizadas.
3. Elija Agregar.
4. Seleccione una de las siguientes opciones:
   - Seleccione Llamadas a la API de AWS y luego una llamada a la API y una frecuencia de recopilación de evidencias.
   - Seleccione Evento de AWS CloudTrail y luego un nombre para el evento.
   - Seleccione Regla administrada por AWS Config y luego un identificador de regla.
   - Seleccione Regla personalizada de AWS Config y luego un identificador de regla.
   - Seleccione Control de AWS Security Hub y luego un control de Security Hub.
   - Seleccione Origen de datos manual y luego una opción:
     - Carga de archivos: utilice esta opción si el control requiere documentación como evidencia.
     - Respuesta de texto: utilice esta opción si el control requiere una respuesta a una pregunta de evaluación de riesgos.

> **Tip**
>
> Para obtener información sobre los tipos de orígenes de datos automatizados y consejos para la solución de problemas, consulte Tipos de orígenes de datos compatibles para evidencias automatizadas.
>
> Si necesita validar la configuración del origen de datos con un experto, elija Origen de datos manual de momento. De esta forma, puede crear el control y añadirlo a un marco ahora y, a continuación, editar el control según sea necesario más adelante.

5. En Nombre del origen de datos, indique un nombre descriptivo.
6. (Opcional) En Detalles adicionales, introduzca una descripción del origen de datos y una descripción de la solución de problemas.
7. Elija Agregar origen de datos.
8. (Opcional) Para añadir otro origen de datos, elija Añadir y repita los pasos 1-7. Puede añadir hasta 100 orígenes de datos.
9. Para eliminar un origen de datos, selecciónelo en la tabla y luego elija Eliminar.
10. Cuando haya terminado, elija Siguiente.

Paso 3 (opcional): definir un plan de acción

A continuación, especifique las acciones que se deben tomar si es necesario corregir este control.

> **Important**
>
> Le recomendamos encarecidamente que no incluya nunca información de identificación confidencial en los campos de formato libre, como, por ejemplo, Plan de acción. Si crea controles personalizados que contienen información confidencial, no podrá compartir ninguno de sus marcos personalizados que contengan estos controles.

Definición de un plan de acción

1. En Título, introduzca un título descriptivo para el plan de acción.
2. En Instrucciones, introduzca instrucciones detalladas para el plan de acción.
3. Elija Next (Siguiente).

Paso 4: revisar y crear el control

Revisión de la información de la pila. Para modificar la información de un paso, seleccione Editar.

Cuando haya terminado, elija Crear.

Pasos a seguir a continuación

Tras crear un nuevo control personalizado, puede añadirlo a un marco personalizado. Para obtener más información, consulte Crear un marco personalizado en AWS Audit Manager y Edición de un marco personalizado en AWS Audit Manager.

Tras añadir el control personalizado a un marco personalizado, puede crear una evaluación y empezar a recopilar evidencias. Para obtener más información, consulte Crear una evaluación en AWS Audit Manager.

Para revisitar el control personalizado más adelante, consulte Encuentre los controles disponibles en AWS Audit Manager. Puede seguir estos pasos para localizar el control personalizado y poder verlo, editarlo o eliminarlo.

Recursos adicionales

Para obtener soluciones a problemas relacionados con los controles en Audit Manager, consulte Solución de problemas de control y conjunto de control.

Creación de una copia editable de un control en AWS Audit Manager

En lugar de crear un control personalizado desde cero, puede utilizar un control estándar existente o un control personalizado como punto de partida y crear una copia editable que cubra sus necesidades. Al hacerlo, el control estándar existente permanece en la biblioteca de controles y se crea un nuevo control con su configuración personalizada.

Requisitos previos

Asegúrese de que su identidad de IAM tenga los permisos adecuados para crear un marco personalizado. AWS Audit Manager Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Para recopilar correctamente pruebas AWS Config de un Security Hub, asegúrese de hacer lo siguiente:

- AWS Config Actívela y, a continuación, aplique la configuración necesaria para AWS Config utilizarla con Audit Manager.
- Siga los pasos indicados en Enable Security Hub y luego aplique la configuración necesaria para usar Security Hub con Audit Manager.

A continuación, Audit Manager puede recopilar evidencias cada vez que se realice una evaluación de una determinada regla de AWS Config o control de Security Hub.

Procedimiento

Tareas

- Paso 1: especificar los detalles de control
- Paso 2: especificar orígenes de evidencias
- Paso 3: (opcional): definir un plan de acción
- Paso 4: revisar y crear el control

Paso 1: especificar los detalles de control

Los detalles del control se heredan del control original. Revise y modifique estos detalles según sea necesario.

> **Important**
>
> Le recomendamos encarecidamente que no incluya nunca información de identificación confidencial en los campos de formato libre, como, por ejemplo, Detalles de control o Información de prueba. Si crea controles personalizados que contienen información confidencial, no podrá compartir ninguno de sus marcos personalizados que contengan estos controles.

Para especificar los detalles del control

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Control de costos.
3. Seleccione el control estándar o el control personalizado en el que desee realizar cambios y luego elija Hacer una copia.
4. Especifique el nuevo nombre del control y elija Continuar.
5. En Detalles del control, personalice los detalles del control según sea necesario.
6. En Información de prueba, modifique las instrucciones según sea necesario.
7. En Etiquetas, personalice las etiquetas según sea necesario.
8. Elija Next (Siguiente).

Paso 2: especificar orígenes de evidencias

Los orígenes de evidencias se heredan del control original. Puede cambiar, añadir o eliminar los orígenes de evidencias según sea necesario.

Especificación de un origen administrado por AWS (recomendado)

> **Tip**
>
> Le recomendamos que, para comenzar, elija uno o varios controles comunes. Si tiene requisitos de conformidad más detallados, también puede elegir uno o varios controles principales específicos.

Para especificar una fuente AWS gestionada

1. En Orígenes administrados por AWS , revise las selecciones actuales y realice los cambios necesarios.
2. Para añadir un control común, siga estos pasos:
   a. Seleccione Usar un control común que coincida con el objetivo de conformidad.
   b. Seleccione un control común en el menú desplegable.
   c. (Opcional) Repita el paso 2 según sea necesario. Puede añadir hasta cinco controles comunes.
3. Para eliminar un control común, elija la X situada junto al nombre del control.
4. Para añadir un control principal, siga estos pasos:
   a. Seleccione Usar un control principal que coincida con una recomendación de AWS .
   b. Seleccione un control común en el menú desplegable.
   c. (Opcional) Repita el paso 4 según sea necesario. Puede añadir hasta 50 controles principales.
5. Para eliminar un control principal, elija la X situada junto al nombre del control.
6. Para editar orígenes de datos administrados por el cliente, utilice el siguiente procedimiento. En caso contrario, elija Siguiente.

Especificación de un origen administrado por el cliente

Para recopilar evidencias automatizadas de un origen de datos, debe elegir un tipo, así como una asignación del tipo de datos. Estos detalles se relacionan con su AWS uso e indican a Audit Manager de dónde debe recopilar las pruebas. Si desea proporcionar sus propias evidencias, entonces debe elegir un origen de datos manual.

> **Note**
>
> Usted es responsable de mantener las asignaciones de orígenes de datos que cree en este paso.

Especificación de un origen administrado por el cliente

1. En Orígenes administrados por el cliente, revise los orígenes de datos actuales y realice los cambios necesarios.
2. Para eliminar un origen de datos, selecciónelo en la tabla y elija Eliminar.
3. Para añadir un nuevo origen de datos, siga estos pasos:
   a. Seleccione Utilizar un origen de datos para recopilar evidencias manuales o automatizadas.
   b. Elija Agregar.
   c. Seleccione una de las siguientes opciones:
      - Seleccione Llamadas a la API de AWS y luego una llamada a la API y una frecuencia de recopilación de evidencias.
      - Seleccione Evento de AWS CloudTrail y luego un nombre para el evento.
      - Seleccione Regla administrada por AWS Config y luego un identificador de regla.
      - Seleccione Regla personalizada de AWS Config y luego un identificador de regla.
      - Seleccione Control de AWS Security Hub y luego un control de Security Hub.
      - Seleccione Origen de datos manual y luego una opción:
        - Carga de archivos: utilice esta opción si el control requiere documentación como evidencia.
        - Respuesta de texto: utilice esta opción si el control requiere una respuesta a una pregunta de evaluación de riesgos.

> **Tip**
>
> Para obtener información sobre los tipos de orígenes de datos automatizados y consejos para la solución de problemas, consulte Tipos de orígenes de datos compatibles para evidencias automatizadas.

Si necesita validar la configuración del origen de datos con un experto, elija Origen de datos manual de momento. De esta forma, puede crear el control y añadirlo a un marco ahora y, a continuación, editar el control según sea necesario más adelante.

d. En Nombre del origen de datos, indique un nombre descriptivo.

e. (Opcional) En Detalles adicionales, introduzca una descripción del origen de datos y una descripción de la solución de problemas.

f. Elija Agregar origen de datos.

g. (Opcional) Para añadir otro origen de datos, elija Añadir y repita el paso 3. Puede añadir hasta 100 orígenes de datos.

4. Cuando haya terminado, elija Siguiente.

Paso 3: (opcional): definir un plan de acción

El plan de acción se hereda del control original. Puede editar este plan de acción según sea necesario.

> **Important**
>
> Le recomendamos encarecidamente que no incluya nunca información de identificación confidencial en los campos de formato libre, como, por ejemplo, Plan de acción. Si crea controles personalizados que contienen información confidencial, no podrá compartir ninguno de sus marcos personalizados que contengan estos controles.

Especificación de instrucciones

1. En Título, revise el título y realice los cambios necesarios.
2. En Instrucciones, revise las instrucciones y realice los cambios necesarios.
3. Elija Next (Siguiente).

Paso 4: revisar y crear el control

Revisión de la información de la pila. Para modificar la información de un paso, seleccione Editar. Cuando haya terminado, elija Crear.

Pasos a seguir a continuación

Tras crear un nuevo control personalizado, puede añadirlo a un marco personalizado. Para obtener más información, consulte Crear un marco personalizado en AWS Audit Manager y Edición de un marco personalizado en AWS Audit Manager.

Tras añadir un control personalizado a un marco personalizado, puede crear una evaluación y empezar a recopilar evidencias. Para obtener más información, consulte Crear una evaluación en AWS Audit Manager.

Para revisitar el control personalizado más adelante, consulte Encuentre los controles disponibles en AWS Audit Manager. Puede seguir estos pasos para localizar el control personalizado y poder verlo, editarlo o eliminarlo.

Recursos adicionales

Para obtener soluciones a problemas relacionados con los controles en Audit Manager, consulte Solución de problemas de control y conjunto de control.

Edición de un control personalizado en AWS Audit Manager

Es posible que tenga que modificar los controles personalizados a medida AWS Audit Manager que cambien sus requisitos de conformidad.

En esta página se describen los pasos para editar los detalles, los orígenes de evidencias y las instrucciones del plan de acción de un control personalizado.

Requisitos previos

En el siguiente procedimiento se da por sentado que ha creado previamente un control personalizado.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para editar un control personalizado en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Siga estos pasos para editar un control personalizado.

> **Note**
>
> Al editar un control, los cambios se aplican a todas las evaluaciones en las que el control esté activo. En todas estas evaluaciones, Audit Manager empezará automáticamente a recopilar evidencias de acuerdo con la definición de control más reciente.

Tareas

- Paso 1: editar los detalles de control
- Paso 2: editar orígenes de evidencias
- Paso 3: editar plan de acción

Paso 1: editar los detalles de control

Revise y edite los detalles del control según sea necesario.

> **Important**
>
> Le recomendamos encarecidamente que no incluya nunca información de identificación confidencial en los campos de formato libre, como, por ejemplo, Detalles de control o Información de prueba. Si crea controles personalizados que contienen información confidencial, no podrá compartir ninguno de sus marcos personalizados que contengan estos controles.

Para editar los detalles de los controles

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Biblioteca de controles y luego la pestaña Personalizado.
3. Seleccione el control que desea modificar y elija Editar.
4. En Detalles de control, edite los detalles del control según sea necesario.
5. En Información de prueba, edite la descripción según sea necesario.
6. Elija Next (Siguiente).

Paso 2: editar orígenes de evidencias

A continuación, puede editar, eliminar o añadir orígenes de evidencias para el control.

> **Note**
>
> Al editar un control para incluir más o menos orígenes de evidencias, esto podría afectar a la cantidad de evidencia que el control recopila en cualquier evaluación en la que esté activo. Por ejemplo, si añade orígenes de evidencias, puede observar que Audit Manager realiza más evaluaciones de recursos y recopila más evidencias que antes. Si elimina orígenes de evidencias, es probable que el control recopile menos evidencias en el futuro.
> Para obtener más información sobre la evaluaciones de recursos y los precios, consulte AWS Audit Manager Pricing.

Para editar una fuente AWS gestionada

Para editar una fuente AWS gestionada

1. En Orígenes administrados por AWS , revise las selecciones actuales y realice los cambios necesarios.
2. Para añadir un control común, siga estos pasos:
   a. Seleccione Usar un control común que coincida con el objetivo de conformidad.
   b. Seleccione un control común en el menú desplegable.
   c. (Opcional) Repita el paso 2 según sea necesario. Puede añadir hasta cinco controles comunes.
3. Para eliminar un control común, elija la X situada junto al nombre del control.
4. Para añadir un control principal, siga estos pasos:
   a. Seleccione Usar un control principal que coincida con una recomendación de AWS .
   b. Seleccione un control común en el menú desplegable.
   c. (Opcional) Repita el paso 4 según sea necesario. Puede añadir hasta 50 controles principales.
5. Para eliminar un control principal, elija la X situada junto al nombre del control.
6. Para añadir orígenes de datos administrados por el cliente, use el siguiente procedimiento. En caso contrario, elija Siguiente.

Edición de un origen administrado por el cliente

> **Note**
>
> Usted es responsable de mantener las asignaciones de orígenes de datos que edite en este paso.

Edición de un origen administrado por el cliente

1. En Orígenes administrados por el cliente, revise los orígenes de datos actuales y realice los cambios necesarios.
2. Para eliminar un origen de datos, selecciónelo en la tabla y luego elija Eliminar.
3. Para añadir un nuevo origen de datos, siga estos pasos:
   a. Seleccione Utilizar un origen de datos para recopilar evidencias manuales o automatizadas.
   b. Elija Agregar.
   c. Seleccione una de las siguientes opciones:
      - Seleccione Llamadas a la API de AWS y luego una llamada a la API y una frecuencia de recopilación de evidencias.
      - Seleccione Evento de AWS CloudTrail y luego un nombre para el evento.
      - Seleccione Regla administrada por AWS Config y luego un identificador de regla.
      - Seleccione Regla personalizada de AWS Config y luego un identificador de regla.
      - Seleccione Control de AWS Security Hub y luego un control de Security Hub.
      - Seleccione Origen de datos manual y luego una opción:
        - Carga de archivos: utilice esta opción si el control requiere documentación como evidencia.
        - Respuesta de texto: utilice esta opción si el control requiere una respuesta a una pregunta de evaluación de riesgos.

> **Tip**
>
> Para obtener información sobre los tipos de orígenes de datos automatizados y consejos para la solución de problemas, consulte Tipos de orígenes de datos compatibles para evidencias automatizadas.

Si necesita validar la configuración del origen de datos con un experto, elija Origen de datos manual de momento. De esta forma, puede crear el control y añadirlo a un marco ahora y, a continuación, editar el control según sea necesario más adelante.

d. En Nombre del origen de datos, indique un nombre descriptivo.

e. (Opcional) En Detalles adicionales, introduzca una descripción del origen de datos y una descripción de la solución de problemas.

f. Elija Agregar origen de datos.

g. (Opcional) Para añadir otro origen de datos, elija Añadir y repita el paso 3. Puede añadir hasta 100 orígenes de datos.

4. Cuando haya terminado, elija Siguiente.

Paso 3: editar plan de acción

A continuación, revise y edite el plan de acción opcional.

> **Important**
>
> Le recomendamos encarecidamente que no incluya nunca información de identificación confidencial en los campos de formato libre, como, por ejemplo, Plan de acción. Si crea controles personalizados que contienen información confidencial, no podrá compartir ninguno de sus marcos personalizados que contengan estos controles.

Para editar un plan de acción

1. En Título, edite el título según sea necesario.
2. En Instrucciones, edite las instrucciones según sea necesario.
3. Elija Next (Siguiente).

Paso 4: revisar y guardar

Revisión de la información de la pila. Para modificar la información de un paso, seleccione Editar.

Cuando haya finalizado, elija Save changes (Guardar cambios).

> **Note**
>
> Tras editar un control, los cambios se aplican de la siguiente manera en todas las evaluaciones activas que incluyen el control:
>
> - En el caso de los controles con llamadas a la AWS API como tipo de origen de datos, los cambios se aplican a las 00:00 UTC del día siguiente.
> - Los cambios surtirán efecto de inmediato en los demás controles.

Pasos a seguir a continuación

Cuando tenga la certeza de que ya no necesita un control personalizado, elimínelo para limpiar el entorno de Audit Manager. Para obtener instrucciones, consulte Eliminar un control personalizado en AWS Audit Manager.

Recursos adicionales

Para obtener soluciones a problemas relacionados con los controles en Audit Manager, consulte Solución de problemas de control y conjunto de control.

Cambio de la frecuencia con la que un control recopila evidencias

AWS Audit Manager puede recopilar pruebas de varias fuentes de datos. La frecuencia de la recopilación de evidencias depende del tipo de origen de datos que utilice el control.

En las siguientes secciones se proporciona más información sobre la frecuencia de recopilación de evidencias para cada tipo de origen de datos de control y sobre cómo cambiarla (si procede).

Temas

- Puntos clave
- Instantáneas de configuración a partir de llamadas a la AWS API
- Comprobaciones de cumplimiento de AWS Config
- Comprobaciones de cumplimiento desde Security Hub
- Registros de actividad de los usuarios de AWS CloudTrail

Puntos clave

- En el caso de las llamadas a la API de AWS , Audit Manager recopila pruebas mediante una llamada de descripción de la API a otro Servicio de AWS. Puede especificar la frecuencia de recopilación de evidencias directamente en Audit Manager (solo para controles personalizados).
- AWS ConfigEn efecto, Audit Manager informa del resultado de una comprobación de conformidad directamente desde AWS Config. La frecuencia sigue los activadores que se definen en la AWS Config regla.
- Audit Manager informa del resultado de una comprobación de conformidad directamente desde el Security Hub al usarse con AWS Security Hub. La frecuencia sigue la programación de comprobación de Security Hub.
- Pues AWS CloudTrail, Audit Manager recopila pruebas de forma continua de CloudTrail. No puede cambiar la frecuencia de este tipo de prueba.

Instantáneas de configuración a partir de llamadas a la AWS API

> **Note**
>
> Lo siguiente se aplica solo a los controles personalizados. No puede cambiar la frecuencia de recopilación de evidencias para un control estándar.

Si un control personalizado utiliza llamadas a la AWS API como tipo de fuente de datos, puede cambiar la frecuencia de recopilación de pruebas en Audit Manager siguiendo estos pasos.

Para cambiar la frecuencia de recopilación de evidencias de un control personalizado con un origen de datos de llamadas a la API

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Biblioteca de controles y luego la pestaña Personalizado.
3. Elija la ACL web que desee editar y, a continuación, seleccione Editar.
4. En la página Editar detalles del control, seleccione Siguiente.
5. En Orígenes administrados por el cliente, busque el origen de datos de la llamada a la API que desea actualizar.
6. Seleccione el origen de datos en tabla y luego Eliminar.
7. Elija Agregar.

8. Elija Llamadas a la API de AWS .
9. Elija la misma llamada a la API que eliminó en el paso 5 y luego seleccione la frecuencia de recopilación de evidencias que prefiera.
10. En Nombre del origen de datos, indique un nombre descriptivo.
11. (Opcional) En Detalles adicionales, introduzca una descripción del origen de datos y una descripción de la solución de problemas.
12. Elija Next (Siguiente).
13. En la página Editar un plan de acción, seleccione Siguiente.
14. En la página Revisar y actualizar, revise la información del control personalizado. Para modificar la información de un paso, seleccione Editar.
15. Cuando haya finalizado, elija Save changes (Guardar cambios).

Después de editar un control, los cambios se aplicarán a las 00:00 UTC del día siguiente en todas las evaluaciones activas que incluyan el control.

Comprobaciones de cumplimiento de AWS Config

> **Note**
>
> Lo siguiente se aplica tanto a los controles estándar como a los controles personalizados que utilizan Reglas de AWS Config como origen de datos.

Si un control se utiliza AWS Config como tipo de fuente de datos, no puede cambiar la frecuencia de recopilación de pruebas directamente en Audit Manager. Esto se debe a que la frecuencia sigue los activadores que se definen en la AWS Config regla.

Existen dos tipos de desencadenantes para Reglas de AWS Config:

1. Cambios de configuración: AWS Config ejecuta evaluaciones de la regla cuando se crean, modifican o eliminan determinados tipos de recursos.
2. Periódico: AWS Config ejecuta las evaluaciones de la regla con la frecuencia que elija (por ejemplo, cada 24 horas).

Para obtener más información sobre los activadores Reglas de AWS Config, consulta los tipos de activadores en la Guía para AWS Config desarrolladores.

Para obtener instrucciones sobre cómo administrar Reglas de AWS Config, consulte Administrar AWS Config las reglas.

Comprobaciones de cumplimiento desde Security Hub

> **Note**
>
> Lo siguiente se aplica tanto a los controles estándar como a los controles personalizados que utilizan las comprobaciones de Security Hub como origen de datos.

Si un control utiliza Security Hub como tipo de origen de datos, no puede cambiar la frecuencia de recopilación de evidencias directamente en Audit Manager. Esto se debe a que la frecuencia sigue la programación de las comprobaciones de Security Hub.

- Las comprobaciones periódicas se ejecutan automáticamente en las 12 horas posteriores a la última ejecución. No puede cambiar la periodicidad.
- Las comprobaciones activadas por cambios se ejecutan cuando el recurso asociado cambia de estado. Incluso si el recurso no cambia de estado, la actualización a tiempo para las comprobaciones activadas por cambios se actualiza cada 18 horas. Esto ayuda a indicar que el control sigue habilitado. En general, Security Hub utiliza reglas activadas por cambios siempre que sea posible.

Para obtener más información, consulte el programa de ejecución de los controles de seguridad en la Guía del usuario de AWS Security Hub .

Registros de actividad de los usuarios de AWS CloudTrail

> **Note**
>
> Lo siguiente se aplica tanto a los controles estándar como a los controles personalizados que utilizan los registros de actividad de los usuarios de AWS CloudTrail como origen de datos.

No puede cambiar la frecuencia de recopilación de pruebas para los controles que utilizan los registros de actividad CloudTrail como tipo de fuente de datos. Audit Manager recopila este tipo CloudTrail de evidencia de forma continua. La frecuencia es continua porque la actividad de los usuarios puede ocurrir en cualquier momento del día.

Eliminar un control personalizado en AWS Audit Manager

Si ha creado un control personalizado y ya no lo necesita, puede eliminarlo del entorno de Audit Manager. Esto le permite limpiar su espacio de trabajo y centrarse en los controles personalizados que son pertinentes para sus tareas y prioridades actuales.

Requisitos previos

En el siguiente procedimiento se da por sentado que ha creado previamente un control personalizado.

Asegúrese de que su identidad de IAM tenga los permisos adecuados para eliminar un control personalizado en AWS Audit Manager. Dos políticas sugeridas que conceden estos permisos son: AWSAuditManagerAdministratorAccess y Permita que la administración de los usuarios acceda a AWS Audit Manager.

Procedimiento

Puede eliminar controles personalizados mediante la consola de Audit Manager, la API de Audit Manager o AWS Command Line Interface (AWS CLI).

> **Important**
>
> Al eliminar un control personalizado se elimina el control de todos los marcos o evaluaciones personalizados con los que esté relacionado actualmente. Por lo tanto, Audit Manager dejará de recopilar pruebas para ese control personalizado en todas sus evaluaciones. Esto incluye las evaluaciones que haya creado previamente antes de eliminar el control personalizado.

Audit Manager console

Eliminación de un control personalizado de la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación, elija Biblioteca de controles y, a continuación, elija la pestaña Controles personalizados.

3. Seleccione el control que desea eliminar y luego elija Eliminar.
4. En la ventana emergente que aparece, seleccione Eliminar para confirmar la eliminación.

AWS CLI

Para eliminar un control personalizado en el AWS CLI

1. En primer lugar, identifique el control personalizado que desea eliminar. Para ello, ejecute el comando list-controls y especifique el `--control-type` como `Custom`.

   ```
   aws auditmanager list-controls --control-type Custom
   ```

   La respuesta devuelve una lista de controles personalizados. Busque el control que desee eliminar y anote el ID del control.

2. A continuación, ejecute el comando delete-control y utilice el parámetro `--control-id` para especificar el control que desee eliminar.

   En el siguiente ejemplo, *`placeholder text`* sustitúyalo por su propia información.

   ```
   aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-
   EXAMPLE11111
   ```

Audit Manager API

Eliminación de un control personalizado mediante la API

1. Utilice la ListControlsoperación y especifique el ControlType como`Custom`. En la respuesta, busque el control que desee eliminar y anote el ID del control.
2. Utilice la DeleteControloperación para eliminar el control personalizado. En la solicitud, utilice el parámetro Id de control para especificar el control que desea eliminar.

Para obtener más información sobre estas operaciones de la API, consulte cualquiera de los enlaces del procedimiento anterior en la Referencia de la API de AWS Audit Manager . Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos AWS SDKs.

Recursos adicionales

Para obtener información sobre la retención de datos en Audit Manager, consulte Eliminación de datos de Audit Manager.

Revisar y configurar sus AWS Audit Manager ajustes

Puede revisar y configurar sus AWS Audit Manager ajustes en cualquier momento para asegurarse de que se ajustan a sus necesidades específicas.

En este capítulo se explica el proceso de acceso, revisión y ajuste de la configuración de Audit Manager step-by-step. Al seguir estos pasos, aprenderá a cambiar la configuración general, la configuración de las evaluaciones y la configuración del buscador de evidencias para que se adapten a los objetivos de conformidad y requisitos empresariales en constante cambio.

Procedimiento

Para comenzar, siga estos pasos para ver la configuración de Audit Manager. Puede ver la configuración de Audit Manager mediante la consola de Audit Manager, la AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

Visualización de la configuración

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Configuración.
3. Elija la pestaña que cumpla con el objetivo.
   - Configuración general: elija esta pestaña para revisar y actualizar la configuración general de Audit Manager.
   - Configuración de la evaluación: seleccione esta pestaña para revisar y actualizar la configuración predeterminada de las evaluaciones.
   - Configuración del buscador de evidencias: elija esta pestaña para revisar y actualizar la configuración del buscador de evidencias.

Pasos a seguir a continuación

Para personalizar la configuración de Audit Manager para su caso de uso, siga los procedimientos que se indican aquí.

- Configuración general
  - Configuración de los ajustes del cifrado de datos

- Adición de un administrador delegado
- Cambio de un administrador delegado
- Eliminación de un administrador delegado
- Desactivar AWS Audit Manager
- Configuración de la evaluación
  - Configuración de los responsables de auditoría predeterminados
  - Configuración del destino del informe de evaluación predeterminado
  - Configuración de notificaciones en Audit Manager
- Configuración del buscador de evidencias
  - Habilitar el buscador de evidencias
  - Confirming the status of evidence finder
  - Configuración del destino de la exportación predeterminada para el buscador de evidencias
  - Deshabilitar el buscador de evidencias

Configuración de los ajustes del cifrado de datos

Puede elegir cómo cifrar los datos en AWS Audit Manager. Audit Manager crea automáticamente un espacio único Clave administrada de AWS para el almacenamiento seguro de sus datos. De forma predeterminada, los datos de Audit Manager se cifran con esta clave KMS. Sin embargo, si desea personalizar la configuración del cifrado de datos, puede especificar su propia clave de cifrado simétrico administrada por el cliente. Usar su propia Clave de KMS le da más flexibilidad, incluida la capacidad de crear, rotar y desactivar claves.

Requisitos previos

Si proporciona una clave gestionada por el cliente, debe figurar en la Región de AWS misma que la de su evaluación para poder generar informes de evaluación y exportar correctamente los resultados de búsqueda del buscador de pruebas.

Procedimiento

Puede actualizar la configuración de cifrado de datos mediante la consola de Audit Manager, AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

> **Note**
>
> Al cambiar la configuración de cifrado de datos de Audit Manager, estos cambios se aplican a cualquier evaluación nueva que cree. Esto incluye todos los informes de evaluación y las exportaciones del buscador de evidencias que cree a partir de sus nuevas evaluaciones. Los cambios no se aplican a las evaluaciones existentes que creó antes de cambiar la configuración del cifrado. Esto incluye los nuevos informes de evaluación y las exportaciones a CSV que cree a partir de las evaluaciones existentes, además de los informes de evaluación y las exportaciones a CSV existentes. Las evaluaciones existentes (y todos sus informes de evaluación y exportaciones a CSV) siguen utilizando la antigua clave KMS. Si la identidad de IAM que genera el informe de evaluación no puede usar la antigua clave de KMS, concede permisos a nivel de política de claves.

Audit Manager console

Actualización de la configuración del cifrado de datos en la consola de Audit Manager

1. En la pestaña de ajustes General, vaya a la sección Cifrado de datos.
2. Para usar la clave KMS predeterminada que proporciona Audit Manager, desactive la casilla Personalizar la configuración de cifrado (avanzada).
3. Para utilizar una clave administrada por el cliente, active la casilla de verificación Personalizar la configuración de cifrado (avanzada). Puede elegir entonces una clave KMS existente o crear una nueva.

AWS CLI

Para actualizar la configuración de cifrado de datos en el AWS CLI

Ejecute el comando update-settings y utilice el parámetro `--kms-key` para especificar su propia clave administrada por el cliente.

En el siguiente ejemplo, *`placeholder text`* sustitúyalo por su propia información.

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

Actualización de la configuración del cifrado de datos mediante la API

Llame a la UpdateSettingsoperación y utilice el parámetro KMSKey para especificar su propia clave gestionada por el cliente.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar esta operación y este parámetro en uno de los idiomas específicos. AWS SDKs

Recursos adicionales

- Para obtener instrucciones sobre cómo crear claves, consulte Creación de claves en la Guía del usuario de AWS Key Management Service .
- Para obtener instrucciones sobre cómo conceder permisos a nivel de política clave, consulte Permitir que los usuarios de otras cuentas usen una clave de KMS en la Guía para AWS Key Management Service desarrolladores.

Adición de un administrador delegado

Si utiliza AWS Organizations y desea habilitar la compatibilidad con varias cuentas AWS Audit Manager, puede designar una cuenta de miembro de su organización como administrador delegado de Audit Manager.

Si desea utilizar Audit Manager en más de una Región de AWS, debe designar una cuenta de administrador delegado por separado en cada región. En la configuración de Audit Manager, debe usar la misma cuenta de administrador delegado en todas las regiones.

Requisitos previos

Tome nota de los siguientes factores que definen cómo funciona el administrador delegado en Audit Manager:

- Su cuenta debe formar parte de una organización.
- Antes de designar un administrador delegado, debe habilitar todas las características de su organización. También debe configurar los ajustes del centro de seguridad de su organización. De

esta forma, Audit Manager puede recopilar evidencias del centro de seguridad de las cuentas de sus miembros.

- La cuenta de administrador delegado debe tener acceso a la clave KMS que proporcionó al configurar Audit Manager.
- No puede usar su cuenta AWS Organizations de administración como administrador delegado en Audit Manager.

Procedimiento

Puede añadir un administrador delegado mediante la consola de Audit Manager, la AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

> **Note**
>
> Tras añadir un administrador delegado en la configuración de Audit Manager, su cuenta de administración ya no podrá crear evaluaciones adicionales en Audit Manager. Además, la recopilación de evidencias se detiene para cualquier evaluación existente creada por la cuenta de administración. Audit Manager recopila y adjunta evidencias a la cuenta de administrador delegado, que es la cuenta principal para gestionar las evaluaciones de la organización.

Audit Manager console

Adición de un administrador delegado en la consola de Audit Manager

1. En la pestaña de configuración General, vaya a la sección Administrador delegado.
2. En ID de cuenta de administrador delegado, introduzca el ID de cuenta del administrador delegado.
3. Elija Delegar.

AWS CLI

Para añadir un administrador delegado en el AWS CLI

Ejecute el register-organization-admin-accountcomando y utilice el `--admin-account-id` parámetro para especificar el ID de cuenta del administrador delegado.

En el siguiente ejemplo, sustituya el *placeholder text* por su propia información.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Adición de un administrador delegado mediante la API

Llame a la RegisterOrganizationAdminAccountoperación y utilice el adminAccountIdparámetro para especificar el ID de cuenta del administrador delegado.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar esta operación y este parámetro en uno de los idiomas AWS SDKs específicos.

Pasos a seguir a continuación

Para cambiar la cuenta de administrador delegado, consulte Cambio de un administrador delegado.

Para eliminar la cuenta de administrador delegado, consulte Eliminación de un administrador delegado.

Recursos adicionales

- Creating and managing an organization
- Solución de problemas AWS Organizations y del administrador delegado

Cambio de un administrador delegado

El cambio de administrador delegado AWS Audit Manager es un proceso de dos pasos. En primer lugar, debe eliminar la cuenta de administrador delegado actual. A continuación, puede añadir una nueva cuenta como administrador delegado.

Siga los pasos que se indican en esta página para cambiar el administrador delegado.

Contenido

- Requisitos previos

- Antes de eliminar la cuenta actual
- Antes de añadir la cuenta nueva
- Procedimiento
- Pasos a seguir a continuación
- Recursos adicionales

Requisitos previos

Antes de eliminar la cuenta actual

Antes de eliminar la cuenta de administrador delegado actual, tenga en cuenta lo siguiente:

- Tarea de limpieza del buscador de evidencias: si el administrador delegado actual (cuenta A) ha habilitado el buscador de evidencias, tendrá que realizar una tarea de limpieza antes de asignar la cuenta B como nuevo administrador delegado.

  Antes de usar su cuenta de administración para eliminar la cuenta A, asegúrese de que dicha cuenta inicie sesión en Audit Manager y deshabilite el buscador de evidencias. Al deshabilitar el buscador de evidencias, se elimina automáticamente el almacén de datos de eventos que se creó en la cuenta al habilitar el buscador de evidencias.

  Si esta tarea no se completa, el almacén de datos del evento permanece en la cuenta A. En ese caso, recomendamos que el administrador delegado original utilice CloudTrail Lake para eliminar manualmente el banco de datos del evento.

  Esta tarea de limpieza es necesaria para garantizar que no acabe con varios almacenes de datos de eventos. Audit Manager ignora un almacén de datos de eventos no utilizado después de eliminar o cambiar una cuenta de administrador delegado. Sin embargo, si no eliminas el almacén de datos de eventos no utilizado, Lake seguirá incurriendo en costes de CloudTrail almacenamiento para él.
- Eliminación de datos: Al eliminar una cuenta de administrador delegado en Audit Manager, no se eliminarán los datos de esa cuenta. Si desea eliminar los datos de los recursos de una cuenta de administrador delegado, debe realizar esa tarea por separado antes de eliminar la cuenta. También puede hacer lo siguiente en la consola de Audit Manager. O puede utilizar una de las operaciones de eliminación de API proporcionadas por Audit Manager. Para obtener una lista de las operaciones de eliminación disponibles, consulte Eliminación de datos de Audit Manager.

En este momento, Audit Manager no ofrece la opción de eliminar las evidencias de un administrador delegado específico. En su lugar, cuando su cuenta de administración anula el registro de Audit Manager, realizamos una limpieza de la cuenta de administrador delegado actual en el momento de anular el registro.

Antes de añadir la cuenta nueva

Antes de añadir la cuenta nueva de administrador delegado, tenga en cuenta lo siguiente:

- La cuenta nueva debe formar parte de una organización.
- Antes de designar un nuevo administrador delegado, debe habilitar todas las características de su organización. También debe configurar los ajustes del centro de seguridad de su organización. De esta forma, Audit Manager puede recopilar evidencias del centro de seguridad de las cuentas de sus miembros.
- La cuenta de administrador delegado debe tener acceso a la clave KMS que proporcionó al configurar Audit Manager.
- No puede usar su cuenta AWS Organizations de administración como administrador delegado en Audit Manager.

Procedimiento

Puede cambiar un administrador delegado mediante la consola de Audit Manager, la AWS Command Line Interface (AWS CLI) o la API de Audit Manager.

> **Warning**
>
> Cuando cambia de administrador delegado, sigue teniendo acceso a las evidencias que recopiló anteriormente con la antigua cuenta de administrador delegado. Sin embargo, Audit Manager deja de recopilar y adjuntar evidencias a la antigua cuenta de administrador delegado.

Audit Manager console

Cambio del administrador delegado actual en la consola de Audit Manager

1. (Opcional) Si el administrador delegado actual (cuenta A) ha habilitado el buscador de evidencias, lleve a cabo la siguiente tarea de limpieza:

   - Antes de asignar la cuenta B como nueva administradora delegada, asegúrese de que la cuenta A inicie sesión en Audit Manager y deshabilite el buscador de evidencias.

     Al deshabilitar el buscador de evidencias, se elimina automáticamente el almacén de datos de eventos que se creó cuando la cuenta A habilitó el buscador de evidencias. Si no completa este paso, la cuenta A debe ir a CloudTrail Lake y eliminar manualmente el almacén de datos de eventos. De lo contrario, el almacén de datos del evento permanecerá en la cuenta A y seguirá incurriendo en gastos de almacenamiento en CloudTrail Lake.
2. En la pestaña de configuración General, vaya a la sección Administrador delegado y elija Eliminar.
3. En la ventana emergente que aparece, seleccione Eliminar para confirmar.
4. En ID de cuenta de administrador delegado, introduzca el ID de cuenta del nuevo administrador delegado.
5. Elija Delegar.

