Manual do usuário

AWS Artifact

AWS Artifact: Manual do usuário

Table of Contents

O que é o AWS Artifact?

AWS Artifact fornece downloads sob demanda de AWS documentos de segurança e conformidade, como certificações ISO AWS, relatórios do setor de cartões de pagamento (PCI) e relatórios de Service Organization Controls (SOC). Você pode enviar os documentos de segurança e conformidade (também conhecidos como artefatos de auditoria) para seus auditores ou reguladores a fim de demonstrar a segurança e a conformidade da infraestrutura da AWS e dos serviços usados por você. Você também pode usar esses documentos como diretrizes para avaliar sua própria arquitetura de nuvem e a eficácia dos controles internos da empresa.

Além disso, AWS Artifact fornece downloads sob demanda de documentos de segurança e conformidade, como certificações ISO e relatórios de Service Organization Controls (SOC) dos provedores de software independente (ISV) que vendem seus produtos em AWS Marketplace. Para obter mais informações, consulte AWS MarketplaceInformações do provedor.

Os clientes da AWS são responsáveis pelo desenvolvimento ou pela obtenção de documentos que demonstram a segurança e a conformidade de suas empresas. Para obter mais informações, consulte o Modelo de responsabilidade compartilhada.

Você também pode usar o AWS Artifact para analisar, aceitar e acompanhar o status de contratos da AWS, como o Business Associate Addendum (BAA). Um BAA geralmente é necessário para empresas que estão sujeitas à Lei de Responsabilidade e Portabilidade de Plano de Saúde (HIPAA) para garantir que informações de saúde protegidas (PHI) sejam protegidas adequadamente. Com o AWS Artifact, você pode aceitar contratos com o AWS e designar as contas da AWS que podem processar legalmente informações restritas. Você pode aceitar um contrato em nome de várias contas. Para aceitar contratos para várias contas, use AWS Organizations para criar uma organização.

Para obter mais informações, consulte AWS Artifact.

Preços

A AWS fornece os documentos e contratos do AWS Artifact gratuitamente para você.

Conceitos básicos do AWS Artifact

AWS Artifact fornece um recurso central para AWS relatórios de segurança e conformidade. Os artefatos disponíveis AWS Artifact incluem relatórios de Controle Organizacional de Serviços (Service Organization Controls (SOC), relatórios do Setor de Cartões de Pagamento (PCI) e certificações de órgãos de credenciamento que validam a implementação e a eficácia operacional dos AWS controles de segurança. Além disso, AWS Artifact fornece acesso sob demanda aos documentos de segurança e conformidade, como certificações ISO e relatórios de Service Organization Controls (SOC) dos provedores de software independente (ISV) que vendem seus produtos em AWS Marketplace. Para obter mais informações, consulte AWS MarketplaceInformações do provedor.

AWS Artifact permite que você aceite e gerencie contratos legais, como o Business Associate Addendum (BAA). Se você usar o AWS Organizations, poderá aceitar contratos em nome de todas as contas da sua organização. Quando aceito, todas as contas-membro existentes e subsequentes são cobertas automaticamente pelo contrato.

Tarefas

- Etapa 1: Cadastrar-se na AWS
- Etapa 2: Fazer download de um relatório
- Etapa 3: gerenciar contratos
- Etapa 4: gerenciar notificações

Etapa 1: Cadastrar-se na AWS

Se você ainda não tem Conta da AWS, siga as etapas a seguir para criar um.

Para se cadastrar em uma Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se cadastra em uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática

recomendada de segurança, atribua acesso administrativo a um usuário administrativo e use somente o usuário raiz para realizar as tarefas que exigem acesso do usuário raiz.

Etapa 2: Fazer download de um relatório

Você pode baixar relatórios usando o Adobe Acrobat Reader. Não há suporte para outros leitores de PDF. Para obter mais informações, consulte Download de relatórios.

Como fazer download de um relatório

1. Abra o console do AWS Artifact em https://console.aws.amazon.com/artifact/.
2. Na AWS Artifact página de início, escolha Exibir relatórios.
3. Na página Relatórios, use a guia AWS relatórios de para acessar relatórios AWS e navegue até a guia Relatórios de terceiros para acessar os relatórios dos provedores de software independente (ISVs) que vendem seus produtos em AWS Marketplace.
4. (Opcional) Insira uma palavra-chave no campo de pesquisa para localizar um relatório.
5. Selecione um relatório, escolha Fazer download de relatório.
6. (Opcional) Na guia Relatórios de terceiros, você pode acessar a página de detalhes de um relatório ISV clicando no título do Relatório para saber mais sobre o relatório.
7. Você pode ser solicitado a aceitar os Termos e Condições que se aplicam ao relatório específico cujo download você esteja fazendo. Recomendamos ler atentamente. Ao terminar, selecione Eu li e concordo com os termos e, em seguida, escolha Aceitar os termos e fazer download do relatório.
8. Abra o arquivo baixado por meio de um visualizador de PDF. Revise os termos e condições de aceitação e role para baixo para encontrar o relatório de auditoria. Os relatórios podem ter informações adicionais incorporadas como anexos ao documento PDF, portanto, verifique se há anexos no arquivo PDF para obter a documentação de apoio. Confira aqui as instruções sobre como visualizar os anexos.

Os relatórios de terceiros só podem ser acessados por AWS clientes que se inscreveram nas AWS MarketplaceInformações do provedor. Para saber mais, consulte AWS MarketplaceInformações do provedor.

Etapa 3: gerenciar contratos

Antes de firmar um contrato, você deve baixar e concordar com os termos do AWS Artifact contrato de confidencialidade (NDA). Cada contrato é confidencial e não pode ser compartilhado com outras pessoas fora da sua empresa.

