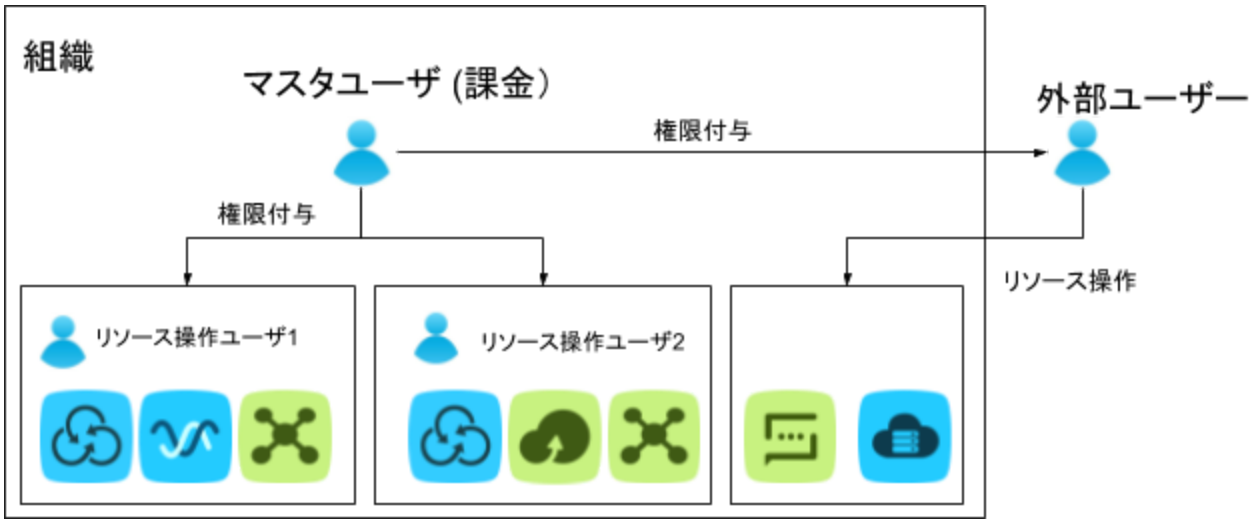
1 プロダクトの概要

Resource Access Management (RAM) は、ユーザー ID の管理およびAlibaba Cloudリソースへのアクセス制御のためのサービスです。RAM を使用することによって、高いアクセス権限を持つ管理者アカウントとリソース使用するユーザーアカウントを分けて管理することができます。RAMの権限付与ポリシーで各ユーザーアカウントの操作可能なリソースを個別に制御することができます。企業の複数のユーザーが共同でリソースを操作する必要な場合、RAMを使用すればAlibaba Cloud アカウントのアクセスキーを他のユーザーとの共有が不要となります。企業のセキュリティーの観点からでは、ユーザーの作業に必要な最低限の権限を付与することにより、セキュリティリスクが軽減されます。



説明: リソース操作する複数のユーザーを作成可能。マスタユーザーが課金を一括管理。組織の外部のユーザーへも権限付与可能です。

2 プロダクトの機能

2-1 ID管理

2-1-1 ユーザー管理

① Alibaba Cloud アカウント (プライマリアカウント)

Alibaba Cloud アカウントは、Alibaba Cloud リソースの所有権およびリソース消費の請求を確認するための基本エンティティです。Alibaba Cloud サービスを使用するために、最初はアカウントを登録する必要があります。登録済みのアカウントはリソースの所有者であり、リソースに対する完全な権限が付与されます。また、このアカウントには利用したりリソース料金が請求されます。デフォルトの設定では、すべてのリソースにアクセス可能なのはリソース所有者のみです。他のユーザーがリソースへアクセスしたい場合、所有者から明確に権限が付与されていなけ

ればなりません。権限管理の観点から見た場合、Alibaba Cloud アカウントは、オペレーティングシステムの root または管理者アカウントと似ており、"root アカウント"、"プライマリアカウント"とも呼ばれます。

② RAM ユーザー
RAM では、(企業の従業員、システム、アプリケーションに対応する) 複数の RAM ユーザーを Alibaba Cloud アカウントで作成できます。RAM ユーザーはリソースを所有せず、個別に課金されることはありません。RAMユーザーの管理と支払いは Alibaba Cloud アカウントごとに行われます。RAM ユーザーは 独立のAlibaba Cloud アカウントではなく、Alibaba Cloud アカウント配下に属しており、属したAlibaba Cloud アカウントでのみ参照できます。Alibaba Cloud アカウントから権限付与された後に、Alibaba Cloud アカウントの下で、コンソールにログオンすることや、API を使用してリソースで操作を実行することができます。

2-1-2 ユーザーグループの管理

多数のRAMユーザーをグループ単位で管理することができます。権限付与ポリシーをグループに追加すると、そのポリシーで付与される権限がこのグループに属しているすべてのRAMユーザーに割り当てられます。

