Manual do usuário

AWS Artifact

AWS Artifact: Manual do usuário

Table of Contents

O que é AWS Artifact?

AWS Artifact fornece downloads sob demanda de documentos de AWS segurança e conformidade. Por exemplo, relatórios sobre conformidade com os padrões da Organização Internacional de Padronização (ISO) e com os Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e com os relatórios de Controles Organizacionais e de Sistemas (SOC). AWS Artifact também fornece downloads de certificações de órgãos de credenciamento que validam a implementação e a eficácia operacional dos controles de segurança. AWS

Com AWS Artifact, você também pode baixar documentos de segurança e conformidade para fornecedores independentes de software (ISVs) que vendem seus produtos em AWS Marketplace. Para obter mais informações, consulte AWS Marketplace Informações do provedor.

Além disso, você pode usar AWS Artifact para revisar, aceitar e rastrear o status de seus contratos com AWS você Conta da AWS e com vários Contas da AWS em sua organização. Para obter mais informações sobre contratos em AWS Artifact, consulteGerenciando contratos em AWS Artifact.

Para demonstrar a segurança e a conformidade da AWS infraestrutura e dos serviços que você usa, você pode enviar AWS Artifact documentos aos seus auditores ou reguladores como artefatos de auditoria. Você também pode usar esses artefatos de auditoria como diretrizes para avaliar sua própria arquitetura de nuvem e avaliar a eficácia dos controles internos da sua empresa. Para obter mais informações sobre artefatos de auditoria, consulte AWS Artifact FAQs.

> **Note**
>
> AWS os clientes são responsáveis por desenvolver ou obter documentos que demonstrem a segurança e a conformidade de suas empresas. Para obter mais informações, consulte Modelo de responsabilidade compartilhada.

Definição de preço

AWS fornece AWS Artifact documentos e acordos para você gratuitamente.

Começando com AWS Artifact

Para começar a usar AWS Artifact, experimente seus principais recursos no AWS Artifact console. No console, você pode baixar relatórios de AWS segurança e conformidade, baixar e aceitar contratos legais e assinar notificações sobre AWS Artifact documentos.

Pré-requisitos

Para usar os recursos do AWS Artifact, você deve ter um Conta da AWS. Para obter instruções de configuração, consulte Configurar um novo Conta da AWS no Guia do usuário de AWS configuração.

Recursos

Para obter instruções sobre como usar os recursos do AWS Artifact, consulte os seguintes tópicos:

- Download de relatórios
- Gerenciamento de contratos
- Configurar notificações

Baixando relatórios em AWS Artifact

Você pode baixar relatórios do AWS Artifact console. Quando você baixa um relatório do AWS Artifact, o relatório é gerado especificamente para você, e cada relatório tem 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.

Sumário

Download de relatório

Para fazer download de um relatório, você deve ter as permissões exigidas. Para obter mais informações, consulte Gerenciamento de identidade e acesso em AWS Artifact.

Quando você se inscreve AWS Artifact, sua conta recebe automaticamente permissões para baixar alguns relatórios. Se você estiver tendo problemas para acessar AWS Artifact, siga as orientações na página de referência AWS Artifact de autorização de serviço.

Como fazer download de um relatório

1. Abra o AWS Artifact console em https://console.aws.amazon.com/artifact/.
2. Na página AWS Artifact inicial, escolha Exibir relatórios.

   Na página Relatórios, na guia AWS relatórios, você pode acessar AWS relatórios (por exemplo, SOC 1/2/3PCI, C5 e assim por diante). Na guia Relatórios de terceiros, você pode acessar relatórios de fornecedores independentes de software (ISVs) que vendem seus produtos em AWS Marketplace.
3. (Opcional) Para encontrar um relatório, insira uma palavra-chave no campo de pesquisa. Você também pode realizar pesquisas direcionadas de relatórios com base em colunas individuais, incluindo título, categoria, série e descrição do relatório. Por exemplo, para encontrar o relatório

do Catálogo de Controles de Conformidade de Computação em Nuvem (C5), você pode pesquisar a coluna Título usando “Título”, o operador “contém” (:) e o termo “C5" (). **`Title : C5`**

4. (Opcional) Para obter mais informações sobre um relatório, escolha o título do relatório para abrir sua página de detalhes.
5. Selecione um relatório, escolha Fazer download de relatório.
6. Você pode ser solicitado a aceitar os termos e condições (Aceite os termos para baixar o relatório) do relatório específico que você está baixando. Recomendamos que você leia atentamente os termos e condições. Ao terminar de ler, selecione Eu li e concordo com os termos e, em seguida, escolha Aceitar os termos e baixar o relatório.
7. Abra o arquivo baixado por meio de um PDF visualizador. 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 PDF documento, portanto, verifique se há anexos no PDF arquivo para obter a documentação de apoio. Para obter instruções sobre como visualizar anexos, consulte. Visualizando anexos em documentos PDF

Visualizando anexos em documentos PDF

Recomendamos os seguintes aplicativos que atualmente oferecem suporte à visualização de PDF anexos:

Adobe Acrobat Reader

Baixe a versão mais recente do Adobe Acrobat Reader no site da Adobe em https://get.adobe.com/reader/.