Para aceitar um contrato com a AWS

1. Abra o console do AWS Artifact em https://console.aws.amazon.com/artifact/.
2. No painel de navegação do AWS Artifact selecione Agreements (Contratos).
3. Escolha Contratos da conta para gerenciar contratos para sua conta ou Contratos da organização para gerenciar contratos em nome de sua organização.
4. Expanda a seção do contrato.
5. Escolha Fazer download e revisar.
6. Leia todos os Termos e Condições. Quando terminar, escolha Aceitar e fazer download.
7. Revise o contrato e marque as caixas de seleção para indicar que você concorda.
8. Escolha Aceitar para aceitar o contrato.

Para obter mais informações, consulte Gerenciamento de contratos.

Etapa 4: gerenciar notificações

Você pode se inscrever para receber notificações sobre a disponibilidade de novos relatórios e contratos ou atualizações de relatórios e contratos existentes. O AWS Artifact usa o serviço de notificação de usuários da AWS para enviar notificações. As notificações são enviadas para os endereços de e-mail fornecidos pelo usuário durante a configuração da notificação.

Para criar uma configuração

1. Abra a página de hubs de notificação no serviço de notificações de usuários da AWS
2. Selecione a(s) região(ões) na(s) qual(is) você deseja armazenar seus recursos de Notificações de Usuários da AWS. Por padrão, seus dados de Notificações do Usuário serão armazenados no Leste dos EUA (Norte da Virgínia) e replicados em outras regiões que você selecionar. Consulte a documentação dos hubs de notificação para obter mais detalhes.
3. Clique em Criar configuração.

4. Para receber notificações de contratos, clique na caixa de seleção Updates on AWS Agreements (Atualizações sobre contratos da AWS).
5. Para receber notificações de relatórios, clique na caixa de seleção Updates on AWS Reports (Updates on AWS Reports). Para receber notificações somente de relatórios em categorias e séries específicas, clique na caixa de seleção de Um subconjunto de relatórios e clique na caixa de seleção das categorias e séries nas quais você está interessado.
6. Insira um nome para a sua configuração.
7. Insira uma lista de e-mails separados por vírgulas para os quais as notificações devem ser enviadas.
8. (Opcional) Para atribuir uma tag à configuração de notificação, insira os pares de valores-chave expandindo a seção Tags. Observação: uma tag é uma etiqueta que você pode atribuir a um recurso da AWS e cada tag consiste em uma chave e um valor opcional que você pode definir. Tags ajudam a gerenciar, pesquisar e filtrar recursos.
9. Clique em Enviar.
10. Um e-mail de verificação será enviado para os endereços de e-mail fornecidos e os destinatários precisarão clicar no link Verificar e-mail dentro do e-mail de verificação enviado a eles. Observe que somente endereços de e-mail verificados começarão a receber notificações.

Para obter mais informações, consulte Gerenciar notificações.

Download de relatórios no AWS Artifact

Você pode fazer download de relatórios no console do AWS Artifact. Ao fazer download de um relatório do AWS Artifact, esse relatório é gerado especificamente para você, e cada relatório contém uma marca d'água exclusiva. Por isso, você deve compartilhá-lo somente com pessoas de confiança. Não envie os relatórios por e-mail como anexos e não os compartilhe online. Para compartilhar um relatório, use um serviço de compartilhamento seguro, como o Amazon WorkDocs. Alguns relatórios exigem que você aceite os Termos e Condições antes de poder fazer download.

Índice

Download de relatório

Para fazer download de um relatório, você deve ter as permissões exigidas. Para obter mais informações, consulte Identity and Access Management no AWS Artifact.

Quando você se cadastra no AWS Artifact, sua conta recebe permissões automaticamente para fazer download de alguns relatórios. Se estiver tendo problemas para acessar AWS Artifact, siga as orientações na página de AWS Artifact Referência de Autorização de Serviço.

Como fazer download de um relatório

1. Abra o console do AWS Artifact em https://console.aws.amazon.com/artifact/.
2. Na AWS Artifactpágina de início, escolha Exibir relatórios.
3. Na página Relatórios, use a guia AWS relatórios de para acessar relatórios AWS e navegue até a guia Relatórios de terceiros para acessar os relatórios dos provedores de software independente (ISVs) que vendem seus produtos em AWS Marketplace.
4. (Opcional) Insira uma palavra-chave no campo de pesquisa para localizar um relatório.
5. Selecione um relatório, escolha Fazer download de relatório.
6. (Opcional) Na guia Relatórios de terceiros, você pode acessar a página de detalhes de um relatório ISV clicando no título do Relatório para saber mais sobre o relatório.

7. Você pode ser solicitado a aceitar os Termos e Condições que se aplicam ao relatório específico cujo download você esteja fazendo. Recomendamos ler atentamente. Ao terminar, selecione Eu li e concordo com os termos e, em seguida, escolha Aceitar os termos e fazer download do relatório.
8. Abra o arquivo baixado por meio de um visualizador de PDF. Revise os termos e condições de aceitação e role para baixo para encontrar o relatório de auditoria. Os relatórios podem ter informações adicionais incorporadas como anexos ao documento PDF, portanto, verifique se há anexos no arquivo PDF para obter a documentação de apoio. Confira aqui as instruções sobre como visualizar os anexos.

Visualizar anexos em documentos PDF

Os seguintes aplicativos que atualmente oferecem suporte à visualização de anexos em PDF são recomendados:

Visualizador do Adobe Acrobat

1. Faça download da versão mais recente do Adobe Acrobat aqui.
2. Abra o arquivo no visualizador do Adobe Acrobat.
3. Para abrir o painel Anexos, clique no ícone de clipe à esquerda do documento PDF ou escolha View > Show/Hide > Navigation Panes > Attachments (Exibir > Mostrar/Ocultar > Painéis de navegação > Anexos).
4. No painel Anexos, clique duas vezes no anexo para visualizar o documento.

Navegador Firefox

1. Baixe o navegador Firefox aqui
2. Abra o arquivo PDF no navegador Firefox usando a opção Abrir arquivo no menu Arquivo.
3. Para abrir os anexos, clique no ícone Alternar da barra lateral no canto superior esquerdo da tela.