AWS CLI

Cambio del administrador delegado actual en la AWS CLI

En primer lugar, ejecute el deregister-organization-admin-accountcomando con el `--admin-account-id` parámetro para especificar el ID de cuenta del administrador delegado actual.

En el siguiente ejemplo, sustituya el *`placeholder text`* por su propia información.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

A continuación, ejecute el register-organization-admin-accountcomando con el `--admin-account-id` parámetro para especificar el ID de cuenta del nuevo administrador delegado.

En el siguiente ejemplo, sustituya el *`placeholder text`* por su propia información.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

Cambio del administrador delegado actual mediante la API

En primer lugar, llame a la DeregisterOrganizationAdminAccountoperación y utilice el adminAccountIdparámetro para especificar el ID de cuenta del administrador delegado actual.

A continuación, llame a la RegisterOrganizationAdminAccountoperación y utilice el adminAccountIdparámetro para especificar el ID de cuenta del nuevo administrador delegado.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar esta operación y este parámetro en uno de los idiomas AWS SDKs específicos.

Pasos a seguir a continuación

Para eliminar la cuenta de administrador delegado, consulte Eliminación de un administrador delegado.

Recursos adicionales

- Creating and managing an organization
- Solución de problemas AWS Organizations y del administrador delegado

Eliminación de un administrador delegado

Al eliminar la cuenta de administrador delegado, se impedirá la recopilación de evidencias adicionales para esa cuenta, pero se conservará el acceso a las evidencias recopiladas anteriormente.

Si necesita eliminar la cuenta de administrador delegado en Audit Manager, puede seguir los pasos que hay que llevar a cabo en esta página. Siga detenidamente los requisitos previos y los procedimientos, ya que implican la limpieza de los recursos para evitar costos de almacenamiento innecesarios.

Requisitos previos

Antes de eliminar la cuenta de administrador delegado actual en Audit Manager, tenga en cuenta lo siguiente:

Tarea de limpieza del buscador de evidencias

Si el administrador delegado actual ha habilitado el buscador de evidencias, debe llevar a cabo una tarea de limpieza.

Antes de usar la cuenta de administración para eliminar el administrador delegado actual, asegúrese de que la cuenta de administrador delegado actual inicie sesión en Audit Manager y deshabilite el buscador de evidencias. Al deshabilitar el buscador de evidencias, se elimina automáticamente el almacén de datos de eventos que se creó en la cuenta al habilitar el buscador de evidencias.

Si esta tarea no se completa, el almacén de datos del evento permanece en su cuenta. En este caso, recomendamos que el administrador delegado original utilice CloudTrail Lake para eliminar manualmente el almacén de datos del evento.

Esta tarea de limpieza es necesaria para garantizar que no acabe con varios almacenes de datos de eventos. Audit Manager ignora un almacén de datos de eventos no utilizado después de eliminar o cambiar una cuenta de administrador delegado. Sin embargo, si no elimina el almacén de datos de eventos no utilizado, Lake seguirá incurriendo en costes de almacenamiento para el almacén de datos de CloudTrail eventos.

Eliminación de datos

Al eliminar una cuenta de administrador delegado de Audit Manager, los datos de esa cuenta no se eliminan. Si desea eliminar los datos de los recursos de una cuenta de administrador delegado, debe realizar esa tarea por separado antes de eliminar la cuenta. También puede hacer lo siguiente en la consola de Audit Manager. O puede utilizar una de las operaciones de eliminación de API proporcionadas por Audit Manager. Para obtener una lista de las operaciones de eliminación disponibles, consulte Eliminación de datos de Audit Manager.

En este momento, Audit Manager no ofrece la opción de eliminar las evidencias de un administrador delegado específico. En su lugar, cuando su cuenta de administración anula el registro de Audit Manager, realizamos una limpieza de la cuenta de administrador delegado actual en el momento de anular el registro.

Procedimiento

Puede añadir un administrador delegado mediante la consola Audit Manager, la AWS Command Line Interface (AWS CLI) o la API Audit Manager.

> **Warning**
>
> Cuando elimina a un administrador delegado, continúa teniendo acceso a la evidencia que recopiló previamente en esa cuenta de administrador delegado. Sin embargo, Audit Manager deja de recopilar y adjuntar evidencias a la antigua cuenta de administrador delegado.

Audit Manager console

Eliminación del administrador delegado actual en la consola de Audit Manager

1. (Opcional) Si el administrador delegado actual ha activado el buscador de evidencias, lleve a cabo la siguiente tarea de limpieza:

   - Asegúrese de que la cuenta de administrador delegado actual inicie sesión en Audit Manager y desactive el buscador de evidencias.

     Al deshabilitar el buscador de evidencias, se elimina automáticamente el almacén de datos de eventos que se creó en la cuenta cuando habilitaron el buscador de evidencias. Si no se completa este paso, la cuenta de administrador delegado debe usar CloudTrail Lake para eliminar manualmente el almacén de datos del evento. De lo contrario, el almacén de datos del evento permanecerá en su cuenta y seguirá incurriendo en gastos de almacenamiento en CloudTrail Lake.
2. En la pestaña de configuración General, vaya a la sección Administrador delegado y elija Eliminar.
3. En la ventana emergente que aparece, seleccione Eliminar para confirmar.

AWS CLI

Al deshabilitar el buscador de evidencias, se elimina automáticamente el almacén de datos de eventos que se creó en la cuenta cuando habilitaron el buscador de evidencias. Si no se completa este paso, la cuenta del administrador delegado debe usar CloudTrail Lake para eliminar manualmente el almacén de datos del evento. De lo contrario, el almacén de datos

del evento permanecerá en su cuenta y seguirá incurriendo en gastos de almacenamiento en CloudTrail Lake.

Eliminación del administrador delegado actual en la AWS CLI

Ejecute el deregister-organization-admin-accountcomando y utilice el `--admin-account-id` parámetro para especificar el ID de cuenta del administrador delegado.

En el siguiente ejemplo, sustituya el *`placeholder text`* por su propia información.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

Eliminación del administrador delegado actual mediante la API

Llame a la DeregisterOrganizationAdminAccountoperación y utilice el adminAccountIdparámetro para especificar el ID de cuenta del administrador delegado.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar esta operación y este parámetro en uno de los idiomas AWS SDKs específicos.

Recursos adicionales

- Solución de problemas AWS Organizations y del administrador delegado

Configuración de los responsables de auditoría predeterminados

Puede utilizar esta configuración para especificar los audit owner predeterminados que tienen acceso principal a las evaluaciones en Audit Manager.

Procedimiento

Puede actualizar esta configuración mediante la consola Audit Manager, la AWS Command Line Interface (AWS CLI) o la API Audit Manager.

Audit Manager console

Puede elegir una de las Cuentas de AWS opciones que aparecen en la tabla o utilizar la barra de búsqueda para buscar otras Cuentas de AWS.

Actualización de los responsables predeterminados de auditoría en la consola de Audit Manager

1. En la pestaña de configuración de la Evaluación, vaya a la sección Propietarios de auditoría predeterminados y seleccione Editar.
2. Para añadir un propietario de auditoría predeterminado, marque la casilla de verificación situada junto al nombre de cuenta en Propietario de auditoría.
3. Para eliminar un propietario de auditoría predeterminado, desmarque la casilla de verificación junto al nombre de la cuenta en Propietario de auditoría.
4. Cuando haya terminado, elija Guardar.

AWS CLI

Para actualizar el propietario de la auditoría predeterminado en el AWS CLI

Ejecute el comando update-settings y use el parámetro `--default-process-owners` para especificar un propietario de auditoría.

En el siguiente ejemplo, *`placeholder text`* sustitúyalo por su propia información. Tenga en cuenta que solo `roleType` puede ser. `PROCESS_OWNER`

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

Actualización del responsable de auditoría predeterminado mediante la API

Llame a la UpdateSettingsoperación y utilice el defaultProcessOwnersparámetro para especificar los propietarios de la auditoría predeterminados. Tenga en cuenta que solo `roleType` puede ser. `PROCESS_OWNER`

Recursos adicionales

- Para obtener más información sobre los propietarios de las auditorías, consulte Propietarios de las auditorías en la sección Conceptos y terminología de esta guía.

Configuración del destino del informe de evaluación predeterminado

Al generar un informe de evaluación, Audit Manager publica el informe en el bucket de S3 que elija. Este bucket de S3 se denomina assessment report destination. Puede elegir el bucket de S3 en el que Audit Manager almacena los informes de evaluación.

Requisitos previos

Consejos de configuración para el destino de su informe de evaluación

Para garantizar la correcta generación del informe de evaluación, le recomendamos que utilice las siguientes configuraciones para el destino del informe de evaluación.

Buckets de la misma región

Le recomendamos que utilice un bucket de S3 que se encuentre en la misma Región de AWS de su evaluación. Si utiliza un bucket y una evaluación de la misma región, el informe de evaluación puede incluir hasta 22 000 elementos de evidencias. Por el contrario, si utiliza un bucket y una evaluación entre regiones, solo se pueden incluir 3500 elementos de evidencias.

Región de AWS

La Región de AWS clave gestionada por el cliente (si la ha proporcionado) debe coincidir con la región de la evaluación y el depósito S3 de destino del informe de evaluación. Para obtener instrucciones sobre cómo cambiar la clave de KMS, consulte Configuración de los ajustes del cifrado de datos. Para obtener una lista de regiones admitidas de Audit Manager, consulte AWS Audit Manager Puntos de conexión y cuotas de en la Referencia general de Amazon Web Services.

Cifrado de buckets de S3

Si el destino de su informe de evaluación tiene una política de buckets que requiere el cifrado del servidor (SSE) mediante SSE-KMS, entonces, la clave de KMS utilizada en esa política de

buckets debe coincidir con la clave de KMS que configuró en los ajustes de cifrado de datos de Audit Manager. Si no ha configurado una clave KMS en la configuración de Audit Manager y la política de buckets de destino de su informe de evaluación requiere SSE, asegúrese de que la política de buckets permita SSE-S3. Para obtener instrucciones sobre cómo configurar la clave de KMS que se utiliza para el cifrado de datos, consulte Configuración de los ajustes del cifrado de datos.

Buckets de S3 entre cuentas

La consola de Audit Manager no admite el uso de un bucket de S3 entre cuentas como destino del informe de evaluación. Es posible especificar un segmento multicuenta como destino del informe de evaluación utilizando el AWS CLI o uno de los siguientes AWS SDKs, pero por motivos de simplicidad, le recomendamos que no lo haga.

> **Tip**
>
> Para una seguridad y un rendimiento óptimos, le recomendamos que utilice un depósito de S3 en la misma AWS cuenta y región que la evaluación.

Si opta por utilizar un bucket de S3 entre cuentas como destino del informe de evaluación, tenga en cuenta las siguientes cuestiones.

- De forma predeterminada, los objetos de S3 (como los informes de evaluación) son propiedad de quien carga el Cuenta de AWS objeto. Puede utilizar la configuración de Propiedad de objetos de S3 para cambiar este comportamiento predeterminado, de modo que cualquier nuevo objeto escrito por cuentas con la lista de control de acceso (ACL) predefinida `bucket-owner-full-control` se convierta automáticamente en propiedad del propietario del bucket.

  Aunque no es obligatorio, le recomendamos que realice los siguientes cambios en la configuración del bucket entre cuentas. Al realizar estos cambios, se garantiza que el propietario del bucket tenga el control total de los informes de evaluación que usted publique en su bucket.

  - Establezca la propiedad del objeto del bucket de S3 en el propietario del bucket preferido, en lugar de en el escritor de objetos predeterminado
  - Añada una política de buckets para asegurarse de que los objetos cargados en ese bucket tengan la ACL `bucket-owner-full-control`
- Para permitir que Audit Manager publique informes en un bucket de S3 entre cuentas, debe añadir la siguiente política de buckets de S3 al destino de su informe de evaluación.

Reemplace los *`placeholder text`* con su propia información. El elemento `Principal` de esta política es el usuario o el rol propietario de la evaluación y crea el informe de la evaluación. El `Resource` especifica el bucket de S3 entre cuentas en el que se publica el informe.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow cross account assessment report publishing",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:user/AssessmentOwnerUserName"
            },
            "Action": [
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:PutObjectAcl",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
            ]
        }
    ]
}
```

Procedimiento

Puede actualizar esta configuración mediante la consola Audit Manager, la AWS Command Line Interface (AWS CLI) o la API Audit Manager.

Audit Manager console

Actualización del destino del informe de evaluación predeterminado en la consola de Audit Manager

1. En la pestaña de configuración de la Evaluación, vaya a la sección Destino del informe de evaluación.
2. Para utilizar un bucket de S3 existente, seleccione un nombre de bucket en el menú desplegable.
3. Para crear un nuevo bucket de S3, elija Crear un bucket nuevo.
4. Cuando haya terminado, elija Guardar.

AWS CLI

Actualización del destino del informe de evaluación predeterminado en la AWS CLI

Ejecute el comando update-settings y utilice el parámetro `--default-assessment-reports-destination` para especificar un bucket de S3.

En el siguiente ejemplo, sustituya el *`placeholder text`* por su propia información:

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://amzn-s3-demo-destination-bucket
```

Audit Manager API

Actualización del destino del informe de evaluación predeterminado mediante la API

Llame a la UpdateSettingsoperación y utilice el parámetro defaultAssessmentReportsDestination para especificar un bucket de S3.

Recursos adicionales

- Crear un bucket
- Informes de evaluación

Configuración de notificaciones en Audit Manager

Puede configurar Audit Manager para enviar notificaciones al tema de Amazon SNS que elija. Si está suscrito a ese tema de SNS, recibirá notificaciones directamente cuando inicie sesión en Audit Manager.

Siga los pasos que se indican en esta página para descubrir cómo ver y actualizar la configuración de las notificaciones para adaptarla a sus preferencias. Puede usar un tema de SNS estándar o un tema de SNS de FIFO (first-in-first-out). Aunque Audit Manager admite el envío de notificaciones a temas de FIFO, no se garantiza el orden en que se envían los mensajes.

Requisitos previos

Si desea utilizar un tema de Amazon SNS que no sea de su propiedad, debe configurar la política de AWS Identity and Access Management (IAM). Más específicamente, debe configurarlo para permitir la publicación desde el nombre de recurso de Amazon (ARN) del tema. Para ver un ejemplo de política que puede usar, consulte Ejemplo 1 (Permisos para el tema SNS).

Procedimiento

Puede actualizar esta configuración mediante la consola Audit Manager, la AWS Command Line Interface (AWS CLI) o la API Audit Manager.

Audit Manager console

Actualización de la configuración de las notificaciones en la consola de Audit Manager

1. En la pestaña de configuración de la Evaluación, vaya a la sección Notificaciones.
2. Para utilizar un tema de SNS existente, seleccione el nombre del tema en el menú desplegable.
3. Para crear un nuevo tema de SNS, elija Crear nuevo tema.
4. Cuando haya terminado, elija Guardar.

AWS CLI

Para actualizar la configuración de notificaciones en el AWS CLI

Ejecute el comando update-settings y utilice el parámetro `--sns-topic` para especificar un tema de SNS.

En el siguiente ejemplo, sustituya la *`placeholder text`* por su propia información:

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

Actualización de la configuración de las notificaciones mediante la API

Llame a la UpdateSettingsoperación y utilice el parámetro SNStopic para especificar un tema de SNS.

Recursos adicionales

- Para obtener instrucciones sobre cómo crear un tema de Amazon SNS, consulte Crear un tema de Amazon SNS en la Guía del usuario de Amazon SNS.
- Para ver un ejemplo de política que puede usar para permitir que Audit Manager envíe notificaciones a temas de Amazon SNS, consulte Ejemplo 1 (Permisos para el tema SNS).
- Para obtener más información sobre la lista de acciones que invocan notificaciones en Audit Manager, consulte Notificaciones en AWS Audit Manager.
- Para obtener soluciones a problemas relacionados con las notificaciones en Audit Manager, consulte Solución de problemas de notificación.

Habilitar el buscador de evidencias

Puede habilitar la característica de buscador de evidencias en Audit Manager para buscar evidencias en la Cuenta de AWS. Si es administrador delegado de Audit Manager, puede buscar evidencias en todas las cuentas de los miembros de su organización.

Siga estos pasos para descubrir cómo habilitar el buscador de evidencias. Presta mucha atención a los requisitos previos, ya que necesitarás permisos específicos para crear y administrar un almacén de datos de eventos en CloudTrail Lake para poder utilizar esta funcionalidad.

Requisitos previos

Permisos necesarios para habilitar el buscador de evidencias

Para habilitar el buscador de evidencias, necesitas permisos para crear y administrar un almacén de datos de eventos en CloudTrail Lake. Para utilizar la función, necesita permisos para realizar

consultas en CloudTrail Lake. Para ver un ejemplo de política de permisos que puede usar, consulte Ejemplo 3 (Permisos para habilitar el buscador de pruebas).

Si necesita ayuda con los permisos, póngase en contacto con su AWS administrador. Si es AWS administrador, puede copiar la declaración de permisos requerida y adjuntarla a una política de IAM.

Procedimiento

Solicitar habilitar el buscador de evidencias

Puede completar esta tarea mediante la consola de Audit Manager, la AWS Command Line Interface (AWS CLI) o la API Audit Manager.

> **Note**
>
> Debe habilitar el buscador de pruebas en cada Región de AWS lugar donde desee buscar pruebas.

Audit Manager console

Solicitud de habilitación del buscador de evidencias en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En la pestaña de configuración del buscador de evidencias, vaya a la sección Buscador de evidencias.
3. Seleccione Política de permisos obligatoria y, a continuación, consulte los permisos de CloudTrail Lake para ver los permisos de búsqueda de pruebas necesarios. Si aún no tiene estos permisos, puede copiar esta declaración de política y adjuntarla a una política de IAM.
4. Elija Habilitar.
5. En la ventana emergente, seleccione Solicitud de habilitación.

AWS CLI

Para solicitar la activación del buscador de pruebas en el AWS CLI

Ejecute el comando update-settings con el parámetro `--evidence-finder-enabled`.

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

Solicitud de habilitación del buscador de evidencias mediante la API

Llame a la UpdateSettingsoperación y utilice el evidenceFinderEnabledparámetro.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar esta operación y este parámetro en uno de los idiomas específicos AWS SDKs.

Pasos a seguir a continuación

Una vez que haya solicitado la habilitación del buscador de evidencias, podrá comprobar el estado de su solicitud. Para obtener instrucciones, consulte Confirming the status of evidence finder.

Recursos adicionales

- Buscador de evidencias
- Solución de problemas con el buscador de evidencias

Confirming the status of evidence finder

Tras enviar la solicitud para habilitar el buscador de evidencias, se necesitarán hasta 10 minutos para habilitar esta característica y crear un almacén de datos de eventos. En cuanto se crea el almacén de datos del evento, todas las evidencias nuevas se incorporan al almacén de datos del evento a partir de ahora.

Cuando el buscador de evidencias está habilitado y se crea el almacén de datos del evento, rellenamos el almacén de datos del evento recién creado con evidencias anteriores equivalentes a un máximo de dos años. Este proceso se realiza automáticamente y tarda hasta siete días en completarse.

Siga los pasos que se indican en esta página para comprobar y comprender el estado de su solicitud y habilitar el buscador de evidencias.

Requisitos previos

Asegúrese de seguir los pasos para habilitar el buscador de evidencias. Para obtener instrucciones, consulte Habilitar el buscador de evidencias.

Procedimiento

Puede comprobar el estado actual del buscador de evidencias mediante la consola de Audit Manager, la AWS CLI o la API de Audit Manager.

Audit Manager console

Visualización del estado actual del buscador de evidencias en la consola de Audit Manager

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Configuración.
3. En Habilitar el buscador de evidencias (opcional), revise el estado actual.

   Cada estado se define de la siguiente manera:

Estado	Descripción
El buscador de evidencias no está habilitado	Aún no ha habilitado correctamente el buscador de evidencias.
Ha solicitado habilitar el buscador de evidencias	Su solicitud está pendiente de la creación del almacén de datos de eventos.
El buscador de evidencias está habilitado	Se ha creado el almacén de datos de eventos. A partir de ahora, puede utilizar el buscador de evidencias. Dependiendo de la cantidad de evidencias que tenga, tardará hasta siete días en rellenar el nuevo almacén de datos de eventos con los datos de las evidencias anteriores. Un panel de información azul indica que la reposición de datos está en curso. Mientras tanto, no dude en empezar a explorar el buscador de evidencias. Sin embargo, tenga en cuenta que

Estado	Descripción
	no todos los datos están disponibles hasta que se complete la reposición.
Ha solicitado deshabilitar el buscador de evidencias	Su solicitud está pendiente de la eliminación del almacén de datos de eventos.
El buscador de evidencias está deshabilitado	Se ha deshabilitado de forma permanente el buscador de evidencias y se ha eliminado el almacén de datos de eventos.

AWS CLI

Para ver el estado actual del buscador de pruebas en el AWS CLI

Ejecute el comando get-settings con el parámetro `--attribute` configurado como `EVIDENCE_FINDER_ENABLEMENT`.

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

Esto devuelve la siguiente información:

enablementStatus

Este atributo muestra el estado actual del buscador de evidencias.

- `ENABLE_IN_PROGRESS`: ha solicitado habilitar el buscador de evidencias. Actualmente se está creando un almacén de datos de eventos para respaldar las consultas de los buscadores de evidencias.
- `ENABLED`: se creó un almacén de datos de eventos y se habilitó el buscador de evidencias. Le recomendamos que espere siete días hasta que el almacén de datos del evento se rellene con sus datos de evidencias anteriores. Mientras tanto, puede utilizar el buscador de evidencias, pero no todos los datos estarán disponibles hasta que se complete el proceso de relleno.
- `DISABLE_IN_PROGRESS`: ha solicitado desactivar el buscador de evidencias y su solicitud está pendiente de que se elimine el almacén de datos de eventos.
- `DISABLED`: ha deshabilitado permanentemente el buscador de evidencias y se ha eliminado el almacén de datos del evento. Después de este punto, no podrá volver a habilitar el buscador de evidencias.

backfillStatus

Este atributo muestra el estado actual de la reposición del buscador de evidencias.

- `NOT_STARTED`: la reposición aún no ha empezado.
- `IN_PROGRESS`: la reposición está en curso. Esto tarda hasta siete días en completarse, según la cantidad de evidencias.
- `COMPLETED`: la reposición ha finalizado. Todas sus evidencias anteriores ahora son consultables.

Audit Manager API

Visualización del estado actual del buscador de evidencias mediante la API

Llame a la GetSettingsoperación con el `attribute` parámetro establecido en`EVIDENCE_FINDER_ENABLEMENT`. Esto devuelve la siguiente información:

enablementStatus

Este atributo muestra el estado actual del buscador de evidencias.

- `ENABLE_IN_PROGRESS`: ha solicitado habilitar el buscador de evidencias. Actualmente se está creando un almacén de datos de eventos para respaldar las consultas de los buscadores de evidencias.
- `ENABLED`: se creó un almacén de datos de eventos y se habilitó el buscador de evidencias. Le recomendamos que espere siete días hasta que el almacén de datos del evento se rellene con sus datos de evidencias anteriores. Mientras tanto, puede utilizar el buscador de evidencias, pero no todos los datos estarán disponibles hasta que se complete el proceso de relleno.
- `DISABLE_IN_PROGRESS`: ha solicitado deshabilitar el buscador de evidencias y su solicitud está pendiente de que se elimine el almacén de datos de eventos.
- `DISABLED`: ha deshabilitado permanentemente el buscador de evidencias y se ha eliminado el almacén de datos del evento. Después de este punto, no podrá volver a habilitar el buscador de evidencias.

backfillStatus

Este atributo muestra el estado actual de la reposición del buscador de evidencias.

- `NOT_STARTED` significa que la reposición aún no ha empezado.
- `IN_PROGRESS` significa que la reposición está en curso. Esto tarda hasta siete días en completarse, según la cantidad de evidencias.
- `COMPLETED` significa que la reposición ha finalizado. Todas sus evidencias anteriores ahora son consultables.

Para obtener más información, consulte evidenceFinderEnablementla Referencia de la API de Audit Manager.

Pasos a seguir a continuación

Una vez que el buscador de evidencias se haya habilitado correctamente, podrá empezar a utilizar la característica. Le recomendamos que espere siete días hasta que el almacén de datos del evento se rellene con sus datos de evidencias anteriores. Mientras tanto, puede utilizar el buscador de evidencias, pero es posible que no todos los datos estén disponibles hasta que se complete el proceso de reposición.

Para comenzar a trabajar con el buscador de evidencias, consulte Búsqueda de evidencias en el buscador de evidencias.

Recursos adicionales

- Solución de problemas con el buscador de evidencias

Deshabilitar el buscador de evidencias

Si ya no desea utilizar el buscador de evidencias, puede deshabilitar esta característica en cualquier momento.

Siga estos pasos para descubrir cómo deshabilitar el buscador de evidencias. Presta mucha atención a los requisitos previos, ya que necesitarás permisos específicos para eliminar el almacén de datos de eventos en CloudTrail Lake que se creó al activar el buscador de evidencias.

Requisitos previos

Permisos necesarios para deshabilitar el buscador de evidencias

Para deshabilitar el buscador de evidencias, necesitas permisos para eliminar un almacén de datos de eventos en CloudTrail Lake. Para ver un ejemplo de política que puede utilizar, consulte Permisos para deshabilitar el buscador de evidencias.

Si necesitas ayuda con los permisos, ponte en contacto con tu AWS administrador. Si es AWS administrador, puede adjuntar la declaración de permisos requerida a una política de IAM.

Procedimiento

Puede completar esta tarea mediante la consola de Audit Manager, la AWS Command Line Interface (AWS CLI) o la API Audit Manager.

> **Warning**
>
> Al deshabilitar el buscador de evidencias, se elimina el almacén de datos de eventos de CloudTrail Lake que creó Audit Manager. Por consiguiente, no puede volver a habilitar la característica. Para volver a utilizar el buscador de evidencias después de deshabilitarlo, debe deshabilitar AWS Audit Manager y, a continuación, volver a habilitar el servicio por completo.

Audit Manager console

Deshabilitación del buscador de evidencias en la consola de Audit Manager

1. En la sección Buscador de evidencias de la página de configuración de Audit Manager, seleccione Deshabilitar.
2. En la ventana emergente que aparece, introduzca **`Yes`** para confirmar su decisión.
3. Seleccione Solicitar deshabilitación.

AWS CLI

Para deshabilitar el buscador de pruebas en el AWS CLI

Ejecute el comando update-settings con el parámetro `--no-evidence-finder-enabled`.

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

Deshabilitación del buscador de evidencias mediante la API

Llame a la UpdateSettingsoperación y utilice el evidenceFinderEnabledparámetro.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar esta operación y este parámetro en uno de los idiomas específicos AWS SDKs.

Recursos adicionales

- Solución de problemas con el buscador de evidencias

Configuración del destino de la exportación predeterminada para el buscador de evidencias

Al ejecutar consultas en el buscador de evidencias, puede exportar los resultados de la búsqueda a un archivo CSV (valores separados por comas). Utilice esta configuración para elegir el bucket de S3 predeterminado en el que Audit Manager guarda los archivos exportados.

Requisitos previos

Su bucket de S3 debe tener la política de permisos necesaria para poder CloudTrail escribir en él los archivos de exportación. Más específicamente, la política de bucket debe incluir una `s3:PutObject` acción y el ARN del bucket, y figurar CloudTrail como principal de servicio.

- Para ver un ejemplo de política de permisos que puede usar, consulte Ejemplos de políticas basadas en recursos para AWS Audit Manager.
- Para obtener instrucciones sobre cómo asociar esta política al bucket de S3, consulte Agregar una política de bucket mediante la consola de Amazon S3.
- Para obtener más consejos, consulte los Consejos de configuración para su destino de exportación en esta página.

Consejos de configuración para el destino de su exportación

Para garantizar una exportación de archivos correcta, le recomendamos que compruebe las siguientes configuraciones para el destino de su exportación.

Región de AWS

La Región de AWS clave administrada por el cliente (si la proporcionó) debe coincidir con la región de su evaluación. Para obtener instrucciones sobre cómo cambiar la clave KMS, consulte Configuración de cifrado de datos de Audit Manager.

Buckets de S3 entre cuentas

La consola de Audit Manager no admite el uso de un bucket de S3 entre cuentas como destino de su exportación. Es posible especificar un segmento multicuenta utilizando la AWS CLI o una de las AWS SDKs, pero por motivos de simplicidad, le recomendamos que no lo haga. Si opta por utilizar un bucket de S3 entre cuentas como destino de su exportación, tenga en cuenta las siguientes cuestiones.

- De forma predeterminada, los objetos de S3 (como las exportaciones a CSV) son propiedad de quien carga el Cuenta de AWS objeto. Puede utilizar la configuración de Propiedad de objetos de S3 para cambiar este comportamiento predeterminado, de modo que cualquier nuevo objeto escrito por cuentas con la lista de control de acceso (ACL) predefinida `bucket-owner-full-control` se convierta automáticamente en propiedad del propietario del bucket.

  Aunque no es obligatorio, le recomendamos que realice los siguientes cambios en la configuración del bucket entre cuentas. Al realizar estos cambios, se garantiza que el propietario del bucket tenga el control total de los archivos exportados que publica en su bucket.

  - Establezca la propiedad del objeto del bucket de S3 en el propietario del bucket preferido, en lugar de en el escritor de objetos predeterminado
  - Añada una política de buckets para asegurarse de que los objetos cargados en ese bucket tengan la ACL `bucket-owner-full-control`
- Para permitir que Audit Manager exporte archivos a un depósito S3 entre cuentas, debe agregar la siguiente política de bucket de S3 a su bucket de destino de exportación. Reemplace los *`placeholder text`* con su propia información. El `Principal` elemento de esta política es el usuario o rol propietario de la evaluación y exporta el archivo. El `Resource` especifica el bucket de S3 entre cuentas al que se exporta el archivo.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow cross account file exports",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:user/AssessmentOwnerUserName"
            },
            "Action": [
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:PutObjectAcl",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
            ]
        }
    ]
}
```

Procedimiento

Puede actualizar esta configuración mediante la consola Audit Manager, la AWS Command Line Interface (AWS CLI) o la API Audit Manager.

Audit Manager console

Actualización de la configuración del destino de exportación en la consola de Audit Manager

1. En la pestaña de configuración del buscador de evidencias, vaya a la sección Destino de exportación.
2. Seleccione una de las siguientes opciones:

- Si quiere eliminar el bucket de S3 actual, seleccione Eliminar para borrar la configuración.
- Si quiere guardar un bucket de S3 predeterminado por primera vez, continúe con el paso 3.

3. Especifique el bucket de S3 en el que desea almacenar los archivos exportados.

   - Seleccione Explorar S3 para elegir de una lista de sus buckets.
   - Como alternativa, puede introducir el URI del bucket en este formato: **`s3://bucketname/prefix`**

   > **Tip**
   >
   > Para mantener el bucket de destino organizado, puede crear una carpeta opcional para sus exportaciones a CSV. Para ello, añada una barra (**/**) y un prefijo al valor del cuadro URI del recurso (por ejemplo, **`/evidenceFinderCSVExports`**). A continuación, Audit Manager incluirá este prefijo cuando añada el archivo CSV al bucket y Amazon S3 generará la ruta especificada por el prefijo. Para obtener más información acerca de los prefijos en Amazon S3, consulte Organizar objetos en la consola de Amazon S3 en la guía del usuario de Amazon Simple Storage Service.

4. Cuando haya terminado, elija Guardar.

Para obtener más información sobre cómo crear un bucket de S3, consulte Crear un bucket en la Guía del usuario de Amazon S3.

AWS CLI

Para actualizar la configuración del destino de exportación en el AWS CLI

Ejecute el comando update-settings y utilice el parámetro `--default-export-destination` para especificar un bucket de S3.

En el siguiente ejemplo, *`placeholder text`* sustitúyalo por su propia información:

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=amzn-s3-demo-destination-bucket
```

Para obtener instrucciones sobre cómo crear un bucket de S3, consulte create-bucket en la Referencia de comandos de la AWS CLI .

Audit Manager API

Actualización de la configuración del destino de exportación mediante la API

Llame a la UpdateSettingsoperación y utilice el defaultExportDestinationparámetro para especificar un bucket de S3.

Para obtener instrucciones sobre cómo crear un bucket de S3, consulte CreateBucketla referencia de la API de Amazon S3.

Notificaciones en AWS Audit Manager

AWS Audit Manager puede notificarle las acciones de los usuarios a través de Amazon Simple Notification Service (Amazon SNS).

Audit Manager envía notificaciones cuando se produce uno de los siguientes eventos:

- El propietario de la auditoría delega un conjunto de controles para su revisión.
- Un delegado envía un conjunto de controles revisado al propietario de la auditoría.
- El propietario de la auditoría completa la revisión de un conjunto de controles.

Recursos adicionales

- Para configurar las notificaciones en Audit Manager, consulte Configuración de notificaciones en Audit Manager.
- Para encontrar respuestas a preguntas y problemas comunes, consulte Solución de problemas de notificación en la sección Solución de problemas de esta guía.

Solución de problemas comunes en AWS Audit Manager

A medida que lo utilice AWS Audit Manager, es posible que encuentre ciertos problemas o desafíos que deban solucionarse. Ya sea que tenga dificultades para configurar las evaluaciones, recopilar evidencias o cualquier otro aspecto del servicio, puede utilizar esta guía de solución de problemas para encontrar nuestras recomendaciones que le ayudarán a resolver problemas comunes de forma rápida y eficaz.

Le recomendamos que revise la lista de temas que aparece a continuación, busque el que mejor se adapte a su situación y siga las instrucciones indicadas para retomar el hilo. Si sigue los pasos de solución de problemas indicados, es probable que pueda resolver el problema de forma independiente y seguir sacando partido de todas las capacidades de Audit Manager. Sin embargo, si el problema no se trata aquí o no puede resolverlo después de seguir los pasos recomendados, le recomendamos que se ponga en contacto con Soporte para obtener más ayuda.

Temas

- Solución de problemas de evaluación y recopilación de pruebas
- Solución de problemas con el informe de evaluación
- Solución de problemas de control y conjunto de control
- Solución de problemas de panel
- Solución de problemas AWS Organizations y del administrador delegado
- Solución de problemas con el buscador de evidencias
- Solución de problemas con los marcos
- Solución de problemas de notificación
- Solución de problemas de permisos y acceso

Solución de problemas de evaluación y recopilación de pruebas

Puede utilizar la información de esta página para resolver problemas comunes de evaluación y recopilación de pruebas en Audit Manager.

Problemas con la recopilación de evidencias

- He creado una evaluación, pero aún no veo ninguna prueba

- Mi evaluación no consiste en recopilar pruebas de control de cumplimiento de AWS Security Hub
- Mi evaluación no consiste en recopilar pruebas de control de cumplimiento de AWS Config
- Mi evaluación no consiste en recopilar pruebas de la actividad de los usuarios de AWS CloudTrail
- Mi evaluación no consiste en recopilar evidencia de datos de configuración para una llamada a la AWS API
- Un control común no está recopilando ninguna evidencia automatizada
- Mis pruebas se generan a intervalos diferentes y no estoy seguro de la frecuencia con la que se recopilan
- He desactivado Audit Manager y, a continuación, he vuelto a activarlo, y ahora mis evaluaciones preexistentes ya no recopilan pruebas
- En la página de detalles de la evaluación se me pide que vuelva a crearla
- ¿Cuál es la diferencia entre un origen de datos y un origen de evidencias?

Problemas con las evaluaciones

- Error al crear mi evaluación
- ¿Qué ocurre si elimino una cuenta incluida en el ámbito de aplicación de mi organización?
- No puedo ver los servicios incluidos en el ámbito de la evaluación
- No puedo editar los servicios incluidos en el ámbito de mi evaluación
- ¿Cuál es la diferencia entre un servicio incluido y un tipo de origen de datos?

He creado una evaluación, pero aún no veo ninguna prueba

Si no ve ninguna prueba, es probable que no haya esperado al menos 24 horas después de crear la evaluación o que se trate de un error de configuración.

Le recomendamos que compruebe lo siguiente:

1. Asegúrese de que hayan pasado 24 horas desde que creó la evaluación. Las pruebas automatizadas pasan a estar disponibles las 24 horas después de crear la evaluación.
2. Asegúrese de utilizar Audit Manager de la Región de AWS misma forma en Servicio de AWS que espera ver pruebas.
3. Si espera ver pruebas de conformidad procedentes de AWS Config y AWS Security Hub, asegúrese de que tanto la consola como la AWS Config de Security Hub muestren los resultados

de estas comprobaciones. Los resultados AWS Config y los de Security Hub deberían mostrarse en el mismo Región de AWS formato en el que utiliza Audit Manager.

Si sigue sin poder ver pruebas en su evaluación y no se debe a uno de estos problemas, compruebe las demás posibles causas que se describen en esta página.

Mi evaluación no consiste en recopilar pruebas de control de cumplimiento de AWS Security Hub

Si no ve las pruebas de verificación de conformidad de un AWS Security Hub control, podría deberse a uno de los siguientes problemas.

Falta la configuración en AWS Security Hub

Este problema puede deberse a que omitió algunos pasos de configuración cuando habilitó AWS Security Hub.

Para solucionar este problema, asegúrese de haber habilitado Security Hub con la configuración requerida para Audit Manager. Para obtener instrucciones, consulte Habilitar y configurar AWS Security Hub.