2-1-3 ロール

RAM-ロールは、RAM ユーザーの種類の 1 つで、仮想ユーザー (シャドウアカウント)とも言えます。仮想ユーザーは固定 ID を持ちますが、認証キー (ログインパスワードまたはアクセスキー) はありません。そして、仮想ユーザーIDに対してポリシーを付与することが可能です。この種類のユーザーが通常の RAM-ユーザ (プライマリユーザー) と異なる点は、主に使用方法にあります。RAMロールへスイッチすると、このロールに付与されたポリシーがユーザに適用されます。実際のユーザーはロールへ切り替えると、ロール の一時セキュリティトークンを受け取ります。この一時セキュリティトークンを使用することによって、ロールに許可されているリソースにアクセスできます。

RAM-ロールを使用するには、実際のユーザー ID に関連付ける必要があります。実際のユーザーが自分に付与された RAM-ロール を使用する場合は、最初に ID を使用してログインし、SwitchRole 操作を実行して実際の ID からロール ID に切り替えます。ロール ID に切り替えると、このロール ID に許可されている操作を実行できるようになりますが、ユーザーの実際の ID のアクセス権限は使用できなくなります。ロール IDから実際の ID に戻るには、ログイン ID に戻る操作を実行する必要があります。ログイン ID に戻ると、実際の ID に対応したアクセス権限を持つようになり、ロールのアクセス権限はなくなります。

2-3 権限付与ポリシー管理

権限は、特定の条件下で特定のリソースに対する特定の操作を許可または拒否するために使用されます。権限が付与されたユーザーは、コンソールまたは API を通じてリソースを操作できます。権限付与ポリシーは、権限付与ポリシー記述言語で定義された権限のグループです。権限付

与ポリシー記述言語で、権限付与されたリソースや操作、および権限付与の条件を正確に記述できます。

RAM ユーザーに権限を付与するには、1 つ以上の権限付与ポリシーをユーザーまたはユーザーグループにバインドします。システム権限付与ポリシーとカスタマイズ権限付与ポリシーの両方をバインドできます。バインド済みの権限付与ポリシーが更新されると、更新されたポリシーは自動的に有効になります。ポリシーを再バインドする必要はありません。

2-3-1 システム権限付与ポリシー

システム権限付与ポリシーは、Alibaba Cloud によって提供される一般的な権限付与ポリシーのグループです。主に、さまざまなプロダクトに対する読み取り専用権限または完全な権限を付与します。Alibaba Cloud によって提供されるシステム権限付与ポリシーは、権限付与にのみ使用できます。編集や変更を行うことはできません。システム権限付与ポリシーの更新や変更は、Alibaba Cloud によって自動的に行われます。

RAM は、次のシステム権限付与ポリシーに対応しています。

システム権限付与ポリシーの名前	権限の説明
AdministratorAccess	すべてのAlibaba Cloud リソースを管理する権限
AliyunCDNFullAccess	CDN を管理する権限
AliyunCDNReadOnlyAccess	CDN に対する読み取り専用権限
AliyunCloudMonitorFullAccess	CloudMonitor を管理する権限
AliyunCloudMonitorReadOnlyAccess	CloudMonitor に対する読み取り専用権限
AliyunECSFullAccess	ECS を管理する権限
AliyunECSReadOnlyAccess	ECS に対する読み取り専用権限
AliyunEIPFullAccess	EIP を管理する権限
AliyunEIPReadOnlyAccess	EIP に対する読み取り専用権限
AliyunESSFullAccess	ESS を管理する権限
AliyunESSReadOnlyAccess	ESS に対する読み取り専用権限
AliyunKvstoreFullAccess	Apsara DB for Redis を管理する権限
AliyunKvstoreReadOnlyAccess	Apsara DB for Redis に対する読み取り専用

	権限
AliyunMNSFullAccess	MNS を管理する権限
AliyunMNSReadOnlyAccess	MNS に対する読み取り専用権限
AliyunOSSFullAccess	OSS を管理する権限
AliyunOSSReadOnlyAccess	OSS に対する読み取り専用権限
AliyunOTSFullAccess	OTS を管理する権限
AliyunOTSReadOnlyAccess	OTS に対する読み取り専用権限
AliyunOTSWriteOnlyAccess	OTS に対する書き込み専用権限
AliyunRAMFullAccess	RAM を管理する権限 (ユーザーと権限を管理するための権限)
AliyunRAMReadOnlyAccess	RAM に対する読み取り専用権限 (ユーザー、グループ、および権限付与の情報を表示する権限)
AliyunRDSFullAccess	RDS を管理する権限
AliyunRDSReadOnlyAccess	RDS に対する読み取り専用権限
AliyunSLBFullAccess	Server Load Balancer を管理する権限
AliyunSLBReadOnlyAccess	Server Load Balancer に対する読み取り専用権限
AliyunSTSAssumeRoleAccess	STS AssumeRole インターフェイスを呼び出す権限
AliyunVPCFullAccess	VPC を管理する権限
AliyunVPCReadOnlyAccess	VPC に対する読み取り専用権限
AliyunYundunAegisFullAccess	Server Guard を管理する権限
AliyunYundunDDosFullAccess	Anti-DDoS を管理する権限