Protegendo os seus documentos

Os documentos do AWS Artifact são confidenciais e devem ser mantidos sempre protegidos. O AWS Artifact usa o modelo de responsabilidade compartilhada AWS em seus documentos. Isso significa

que a AWS é responsável por manter os documentos seguros enquanto eles estiverem na Nuvem AWS, mas você é responsável por mantê-los seguros após obtê-los por download. AWS Artifact talvez exija que você aceite os Termos e Condições antes de fazer download dos documentos. Cada download de documento tem uma marca d'água rastreável exclusiva.

Você tem permissão para compartilhar somente os documentos marcados como confidenciais em sua empresa, com reguladores ou auditores. Você não tem permissão para compartilhar esses documentos com seus clientes ou em seu site. É altamente recomendável que você use um serviço de compartilhamento de documentos confiável, como o Amazon WorkDocs, para compartilhar documentos com outras pessoas. Não envie os documentos por e-mail nem os envie para um site que não seja seguro.

Solução de problemas

Se você não conseguir fazer o download de um documento ou receber uma mensagem de erro, consulte Solução de problemas nas AWS Artifact Perguntas frequentes.

Gerenciamento de contratos no AWS Artifact

Os contratos do AWS Artifact permitem que você use o AWS Management Console para analisar, aceitar e gerenciar contratos para sua conta ou organização. Por exemplo, um contrato de Business Associate Addendum (BAA) geralmente é necessário para empresas que estão sujeitas à Lei de Responsabilidade e Portabilidade de Plano de Saúde (HIPAA) para garantir que informações de saúde protegidas (PHI) sejam protegidas adequadamente. Você pode usar o AWS Artifact para aceitar um contrato, como o BAA com a AWS, e designar uma conta da AWS que possa processar PHI legalmente. Se você usar o AWS Organizations, poderá aceitar contratos, como o BAA da AWS, em nome de todas as contas da sua organização. Todas as contas-membro existentes e subsequentes são cobertas automaticamente pelo contrato e podem processar legalmente informações de saúde protegidas (PHI).

Você também pode usar o AWS Artifact para confirmar que sua conta ou organização da AWS aceitou um contrato e para analisar os termos do contrato aceito para entender suas obrigações. Se a sua conta ou organização não precisar mais usar o contrato aceito, você poderá usar o AWS Artifact para rescindir o contrato. Se você rescindir o contrato, mas depois perceber que precisa dele, poderá ativá-lo novamente.

Índice

Gerenciamento de um contrato para uma única conta em AWS Artifact

Você pode aceitar contratos apenas para sua conta, mesmo que ela seja uma conta-membro em uma organização no AWS Organizations. Para obter mais informações sobre o AWS Organizations, consulte o Guia do usuário do AWS Organizations.

Aceitação de um contrato com a AWS

Antes de aceitar um contrato, recomendamos que você consulte suas equipes jurídica, de privacidade e de conformidade.

Permissões obrigatórias

Se você for um administrador de uma conta, você poderá oferecer aos usuários do IAM e aos usuários federados com funções as permissões para acessar e gerenciar um ou mais contratos. Por padrão, somente os usuários com privilégios administrativos podem aceitar um contrato. Para aceitar um contrato, os usuários do IAM e os usuários federados precisam ter as seguintes permissões:

```
artifact:DownloadAgreement
artifact:AcceptAgreement
```

Para obter mais informações, consulte Gerenciamento de identidade e acesso.

Para aceitar um contrato com a AWS

1. Abra o console do AWS Artifact em https://console.aws.amazon.com/artifact/.
2. No painel de navegação do AWS Artifact selecione Contratos.
3. Selecione a guia Contratos da conta.
4. Expanda a seção do contrato.
5. Escolha Fazer download e revisar.
6. Leia todos os Termos e Condições. Quando terminar, escolha Aceitar e fazer download.
7. Revise o contrato e marque as caixas de seleção para indicar que você concorda.
8. Selecione Aceitar para aceitar o contrato apenas para sua conta.

Rescisão de um contrato com a AWS

Se usou o console do AWS Artifact para aceitar um contrato, você poderá usar o console para rescindir esse contrato. Caso contrário, consulte Contratos offline.

Permissões obrigatórias

Para encerrar um contrato, os usuários do IAM e os usuários federados precisam ter as seguintes permissões:

```
artifact:TerminateAgreement
```

Para obter mais informações, consulte Gerenciamento de identidade e acesso.

Para rescindir um contrato online com a AWS

1. Abra o console do AWS Artifact em https://console.aws.amazon.com/artifact/.
2. No painel de navegação do AWS Artifact selecione Contratos.
3. Selecione a guia Contratos da conta.
4. Selecione o contrato e escolha Rescindir contrato.
5. Marque todas as caixas de seleção para indicar que você concorda em rescindir o contrato.
6. Escolha Terminate. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

Gerenciamento de um contrato para várias contas em AWS Artifact

Se você for o proprietário da conta de gerenciamento de uma organização do AWS Organizations, poderá aceitar um contrato em nome de todas as contas de sua organização. Você deve estar conectado à conta de gerenciamento com as permissões corretas do AWS Artifact para aceitar ou rescindir contratos da organização. Os usuários de contas-membro com permissões do `organizations:DescribeOrganization` podem visualizar os contratos da organização que foram aceitos em seu nome.

Se a conta não faz parte de uma organização, crie ou ingresse em uma organização seguindo as instruções em Criar e gerenciar uma organização no AWS Organizations Guia do Usuário.

O AWS Organizations tem dois conjuntos de recursos disponíveis: recursos de faturamento consolidado e todos os recursos. Para usar o AWS Artifact para sua organização, a organização à qual você pertence precisa estar habilitada para todos os recursos. Se a organização está configurada somente para o faturamento consolidado, consulte Ativação de todos os recursos na sua organização no AWS Organizations Guia do Usuário.