Se ha introducido incorrectamente un nombre de control de Security Hub en su **`ControlMappingSource`**

Cuando utiliza la API Audit Manager para crear un control personalizado, puede especificar un control de Security Hub como asignación de origen de datos para la recopilación de pruebas. Para ello, introduzca un ID de control como `keywordValue`.

Si no ve pruebas de verificación de conformidad de un control de Security Hub, es posible que el `keywordValue` se haya introducido incorrectamente en su `ControlMappingSource`. El `keywordValue` distingue entre mayúsculas y minúsculas. Si la introduce de forma incorrecta, es posible que Audit Manager no reconozca esa regla. Como resultado, es posible que no recopile las pruebas de verificación de cumplimiento de ese control como se esperaba.

Para solucionar este problema, actualice el control personalizado y revise el `keywordValue`. El formato correcto de una palabra clave de Security Hub varía. Para mayor precisión, consulte la lista de Controles de Security Hub compatibles .

`AuditManagerSecurityHubFindingsReceiver`Falta EventBridge la regla de Amazon

Al activar Audit Manager, `AuditManagerSecurityHubFindingsReceiver` se crea y activa automáticamente una regla denominada en Amazon EventBridge. Esta regla permite a Audit Manager recopilar las conclusiones de Security Hub como pruebas.

Si esta regla no aparece ni habilitada en el Región de AWS lugar donde usa Security Hub, Audit Manager no podrá recopilar los resultados del Security Hub para esa región.

Para resolver este problema, ve a la EventBridge consola y confirma que la `AuditManagerSecurityHubFindingsReceiver` regla existe en tu Cuenta de AWS. Si la regla no existe, le recomendamos que desactive Audit Manager y, a continuación, vuelva a activar el servicio. Si esta acción no resuelve el problema o si la desactivación de Audit Manager no es una opción, pongáse en contacto con nosotros Soporte para obtener ayuda.

AWS Config Reglas vinculadas a servicios creadas por Security Hub

Tenga en cuenta que Audit Manager no recopila pruebas de las AWS Config reglas vinculadas a servicios que crea Security Hub. Se trata de un tipo específico de AWS Config regla gestionada que el servicio Security Hub habilita y controla. Security Hub crea instancias de estas reglas vinculadas a servicios en su AWS entorno, incluso si ya existen otras instancias de las mismas reglas. Como resultado, para evitar la duplicación de pruebas, Audit Manager no admite la recopilación de pruebas a partir de las reglas vinculadas a los servicios.

He deshabilitado un control de seguridad en Security Hub ¿Audit Manager recopila evidencias de comprobación de conformidad para ese control de seguridad?

Audit Manager no recopila evidencias de los controles de seguridad deshabilitados.

Si establece el estado de un control de seguridad en Deshabilitado en Security Hub, no se realizará ninguna comprobación de seguridad para ese control en la cuenta ni en la región actuales. Como resultado, no hay resultados de seguridad disponibles en Security Hub, y Audit Manager no recopila ninguna evidencia relacionada.

Al respetar el estado de deshabilitado que estableció en Security Hub, Audit Manager se asegura de que su evaluación refleje con precisión los controles de seguridad activos y los resultados pertinentes para el entorno, excluyendo cualquier control que haya deshabilitado de forma intencionada.

He establecido el estado de un resultado en **`Suppressed`** en Security Hub ¿Audit Manager recopila evidencias de comprobación de conformidad sobre ese resultado?

Audit Manager recopila evidencias para los controles de seguridad que han suprimido los resultados.

Si ha establecido el estado del flujo de trabajo de un resultado en Suprimido en Security Hub, esto significa que ha revisado el resultado y no cree que sea necesario realizar ninguna acción. En Audit Manager, estos resultados suprimidos se recopilan como evidencias y se asocian a la evaluación. Los detalles de las evidencias muestran el estado de `SUPPRESSED` de la evaluación notificado directamente desde Security Hub.

Este método garantiza que la evaluación de Audit Manager represente con precisión los resultados de Security Hub y, al mismo tiempo, proporciona visibilidad de cualquier resultado suprimido que pueda requerir una revisión o consideración adicionales en una auditoría.

Mi evaluación no consiste en recopilar pruebas de control de cumplimiento de AWS Config

Si no ves las pruebas de verificación de conformidad de una AWS Config regla, podría deberse a uno de los siguientes problemas.

El identificador de la regla se ingresó incorrectamente en su **`ControlMappingSource`**

Cuando utiliza la API Audit Manager para crear un control personalizado, puede especificar una AWS Config regla como mapeo de fuentes de datos para la recopilación de pruebas. Lo `keywordValue`que especifique depende del tipo de regla.

Si no ve las pruebas de verificación de conformidad de una AWS Config regla, es posible que la `keywordValue` haya introducido incorrectamente en la suya`ControlMappingSource`. El `keywordValue` distingue entre mayúsculas y minúsculas. Si la introduce de forma incorrecta, es posible que Audit Manager no reconozca la regla. Como consecuencia, es posible que no recopile evidencia de verificación de cumplimiento para esa regla según lo previsto.

Para solucionar este problema, actualice el control personalizado y revise el `keywordValue`.

- En el caso de las reglas personalizadas, asegúrese de que `keywordValue` tenga el prefijo `Custom_` seguido del nombre de la regla personalizada. El formato del nombre de la regla

personalizada puede variar. Para mayor precisión, visite la AWS Config consola para comprobar los nombres de las reglas personalizadas.

- En el caso de las reglas administradas, asegúrese de que `keywordValue` es el identificador de la regla en `ALL_CAPS_WITH_UNDERSCORES`. Por ejemplo, `CLOUDWATCH_LOG_GROUP_ENCRYPTED`. Para mayor precisión, consulte la lista de palabras clave de reglas administradas compatibles.

> **Note**
>
> En el caso de algunas reglas administradas, el identificador de la regla es diferente del nombre de la regla. Por ejemplo, el identificador de regla para restricted-ssh es `INCOMING_SSH_DISABLED`. Asegúrese de usar el identificador de la regla, no el nombre de la regla. Para buscar un identificador de regla, elija una regla de la lista de reglas administradas y busque su valor de identificador.

La regla es una regla vinculada a un servicio AWS Config

Puede usar reglas administradas y reglas personalizadas como asignación de origen de datos para la recopilación de pruebas. Sin embargo, Audit Manager no recopila pruebas de la mayoría de las reglas vinculadas a los servicios.

Solo hay dos tipos de reglas vinculadas a servicios de las que Audit Manager recopila pruebas:

- Reglas vinculadas a servicios de los paquetes de conformidad
- Reglas vinculadas a servicios de AWS Organizations

Audit Manager no recopila pruebas de otras reglas vinculadas a servicios, específicamente de las reglas con un nombre de recurso de Amazon (ARN) que contenga el siguiente prefijo: `arn:aws:config:*:*:config-rule/aws-service-rule/...`

La razón por la que Audit Manager no recopila pruebas de la mayoría de AWS Config las reglas vinculadas a los servicios es para evitar la duplicación de pruebas en sus evaluaciones. Una regla vinculada a un servicio es un tipo específico de regla administrada que permite Servicios de AWS a otras personas crear AWS Config reglas en tu cuenta. Por ejemplo, algunos controles de Security Hub utilizan una regla AWS Config vinculada a un servicio para ejecutar comprobaciones de seguridad. Para cada control de Security Hub que utilice una AWS Config regla vinculada a un servicio, Security Hub crea una instancia de la AWS Config regla requerida en su AWS entorno. Esto sucede incluso si la regla original ya existe en la cuenta. Por lo tanto, para evitar recopilar la

misma evidencia de la misma regla dos veces, Audit Manager ignora la regla vinculada al servicio y no recopila evidencia a partir de ella.

AWS Config no está habilitado

AWS Config debe estar habilitado en su Cuenta de AWS. Una vez que se haya configurado de esta AWS Config manera, Audit Manager recopila pruebas cada vez que se realiza la evaluación de una AWS Config regla. Asegúrese de haber activado AWS Config en su Cuenta de AWS. Para obtener instrucciones, consulte Habilitar y configurar AWS Config.

La AWS Config regla evaluaba la configuración de un recurso antes de configurar la evaluación

Si la AWS Config regla está configurada para evaluar los cambios de configuración de un recurso específico, es posible que vea una discrepancia entre la evaluación AWS Config y la evidencia en Audit Manager. Esto ocurre si la evaluación de la regla se realizó antes de configurar el control en la evaluación de Audit Manager. En este caso, Audit Manager no genera pruebas hasta que el recurso subyacente vuelve a cambiar de estado y desencadena una reevaluación de la regla.

Como solución alternativa, puede navegar hasta la regla en la AWS Config consola y volver a evaluarla manualmente. Esto requiere una nueva evaluación de todos los recursos que pertenecen a esa regla.

Mi evaluación no consiste en recopilar pruebas de la actividad de los usuarios de AWS CloudTrail

Cuando utiliza la API Audit Manager para crear un control personalizado, puede especificar un nombre de CloudTrail evento como mapeo de fuentes de datos para la recopilación de pruebas. Para ello, introduzca el nombre del evento como `keywordValue`.

Si no ve ninguna evidencia de la actividad del usuario en relación con un CloudTrail evento, es posible que `keywordValue` se haya introducido incorrectamente en el suyo`ControlMappingSource`. El `keywordValue` distingue entre mayúsculas y minúsculas. Si la introduce de forma incorrecta, es posible que Audit Manager no reconozca el nombre del evento. Como resultado, es posible que no recopile las pruebas de la actividad del usuario en relación con ese evento según lo previsto.

Para solucionar este problema, actualice el control personalizado y revise el `keywordValue`. Asegúrese de que el evento esté escrito como `serviceprefix_ActionName`. Por ejemplo, `cloudtrail_StartLogging`. Para mayor precisión, revise el prefijo Servicio de AWS y los nombres de las acciones en la Referencia de autorización de servicio.

Mi evaluación no consiste en recopilar evidencia de datos de configuración para una llamada a la AWS API

Cuando utiliza la API Audit Manager para crear un control personalizado, puede especificar una llamada a la AWS API como mapeo de fuentes de datos para la recopilación de pruebas. Para ello, debe introducir la llamada a la API como `keywordValue`.

Si no ves evidencia de los datos de configuración de una llamada a la AWS API, es posible que la hayas `keywordValue` introducido incorrectamente en la tuya`ControlMappingSource`. El `keywordValue` distingue entre mayúsculas y minúsculas. Si lo introduce de forma incorrecta, es posible que Audit Manager no reconozca la llamada a la API. Como resultado, es posible que no recopile pruebas de datos de configuración para esa llamada a la API según lo previsto.

Para solucionar este problema, actualice el control personalizado y revise el `keywordValue`. Asegúrese de que la llamada a la API esté escrita como `serviceprefix_ActionName`. Por ejemplo, `iam_ListGroups`. Para mayor precisión, consulte la lista de AWS Las llamadas a la API son compatibles con AWS Audit Manager.

Un control común no está recopilando ninguna evidencia automatizada

Al revisar un control común, es posible que aparezca el siguiente mensaje: Este control común no recopila evidencias automatizadas de los controles principales.

Esto significa que actualmente ninguna fuente de evidencia AWS gestionada puede respaldar este control común. Como resultado, la pestaña Orígenes de evidencias está vacía y no se muestra ningún control principal.

Cuando un control común no recopila ninguna evidencia automatizada, se denomina control común manual. Los controles manuales habituales suelen requerir el suministro de registros y firmas físicas, o detalles sobre los eventos que se producen fuera de su AWS entorno. Por este motivo, a menudo no hay fuentes de AWS datos que puedan proporcionar pruebas que respalden los requisitos del control.

Si un control común es manual, puede seguir utilizándolo como origen de evidencias para un control personalizado. La única diferencia es que el control común no recopilará ninguna evidencia automáticamente. En cambio, tendrá que cargar manualmente sus propias evidencias para respaldar los requisitos del control común.

Adición de evidencias a un control común manual

1. Creación de un control personalizado
   - Siga los pasos para crear o editar un control personalizado.
   - Cuando especifique los orígenes de evidencias en el paso 2, elija el control común manual como origen de evidencia.
2. Creación de un marco personalizado
   - Siga los pasos para crear o editar un marco personalizado.
   - Cuando especifique un conjunto de controles en el paso 2, incluya el nuevo control personalizado.
3. Creación de una evaluación
   - Siga los pasos para crear una evaluación a partir de un marco personalizado.
   - En este momento, el control común manual es ahora un origen de evidencia en un control de evaluación activo.
4. Carga de evidencias manuales
   - Siga los pasos para añadir evidencias manuales al control de la evaluación.

> **Note**
>
> A medida que haya más fuentes de AWS datos disponibles en el futuro, es AWS posible que se actualice el control común para incluir los controles básicos como fuentes de evidencia. En este caso, si el control común es un origen de evidencia en uno varios de los controles de evaluación activos, se beneficiará de estas actualizaciones automáticamente. No necesitará ninguna otra configuración por su parte y empezará a recopilar evidencias automatizadas que respalden el control común.

Mis pruebas se generan a intervalos diferentes y no estoy seguro de la frecuencia con la que se recopilan

Los controles de las evaluaciones de Audit Manager se asignan a varios orígenes de datos. Cada origen de datos tiene una frecuencia de recopilación de evidencias diferente. Como resultado, no hay one-size-fits-all respuesta sobre la frecuencia con la que se recopilan las pruebas. Algunas fuentes

de datos evalúan el cumplimiento, mientras que otras solo recopilan el estado de los recursos y modifican los datos sin determinar el cumplimiento.

El siguiente es un resumen de los distintos tipos orígenes de datos y de la frecuencia con la que recopilan pruebas.

Data source type	Descripción	Frecuencia de recolección de evidencia	Cuando este control está activo en una evaluación
AWS CloudTrail	Realiza un seguimiento de la actividad de un usuario específico.	Continuo	Audit Manager filtra los CloudTrail registros en función de la palabra clave que elija. Los registros procesados se importan como evidencia de la Actividad del usuario.
AWS Security Hub	Captura una instantánea del estado de seguridad de sus recursos mediante el informe de los resultados de Security Hub.	Según la programación de la comprobación del Security Hub (normalmente cada 12 horas)	Audit Manager recupera los resultados de seguridad directamente desde Security Hub. El resultado se importa como evidencia de Control de conformidad.
AWS Config	Captura una instantánea del estado de seguridad de sus recursos al informar sobre los resultados obtenidos AWS Config.	En función de la configuración definida en la AWS Config regla	Audit Manager recupera la evaluación de la regla directamente de AWS Config. La evaluación se importa como evidencia de Control de conformidad.

Data source type	Descripción	Frecuencia de recolección de evidencia	Cuando este control está activo en una evaluación
AWS Llamadas a la API	Toma una instantánea de la configuración de los recursos directamente mediante una llamada a la API especificada Servicio de AWS.	Diariamente, semanalmente o mensualmente	Audit Manager realiza la llamada a la API en función de la frecuencia que especifique. La respuesta se importa como evidencia de Datos de configuración.

Independientemente de la frecuencia de recopilación de evidencias, las nuevas evidencias se recopilan automáticamente mientras la evaluación esté activa. Para obtener más información, consulte Frecuencia de recolección de evidencias.

Para obtener más información, consulte Tipos de orígenes de datos compatibles para evidencias automatizadas y Cambio de la frecuencia con la que un control recopila evidencias.

He desactivado Audit Manager y, a continuación, he vuelto a activarlo, y ahora mis evaluaciones preexistentes ya no recopilan pruebas

Cuando desactiva Audit Manager y decide no eliminar sus datos, las evaluaciones existentes pasan a un estado latente y dejan de recopilar pruebas. Esto significa que cuando vuelva a activar Audit Manager, las evaluaciones que creó anteriormente permanecerán disponibles. Sin embargo, no reanudan automáticamente la recopilación de pruebas.

Para volver a recopilar evidencias para una evaluación preexistente, edite la evaluación y seleccione Guardar sin realizar ningún cambio.

En la página de detalles de la evaluación se me pide que vuelva a crearla

Si aparece un mensaje en el que se indica Crear nueva evaluación para recopilar evidencias más completas, esto indica que Audit Manager ahora proporciona una nueva definición del marco estándar a partir del cual se creó la evaluación.

En la nueva definición del marco, todos los controles estándar del marco ahora pueden recopilar evidencias de orígenes administrados por AWS. Esto significa que cada vez que hay una actualización de los orígenes de datos subyacentes para un control común o principal, Audit Manager aplicará automáticamente la misma actualización a todos los controles estándar relacionados.

Para aprovechar estas fuentes AWS gestionadas, le recomendamos que cree una nueva evaluación a partir del marco actualizado. Una vez realizado este paso, puede cambiar el estado de la evaluación anterior a Inactivo. Esta acción ayuda a garantizar que su nueva evaluación recopile la evidencia más precisa y completa disponible de fuentes AWS gestionadas. Si no realiza ninguna acción, la evaluación seguirá utilizando el marco y las definiciones de control anteriores para recopilar evidencias de la misma forma que antes.

¿Cuál es la diferencia entre un origen de datos y un origen de evidencias?

Un origen de evidencias determina de dónde se recopilan las evidencias. Puede ser un origen de datos individual o una agrupación predefinida de orígenes de datos que se asigna a un control principal o a un control común.

Un origen de datos es el tipo de origen de evidencia más detallado. Un origen de datos incluye los siguientes detalles que indican a Audit Manager de dónde exactamente debe recopilar los datos de evidencia:

- Tipo de fuente de datos (por ejemplo, AWS Config)

- Mapeo de fuentes de datos (por ejemplo, una AWS Config regla específica, como`s3-bucket-public-write-prohibited`)

Error al crear mi evaluación

Si se produce un error al crear la evaluación, podría deberse a uno de los siguientes problemas.

Ha seleccionado demasiadas Cuentas de AWS en el ámbito de su evaluación

Si lo utiliza AWS Organizations, Audit Manager puede admitir hasta 200 cuentas de miembros en el ámbito de una sola evaluación. Si supera este número, no se podrá crear la evaluación.

Como solución alternativa, puede ejecutar varias evaluaciones con diferentes cuentas para cada evaluación, hasta 250 cuentas de miembros únicas en todas las evaluaciones.

Una cuenta incluida en su ámbito ya está siendo evaluada por otra evaluación activa

Si intenta crear una evaluación que incluya una cuenta que ya esté dentro del ámbito de aplicación de otra evaluación activa, no se podrá crear la evaluación. Esto puede suceder cuando varios equipos u organizaciones intentan evaluar la misma cuenta simultáneamente.

Es posible que veas un mensaje de error similar a:`Scope: AWS Account [account-id] has assessments in progress`.

Para resolver este problema, puede realizar una de las siguientes acciones:

- Coordínese con otros equipos: póngase en contacto con otros equipos de su organización para determinar qué evaluaciones utilizan actualmente la cuenta en cuestión. A continuación, podrá coordinarse para evitar la superposición de los alcances de las evaluaciones.
- Modifique el alcance de la evaluación: elimine la cuenta conflictiva del ámbito de la evaluación y cree la evaluación con las cuentas restantes. Puede evaluar la cuenta conflictiva por separado una vez que se haya completado la otra evaluación.
- Espere a que se complete la otra evaluación: si la otra evaluación es temporal o está a punto de completarse, puede esperar a que finalice antes de crear la evaluación con el alcance deseado.

> **Note**
>
> Esta restricción ayuda a garantizar que la recopilación de pruebas no entre varias evaluaciones y que los resultados de la auditoría sigan siendo precisos y coherentes.

¿Qué ocurre si elimino una cuenta incluida en el ámbito de aplicación de mi organización?

Cuando se elimina una cuenta incluida en el ámbito de su organización, Audit Manager deja de recopilar pruebas de esa cuenta y se eliminará de todas las evaluaciones en las que la cuenta esté incluida en el ámbito de aplicación. Eliminar la cuenta de un miembro de todas las evaluaciones también reducirá el número total de cuentas únicas incluidas en el ámbito de aplicación, lo que le permitirá añadir una cuenta nueva de su organización.

No puedo ver los servicios incluidos en el ámbito de la evaluación

Si no se muestra la pestaña Servicios de AWS, esto significa que Audit Manager administra los servicios incluidos. Al crear una nueva evaluación, Audit Manager administrará los servicios incluidos a partir de ese momento.

Si tiene una evaluación anterior, es posible que haya visto esta pestaña anteriormente en la evaluación. Sin embargo, Audit Manager elimina automáticamente esta pestaña de la evaluación y se hace cargo de la administración de los servicios incluidos cuando se produce alguno de los siguientes eventos:

- Edita la evaluación
- Edita uno de los controles personalizados que se utilizan en la evaluación

Audit Manager deduce los servicios incluidos examinando los controles de evaluación y sus orígenes de datos y asignando esta información a los Servicios de AWS correspondientes. Si un origen de datos subyacente cambia para la evaluación, actualizaremos automáticamente el ámbito según sea necesario para reflejar los servicios correctos. Esto garantiza que su evaluación recopile pruebas precisas y completas sobre todos los servicios relevantes de su AWS entorno.

No puedo editar los servicios incluidos en el ámbito de mi evaluación

El flujo de trabajo de Edición de una evaluación en AWS Audit Manager ya no incluye el paso Editar servicios. Esto se debe a que Audit Manager ahora gestiona cuáles Servicios de AWS están dentro del ámbito de su evaluación.

Si tiene una evaluación anterior, es posible que haya definido manualmente los servicios incluidos al crearla. Sin embargo, no puede editar estos servicios en el futuro. Audit Manager se hace cargo

automáticamente de la administración de los servicios incluidos cuando se produce alguno de los siguientes eventos:

- Edita la evaluación
- Edita uno de los controles personalizados que se utilizan en la evaluación

Audit Manager deduce los servicios incluidos examinando los controles de evaluación y sus orígenes de datos y asignando esta información a los Servicios de AWS correspondientes. Si un origen de datos subyacente cambia para la evaluación, actualizaremos automáticamente el ámbito según sea necesario para reflejar los servicios correctos. Esto garantiza que su evaluación recopile pruebas precisas y completas sobre todos los servicios relevantes de su AWS entorno.

¿Cuál es la diferencia entre un servicio incluido y un tipo de origen de datos?

Un service in scope es un Servicio de AWS que se incluye en la evaluación. Cuando un servicio está incluido, Audit Manager recopila evidencia sobre el uso que usted hace de ese servicio y sus recursos.

> **Note**
>
> Audit Manager gestiona cuáles Servicios de AWS están dentro del alcance de sus evaluaciones. Si tiene una evaluación anterior, es posible que haya especificado manualmente los servicios incluidos en el pasado. De ahora en adelante, no podrá especificar ni editar los servicios incluidos.

Un tipo de origen de datos indica de dónde se recopilan exactamente las pruebas. Si carga sus propias evidencias, el tipo de origen de datos es Manual. Si Audit Manager recopila evidencias, el origen de datos puede ser de cuatro tipos.

1. AWS Security Hub — Captura una instantánea del estado de seguridad de sus recursos mediante el informe de los hallazgos de Security Hub.
2. AWS Config — Captura una instantánea del estado de seguridad de sus recursos mediante un informe de los resultados obtenidos AWS Config.
3. AWS CloudTrail — Realiza un seguimiento de la actividad de un usuario específico en relación con un recurso.

4. AWS Llamadas a la API: toma una instantánea de la configuración de los recursos directamente a través de una llamada a la API a una persona específica Servicio de AWS.

Estos son dos ejemplos para ilustrar la diferencia entre el alcance de un servicio y el tipo de origen de datos.

Ejemplo 1

Supongamos que desea recopilar pruebas para un control denominado 4.1.2: no permitir el acceso de escritura pública a los buckets de S3. Este control comprueba los niveles de acceso de sus políticas de bucket de S3. Para este control, Audit Manager utiliza una AWS Config regla específica (s3- bucket-public-write-prohibited) para buscar una evaluación de sus buckets de S3. Esto se muestra en el siguiente ejemplo:

- El service in scope es Amazon S3
- Los recursos que se están evaluando son sus buckets de S3
- El tipo de fuente de datos es AWS Config
- El mapeo de la fuente de datos es una AWS Config regla específica (`s3-bucket-public-write-prohibited`)

Ejemplo 2

Supongamos que desea recopilar pruebas para un control de la HIPAA denominado 164.308(a)(5)(ii)(C). Este control requiere un procedimiento de supervisión para detectar inicios de sesión inadecuados. Para este control, Audit Manager utiliza CloudTrail los registros para buscar todos los eventos de inicio de sesión AWS de Management Console. Esto se muestra en el siguiente ejemplo:

- El service in scope es IAM
- Los recursos que se están evaluando son sus usuarios
- El tipo de fuente de datos es CloudTrail
- El mapeo de la fuente de datos es un CloudTrail evento específico (`ConsoleLogin`)

Solución de problemas con el informe de evaluación

Puede utilizar la información de esta página para resolver problemas comunes de los informes de evaluación en Audit Manager.

Temas

- No se pudo generar mi informe de evaluación
- He seguido la lista de verificación anterior y mi informe de evaluación sigue sin generarse
- Cuando intento generar un informe, aparece un error de acceso denegado
- No puedo abrir el informe de evaluación
- Cuando elijo el nombre de una prueba en un informe, no se me redirige a los detalles de la evidencia
- La generación de mi informe de evaluación está bloqueada en el estado En curso y no estoy seguro de cómo afecta esto a mi facturación
- Recursos adicionales

No se pudo generar mi informe de evaluación

Es posible que el informe de evaluación no se haya generado por varias razones. Puede empezar a solucionar este problema comprobando las causas más frecuentes. Use la siguiente lista de verificación para empezar.

1. Compruebe si alguno de sus Región de AWS datos no coincide:
   a. ¿La Región de AWS clave gestionada por el cliente coincide con la Región de AWS de su evaluación?

      Si proporcionó su propia clave KMS para el cifrado de datos de Audit Manager, la clave debe coincidir Región de AWS con la de su evaluación. Para resolver este problema, cambie la clave KMS por una que esté en la misma Región que la evaluación. Para obtener instrucciones sobre cómo cambiar la clave de KMS, consulte Configuración de los ajustes del cifrado de datos.

   b. ¿La Región de AWS clave administrada por el cliente coincide con la Región de AWS de su bucket de S3?

      Si proporcionó su propia clave KMS para el cifrado de datos de Audit Manager, la clave debe estar en el mismo Región de AWS lugar que el depósito de S3 que utiliza como destino del informe de evaluación. Para resolver este problema, puede cambiar la clave KMS o el bucket de S3 para que ambos estén en la misma región que la evaluación. Para obtener instrucciones sobre cómo cambiar la clave de KMS, consulte Configuración de los ajustes del cifrado de datos. Para obtener instrucciones sobre cómo cambiar el bucket de S3, consulte Configuración del destino del informe de evaluación predeterminado.

2. Compruebe los permisos del bucket de S3 que está utilizando como destino del informe de evaluación:

   a. ¿La entidad de IAM que genera el informe de evaluación tiene los permisos necesarios para el bucket de S3?

      La entidad de IAM debe tener los permisos del bucket de S3 necesarios para publicar los informes en ese bucket. Proporcionamos un ejemplo de política que puede utilizar.

   b. ¿El bucket de S3 tiene una política de bucket que requiera el cifrado del servidor (SSE) mediante SSE-KMS?

      En caso afirmativo, la clave de KMS que se utiliza en esa política de bucket debe coincidir con la clave de KMS que se especifica en la configuración de cifrado de datos de Audit Manager. Si no configuró una clave KMS en la configuración de Audit Manager y su política de bucket de S3 requiere SSE, asegúrese de que la política de bucket permita SSE-S3. Para obtener instrucciones sobre cómo cambiar la clave de KMS, consulte Configuración de los ajustes del cifrado de datos. Para obtener instrucciones sobre cómo cambiar el bucket de S3, consulte Configuración del destino del informe de evaluación predeterminado.

Si sigue sin poder generar correctamente un informe de evaluación, revise los siguientes problemas en esta página.

He seguido la lista de verificación anterior y mi informe de evaluación sigue sin generarse

Audit Manager limita la cantidad de evidencia que se puede añadir a un informe de evaluación. El límite se basa en la Región de AWS evaluación, en la región del depósito de S3 que se utiliza como destino del informe de evaluación y en si la evaluación utiliza un sistema gestionado por el cliente AWS KMS key.

1. El límite es de 22.000 para los informes de la misma región (en los que el bucket de S3 y la evaluación están en la misma Región de AWS)
2. El límite es de 3500 para los informes de la misma región (en los que el bucket de S3 y la evaluación están en la misma Regiones de AWS)
3. El límite es de 3500 si la evaluación utiliza una clave KMS administrada por el cliente

Si intenta generar un informe que contenga más pruebas que estas, la operación podría fallar.

Como solución alternativa, puede generar varios informes de evaluación en lugar de un informe de evaluación más grande. De este modo, puede exportar las pruebas de su evaluación a lotes de un tamaño más manejable.

Cuando intento generar un informe, aparece un error de acceso denegado

Aparecerá un error `access denied` si la evaluación la creó una cuenta de administrador delegado a la que no pertenece la clave KMS especificada en la configuración de Audit Manager. Para evitar este error, cuando designe un administrador delegado para Audit Manager, asegúrese de que la cuenta de administrador delegado tenga acceso a la clave KMS que proporcionó al configurar Audit Manager.

También puede recibir un error `access denied` si no tiene permisos de escritura para el bucket de S3 que utiliza como destino del informe de evaluación.

Si aparece un error `access denied`, asegúrese de cumplir los siguientes requisitos:

- La clave KMS en la configuración de Audit Manager otorga permisos al administrador delegado. Para configurarlo, siga las instrucciones de la AWS Key Management Service Guía para desarrolladores sobre cómo permitir que los usuarios de otras cuentas usen una clave KMS. Para obtener instrucciones sobre cómo revisar y cambiar la configuración del cifrado en Audit Manager, consulte Configuración de los ajustes del cifrado de datos.
- Tiene una política de permisos que le otorga acceso de escritura al bucket de S3 que utiliza como destino del informe de evaluación. Más específicamente, su política de permisos contiene una acción `s3:PutObject`, especifica el ARN del bucket de S3 e incluye la clave KMS que se utiliza para cifrar los informes de evaluación. Para ver un ejemplo de política que puede usar, consulte Ejemplo 2 (permisos de destino del informe de evaluación).

> **Note**
>
> Al cambiar la configuración de cifrado de datos de Audit Manager, estos cambios se aplican a cualquier evaluación nueva que cree. Esto incluye todos los informes de evaluación que cree a partir de sus nuevas evaluaciones.
> Los cambios no se aplican a las evaluaciones existentes que creó antes de cambiar la configuración del cifrado. Esto incluye los nuevos informes de evaluación que se crean a partir de las evaluaciones existentes, además de los informes de evaluación existentes. Las evaluaciones existentes (y todos sus informes de evaluación) siguen utilizando la antigua

clave KMS. Si la identidad de IAM que genera el informe de evaluación no tiene permisos para usar la antigua clave de KMS, puede conceder permisos a nivel de política clave.

No puedo abrir el informe de evaluación

Si no puede descomprimir el informe de evaluación en Windows, es probable que el Explorador de Windows no pueda extraerlo porque la ruta del archivo tiene varias carpetas anidadas o nombres largos. Esto se debe a que, según el sistema de nombres de archivos de Windows, la ruta de la carpeta, el nombre y la extensión del archivo no pueden superar los 259 caracteres. De lo contrario, se produce un error `Destination Path Too Long`.

Para resolver este problema, intente mover el archivo zip a la carpeta principal de su ubicación actual. A continuación, puede volver a intentar descomprimirlo desde allí. Como alternativa, también puede intentar acortar el nombre del archivo zip o extraerlo a una ubicación diferente que tenga una ruta de archivo más corta.

Cuando elijo el nombre de una prueba en un informe, no se me redirige a los detalles de la evidencia

Este problema puede producirse si está interactuando con el informe de evaluación en un navegador o si utiliza el lector de PDF predeterminado que viene instalado en su sistema operativo. Algunos lectores de PDF predeterminados del navegador y del sistema no permiten abrir los enlaces correspondientes. Esto significa que, si bien los hipervínculos pueden funcionar dentro del PDF con el resumen del informe de evaluación (como los nombres de los controles con hipervínculos en el índice), los hipervínculos se ignoran cuando se intenta pasar del PDF con el resumen de la evaluación a otro PDF con detalles probatorios.

Si se produce este problema, le recomendamos que utilice un lector de PDF específico para interactuar con los informes de evaluación. Para disfrutar de una experiencia fiable, le recomendamos que instale y utilice Adobe Acrobat Reader, que puede descargar en el sitio web de Adobe. También hay otros lectores de PDF disponibles, pero se ha demostrado que Adobe Acrobat Reader funciona de forma coherente y fiable con los informes de evaluación de Audit Manager.

La generación de mi informe de evaluación está bloqueada en el estado En curso y no estoy seguro de cómo afecta esto a mi facturación

La generación de los informes de evaluación no afecta a la facturación. Solo se le facturará en función de la evidencia que recopilen sus evaluaciones. Para obtener más información sobre los precios, consulte Precios de AWS Audit Manager.

Recursos adicionales

Las siguientes páginas contienen una guía de solución de problemas sobre la generación de un informe de evaluación a partir del buscador de evidencias:

- No puedo generar varios informes de evaluación a partir de los resultados de mi búsqueda
- No puedo incluir pruebas específicas de los resultados de mi búsqueda
- No todos los resultados de mi buscador de evidencias se incluyen en el informe de evaluación
- Quiero generar un informe de evaluación a partir de los resultados de mi búsqueda, pero el enunciado de mi consulta no funciona

Solución de problemas de control y conjunto de control

Puede utilizar la información de esta página para resolver problemas comunes con los controles de Audit Manager.

Problemas generales

- No veo ningún control o conjunto de controles en mi evaluación
- No puedo subir pruebas manuales a un control
- ¿Qué significa si en un control se indica Reemplazo disponible?

Problema de integración de AWS Config

- Necesito usar varias AWS Config reglas como fuente de datos para un solo control
- La opción de regla personalizada no está disponible cuando configuro un origen de datos de control
- La opción de regla personalizada está disponible, pero no aparece ninguna regla en la lista desplegable

- Hay algunas reglas personalizadas disponibles, pero no puedo ver la regla que quiero usar
- No veo la regla administrada que quiero usar
- Quiero compartir un marco personalizado, pero tiene controles que utilizan AWS Config reglas personalizadas como fuente de datos. ¿Puede el destinatario recopilar pruebas para estos controles?
- ¿Qué ocurre cuando se actualiza una regla personalizada en AWS Config? ¿Tengo que tomar alguna medida en Audit Manager?

No veo ningún control o conjunto de controles en mi evaluación

En resumen, para ver los controles de una evaluación, debe especificarse como propietario de la auditoría de esa evaluación. Además, necesita los permisos de IAM necesarios para ver y gestionar los recursos de Audit Manager relacionados.

Si necesita acceder a los controles de una evaluación, pida a uno de los propietarios de la auditoría de esa evaluación que lo especifique como propietario de la auditoría. Puede especificar los propietarios de la auditoría al crear o editar una evaluación.

Asegúrese también de que el usuario cuente con los permisos necesarios para administrar la evaluación. Recomendamos que los propietarios de la auditoría utilicen la AWSAuditManagerAdministratorAccesspolítica. Si necesita ayuda con los permisos de IAM, póngase en contacto con su administrador o con AWS Soporte. Para obtener información sobre cómo añadir una política de IAM a un usuario, consulte Adición de permisos a un usuario y Adición y eliminación de permisos de identidad de IAM en la Guía del usuario de IAM.

No puedo subir pruebas manuales a un control

Si no puede cargar pruebas manualmente en un control, es probable que se deba a que el control está inactivo.

Para cargar pruebas manuales en un control, primero debe cambiar el estado del control a En revisión o Revisado. Para obtener instrucciones, consulte Cambiar el estado de un control de evaluación en AWS Audit Manager.

> **Important**
>
> Cada uno de ellos solo Cuenta de AWS puede cargar manualmente hasta 100 archivos de pruebas a un control cada día. Si supera este límite diario no podrá realizar ninguna

carga manual adicional en ese control. Si necesita cargar una gran cantidad de evidencias manuales en un solo control, hágalo en lotes durante varios días.

¿Qué significa si en un control se indica Reemplazo disponible?

Si aparece este mensaje, esto significa que hay disponible una definición de control actualizada para uno o varios de los controles estándar del marco personalizado. Le recomendamos que sustituya estos controles para poder sacar partido de los orígenes de evidencias mejorados que ahora proporciona Audit Manager.

Para obtener instrucciones sobre cómo proceder, consulte En la página de detalles del marco personalizado se me pide que vuelva a crear el marco personalizado.

Necesito usar varias AWS Config reglas como fuente de datos para un solo control

Puede usar una combinación de reglas administradas y reglas personalizadas para un solo control. Para ello, defina varios orígenes de datos para el control y seleccione el tipo de regla que prefiera para cada uno de ellos. Puede definir hasta 100 orígenes de datos administrados por el cliente para un único control personalizado.

La opción de regla personalizada no está disponible cuando configuro un origen de datos de control

Por lo tanto, usted no tiene permisos para ver las reglas personalizadas de su Cuenta de AWS o organización. Más específicamente, no tiene permisos para realizar la DescribeConfigRulesoperación en la consola de Audit Manager.

Para resolver este problema, póngase en contacto con el AWS administrador para obtener ayuda. Si es AWS administrador, puede proporcionar permisos a sus usuarios o grupos gestionando sus políticas de IAM.

La opción de regla personalizada está disponible, pero no aparece ninguna regla en la lista desplegable

Esto significa que no hay reglas personalizadas habilitadas ni disponibles para su uso en su Cuenta de AWS u organización.

Si aún no tienes ninguna regla personalizada AWS Config, puedes crear una. Para obtener instrucciones, consulte AWS Config reglas personalizadas en Guía de desarrolladores de AWS Config .