Para obter instruções sobre como visualizar PDF anexos no Acrobat Reader, consulte Links e anexos no site de suporte PDFs da Adobe.

Navegador Firefox

1. Baixe a versão mais recente do navegador Firefox no site da Mozilla em https://www.mozilla.org/en-US/firefox/new/.
2. Abra o PDF arquivo no PDF visualizador embutido do Firefox. Para obter instruções, consulte Exibir PDF arquivos no Firefox ou escolha outro visualizador no site de suporte da Mozilla.
3. Para ver PDF anexos no PDF visualizador embutido do Firefox, escolha Alternar barra lateral, Mostrar anexos.

Protegendo os seus documentos

AWS Artifact os documentos são confidenciais e devem ser mantidos em segurança o tempo todo. AWS Artifact usa o modelo de responsabilidade AWS compartilhada para seus documentos. Isso significa que AWS é responsável por manter os documentos seguros enquanto eles estão na AWS nuvem, mas você é responsável por mantê-los seguros depois de baixá-los. AWS Artifact pode exigir que você aceite os Termos e condições antes de poder baixar os 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 seguro de compartilhamento de documentos, como a 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 baixar um documento ou receber uma mensagem de erro, consulte Solução de problemas no AWS Artifact FAQ.

Gerenciando contratos em AWS Artifact

Você pode usar AWS Artifact para revisar e gerenciar contratos para sua Conta da AWS organização. Por exemplo, empresas sujeitas à Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) normalmente exigem um acordo de Adendo de Associado Comercial (BAA) AWS para garantir que as informações de saúde protegidas (PHI) sejam protegidas adequadamente. No AWS Artifact console, você pode revisar e aceitar esses contratos e designar um Conta da AWS que possa ser PHI processado legalmente.

Se você usa AWS Organizations, você pode aceitar acordos, como um BAA com AWS, em nome de todos Contas da AWS em sua organização. Todas as contas de membros existentes e subsequentes são automaticamente cobertas pelo contrato e podem ser processadas legalmentePHI.

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

Sumário

Aceitando acordos para sua Conta da AWS entrada AWS Artifact

Você pode usar o AWS Artifact console para revisar e aceitar contratos com AWS o seu Conta da AWS.

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

Permissões obrigatórias

Se você for administrador de uma conta, poderá conceder IAM aos usuários e usuários federados as permissões para acessar e gerenciar um ou mais de seus contratos. Por padrão, somente os usuários com privilégios administrativos podem aceitar um contrato. Para aceitar um contrato, IAM os usuários federados devem ter as permissões necessárias.

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

Para aceitar um acordo com AWS

1. Abra o AWS Artifact console em https://console.aws.amazon.com/artifact/.
2. No painel de AWS Artifact navegação, escolha Acordos.
3. Selecione a guia Contratos da conta.
4. Abra o AWS Artifact console em https://console.aws.amazon.com/artifact/.
5. No painel de navegação, escolha Acordos.
6. Na página Acordos, faça o seguinte:
   - Para aceitar um contrato somente para sua conta, escolha a guia Contratos de conta.
   - Para aceitar um contrato em nome da sua organização, escolha a guia Acordos da organização.
7. Selecione um contrato e, em seguida, escolha Baixar contrato.

   A caixa de diálogo NDAAceitar o download do relatório é exibida.
8. Antes de fazer o download do contrato selecionado, você deve primeiro aceitar os termos do Contrato de AWS Artifact Confidencialidade (AWS Artifact NDA).

   a. Na caixa de diálogo NDAAceitar o download do relatório, revise AWS Artifact NDA o.

   b. (Opcional) Para imprimir uma cópia do AWS Artifact NDA (ou salvá-la comoPDF), escolha Imprimir NDA.

   c. Selecione Eu li e concordo com todos os termos doNDA.

   d. Para aceitar AWS Artifact NDA e baixar um PDF dos contratos que você selecionou, escolha Aceitar NDA e fazer o download.
9. Em um PDF visualizador, revise o contrato PDF que você baixou.
10. No AWS Artifact console, com o contrato selecionado, escolha Aceitar contrato.
11. Na caixa de diálogo Aceitar contrato, faça o seguinte:

a. Revise o contrato.
b. Selecione Eu concordo com todos esses termos e condições.
c. Escolha Aceitar contrato.

12. Selecione Aceitar para aceitar o contrato apenas para sua conta.

Rescisão de contratos para você Conta da AWSAWS Artifact

Se você usou o AWS Artifact console para aceitar um contrato para um único Conta da AWS, poderá usar o console para rescindir esse contrato. Caso contrário, consulte Acordos off-line em AWS Artifact.