Se uma conta-membro for removida de uma organização, ela não será mais coberta pelos contratos da organização. Os administradores das contas de gerenciamento deverão informar às contas-membro antes de removê-las da organização, para que elas possam colocar novos contratos em vigor, se necessário. Uma lista de contratos ativos da organização pode ser visualizada em AWS ArtifactContratos da organização.

Para obter mais informações, consulte Gerenciar contas AWS em sua organização no Guia do usuário do AWS Organizations.

Aceitação de um contrato para sua organização

Você pode aceitar um contrato em nome de todas as contas-membro de sua organização no AWS Organizations. Antes de aceitar um contrato, recomendamos que você consulte suas equipes jurídica, de privacidade e de conformidade.

Permissões obrigatórias

Para aceitar um contrato, o proprietário da conta de gerenciamento deve ter as seguintes permissões:

```
artifact:DownloadAgreement
artifact:AcceptAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

Para obter mais informações, consulte Gerenciamento de identidade e acesso.

Para aceitar um contrato para uma organização

1. Abra o console do AWS Artifact em https://console.aws.amazon.com/artifact/.
2. No painel do AWS Artifact, selecione Contratos.
3. Selecione a guia Contratos da organização.
4. Expanda a seção do contrato.
5. Escolha Fazer download e revisar.
6. Leia todos os Termos e Condições. Quando terminar, escolha Aceitar e fazer download.
7. Revise o contrato e marque as caixas de seleção para indicar que você concorda.
8. Selecione Accept (Aceitar) para aceitar o contrato para todas as contas existentes e futuras da sua organização.

Rescisão de um contrato da organização

Se usou o console do AWS Artifact para aceitar um contrato em nome de todas as contas-membro de uma organização, você poderá usar o console para rescindir esse contrato. Caso contrário, consulte Contratos offline.

Permissões obrigatórias

Para rescindir um contrato, o proprietário da conta de gerenciamento deve ter as seguintes permissões:

```
artifact:DownloadAgreement
artifact:TerminateAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

Para obter mais informações, consulte Gerenciamento de identidade e acesso.

Para rescindir um contrato de organização online com a AWS

1. Abra o console do AWS Artifact em https://console.aws.amazon.com/artifact/.
2. No painel do AWS Artifact, selecione Contratos.
3. Selecione a guia Contratos da organização.
4. Selecione o contrato e escolha Encerrar contrato.
5. Marque todas as caixas de seleção para indicar que você concorda em rescindir o contrato.
6. Escolha Terminate. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

Gerenciar um contrato offline existente em AWS Artifact

Se você tiver um contrato offline existente, o AWS Artifact exibirá os contratos que você aceitou offline. Por exemplo, o console pode exibir o Offline Business Associate Addendum (BAA) com status Active (Ativo). O status ativo indica que o contrato foi aceito. Para rescindir um contrato offline, consulte as diretrizes e instruções de rescisão incluídas no contrato.

Se a sua conta for a conta de gerenciamento em uma organização AWS Organizations, você poderá usar o AWS Artifact para aplicar os termos do contrato offline a todas as contas de sua

organização. Para aplicar um contrato que você aceitou offline à sua organização e a todas as contas da organização, você deve ter as seguintes permissões:

```
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

Se a sua conta for uma conta-membro em uma organização, você precisará ter as seguintes permissões para visualizar os contratos da organização offline:

```
organizations:DescribeOrganization
```

Para obter mais informações, consulte Gerenciamento de identidade e acesso.

Gerenciar notificações em AWS Artifact

As notificações do AWS Artifact permitem que você configure notificações por e-mail. Na página de configurações de notificação, você pode se inscrever para receber notificações e gerenciar outras configurações de notificação conforme descrito abaixo. O AWS Artifact envia notificações usando o serviço Notificações de Usuários da AWS. Para usar as notificações do AWS Artifact, você deve ter as permissões necessárias para os serviços AWS Artifact e Notificações de Usuários da AWS. Para obter mais informações, consulte Gerenciamento de identidade e acesso.

Índice

Configuração de suas notificações

Antes de começar a receber notificações, você precisará especificar a(s) região(ões) em que seus dados de Notificações do Usuário serão armazenados. Siga as etapas abaixo para configurar hubs de notificação.

Para configurar hubs de notificação

1. Abra a página de hubs de notificação no serviço Notificações de Usuários da AWS.
2. Selecione a(s) região(ões) em que você gostaria de armazenar seus recursos de notificações de usuários da AWS. Por padrão, seus dados de Notificações do Usuário serão armazenados no Leste dos EUA (Norte da Virgínia) e serão replicados nas outras regiões que você selecionou. Consulte a documentação dos hubs de notificação para obter mais detalhes.
3. Clique em Enviar.

Para assinar as notificações do

1. Abra a página de configurações de notificação do AWS Artifact.
2. Clique no botão Inscrever-se nas notificações do Artifact para assinar as notificações no AWS Artifact.

Cancelar assinatura para notificações

1. Abra a página de configurações de notificação do AWS Artifact.
2. Clique no botão Subscribe to Artifact notifications (Inscrever-se nas notificações do Artifact) para cancelar a assinatura para notificações no AWS Artitfact.

Para criar uma configuração

1. Abra a página de configurações de notificação do AWS Artifact.
2. Clique em Criar configuração.
3. Para receber notificações de contratos, mantenha a caixa de seleção marcada ao lado de Atualizações sobre contratos da AWS.
4. Para receber notificações de relatórios, mantenha a caixa de seleção marcada ao lado de Atualizações nos relatórios da AWS.
5. Para receber notificações de todos os relatórios, mantenha a caixa de seleção marcada ao lado de Todos os relatórios.
6. Para receber notificações somente para relatórios em categorias e séries específicas, clique na caixa de seleção de Um subconjunto de relatórios. Em seguida, clique na caixa de seleção das categorias e séries nas quais você está interessado.
7. Insira um nome para a sua configuração.
8. Insira uma lista separada por vírgulas de e-mails para os quais as notificações devem ser enviadas.
9. (Opcional) Para atribuir uma tag à configuração de notificação, insira os pares de valores-chave expandindo a seção Tags. Observação: uma tag é uma etiqueta que você pode atribuir a um recurso da AWS e cada tag consiste em uma chave e um valor opcional que você pode definir. Tags ajudam a gerenciar, pesquisar e filtrar recursos.
10. Clique em Criar configuração.
11. Um e-mail de verificação será enviado para os endereços de e-mail fornecidos e os destinatários precisarão clicar no link Verify email (Verificar e-mail) dentro do e-mail de verificação enviado a eles. Observe que somente endereços de e-mail verificados começarão a receber notificações.

Para editar uma configuração

1. Abra a página de configurações de notificação do AWS Artifact.

2. Clique na linha da configuração que você gostaria de editar.
3. Clique no botão Editar na parte superior direita da página.
4. Você pode editar qualquer um dos campos. Quando estiver satisfeito com sua alteração, pressione Salvar alterações.
5. Se você tiver adicionado novos endereços de e-mail, um e-mail de verificação será enviado para cada um desses endereços de e-mail. Clique no link Verificar e-mail dentro do e-mail de verificação.

Para excluir uma configuração

1. Abra a página de configurações de notificação do AWS Artifact.
2. Clique na linha da configuração que você gostaria de excluir.
3. Clique em Excluir.
4. Depois de ler a mensagem de aviso, clique em Excluir.

Atribuir tags a uma configuração

Uma tag é um rótulo atribuído a um recurso da AWS. Cada tag consiste em uma chave e um valor opcional, ambos definidos por você. Tags ajudam a gerenciar, pesquisar e filtrar recursos. Opcionalmente, você pode definir tags ao criar ou editar uma configuração. Para ler mais, consulte Recursos de marcação

Solução de problemas

Se receber uma mensagem de erro ao usar as notificações do AWS Artifact, consulte Solução de problemas nas AWS Artifact perguntas frequentes.

Identity and Access Management no AWS Artifact

Ao se cadastrar na AWS, você fornece um endereço de e-mail e uma senha que são associados à sua conta da AWS. Estas são suas credenciais raiz e elas fornecem acesso total a todos os seus recursos da AWS, incluindo os recursos para AWS Artifact. No entanto, é altamente recomendável que você não use a conta raiz para acesso diário. Também é recomendável que você não compartilhe as credenciais da conta com outras pessoas para evitar conceder a elas acesso total à sua conta.

Em vez fazer login na conta AWS com suas credenciais raiz ou compartilhar suas credenciais com outras pessoas, crie uma identidade especial de usuário chamada usuário do IAM para você e para qualquer pessoa que possa precisar de acesso a um documento ou contrato no AWS Artifact. Com essa abordagem, você pode fornecer informações individuais de login para cada usuário e conceder a cada um deles somente as permissões de que precisam para trabalhar com documentos específicos. Você também pode conceder a vários usuários do IAM; as mesmas permissões. Para isso, conceda as permissões a um grupo do IAM; e adicione os usuários do IAM ao grupo.

Se você já gerencia identidades de usuários fora da AWS, pode usar provedores de identidade do IAM em vez de criar usuários do IAM. Para obter mais informações, consulte Provedores de identidade e federação no Guia do usuário do IAM.

Conteúdos

Configurar o acesso do usuário ao AWS Artifact

Conclua as etapas a seguir para conceder permissões aos usuários AWS Artifact com base no nível de acesso de que precisam.

Tarefas

Etapa 1: criar uma política do IAM

Como administrador do IAM, você pode criar uma política que conceda permissões a AWS Artifact ações e recursos.

Para criar uma política do IAM

Use o procedimento a seguir para criar uma política do IAM que você pode usar para conceder permissões aos seus usuários e grupos do IAM.

1. Abra o console IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies.
3. Escolha Criar política.
4. Escolha a guia JSON.
5. Insira um documento de política. Você pode criar sua própria política ou usar uma das políticas de Políticas de exemplo do IAM.
6. Escolha Revisar política. O validador de política indica se há qualquer erro de sintaxe.
7. Na página Revisar política, insira um nome exclusivo que o ajude a lembrar a finalidade da política. Você também pode adicionar uma descrição.
8. Escolha Create policy (Criar política).

Etapa 2: Criar um grupo do IAM e associar a política

Como administrador do IAM, é possível criar um grupo e anexar a política que você criou para o grupo. Você pode adicionar usuários do IAM ao grupo a qualquer momento.

Para criar um grupo do IAM e anexar sua política

1. No painel de navegação, escolha Grupos e escolha, Criar novo grupo.
2. Em Nome do grupo, insira um nome para o grupo e selecione Próxima etapa.
3. No campo de pesquisa, digite o nome da política que você criou. Marque a caixa de seleção da sua política e escolha Próxima etapa.
4. Revise o nome e as políticas do grupo. Quando você estiver pronto, selecione Criar grupo.

Etapa 3: criar usuários do IAM e adicioná-los ao grupo

Como administrador do IAM, é possível adicionar usuário a um grupo a qualquer momento. Isso concede aos usuários as permissões concedidas ao grupo.

Para criar um usuário do IAM e adicionar esse usuário ao grupo

1. No painel de navegação, escolha Usuários e depois Adicionar usuário.
2. Em Nome do usuário insira os nomes de um ou mais usuários.
3. Marque a caixa de seleção ao lado do acesso ao AWS Management Console. Configure uma senha personalizada ou gerada automaticamente. Se preferir, você pode selecionar Usuário deve criar uma senha no próximo login para exigir uma senha quando o usuário fizer login pela primeira vez.
4. Escolha Próximo: permissões.
5. Escolha Adicionar usuário ao grupo e selecione o grupo que você criou.
6. Escolha Próximo: tags. Se preferir, você pode adicionar tags aos seus usuários.
7. Escolha Próximo: revisar. Quando estiver pronto, escolha Criar usuário.

Migrar para permissões refinadas

O AWS Artifact agora permite que os clientes usem permissões refinadas. Por meio dessas permissões refinadas, os clientes terão controle granular sobre o fornecimento de acesso a recursos, como aceitar termos e baixar relatórios.

Para acessar relatórios por meio de permissões refinadas, os clientes devem utilizar a política gerenciada AWSArtifactReportsReadOnlyAccess ou atualizar suas permissões de acordo com a recomendação abaixo. Depois, os clientes devem aceitar usando o link testar a nova página de relatórios da AWS, disponível no console.

Os usuários terão a opção de acessar os relatórios com as permissões antigas com o link usar página de relatórios antiga disponível no console caso haja algum problema em atualizar para as novas permissões.

Migrar para novas permissões

Migrar permissões não específicas do recurso

Os usuários precisam substituir a política existente que contêm as permissões antigas por uma política com permissões refinadas

Política antiga:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get"
      ],
      "Resource": [
        "arn:aws:artifact:::report-package/*"
      ]
    }
  ]
}
```