Si espera ver una regla personalizada, consulte el siguiente elemento de solución de problemas.

Hay algunas reglas personalizadas disponibles, pero no puedo ver la regla que quiero usar

Si no ve la regla personalizada que esperas encontrar, puede deberse a uno de los siguientes problemas.

Su cuenta está excluida de la regla

Es posible que la cuenta de administrador delegado que está utilizando esté excluida de la regla.

La cuenta de administración de tu organización (o una de las cuentas de administrador AWS Config delegado) puede crear reglas organizativas personalizadas mediante AWS Command Line Interface (AWS CLI). Cuando lo hacen, pueden especificar una lista de cuentas que se van a excluir de la regla. Si su cuenta está en esta lista, la regla no está disponible en Audit Manager.

Para resolver este problema, ponte en contacto con el AWS Config administrador para obtener ayuda. Si es AWS Config administrador, puede actualizar la lista de cuentas excluidas ejecutando el put-organization-config-rulecomando.

La regla no se creó y activó correctamente en AWS Config

También es posible que la regla personalizada no se haya creado y activado correctamente. Si se ha producido un error al crear la regla, o la regla no está habilitada, no aparecerá en la lista de reglas disponibles en Audit Manager.

Para obtener ayuda con este problema, le recomendamos que se ponga en contacto con su AWS Config administrador.

La regla es una regla administrada

Si no encuentra la regla que busca en la lista desplegable de reglas personalizadas, es posible que se trate de una regla administrada.

Puede usar la AWS Config consola para comprobar si una regla es una regla administrada. Para ello, elija Reglas en el menú de navegación de la izquierda y busque la regla en la tabla. Si la regla es una regla administrada, la columna Tipo muestra la regla AWS administrada.

Una vez que haya confirmado que se trata de una regla administrada, vuelva a Audit Manager y seleccione Regla administrada como tipo de regla. A continuación, busque la palabra clave identificadora de la regla administrada en la lista desplegable de reglas administradas.

No veo la regla administrada que quiero usar

Antes de seleccionar una regla de la lista desplegable de la consola de Audit Manager, asegúrese de haber seleccionado Regla administrada como tipo de regla.

Si sigue sin ver la regla administrada que espera encontrar, es posible que esté buscando el nombre de la regla. En su lugar, debe buscar el identificador de la regla.

Si utiliza una regla administrada por defecto, el nombre y el identificador son similares. El nombre está en minúsculas y usa guiones (por ejemplo, `iam-policy-in-use`). El identificador está en mayúsculas y utiliza guiones bajos (por ejemplo, `IAM_POLICY_IN_USE`). Para encontrar el identificador de una regla administrada predeterminada, revise la lista de palabras clave de reglas AWS Config administradas compatibles y siga el enlace de la regla que desee usar. Esto le llevará a la AWS Config documentación de esa regla administrada. Desde aquí, puede ver tanto el nombre como el identificador. Busque la palabra clave del identificador en la lista desplegable de Audit Manager.

Si utiliza una regla administrada personalizada, puede usar la consola de AWS Config para buscar el identificador de la regla. Por ejemplo, supongamos que desea utilizar la regla administrada llamada

`customized-iam-policy-in-use`. Para encontrar el identificador de esta regla, vaya a la AWS Config consola, elija Reglas en el menú de navegación de la izquierda y elija la regla en la tabla.

Elija Editar para abrir los detalles sobre la regla administrada.

En la sección Detalles, puede encontrar el identificador de origen a partir del cual se creó la regla administrada (`IAM_POLICY_IN_USE`).

Ahora puede volver a la consola de Audit Manager y seleccionar la misma palabra clave identificadora en la lista desplegable.

Quiero compartir un marco personalizado, pero tiene controles que utilizan AWS Config reglas personalizadas como fuente de datos. ¿Puede el destinatario recopilar pruebas para estos controles?

Sí, el destinatario puede recopilar pruebas para estos controles, pero se necesitan algunos pasos para lograrlo.

Para que Audit Manager recopile pruebas utilizando una AWS Config regla como mapeo de fuentes de datos, debe cumplirse lo siguiente. Esto es cierto para las reglas administradas y las reglas personalizadas.

1. La regla debe existir en el AWS entorno del destinatario
2. La regla debe estar habilitada en el AWS entorno del destinatario

Recuerde que es probable que AWS Config las reglas personalizadas de su cuenta aún no existan en el AWS entorno del destinatario. Además, cuando el destinatario acepta la solicitud de compartición, Audit Manager no vuelve a crear ninguna de sus reglas personalizadas en su cuenta. Para que el destinatario pueda recopilar pruebas utilizando sus reglas personalizadas como mapeo de fuentes de datos, debe crear las mismas reglas personalizadas en su instancia de AWS Config. Una vez que el destinatario crea y, a continuación, activa las reglas, Audit Manager puede recopilar pruebas de ese origen de datos.

Le recomendamos que se comunique con el destinatario para informarle si es necesario crear alguna regla personalizada en su instancia de AWS Config.

¿Qué ocurre cuando se actualiza una regla personalizada en AWS Config? ¿Tengo que tomar alguna medida en Audit Manager?

Para actualizaciones de reglas en su AWS entorno

Si actualiza una regla personalizada en su AWS entorno, no es necesario realizar ninguna acción en Audit Manager. Audit Manager detecta y gestiona las actualizaciones de reglas como se describe en la tabla siguiente. Audit Manager no le notifica cuando se detecta una actualización de reglas.

Escenario	¿Qué hace Audit Manager?	Qué necesita
Se actualiza una regla personalizada en su instancia de AWS Config	Audit Manager sigue informando de las conclusiones de esa regla mediante la definición de regla actualizada.	No es necesario ninguna acción.
Se elimina una regla personalizada en su instancia de AWS Config	Audit Manager deja de informar de los resultados de la regla eliminada.	No es necesario ninguna acción. Si lo desea, puede editar los controles personalizados que utilizaban la regla eliminada

Escenario	¿Qué hace Audit Manager?	Qué necesita
		como asignación de origen de datos. Esto ayuda a limpiar la configuración de la origen de datos al eliminar la regla eliminada. De lo contrario , el nombre de la regla eliminada permanece como una asignación de origen de datos no utilizada.

Para actualizaciones de reglas fuera de su AWS entorno

Si se actualiza una regla personalizada fuera de su AWS entorno, Audit Manager no detectará la actualización de la regla. Esto es algo que debe tener en cuenta si utiliza marcos personalizados compartidos. Esto se debe a que, en este escenario, el remitente y el destinatario trabajan cada uno en AWS entornos separados. En la tabla siguiente se indican las acciones recomendadas para este escenario.

Su función	Escenario	Acción recomendada
Remite	• Compartió un marco que utiliza reglas personalizadas como asignación de origen de datos. • Después de compartir el marco, actualizó o eliminó una de esas reglas en AWS Config.	Informe al destinatario acerca de su actualización. De esta forma, pueden aplicar la misma actualización y mantenerse sincronizados con la definición de regla más reciente.
Recipie	• Ha aceptado un marco compartido que utiliza reglas personalizadas como asignación de origen de datos. • Tras volver a crear las reglas personalizadas en la instancia de AWS Config, el remitente actualizó o eliminó una de esas reglas.	Actualice la regla correspondiente en su propia instancia de AWS Config.

Solución de problemas de panel

Puede utilizar la información de esta página para resolver problemas comunes del panel de control en Audit Manager.

Temas

- No hay ningún dato en mi panel
- La opción de descarga en formato CSV no está disponible
- No veo el archivo descargado cuando intento descargar un archivo CSV
- Falta un control o dominio de control específico en el panel de control
- Veo controles similares o duplicados que aparecen en el mismo dominio de control
- La instantánea diaria muestra cantidades variables de evidencia cada día. ¿Es esto normal?

No hay ningún dato en mi panel

Si los números del widget de Instantánea diaria muestran un guión (-), esto indica que no hay datos disponibles. Debe tener al menos una evaluación activa para ver los datos en el panel de control. Para empezar, cree una evaluación. Tras un periodo de 24 horas, los datos de la evaluación comenzarán a aparecer en el panel de control.

> **Note**
>
> Si los números del widget de instantáneas diarias muestran un cero (0), esto indica que las evaluaciones activas (o la evaluación seleccionada) no contienen pruebas que no cumplan con los requisitos.

La opción de descarga en formato CSV no está disponible

Esta opción solo está disponible para evaluaciones individuales. Asegúrese de haber aplicado una Filtro de evaluación al panel de control e inténtelo de nuevo. Recuerde que solo puede descargar un archivo CSV a la vez.

No veo el archivo descargado cuando intento descargar un archivo CSV

Si un dominio de control contiene una gran cantidad de controles, es posible que se produzca un breve retraso mientras Audit Manager genera el archivo CSV. Una vez generado el archivo, se descarga automáticamente.

Si sigue sin ver el archivo descargado, asegúrese de que la conexión a Internet funciona correctamente y de que utiliza la versión más reciente del navegador web. Además, compruebe su carpeta de descargas recientes. Los archivos se descargan en la ubicación predeterminada que determine el navegador. Si esto no resuelve el problema, intente descargar el archivo con otro navegador.

Falta un control o dominio de control específico en el panel de control

Es probable que esto signifique que sus evaluaciones activas (o una evaluación específica) no contienen datos relevantes para ese control o dominio de control.

Un dominio de control se muestra en el panel de control solo si se cumplen los dos criterios siguientes:

- Las evaluaciones activas (o la evaluación específica) contienen al menos un control relacionado con ese dominio
- Al menos un control de ese dominio recopiló pruebas en la fecha que aparece en la parte superior del panel

Un control se muestra dentro de un dominio solo si recopiló pruebas en la fecha que aparece en la parte superior del panel.

Veo controles similares o duplicados que aparecen en el mismo dominio de control

Este problema puede producirse si las evaluaciones recopilan evidencias de diferentes versiones del mismo control estándar.

Esto ocurre en las siguientes situaciones:

Situación 1: tiene dos evaluaciones creadas a partir del mismo marco estándar

- Ha creado una evaluación a partir de un marco estándar antes del lanzamiento de la biblioteca de controles comunes.

Esta evaluación recopila evidencias mediante controles estándar obsoletos.

- También ha creado una evaluación a partir del mismo marco estándar después del lanzamiento de la biblioteca de controles comunes.

  Esta evaluación recopila evidencias mediante las nuevas versiones de los controles estándar.
- Como resultado, las evaluaciones recopilan evidencias de diferentes versiones de los mismos controles estándar.

Situación 2: tiene dos evaluaciones creadas a partir de un marco personalizado que utiliza controles estándar

- Ha creado una evaluación a partir de un marco personalizado antes del lanzamiento de la biblioteca de controles comunes.

  Esta evaluación recopila evidencias mediante controles estándar obsoletos.
- También ha creado una evaluación a partir del mismo marco personalizado después del lanzamiento de la biblioteca de controles comunes.

  Esta evaluación recopila evidencias mediante las nuevas versiones de los controles estándar.
- Como resultado, las evaluaciones recopilan evidencias de diferentes versiones de los mismos controles estándar.

Ejemplo: supongamos que tiene una evaluación preexistente que creó a partir del marco estándar PCI DSS antes del 6 de junio de 2024. Además, creó una nueva evaluación a partir del marco estándar después del 6 de junio de 2024. Como resultado, la primera evaluación recopila evidencias mediante la versión obsoleta de los controles estándar de PCI DSS. La segunda evaluación recopila evidencias mediante la nueva versión de los controles estándar. Como ambas versiones de los controles de PCI DSS recopilan evidencias de forma activa en las evaluaciones, es probable que vea que ambos conjuntos de controles aparecen en el panel, en el mismo dominio de control. Sin embargo, en casos excepcionales, el control obsoleto y el control nuevo pueden aparecer en distintos dominios de control en el panel.

Puede seguir recopilando evidencias y consultando información sobre los controles y los marcos estándar obsoletos en el panel. Sin embargo, le recomendamos que utilice los nuevos controles y marcos que proporciona Audit Manager tras el lanzamiento de la biblioteca de controles comunes el 6 de junio de 2024. Los nuevos controles estándar pueden recopilar evidencias de AWS managed source. Esto significa que cada vez que hay una actualización de los orígenes de datos subyacentes

para un control común o principal, Audit Manager aplicará automáticamente la misma actualización a todos los controles estándar relacionados.

La instantánea diaria muestra cantidades variables de evidencia cada día. ¿Es esto normal?

No todas las pruebas se recopilan a diario. Los controles de las evaluaciones de Audit Manager se asignan a diferentes origenes de datos, y cada una puede tener un calendario de recopilación de pruebas diferente. Como resultado, se espera que la instantánea diaria muestre una cantidad variable de evidencia cada día. Para obtener más información, consulte Frecuencia de recolección de evidencias.

Solución de problemas AWS Organizations y del administrador delegado

Puede utilizar la información de esta página para resolver los problemas habituales de los administradores delegados en Audit Manager.

Temas

- No puedo configurar Audit Manager con mi cuenta de administrador delegado
- Cuando creo una evaluación, no puedo ver las cuentas de mi organización en Cuentas incluidas
- Aparece un error de acceso denegado cuando intento generar un informe de evaluación con mi cuenta de administrador delegado
- ¿Qué ocurre en Audit Manager si desvinculo la cuenta de un miembro de mi organización?
- ¿Qué ocurre si vuelvo a vincular la cuenta de un miembro a mi organización?
- ¿Qué ocurre si migro la cuenta de un miembro de una organización a otra?

No puedo configurar Audit Manager con mi cuenta de administrador delegado

Aunque se admiten varios administradores delegados AWS Organizations, Audit Manager solo permite un administrador delegado. Si intenta designar varios administradores delegados en Audit Manager, recibirá el siguiente mensaje de error como el que sigue:

- Consola: `You have exceeded the allowed number of delegated administrators for the delegated service`
- CLI: `An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 2222222222222 to 333333333333`

Elija la cuenta individual que desee usar como administrador delegado en Audit Manager. Asegúrese de registrar primero la cuenta de administrador delegado en Organizations y, a continuación, de añadir la misma cuenta que un administrador delegado en Audit Manager.

Cuando creo una evaluación, no puedo ver las cuentas de mi organización en Cuentas incluidas

Si desea que la evaluación de Audit Manager incluya varias cuentas de su organización, debe especificar un administrador delegado.

Asegúrese de configurar una cuenta de administrador delegado para Audit Manager. Para obtener instrucciones, consulte Adición de un administrador delegado.

Algunas cuestiones a tener en cuenta:

- No puede usar su cuenta AWS Organizations de administración como administrador delegado en Audit Manager.
- Si desea activar Audit Manager en más de una Región de AWS, debe designar una cuenta de administrador delegado por separado en cada región. En la configuración de Audit Manager, designe la misma cuenta de administrador delegado en todas las regiones.
- Cuando designe un administrador delegado, asegúrese de que la cuenta de administrador delegado tenga acceso a la clave de KMS que proporcionó al configurar Audit Manager. Para obtener información sobre cómo revisar y cambiar la configuración del cifrado, consulte Configuración de los ajustes del cifrado de datos.

Aparece un error de acceso denegado cuando intento generar un informe de evaluación con mi cuenta de administrador delegado

Aparecerá un error `access denied` si la evaluación la creó una cuenta de administrador delegado a la que no pertenece la clave KMS especificada en la configuración de Audit Manager. Para evitar

este error, cuando designe un administrador delegado para Audit Manager, asegúrese de que la cuenta de administrador delegado tenga acceso a la clave KMS que proporcionó al configurar Audit Manager.

También puede recibir un error `access denied` si no tiene permisos de escritura para el bucket de S3 que utiliza como destino del informe de evaluación.

Si aparece un error `access denied`, asegúrese de cumplir los siguientes requisitos:

- La clave KMS en la configuración de Audit Manager otorga permisos al administrador delegado. Para configurarlo, siga las instrucciones de la AWS Key Management Service Guía para desarrolladores sobre cómo permitir que los usuarios de otras cuentas usen una clave KMS. Para obtener instrucciones sobre cómo revisar y cambiar la configuración del cifrado en Audit Manager, consulte Configuración de los ajustes del cifrado de datos.
- Tiene una política de permisos que le otorga acceso de escritura al destino del informe de evaluación. Más específicamente, su política de permisos contiene una acción `s3:PutObject`, especifica el ARN del bucket de S3 e incluye la clave KMS que se utiliza para cifrar los informes de evaluación. Para ver un ejemplo de política que puede usar, consulte Ejemplo 2 (permisos de destino del informe de evaluación).

> **Note**
>
> Al cambiar la configuración de cifrado de datos de Audit Manager, estos cambios se aplican a cualquier evaluación nueva que cree. Esto incluye todos los informes de evaluación que cree a partir de sus nuevas evaluaciones.
> Los cambios no se aplican a las evaluaciones existentes que creó antes de cambiar la configuración del cifrado. Esto incluye los nuevos informes de evaluación que se crean a partir de las evaluaciones existentes, además de los informes de evaluación existentes. Las evaluaciones existentes (y todos sus informes de evaluación) siguen utilizando la antigua clave KMS. Si la identidad de IAM que genera el informe de evaluación no tiene permisos para usar la antigua clave de KMS, puede conceder permisos a nivel de política clave.

¿Qué ocurre en Audit Manager si desvinculo la cuenta de un miembro de mi organización?

Al desvincular la cuenta de un miembro de una organización, Audit Manager recibe una notificación sobre este evento. A continuación, Audit Manager elimina esa Cuenta de AWS automáticamente de las listas de cuentas incluidas de sus evaluaciones existentes. Al especificar el ámbito de las nuevas evaluaciones en el futuro, la cuenta desvinculada ya no aparece en la lista de Cuentas de AWS elegibles.

Cuando Audit Manager elimina una cuenta de miembro desvinculada de las listas de cuentas incluidas de sus evaluaciones, no se le notifica este cambio. Además, a la cuenta de miembro desvinculada no se le notifica que Audit Manager ya no está activado en su cuenta.

¿Qué ocurre si vuelvo a vincular la cuenta de un miembro a mi organización?

Cuando vuelve a vincular una cuenta de miembro a u organización, esa cuenta no se añade automáticamente al ámbito de sus evaluaciones de Audit Manager existentes. Sin embargo, la cuenta de miembro que se ha vuelto a vincular ahora aparece como apta Cuenta de AWS al especificar las cuentas incluidas en el ámbito de sus evaluaciones.

- En el caso de las evaluaciones existentes, puede editar manualmente el ámbito de la evaluación para añadir la cuenta de miembro revinculada. Para obtener instrucciones, consulte Paso 2: Editar Cuentas de AWS el alcance.
- Para las nuevas evaluaciones, puede añadir la cuenta revinculada durante la configuración de la evaluación. Para obtener instrucciones, consulte Paso 2: especificar Cuentas de AWS el alcance.

¿Qué ocurre si migro la cuenta de un miembro de una organización a otra?

Si la cuenta de un miembro tiene Audit Manager activado en la organización 1 y, a continuación, migra a la organización 2, Audit Manager no estará habilitado para la organización 2 como resultado.

Solución de problemas con el buscador de evidencias

Utilice la información de esta página para resolver problemas comunes relacionados con el buscador de evidencias en Audit Manager.

Problemas generales relacionados con el buscador de evidencias

- No puedo habilitar el buscador de evidencias
- He activado el buscador de evidencias, pero no veo pruebas anteriores en los resultados de mi búsqueda
- No puedo desactivar el buscador de evidencias
- Mi consulta de búsqueda falla
- Veo que un dominio de control está marcado como obsoleto ¿Qué significa esto?

Problemas con el informe de evaluación del buscador de evidencias

- No puedo generar varios informes de evaluación a partir de los resultados de mi búsqueda
- No puedo incluir pruebas específicas de los resultados de mi búsqueda
- No todos los resultados de mi buscador de evidencias se incluyen en el informe de evaluación
- Quiero generar un informe de evaluación a partir de los resultados de mi búsqueda, pero el enunciado de mi consulta no funciona
- Recursos adicionales

Problemas de exportación a CSV del del buscador de evidencias

- Mi exportación CSV ha fallado
- No puedo exportar pruebas específicas de los resultados de mi búsqueda
- No puedo exportar varios archivos CSV a la vez

No puedo habilitar el buscador de evidencias

Algunas razones comunes por las que no puede cerrar una incluyen las siguientes situaciones:

Le faltan permisos

Si está intentando habilitar el buscador de evidencias por primera vez, asegúrese de tener los permisos necesarios para habilitarlo. Estos permisos le permiten crear y administrar un almacén de datos de eventos en CloudTrail Lake, que es necesario para respaldar las consultas de búsqueda de evidencias. Los permisos también le permiten realizar consultas de búsqueda en el buscador de evidencias.

Si necesitas ayuda con los permisos, ponte en contacto con tu AWS administrador. Si es AWS administrador, puede copiar la declaración de permisos requerida y adjuntarla a una política de IAM.

Está utilizando la cuenta de administración de Organizations

Recuerde que no puede usar la cuenta de administración para habilitar el buscador de evidencias. Inicie sesión como la cuenta de administrador delegado e inténtelo de nuevo.

Ha desactivado anteriormente el buscador de evidencias

Actualmente, no se permite volver a habilitar el buscador de evidencias. Si anteriormente desactivó el buscador de evidencias, no podrá volver a habilitarlo.

He activado el buscador de evidencias, pero no veo pruebas anteriores en los resultados de mi búsqueda

Al activar el buscador de evidencias, todos los datos de las pruebas anteriores tardan hasta 7 días en estar disponibles.

Durante este período de 7 días, se rellena un almacén de datos de eventos con los datos probatorios de los últimos dos años. Esto significa que si utiliza el buscador de evidencias inmediatamente después de activarlo, no estarán disponibles todos los resultados hasta que haya completado el proceso de relleno.

Para obtener instrucciones sobre cómo comprobar el estado de la reposición de datos, consulte Confirming the status of evidence finder.

No puedo desactivar el buscador de evidencias

Esto podría deberse a una de las siguientes causas.

Le faltan permisos

Si está intentando deshabilitar el buscador de evidencias, asegúrese de tener los permisos necesarios para deshabilitarlo. Estos permisos te permiten actualizar y eliminar un almacén de datos de eventos en CloudTrail Lake, lo cual es necesario para deshabilitar el buscador de evidencias.

Si necesitas ayuda con los permisos, ponte en contacto con tu AWS administrador. Si es AWS administrador, puede copiar la declaración de permisos requerida y adjuntarla a una política de IAM.

Todavía se está tramitando una solicitud para habilitar el buscador de evidencias

Cuando solicita habilitar el buscador de evidencias, creamos un almacén de datos de eventos para respaldar las consultas del buscador de evidencias. No puede deshabilitar el buscador de evidencias mientras se crea el almacén de datos del evento.

Para continuar, espere a que se cree el almacén de datos de eventos e inténtelo de nuevo. Para obtener más información, consulte Confirming the status of evidence finder.

Ya ha solicitado desactivar el buscador de evidencias

Cuando solicita la desactivación del buscador de evidencias, eliminamos el almacén de datos de eventos que se utiliza para las consultas del buscador de evidencias. Si intenta volver a desactivar el buscador de evidencias mientras se elimina el almacén de datos de eventos, aparecerá un mensaje de error.

En este caso, no es necesario realizar ninguna acción. Espere a que se elimine el almacén de datos de eventos. Tan pronto como se complete, el buscador de evidencias se desactivará. Para obtener más información, consulte Confirming the status of evidence finder.

Mi consulta de búsqueda falla

Una consulta de búsqueda fallida puede deberse a una de las siguientes razones.

Le faltan permisos

Compruebe que el usuario tiene los permisos necesarios para ejecutar consultas de búsqueda y acceder a los resultados de la búsqueda. En concreto, necesita permisos para las siguientes CloudTrail acciones:

- StartQuery
- DescribeQuery
- CancelQuery
- GetQueryResults

Si necesita ayuda con los permisos, póngase en contacto con su AWS administrador. Si es AWS administrador, puede copiar la declaración de permisos requerida y adjuntarla a una política de IAM.

Está ejecutando el número máximo de consultas

Puede ejecutar hasta 5 consultas a la vez. Si ejecuta el número máximo de consultas simultáneas, se producirá un error `MaxConcurrentQueriesException`. Si aparece este mensaje de error, espere un minuto a que finalicen algunas consultas y, a continuación, vuelva a ejecutar la consulta.

La declaración de consulta contiene un error de validación

Si utiliza la API o la CLI para realizar la StartQueryoperación de CloudTrail Lake, asegúrese de que la suya `queryStatement` sea válida. Si la declaración de consulta contiene errores de validación, una sintaxis incorrecta o palabras clave no compatibles, el resultado es un `InvalidQueryStatementException`.

Para obtener más información sobre cómo escribir una consulta, consulte Creación o edición de una consulta en la Guía del usuario de AWS CloudTrail .

Para ver ejemplos de sintaxis válida, revise los siguientes ejemplos de instrucciones de consulta que se pueden utilizar para consultar un almacén de datos de eventos de Audit Manager.

Ejemplo 1: investigue las pruebas y su estado de conformidad

En este ejemplo, se buscan pruebas con cualquier estado de conformidad en todas las evaluaciones consideradas, dentro de un intervalo de fechas específico.

```
SELECT eventData.evidenceId, eventData.resourceArn,
 eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02
 00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

Ejemplo 2: determine las pruebas de incumplimiento de un control

En este ejemplo, se buscan todas las pruebas que no cumplen con las normas de un intervalo de fechas especificado para una evaluación y un control específicos.

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-
ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN
```

```
 ('NON_COMPLIANT','FAILED','WARNING') AND eventData.controlId IN ('aa11bb22-cc33-
dd44-ee55-ff66gg77hh88')
```

Ejemplo 3: cuente las pruebas por su nombre

En este ejemplo, se enumeran las pruebas totales de una evaluación en un intervalo de fechas específico, agrupadas por nombre y ordenadas por recuento de pruebas.

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM  $EDS_ID
 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime
 > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY
 eventData.eventName ORDER BY totalEvidence DESC
```

Ejemplo 4: explore las pruebas por origen de datos y servicio

En este ejemplo, se buscan todas las pruebas de un intervalo de fechas especificado para un servicio y un origen de datos específicos.

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND
 eventData.dataSource IN ('AWS API calls')
```

Ejemplo 5: Explore las pruebas de conformidad por origen de datos y dominio de control

En este ejemplo, se buscan pruebas de conformidad para dominios de control específicos, donde las pruebas provienen de un origen de datos que no es AWS Config.

```
 SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN
 ('PASSED','COMPLIANT') AND eventData.controlDomainName IN ('Logging and
 monitoring','Data security and privacy') AND eventData.dataSource NOT IN ('AWS
 Config')
```

Otras excepciones de API

La StartQueryAPI puede fallar por varios otros motivos. Para obtener una lista completa de los posibles errores y descripciones, consulta la referencia sobre StartQuery errores en la AWS CloudTrail API.

Veo que un dominio de control está marcado como obsoleto ¿Qué significa esto?

Al aplicar un filtro de dominio de control en el buscador de evidencias, es posible que observe que algunos dominios de control disponibles se describen como Obsoletos.

A partir del 6 de junio de 2024, Audit Manager admite un nuevo conjunto de dominios de control proporcionados por AWS Control Catalog. Para obtener una lista de estos dominios de control, consulta la referencia de ListDomainsla API del Catálogo de AWS Control.

Si un dominio de control está marcado como Obsoleto, esto significa que el dominio de control que está viendo no es uno de los nuevos dominios de control proporcionados por AWS Control Catalog. Audit Manager sigue siendo compatible con estos dominios de control obsoletos para que pueda seguir utilizándolos como criterio a la hora de buscar evidencias.

Aunque seguimos admitiendo los dominios de control obsoletos, le recomendamos que utilice los nuevos dominios de control. Los nuevos dominios de control se asignan a los controles estándar actualizados que se lanzaron como parte de la biblioteca de controles comunes el 6 de junio de 2024. En esta fecha, publicamos controles estándar actualizados que pueden recopilar evidencias de orígenes administrados por AWS. Esto significa que cada vez que hay una actualización de los orígenes de datos subyacentes para un control común o principal, Audit Manager aplicará automáticamente la misma actualización a todos los controles estándar relacionados.

No puedo generar varios informes de evaluación a partir de los resultados de mi búsqueda

Este error se debe a que se ejecutan demasiadas consultas de CloudTrail Lake al mismo tiempo.

Este error puede producirse si agrupa los resultados de la búsqueda e intenta generar inmediatamente informes de evaluación para cada partida de los resultados agrupados. Cuando obtiene los resultados de la búsqueda y genera un informe de evaluación, cada acción invoca una consulta. Solo puede ejecutar hasta 5 consultas a la vez. Si ejecuta el número máximo de consultas simultáneas, se mostrará un error `MaxConcurrentQueriesException`.

Para evitar este error, asegúrese de no generar demasiados informes de evaluación a la vez. Si ejecuta el número máximo de consultas simultáneas, se mostrará un error `MaxConcurrentQueriesException`. Si recibe este mensaje de error, espere unos minutos a que se completen los informes de evaluación en curso.

Puede comprobar el estado de los informes de evaluación desde la página del centro de descargas de la consola de Audit Manager. Una vez completados los informes, vuelva a los resultados agrupados en el buscador de evidencias. A continuación, podrá seguir obteniendo los resultados y generar un informe de evaluación para cada partida.

No puedo incluir pruebas específicas de los resultados de mi búsqueda

Todos los resultados de la búsqueda se incluyen en el informe de evaluación. No puede añadir filas individuales de forma selectiva a su conjunto de resultados de búsqueda.

Si solo quiere incluir resultados de búsqueda específicos en el informe de evaluación, le recomendamos que edite sus filtros de búsqueda actuales. De esta forma, puede restringir los resultados para centrarse únicamente en las pruebas que desee incluir en el informe.

No todos los resultados de mi buscador de evidencias se incluyen en el informe de evaluación

Al generar un informe de evaluación, hay límites en cuanto a la cantidad de evidencia que se puede añadir. El límite se basa en la Región de AWS evaluación, en la región del depósito de S3 que se utiliza como destino del informe de evaluación y en si la evaluación utiliza una evaluación gestionada por el cliente AWS KMS key.

1. El límite es de 22.000 para los informes de la misma región (en los que el bucket de S3 y la evaluación están en la misma Región de AWS)
2. El límite es de 3500 para los informes de la misma región (en los que el bucket de S3 y la evaluación están en la misma Regiones de AWS)
3. El límite es de 3500 si la evaluación utiliza una clave KMS administrada por el cliente

Si supera este límite, el informe aún se crea. Sin embargo, Audit Manager agrega solo los primeros 3500 o 22.000 elementos de evidencia al informe.

Para evitar este problema, le recomendamos que edite los filtros de búsqueda actuales. De esta forma, puede reducir los resultados de la búsqueda segmentando una cantidad menor de pruebas. Si es necesario, puede repetir este método y generar varios informes de evaluación en lugar de un informe más grande.

Quiero generar un informe de evaluación a partir de los resultados de mi búsqueda, pero el enunciado de mi consulta no funciona

Si utilizas la CreateAssessmentReportAPI y tu declaración de consulta devuelve una excepción de validación, consulta la siguiente tabla para obtener instrucciones sobre cómo solucionarlo.

> **Note**
>
> Incluso si una sentencia de consulta funciona CloudTrail, es posible que la misma consulta no sea válida para la generación de informes de evaluación en Audit Manager. Esto se debe a algunas diferencias en la validación de consultas entre los dos servicios.

Cláusul	Problema	Solución	Notas
`SELECT`	La cláusula `SELECT` contiene un nombre de columna	Elimine la cláusula `SELECT` y sustitúyala por `SELECT eventJson` .	Solo se admite `SELECT eventJson` . Esta validación la gestiona Audit Manager.
`FROM`	La cláusula `FROM` contiene un ID de almacén de datos de eventos no válido o El ID del almacén de datos de eventos proporcionado no	Elimine la cláusula `FROM` y sustitúyala por `FROM` *`edsID`*, donde el valor de `edsID` coincide con el ID del almacén de datos de eventos que se especifica en la configuración de Audit Manager.	Esta validación la gestiona Audit Manager.

Cláusul	Problema	Solución	Notas
	coincide con el ID del almacén de datos de eventos en la configuración de su Audit Manager.	Puede recuperar el ARN del almacén de datos de eventos desde la configuración de Audit Manager. Para obtener más información, consulte GetSettings en la Referencia de la API de AWS Audit Manager .	
`GROUP BY`	Hay una cláusula `GROUP BY` en la consulta	Elimine la cláusula `GROUP BY`.	Esta validación la gestiona Audit Manager.
`HAVING`	Hay una cláusula `HAVING` en la consulta	Elimine la cláusula `HAVING`.	Esta validación la gestiona Audit Manager.
`LIMIT`	La cláusula `LIMIT` contiene un valor que supera el límite máximo permitido	Si la cláusula `LIMIT` existe, asegúrese de que su valor sea igual o inferior al límite máximo admitido: • Para los informes de la misma región, el límite es de 22.000 • Para los informes entre regiones, el límite es de 3500 • En el caso de los informes en los que la evaluación relacionada utiliza una evaluación gestionada por el cliente AWS KMS key, el límite es de 3500	En la consola, no hay límite en cuanto al número de resultados de evidencias que se pueden devolver. Sin embargo, al generar un informe de evaluación, se aplica un límite a la cantidad de evidencias que se pueden incluir. Si no se proporciona ningún valor `LIMIT` en el enunciado de consulta, se aplican los límites máximos predeterminados. Esta validación la gestiona Audit Manager.

Cláusul	Problema	Solución	Notas
`ORDER BY`	La cláusula `ORDER BY` contiene funciones agregadas o alias que no están presentes en la cláusula `SELECT`	Asegúrese de que la cláusula `ORDER BY` no contenga ninguna condición mediante el uso de funciones agregadas o alias.	La CloudTrail StartQuery API gestiona esta validación.
`WHERE`	La cláusula `WHERE` contiene más de una `assessmentId` o La cláusula `WHERE` contiene un `assessmentId` valor que no coincide con el `assessmentId` de su solicitud `createAssessmentReport` o La cláusula `WHERE` contiene un nombre de columna no compatible	Asegúrese de que solo se especifique un AssessmentID y de que coincida con el parámetro AssessmentID que especificó en la solicitud de API`createAssessmentReport` . Elimine los nombres de columna no admitidos.	La CloudTrail StartQuery API gestiona esta validación.

Ejemplos

Los siguientes ejemplos muestran cómo se puede utilizar el `queryStatement` parámetro al llamar a la CreateAssessmentReportoperación. Antes de usar estas consultas, *`placeholder text`* reemplácelas por sus propios `assessmentId` valores `edsId` y.

Ejemplo 1: crear un informe (se aplica el límite para la misma región)

En este ejemplo, se crea un informe que incluye los resultados de los buckets de S3 creados entre el 22 y el 23 de enero de 2022.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND
 eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

Ejemplo 2: crear un informe (se aplica un límite entre regiones)

En este ejemplo, se crea un informe que incluye todos los resultados del almacén de datos de eventos y la evaluación del evento especificados, sin especificar ningún intervalo de fechas.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

Ejemplo 3: crear un informe (por debajo del límite predeterminado)

En este ejemplo, se crea un informe que incluye todos los resultados del almacén de datos de eventos y la evaluación del evento especificados, con un límite inferior al máximo predeterminado.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

Recursos adicionales

La siguiente página contiene una guía general para la solución de problemas relacionados con los informes de evaluación:

- Solución de problemas con el informe de evaluación

Mi exportación CSV ha fallado

La exportación de CSV puede fallar por varias razones. Puede solucionar este problema comprobando las causas más frecuentes.

Primero, asegúrese de que cumple los requisitos previos para usar la característica de exportación de CSV:

Ha activado correctamente el buscador de evidencias

Si no ha activado el buscador de evidencias, no podrá ejecutar una consulta de búsqueda ni exportar los resultados de la búsqueda.

El relleno de su almacén de datos de eventos está completo

Si utiliza el buscador de evidencias inmediatamente después de activarlo y aún está rellenando las pruebas, es posible que algunos resultados no estén disponibles. Para comprobar el estado de la reposición, consulte Confirming the status of evidence finder.

La consulta de búsqueda se ha realizado correctamente

Audit Manager no puede exportar los resultados de una consulta fallida. Para solucionar problemas relacionados con una consulta fallida, consulte Mi consulta de búsqueda falla.

Una vez que haya confirmado que cumple los requisitos previos, utilice la siguiente lista de comprobación para comprobar si hay posibles problemas:

1. Verifique el estado de la consulta de búsqueda:
   a. ¿Se ha cancelado la consulta? El buscador de evidencias muestra resultados parciales que se hayan procesado antes de que se cancelara la consulta. Sin embargo, Audit Manager no exporta resultados parciales a su bucket de S3 ni al centro de descargas.
   b. ¿La consulta lleva ejecutándose más de una hora? Es posible que las consultas que se ejecuten durante más de una hora agoten el tiempo de espera. El buscador de evidencias muestra resultados parciales que se hayan procesado antes de que se agotara el tiempo de espera de la consulta. Sin embargo, Audit Manager no exporta resultados parciales. Para evitar que se agote el tiempo de espera, puede reducir la cantidad de evidencias escaneadas por Editar filtros de búsqueda para especificar un intervalo más reducido.
2. Comprueba el nombre y el URI del bucket de S3 de destino de exportación:
   a. ¿Existe el bucket que ha especificado? Si ha introducido el URI de un bucket de forma manual, asegúrese de no haber escrito nada mal. Un error tipográfico o un URI incorrecto pueden provocar un error `RESOURCE_NOT_FOUND` cuando Audit Manager intente exportar el archivo CSV a Amazon S3.
3. Compruebe los permisos del bucket de S3 de destino de exportación:
   a. ¿Tiene permisos de escritura del bucket de S3? Debe disponer de acceso de escritura para el bucket de S3 que utilice como destino de exportación. Más específicamente, la política de

permisos de IAM debe incluir una `s3:PutObject` acción y el ARN del bucket, y CloudTrail figurar como principal del servicio. Proporcionamos un ejemplo de política que puede utilizar.