Permissões obrigatórias

Para rescindir um contrato, IAM os usuários federados devem ter as permissões necessárias.

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

Para rescindir seu contrato on-line com AWS

1. Abra o AWS Artifact console em https://console.aws.amazon.com/artifact/.
2. No painel de AWS Artifact navegação, escolha Acordos.
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 Encerrar. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

Aceitando acordos para sua organização em AWS Artifact

Se você for o proprietário da conta de gerenciamento de uma AWS Organizations organização, poderá aceitar um contrato AWS em nome de todos Contas da AWS na sua organização.

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

AWS Organizations tem dois conjuntos de recursos disponíveis: recursos de faturamento consolidado e todos os recursos. Para ser usada AWS Artifact em sua organização, a organização à qual você pertence deve 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.

Para aceitar ou rescindir os contratos da organização, você deve estar conectado à conta de gerenciamento com as AWS Artifact permissões corretas. Os usuários de contas de membros que têm `organizations:DescribeOrganization` permissões podem visualizar os acordos da organização que são aceitos em seu nome.

Para obter mais informações, consulte Gerenciamento de contas em uma organização AWS Organizations no Guia do AWS Organizations usuário.

Permissões obrigatórias

Para aceitar um contrato, o proprietário da conta de gerenciamento deve ter as permissões necessárias.

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

Para aceitar um contrato para uma organização

1. Abra o AWS Artifact console em https://console.aws.amazon.com/artifact/.
2. No AWS Artifact painel, escolha Acordos.
3. Selecione a guia Contratos da organização.
4. Abra o AWS Artifact console em https://console.aws.amazon.com/artifact/.
5. No painel de navegação, escolha Acordos.
6. Na página Acordos, faça o seguinte:
   - Para aceitar um contrato somente para sua conta, escolha a guia Contratos de conta.
   - Para aceitar um contrato em nome da sua organização, escolha a guia Acordos da organização.
7. Selecione um contrato e, em seguida, escolha Baixar contrato.

   A caixa de diálogo NDAAceitar o download do relatório é exibida.
8. Antes de fazer o download do contrato selecionado, você deve primeiro aceitar os termos do Contrato de AWS Artifact Confidencialidade (AWS Artifact NDA).

a. Na caixa de diálogo NDAAceitar o download do relatório, revise AWS Artifact NDA o.
b. (Opcional) Para imprimir uma cópia do AWS Artifact NDA (ou salvá-la comoPDF), escolha Imprimir NDA.
c. Selecione Eu li e concordo com todos os termos doNDA.
d. Para aceitar AWS Artifact NDA e baixar um PDF dos contratos que você selecionou, escolha Aceitar NDA e fazer o download.

9. Em um PDF visualizador, revise o contrato PDF que você baixou.
10. No AWS Artifact console, com o contrato selecionado, escolha Aceitar contrato.
11. Na caixa de diálogo Aceitar contrato, faça o seguinte:

a. Revise o contrato.
b. Selecione Eu concordo com todos esses termos e condições.
c. Escolha Aceitar contrato.

12. Escolha Aceitar para aceitar o contrato para todas as contas existentes e futuras em sua organização.

Rescisão de contratos para sua organização em AWS Artifact

Se você usou o AWS Artifact console para aceitar um contrato em nome de todas as contas membros de uma organização em AWS Organizations, poderá usar o console para rescindir esse contrato. Caso contrário, consulte Acordos off-line em AWS Artifact.

Se uma conta de membro for removida de uma organização, essa conta de membro estará mais coberta pelos acordos da organização. Antes de remover as contas dos membros de uma organização, um administrador da conta de gerenciamento deve comunicar isso às contas dos membros para que eles possam estabelecer novos contratos, se necessário. Você pode ver uma lista de acordos organizacionais ativos no AWS Artifact console na página Acordos, em Acordos organizacionais.

Para obter mais informações sobre AWS Organizations, consulte Gerenciamento de contas em uma organização AWS Organizations no Guia do AWS Organizations usuário.

Permissões obrigatórias

Para rescindir um contrato, o proprietário da conta de gerenciamento deve ter as permissões necessárias.

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

Para rescindir seu contrato de organização on-line com AWS

1. Abra o AWS Artifact console em https://console.aws.amazon.com/artifact/.
2. No AWS Artifact painel, escolha Acordos.
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 Encerrar. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

Acordos off-line em AWS Artifact

Se você tiver um contrato off-line existente, AWS Artifact exibirá os contratos que você aceitou off-line. Por exemplo, o console pode exibir o Adendo de Associado Comercial Offline (BAA) com um status 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 sua conta for a conta de gerenciamento em uma AWS Organizations organização, você poderá usar AWS Artifact para aplicar os termos do seu contrato offline a todas as contas em sua organização. Para aplicar um contrato que você aceitou offline à sua organização e a todas as contas da sua organização, você deve ter as permissões necessárias.