Nova política com permissões refinadas:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

Migrar permissões não específicas do recurso

Os usuários precisam substituir a política existente com as permissões antigas por uma política com permissões refinadas. As permissões-curinga do recurso de relatório foram substituídas por chaves de condição.

Política antiga:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get"
      ],
      "Resource": [
        "arn:aws:artifact:::report-package/Certifications and Attestations/SOC/*",
        "arn:aws:artifact:::report-package/Certifications and Attestations/PCI/*",
        "arn:aws:artifact:::report-package/Certifications and Attestations/ISO/*"
      ]
    }
  ]
}
```

Nova política com permissões refinadas e chaves de condição.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications and Attestations"
          ]
        }
      }
    }
  ]
}
```

Políticas de exemplo do IAM

Você pode criar políticas de permissões que concedam permissões ao usuários do IAM. Você pode conceder aos usuários acesso a AWS Artifact relatórios e a capacidade de aceitar e baixar contratos em nome de uma única conta ou organização.

Os Exemplo de políticas a seguir mostram as permissões que você pode atribuir aos usuários do IAM com base no nível de acesso de que eles precisam.

- Exemplos de políticas para gerenciar AWS relatórios com permissões refinadas
- Exemplo de políticas para gerenciar relatórios de terceiros
- Exemplo de políticas para gerenciar contratos
- Exemplos de políticas para integração com AWS Organizations
- Exemplo de políticas para gerenciar contratos para a conta de gerenciamento
- Exemplo de políticas para gerenciar contratos da organização
- Exemplo de políticas para gerenciar notificações

Example Exemplos de políticas para gerenciar AWS relatórios por meio de permissões refinadas

> **Tip**
>
> Você deve considerar o uso da política AWSArtifactReportsReadOnlyAccess gerenciada em vez de definir sua própria política.

A política a seguir concede permissão para baixar todos os AWS relatórios por meio de permissões refinadas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

A política a seguir concede permissão para baixar somente os relatórios AWS SOC, PCI e ISO por meio de permissões refinadas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications And Attestations"
          ]
        }
      }
    }
  ]
}
```

Example Exemplo de políticas para gerenciar relatórios de terceiros

> **Tip**
>
> Você deve considerar o uso da política AWSArtifactReportsReadOnlyAccess gerenciada em vez de definir sua própria política.

Os relatórios de terceiros são indicados pelo recurso do IAM. `report`

A política a seguir concede permissão para todas as funcionalidades de relatórios de terceiros.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
```

```
  ]
}
```

A política a seguir concede permissão para fazer download de relatórios de terceiros.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

A política a seguir concede permissão para listar relatórios de terceiros.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReport"
      ],
      "Resource": "*"
    }
  ]
}
```

A política a seguir concede permissão para visualizar informações de relatórios de terceiros.

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

```
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh"
      ]
    }
  ]
}
```

Example Exemplo de políticas para gerenciar contratos

A política a seguir concede permissão para fazer download de todos os contratos. Os usuários do IAM precisam ter essa permissão para aceitar contratos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

A política a seguir concede permissão para aceitar um contrato.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "*"
```

```
      ]
    }
  ]
}
```

A política a seguir concede permissão para rescindir um contrato.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

A política a seguir concede permissões para gerenciar contratos de conta única.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

Example Exemplos de políticas para integração com AWS Organizations

A política a seguir concede permissão para criar a função do IAM que AWS Artifact usa para integração com AWS Organizations. A conta de gerenciamento da sua organização deve ter essas permissões para começar a usar os Contratos da organização.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam::*:role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

A política a seguir concede permissão para conceder AWS Artifact as permissões de uso AWS Organizations. A conta de gerenciamento da sua organização deve ter essas permissões para começar a usar os Contratos da organização.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example Exemplo de políticas para gerenciar contratos para a conta de gerenciamento

A política a seguir concede permissões para gerenciar contratos para a conta de gerenciamento.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam::*:role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example Exemplo de políticas para gerenciar contratos da organização

A política a seguir concede permissões para gerenciar contratos da organização. Outro usuário com as permissões necessárias deve configurar os contratos da organização.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

A política a seguir concede permissões para exibir contratos da organização.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
```

```
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example Exemplo de políticas para gerenciar notificações

A política a seguir concede permissões completas para usar AWS Artifact notificações.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DisassociateChannel",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:DeleteEmailContact",
```

```
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:SendActivationCode"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

A política a seguir concede permissão para listar todas as configurações.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

A política a seguir concede permissão para criar uma configuração.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
```

```
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:SendActivationCode",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:ListEventRules",
        "notifications:ListNotificationHubs",
        "notifications:TagResource",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

A política a seguir concede permissão para editar uma configuração.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:DisassociateChannel",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
```