4. Compruebe si alguno de sus Región de AWS datos no coincide:
   a. ¿La Región de AWS clave gestionada por el cliente coincide con la Región de AWS de su evaluación? Si proporcionó una clave administrada por el cliente para el cifrado de datos, debe estar en la misma Región de AWS que la de su evaluación. Para obtener instrucciones sobre cómo cambiar la clave de KMS, consulte Configuración de los ajustes del cifrado de datos.
5. Compruebe los permisos de su cuenta de administrador delegado:
   a. ¿La clave administrada por el cliente en la configuración de Audit Manager concede permisos a su administrador delegado? Si utiliza una cuenta de administrador delegado y especificó una clave administrada por el cliente para el cifrado de datos, asegúrese de que el administrador delegado tenga acceso a esa clave de KMS. Para obtener más información, consulte Permitir que los usuarios de otras cuentas utilicen una clave de KMS en la AWS Key Management Service Guía para desarrolladores. Para revisar y cambiar la configuración del cifrado de Audit Manager, consulte Configuración de los ajustes del cifrado de datos.

> **Note**
>
> Si cambia la configuración de cifrado de datos de Audit Manager, estos cambios se aplicarán a las nuevas evaluaciones que cree en el futuro. Esto incluye cualquier archivo CSV que exporte de sus nuevas evaluaciones.
> Los cambios no se aplican a las evaluaciones existentes que creó antes de cambiar la configuración del cifrado. Esto incluye las nuevas exportaciones a CSV de las evaluaciones existentes, además de las exportaciones a CSV existentes. Las evaluaciones existentes (y todas sus exportaciones a CSV) siguen utilizando la antigua clave KMS. Si la identidad de IAM que exporta el archivo CSV no tiene permisos para usar la clave KMS anterior, puedes conceder permisos a nivel de política clave.

No puedo exportar pruebas específicas de los resultados de mi búsqueda

Todos los resultados de la búsqueda se incluyen en los resultados.

Si quiere incluir solo pruebas específicas en el archivo CSV, le recomendamos que edite sus filtros de búsqueda actuales. De esta forma, puede restringir los resultados para centrarse únicamente en las pruebas que desee exportar.

No puedo exportar varios archivos CSV a la vez

Este error se debe a que se ejecutan demasiadas consultas de CloudTrail Lake al mismo tiempo.

Esto puede ocurrir si agrupa los resultados de la búsqueda e intenta exportar inmediatamente un archivo CSV para cada partida de los resultados agrupados. Al obtener los resultados de la búsqueda y exportar un archivo CSV, cada una de estas acciones invoca una consulta. Solo puede ejecutar hasta cinco consultas a la vez. Si ejecuta el número máximo de consultas simultáneas, se mostrará un error `MaxConcurrentQueriesException`.

Para evitar este error, asegúrese de no exportar demasiados archivos CSV a la vez.

Para resolver este error, espere a que se completen las exportaciones CSV en curso. La mayoría de las exportaciones tardan unos minutos. Sin embargo, si exporta una gran cantidad de datos, la exportación puede tardar hasta una hora en completarse. No dude en salir del buscador de evidencias mientras la exportación esté en curso.

Puede comprobar el estado de la exportación desde el centro de descargas de la consola Audit Manager. Cuando los archivos exportados estén listos, vuelva a los resultados agrupados en el buscador de evidencias. A continuación, podrá seguir obteniendo los resultados y exportar un archivo CSV para cada partida.

Solución de problemas con los marcos

Puede utilizar la información de esta página para resolver problemas comunes con los marcos en Audit Manager.

Problemas generales con los marcos

- En la página de detalles del marco personalizado se me pide que vuelva a crear el marco personalizado
- No puedo crear una copia del marco personalizado

Problemas con el uso compartido de los marcos

- El estado de mi solicitud de compartir enviada aparece como Fallido
- Mi solicitud de uso compartido tiene un punto azul al lado. ¿Qué significa esto?

- Mi marco compartido tiene controles que utilizan AWS Config reglas personalizadas como fuente de datos. ¿Puede el destinatario recopilar pruebas para estos controles?
- He actualizado una regla personalizada que se usa en un marco compartido. ¿Tengo que tomar alguna medida?

En la página de detalles del marco personalizado se me pide que vuelva a crear el marco personalizado

Si aparece un mensaje en el que se indica Hay definiciones de control actualizadas disponibles, esto significa que Audit Manager ahora proporciona definiciones más recientes para algunos de los controles estándar que se encuentran en el marco personalizado.

Los controles estándar ahora pueden recopilar evidencias de AWS managed source. Esto significa que cada vez que Audit Manager actualice los orígenes de datos subyacentes para un control común o principal, la misma actualización se aplicará automáticamente a los controles estándar relacionados. Esto le ayuda a garantizar la conformidad continua a medida que cambia el entorno de conformidad de la nube. Para asegurarse de aprovechar estas fuentes AWS administradas, le recomendamos que sustituya los controles en su marco personalizado.

En el marco personalizado, Audit Manager indica los controles que tienen reemplazos disponibles. Deberá reemplazar estos controles antes de crear una copia del marco personalizado. La próxima vez que edite el marco personalizado, le pediremos que reemplace estos controles junto con cualquier otra modificación que desee realizar.

Hay dos formas de reemplazar los controles en el marco personalizado:

1. Volver a crear el marco personalizado

Si hay un gran número de controles con reemplazos disponibles, le recomendamos que vuelva a crear el marco personalizado. Es probable que esta sea la mejor opción si el marco personalizado se basa en un marco estándar.

- Por ejemplo, supongamos que ha creado el marco personalizado con NIST SP 800-53 Rev 5 como punto de partida. Este marco estándar tiene 1007 controles estándar, y ha añadido 20 controles personalizados.
- En este caso, la opción más eficaz es buscar `NIST 800-53 (Rev. 5) Low-Moderate-High` en la biblioteca de marcos y crear una copia editable de ese marco. Durante este proceso, puede añadir los mismos 20 controles personalizados que ha utilizado anteriormente. Dado que ahora utiliza la definición más reciente del marco estándar como punto de partida, el marco personalizado hereda automáticamente las definiciones más recientes de todos los 1007 controles estándar.

2. Editar el marco personalizado

Si hay un número reducido de controles con reemplazos disponibles, le recomendamos que edite el marco personalizado y reemplace los controles manualmente.

- Por ejemplo, supongamos que ha creado el marco personalizado desde cero. En el marco personalizado, ha añadido 20 controles personalizados que ha creado usted mismo y ocho controles estándar del marco estándar de Essential Eight del ACSC .
- En este caso, dado que habría actualizaciones disponibles para un máximo de ocho controles, la opción más eficaz es editar el marco personalizado y reemplazar esos controles uno por uno. Para obtener instrucciones, consulte el siguiente procedimiento.

Reemplazo manual de los controles del marco personalizado

Reemplazo manual de los controles del marco personalizado

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. En el panel de navegación izquierdo, elija Biblioteca de marcos y luego la pestaña Marcos personalizados.
3. Seleccione el marco que desee editar, elija Acciones y, a continuación, elija Editar.
4. En la página Editar detalles del marco, seleccione Siguiente.
5. En la página Editar conjuntos de controles, revise el nombre de cada conjunto de controles para ver si alguno de sus controles tiene reemplazos disponibles.
6. Elija un conjunto de controles afectado para ampliarlo e identifique los controles que deben reemplazarse.

> **Tip**
>
> Para identificar los controles de forma más rápida, escriba **`Replacement available`** en el cuadro de búsqueda.

7. Para eliminar los controles afectados, seleccione la casilla de verificación y elija Eliminar del conjunto de controles.
8. Vuelva a añadir los mismos controles. Esta acción reemplaza los controles que acaba de eliminar por la definición de control más reciente.
   a. En Añadir controles, utilice la lista desplegable Tipo de control y seleccione Controles estándar.
   b. Busque el reemplazo del control que acaba de eliminar.

      > **Tip**
      >
      > En algunos casos, es posible que el nombre del control de reemplazo no sea exactamente el mismo que el original. En este caso, es probable que el nombre del control de reemplazo sea muy similar al original. En casos excepcionales, dos controles pueden reemplazar un control (o a la inversa).
      > Si no puede encontrar un control de reemplazo, le recomendamos que realice una búsqueda parcial. Para ello, escriba parte del nombre del control original o una palabra clave que represente lo que busca. También puede buscar por tipo de conformidad para reducir aún más la lista de resultados.

   c. Seleccione la casilla de verificación situada junto a un control y elija Añadir al conjunto de controles.
   d. En la ventana emergente que aparece, seleccione Añadir para confirmar.
9. Repita los pasos 6 a 8 según sea necesario hasta que haya reemplazado todos los controles.
10. Elija Siguiente.
11. En la página Revisar y guardar, revise los cambios y luego seleccione Guardar cambios.

No puedo crear una copia del marco personalizado

Si el botón Hacer una copia no está disponible en la página de detalles del marco, esto significa que debe reemplazar algunos de los controles del marco personalizado.

Para obtener instrucciones sobre cómo proceder, consulte En la página de detalles del marco personalizado se me pide que vuelva a crear el marco personalizado.

El estado de mi solicitud de compartir enviada aparece como Fallido

Si intenta compartir un marco personalizado y se produce un error en la operación, le recomendamos que compruebe lo siguiente:

1. Asegúrese de que Audit Manager esté activado en el destinatario Cuenta de AWS y en la región especificada. Para obtener una lista de AWS Audit Manager las regiones compatibles, consulte los AWS Audit Manager puntos de conexión y las cuotas en la Referencia general de Amazon Web Services.
2. Asegúrese de haber introducido el Cuenta de AWS ID correcto al especificar la cuenta del destinatario.
3. Asegúrese de no haber especificado una cuenta AWS Organizations de administración como destinatario. Puede compartir un marco personalizado con un administrador delegado, pero si intenta compartir un marco personalizado con una cuenta de administración, la operación fallará.
4. Si utiliza una clave administrada por el cliente para cifrar los datos de Audit Manager, asegúrese de que la clave KMS esté habilitada. Si la clave de KMS está deshabilitada e intenta compartir un marco personalizado, la operación no se realizará correctamente. Para obtener instrucciones sobre cómo habilitar una clave KMS deshabilitada, consulte Habilitar y deshabilitar claves en la AWS Key Management Service Guía para desarrolladores.

Mi solicitud de uso compartido tiene un punto azul al lado. ¿Qué significa esto?

Una notificación con un punto azul indica que una solicitud de compartición requiere tu atención.

Notificaciones con puntos azules para los remitentes

Aparece un punto de notificación azul junto a las solicitudes de uso compartido enviadas con el estado de a punto de vencer. Audit Manager muestra la notificación con un punto azul para que

pueda recordar al destinatario que tome medidas con respecto a la solicitud de compartición antes de que caduque.

Para que desaparezca el punto azul de la notificación, el destinatario debe aceptar o rechazar la solicitud. El punto azul también desaparece si revoca la solicitud de compartir.

Puede usar el siguiente procedimiento para comprobar si hay solicitudes de uso compartido que estén venciendo y enviar un recordatorio opcional al destinatario para que tome las medidas oportunas.

Para ver las notificaciones de las solicitudes enviadas

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. Si tiene una notificación de solicitud de uso compartido, Audit Manager muestra un punto rojo junto al icono del menú de navegación.

3. Despliegue el panel de navegación y busque junto a Solicitudes de uso compartido. Una insignia de notificación indica el número de solicitudes de uso compartido que requieren su atención.

4. Seleccione Compartir solicitudes y, a continuación, seleccione la pestaña Solicitudes enviadas.
5. Busque el punto azul para identificar las solicitudes de uso compartido que vencen en los próximos 30 días. Como alternativa, también puede ver las solicitudes de acciones que van a caducar seleccionando Vencimiento en el menú desplegable del filtro de todos los estados.

6. (Opcional) Recuerde al destinatario que debe tomar medidas con respecto a la solicitud de uso compartido antes de que caduque. Este paso es opcional, ya que Audit Manager envía una notificación a la consola para informar al destinatario cuando una solicitud de compartición está activa o va a caducar. Sin embargo, también puede enviar su propio recordatorio al destinatario a través del canal de comunicación que prefiera.

Notificaciones con puntos azules para los destinatarios

Junto a las solicitudes de uso compartido recibidas, aparece un punto de notificación azul con el estado Activo o A punto de vencer. Audit Manager muestra la notificación con un punto azul para recordarle que debe tomar medidas con respecto a la solicitud de participación antes de que venza. Para que desaparezca el punto azul de notificación, debe aceptar o rechazar la solicitud. El punto azul también desaparece si el remitente revoca la solicitud de compartir.

Puede utilizar el siguiente procedimiento para comprobar si hay solicitudes de uso compartido activas y vencidas.

Para ver las notificaciones de las solicitudes recibidas

1. Abra la consola de AWS Audit Manager en https://console.aws.amazon.com/auditmanager/casa.
2. Si tiene una notificación de solicitud de uso compartido, Audit Manager muestra un punto rojo junto al icono del menú de navegación.

3. Despliegue el panel de navegación y busque junto a Solicitudes de uso compartido. Una insignia de notificación indica el número de solicitudes de uso compartido que requieren tu atención.

4. Seleccione Solicitudes de uso compartido. De forma predeterminada, esta página se abre en la pestaña Solicitudes recibidas.
5. Busque los elementos con un punto azul para identificar las solicitudes de uso compartido que requieren su acción.

6. (Opcional) Para ver solo las solicitudes que vencen en los próximos 30 días, busque la lista desplegable Todos los estados y seleccione A punto de vencer.

Mi marco compartido tiene controles que utilizan AWS Config reglas personalizadas como fuente de datos. ¿Puede el destinatario recopilar pruebas para estos controles?

Sí, su destinatario puede recopilar pruebas para estos controles, pero son necesarios algunos pasos para lograrlo.

Para que Audit Manager recopile pruebas utilizando una AWS Config regla como mapeo de fuentes de datos, debe cumplirse lo siguiente. Estos criterios se aplican tanto a las reglas administradas como a las reglas personalizadas.

- La regla debe existir en el AWS entorno del destinatario.
- La regla debe estar habilitada en el AWS entorno del destinatario.

Recuerde que es probable que las AWS Config reglas de su cuenta aún no existan en el AWS entorno del destinatario. Además, cuando el destinatario acepta la solicitud de compartición, Audit Manager no vuelve a crear ninguna de sus reglas personalizadas en su cuenta. Para que el destinatario pueda recopilar pruebas utilizando sus reglas personalizadas como mapeo de fuentes de datos, debe crear las mismas reglas personalizadas en su instancia de AWS Config. Una vez que el destinatario crea y activa las reglas AWS Config, Audit Manager puede recopilar pruebas de esa fuente de datos.

Le recomendamos que se comunique con el destinatario para informarle si debe crearse alguna AWS Config regla personalizada en su instancia de AWS Config.

He actualizado una regla personalizada que se usa en un marco compartido. ¿Tengo que tomar alguna medida?

Para actualizaciones de reglas en su AWS entorno

Al actualizar una regla personalizada en su AWS entorno, no es necesario realizar ninguna acción en Audit Manager. Audit Manager detecta y gestiona las actualizaciones de reglas de la forma que se describe en la siguiente tabla. Audit Manager no le notifica cuando se detecta una actualización de reglas.

Escenario	¿Qué hace Audit Manager?	Qué necesita
Se actualiza una regla personalizada en su instancia de AWS Config.	Audit Manager sigue informando de las conclusiones de esa regla mediante la definición de regla actualizada.	No es necesario ninguna acción.
Se elimina una regla personalizada en su instancia de AWS Config.	Audit Manager deja de informar de los resultados de la regla eliminada.	No es necesario ninguna acción. Si lo desea, puede editar los controles personalizados que utilizaban la regla eliminada como asignación de origen de datos. A continuación, puede eliminar la regla eliminada

Escenario	¿Qué hace Audit Manager?	Qué necesita
		para limpiar la configura ción de la origen de datos del control. De lo contrario , el nombre de la regla eliminada permanece como una asignación de origen de datos no utilizada.

Para actualizaciones de reglas fuera de su AWS entorno

En el AWS entorno del destinatario, Audit Manager no detecta la actualización de la regla. Esto se debe a que los remitentes y los destinatarios trabajan en AWS entornos separados. En la tabla siguiente se indican las acciones recomendadas para este escenario.

Su función	Escenario	Acción recomendada
Remite	• Compartió un marco que utiliza reglas personalizadas como asignación de origen de datos. • Después de compartir el marco, actualizó o eliminó una de esas reglas. AWS Config	Póngase en contacto con el destinatario para informarle de la actualización. De esta forma, pueden realizar la misma actualización y mantenerse sincroniz ados con la definición de regla más reciente.
Recipie	• Ha aceptado un marco compartido que utiliza reglas personalizadas como asignació n de origen de datos. • Tras volver a crear las reglas personali zadas en la instancia de AWS Config, el remitente actualizó o eliminó una de esas reglas.	Actualice la regla correspondiente en su propia instancia de AWS Config.

Solución de problemas de notificación

Puede utilizar la información de esta página para resolver problemas de notificación comunes en Audit Manager.

Temas

- He especificado un tema de Amazon SNS en Audit Manager, pero no recibo ninguna notificación
- He especificado un tema de FIFO, pero no recibo las notificaciones en el orden esperado

He especificado un tema de Amazon SNS en Audit Manager, pero no recibo ninguna notificación

Si su tema de Amazon SNS utiliza AWS KMS el cifrado del lado del servidor (SSE), es posible que le falten los permisos necesarios para su política de claves. AWS KMS También es posible que no reciba las notificaciones si no ha suscrito un punto de conexión a su tema.

Si no recibe notificaciones, asegúrese de haber hecho lo siguiente:

- Adjuntó la política de permisos requerida a su clave de KMS. Para ver un ejemplo de política que puede usar, consulte Ejemplo 2 (permisos para la clave de KMS que se adjunta al tema de SNS).
- Has suscrito un punto de conexión al tema a través del cual se envían las notificaciones. Cuando suscriba un punto de conexión de correo electrónico a un tema, recibirá un correo electrónico que le pedirá que confirme su suscripción. Debe confirmar la suscripción para comenzar a recibir notificaciones de correo electrónico. Para obtener más información, consulte Introducción en la Guía para desarrolladores de Amazon SNS.

He especificado un tema de FIFO, pero no recibo las notificaciones en el orden esperado

Audit Manager admite el envío de notificaciones a temas de FIFO SNS. Sin embargo, no se garantiza el orden en el que Audit Manager envía las notificaciones a sus temas de FIFO.

Solución de problemas de permisos y acceso

Puede utilizar la información de esta página para resolver problemas de permisos comunes en Audit Manager.

Temas

- He seguido el procedimiento de configuración de Audit Manager, pero no tengo suficientes privilegios de IAM
- He especificado a alguien como propietario de la auditoría, pero aún no tiene acceso completo a la evaluación. ¿Por qué sucede esto?
- No puedo realizar una acción en Audit Manager
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Audit Manager
- Aparece un error de acceso denegado, a pesar de tener los permisos necesarios de Audit Manager
- Recursos adicionales

He seguido el procedimiento de configuración de Audit Manager, pero no tengo suficientes privilegios de IAM

El usuario, rol o grupo que usa para acceder a Audit Manager debe tener los permisos necesarios. Además, su política basada en la identidad no debería ser demasiado restrictiva. De lo contrario, la consola no funcionará según lo previsto. En esta guía se proporciona un ejemplo de política que puede utilizar en Permita los permisos mínimos necesarios para activar Audit Manager. Dependiendo de su caso de uso, es posible que necesite permisos más amplios y menos restrictivos. Por ejemplo, recomendamos que los propietarios de las auditorías tengan acceso de administrador. Esto es para que puedan modificar la configuración de Audit Manager y gestionar recursos como las evaluaciones, los marcos, los controles y los informes de evaluación. Es posible que otros usuarios, como los delegados, solo necesiten acceso de gestión o acceso de solo lectura.

Asegúrese de añadir los permisos adecuados para su usuario, función o grupo. Para los propietarios de auditorías, la política recomendada es. AWSAuditManagerAdministratorAccess Para los delegados, puede utilizar the management access example policy que se proporciona en la página IAM policy examples. Puede utilizar estas políticas de ejemplo como punto de partida y realizar los cambios que necesite para que se ajusten a sus necesidades.

Le recomendamos que dedique un tiempo a personalizar sus permisos para que se ajusten a sus requisitos específicos. Si necesita ayuda con los permisos de IAM, póngase en contacto con su administrador o con AWS Soporte.

He especificado a alguien como propietario de la auditoría, pero aún no tiene acceso completo a la evaluación. ¿Por qué sucede esto?

Especificar a alguien como propietario de una auditoría por sí solo no le proporciona acceso completo a una evaluación. Los propietarios de la auditoría también deben tener los permisos de IAM necesarios para acceder a los recursos de Audit Manager y gestionarlos. Es decir, además de especificar un usuario como propietario de la auditoría, también debe adjuntar a ese usuario las políticas de IAM necesarias. La razón es porque, al requerir ambas, Audit Manager garantiza que usted tiene el control total sobre todos los detalles de cada evaluación.

> **Note**
>
> Para los propietarios de auditorías, le recomendamos que utilicen la AWSAuditManagerAdministratorAccesspolítica. Para obtener más información, consulte Políticas recomendadas para los usuarios de AWS Audit Manager.

No puedo realizar una acción en Audit Manager

Si no tiene los permisos necesarios para usar la AWS Audit Manager consola o las operaciones de la API de Audit Manager, es probable que se produzca un `AccessDeniedException` error.

Para resolver este problema, debe ponerse en contacto con el administrador para recibir ayuda. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Audit Manager

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puede utilizar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si Audit Manager admite estas características, consulte ¿Cómo AWS Audit Manager funciona con IAM.

- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Aparece un error de acceso denegado, a pesar de tener los permisos necesarios de Audit Manager

Si tu cuenta forma parte de una organización, es posible que el `Access Denied` error se deba a una política de control de servicios (SCP). SCPs son políticas que se utilizan para administrar los permisos de una organización. Cuando existe una SCP, puede denegar permisos específicos a todas las cuentas de miembros, incluida la cuenta de administrador delegado que utilice en Audit Manager.

Por ejemplo, si su organización cuenta con un SCP que deniega los permisos para AWS Control Catalog APIs, no podrá ver los recursos que proporciona Control Catalog. Esto es cierto incluso si tiene los permisos necesarios para Audit Manager, como la AWSAuditManagerAdministratorAccesspolítica. El SCP anula los permisos de política gestionados al denegar explícitamente el acceso al catálogo de control. APIs

A continuación se muestra un ejemplo de una SCP. Con esta SCP establecida, a la cuenta de administrador delegado se le deniega el acceso a los controles comunes, los objetivos de control y los dominios de control necesarios para utilizar la característica de controles comunes de Audit Manager.