Se sua conta for uma conta de membro em uma organização, você deverá ter as permissões para ver seus contratos organizacionais offline.

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

Configurando notificações por e-mail no AWS Artifact

Você pode usar o AWS Artifact console para configurar notificações por e-mail para atualizações sobre contratos e relatórios em AWS Artifact. AWS Artifact envia essas notificações por e-mail usando Notificações de Usuários da AWS. Para receber notificações AWS Artifact por e-mail, você deve primeiro selecionar os hubs de Notificações de Usuários da AWS notificação no Notificações de Usuários console. Em seguida, no AWS Artifact console, você pode criar uma configuração para as configurações de notificação, na qual você especifica seus destinatários da notificação e quais notificações eles recebem.

Para configurar notificações AWS Artifact por e-mail, você deve ter as permissões necessárias para AWS Artifact Notificações de Usuários da AWS e. Para obter mais informações, consulte Gerenciamento de identidade e acesso em AWS Artifact.

Conteúdo

Pré-requisito: selecionar hubs de notificação em Notificações de Usuários

Antes de receber notificações AWS Artifact por e-mail, você deve primeiro abrir o Notificações de Usuários console e selecionar os hubs de notificação no Regiões da AWS local em que deseja armazenar seus Notificações de Usuários dados. É necessário selecionar hubs de notificação para Notificações de Usuários da AWS, que AWS Artifact usam para enviar notificações.

Para selecionar hubs de notificação

1. Abra a página Hubs de notificação do Notificações de Usuários da AWS console.
2. Selecione os hubs de notificação no Regiões da AWS local em que você deseja armazenar seus Notificações de Usuários da AWS recursos. Por padrão, seus Notificações de Usuários dados são armazenados na região Leste dos EUA (Norte da Virgínia). Notificações de Usuários replica seus dados de notificações nas outras regiões que você selecionar. Para obter mais

informações, consulte a documentação dos hubs de notificação no Guia do Notificações de Usuários da AWS usuário.

3. Escolha Save and continue.

Criando uma configuração para as configurações AWS Artifact de notificação

Depois de selecionar seus hubs de Notificações de Usuários notificação, você pode criar uma configuração para as configurações de notificação no AWS Artifact console. Na configuração que você cria, você especifica os endereços de e-mail do destinatário que deseja receber AWS Artifact notificações. Você também especifica sobre quais atualizações esses destinatários devem receber notificações, como atualizações para AWS Artifact contratos e atualizações para todos (ou um subconjunto de) AWS Artifact relatórios.

Para criar uma configuração

1. Abra a página de configurações de notificação do AWS Artifact console.
2. Escolha Criar configuração.
3. Na página Criar configuração, faça o seguinte:
   - Para receber notificações de contratos, em Acordos, mantenha a opção Atualizações sobre AWS contratos selecionada.
   - Para receber notificações de relatórios, em Relatórios, mantenha a opção Atualizações nos AWS relatórios selecionada.
     a. Para receber notificações de todos os relatórios, escolha Todos os relatórios.
     b. Para receber notificações somente para relatórios em categorias e séries específicas, escolha Um subconjunto de relatórios. Em seguida, selecione as categorias e séries nas quais você está interessado.
   - Em Nome da configuração, insira um Nome para sua configuração.
   - Em E-mail, para Destinatários, insira uma lista separada por vírgula dos endereços de e-mail dos quais você deseja receber AWS Artifact e-mails de notificação.
   - (Opcional) Para adicionar tags à configuração de notificação, expanda Tags, escolha Adicionar nova tag e insira tags como pares de valores-chave. Para obter mais informações sobre como marcar Notificações de Usuários recursos, consulte Como marcar seus

Notificações de Usuários da AWS recursos no Guia do Notificações de Usuários da AWS usuário.

- Escolha Criar configuração.

  Notificações de Usuários envia um e-mail de verificação para cada um dos endereços de e-mail do destinatário que você forneceu. Para verificar o endereço de e-mail, no e-mail de verificação, o destinatário deve escolher Verificar e-mail. Somente endereços de e-mail verificados receberão AWS Artifact notificações.

Editando uma configuração para configurações AWS Artifact de notificação

Depois de criar uma configuração para as configurações de AWS Artifact notificação, você pode editar a configuração a qualquer momento para alterar suas configurações de notificação. Por exemplo, para adicionar ou remover destinatários, altere os tipos de notificações que eles recebem e adicione ou remova tags.

Para editar uma configuração

1. Abra a página de configurações de notificação do AWS Artifact console.
2. Selecione a configuração que você deseja editar.
3. Selecione Editar.
4. Edite qualquer uma das seleções e campos de configuração. Ao terminar, escolha Salvar alterações.

   Se você adicionou novos endereços de e-mail como destinatários da notificação, Notificações de Usuários da AWS envie um e-mail de verificação para esses endereços de e-mail. Para verificar o endereço de e-mail, no e-mail de verificação, o destinatário deve escolher Verificar e-mail. Somente endereços de e-mail verificados receberão AWS Artifact notificações.