```
    }
  ]
}
```

A política a seguir concede permissão para excluir uma configuração.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeleteNotificationConfiguration",
        "notifications:ListEventRules"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

A política a seguir concede permissão para exibir informações de uma configuração.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

A política a seguir concede permissão para registrar ou cancelar o registro de hubs de notificação.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeregisterNotificationHub",
        "notifications:RegisterNotificationHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Políticas gerenciadas pela AWS para o AWS Artifact

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

Lembre-se de que as políticas gerenciadas pela AWS podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para todos AWS os clientes da usarem. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em uma política gerenciada pela AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política está vinculada. É mais provável que a AWS atualize uma política gerenciada pela AWS quando um novo AWS service (Serviço da AWS) é lançado ou novas operações de API são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte AWSPolíticas gerenciadas pela no Manual do usuário do IAM.

Política gerenciada pela AWS: AWSArtifactReportsReadOnlyAccess

É possível anexar a política `AWSArtifactReportsReadOnlyAccess` a suas identidades do IAM.

Essa política concede permissões *somente leitura* que permitem listar, visualizar e baixar relatórios.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `artifact`: permite que as entidades principais listem, visualizem e baixem relatórios do AWS Artifact.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

Atualizações do Artifact para as políticas gerenciadas pela AWS

Visualize os detalhes sobre as atualizações das políticas gerenciadas pela AWS para o Artifact desde que esse serviço começou a rastrear tais alterações. Para receber alertas automáticos sobre as alterações feitas nesta página, inscreva-se para receber feeds RSS na página Histórico de documentos do Artifact.

Alteração	Descrição	Data
O Artifact começou a rastrear alterações	A Artifact começou a rastrear as alterações em suas políticas gerenciadas pela AWS e introduziu a política AWSArtifactReportsReadOnlyAccess.	15/12/2023

Uso de funções vinculadas ao serviço do AWS Artifact

O AWS Artifact usa AWS Identity and Access Management funções vinculadas a serviços (IAM). A função vinculada a serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao AWS Artifact. As funções vinculadas a serviço são predefinidas pelo AWS Artifact e incluem todas as permissões que o produto requer para chamar outros produtos da AWS em seu nome.

Um perfil vinculado ao serviço facilita a configuração do AWS Artifact porque você não precisa adicionar as permissões necessárias manualmente. O AWS Artifact define as permissões das funções vinculadas ao serviço e, exceto se definido de outra forma, somente o AWS Artifact pode assumir suas funções. As permissões definidas incluem as políticas de confiança e de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você só pode excluir um perfil vinculado a serviço depois de excluir os recursos relacionados. Isso protege seus recursos do AWS Artifact, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros produtos que oferecem suporte às funções vinculadas a serviços, consulte AWS services that work with IAM (Produtos da compatíveis com o IAM) e procure os serviços que apresentam Yes (Sim) na coluna Service-linked roles (Funções vinculadas a serviços). Escolha Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculada a serviço para o AWS Artifact

O AWS Artifact usa a função vinculada ao serviço chamada AWSServiceRoleForArtifact — Permite que o AWS Artifact colete informações sobre uma organização por meio do serviço AWS Organizations.

O perfil vinculado ao serviço AWSServiceRoleForArtifact confia nos seguintes serviços para assumir o perfil:

- `artifact.amazonaws.com`

A política de permissão de função chamada AWSArtifactServiceRolePolicy permite que o AWS Artifact conclua as seguintes ações no recurso `organizations`.

- `DescribeOrganization`
- `DescribeAccount`
- `ListAccounts`
- `ListAWSServiceAccessForOrganization`

Criação de uma função vinculada a serviço para o AWS Artifact

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você acessa a guia Contratos da Organização em uma conta de gerenciamento da organização e seleciona o link “Get started” na AWS Management Console, o AWS Artifact cria a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, você poderá usar esse mesmo processo para recriar o perfil em sua conta. Quando você acessa a guia Contratos da Organização em uma conta de gerenciamento da organização e seleciona o link “Get started”, o AWS Artifact cria a função vinculada ao serviço para você novamente.

Edição de uma função vinculada a serviço para o AWS Artifact

O AWS Artifact não permite editar a função vinculada ao serviço AWSServiceRoleForArtifact. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ela. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Exclusão de uma função vinculada a serviço para o AWS Artifact

Se você não precisar mais usar um recurso ou serviço que exija uma função vinculada a um serviço, recomendamos que você exclua essa função. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de exclui-la manualmente.

> **Note**
>
> Se o serviço AWS Artifact estiver usando a função quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir os recursos do AWS Artifact usados por AWSServiceRoleForArtifact

1. Visite a tabela “Contratos da organização” no console do AWS Artifact
2. Encerrar quaisquer contratos ativos da organização

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API AWS para excluir o perfil vinculado ao serviço AWSServiceRoleForArtifact. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões compatíveis com funções vinculadas ao serviço do AWS Artifact

O AWS Artifact não oferece suporte ao uso de funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Você pode usar a função AWSServiceRoleForArtifact nas regiões a seguir.

Nome da região	Identidade da região	Suporte no AWS Artifact
Leste dos EUA (Norte da Virgínia)	us-east-1	Sim
Leste dos EUA (Ohio)	us-east-2	Não
Oeste dos EUA (Norte da Califórnia)	us-west-1	Não
Oeste dos EUA (Oregon)	us-west-2	Sim
África (Cidade do Cabo)	af-south-1	Não
Ásia-Pacífico (Hong Kong)	ap-east-1	Não
Ásia-Pacífico (Jacarta)	ap-southeast-3	Não

Nome da região	Identidade da região	Suporte no AWS Artifact
Ásia-Pacífico (Mumbai)	ap-south-1	Não
Ásia-Pacífico (Osaka)	ap-northeast-3	Não
Ásia-Pacífico (Seul)	ap-northeast-2	Não
Ásia-Pacífico (Singapura)	ap-southeast-1	Não
Ásia-Pacífico (Sydney)	ap-southeast-2	Não
Ásia-Pacífico (Tóquio)	ap-northeast-1	Não
Canadá (Central)	ca-central-1	Não
Europa (Frankfurt)	eu-central-1	Não
Europa (Irlanda)	eu-west-1	Não
Europa (Londres)	eu-west-2	Não
Europa (Milão)	eu-south-1	Não
Europa (Paris)	eu-west-3	Não
Europa (Estocolmo)	eu-north-1	Não
Oriente Médio (Barém)	me-south-1	Não
Oriente Médio (Emirados Árabes Unidos)	me-central-1	Não
América do Sul (São Paulo)	sa-east-1	Não
AWS GovCloud (Leste dos EUA)	us-gov-east-1	Não
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	Não

Usar chaves de condição do IAM

Você pode usar as chaves de condição do IAM para fornecer acesso refinado aos relatórios do AWS Artifact, baseado em categorias e séries de relatórios específicas.

Os exemplos de políticas a seguir mostram as permissões que você pode atribuir aos usuários do IAM baseado em categorias e séries de relatórios específicas.

Example Exemplo de políticas para gerenciar acesso para leitura de relatórios da AWS

Os relatórios do AWS Artifact são indicados pelo recurso `report` do IAM.

A política a seguir concede permissão de ler de todos os relatórios do AWS Artifact da categoria `Certifications and Attestations`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

A política a seguir permite que você conceda permissão para ler todos os relatórios do AWS Artifact da série SOC.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "artifact:ListReports"
            ],
            "Resource": "*"
        },{
            "Effect": "Allow",
            "Action": [
                "artifact:GetReport",
                "artifact:GetReportMetadata",
                "artifact:GetTermForReport"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "artifact:ReportSeries": "SOC",
                    "artifact:ReportCategory": "Certifications and Attestations"
                }
            }
        }
    ]
}
```