JSON

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "controlcatalog:ListCommonControls",
                "controlcatalog:ListObjectives",
                "controlcatalog:ListDomains"
            ],
            "Resource": "*"
        }
    ]
}
```

Para resolver este problema, recomendamos que siga los pasos que se indican a continuación:

1. Confirme si hay una SCP asociada a la organización. Para obtener instrucciones, consulte Getting information about your organization's policies en la Guía del usuario de AWS Organizations.
2. Identifique si la SCP está provocando el error `Access Denied`.
3. Actualícela para asegurarse de que la cuenta de administrador delegado tenga el acceso necesario para Audit Manager. Para obtener instrucciones, consulte Updating an SCP en la Guía del usuario de AWS Organizations.

Recursos adicionales

Las siguientes páginas contienen instrucciones para solucionar otros problemas que pueden deberse a la falta de permisos:

- No veo ningún control o conjunto de controles en mi evaluación
- La opción de regla personalizada no está disponible cuando configuro un origen de datos de control
- Cuando intento generar un informe, aparece un error de acceso denegado
- Aparece un error de acceso denegado cuando intento generar un informe de evaluación con mi cuenta de administrador delegado
- No puedo habilitar el buscador de evidencias
- No puedo desactivar el buscador de evidencias
- Mi consulta de búsqueda falla

- He especificado un tema de Amazon SNS en Audit Manager, pero no recibo ninguna notificación

Recursos de etiquetado AWS Audit Manager

Una etiqueta es una etiqueta de metadatos que se asigna o que se AWS asigna a un AWS recurso. Cada etiqueta consta de una clave y un valor. En el caso de etiquetas que usted asigna, debe definir la clave y el valor. Por ejemplo, puede definir la clave como `stage` y el valor de un recurso como `test`.

Las etiquetas le ayudan a hacer lo siguiente:

- Localice fácilmente sus recursos de Audit Manager. Puede utilizar etiquetas como criterios de búsqueda al navegar por la biblioteca de marcos y la biblioteca de control.
- Asocie su recurso a un tipo de conformidad. Puede etiquetar varios recursos con una etiqueta específica de cumplimiento para asociar esos recursos a un marco específico.
- Identifique y organice sus AWS recursos. Muchos Servicios de AWS admiten el etiquetado, por lo que puede asignar la misma etiqueta a los recursos de diferentes servicios para indicar que los recursos están relacionados.
- Realice un seguimiento de sus AWS costes. Estas etiquetas se activan en el Administración de facturación y costos de AWS panel de control. AWS utiliza las etiquetas para clasificar los costes y entregarle un informe mensual de asignación de costes. Para obtener más información, consulte Uso de etiquetas de asignación de costes en la Guía del usuario de Administración de facturación y costos de AWS .

En las siguientes secciones se proporciona más información sobre las etiquetas de AWS Audit Manager.

Contenido

- Recursos compatibles en Audit Manager
- Restricciones de las etiquetas
- Recursos adicionales

Recursos compatibles en Audit Manager

Los siguientes recursos de Audit Manager admiten el etiquetado:

- Evaluaciones

- Controles
- Marcos

Restricciones de las etiquetas

Las siguientes restricciones básicas se aplican a las etiquetas en los recursos de Audit Manager:

- Cantidad máxima de etiquetas que puede asignar a un recurso: 50
- Longitud máxima de la clave: 128 caracteres Unicode
- Longitud máxima del valor: 256 caracteres Unicode
- Caracteres válidos para claves y valores: a-z, A-Z, 0-9, espacio y los siguientes caracteres: _ . : / = + - y @
- Las claves y los valores distinguen entre mayúsculas y minúsculas
- No lo utilices `aws:` como prefijo para las claves; está reservado para su AWS uso

Recursos adicionales

Puede configurar las etiquetas como propiedades al crear una evaluación, un marco o un control. Puede añadir, editar y eliminar etiquetas a través de la consola Audit Manager, AWS Command Line Interface (AWS CLI) y la API Audit Manager. Para obtener más información, consulte los enlaces siguientes.

- Para etiquetar las evaluaciones:
  - Crear una evaluación en AWS Audit Manager y Edición de una evaluación en AWS Audit Manager en la sección Evaluaciones de esta guía
  - Pestaña Etiquetas en la página Revisión de una evaluación de esta guía
  - CreateAssessmenty UpdateAssessmenten la referencia de la AWS Audit Manager API
  - TagResourcey UntagResourceen la Referencia de la AWS Audit Manager API
- Para etiquetar los marcos:
  - Crear un marco personalizado en AWS Audit Manager y Edición de un marco personalizado en AWS Audit Manager en la sección Bibliotecas de marcos de esta guía
  - Tags tab en la página Visualización de los detalles de los marcos de esta guía
  - CreateAssessmentFrameworky UpdateAssessmentFrameworken la Referencia de la AWS Audit Manager API

  - TagResourcey UntagResourceen la Referencia de la AWS Audit Manager API
- Para etiquetar controles:
  - Crear un control personalizado en AWS Audit Manager y Edición de un control personalizado en AWS Audit Manager en la sección Biblioteca de control de esta guía
  - La sección Tags de la página Revisión de un control personalizado de esta guía
  - La sección Tags de la página Revisión de un control estándar de esta guía
  - CreateControly UpdateControlen la Referencia de la AWS Audit Manager API
  - TagResourcey UntagResourceen la Referencia de la AWS Audit Manager API

Entender las cuotas y restricciones para AWS Audit Manager

Cuenta de AWS Tiene cuotas predeterminadas, anteriormente denominadas límites, para cada una de ellas Servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de la región. Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

La mayoría de las cuotas de Audit Manager, pero no todas, aparecen en el espacio de AWS Audit Manager nombres de la consola de Service Quotas. Para aprender cómo solicitar un aumento de cuota, consulte Administrar las cuotas de Audit Manager.

Contenido

- Cuotas de Audit Manager
- Administrar las cuotas de Audit Manager
- Recursos adicionales

Cuotas de Audit Manager

Las siguientes AWS Audit Manager cuotas son Cuenta de AWS por región.

Recurso	Cuota
Evaluaciones	Número de evaluaciones activas por cuenta: 100
Informes de evaluación	Número de elementos de prueba que puede añadir a un informe de evaluación: • Para los informes de la misma región (en los que la evaluación y el bucket S3 de destino del informe de evaluación se encuentran en el mismo lugar Región de AWS): 22 000 • Para los informes de distintas regiones (en los que la evaluación y el bucket S3 de destino del informe de evaluación se encuentra n en el mismo lugar Regiones de AWS): 3500

Recurso	Cuota
	• En el caso de los informes en los que la evaluación correspon diente utiliza una gestión por parte del cliente AWS KMS key: 3500
Controles	Número de tareas simultáneas por cuenta: 500
Evidencia	Tamaño máximo de un único archivo de pruebas manuales: 100 MB Número de cargas manuales diarias de pruebas por control: 100 Tip Si necesita cargar una gran cantidad de pruebas manuales en un solo control, le recomendamos que cargue las pruebas en lotes durante varios días.
Marcos	Número de marcos personalizados por cuenta: 100 Note Las cuotas de marcos se aplican a todos los marcos personalizados compartidos de su biblioteca de marcos, independientemente de quién haya creado el marco.
Destinatarios de marcos personalizados compartidos	Número de cuentas receptoras activas: 100
Acceso a la API	Número total de transacciones por segundo (TPS) APIs: 20 TPS

Administrar las cuotas de Audit Manager

AWS Audit Manager está integrado con Service Quotas, y Servicio de AWS le permite ver y gestionar sus cuotas desde una ubicación central. Con Service Quotas, resulta más sencillo buscar el valor de las cuotas de servicio de Audit Manager.

Para ver las service quotas de Audit Manager mediante la consola

1. Abra la consola de Service Quotas en https://console.aws.amazon.com/servicequotas/.
2. En el panel de navegación, elija Servicios de AWS.
3. En la lista Servicios de AWS services, busque y seleccioneAWS Audit Manager.
4. En la lista de cuotas de servicio, puede ver el nombre de la cuota de servicio, el valor de la cuota aplicada (si está disponible), el valor de la cuota AWS predeterminado y si la cuota es ajustable.
5. Para ver información adicional sobre una cuota de servicio, como, por ejemplo, la descripción, elija el nombre de cuota.
6. (Opcional) Para solicitar un aumento de cuota, seleccione la cuota que desea aumentar, seleccione Solicitar aumento de cuota, escriba o seleccione la información necesaria y seleccione Solicitar.

Recursos adicionales

Para obtener más información sobre cómo administrar las cuotas, consulte Requesting a quota increase en la Guía del usuario de Service Quotas.

Para obtener más información acerca de las cuotas de servicio, consulte ¿Qué son las cuotas de servicio? en la Guía del usuario de Service Quotas.

Ejemplos de código para Audit Manager mediante AWS SDKs

Los siguientes ejemplos de código muestran cómo utilizar Audit Manager con un kit de desarrollo de AWS software (SDK).

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica a través de llamadas a varias funciones dentro del servicio o combinado con otros Servicios de AWS.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteAWS Audit Manager Utilizándolo con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código

- Escenarios para el uso de Audit Manager AWS SDKs
  - Cree un marco personalizado de Audit Manager a partir de un paquete de AWS Config conformidad mediante un SDK AWS
  - Cree un marco personalizado de Audit Manager que contenga controles de Security Hub mediante un AWS SDK
  - Cree un informe de evaluación de Audit Manager que contenga un día de pruebas utilizando un AWS SDK

Escenarios para el uso de Audit Manager AWS SDKs

Los siguientes ejemplos de código muestran cómo implementar escenarios comunes en Audit Manager con AWS SDKs. En estas situaciones se muestra cómo llevar a cabo tareas específicas con llamadas a varias funciones dentro de Audit Manager o en combinación con otros Servicios de AWS. En cada escenario se incluye un enlace al código fuente completo, con instrucciones de configuración y ejecución del código.

Los escenarios requieren un nivel intermedio de experiencia para ayudarlo a entender las acciones de servicio en su contexto.

Ejemplos

- Cree un marco personalizado de Audit Manager a partir de un paquete de AWS Config conformidad mediante un SDK AWS

- Cree un marco personalizado de Audit Manager que contenga controles de Security Hub mediante un AWS SDK
- Cree un informe de evaluación de Audit Manager que contenga un día de pruebas utilizando un AWS SDK

Cree un marco personalizado de Audit Manager a partir de un paquete de AWS Config conformidad mediante un SDK AWS

En el siguiente ejemplo de código, se muestra cómo:

- Obtenga una lista de paquetes de AWS Config conformidad.
- Crear un control personalizado de Audit Manager para cada regla gestionada de un paquete de conformidad.
- Crear un marco personalizado de Audit Manager que contenga los controles.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


class ConformancePack:
    def __init__(self, config_client, auditmanager_client):
        self.config_client = config_client
        self.auditmanager_client = auditmanager_client

    def get_conformance_pack(self):
```

```
        """
        Return a selected conformance pack from the list of conformance packs.

        :return: selected conformance pack
        """
        try:
            conformance_packs = self.config_client.describe_conformance_packs()
            print(
                "Number of conformance packs fetched: ",
                len(conformance_packs.get("ConformancePackDetails")),
            )
            print("Fetched the following conformance packs: ")
            all_cpack_names = {
                cp["ConformancePackName"]
                for cp in conformance_packs.get("ConformancePackDetails")
            }
            for pack in all_cpack_names:
                print(f"\t{pack}")
            cpack_name = input(
                "Provide ConformancePackName that you want to create a custom "
                "framework for: "
            )
            if cpack_name not in all_cpack_names:
                print(f"{cpack_name} is not in the list of conformance packs!")
                print(
                    "Provide a conformance pack name from the available list of "
                    "conformance packs."
                )
                raise Exception("Invalid conformance pack")
            print("-" * 88)
        except ClientError:
            logger.exception("Couldn't select conformance pack.")
            raise
        else:
            return cpack_name

    def create_custom_controls(self, cpack_name):
        """
        Create custom controls for all managed AWS Config rules in a conformance
pack.

        :param cpack_name: The name of the conformance pack to create controls
for.
        :return: The list of custom control IDs.
```

```
        """
        try:
            rules_in_pack =
self.config_client.describe_conformance_pack_compliance(
                ConformancePackName=cpack_name
            )
            print(
                "Number of rules in the conformance pack: ",
                len(rules_in_pack.get("ConformancePackRuleComplianceList")),
            )
            for rule in rules_in_pack.get("ConformancePackRuleComplianceList"):
                print(f"\t{rule.get('ConfigRuleName')}")
            print("-" * 88)
            print(
                "Creating a custom control for each rule and a custom framework "
                "consisting of these rules in Audit Manager."
            )
            am_controls = []
            for rule in rules_in_pack.get("ConformancePackRuleComplianceList"):
                config_rule = self.config_client.describe_config_rules(
                    ConfigRuleNames=[rule.get("ConfigRuleName")]
                )
                source_id = (
                    config_rule.get("ConfigRules")[0]
                    .get("Source", {})
                    .get("SourceIdentifier")
                )
                custom_control = self.auditmanager_client.create_control(
                    name="Config-" + rule.get("ConfigRuleName"),
                    controlMappingSources=[
                        {
                            "sourceName": "ConfigRule",
                            "sourceSetUpOption": "System_Controls_Mapping",
                            "sourceType": "AWS_Config",
                            "sourceKeyword": {
                                "keywordInputType": "SELECT_FROM_LIST",
                                "keywordValue": source_id,
                            },
                        }
                    ],
                ).get("control", {})
                am_controls.append({"id": custom_control.get("id")})
            print("Successfully created a control for each config rule.")
            print("-" * 88)
```

```
        except ClientError:
            logger.exception("Failed to create custom controls.")
            raise
        else:
            return am_controls

    def create_custom_framework(self, cpack_name, am_control_ids):
        """
        Create a custom Audit Manager framework from a selected AWS Config
 conformance
        pack.

        :param cpack_name: The name of the conformance pack to create a framework
 from.
        :param am_control_ids: The IDs of the custom controls created from the
                               conformance pack.
        """
        try:
            print("Creating custom framework...")
            custom_framework =
 self.auditmanager_client.create_assessment_framework(
                name="Config-Conformance-pack-" + cpack_name,
                controlSets=[{"name": cpack_name, "controls": am_control_ids}],
            )
            print(
                f"Successfully created the custom framework: ",
                f"{custom_framework.get('framework').get('name')}: ",
                f"{custom_framework.get('framework').get('id')}",
            )
            print("-" * 88)
        except ClientError:
            logger.exception("Failed to create custom framework.")
            raise


def run_demo():
    print("-" * 88)
    print("Welcome to the AWS Audit Manager custom framework demo!")
    print("-" * 88)
    print(
        "You can use this sample to select a conformance pack from AWS Config and
 "
        "use AWS Audit Manager to create a custom control for all the managed "
        "rules under the conformance pack. A custom framework is also created "
```

```
        "with these controls."
    )
    print("-" * 88)
    conf_pack = ConformancePack(boto3.client("config"),
 boto3.client("auditmanager"))
    cpack_name = conf_pack.get_conformance_pack()
    am_controls = conf_pack.create_custom_controls(cpack_name)
    conf_pack.create_custom_framework(cpack_name, am_controls)


if __name__ == "__main__":
    run_demo()
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Python (Boto3).
  - CreateAssessmentFramework
  - CreateControl

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteAWS Audit Manager Utilizándolo con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Cree un marco personalizado de Audit Manager que contenga controles de Security Hub mediante un AWS SDK

En el siguiente ejemplo de código, se muestra cómo:

- Obtener una lista de todos los controles estándar que tienen Security Hub como origen de datos.
- Crear un marco personalizado de Audit Manager que contenga los controles.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


class SecurityHub:
    def __init__(self, auditmanager_client):
        self.auditmanager_client = auditmanager_client

    def get_sechub_controls(self):
        """
        Gets the list of controls that use Security Hub as their data source.

        :return: The list of Security Hub controls.
        """
        print("-" * 88)
        next_token = None
        page = 1
        sechub_control_list = []
        while True:
            print("Page [" + str(page) + "]")
            if next_token is None:
                control_list = self.auditmanager_client.list_controls(
                    controlType="Standard", maxResults=100
                )
            else:
                control_list = self.auditmanager_client.list_controls(
                    controlType="Standard", nextToken=next_token, maxResults=100
                )
```

```
            print("Total controls found:",
 len(control_list.get("controlMetadataList")))
            for control in control_list.get("controlMetadataList"):
                control_details = self.auditmanager_client.get_control(
                    controlId=control.get("id")
                ).get("control", {})
                if "AWS Security Hub" in control_details.get("controlSources"):
                    sechub_control_list.append({"id": control_details.get("id")})
            next_token = control_list.get("nextToken")
            if not next_token:
                break
            page += 1
        print("Number of Security Hub controls found: ",
 len(sechub_control_list))
        return sechub_control_list

    def create_custom_framework(self, am_controls):
        """
        Create a custom framework with a list of controls.

        :param am_controls: The list of controls to include in the framework.
        """
        try:
            print("Creating custom framework...")
            custom_framework =
 self.auditmanager_client.create_assessment_framework(
                name="All Security Hub Controls Framework",
                controlSets=[{"name": "Security-Hub", "controls": am_controls}],
            )
            print(
                f"Successfully created the custom framework: "
                f"{custom_framework.get('framework').get('name')}: "
                f"{custom_framework.get('framework').get('id')}"
            )
            print("-" * 88)
        except ClientError:
            logger.exception("Failed to create custom framework.")
            raise


def run_demo():
    print("-" * 88)
    print("Welcome to the AWS Audit Manager Security Hub demo!")
    print("-" * 88)
```

```
    print(" This script creates a custom framework with all Security Hub
 controls.")
    print("-" * 88)
    sechub = SecurityHub(boto3.client("auditmanager"))
    am_controls = sechub.get_sechub_controls()
    sechub.create_custom_framework(am_controls)


if __name__ == "__main__":
    run_demo()
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Python (Boto3).
  - CreateAssessmentFramework
  - GetControl
  - ListControls

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteAWS Audit Manager Utilizándolo con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Cree un informe de evaluación de Audit Manager que contenga un día de pruebas utilizando un AWS SDK

En el siguiente ejemplo de código, se muestra cómo crear un informe de evaluación de Audit Manager con un día de evidencia.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import dateutil.parser
```

```
import logging
import time
import urllib.request
import uuid
import boto3
from botocore.exceptions import ClientError


logger = logging.getLogger(__name__)


class AuditReport:
    def __init__(self, auditmanager_client):
        self.auditmanager_client = auditmanager_client

    def get_input(self):
        print("-" * 40)
        try:
            assessment_id = input("Provide assessment id [uuid]: ").lower()
            try:
                assessment_uuid = uuid.UUID(assessment_id)
            except ValueError:
                logger.error("Assessment Id is not a valid UUID: %s",
 assessment_id)
                raise
            evidence_folder = input("Provide evidence date [yyyy-mm-dd]: ")
            try:
                evidence_date = dateutil.parser.parse(evidence_folder).date()
            except ValueError:
                logger.error("Invalid date : %s", evidence_folder)
                raise
            try:
                self.auditmanager_client.get_assessment(
                    assessmentId=str(assessment_uuid)
                )
            except ClientError:
                logger.exception("Couldn't get assessment %s.", assessment_uuid)
                raise
        except (ValueError, ClientError):
            return None, None
        else:
            return assessment_uuid, evidence_date

    def clear_staging(self, assessment_uuid, evidence_date):
```

```
        """
        Find all the evidence in the report and clear it.
        """
        next_token = None
        page = 1
        interested_folder_id_list = []
        while True:
            print(f"Page [{page}]")
            if next_token is None:
                folder_list = (
                    self.auditmanager_client.get_evidence_folders_by_assessment(
                        assessmentId=str(assessment_uuid), maxResults=1000
                    )
                )
            else:
                folder_list = (
                    self.auditmanager_client.get_evidence_folders_by_assessment(
                        assessmentId=str(assessment_uuid),
                        nextToken=next_token,
                        maxResults=1000,
                    )
                )
            folders = folder_list.get("evidenceFolders")
            print(f"Got {len(folders)} folders.")
            for folder in folders:
                folder_id = folder.get("id")
                if folder.get("name") == str(evidence_date):
                    interested_folder_id_list.append(folder_id)
                if folder.get("assessmentReportSelectionCount") == folder.get(
                    "totalEvidence"
                ):
                    print(
                        f"Removing folder from report selection :
{folder.get('name')} "
                        f"{folder_id} {folder.get('controlId')}"
                    )

self.auditmanager_client.disassociate_assessment_report_evidence_folder(
                        assessmentId=str(assessment_uuid),
evidenceFolderId=folder_id
                    )
                elif folder.get("assessmentReportSelectionCount") > 0:
                    # Get all evidence in the folder and
                    # add selected evidence in the selected_evidence_list.
```

```
                    evidence_list = (
                        self.auditmanager_client.get_evidence_by_evidence_folder(
                            assessmentId=str(assessment_uuid),
                            controlSetId=folder_id,
                            evidenceFolderId=folder_id,
                            maxResults=1000,
                        )
                    )
                    selected_evidence_list = []
                    for evidence in evidence_list.get("evidence"):
                        if evidence.get("assessmentReportSelection") == "Yes":
                            selected_evidence_list.append(evidence.get("id"))
                    print(
                        f"Removing evidence report selection :
{folder.get('name')} "
                        f"{len(selected_evidence_list)}"
                    )

self.auditmanager_client.batch_disassociate_assessment_report_evidence(
                        assessmentId=str(assessment_uuid),
                        evidenceFolderId=folder_id,
                        evidenceIds=selected_evidence_list,
                    )
            next_token = folder_list.get("nextToken")
            if not next_token:
                break
            page += 1
        return interested_folder_id_list

    def add_folder_to_staging(self, assessment_uuid, folder_id_list):
        print(f"Adding folders to report : {folder_id_list}")
        for folder in folder_id_list:
            self.auditmanager_client.associate_assessment_report_evidence_folder(
                assessmentId=str(assessment_uuid), evidenceFolderId=folder
            )

    def get_report(self, assessment_uuid):
        report = self.auditmanager_client.create_assessment_report(
            name="ReportViaScript",
            description="testing",
            assessmentId=str(assessment_uuid),
        )
        if self._is_report_generated(report.get("assessmentReport").get("id")):
            report_url = self.auditmanager_client.get_assessment_report_url(
```

```
                assessmentReportId=report.get("assessmentReport").get("id"),
                assessmentId=str(assessment_uuid),
            )
            print(report_url.get("preSignedUrl"))
            urllib.request.urlretrieve(
                report_url.get("preSignedUrl").get("link"),
                report_url.get("preSignedUrl").get("hyperlinkName"),
            )
            print(
                f"Report saved as
 {report_url.get('preSignedUrl').get('hyperlinkName')}."
            )
        else:
            print("Report generation did not finish in 15 minutes.")
            print(
                "Failed to download report. Go to the console and manually
 download "
                "the report."
            )

    def _is_report_generated(self, assessment_report_id):
        max_wait_time = 0
        while max_wait_time < 900:
            print(f"Checking status of the report {assessment_report_id}")
            report_list =
 self.auditmanager_client.list_assessment_reports(maxResults=1)
            if (
                report_list.get("assessmentReports")[0].get("id")
                == assessment_report_id
                and report_list.get("assessmentReports")[0].get("status") ==
 "COMPLETE"
            ):
                return True
            print("Sleeping for 5 seconds...")
            time.sleep(5)
            max_wait_time += 5


def run_demo():
    print("-" * 88)
    print("Welcome to the AWS Audit Manager samples demo!")
    print("-" * 88)
    print(
```

```
        "This script creates an assessment report for an assessment with all the
 "
        "evidence collected on the provided date."
    )
    print("-" * 88)

    report = AuditReport(boto3.client("auditmanager"))
    assessment_uuid, evidence_date = report.get_input()
    if assessment_uuid is not None and evidence_date is not None:
        folder_id_list = report.clear_staging(assessment_uuid, evidence_date)
        report.add_folder_to_staging(assessment_uuid, folder_id_list)
        report.get_report(assessment_uuid)


if __name__ == "__main__":
    run_demo()
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Python (Boto3).
  - AssociateAssessmentReportEvidenceFolder
  - BatchDisassociateAssessmentReportEvidence
  - CreateAssessmentReport
  - DisassociateAssessmentReportEvidenceFolder
  - GetAssessment
  - GetAssessmentReportUrl
  - GetEvidenceByEvidenceFolder
  - GetEvidenceFoldersByAssessment
  - ListAssessmentReports

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteAWS Audit Manager Utilizándolo con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Comprenda la seguridad y la protección de datos en AWS Audit Manager

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que se ejecuta Servicios de AWS en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento aplicables AWS Audit Manager, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y AWS servicios incluidos .
- Seguridad en la nube: su responsabilidad viene determinada por lo Servicio de AWS que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Audit Manager. En los siguientes temas, se le mostrará cómo configurar Audit Manager para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros Servicios de AWS que le ayuden a supervisar y proteger sus recursos de Audit Manager.

Temas

- Protección de datos en AWS Audit Manager
- Administración de identidad y acceso para AWS Audit Manager
- Validación de conformidad para AWS Audit Manager
- Comprender la resiliencia en AWS Audit Manager
- Seguridad de la infraestructura en AWS Audit Manager
- AWS Audit Manager y puntos finales de VPC de interfaz ()AWS PrivateLink
- Inicio de sesión y supervisión AWS Audit Manager
- Comprenda la configuración y el análisis de vulnerabilidades en AWS Audit Manager

Protección de datos en AWS Audit Manager

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Audit Manager. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Audit Manager u otro Servicios de

AWS mediante la consola, la API o AWS SDKs. AWS CLI Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Además de la recomendación anterior, recomendamos específicamente que los clientes de Audit Manager no incluyan información de identificación confidencial en los campos de formato libre al crear evaluaciones, controles personalizados, marcos personalizados y comentarios de las delegaciones.

Eliminación de datos de Audit Manager

Hay varias formas de eliminar los datos de Audit Manager.

Eliminación de datos al deshabilitar Audit Manager

Al deshabilitar Audit Manager, puede decidir si desea eliminar todos los datos de Audit Manager. Si decide eliminar sus datos, se eliminarán en un plazo de 7 días a partir de la desactivación de Audit Manager. Una vez eliminados los datos, no los puede recuperar.

Eliminación automática de datos

Algunos datos de Audit Manager se eliminan automáticamente después de un período de tiempo específico. Audit Manager conserva los datos de los clientes de la siguiente manera.

Tipo de datos:	Periodo de retención de datos	Notas
Evidencia	Los datos se conservan durante 2 años desde el momento de la creación	Incluye evidencias automatizadas y evidencias manuales
Recursos creados por los clientes	Los datos se conservan indefinidamente	Incluye evaluaciones, informes de evaluación, controles personalizados y marcos personalizados

Eliminación manual de datos

Puede eliminar recursos de Audit Manager individuales en cualquier momento. Para obtener instrucciones, consulte lo siguiente:

- Eliminar una evaluación en AWS Audit Manager
  - Consulte también: DeleteAssessmenten la referencia de la AWS Audit Manager API
- Eliminar un marco personalizado en AWS Audit Manager
  - Consulte también: DeleteAssessmentFrameworken la referencia de la AWS Audit Manager API
- Eliminación de solicitudes de uso compartido en AWS Audit Manager
  - Consulte también: DeleteAssessmentFrameworkShareen la referencia de la AWS Audit Manager API
- Eliminación de una ejecución de evaluación
  - Consulte también: DeleteAssessmentReporten la referencia de la AWS Audit Manager API
- Eliminar un control personalizado en AWS Audit Manager
  - Consulte también: DeleteControlen la referencia de la AWS Audit Manager API

Para eliminar otros datos de recursos que pueda haber creado al utilizar Audit Manager, consulte lo siguiente:

- Eliminar un almacén de datos de eventos en la Guía del usuario de AWS CloudTrail
- Eliminar un bucket en la Guía del usuario de Amazon Simple Storage Service (Amazon S3).

Cifrado en reposo

Para cifrar los datos en reposo, Audit Manager utiliza el cifrado del lado del servidor Claves administradas por AWS para todos sus registros y almacenes de datos.

Sus datos se cifran mediante una clave gestionada por el cliente o una Clave propiedad de AWS, según la configuración que haya seleccionado. Si no proporciona una clave gestionada por el cliente, Audit Manager utilizará una Clave propiedad de AWS para cifrar el contenido. Todos los metadatos de los servicios en DynamoDB y Amazon S3 en Audit Manager se cifran mediante una Clave propiedad de AWS.

Audit Manager cifra los datos de la siguiente manera:

- Los metadatos del servicio almacenados en Amazon S3 se cifran Clave propiedad de AWS mediante un SSE-KMS.
- Los metadatos del servicio almacenados en DynamoDB se cifran en el servidor mediante KMS y una Clave propiedad de AWS.
- El contenido almacenado en DynamoDB se cifra en el lado del cliente mediante una clave administrada por el cliente o una Clave propiedad de AWS. La clave KMS se basa en la configuración que haya elegido.
- El contenido almacenado en Amazon S3 en Audit Manager se cifra mediante SSE-KMS. La clave KMS se basa en su selección y puede ser una clave administrada por el cliente o una Clave propiedad de AWS.
- Los informes de evaluación publicados en su bucket de S3 se cifran de la siguiente manera:
  - Si ha proporcionado una clave administrada por el cliente, sus datos se cifran mediante SSE-KMS.
  - Si utilizó el Clave propiedad de AWS, sus datos se cifran mediante el SSE-S3.

Cifrado en tránsito

Audit Manager proporciona puntos de enlace seguros y privados para cifrar datos en tránsito. Los puntos finales seguros y privados permiten AWS proteger la integridad de las solicitudes de API a Audit Manager.

Tránsito entre servicios

De forma predeterminada, todas las comunicaciones entre servicios se protegen mediante el cifrado de seguridad de la capa de transporte (TLS).

Administración de claves

Audit Manager admite Claves propiedad de AWS tanto claves administradas por el cliente como para cifrar todos los recursos de Audit Manager (evaluaciones, controles, marcos, pruebas e informes de evaluación guardados en depósitos de S3 en sus cuentas).

Recomendamos utilizar una clave administrada por el cliente. De este modo, puede ver y administrar las claves de cifrado que protegen sus datos, incluida la visualización de los registros de su uso en AWS CloudTrail. Al elegir una clave administrada por el cliente, Audit Manager crea una concesión en la clave de KMS para que pueda usarse para cifrar su contenido.

> **Warning**
>
> Después de eliminar o desactivar una clave KMS que se utiliza para cifrar recursos del Audit Manager, ya no podrá descifrar el recurso que estaba cifrado bajo esa clave KMS, lo que significa que los datos se vuelven irrecuperables.
> Eliminar una clave de KMS en AWS Key Management Service (AWS KMS) es destructivo y potencialmente peligroso. Para obtener más información sobre la eliminación de claves de KMS, consulte Eliminar AWS KMS keys en la Guía del usuario de AWS Key Management Service .

Puede especificar la configuración de cifrado al habilitar Audit Manager mediante la AWS Management Console API Audit Manager o AWS Command Line Interface (AWS CLI). Para obtener instrucciones, consulte Habilitar AWS Audit Manager.

Puede revisar y cambiar la configuración de cifrado en cualquier momento. Para obtener instrucciones, consulte Configuración de los ajustes del cifrado de datos.

Para obtener más información sobre cómo configurar las claves administradas por el cliente, consulte Creación de claves en la Guía del usuario de AWS Key Management Service .

Administración de identidad y acceso para AWS Audit Manager

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Audit Manager. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- ¿Cómo AWS Audit Manager funciona con IAM
- Ejemplos de políticas basadas en la identidad para AWS Audit Manager
- Prevención de la sustitución confusa entre servicios

- Ejemplos de políticas basadas en recursos para AWS Audit Manager
- AWS políticas gestionadas para AWS Audit Manager
- Solución de problemas de AWS Audit Manager identidad y acceso
- Uso de funciones vinculadas a servicios para AWS Audit Manager

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en Audit Manager.

Usuario de servicio: si utiliza el servicio de Audit Manager para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Audit Manager para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a alguna característica de la administración de costos de Audit Manager, consulte Solución de problemas de AWS Audit Manager identidad y acceso.

Administrador de servicio: si está a cargo de los recursos de Audit Manager en su empresa, probablemente tenga acceso completo a Audit Manager. Su trabajo consiste en determinar a qué características y recursos de Audit Manager deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Audit Manager, consulte ¿Cómo AWS Audit Manager funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Audit Manager. Para consultar ejemplos de políticas de Audit Manager basadas en identidades que puede utilizar en IAM, consulte Ejemplos de políticas basadas en la identidad para AWS Audit Manager.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades

de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor AWS en IAM en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al

que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI

o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para

obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades

del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo AWS Audit Manager funciona con IAM

Antes de utilizar IAM para administrar el acceso a Audit Manager, conozca qué características de IAM se pueden utilizar con Audit Manager.

Funciones de IAM que puede utilizar con AWS Audit Manager

Característica de IAM	Compatibilidad Audit Manager
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de políticas	Parcial
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	No

Característica de IAM	Compatibilidad Audit Manager
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo AWS Audit Manager funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para AWS Audit Manager

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

AWS Audit Manager crea una política gestionada con el nombre `AWSAuditManagerAdministratorAccess` de los administradores de Audit Manager. Esta política otorga acceso administrativo completo a Audit Manager. Los administradores pueden adjuntar esta política a cualquier rol o usuario existente o crear un nuevo rol con esta política.

Políticas recomendadas para los usuarios de AWS Audit Manager

AWS Audit Manager le permite mantener la separación de funciones entre los diferentes usuarios y para las diferentes auditorías mediante el uso de diferentes políticas de IAM. Las dos personas de Audit Manager y sus políticas recomendadas se definen de la siguiente manera.

Persona	Descripción y política recomendada
Propietario de la auditoría	• Esta persona debe tener los permisos necesarios para gestionar las evaluaciones. AWS Audit Manager • La política que se recomienda usar para esta persona es la política administrada denominada AWSAuditManagerAdministratorAccess. Puede utilizar esta política como punto de partida y reducir estos permisos según sea necesario para que se ajusten a sus requisitos.
Delegado	• Esta persona puede acceder a los conjuntos de control delegados de una evaluación. Puede actualizar el estado del control, añadir comentarios, enviar un conjunto de controles para su revisión y añadir evidencias al informe de evaluación. • La política recomendada para esta persona es la siguiente política de ejemplo: Permita que la administración de los usuarios acceda a AWS Audit Manager. Puede utilizar esta política como punto de partida y realizar los cambios necesarios para adaptarlos a sus requisitos.

Ejemplos de políticas basadas en la identidad para AWS Audit Manager

Para ver ejemplos de políticas basadas en la identidad de Audit Manager, consulte Ejemplos de políticas basadas en la identidad para AWS Audit Manager.

Políticas basadas en recursos dentro AWS Audit Manager

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Aunque AWS Audit Manager no permite administrar las políticas basadas en recursos a través de IAM, el servicio implementa y administra internamente las políticas basadas en recursos en los dos escenarios siguientes:

- Cuando se asigna a los responsables de la auditoría una evaluación, se adjunta a la evaluación una política basada en los recursos, en la que el director es el propietario de la auditoría. Para obtener más información, consulte Paso 3: especificar los responsables de la auditoría y Paso 3: editar los responsables de la auditoría.
- Cuando se delega un conjunto de control de una evaluación, se adjunta al conjunto de controles una política basada en recursos en la que el director es el delegado. Para obtener más información, consulte Delegar un conjunto de controles para su revisión en AWS Audit Manager.

Acciones políticas para AWS Audit Manager

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de AWS Audit Manager acciones, consulte Acciones definidas por AWS Audit Manager en la Referencia de autorización de servicios.

Las acciones políticas AWS Audit Manager utilizan el siguiente prefijo antes de la acción.

```
auditmanager
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "auditmanager:GetEvidenceDetails",
      "auditmanager:GetEvidenceEventDetails"
         ]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Get`, incluya la siguiente acción.

```
"Action": "auditmanager:Get*"
```

Para ver ejemplos de políticas basadas en la identidad de Audit Manager, consulte Ejemplos de políticas basadas en la identidad para AWS Audit Manager.

Recursos de políticas para AWS Audit Manager

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de AWS Audit Manager recursos y sus ARNs correspondientes, consulte Recursos definidos por AWS Audit Manager en la Referencia de autorización de servicios. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recursos, consulte Acciones definidas por AWS Audit Manager.

Una evaluación de Audit Manager tiene el siguiente formato de Nombre de recurso de Amazon (ARN):

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Un conjunto de controles de Audit Manager tiene el siguiente formato de ARN:

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

Un control de Audit Manager tiene el siguiente formato de ARN:

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

Para obtener más información sobre el formato de ARNs, consulte Amazon Resource Names (ARNs).

Por ejemplo, para especificar la evaluación `i-1234567890abcdef0` en la instrucción, utilice el siguiente ARN.

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

Para especificar todas las instancias que pertenecen a una cuenta específica, utilice el carácter comodín (*).

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

Algunas acciones de Audit Manager, como las empleadas para la creación de recursos, no se pueden llevar a cabo en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

```
"Resource": "*"
```

En muchas acciones de la API de Audit Manager se utilizan varios recursos. Por ejemplo, `ListAssessments` devuelve una lista de metadatos de evaluación a los que pueden acceder las personas que hayan iniciado sesión actualmente Cuenta de AWS. Por lo tanto, un usuario debe tener permisos para ver las evaluaciones. Para especificar varios recursos en una sola sentencia, sepárelos ARNs con comas.

```
"Resource": [
      "resource1",
      "resource2"
```

Para ver una lista de los tipos de recursos de Audit Manager y sus tipos ARNs, consulte Recursos definidos por AWS Audit Manager en la Guía del usuario de IAM. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recursos, consulte Acciones definidas por AWS Audit Manager.

Algunas acciones de la API de Audit Manager admiten varios recursos. Por ejemplo, `GetChangeLogs` accede a un `assessmentID`, `controlID` y `controlSetId`, por lo tanto, una entidad principal debe tener permisos para acceder a cada uno de estos recursos. Para especificar varios recursos en una sola declaración, sepárelos ARNs con comas.

```
"Resource": [
      "assessmentId",
      "controlId",
      "controlSetId"
```

Claves de condición de la política para AWS Audit Manager

Compatibilidad con claves de condición de políticas específicas del servicio: parcial

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios

valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

Cuando la entidad principal de una declaración de política es una entidad principal del servicio de AWS, recomendamos encarecidamente que utilice las claves de condición globales `aws:SourceArn` o `aws:SourceAccount` en la política. Puede utilizar estas claves de contexto de condición global para evitar que se produzca una situación de subdirección confusa. Las siguientes políticas documentadas muestran cómo se pueden utilizar las claves contextuales de condición global `aws:SourceArn` y `aws:SourceAccount` en Audit Manager para evitar el problema del adjunto confundido.

- Ejemplo de política para un tema de SNS que se utiliza para las notificaciones de Audit Manager
- Ejemplo de política para una clave de KMS que se usa con un tema de SNS

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder a un usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de usuario. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

Audit Manager no proporciona ninguna clave de condición específica del servicio, pero sí admite el uso de algunas claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Listas de control de acceso (ACLs) en AWS Audit Manager

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos (ABAC) con AWS Audit Manager

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de

entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Para obtener más información sobre el etiquetado de AWS Audit Manager recursos, consulte. Recursos de etiquetado AWS Audit Manager

Uso de credenciales temporales con AWS Audit Manager

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda

generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para AWS Audit Manager

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en AWSél, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para AWS Audit Manager

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de AWS Audit Manager . Edite los roles de servicio solo cuando Audit Manager proporcione orientación para hacerlo.

Funciones vinculadas al servicio para AWS Audit Manager

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre las funciones vinculadas al servicio, consulte. AWS Audit ManagerUso de funciones vinculadas a servicios para AWS Audit Manager

Ejemplos de políticas basadas en la identidad para AWS Audit Manager

De forma predeterminada, los usuarios y roles no tienen permiso para crear o modificar recursos del Audit Manager. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AWS Audit Manager, incluido el ARNs formato de cada uno de los tipos de recursos, consulte las claves de condición, recursos y acciones de AWS Audit Manager en la Referencia de autorización de servicios.

Contenido

- Prácticas recomendadas sobre las políticas
- Permita los permisos mínimos necesarios para activar Audit Manager
- Permitir a los usuarios acceso de administrador total a AWS Audit Manager
  - Ejemplo 1 (política gestionada, AWSAuditManagerAdministratorAccess)
  - Ejemplo 2 (permisos de destino del informe de evaluación)
  - Ejemplo 3 (Permisos para habilitar el buscador de pruebas)
  - Ejemplo 4 (Permisos para deshabilitar el buscador de pruebas)
- Permita que la administración de los usuarios acceda a AWS Audit Manager
- Permita a los usuarios el acceso de solo lectura a AWS Audit Manager
- Cómo permitir a los usuarios consultar sus propios permisos
- AWS Audit Manager Permitir el envío de notificaciones a los temas de Amazon SNS
  - Ejemplo 1 (Permisos para el tema SNS)
  - Ejemplo 2 (permisos para la clave de KMS que se adjunta al tema de SNS)
- Permita a los usuarios realizar consultas de búsqueda en el buscador de evidencias

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Audit Manager de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos en muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la

MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Permita los permisos mínimos necesarios para activar Audit Manager

En este ejemplo se muestra cómo puede permitir que se habiliten cuentas sin función de administrador para habilitar AWS Audit Manager.

> **Note**
>
> Lo que ofrecemos aquí es una política básica que concede los permisos mínimos necesarios para activar Audit Manager. Todos los permisos de la política siguiente son obligatorios. Si omite alguna parte de esta política, no podrá habilitar Audit Manager.
> Le recomendamos que dedique un tiempo a personalizar sus permisos para que se adapten a sus necesidades específicas. Si necesita ayuda, póngase en contacto con su administrador o con AWS Support.

Para conceder el acceso mínimo necesario para activar Audit Manager, utilice los siguientes permisos.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "auditmanager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
```

```
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                   ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
}
```

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API o a la AWS CLI API. AWS En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Permitir a los usuarios acceso de administrador total a AWS Audit Manager

Los siguientes ejemplos de políticas otorgan acceso de administrador total a AWS Audit Manager.

- Ejemplo 1 (política gestionada, `AWSAuditManagerAdministratorAccess`)
- Ejemplo 2 (permisos de destino del informe de evaluación)
- Ejemplo 3 (Permisos para habilitar el buscador de pruebas)
- Ejemplo 4 (Permisos para deshabilitar el buscador de pruebas)

Ejemplo 1 (política gestionada, **`AWSAuditManagerAdministratorAccess`**)

La AWSAuditManagerAdministratorAccesspolítica incluye la capacidad de activar y desactivar Audit Manager, la posibilidad de cambiar la configuración de Audit Manager y la capacidad de gestionar todos los recursos del Audit Manager, como las evaluaciones, los marcos, los controles y los informes de evaluación.

Ejemplo 2 (permisos de destino del informe de evaluación)

Esta política le concede permiso para acceder a un bucket de S3 específico y para añadir y eliminar archivos de él. Esto le permite utilizar el bucket especificado como destino del informe de evaluación en Audit Manager.

Reemplace los *`placeholder text`* con su propia información. Incluya el bucket de S3 que utiliza como destino del informe de evaluación y la clave KMS que utiliza para cifrar los informes de evaluación.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "s3:PutObject",
```

```
                "s3:GetObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:GetBucketLocation",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
        }
    ]
},
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

Ejemplo 3 (Permisos para habilitar el buscador de pruebas)

Se requiere la siguiente política de permisos si desea activar y utilizar la característica de búsqueda de evidencias. Esta declaración de política permite a Audit Manager crear un banco de datos de eventos de CloudTrail Lake y ejecutar consultas de búsqueda.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Sid": "ManageCloudTrailLakeQueryAccess",
           "Effect": "Allow",
           "Action": [
```

```
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
        },
        {
            "Sid": "ManageCloudTrailLakeAccess",
            "Effect": "Allow",
            "Action": [
                 "cloudtrail:CreateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
         }
    ]
}
```

Ejemplo 4 (Permisos para deshabilitar el buscador de pruebas)

Este ejemplo de política otorga permiso para deshabilitar la característica de búsqueda de evidencias en Audit Manager. Esto implica eliminar el almacén de datos de eventos que se creó cuando habilitó la característica por primera vez.

Antes de usar esta política, *`placeholder text`* sustitúyala por tu propia información. Debe especificar el UUID del almacén de datos de eventos que se creó al activar el buscador de evidencias. Puede recuperar el ARN del almacén de datos de eventos desde la configuración de Audit Manager. Para obtener más información, consulta GetSettings en la AWS Audit Manager Referencia de la API de .

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DeleteEventDataStore",
                "cloudtrail:UpdateEventDataStore"
            ],
```

```
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
}
```

Permita que la administración de los usuarios acceda a AWS Audit Manager

En este ejemplo se muestra cómo puede permitir el acceso de administración de no administradores a AWS Audit Manager.

Esta política permite gestionar todos los recursos de Audit Manager (evaluaciones, marcos y controles), pero no permite activar o desactivar Audit Manager ni modificar la configuración del Audit Manager.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:AssociateAssessmentReportEvidenceFolder",
                "auditmanager:BatchAssociateAssessmentReportEvidence",
                "auditmanager:BatchCreateDelegationByAssessment",
                "auditmanager:BatchDeleteDelegationByAssessment",
                "auditmanager:BatchDisassociateAssessmentReportEvidence",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:CreateAssessment",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:CreateAssessmentReport",
                "auditmanager:CreateControl",
                "auditmanager:DeleteControl",
                "auditmanager:DeleteAssessment",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:DeleteAssessmentFrameworkShare",
                "auditmanager:DeleteAssessmentReport",
                "auditmanager:DisassociateAssessmentReportEvidenceFolder",
                "auditmanager:GetAccountStatus",
                "auditmanager:GetAssessment",
```

```
                "auditmanager:GetAssessmentFramework",
                "auditmanager:GetControl",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:GetAssessmentReportUrl",
                "auditmanager:GetChangeLogs",
                "auditmanager:GetDelegations",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder",
                "auditmanager:GetEvidenceFileUploadUrl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidenceFoldersByAssessment",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:GetInsights",
                "auditmanager:GetInsightsByAssessment",
                "auditmanager:GetOrganizationAdminAccount",
                "auditmanager:ListAssessments",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListControls",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:ListNotifications",
                "auditmanager:ListAssessmentControlInsightsByControlDomain",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:ListAssessmentFrameworkShareRequests",
                "auditmanager:ListControlDomainInsights",
                "auditmanager:ListControlDomainInsightsByAssessment",
                "auditmanager:ListControlInsightsByControlDomain",
                "auditmanager:ListTagsForResource",
                "auditmanager:StartAssessmentFrameworkShare",
                "auditmanager:TagResource",
                "auditmanager:UntagResource",
                "auditmanager:UpdateControl",
                "auditmanager:UpdateAssessment",
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:UpdateAssessmentFrameworkShare",
                "auditmanager:UpdateAssessmentStatus",
                "auditmanager:ValidateAssessmentReportIntegrity"
            ],
            "Resource": "*"
        },
        {
    "Sid": "ControlCatalogAccess",
```

```
      "Effect": "Allow",
      "Action": [
   "controlcatalog:ListCommonControls",
   "controlcatalog:ListDomains",
   "controlcatalog:ListObjectives"
      ],
      "Resource": "*"
         },
         {
             "Sid": "OrganizationsAccess",
             "Effect": "Allow",
             "Action": [
                 "organizations:ListAccountsForParent",
                 "organizations:ListAccounts",
                 "organizations:DescribeOrganization",
                 "organizations:DescribeOrganizationalUnit",
                 "organizations:DescribeAccount",
                 "organizations:ListParents",
                 "organizations:ListChildren"
             ],
             "Resource": "*"
         },
         {
             "Sid": "IAMAccess",
             "Effect": "Allow",
             "Action": [
                 "iam:GetUser",
                 "iam:ListUsers",
                 "iam:ListRoles"
             ],
             "Resource": "*"
         },
         {
             "Sid": "S3Access",
             "Effect": "Allow",
             "Action": [
                 "s3:ListAllMyBuckets"
             ],
             "Resource": "*"
         },
         {
             "Sid": "KmsAccess",
             "Effect": "Allow",
             "Action": [
```

```
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Permita a los usuarios el acceso de solo lectura a AWS Audit Manager

Esta política otorga acceso de solo lectura a AWS Audit Manager recursos como evaluaciones, marcos y controles.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:Get*",
                "auditmanager:List*"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

AWS Audit Manager Permitir el envío de notificaciones a los temas de Amazon SNS

Las políticas de este ejemplo conceden a Audit Manager permisos para enviar notificaciones a un tema de Amazon SNS existente.

- Ejemplo 1: si desea recibir notificaciones de Audit Manager, utilice este ejemplo para añadir permisos a la política de acceso a los temas de SNS.
- Ejemplo 2: Si su tema de SNS utiliza AWS Key Management Service (AWS KMS) para el cifrado del lado del servidor (SSE), utilice este ejemplo para añadir permisos a la política de acceso a claves de KMS.

En el siguiente ejemplo de política, la entidad principal que obtiene los permisos es la entidad principal del servicio Audit Manager, que es `auditmanager.amazonaws.com`. Cuando la entidad principal de una declaración de política es una entidad principal del servicio de AWS, recomendamos encarecidamente que utilice las claves de condición globales `aws:SourceArn` o `aws:SourceAccount` en la política. Puede utilizar estas claves de contexto de condición global para evitar que se produzca una situación de subdirección confusa.

Ejemplo 1 (Permisos para el tema SNS)

Esta declaración de política permite a Audit Manager publicar eventos en el tema SNS especificado. Cualquier solicitud de publicación sobre el tema de SNS especificado debe cumplir las condiciones de la política.

Antes de usar esta política, sustitúyala por tu *`placeholder text`* propia información. Tome nota de lo siguiente:

- Si utiliza la clave de condición `aws:SourceArn` en esta política, el valor debe ser el ARN del recurso Audit Manager del que proviene la notificación. En el ejemplo siguiente, `aws:SourceArn` utiliza un comodín (`*`) como identificador del recurso. Esto permite todas las solicitudes que provienen de Audit Manager en todos los recursos de Audit Manager. Con la clave de condición global `aws:SourceArn`, puede utilizar el operador de condición `StringLike` o `ArnLike`. La práctica recomendada consiste en utilizar `ArnLike`.

- Si utiliza la clave de condición `aws:SourceAccount`, puede utilizar el operador de condición `StringEquals` o `StringLike`. La práctica recomendada consiste en usar `StringEquals` para implementar privilegios mínimos.
- Si utiliza ambos `aws:SourceAccount` y `aws:SourceArn`, los valores de la cuenta deben mostrar el mismo ID de cuenta.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
      "Sid": "AllowAuditManagerToUseSNSTopic",
      "Effect": "Allow",
      "Principal": {
        "Service": ".amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:accountID:topicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws::region:accountID:*"
        }
      }
    }
}
```

El siguiente ejemplo alternativo usa solo la clave de condición `aws:SourceArn`, con el operador de condición `StringLike`:

```
"Condition": {
  "StringLike": {
    "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
  }
}
```

El siguiente ejemplo alternativo usa solo la clave de condición `aws:SourceAccount`, con el operador de condición `StringLike`:

```
"Condition": {
  "StringLike": {
    "aws:SourceAccount": "accountID"
   }
 }
```

Ejemplo 2 (permisos para la clave de KMS que se adjunta al tema de SNS)

Esta declaración de política permite a Audit Manager utilizar la clave KMS para generar la clave de datos que utiliza para cifrar un tema SNS. Cualquier solicitud de uso de la clave KMS para la operación especificada debe cumplir las condiciones de la política.

Antes de usar esta política, *`placeholder text`* sustitúyala por tu propia información. Tome nota de lo siguiente:

- Si usa la clave de condición `aws:SourceArn` en esta política, el valor debe ser el ARN del recurso que se está cifrando. Por ejemplo, en este caso, es el tema del SNS de su cuenta. Establezca el valor en el ARN o un patrón ARN con caracteres comodín (`*`). Con la clave de condición `aws:SourceArn`, puede utilizar el operador de condición `StringLike` o `ArnLike`. La práctica recomendada consiste en utilizar `ArnLike`.
- Si utiliza la clave de condición `aws:SourceAccount`, puede utilizar el operador de condición `StringEquals` o `StringLike`. La práctica recomendada consiste en usar `StringEquals` para implementar privilegios mínimos. Puede usar `aws:SourceAccount` si no conoce el ARN del tema de SNS.
- Si utiliza ambos `aws:SourceAccount` y `aws:SourceArn`, los valores de la cuenta deben mostrar el mismo ID de cuenta.