Excluindo uma configuração para configurações de AWS Artifact notificação

Se você não precisar mais de uma configuração criada para as configurações de AWS Artifact notificação, poderá excluí-la no AWS Artifact console.

Para excluir uma configuração

1. Abra a página de configurações de notificação do AWS Artifact console.
2. Selecione a configuração que você deseja excluir.
3. Escolha Excluir.
4. Na caixa de diálogo Excluir configuração, escolha Excluir.

Gerenciamento de identidade e acesso em AWS Artifact

Ao se inscrever AWS, você fornece um endereço de e-mail e uma senha associados à sua AWS conta. Essas são suas credenciais raiz e fornecem acesso completo a todos os seus AWS recursos, incluindo 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 de entrar na sua AWS conta com credenciais raiz ou compartilhar suas credenciais com outras pessoas, você deve criar uma identidade de usuário especial chamada de IAMusuário para você e para qualquer pessoa que precise acessar um documento ou contrato. 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 externamente AWS, pode usar provedores de IAM identidade em vez de criar IAM usuários. Para obter mais informações, consulte Provedores de identidade e federação no Guia IAM do usuário.

Sumário

Concedendo acesso ao 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 IAM administrador, 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 IAM política que você possa usar para conceder permissões aos seus IAM usuários e grupos.

1. Abra o IAM console em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione Políticas.
3. Escolha Criar política.
4. Escolha a JSONguia.
5. Insira um documento de política. Você pode criar sua própria política ou usar uma das políticas de Exemplos de IAM políticas para AWS Artifact.
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 Criar política.

Etapa 2: criar um IAM grupo e anexar a política

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

Para criar um IAM grupo 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 IAM usuários e adicioná-los ao grupo

Como IAM administrador, você pode adicionar usuários a um grupo a qualquer momento. Isso concede aos usuários as permissões concedidas ao grupo.

Para criar um IAM usuário e adicioná-lo a um 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. Selecione Next: Permissions (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. Selecione Next: Review (Próximo: revisar). Quando estiver pronto, escolha Criar usuário.

Migrando relatórios para permissões refinadas para AWS Artifact

Agora você pode usar permissões refinadas para. AWS Artifact Por meio dessas permissões refinadas, você tem controle granular sobre o fornecimento de acesso a recursos, como aceitar termos e baixar relatórios.

Para acessar relatórios por meio de permissões refinadas, você pode utilizar a Política AWSArtifactReportsReadOnlyAccessGerenciada ou atualizar suas permissões conforme a recomendação abaixo. Se você já havia optado por não usar permissões refinadas, você deve optar por usar o link “aceitar permissões refinadas para relatórios do Artifact AWS” disponível no console de relatórios.

Você tem a opção de acessar os relatórios com permissões antigas por meio do link “desativar as permissões refinadas para relatórios do AWS Artifact”, disponível no console, se houver um problema com a atualização das novas permissões.

Migração de relatórios para novas permissões

Migrar permissões não específicas de recursos

Substitua sua política existente contendo permissões legadas por uma política contendo 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

Substitua sua política existente contendo permissões legadas por uma política contendo 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 e chaves de condição refinadas:

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

Migração para permissões refinadas para contratos do Artifact AWS

AWSO Artifact agora permite que os clientes usem permissões refinadas para contratos. Por meio dessas permissões refinadas, os clientes têm controle granular sobre o fornecimento de acesso a recursos como visualização e aceitação de contratos de confidencialidade, bem como aceitação e rescisão de contratos.

Para acessar contratos por meio de permissões refinadas, você pode utilizar as políticas AWSArtifactAgreementsFullAccess gerenciadas AWSArtifactAgreementsReadOnlyAccessou atualizar suas permissões de acordo com a recomendação abaixo. Se você já havia optado por não usar permissões refinadas, você deve optar por usar o link “aceitar permissões refinadas para contratos do Artifact AWS”, disponível no console de contratos.

Você tem a opção de acessar os contratos com permissões antigas por meio do link “desativar as permissões refinadas para contratos de AWS Artifact”, disponível no console, se houver um problema com a atualização das novas permissões.

Migrar para novas permissões

A IAM ação legada DownloadAgreement "" foi substituída pela ação "GetAgreement" para baixar contratos não aceitos e pela ação "GetCustomerAgreement" para baixar contratos aceitos. Além disso, ações mais granulares foram introduzidas para controlar o acesso para visualização e aceitação de acordos de confidencialidade ()NDAs. Para aproveitar essas ações granulares e manter a capacidade de visualizar e executar contratos, os usuários devem substituir a política existente contendo permissões legadas por uma política contendo permissões refinadas.