A política a seguir permite que você conceda permissão para ler todos os relatórios do AWS Artifact, exceto os da categoria `Certifications and Attestations`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
```

```
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": "SOC",
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

Registrar em log chamadas de API do AWS Artifact com o AWS CloudTrail

O AWS Artifact é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS no AWS Artifact. O CloudTrail captura as chamadas de API do AWS Artifact como eventos. As chamadas capturadas incluem as chamadas do console do AWS Artifact e as chamadas de código para as operações da API do AWS Artifact. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o AWS Artifact. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o AWS Artifact, o endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações do AWS Artifact no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre uma atividade no AWS Artifact, ela é registrada em um evento do CloudTrail junto com outros eventos de serviços da AWS em Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Viewing events with CloudTrail Event history (Como visualizar eventos com o histórico de eventos do CloudTrail).

Para obter um registro contínuo de eventos na sua Conta da AWS, incluindo eventos para o AWS Artifact, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail

- Receiving CloudTrail log files from multiple regions e Receiving CloudTrail log files from multiple accounts

O AWS Artifact é compatível com as seguintes ações como eventos nos arquivos de log do CloudTrail:

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre entradas de arquivos de log do AWS Artifact

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação GetReportMetadata.

```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:03:36Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "errorCode": "AccessDenied",
      "errorMessage": "User: arn:aws:iam::999999999999:user/myUserName is not
 authorized to perform: artifact:GetReportMetadata on resource: arn:aws:artifact:us-
east-1::report/report-f1DIWBmGa2Lhsadg",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:04:42Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
```

```
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "requestParameters": {
        "reportId": "report-f1DIWBmGa2Lhsadg"
      },
      "responseElements": null,
      "requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    }
  ]
}
```

Histórico da documentação do AWS Artifact

A seguinte tabela descreve todas as versões de AWS Artifact.

Alteração	Descrição	Data
Acesso refinado a relatórios e política gerenciada AWSArtifactReportReadOnlyAccess	Habilitado o acesso refinado aos Artifact Reports, habilitadas as chaves de condição de relatório e lançada a política gerenciada AWSArtifactReportsReadOnlyAccess.	15 de dezembro de 2023
Função vinculada a serviços do AWS Artifact	Foi adicionada documentação de funções vinculadas a serviços e exemplos de políticas atualizadas para a integração entre o AWS Artifact e o AWS Organizations.	26 de setembro de 2023
Notificações	Publicou a documentação para gerenciar notificações e fez atualizações relevantes no guia de referência da API, na documentação de registro do CloudTrail e na página AWS Artifact Identity and Access Management.	1º de agosto de 2023
Relatórios de terceiros - Disponível ao público em geral	Foi adicionada documentação de referência da API, documentação de registro do CloudTrail e disponibilizou relatórios de terceiros ao público em geral.	27 de janeiro de 2023

Relatórios de terceiros (versão prévia)	Lançou relatórios de conformidade dos provedores de software independentes (ISVs) que vendem seus produtos no. AWS Marketplace Além disso, foram adicionados exemplos de políticas à página de gerenciamento de identidade e acesso para relatórios de terceiros.	30 de novembro de 2022
Segurança	Seção adicionada à página de gerenciamento de identidade e acesso para prevenção confusa de delegados.	20 de dezembro de 2021
Relatórios	O contrato de confidencialidade foi removido e os termos e condições foram introduzidos para downloads de relatórios.	17 de dezembro de 2020
Página inicial e pesquisa	Adicionamos a página inicial do serviço e a barra de pesquisa na página de relatórios e contratos.	15 de maio de 2020
Lançamento do GovCloud	Lançado AWS Artifact nas regiões do GovCloud.	7 de novembro de 2019
AWS Organizations Contratos	Adicionado suporte para gerenciar contratos para uma organização.	20 de junho de 2018
Contratos	Foi adicionado suporte para gerenciar contratos AWS Artifact.	17 de junho de 2017

Lançamento inicial	Essa versão apresenta o AWS Artifact.	30 de novembro de 2016

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.