JSON

```
{
     "Version": "2012-10-17",
     "Statement": {
       "Sid": "AllowAuditManagerToUseKMSKey",
       "Effect": "Allow",
       "Principal": {
```

```
            "Service": ".amazonaws.com"
        },
        "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": "arn:aws:kms:region:accountID:key/*",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "accountID"
             }
             "ArnLike": {
                 "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
             }
       }
     }
   ]
 }
```

El siguiente ejemplo alternativo usa solo la clave de condición `aws:SourceArn`, con el operador de condición `StringLike`:

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
        }
      }
```

El siguiente ejemplo alternativo usa solo la clave de condición `aws:SourceAccount`, con el operador de condición `StringLike`:

```
    "Condition": {
      "StringLike": {
       "aws:SourceAccount": "accountID"
      }
     }
```

Permita a los usuarios realizar consultas de búsqueda en el buscador de evidencias

La siguiente política otorga permisos para realizar consultas en un banco de datos de eventos de CloudTrail Lake. Esta política de permisos es necesaria si desea utilizar la característica de búsqueda de pruebas.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageCloudTrailLakeQueryAccess",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puedes producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio de llamadas puede ser manipulado para utilizar sus permisos para actuar sobre los recursos de otro cliente cuando no tiene permiso para hacerlo. Para evitarlo, Amazon Web Services proporciona herramientas que le ayudan a proteger sus datos en todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Recomendamos utilizar las claves de contexto de condición `aws:SourceAccount`global `aws:SourceArn`y las claves de contexto en las políticas de recursos para limitar los permisos que se AWS Audit Manager conceden a otro servicio para acceder a sus recursos.

- Utiliza `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. También puede utilizar `aws:SourceArn` con un comodín (`*`) si desea especificar varios recursos.

  Por ejemplo: puede utilizar un tema de Amazon SNS para recibir notificaciones de actividad de Audit Manager. En este caso, en la política de acceso al tema de SNS, el valor ARN de `aws:SourceArn` es el recurso Audit Manager del que proviene la notificación. Como es probable que tenga varios recursos de Audit Manager, le recomendamos que utilice `aws:SourceArn` con un comodín. Esto le permite especificar todos los recursos de Audit Manager en su política de acceso a los temas de SNS.
- Utiliza `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.
- Si el valor de `aws:SourceArn` no contiene el ID de cuenta, como un ARN de bucket de Amazon S3, debe utilizar ambas claves de contexto de condición global para limitar los permisos.
- Si utiliza las dos condiciones y el valor `aws:SourceArn` contiene el ID de la cuenta, el valor `aws:SourceAccount` y la cuenta del valor `aws:SourceArn` deben mostrar el mismo ID de cuenta cuando se empleen en la misma instrucción de política.
- La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el Nombre de recurso de Amazon (ARN) completo del recurso o si está especificando varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con caracteres comodines (`*`) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:servicename:*:123456789012:*`.

Audit Manager confundió al soporte adjunto

Audit Manager proporciona un soporte adjunto confuso en los siguientes escenarios. Estos ejemplos de políticas muestran cómo se pueden utilizar las claves de condición `aws:SourceArn` y `aws:SourceAccount` para evitar el problema del suplente confuso.

- Política de ejemplo: el tema de SNS que utiliza para recibir las notificaciones de Audit Manager
- Ejemplo de política: la clave de KMS que se utiliza para cifrar el tema de SNS

Audit Manager no proporciona un soporte adjunto confuso para la clave administrada por el cliente que usted proporciona en la configuración Configuración de los ajustes del cifrado de datos de Audit Manager. Si ha proporcionado su propia clave administrada por el cliente, no puede usar las condiciones `aws:SourceAccount` ni `aws:SourceArn` en esa política de claves de KMS.

Ejemplos de políticas basadas en recursos para AWS Audit Manager

Política de buckets de Amazon S3

La siguiente política permite CloudTrail enviar los resultados de las consultas del buscador de evidencias al bucket S3 especificado. Como práctica recomendada de seguridad, la clave de condición global de IAM `aws:SourceArn` ayuda a garantizar que solo se CloudTrail escriba en el depósito de S3 para el almacén de datos de eventos.

> **Important**
>
> Debe especificar un bucket de S3 para la entrega de los resultados de las consultas de CloudTrail Lake. Para obtener más información, consulte Especificar un depósito existente para los resultados de la consulta de CloudTrail Lake.

*`placeholder text`*Sustitúyala por tu propia información, de la siguiente manera:

- *`amzn-s3-demo-destination-bucket`*Sustitúyalo por el depósito S3 que utiliza como destino de exportación.
- *`myQueryRunningRegion`*Sustitúyalo por el apropiado Región de AWS para su configuración.
- *`myAccountID`*Sustitúyalo por el Cuenta de AWS identificador para el que se utiliza CloudTrail. Puede que no sea el mismo que el Cuenta de AWS ID del bucket de S3. Si se trata de un almacén de datos de eventos de la organización, debe utilizar la Cuenta de AWS para la cuenta de administración.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket",
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
"arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
"arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        }
    ]
    }
```

AWS Key Management Service política

Si su bucket de S3 tiene el cifrado predeterminado establecido CloudTrail en`SSE-KMS`, concédale acceso a la política de recursos de su AWS Key Management Service clave para que pueda usarla. En este caso, añada la siguiente política de recursos a la AWS KMS clave.

JSON

```
{
 "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS políticas gestionadas para AWS Audit Manager

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Temas

- AWS política gestionada: AWSAudit ManagerAdministratorAccess
- AWS política gestionada: AWSAudit ManagerServiceRolePolicy
- AWS Audit Manager actualizaciones de las políticas AWS gestionadas

AWS política gestionada: AWSAudit ManagerAdministratorAccess

Puede adjuntar la política `AWSAuditManagerAdministratorAccess` a las identidades de IAM.

Esta política otorga permisos administrativos que permiten el acceso total de la administración a AWS Audit Manager. Este acceso incluye la capacidad de habilitar y deshabilitar AWS Audit Manager, cambiar la configuración y administrar todos los recursos de Audit Manager AWS Audit Manager, como las evaluaciones, los marcos, los controles y los informes de evaluación.

AWS Audit Manager requiere amplios permisos en varios AWS servicios. Esto se debe a que AWS Audit Manager se integra con varios AWS servicios para recopilar pruebas automáticamente de Cuenta de AWS los servicios incluidos en el ámbito de una evaluación.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `Audit Manager`: Permite a las entidades principales tener plenos permisos sobre los recursos AWS Audit Manager .
- `Organizations`: Permite a las entidades principales enumerar las cuentas y las unidades organizativas y registrar o anular el registro de un administrador delegado. Esto es necesario para poder habilitar la compatibilidad con varias cuentas y poder AWS Audit Manager realizar evaluaciones en varias cuentas y consolidar las pruebas en una cuenta de administrador delegado.

- `iam`: Permite a las entidades principales obtener y enumerar los usuarios en IAM y crear un rol vinculado al servicio. Esto es necesario para poder designar a los responsables y delegados de la auditoría para una evaluación. Esta política también permite a las entidades principales eliminar el rol vinculado al servicio y recuperar el estado de eliminación. Esto es necesario para AWS Audit Manager poder limpiar los recursos y eliminar el rol vinculado al servicio si decide deshabilitar el servicio en el. AWS Management Console
- `s3`: Permite a las entidades principales enumerar los buckets de Amazon Simple Storage Service (Amazon S3) disponibles. Esta capacidad es necesaria para que pueda designar el bucket de S3 en el que desea almacenar los informes de evidencias o cargar las evidencias manualmente.
- `kms`: Permite a las entidades principales enumerar y describir claves, enumerar alias y crear concesiones. Esto es necesario para que pueda elegir las claves administradas por el cliente para el cifrado de datos.
- `sns`: Permite a las entidades principales publicar temas de suscripción en Amazon SNS. Esto es necesario para que pueda especificar a qué tema de SNS quiere que AWS Audit Manager envíe las notificaciones.
- `events`— Permite a los directores enumerar y gestionar los cheques desde. AWS Security Hub Esto es necesario para AWS Audit Manager poder recopilar automáticamente AWS Security Hub los resultados de los AWS servicios que supervisan. AWS Security Hub A continuación, puede convertir estos datos en evidencias para incluirlas en sus evaluaciones AWS Audit Manager .
- `tag`: Permite a las entidades principales recuperar los recursos etiquetados. Esto es necesario para poder utilizar las etiquetas como filtro de búsqueda al explorar los marcos, los controles y las evaluaciones AWS Audit Manager.
- `controlcatalog`— Permite a los directores enumerar los dominios, los objetivos y los controles comunes que proporciona AWS Control Catalog. Esto es necesario para que se pueda utilizar la característica de controles comunes en AWS Audit Manager. Con estos permisos establecidos, puede ver una lista de los controles más comunes en la biblioteca de AWS Audit Manager controles y filtrar los controles por dominio y objetivo. También puede utilizar los controles comunes como origen de evidencia al crear un control personalizado.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
```

```
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
     "Sid": "ControlCatalogAccess",
     "Effect": "Allow",
     "Action": [
  "controlcatalog:ListCommonControls",
  "controlcatalog:ListDomains",
  "controlcatalog:ListObjectives"
     ],
     "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AWSAudit ManagerServiceRolePolicy

No puede asociar `AWSAuditManagerServiceRolePolicy` a sus entidades IAM. Esta política está asociada a un rol vinculado al servicio`AWSServiceRoleForAuditManager`, que permite AWS Audit Manager realizar acciones en su nombre. Para obtener más información, consulte Uso de funciones vinculadas a servicios para AWS Audit Manager.

La política de permisos de funciones, `AWSAuditManagerServiceRolePolicy`, permite que AWS Audit Manager recopile evidencias automatizadas haciendo lo siguiente en su nombre:

- Recopilar datos de las siguientes fuentes de datos:
  - Eventos de gestión desde AWS CloudTrail
  - Comprobaciones de cumplimiento de Reglas de AWS Config
  - Controles de conformidad de AWS Security Hub
- Utilice las llamadas a la API para describir las configuraciones de sus recursos para los siguientes Servicios de AWS.

> **Tip**
>
> Para obtener más información sobre las llamadas a la API que Audit Manager utiliza para recopilar evidencias de estos servicios, consulte Se admiten llamadas a la API para orígenes de datos de control personalizadas en esta guía.

  - Amazon API Gateway
  - AWS Backup
  - Amazon Bedrock
  - AWS Certificate Manager
  - Amazon CloudFront
  - AWS CloudTrail
  - Amazon CloudWatch
  - Amazon CloudWatch Logs
  - Grupos de usuarios de Amazon Cognito
  - AWS Config
  - Amazon Data Firehose
  - AWS Direct Connect
  - Amazon DynamoDB
  - Amazon EC2
  - Amazon EC2 Auto Scaling
  - Amazon Elastic Container Service

- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Elastic Load Balancing
- Amazon EMR
- Amazon EventBridge
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (YO SOY)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Transmisión gestionada de Amazon para Apache Kafka
- OpenSearch Servicio Amazon
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- Amazon SageMaker AI
- AWS Secrets Manager
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

Detalles de los permisos

~~`AWSAuditManagerServiceRolePolicy`permite AWS Audit Manager realizar las siguientes~~ acciones en los recursos especificados:

- acm:GetAccountConfiguration
- acm:ListCertificates
- apigateway:GET
- autoscaling:DescribeAutoScalingGroups
- backup:ListBackupPlans
- backup:ListRecoveryPointsByResource
- bedrock:GetCustomModel
- bedrock:GetFoundationModel
- bedrock:GetModelCustomizationJob
- bedrock:GetModelInvocationLoggingConfiguration
- bedrock:ListCustomModels
- bedrock:ListFoundationModels
- bedrock:ListGuardrails
- bedrock:ListModelCustomizationJobs
- cloudfront:GetDistribution
- cloudfront:GetDistributionConfig
- cloudfront:ListDistributions
- cloudtrail:DescribeTrails
- cloudtrail:GetTrail
- cloudtrail:ListTrails
- cloudtrail:LookupEvents
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways

- directconnect:DescribeVirtualGateways
- dynamodb:DescribeBackup
- dynamodb:DescribeContinuousBackups
- dynamodb:DescribeTable
- dynamodb:DescribeTableReplicaAutoScaling
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations

- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules

- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupsForUser
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders

- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy

- `rds:DescribeCertificates`
- `rds:DescribeDBClusterEndpoints`
- `rds:DescribeDBClusterParameterGroups`
- `rds:DescribeDBClusters`
- `rds:DescribeDBInstances`
- `rds:DescribeDBInstanceAutomatedBackups`
- `rds:DescribeDBSecurityGroups`
- `redshift:DescribeClusters`
- `redshift:DescribeClusterSnapshots`
- `redshift:DescribeLoggingStatus`
- `route53:GetQueryLoggingConfig`
- `s3:GetBucketAcl`
- `s3:GetBucketLogging`
- `s3:GetBucketOwnershipControls`
- `s3:GetBucketPolicy`
  - Esta acción de la API opera dentro del ámbito de Cuenta de AWS donde service-linked-role esté disponible. No puede acceder a las políticas de bucket entre cuentas.
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketTagging`
- `s3:GetBucketVersioning`
- `s3:GetEncryptionConfiguration`
- `s3:GetLifecycleConfiguration`
- `s3:ListAllMyBuckets`
- `sagemaker:DescribeAlgorithm`
- `sagemaker:DescribeDomain`
- `sagemaker:DescribeEndpoint`
- `sagemaker:DescribeEndpointConfig`
- `sagemaker:DescribeFlowDefinition`
- `sagemaker:DescribeHumanTaskUi`
- `sagemaker:DescribeLabelingJob`

- sagemaker:DescribeModel
- sagemaker:DescribeModelBiasJobDefinition
- sagemaker:DescribeModelCard
- sagemaker:DescribeModelQualityJobDefinition
- sagemaker:DescribeTrainingJob
- sagemaker:DescribeUserProfile
- sagemaker:ListAlgorithms
- sagemaker:ListDomains
- sagemaker:ListEndpointConfigs
- sagemaker:ListEndpoints
- sagemaker:ListFlowDefinitions
- sagemaker:ListHumanTaskUis
- sagemaker:ListLabelingJobs
- sagemaker:ListModels
- sagemaker:ListModelBiasJobDefinitions
- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions
- sagemaker:ListMonitoringAlerts
- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets
- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:GetRule
- waf-regional:GetWebAcl

- waf-regional:ListRuleGroups
- waf-regional:ListRules
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:GetRule
- waf:GetRuleGroup
- waf:ListActivatedRulesInRuleGroup
- waf:ListRuleGroups
- waf:ListRules
- waf:ListWebAcls
- wafv2:ListWebAcls

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "autoscaling:DescribeAutoScalingGroups",
    "backup:ListBackupPlans",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
    "bedrock:ListGuardrails",
    "bedrock:ListModelCustomizationJobs",
    "cloudfront:GetDistribution",
    "cloudfront:GetDistributionConfig",
    "cloudfront:ListDistributions",
    "cloudtrail:GetTrail",
```

```
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTable",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:GetLaunchTemplateData",
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecs:DescribeClusters",
        "eks:DescribeAddonVersions",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServiceUpdates",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSslPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListSecurityConfigurations",
        "events:DescribeRule",
        "events:ListConnections",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRules",
        "firehose:ListDeliveryStreams",
        "fsx:DescribeFileSystems",
        "guardduty:ListDetectors",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccessKeyLastUsed",
        "iam:GetCredentialReport",
        "iam:GetGroupPolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupsForUser",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListOpenIdConnectProviders",
        "iam:ListPolicies",
```

```
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSamlProviders",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListAccessKeys",
        "iam:ListAttachedRolePolicies",
        "iam:ListMfaDeviceTags",
        "iam:ListMfaDevices",
        "kafka:ListClusters",
        "kafka:ListKafkaVersions",
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "license-manager:ListAssociationsForLicenseConfiguration",
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListUsageForLicenseConfiguration",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "es:DescribeDomains",
        "es:DescribeDomain",
        "es:DescribeDomainConfig",
        "es:ListDomainNames",
        "organizations:DescribeOrganization",
        "organizations:DescribePolicy",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
```

```
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeLoggingStatus",
        "route53:GetQueryLoggingConfig",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListModels",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListUserProfiles",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:ListAllMyBuckets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "securityhub:DescribeStandards",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:ListQueues",
        "waf-regional:GetRule",
```

```
    "waf-regional:GetWebAcl",
    "waf:GetRule",
    "waf:GetRuleGroup",
    "waf:ListActivatedRulesInRuleGroup",
    "waf:ListWebAcls",
    "wafv2:ListWebAcls",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf-regional:ListRules",
    "waf:ListRuleGroups",
    "waf:ListRules"
   ],
   "Resource": "*",
   "Sid": "APIsAccess"
  },
  {
   "Sid": "S3Access",
   "Effect": "Allow",
   "Action": [
    "s3:GetBucketAcl",
    "s3:GetBucketLogging",
    "s3:GetBucketOwnershipControls",
    "s3:GetBucketPolicy",
    "s3:GetBucketTagging"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${aws:PrincipalAccount}"
     ]
    }
   }
  },
  {
   "Sid": "APIGatewayAccess",
   "Effect": "Allow",
   "Action": [
    "apigateway:GET"
   ],
   "Resource": [
    "arn:aws:apigateway:*::/restapis",
```

```
    "arn:aws:apigateway:*::/restapis/*/stages/*",
    "arn:aws:apigateway:*::/restapis/*/stages"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${aws:PrincipalAccount}"
     ]
    }
   }
  },
  {
   "Sid": "CreateEventsAccess",
   "Effect": "Allow",
   "Action": [
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
   "Condition": {
    "StringEquals": {
     "events:detail-type": "Security Hub Findings - Imported"
    },
    "Null": {
     "events:source": "false"
    },
    "ForAllValues:StringEquals": {
     "events:source": [
      "aws.securityhub"
     ]
    }
   }
  },
  {
   "Sid": "EventsAccess",
   "Effect": "Allow",
   "Action": [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
```

```
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
   }
  ]
}
```

AWS Audit Manager actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS Audit Manager desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS Audit Manager documento.

Cambio	Descripción	Fecha
AWSAuditManagerServiceRolePolicy: actualización de una política actual	El rol vinculado al servicio ahora permite AWS Audit Manager realizar la `bedrock:ListGuardrails` acción. Esta acción de la API es necesaria para respaldar el AWS Marco generativo de mejores prácticas de IA, versión 2. Permite a Audit Manager recopilar evidencias automatizadas sobre las barreras de protección establecidas para los conjuntos de datos de entrenamiento de datos de modelos de IA generativa.	24/09/2024
AWSAuditManagerServiceRolePolicy: actualización de una política actual	Hemos añadido los siguientes permisos a. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager ahora puede realizar las siguientes acciones para recopilar pruebas automatizadas sobre los recursos de su propiedad Cuenta de AWS. • `sagemaker:DescribeAlgorithm` • `sagemaker:DescribeDomain` • `sagemaker:DescribeEndpoint`	06/10/2024

Cambio	Descripción	Fecha
	• sagemaker:DescribeFlowDefinition • sagemaker:DescribeHumanTaskUi • sagemaker:DescribeLabelingJob • sagemaker:DescribeModel • sagemaker:DescribeModelBiasJobDefinition • sagemaker:DescribeModelCard • sagemaker:DescribeModelQualityJobDefinition • sagemaker:DescribeTrainingJob • sagemaker:DescribeUserProfile • sagemaker:ListAlgorithms • sagemaker:ListDomains • sagemaker:ListEndpoints • sagemaker:ListFlowDefinitions • sagemaker:ListHumanTaskUis • sagemaker:ListLabelingJobs • sagemaker:ListModels • sagemaker:ListModelBiasJobDefinitions • sagemaker:ListModelCards • sagemaker:ListModelQualityJobDefinitions • sagemaker:ListMonitoringAlerts • sagemaker:ListMonitoringSchedules • sagemaker:ListTrainingJobs • sagemaker:ListUserProfiles	

Cambio	Descripción	Fecha
AWSAuditManagerServiceRolePolicy: actualización de una política actual	Hemos añadido los siguientes permisos a. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager ahora puede realizar las siguientes acciones para recopilar pruebas automatizadas sobre los recursos de su propiedad Cuenta de AWS. • `iam:ListAttachedGroupPolicies` • `iam:ListAttachedUserPolicies` • `iam:ListGroupsForUser` • `es:ListDomainNames` También hemos añadido un nuevo recurso en la sección `APIGatewayAccess` de la política (`arn:aws:apigateway:*::/restapis`). La política ahora concede el permiso especificado (en este caso, la `apigateway:GET` acción) no solo en las etapas y los recursos de etapa de API Gateway REST APIs, sino también en las APIs propias REST. Este cambio amplía de manera efectiva el alcance de la política para incluir la capacidad de recuperar información sobre el REST de API Gateway en APIs sí, además de las etapas y los recursos de etapa asociados a ellas APIs.	17/05/2024

Cambio	Descripción	Fecha
AWSAuditManagerAdministratorAccess: actualización de una política actual	Hemos agregado los siguientes permisos a `AWSAuditManagerAdministratorAccess` : • `controlcatalog:ListCommonControls` • `controlcatalog:ListDomains` • `controlcatalog:ListObjectives` Esta actualización le permite ver los dominios de control, los objetivos de control y los controles comunes que proporciona AWS Control Catalog. Estos permisos son necesarios si desea utilizar la característica de controles comunes en AWS Audit Manager.	15/05/2024

Cambio	Descripción	Fecha
AWSAuditManagerServiceRolePolicy : actualización de una política actual	Hemos añadido los siguientes permisos a. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager ahora puede realizar las siguientes acciones para recopilar pruebas automatizadas sobre los recursos de su propiedad Cuenta de AWS. • `apigateway:GET` • `autoscaling:DescribeAutoScalingGroups` • `backup:ListBackupPlans` • `cloudfront:GetDistribution` • `cloudfront:GetDistributionConfig` • `cloudfront:ListDistributions` • `cloudtrail:GetTrail` • `cloudtrail:ListTrails` • `dynamodb:DescribeContinuousBackups` • `dynamodb:DescribeBackup` • `dynamodb:DescribeTableReplicaAutoScaling` • `ec2:DescribeInstanceCreditSpecifications` • `ec2:DescribeInstanceAttribute` • `ec2:DescribeSecurityGroupRules` • `ec2:DescribeVpcEndpointConnections` • `ec2:DescribeVpcEndpointServiceConfigurations` • `ec2:GetLaunchTemplateData`	15/05/2024

Cambio	Descripción	Fecha
	• es:DescribeDomains • es:DescribeDomain • es:DescribeDomainConfig • iam:GetAccessKeyLastUsed • iam:GetGroupPolicy • iam:GetPolicy • iam:GetPolicyVersion • iam:GetRolePolicy • iam:GetUser • iam:GetUserPolicy • iam:ListAccessKeys • iam:ListAttachedRolePolicies • iam:ListMfaDeviceTags • iam:ListMfaDevices • iam:ListPolicyVersions • logs:GetDataProtectionPolicy • rds:DescribeDBInstanceAutomatedBackups • rds:DescribeDBClusterEndpoints • rds:DescribeDBClusterParameterGroups • redshift:DescribeClusterSnapshots • redshift:DescribeLoggingStatus • s3:GetBucketAcl • s3:GetBucketLogging • s3:GetBucketOwnershipControls • s3:GetBucketTagging • sagemaker:DescribeEndpointConfig	

Cambio	Descripción	Fecha
	• `sagemaker:ListEndpointConfigs` • `secretsmanager:DescribeSecret` • `secretsmanager:ListSecrets` • `sns:ListTagsForResource` • `waf-regional:GetRule` • `waf-regional:GetWebAcl` • `waf-regional:ListRules` • `waf:GetRule` • `waf:GetRuleGroup` • `waf:ListRuleGroups` • `waf:ListRules` • `waf:ListWebAcls` • `wafv2:ListWebAcls`	
AWSAuditManagerServiceRolePolicy : actualización de una política actual	El rol vinculado al servicio ahora permite realizar AWS Audit Manager la acción. `s3:GetBucketPolicy` Esta acción de la API es necesaria para respaldar el AWS Marco generativo de mejores prácticas de IA, versión 2. Le permite a Audit Manager recopilar pruebas automatizadas sobre las restricciones de políticas vigentes para los conjuntos de datos de entrenamiento de datos de modelos de IA generativa. La `GetBucketPolicy` acción opera dentro del ámbito en el que Cuenta de AWS service-linked-role esté disponible. No puede acceder a las políticas de bucket entre cuentas.	12/06/2023

Cambio	Descripción	Fecha
AWSAuditManagerServiceRolePolicy : actualización de una política actual	Hemos añadido los siguientes permisos a. `AWSAuditManagerServiceRolePolicy` AWS Audit Manager ahora puede realizar las siguientes acciones para recopilar pruebas automatizadas sobre los recursos de su propiedad Cuenta de AWS. • `acm:GetAccountConfiguration` • `acm:ListCertificates` • `backup:ListRecoveryPointsBy Resource` • `bedrock:GetCustomModel` • `bedrock:GetFoundationModel` • `bedrock:GetModelCustomizati onJob` • `bedrock:GetModelInvocationL oggingConfiguration` • `bedrock:ListCustomModels` • `bedrock:ListFoundationModels` • `bedrock:ListModelCustomizat ionJobs` • `cloudtrail:LookupEvents` • `cloudwatch:DescribeAlarmsFo rMetric` • `cloudwatch:GetMetricStatistics` • `cloudwatch:ListMetrics` • `directconnect:DescribeDirec tConnectGateways` • `directconnect:DescribeVirtu alGateways` • `dynamodb:ListBackups`	11/06/2023

Cambio	Descripción	Fecha
	• dynamodb:ListGlobalTables • ec2:DescribeAddresses • ec2:DescribeCustomerGateways • ec2:DescribeEgressOnlyInternetGateways • ec2:DescribeInternetGateways • ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations • ec2:DescribeLocalGateways • ec2:DescribeLocalGatewayVirtualInterfaces • ec2:DescribeNatGateways • ec2:DescribeTransitGateways • ec2:DescribeVpcPeeringConnections • ec2:DescribeVpnConnections • ec2:DescribeVpnGateways • ec2:GetEbsDefaultKmsKeyId • ec2:GetEbsEncryptionByDefault • ecs:DescribeClusters • eks:DescribeAddonVersions • elasticache:DescribeCacheClusters • elasticache:DescribeServiceUpdates • elasticfilesystem:DescribeAccessPoints • elasticloadbalancing:DescribeLoadBalancers	

Cambio	Descripción	Fecha
	• elasticloadbalancing:DescribeSslPolicies • elasticloadbalancing:DescribeTargetGroups • elasticmapreduce:ListClusters • elasticmapreduce:ListSecurityConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems • iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices • kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates	

Cambio	Descripción	Fecha
	• rds:DescribeDbClusterEndpoints • rds:DescribeDbClusterParameterGroups • rds:DescribeDbClusters • rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns:ListTopics • sqs:ListQueues • waf-regional:GetLoggingConfiguration • waf-regional:ListRuleGroups • waf-regional:ListSubscribedRuleGroups • waf-regional:ListWebACLs	
AWSAuditManagerServiceRolePolicy : actualización de una política actual	Hemos agregado los siguientes permisos a AWSAuditManagerServiceRolePolicy : • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets	07/07/2022

Cambio	Descripción	Fecha
AWSAuditManagerServiceRolePolicy: actualización de una política actual	El rol vinculado al servicio ahora permite realizar AWS Audit Manager la acción. `organizations:DescribeOrganization` También hemos reducido el alcance del recurso `CreateEventsAccess`, pasando de ser un carácter comodín (`*`) a un tipo específico de recurso (`arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver`). Por último, añadimos un operador de condición `Null` a la clave de condición `events:source` para confirmar que existe un valor de origen y que su valor no es nulo.	20/05/2022
AWSAuditManagerAdministratorAccess: actualización de una política actual	Hemos actualizado la política de condiciones de clave `events:source` para que refleje que se trata de una clave con varios valores.	29/04/2022
AWSAuditManagerServiceRolePolicy: actualización de una política actual	Hemos actualizado la política de condiciones de clave `events:source` para que refleje que se trata de una clave con varios valores.	16/03/2022
AWS Audit Manager comenzó a rastrear los cambios	AWS Audit Manager comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	05/06/2021

Solución de problemas de AWS Audit Manager identidad y acceso

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Audit Manager e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en AWS Audit Manager

- No estoy autorizado a realizar iam: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Audit Manager recursos

No estoy autorizado a realizar ninguna acción en AWS Audit Manager

El `AccessDeniedException` error aparece cuando un usuario no tiene permiso para usar AWS Audit Manager las operaciones de la API Audit Manager.

En este caso, su administrador debe actualizar la política para permitirle acceso.

No estoy autorizado a realizar iam: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Audit Manager.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Audit Manager. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Audit Manager recursos

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que

asuma el rol. En el caso de los servicios que respaldan las políticas basadas en recursos o las listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si Audit Manager admite estas características, consulte ¿Cómo AWS Audit Manager funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Uso de funciones vinculadas a servicios para AWS Audit Manager

AWS Audit Manager utiliza funciones vinculadas al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Audit Manager. Audit Manager predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS Audit Manager , ya que no es necesario añadir manualmente los permisos necesarios. Audit Manager define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Audit Manager puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Para obtener información sobre otros servicios que admiten roles vinculados al servicio, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado al servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de rol vinculado al servicio para AWS Audit Manager

Audit Manager usa el rol vinculado al servicio denominado**`AWSServiceRoleForAuditManager`**, que permite el acceso a los servicios y recursos de AWS utilizados o administrados por. AWS Audit Manager

El rol vinculado a servicios `AWSServiceRoleForAuditManager` confía en el servicio `auditmanager.amazonaws.com` para asumir el rol.

La política de permisos de funciones permite a Audit Manager recopilar pruebas automatizadas sobre su AWS uso. `AWSAuditManagerServiceRolePolicy` Más específicamente, puede tomar las siguientes acciones en su nombre.

- Audit Manager se puede utilizar AWS Security Hub para recopilar pruebas de verificación de conformidad. En este caso, Audit Manager utiliza el siguiente permiso para informar de los resultados de las comprobaciones de seguridad directamente desde AWS Security Hub. A continuación, adjunta los resultados a los controles de evaluación pertinentes como evidencia.
  - `securityhub:DescribeStandards`

> **Note**
>
> Para obtener más información sobre qué controles específicos de Security Hub puede describir Audit Manager, consulte los controles AWS Security Hub compatibles con AWS Audit Manager.

- Audit Manager se puede utilizar AWS Config para recopilar pruebas de verificación de conformidad. En este caso, Audit Manager utiliza los siguientes permisos para informar de los resultados de las evaluaciones de AWS Config reglas directamente desde AWS Config. A continuación, adjunta los resultados a los controles de evaluación pertinentes como evidencia.
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`
  - `config:ListDiscoveredResources`

> **Note**
>
> Para obtener más información sobre qué AWS Config reglas específicas puede describir Audit Manager, consulte AWS Config Reglas compatibles con AWS Audit Manager.

- Audit Manager se puede utilizar AWS CloudTrail para recopilar pruebas de la actividad del usuario. En este caso, Audit Manager utiliza los siguientes permisos para capturar la actividad del usuario en CloudTrail los registros. A continuación, adjunta la actividad de los controles de evaluación pertinentes como evidencia.
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

> **Note**
>
> Para obtener más información sobre qué CloudTrail eventos específicos puede describir Audit Manager, consulte los nombres de AWS CloudTrail eventos compatibles con AWS Audit Manager.

- Audit Manager puede utilizar las llamadas a la AWS API para recopilar pruebas de configuración de recursos. En este caso, Audit Manager utiliza los siguientes permisos para llamar a los de solo lectura APIs que describen las configuraciones de los recursos para lo siguiente. Servicios de AWS A continuación, adjunta las respuestas de la API a los controles de evaluación pertinentes como evidencia.
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `apigateway:GET`
  - `autoscaling:DescribeAutoScalingGroups`
  - `backup:ListBackupPlans`
  - `backup:ListRecoveryPointsByResource`
  - `bedrock:GetCustomModel`
  - `bedrock:GetFoundationModel`
  - `bedrock:GetModelCustomizationJob`
  - `bedrock:GetModelInvocationLoggingConfiguration`
  - `bedrock:ListCustomModels`
  - `bedrock:ListFoundationModels`
  - `bedrock:ListGuardrails`
  - `bedrock:ListModelCustomizationJobs`
  - `cloudfront:GetDistribution`

- cloudfront:GetDistributionConfig
- cloudfront:ListDistributions
- cloudtrail:DescribeTrails
- cloudtrail:GetTrail
- cloudtrail:ListTrails
- cloudtrail:LookupEvents
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeBackup
- dynamodb:DescribeContinuousBackups
- dynamodb:DescribeTable
- dynamodb:DescribeTableReplicaAutoScaling
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute

- ec2:DescribeInstances

- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies

- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy

- iam:GetPolicy

- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListGroupsForUser
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants

- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups
- rds:DescribeDBSecurityGroups
- redshift:DescribeClusters
- redshift:DescribeClusterSnapshots
- redshift:DescribeLoggingStatus
- route53:GetQueryLoggingConfig
- s3:GetBucketAcl
- s3:GetBucketLogging
- s3:GetBucketOwnershipControls
- s3:GetBucketPolicy

  - Esta acción de la API funciona dentro del ámbito en el Cuenta de AWS que service-linked-role esté disponible. No puede acceder a las políticas de bucket entre cuentas.
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketTagging`
- `s3:GetBucketVersioning`
- `s3:GetEncryptionConfiguration`
- `s3:GetLifecycleConfiguration`
- `s3:ListAllMyBuckets`
- `sagemaker:DescribeAlgorithm`
- `sagemaker:DescribeDomain`
- `sagemaker:DescribeEndpoint`
- `sagemaker:DescribeEndpointConfig`
- `sagemaker:DescribeFlowDefinition`
- `sagemaker:DescribeHumanTaskUi`
- `sagemaker:DescribeLabelingJob`
- `sagemaker:DescribeModel`
- `sagemaker:DescribeModelBiasJobDefinition`
- `sagemaker:DescribeModelCard`
- `sagemaker:DescribeModelQualityJobDefinition`
- `sagemaker:DescribeTrainingJob`
- `sagemaker:DescribeUserProfile`
- `sagemaker:ListAlgorithms`
- `sagemaker:ListDomains`
- `sagemaker:ListEndpointConfigs`
- `sagemaker:ListEndpoints`
- `sagemaker:ListFlowDefinitions`
- `sagemaker:ListHumanTaskUis`
- `sagemaker:ListLabelingJobs`
- `sagemaker:ListModels`

- `sagemaker:ListModelBiasJobDefinitions`

- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions
- sagemaker:ListMonitoringAlerts
- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets
- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:GetRule
- waf-regional:GetWebAcl
- waf-regional:ListRuleGroups
- waf-regional:ListRules
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:GetRule
- waf:GetRuleGroup
- waf:ListActivatedRulesInRuleGroup
- waf:ListRuleGroups
- waf:ListRules
- waf:ListWebAcls
- wafv2:ListWebAcls

> **Note**
>
> Para obtener más información sobre las llamadas a la API específicas que Audit Manager puede describir, consulte Se admiten llamadas a la API para orígenes de datos de control personalizadas.

Para ver todos los detalles de los permisos del rol vinculado al servicio `AWSServiceRoleForAuditManager`, consulte AWSAuditManagerServiceRolePolicy en la Guía de referencia de políticas administradas de AWS .

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Crear el rol AWS Audit Manager vinculado al servicio

No necesita crear manualmente un rol vinculado a servicios. Cuando lo habilitas AWS Audit Manager, el servicio crea automáticamente el rol vinculado al servicio por ti. Puede activar Audit Manager desde la página de incorporación de AWS Management Console, o mediante la API o AWS CLI. Para obtener más información, consulte Habilitar AWS Audit Manager en este guía del usuario.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta.