Migre as permissões para baixar o contrato no nível da conta

Política antiga:

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

Nova política com permissões refinadas:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:GetAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptNdaForAgreement"
```

```
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

Migre permissões não específicas de recursos para baixar, aceitar e rescindir contratos no nível da conta

Política antiga:

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

Nova política com permissões refinadas:

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
        "Sid": "ListAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:ListAgreements",
```

```
            "artifact:ListCustomerAgreements"
        ],
        "Resource": "*"
      },
      {
        "Sid": "AWSAgreementActions",
        "Effect": "Allow",
        "Action": [
          "artifact:GetAgreement",
          "artifact:AcceptNdaForAgreement",
          "artifact:GetNdaForAgreement",
          "artifact:AcceptAgreement"
        ],
        "Resource": "arn:aws:artifact:::agreement/*"
      },
      {
        "Sid": "CustomerAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:GetCustomerAgreement",
            "artifact:TerminateAgreement"
        ],
        "Resource": "arn:aws:artifact::*:customer-agreement/*"
      }
    ]
}
```

Migre permissões não específicas de recursos para baixar, aceitar e rescindir contratos no nível da organização

Política antiga:

```
{
  "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": "*"
    }
  ]
}
```

Nova política com permissões refinadas:

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

```
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
```

```
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Migre permissões específicas de recursos para baixar, aceitar e rescindir contratos no nível da conta

Política antiga:

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

Nova política com permissões refinadas:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/agreement-9c1kBcYznTkcpRIm"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

Migre permissões específicas de recursos para baixar, aceitar e rescindir contratos em nível organizacional

Política antiga:

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/AWS Organizations Business Associate Addendum"
      ]
    },
    {
      "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": "*"
    }
  ]
}
```

Nova política com permissões refinadas:

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

```
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/agreement-y03aUwMAEorHtqjv"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Mapeamento de recursos legados a refinados para contratos

Os contratos ARN foram atualizados para obter permissões refinadas. Quaisquer referências anteriores aos recursos do contrato antigo devem ser substituídas por novasARN. Abaixo está o ARN mapeamento do contrato entre recursos legados e recursos refinados.

Nome do contrato	Artifact ARN for Legacy: permissões	Artifato ARN para permissões refinadas
AWSAdendo de associado comercial	arn:aws:artifact: ::agreeme nt/ Adendo de associado comercial AWS	arn:aws:artefact: ::acordo/ acordo-9c1 T kBcYzn kcpRIm
AWSAdendo de violação de dados notificável da Nova Zelândia	arn:aws:artifact: ::agreement/ Adendo de violação de dados notificável da Nova Zelândia AWS	arn:aws:artefact: ::acordo/ acordo-3 YRq9rGUIu72r7Gt

Nome do contrato	Artifact ARN for Legacy: permissões	Artifato ARN para permissões refinadas
AWSAdendo de violação de dados notificável na Austrália	arn:aws:artifact: ::agreeme nt/ Adendo australiano de violação de dados notificável AWS	arn:aws:artefact: ::acordo/ acordo- 8 9 sbLSDe bitmAXNr
AWSSECAdenda da Regra 17a-4	arn:aws:artefact: ::agreement/ Adendo da regra 17a-4 AWS SEC	arn: aws:artefact: ::acordo/ acordo-bexgr7sjv XAW4Gxu
AWSSECAdenda da Regra 18a-6	arn:aws:artefact: ::agreement/ Adendo da Regra 18a-6 AWS SEC	arn:aws:artefact: ::acordo/ acordo- HZTdNwJuq OKLReXC
AWSAdendo de Associado Comercial da Organizations	arn:aws:artifact: ::agreeme nt/ Adendo de associado comercial da Organizations AWS	arn:aws:artefact: ::acordo/ acordo-y03 aUw MAEorHtqjv
AWSAdendo de violação de dados notificável da Organizat ions Australian	arn:aws:artifact: ::agreement/ Adendo de violação de dados notificável da Organizations Australian AWS	arn:aws:artefact: ::Acordo/ acordo-Y pDMFXTe PE7kEg4b
AWSAdendo de violação de dados notificável da Organizat ions New Zealand	arn:aws:artifact: ::agreement/ Adendo de violação de dados notificável da Organizations New Zealand New Zealand AWS	arn:aws:artefact: ::acordo/ acordo- 3 V52 uojEjr vOnvrh

Exemplos de IAM políticas para AWS Artifact

Você pode criar políticas de permissões que concedam permissões aos IAM usuários. 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 exemplos de políticas a seguir mostram permissões que você pode atribuir aos IAM usuários com base no nível de acesso necessário.

- 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 ISO relatórios AWS SOC,PCI, e 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. 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 os detalhes de um relatório de terceiros para todas as versões.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:*"
      ]
    }
  ]
}
```

A política a seguir concede permissão para visualizar os detalhes de um relatório de terceiros para uma versão específica.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:1"
      ]
    }
  ]
}
```

> **Tip**
>
> Você deve considerar usar a AWSArtifactAgreementsReadOnlyAccesspolítica AWSArtifactAgreementsFullAccess gerenciada em vez de definir sua própria política.