2-3-2 カスタマイズ権限付与ポリシー

システム権限付与ポリシーが大まかで要件を満たすことができない場合は、カスタマイズ権限付与ポリシーで細かく権限を設定できます。たとえば、特定の ECS インスタンスに対する操作権限を制御する場合や、Bob というユーザーに oss://sample_bucket/bob/ のすべてのオブジェクト

に対する読み取り専用権限を付与し、IP アドレスを企業ネットワークの IP アドレスに制限する必要がある場合は、カスタマイズ権限付与ポリシーを使用して、こうした詳細な要件に対応することができます。

2-4 セキュリティトークンサービス(STS)

Alibaba Cloud の Security Token Service (STS) には、Alibaba Cloud アカウント (または RAM ユーザー) 用の短期のアクセス権限の管理が用意されています。STS を使用すると、(ローカルのアカウントシステムで管理される) フェデレーションユーザーに対して、有効期限とアクセス権限をカスタマイズしたアクセス資格情報を発行できます。フェデレーションユーザーは、STS の一時的なアクセス資格情報を使用することにより、Alibaba Cloud サービス API を直接呼び出すことや、Alibaba Cloud 管理コンソールにログオンして認証済みリソースにアクセスすることができます。

2-5 MFA (Multi-Factor Authentication)

Multi-Factor Authentication（2段階認証）は、ユーザ名とパスワード認証に加えて、ユーザが所有するデバイスを認証する、セキュリティを強化するベストプラクティスです。MFAを有効にすると、ユーザ名とパスワード（第1の要素、ユーザが知っている情報）を入力した後で、デバイスからの認証コード（第2の要素、ユーザが所有するもの）を入力することが必要となります。複数の要素で認証することによってアカウントのセキュリティを強化されます。

AlibabaクラウドのRAMはMFAの認証をサポートします。ユーザはAlibabaアカウントのMFAを有効することも、Alibabaアカウントが管理しているRAMユーザアカウントのMFAを個別に有効することが可能です。RAMは仮想MFAアプリケーションをサポートします。MFAの使用に対しては追加料金は発生しません。

Alibabaクラウドがサポートする仮想MFAアプリケーションは以下となります。

Android	Google Authenticator
iPhone	Google Authenticator

2-6 RAMとクラウドリソースのクォータ制限について

Alibaba Cloudでは、アカウントごとにクラウドリソースの購入可能な数量が制限されます（クォータ制限）。例えば、日本リージョンにおいて、Alibabaアカウントの従量課金のECSインスタンスはデフォルトで最大10インスタンス購入可能です。RAMユーザーはrootアカウントのリ

ソースクォータ制限を引き継ぐため、購入可能なリソースの上限はrootアカウントのクォータ上限と同様です。一つのrootアカウント上で複数のRAMアカウントの運用を行う場合、すべてのRAMアカウントでこの上限は共有されます。例えば、従量課金のECSインスタンスの場合、すべてのRAMユーザーで合計最大10ECSインスタンスまで購入できることになります。

　この上限は、サポートにて引き上げることが可能です。サポートチケットを起票し、当社カスタマーサポートへクラウドリソースクォータ上限引き上げの旨、ご依頼ください。

付録

RAMの様々な上限

項目	上限
最大のユーザ数	100
最大のグループ数	20
ユーザーが参加可能な最大のグループ数	5
1ユーザーあたりのアクセスキー数	2
1ユーザーあたりのMFA	1
最大のMFAデバイス	100
最大のユーザー定義可能な権限付与プロシー	50
最大の権限付与ポリシーのバージョン	5
1ユーザーへ付与可能な権限付与ポリシー数	5
1グループへ付与可能な権限付与ポリシー数	5
ユーザ名の最大の文字数	64
グループ名の最大の文字数	64
ポリシー名の最大の文字数	128
ロール名の最大の文字数	64
最大のロール数	100
Canonical名の最大の文字数	64
権限付与ポリシ—の最大の文字数	2048

SB Cloud

ご利用上の注意事項

この資料は、Alibaba Cloudの提供するクラウドサービスの機能について説明したもので、サービスのご利用を検討する際の参考となる技術的情報を提供するものです。
今後、本資料はクラウドサービスの機能追加・変更等に合わせて、予告なく変更される場合があります。閲覧された情報は最新のものではない場合がありますので、予めご了承下さい。

改版履歴

日付	版数	変更内容
2017/3/28	1.0	初版作成
2017/4/13	1.1	「2-6 RAMとクラウドリソースのクォータ制限について」を追加

SB Cloud