Edición del rol vinculado al AWS Audit Manager servicio

AWS Audit Manager no permite editar el rol vinculado al `AWSServiceRoleForAuditManager` servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Permitir a una entidad de IAM editar la descripción del rol vinculado a servicio **`AWSServiceRoleForAuditManager`**

Agregue la siguiente instrucción a la política de permisos de la entidad de IAM que tiene que editar la descripción del rol vinculado al servicio.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
}
```

Eliminar el rol vinculado al servicio AWS Audit Manager

Si ya no utiliza Audit Manager, le recomendamos que elimine el rol vinculado a servicios `AWSServiceRoleForAuditManager`. De esta forma, no tendrá una entidad no utilizada cuya supervisión o mantenimiento no se realizan de forma activa. Sin embargo, debe limpiar el rol vinculado al servicio antes de eliminarlo.

Limpieza del rol vinculado al servicio de

Antes de poder utilizar IAM para eliminar el rol vinculado a un servicio de Audit Manager, primero debe confirmar que dicho rol no tiene sesiones activas y eliminar los recursos que utiliza. Para ello, asegúrese de que Audit Manager esté dado de baja en todos los registros. Regiones de AWS Tras anular el registro, Audit Manager ya no utiliza el rol vinculado al servicio.

Para obtener instrucciones sobre cómo anular el registro de Audit Manager, consulte los siguientes recursos:

- Desactivar AWS Audit Manager en esta guía
- DeregisterAccount en la Referencia de la API de AWS Audit Manager
- anular el registro de la cuenta en la referencia deAWS CLI AWS Audit Manager

Para obtener instrucciones sobre cómo eliminar los recursos de Audit Manager manualmente, consulte Eliminación de datos de Audit Manager en esta guía.

Eliminación del rol vinculado a un servicio

Puede eliminar el rol vinculado al servicio utilizando la consola de IAM, la AWS Command Line Interface (AWS CLI) o la API de IAM.

IAM console

Siga estos pasos para eliminar un rol vinculado en la consola de IAM.

Para eliminar un rol vinculado a un servicio (consola)

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en. https://console.aws.amazon.com/iam/
2. En el panel de navegación de la consola de IAM, elija Roles. A continuación, maqrue la casilla de verificación situada junto a `AWSServiceRoleForAuditManager`, no el nombre o la propia fila.
3. En Acciones de rol en la parte superior de la página, elija Eliminar.
4. En el cuadro de diálogo de confirmación, revise la información de acceso reciente, donde se indica cuándo accedió cada uno de los roles seleccionados a un servicio de Servicio de AWS por última vez. Esto lo ayuda a confirmar si el rol está actualmente activo. Si desea continuar, introduzca **`AWSServiceRoleForAuditManager`** en el campo de entrada de texto y seleccione Eliminar para enviar la solicitud de eliminación del rol vinculado al servicio.
5. Consulte las notificaciones de la consola de IAM para monitorear el progreso de la eliminación del rol vinculado al servicio. Como el proceso de eliminación del rol vinculado al servicio de IAM es asíncrono, dicha tarea puede realizarse correctamente o fallar después de que envía la solicitud de eliminación. Si el proceso se realiza correctamente, el rol se elimina de la lista y aparece un mensaje de confirmación en la parte superior de la página.

AWS CLI

Puede utilizar los comandos de IAM desde el AWS CLI para eliminar un rol vinculado a un servicio.

Para eliminar un rol vinculado a un servicio (AWS CLI)

1. Introduzca el siguiente comando para enumerar el rol de su cuenta:

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. Como los roles vinculados a servicios no se puede eliminar si están en uso o tienen recursos asociados, debe enviar una solicitud de eliminación. Esta solicitud puede denegarse si no se cumplen estas condiciones. Debe apuntar el valor `deletion-task-id` de la respuesta para comprobar el estado de la tarea de eliminación.

Ingrese el siguiente comando para enviar una solicitud de eliminación de un rol vinculado a un servicio:

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. Utilice el siguiente comando para comprobar el estado de la tarea de eliminación:

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

El estado de la tarea de eliminación puede ser `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` o `FAILED`. Si ocurre un error durante la eliminación, la llamada devuelve el motivo del error para que pueda resolver el problema.

IAM API

Puede utilizar la API de IAM para eliminar un rol vinculado a un servicio.

Para eliminar un rol vinculado a un servicio (API)

1. Llame GetRolepara incluir el rol en su cuenta. En la solicitud, especifique que `AWSServiceRoleForAuditManager` es el `RoleName`.
2. Como los roles vinculados a servicios no se puede eliminar si están en uso o tienen recursos asociados, debe enviar una solicitud de eliminación. Esta solicitud puede denegarse si no se cumplen estas condiciones. Debe apuntar el valor `DeletionTaskId` de la respuesta para comprobar el estado de la tarea de eliminación.

   Para enviar una solicitud de eliminación de un rol vinculado a un servicio, llama. DeleteServiceLinkedRole En la solicitud, especifique que `AWSServiceRoleForAuditManager` es el `RoleName`.
3. Para comprobar el estado de la tarea de eliminación, realice una llamada a GetServiceLinkedRoleDeletionStatus. En la solicitud, especifique el valor de `DeletionTaskId`.

   El estado de la tarea de eliminación puede ser `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` o `FAILED`. Si ocurre un error durante la eliminación, la llamada devuelve el motivo del error para que pueda resolver el problema.

Consejos para eliminar el rol vinculado a servicios en Audit Manager

Es posible que el proceso de eliminación del rol vinculado a servicios en Audit Manager no se realice correctamente si Audit Manager utiliza el rol o tiene recursos asociados. Esto puede ocurrir en las siguientes situaciones:

1. Su cuenta sigue registrada en Audit Manager en una o varias Regiones de AWS.
2. Su cuenta forma parte de una AWS organización y la cuenta de administración o la cuenta de administrador delegado siguen integradas en Audit Manager.

Para resolver un problema de eliminación fallida, comience por comprobar si forma parte de Cuenta de AWS una organización. Para ello, llama a la operación de la DescribeOrganizationAPI o navega a la AWS Organizations consola.

Si forma Cuenta de AWS parte de una organización

1. Utilice la cuenta de administración para eliminar el administrador delegado en Audit Manager en todas las Regiones de AWS en las que haya añadido uno.
2. Utilice su cuenta de administración para anular el registro de Audit Manager en todos los Regiones de AWS lugares en los que utilizó el servicio.
3. Intente de nuevo eliminar el rol vinculado a servicios mediante los pasos indicados en el procedimiento anterior.

Si no Cuenta de AWS forma parte de una organización

1. Asegúrese de anular el registro de Audit Manager en todos los Regiones de AWS lugares en los que utilizó el servicio.
2. Intente de nuevo eliminar el rol vinculado a servicios mediante los pasos indicados en el procedimiento anterior.

Tras anular el registro de Audit Manager, el servicio dejará de utilizar el rol vinculado a servicios. A continuación, podrá eliminar el rol correctamente.

Regiones compatibles para funciones vinculadas al servicio AWS Audit Manager

AWS Audit Manager admite el uso de funciones vinculadas al servicio en todos los lugares en los que el servicio Regiones de AWS esté disponible. Para obtener más información, consulte puntos de conexión de servicio de AWS.

Validación de conformidad para AWS Audit Manager

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos

de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.

- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Comprender la resiliencia en AWS Audit Manager

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia.

Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de la infraestructura en AWS Audit Manager

Como servicio gestionado, AWS Audit Manager está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utilice las llamadas a la API AWS publicadas para acceder a AWS Audit Manager a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.

- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Puede llamar a estas operaciones de API desde cualquier ubicación de la red, pero AWS Audit Manager admite políticas de acceso basadas en los recursos, que pueden incluir restricciones basadas en la dirección IP de origen. También puede utilizar las políticas de Audit Manager para controlar el acceso desde puntos de enlace específicos o específicos de Amazon Virtual Private Cloud (Amazon VPC). VPCs En efecto, esto aísla el acceso de red a un recurso de Audit Manager determinado únicamente de la VPC específica de la red. AWS

AWS Audit Manager y puntos finales de VPC de interfaz ()AWS PrivateLink

Puede establecer una conexión privada entre su VPC y crear un punto final AWS Audit Manager de VPC de interfaz. Los puntos finales de interfaz funcionan con una tecnología que le permite acceder de forma privada a Audit Manager APIs sin una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión AWS Direct Connect. AWS PrivateLink Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con Audit Manager. APIs El tráfico entre su VPC y AWS Audit Manager no sale de la AWS red.

Cada punto de conexión de la interfaz está representado por una o más interfaces de red elásticas en las subredes.

Para obtener más información, consulte Puntos de conexión de VPC de interfaz (AWS PrivateLink) en la Guía del usuario de Amazon VPC.

Consideraciones sobre los puntos AWS Audit Manager finales de VPC

Antes de configurar un punto de enlace de VPC de interfaz AWS Audit Manager, asegúrese de revisar las propiedades y limitaciones del punto de enlace de interfaz en la Guía del usuario de Amazon VPC.

AWS Audit Manager admite realizar llamadas a todas sus acciones de API desde su VPC.

Creación de un punto de conexión de VPC de interfaz para AWS Audit Manager

Puede crear un punto de enlace de VPC para el AWS Audit Manager servicio mediante la consola de Amazon VPC o el (). AWS Command Line Interface AWS CLI Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Cree un punto final de VPC para AWS Audit Manager usar el siguiente nombre de servicio:

- `com.amazonaws.region.auditmanager`

Si habilitas el DNS privado para el punto final, puedes realizar solicitudes a la API para AWS Audit Manager utilizar su nombre de DNS predeterminado para la región, por ejemplo. `auditmanager.us-east-1.amazonaws.com`

Para más información, consulte Acceso a un servicio a través de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Crear una política de puntos de conexión de VPC para AWS Audit Manager

Puede asociar una política de punto de conexión con su punto de conexión de VPC que controla el acceso a AWS Audit Manager. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para más información, consulte Control del acceso a los servicios con puntos de enlace de la VPC en la Guía del usuario de Amazon VPC.

Ejemplo: política de puntos finales de VPC para acciones AWS Audit Manager

El siguiente es un ejemplo de una política de puntos finales para AWS Audit Manager. Cuando se asocia con un punto de conexión, esta política concede acceso a las acciones de Audit Manager mostradas para todas las entidades principales en todos los recursos.

```
{
```

```
    "Statement":[
       {
          "Principal":"*",
          "Effect":"Allow",
          "Action":[
             "auditmanager:GetAssessment",
             "auditmanager:GetServicesInScope",
             "auditmanager:ListNotifications"
          ],
          "Resource":"*"
       }
    ]
}
```

Inicio de sesión y supervisión AWS Audit Manager

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Audit Manager y sus demás AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para vigilar Audit Manager, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- AWS CloudTrail captura las llamadas a la API y otros eventos relacionados que realiza la Cuenta de AWS o que se realizan en nombre de esta. Además, entrega los archivos de registro a un bucket de Amazon S3 especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que estas se realizaron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.
- Amazon EventBridge es un servicio de bus de eventos sin servidor que facilita la conexión de sus aplicaciones con datos de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones Software-as-a-Service (SaaS) y AWS servicios, y dirige esos datos a destinos como Lambda. Esto le permite monitorear los eventos que ocurren en los servicios y crear arquitecturas basadas en eventos. Para obtener más información, consulta la Guía del EventBridge usuario de Amazon.

Monitorización AWS Audit Manager con Amazon EventBridge

Amazon le EventBridge ayuda a automatizar los eventos del sistema Servicios de AWS y a responder automáticamente a ellos, como problemas de disponibilidad de las aplicaciones o cambios en los recursos.

Puede usar EventBridge reglas para detectar eventos de Audit Manager y reaccionar ante ellos. Según las reglas que cree, EventBridge invoca una o más acciones objetivo cuando un evento coincide con los valores que especifique en una regla. Dependiendo del tipo de evento, es posible que desee enviar notificaciones, capturar información sobre el evento, tomar medidas correctivas, iniciar eventos o adoptar otras acciones.

Por ejemplo: puede detectar cada vez que se produzcan los siguientes eventos de Audit Manager en su cuenta:

- El propietario de una auditoría crea, actualiza o elimina una evaluación
- El propietario de la auditoría delega un conjunto de controles para su revisión
- Un delegado completa su revisión y devuelve el conjunto de controles revisado al propietario de la auditoría
- El propietario de la auditoría actualiza el estado de un control de evaluación

Entre las acciones que se pueden activar automáticamente se incluyen las siguientes:

- Usa una AWS Lambda función para pasar una notificación a un canal de Slack.
- Envíe datos acerca de la verificación a un Amazon Kinesis Data Streams para permitir una supervisión completa y en tiempo real del estado.
- Envía un tema de Amazon Simple Notification Service (Amazon SNS) a su correo electrónico.
- Recibe una notificación con una acción de CloudWatch alarma de Amazon.

> **Note**
>
> Audit Manager ofrece eventos de forma duradera. Esto significa que Audit Manager intentará enviar eventos correctamente al EventBridge menos una vez. En los casos en los que los eventos no se puedan entregar debido a una interrupción del EventBridge servicio, Audit Manager los volverá a intentar más adelante durante un máximo de 24 horas.

EventBridge formato de ejemplo para Audit Manager

El siguiente código JSON muestra un ejemplo de un evento de creación de una evaluación en Audit Manager. Para obtener información sobre cualquiera de los campos de este evento, consulte la referencia de la estructura del evento.

```
{
    "version": "0",
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
    "detail-type": "Assessment Created",
    "source": "aws.auditmanager",
    "account": "111122223333",
    "time": "2023-07-27T00:38:33Z",
    "region": "us-west-2",
    "resources":
        [
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-
i9j0-k1l2m3n4o5p6"
        ],
    "detail":
    {
        "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
        "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
        "assessmentTenantId": "111122223333",
        "assessmentName": "myAssessment",
        "eventTime": 1690418289068,
        "eventName": "CREATE",
        "eventType": "ASSESSMENT",
        "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
    }
}
```

Requisitos previos para crear una regla EventBridge

Antes de crear reglas para los eventos de Audit Manager, recomendamos que haga lo siguiente:

- Familiarícese con los eventos, las reglas y los objetivos en EventBridge. Para obtener más información, consulta ¿Qué es Amazon EventBridge? en la Guía del EventBridge usuario de Amazon.
- Crear un destino que se va a usar en su regla de eventos. Por ejemplo: puede crear un tema de Amazon SNS de modo que cada vez que se complete una revisión de un conjunto de controles, reciba un mensaje de texto o un correo electrónico. Para más información, consulte Destinos de EventBridge .

Creación de una EventBridge regla para Audit Manager

Siga estos pasos para crear una EventBridge regla que se active en un evento emitido por Audit Manager. Los eventos se emiten en la medida de lo posible.

Para crear una EventBridge regla para Audit Manager

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. En el panel de navegación, seleccione Reglas.
3. Seleccione Creación de regla.
4. En la página Crear detalles de la regla, ingrese un nombre y una descripción para la regla.
5. Mantenga los valores predeterminados para Event bus (Bus de eventos) y Rules type (Tipo de regla) y luego seleccione Next (Siguiente).
6. En la página Crear un patrón de eventos, en Origen del evento, elige AWS eventos o eventos EventBridge asociados.
7. En Método de creación, elija Patrón personalizado (editor JSON).
8. En Patrón de eventos, escriba un patrón de eventos en JSON y especifique los campos que quiere usar para hacer coincidir.

   Para que coincida con un evento de Audit Manager, puede utilizar el siguiente patrón simple:

   ```
   {
     "detail-type": ["Event"]
   }
   ```

   Event Sustitúyalo por uno de los siguientes valores admitidos:

   a. Introduzca `Assessment Created` para recibir notificaciones cuando se cree una evaluación.
   b. Introduzca `Assessment Updated` para recibir notificaciones cuando se cree una evaluación.
   c. Introduzca `Assessment Deleted` para recibir notificaciones cuando se elimine una evaluación.
   d. Introduzca `Assessment ControlSet Delegation Created` para recibir notificaciones cuando se delegue la revisión de un conjunto de controles.

e. Introduzca `Assessment ControlSet Reviewed` para recibir notificaciones cuando se revise un conjunto de control de evaluación.

f. Introduzca `Assessment Control Reviewed` para recibir notificaciones cuando se revise un control de evaluación.

> **Tip**
>
> Añada más campos a su patrón de eventos según sea necesario. Para obtener más información sobre los campos disponibles, consulta Amazon EventBridge Event Patterns.

9. Elija Siguiente.
10. En la página Seleccionar objetivos, elija el destino que haya creado para esta regla y, a continuación, configure las opciones adicionales necesarias para dicho tipo. Por ejemplo, si elige Amazon SNS, asegúrese de que el tema de SNS esté configurado correctamente para que se le notifique por correo electrónico o SMS.

> **Tip**
>
> Los campos que se muestran varían en función del servicio seleccionado. Para obtener más información sobre los objetivos disponibles, consulte Objetivos disponibles en la EventBridge consola.

11. Para muchos tipos de objetivos, EventBridge necesita permisos para enviar eventos al objetivo. En estos casos, EventBridge puede crear la función de IAM necesaria para que se ejecute la regla.

    a. Para crear un rol de IAM automáticamente, elija Creación de un nuevo rol para este recurso específico.

    b. Para utilizar un rol de IAM que haya creado antes, elija Use existing role (Usar rol existente).

12. (Opcional) Elija Add another target (Agregar otro destino) para agregar otro destino para esta regla.
13. Elija Siguiente.
14. (Opcional) En la página Add tags (Agregar etiquetas) agregue etiquetas a su clave y, a continuación, elija Next (Siguiente).

15. En la página Review and create (Revisar y crear), revise la configuración de las reglas para asegurarse de que se ajustan a los requisitos de supervisión de eventos.
16. Elija Crear regla. Su regla se controlará ahora para eventos de Audit Manager y, a continuación, envíelos al destino que especificó.

Registrar las llamadas a AWS Audit Manager la API con CloudTrail

Audit Manager está integrado con CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un miembro Servicio de AWS de Audit Manager. CloudTrail captura todas las llamadas a la API de Audit Manager como eventos. Las llamadas que se capturan incluyen llamadas desde la consola de Audit Manager y llamadas de código a las operaciones de la API de Audit Manager.

Si crea un registro, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Audit Manager. Si no configura un registro, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos.

Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Audit Manager, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Información de Audit Manager en CloudTrail

CloudTrail está habilitada en su cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Audit Manager, esa actividad se registra en un CloudTrail evento junto con otros Servicio de AWS eventos en el historial de eventos.

Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail .

Para obtener un registro continuo de los eventos de su Cuenta de AWS empresa, incluidos los eventos de Audit Manager, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique.

Además, puede configurar otros Servicios de AWS para que analicen más a fondo los datos de eventos recopilados en los CloudTrail registros y actúen en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail Integraciones y servicios compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de Audit Manager se registran CloudTrail y se documentan en la Referencia de la AWS Audit Manager API. Por ejemplo, las llamadas a las `CreateControl` operaciones de la `UpdateAssessmentFramework` API y la API generan entradas en los archivos de CloudTrail registro. `DeleteControl`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

Para obtener más información, consulte el Elemento userIdentity de CloudTrail .

Descripción de las entradas del archivo de registros de Audit Manager

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateAssessment`acción.

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
        arn:"arn:aws:iam::accountId:user/userName",
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"auditmanager.amazonaws.com",
      eventName:"CreateAssessment",
      awsRegion:"us-west-2",
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters:{
        frameworkId:"frameworkId",
        assessmentReportsDestination:{
          destination:"***",
          destinationType:"S3"
        },
        clientToken:"***",
        scope:{
          awsServices:[
            {
              serviceName:"license-manager"
            }
          ],
          awsAccounts:"***"
        },
        roles:"***",
```

```
        name:"***",
        description:"***",
        tags:"***"
      },
      responseElements:{
        assessment:"***"
      },
      requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
      eventID:"a782029a-959e-4549-81df-9f6596775cb0",
      readOnly:false,
      eventType:"AwsApiCall",
      recipientAccountId:"recipientAccountId"
    }
```

Comprenda la configuración y el análisis de vulnerabilidades en AWS Audit Manager

La configuración y los controles de TI son una responsabilidad compartida entre usted AWS y usted, nuestro cliente. Para obtener más información, consulte el modelo de responsabilidad AWS compartida.

Desactivar AWS Audit Manager

Puede deshabilitar Audit Manager si ya no desea utilizar el servicio. Al deshabilitar Audit Manager, también tiene la opción de eliminar todos los datos.

De forma predeterminada, los datos no se eliminan al deshabilitar Audit Manager. Los datos de sus evidencias se conservan durante dos años desde el momento de su creación. Sus demás recursos de Audit Manager (incluidas las evaluaciones, los controles personalizados y los marcos personalizados) se retienen indefinidamente y estarán disponibles si vuelve a habilitar Audit Manager en el futuro. Para obtener más información sobre la retención de datos, consulte Protección de datos en esta guía.

Si decide eliminar sus datos, Audit Manager eliminará todos los datos de evidencia junto con todos los recursos de Audit Manager que haya creado (incluidas las evaluaciones, los controles personalizados y los marcos personalizados). Todos sus datos se eliminarán en un plazo de siete días a partir de la deshabilitación de Audit Manager.

Temas

- Procedimiento
- Pasos a seguir a continuación
- Recursos adicionales

Procedimiento

Puede deshabilitar Audit Manager mediante la consola de Audit Manager, la AWS Command Line Interface (AWS CLI) o la API Audit Manager.

> **Warning**
>
> - Al deshabilitar Audit Manager, se revoca su acceso y el servicio ya no recopila evidencias de ninguna evaluación existente. No puede acceder a ningún elemento del servicio a menos que vuelva a habilitar Audit Manager.
> - Eliminar todos los datos es una acción permanente. Si decide volver a habilitar Audit Manager en el futuro, sus datos no se podrán recuperar.

Audit Manager console

Deshabilitación de Audit Manager en la consola de Audit Manager

1. En la pestaña Configuración general, vaya a la sección Deshabilitar AWS Audit Manager.
2. Elija Deshabilitar.
3. En la ventana emergente, revise su configuración actual de retención de datos.
   a. Para continuar con la selección actual, seleccione Deshabilitar Audit Manager.
   b. Para cambiar la selección actual, ejecute los pasos siguientes:
      i. Pulse Cancelar para volver a la página de configuración.
      ii. Para usar la configuración de retención de datos predeterminada, desactive Eliminar todos los datos. Esta selección retiene los datos relativos a las evidencias durante dos años a partir del momento de su creación y conserva otros recursos de Audit Manager de forma indefinida.
      iii. Para eliminar sus datos, active Eliminar todos los datos.
      iv. Seleccione Deshabilitar y, a continuación, elija Deshabilitar Audit Manager para confirmar su elección.

AWS CLI

Antes de comenzar

Antes de deshabilitar Audit Manager, puede ejecutar el comando update-settings para establecer la política de retención de datos que prefiera. De forma predeterminada, Audit Manager retiene sus datos. Si desea solicitar la eliminación de sus datos, utilice el parámetro `--deregistration-policy` con el valor `deleteResources` establecido en`ALL`.

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

Para deshabilitar Audit Manager en el AWS CLI

Cuando esté listo para deshabilitar Audit Manager, ejecute el comando deregister-account.

```
aws auditmanager deregister-account
```

Audit Manager API

Antes de comenzar

Antes de deshabilitar Audit Manager, puede utilizar la operación de la UpdateSettingsAPI para establecer la política de retención de datos que prefiera. De forma predeterminada, Audit Manager retiene sus datos. Si desea eliminar sus datos, puede usar el DeregistrationPolicyatributo para solicitar la eliminación de sus datos.

Deshabilitación de Audit Manager mediante la API

Cuando esté listo para deshabilitar Audit Manager, llame a la DeregisterAccountoperación.

Para obtener más información, seleccione uno de los enlaces anteriores para obtener más información en la Referencia de la API de Audit Manager. Esto incluye información sobre cómo utilizar estas operaciones y parámetros en uno de los idiomas específicos AWS SDKs.

Pasos a seguir a continuación

Si necesita volver a habilitar Audit Manager después de deshabilitarlo, siga estos pasos para que el servicio vuelva a funcionar.

Para volver a habilitar Audit Manager después de deshabilitarlo

Vaya a la página de inicio del servicio Audit Manager y siga los pasos para configurar Audit Manager como un nuevo usuario. Para obtener más información, consulte Configuración AWS Audit Manager con los ajustes recomendados.

> **Tip**
>
> - Si eligió eliminar sus datos al deshabilitar Audit Manager, debe esperar a que se eliminen los datos para poder volver a habilitar el servicio. En función de la cantidad de datos de la que disponga, esto puede tardar hasta siete días. Sin embargo, no dude en intentar volver a activar Audit Manager antes de esa fecha. En muchos casos, los datos se eliminan en tan solo una hora.
> - Si optó por no eliminar sus datos al deshabilitar Audit Manager, sus evaluaciones actuales pasarán a un estado latente y, en consecuencia, dejarán de recopilar evidencias. Para volver a recopilar evidencias para una evaluación preexistente, edite la evaluación y seleccione Guardar sin realizar ningún cambio.

Recursos adicionales

- Para obtener más información sobre la retención de datos en Audit manager, consulte Protección de datos en esta guía.

Historial de documentos de la Guía AWS Audit Manager del usuario

En la siguiente tabla se describen los cambios importantes en cada versión de la Guía del AWS Audit Manager usuario a partir del 8 de diciembre de 2020.

Cambio	Descripción	Fecha
Actualizaciones de cinco marcos compatibles	Se han actualizado los siguientes marcos: • CCCS Medium Cloud Control • Anexo A de la norma de la ISO/IEC 27001:2013 • PCI DSS V3.2.1 • PCI DSS V4.0 • SSAE-18 SOC 2	17 de julio de 2025
Actualizaciones de cinco marcos compatibles	Se han actualizado los siguientes marcos: • Amazon Web Services (AWS) Well Architected Framework (WAF) v10 • Controles básicos de seguridad de FedRAMP r4 • NIST SP 800-171 Rev. 2 • NIST-CSF-v1.1 • NIST-SP-800-53-R5	19 de junio de 2025
Actualizaciones de tres marcos compatibles	Se han actualizado los siguientes marcos: • Essential Eight del ACSC	4 de junio de 2025

	• ACSC ISM • CIS Critical Security Controls versión 8.0, IG1	
Marco compatible actualizado: CIS Controls v7.1, IG1	Se ha actualizado el IG1 marco CIS Controls v7.1. Para obtener más información, consulte CIS Controls v7.1,. IG1	14 de mayo de 2025
Política s3_ ListBuckets actualizada	AWS Audit Manager ha actualizado la `s3_ListBuckets` política y la documentación para adaptarla `s3_GetBucketEncryption` a la política. Para obtener más información, consulta las llamadas a la API compatibles para las fuentes de datos de control personalizadas.	24 de marzo de 2025
Política AWS gestionada actualizada	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	24 de septiembre de 2024
Nuevo marco compatible: mejores prácticas de IA AWS generativa v2	Ya está disponible un nuevo marco prediseñado en. AWS Audit Manager Para obtener más información, consulte Prácticas recomendadas de IA generativa de AWS v2.	11 de junio de 2024

Política AWS gestionada actualizada	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	10 de junio de 2024
Uso de controles comunes para simplificar la forma en que se ejecutan las evaluaciones comparándolas con los controles empresariales	Al crear un control personalizado, podrá utilizar los controles comunes como origen de evidencias. Cada control común se asigna a una agrupación gestionada de fuentes de AWS datos relevantes. Estas agrupaciones predefinidas agilizan la recopilación de pruebas al eliminar la necesidad de identificar qué AWS recursos deben evaluarse para un control determinado. Para obtener información sobre cómo buscar controles comunes y utilizarlos como orígenes de evidencia, consulte Control library.	6 de junio de 2024
Política AWS gestionada actualizada	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	17 de mayo de 2024

Política AWS gestionada actualizada	AWS Audit Manager ha actualizado la AWSAuditManagerAdministratorAccesspolítica. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	15 de mayo de 2024
Política AWS gestionada actualizada	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	15 de mayo de 2024
Support para llamadas AWS API adicionales	Ahora puede usar llamadas a la AWS API adicionales como fuentes de datos para sus controles personalizados en Audit Manager. Para obtener más información, consulte Llamadas a la API compatibles para orígenes de datos de control personalizados.	15 de mayo de 2024
Nuevo marco compatible: PCI DSS V4.0	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte PCI DSS V4.0.	19 de diciembre de 2023

Support para llamadas AWS API adicionales	Ahora puede usar llamadas a la AWS API adicionales como fuentes de datos para sus controles personalizados en Audit Manager. Para obtener más información, consulte Llamadas a la API compatibles para orígenes de datos de control personalizados.	7 de diciembre de 2023
Política AWS gestionada actualizada	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	6 de diciembre de 2023
Support for AWS Security Hub consolidated control findings	Audit Manager ahora admite controles consolidados en AWS Security Hub. Para obtener más información, consulte AWS Security Hub los controles compatibles con AWS Audit Manager.	16 de noviembre de 2023
Integración con MetricStream	Ahora puede incorporar pruebas de Audit Manager a MetricStream. Para obtener más información, consulte Integraciones con productos GRC de terceros.	14 de noviembre de 2023

Nuevo marco compatible: mejores prácticas de IA AWS generativa	Ya está disponible un nuevo marco prediseñado en. AWS Audit Manager Para obtener más información, consulte generative AI best practices framework v1.	8 de noviembre de 2023
Política AWS gestionada actualizada	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	6 de noviembre de 2023
Integración con Amazon EventBridge	Ahora puede monitorear los eventos que ocurren en AWS Audit Manager él y usarlos como parte de su arquitectura basada en eventos. Para obtener más información, consulta Monitoring AWS Audit Manager with Amazon EventBridge.	18 de agosto de 2023

Soporte para evaluaciones de riesgo y nuevas opciones de evidencias manuales	Ahora puede utilizar el flujo de trabajo de creación de controles personalizados para respaldar las evaluaciones de riesgos. Ahora, un control puede representar una pregunta de evaluación de riesgos y usted puede proporcionar una respuesta cargando un archivo o introduciendo texto como evidencia manual. Para obtener más información, consulte Crear un control personalizado y Añadir evidencia manual.	12 de junio de 2023
Soporte para exportaciones a CSV	Ahora puede exportar los resultados de búsqueda del buscador de evidencias en formato CSV. Para obtener más información, consulte Exportar resultados de búsqueda.	9 de junio de 2023
Nuevo marco compatible: Manual de seguridad de la información del Centro Australiano de Ciberseguridad (ACSC)	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte el Manual de seguridad de la información del Centro Australiano de Ciberseguridad (ACSC).	24 de marzo de 2023

Informes de evaluación mejorados	Hemos mejorado el formato y el contenido de los informes de evaluación de Audit Manager. Para obtener más información sobre cómo navegar e interpretar los informes de evaluació n, consulte Informes de evaluación.	23 de marzo de 2023
Soporte para llamadas a la API paginadas	AWS Audit Manager ahora admite llamadas a la API paginadas como fuente de datos para la recopilación de pruebas. Para obtener más información, consulte Llamadas a la API paginadas.	8 de marzo de 2023
Nuevo marco compatible: Regla de seguridad ómnibus final de la HIPAA de 2013	Ya está disponible un nuevo marco prediseñado en. AWS Audit Manager Para obtener más información, consulte la Regla de seguridad ómnibus final de la HIPAA de 2013. Con fines de diferenciación, el marco HIPAA que existía anteriormente (anteriormente denominado HIPAA en la biblioteca de marcos) ahora se denomina Regla de seguridad de la HIPPA de 2003.	8 de marzo de 2023

Support para llamadas AWS API adicionales	Ahora puede usar nueve llamadas a la AWS API adicionales como fuente de datos para sus controles personalizados en Audit Manager. Para obtener más información, consulte Llamadas a la API compatibles para orígenes de datos de control personalizados.	3 de marzo de 2023
Guía actualizada para implementar las prácticas recomendadas de IAM	Se ha actualizado la guía para implementar las prácticas recomendadas de IAM. Para obtener más información, consulta prácticas recomendadas de seguridad en IAM.	6 de enero de 2023
Nueva configuración de retención de datos	Ahora puede especificar si desea eliminar todos sus datos al deshabilitar Audit Manager. Para obtener más información, consulte Deshabilitar AWS Audit Manager y Eliminar datos de Audit Manager.	6 de enero de 2023
Soporte para el buscador de evidencias	Ahora puede utilizar el buscador de evidencias para realizar consultas de búsqueda sobre los datos de las evidencias. Para obtener más información, consulte Buscador de evidencias.	18 de noviembre de 2022

Nuevo marco compatible: Australian Cyber Security Centre (ACSC) Essential Eight	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte Australian Cyber Security Centre (ACSC) Essential Eight.	24 de agosto de 2022
Política AWS gestionada actualizada	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	7 de julio de 2022
Política AWS gestionada actualizada	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	20 de mayo de 2022
Nuevo marco compatible: Canadian Centre for Cyber Security Medium Cloud Control Profile	Ahora hay disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte Canadian Centre for Cyber Security Medium Cloud Control Profile.	6 de mayo de 2022

Política AWS gestionada actualizada	AWS Audit Manager ha actualizado la AWSAuditManagerAdministratorAccesspolítica. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	29 de abril de 2022
Support para reglas AWS Config gestionadas adicionales	Ahora puede usar 91 reglas AWS Config administradas adicionales como fuente de datos para sus controles personalizados en Audit Manager. Para obtener más información, consulte Uso de reglas AWS Config administradas con AWS Audit Manager.	27 de abril de 2022
Support para reglas AWS Config personalizadas	Ahora puede usar reglas AWS Config personalizadas como fuente de datos para sus controles personalizados en Audit Manager. Para obtener más información, consulte Uso de reglas AWS Config personalizadas con AWS Audit Manager.	27 de abril de 2022
Nuevo marco compatible: ISO/IEC 27001:2013, anexo A	Ya está disponible un nuevo marco prediseñado en. AWS Audit Manager Para obtener más información, consulte el Anexo A de la norma ISO/IEC 27001:2013.	7 de abril de 2022

Política AWS gestionada actualizada	AWS Audit Manager ha actualizado la AWSAuditManagerServiceRolePolicy. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	16 de marzo de 2022
Nuevos marcos compatibles: CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4	Ya están disponibles dos nuevos marcos prediseñados AWS Audit Manager: CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4, Level 1, y CIS Benchmark para CIS Amazon Web Services Foundations Benchmark v1.4, Level 1 y 2. Para obtener más información, consulte CIS Benchmark para CIS AWS Audit Manager Foundations Benchmark v1.4.0.	2 de marzo de 2022
Nuevo marco compatible: CIS Controls v8 IG1	Ya está disponible un nuevo marco prediseñado en. AWS Audit Manager Para obtener más información, consulte CIS Controls IG1 v8.	2 de marzo de 2022
AWS Audit Manager panel	Ahora puede utilizar el panel de control de Audit Manager para supervisar sus evaluaciones activas e identificar rápidamente las evidencias no conformes. Para obtener más información, consulte Uso del panel de Audit Manager.	18 de noviembre de 2021

Compartir un marco personalizado	Ahora puede compartir sus marcos personalizados de Audit Manager con otro Cuenta de AWS o replicarlos en otro Región de AWS con su propia cuenta. Para obtener más información, consulte Compartir un marco personalizado.	22 de octubre de 2021
Nuevos ejemplos de AWS Audit Manager controles	Ahora puede revisar ejemplos de controles y aprender cómo Audit Manager ayuda a adaptar su AWS entorno a sus requisitos. Para obtener más información, consulte Ejemplos de AWS Audit Manager controles.	21 de septiembre de 2021
Nuevo marco compatible: Gramm-Leach-Bliley Act (GLBA)	Ya está disponible un nuevo marco prediseñado en. AWS Audit Manager Para obtener más información, consulte Gramm-Leach-Bliley Act (GLBA).	2 de septiembre de 2021
Nuevo capítulo de solución de problemas	Ahora está disponible un nuevo capítulo de solución de problemas. Para obtener más información, consulte Solución de problemas en AWS Audit Manager.	23 de agosto de 2021

Nuevo capítulo y tutorial sobre la delegación	Hemos ampliado la documentación de nuestra delegación en un nuevo capítulo. Para obtener más información, consulte Delegaciones en AWS Audit Manager. También hemos añadido un nuevo tutorial dirigido a los delegados que estén revisando un conjunto de controles por primera vez AWS Audit Manager. Para obtener más informaci ón, consulte el Tutorial para delegados: Revisión de un conjunto de controles.	25 de junio de 2021
Nuevo marco compatible: NIST SP 800-171 Rev. 2	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte NIST SP 800-171 Rev. 2.	17 de junio de 2021
Informes de evaluación mejorados	Hemos mejorado el formato y el contenido de los informes de AWS Audit Manager evaluación. Para obtener más información sobre cómo navegar y comprende r los informes de evaluació n, consulte Informes de evaluación.	8 de junio de 2021

Nueva página de políticas AWS gestionadas	AWS Audit Manager ha empezado a realizar un seguimiento de los cambios de sus políticas gestionadas. Para más información, consulte Políticas administradas de AWS para AWS Audit Manager.	6 de mayo de 2021
Nuevo marco compatible: Versión 1.1 del Marco de Ciberseguridad del NIST	Ya está disponible un nuevo marco prediseñado en AWS Audit Manager. Para obtener más información, consulte la Versión 1.1 del Marco de Ciberseguridad del NIST.	5 de mayo de 2021
Nuevo marco compatible: AWS Well-Architected	Ya está disponible un nuevo marco prediseñado en. AWS Audit Manager Para obtener más información, consulte AWS Well-Architected.	5 de mayo de 2021
Nuevo marco compatible: mejores AWS prácticas fundamentales de seguridad	Ya está disponible un nuevo marco prediseñado en. AWS Audit Manager Para obtener más información, consulte Prácticas recomendadas de seguridad básica de AWS.	5 de mayo de 2021
Nuevo marco compatible: GxP, anexo 11 de la UE	Ahora hay disponible un nuevo marco prediseñado en. AWS Audit Manager Para obtener más información, consulte el GxP, anexo 11 de la UE.	28 de abril de 2021

Nuevo marco compatible: NIST 800-53 (Rev. 5) Low-Moderate-High	Ya está disponible un nuevo marco prediseñado en. AWS Audit Manager Para obtener más información, consulte el NIST 800-53 (Rev. 5). Low-Moderate-High	25 de marzo de 2021
Nuevos marcos compatibles: CIS Benchmark para CIS AWS Audit Manager Foundations Benchmark v1.3	Ya están disponibles dos nuevos marcos prediseñados AWS Audit Manager: CIS Benchmark para CIS AWS Audit Manager Foundations Benchmark v1.3.0, nivel 1, y CIS Benchmark para CIS AWS Audit Manager Foundations Benchmark v1.3.0, niveles 1 y 2. Para obtener más información, consulte CIS Benchmark para CIS AWS Audit Manager Foundations Benchmark v1.3.0.	22 de marzo de 2021
Versión inicial	Versión inicial de la guía del AWS Audit Manager usuario y la referencia de la API.	8 de diciembre de 2020

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.