Example Exemplo de políticas para gerenciar contratos

A política a seguir concede permissão para fazer download de todos os contratos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
```

```
}
```

A política a seguir concede permissão para aceitar todos os contratos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    }
  ]
}
```

A política a seguir concede permissão para rescindir todos os contratos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
```

```
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

A política a seguir concede permissões para visualizar e executar contratos em nível de conta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
```

```
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

Example Exemplos de políticas para integração com AWS Organizations

A política a seguir concede permissão para criar a IAM função 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": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

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": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
```

```
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "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": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-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": [
        "*"
```

```
      ]
    }
  ]
}
```

Usando políticas AWS gerenciadas para AWS Artifact

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomenda-se que as permissões sejam ainda mais reduzidas, definindo políticas gerenciadas pelo cliente da específicas para os casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas API operações são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte políticas gerenciadas AWS no Guia do Usuário IAM.

AWS política gerenciada: AWSArtifactReportsReadOnlyAccess

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

Essa política concede *`read-only`* permissões que permitem listar, visualizar e baixar relatórios.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `artifact`— Permite que os diretores 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": "*"
    }
  ]
}
```

AWS política gerenciada: AWSArtifactAgreementsReadOnlyAccess

É possível anexar a política `AWSArtifactAgreementsReadOnlyAccess` às suas identidades do IAM.

Esta política concede *`read-only`* acesso à lista dos contratos de serviço do AWS Artifact e ao download dos contratos aceitos. Também inclui permissões para listar e descrever os detalhes da organização. Além disso, a política fornece a capacidade de verificar se a função vinculada ao serviço necessária existe.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `artifact`— Permite que os diretores listem todos os contratos e visualizem os contratos aceitos de AWS Artifact.
- `IAM`— Permite que os diretores verifiquem se a função vinculada ao serviço existe usando GetRole.
- `organization`— Permite que os diretores descrevam a organização e listem o acesso ao serviço para a organização.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetCustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "AWSOrganizationActions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetRole",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

AWS política gerenciada: AWSArtifactAgreementsFullAccess

É possível anexar a política `AWSArtifactAgreementsFullAccess` às suas identidades do IAM.

Essa política concede *`full`* permissões para listar, baixar, aceitar e rescindir contratos do AWS Artifact. Também inclui permissões para listar e habilitar o acesso ao AWS serviço no serviço Organização, bem como descrever os detalhes da organização. Além disso, a política permite verificar se a função vinculada ao serviço necessária existe e criar uma, caso não exista.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `artifact`— Permite que os diretores listem, baixem, aceitem e rescindam os contratos de. AWS Artifact
- `IAM`— Permite que os diretores criem uma função vinculada ao serviço e verifiquem se a função vinculada ao serviço existe usando GetRole.
- `organization`— Permite que os diretores descrevam a organização e liste/habilitem o acesso ao serviço para a organização.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
```

```
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
```

```
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Artifact atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS Artifact desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o RSS feed na página Histórico do AWS Artifact documento.

Alteração	Descrição	Data
AWS Artifact começou a rastrear alterações	AWS Artifact começou a rastrear as mudanças em suas políticas AWS gerenciadas e introduziu AWSArtifactReportsReadOnlyAccess.	2023-12-15
AWSAcordos introduzidos e políticas gerenciadas	Políticas introduzidas AWSArtifactAgreementsReadOnlyAccess e AWSArtifactAgreementsFullAccess gerenciadas.	2024-11-21

Usar funções vinculadas ao serviço do AWS Artifact

AWS Artifact usa AWS Identity and Access Management (IAM) funções vinculadas ao serviço. Uma função vinculada ao serviço é um tipo exclusivo de IAM função vinculada diretamente a. AWS Artifact As funções vinculadas ao serviço são predefinidas AWS Artifact e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração AWS Artifact porque você não precisa adicionar manualmente as permissões necessárias. AWS Artifact define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS Artifact pode

assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra IAM entidade.

Você só pode excluir um perfil vinculado a serviço depois de excluir os recursos relacionados. Isso protege seus AWS Artifact recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS serviços que funcionam com IAM e procure os serviços que têm Sim na coluna Funções vinculadas ao serviço. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculadas ao serviço para AWS Artifact

AWS Artifact usa a função vinculada ao serviço chamada AWSServiceRoleForArtifact— Permite AWS Artifact coletar informações sobre uma organização por meio de. AWS Organizations

A função AWSServiceRoleForArtifact vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `artifact.amazonaws.com`

A política de permissões de função nomeada AWSArtifactServiceRolePolicy AWS Artifact permite concluir as seguintes ações no `organizations` recurso.

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

Criação de uma função vinculada ao serviço para AWS Artifact

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você acessa a guia Contratos da organização em uma conta de gerenciamento da organização e escolhe o link Começar no AWS Management Console, AWS Artifact cria a função vinculada ao serviço para você.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você acessa a guia Contratos da

organização em uma conta de gerenciamento da organização e escolhe o link Começar, AWS Artifact cria a função vinculada ao serviço para você novamente.

Editando uma função vinculada ao serviço para AWS Artifact

AWS Artifact não permite que você edite a função AWSServiceRoleForArtifact vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, você pode editar a descrição da função usandoIAM. Para obter mais informações, consulte Edição de uma função vinculada ao serviço no Guia do IAMusuário.

Excluindo uma função vinculada ao serviço para AWS Artifact

Se você não precisar mais usar um atributo 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 excluí-la manualmente.

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

Para excluir AWS Artifact recursos usados pelo AWSServiceRoleForArtifact

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

Para excluir manualmente a função vinculada ao serviço usando IAM

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

Regiões suportadas para funções vinculadas a AWS Artifact serviços

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

Nome da região	Identidade da região	Support em AWS Artifact
Leste dos EUA (Norte da Virgínia)	us-east-1	Sim
Leste dos EUA (Ohio)	us-east-2	Não
Oeste dos EUA (N. 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
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

Nome da região	Identidade da região	Support em AWS Artifact
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 (UAE)	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

Usando chaves de IAM condição para AWS Artifact relatórios

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

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

Example Exemplos de políticas para gerenciar o acesso de leitura de AWS relatórios

AWS Artifact os relatórios são indicados pelo IAM recurso,. `report`

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

```
{
  "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 AWS Artifact relatórios da SOC série.

```
{
    "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 AWS Artifact relatórios, exceto os da `Certifications and Attestations` categoria.

```
{
  "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"
        }
      }
    }
  ]
}
```

Registrando AWS Artifact API chamadas com AWS CloudTrail

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

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

AWS Artifact informações em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre em AWS Artifact, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua Conta da AWS, incluindo eventos para AWS Artifact, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para 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 eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte as informações a seguir.

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando SNS notificações da Amazon para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

AWS Artifact suporta o registro das seguintes ações como eventos em arquivos de CloudTrail log:

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings
- AcceptAgreement
- AcceptNdaForAgreement
- GetAgreement
- GetCustomerAgreement
- GetNdaForAgreement
- ListAgreements
- ListCustomerAgreements
- TerminateAgreement

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

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o CloudTrail userIdentityelemento.

Entendendo as entradas do arquivo de AWS Artifact log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log 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 da solicitação e assim por diante.

CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das API chamadas públicas, portanto, eles não aparecem em nenhuma ordem específica.

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


```
{
  "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 do documento para AWS Artifact

A tabela a seguir fornece um histórico de AWS Artifact lançamentos e alterações relacionadas ao Guia AWS Artifact do usuário.

Alteração	Descrição	Data
Permissões refinadas para execução de contratos e políticas gerenciadas AWSArtifactAgreementsFullAccess AWSArtifactAgreementsReadOnlyAccess	Permitiu acesso refinado para execução de AWS Artifact contratos e políticas lançadas AWSArtifactAgreementsFullAccesse AWSArtifactAgreementsReadOnlyAccess AWS gerenciadas.	21 de novembro de 2024
Acesso detalhado a relatórios e política gerenciada AWSArtifactReportReadOnlyAccess	Habilitou o acesso refinado aos AWS Artifact relatórios, habilitou as chaves de condição do relatório e lançou AWSArtifactReportsReadOnlyAccess a política gerenciada.	15 de dezembro de 2023
AWS Artifact função vinculada ao serviço	Foi adicionada documentação de funções vinculadas a serviços e exemplos de políticas atualizadas para integração AWS Artifact . AWS Organizations	26 de setembro de 2023
Notificações	Publicou a documentação para gerenciar notificações e fez atualizações relevantes na AWS Artifact API Referência, na documentação de CloudTrail registro e na página	1º de agosto de 2023

	de gerenciamento de identidad e e acesso.	
Relatórios de terceiros - Disponível ao público em geral	Adicionou documentação de API referência e documenta ção de CloudTrail registro e disponibilizou relatórios de terceiros para o público em geral.	27 de janeiro de 2023
Relatórios de terceiros (versão prévia)	Lançou relatórios de conformid ade dos fornecedores independentes de software (ISVs) que vendem seus produtos em AWS Marketpla ce. Foram adicionados exemplos de políticas à página de gerenciamento de identidad e e acesso para relatórios de terceiros.	30 de novembro de 2022
Segurança	Seção adicionada à página de gerenciamento de identidad e e acesso para prevenção confusa de delegados.	20 de dezembro de 2021
Relatórios	Removeu o acordo de confidencialidade e introduzi u termos e condições 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
GovCloud lançar	Lançado AWS Artifact em AWS GovCloud (US) Regions.	7 de novembro de 2019

AWS Organizations acordos	Adicionado suporte para gerenciar contratos para uma organização.	20 de junho de 2018
Contratos	Foi adicionado suporte para gerenciar AWS Artifact contratos.	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.