Alibaba Cloud
云服#器 ECS

セキュリティ

Document Version20191030

目次

1 セキュリティグループ

1.1 セキュリティグループ

セキュリティグループは **SPI (Stateful Packet Inspection)** を提供する仮想ファイアウォールであり、動的パケットフィルタリングとしても知られています。 セキュリティグループは、複数の **ECS** インスタンスへのネットワークアクセス制御の設定に使用されます。 特に、セキュリティグループは論理的にクラウド上のセキュリティドメインと分離しています。

セキュリティグループは、同じリージョン内で、同一のセキュリティ要件を持ち互いに信頼関係のあるインスタンスが組み合わされて作られています。 それぞれのインスタンスは、少なくとも **1** つのセキュリティグループに属する必要があります。これは、インスタンスの作成中に指定されます。 同じセキュリティグループにあるインスタンスはイントラネットを通じて通信できますが、異なるセキュリティグループにあるインスタンスは、デフォルトでは、他のインスタンスから分離されます。 しかし、**2** つのセキュリティグループ間の相互アクセスは許可されます。

セキュリティグループの制限

- デフォルトでは、リージョンごとに最大 **100** 個のセキュリティグループを作成できます。 この制限数は、ご利用のメンバーシップのレベルに応じて増やすことができます。 上限の引き上げには、チケットを起票し、サポートセンターへお問い合わせください。
- それぞれのインスタンスの **ENI (Elastic Network Interface)** は デフォルトで **5** つまでセキュリティグループを結合できます。 ご利用のメンバーシップのレベルに応じて、上限を **10** 個または **16** 個に引き上げるために、チケットを起票し、サポートセンターへお問い合わせください。
- セキュリティグループのネットワークタイプとして、クラシックネットワークまたは **VPC (Virtual Private Cloud)** のどちらかを選択できます。
  - クラシックネットワークインスタンスでは、同一リージョンでクラシックネットワークのセキュリティグループを結合できます。

    クラシックネットワーク内のセキュリティグループは、最大で **1,000** 個のインスタンスを含むことができます。 イントラネット間で **1,000** 個以上のインスタンスにアクセスする必

要がある場合、異なるセキュリティグループに割り当て、セキュリティグループ間で相互アクセスを許可します。

- **VPC** インスタンスでは、同一の **VPC** 上でセキュリティグループを結合できます。

  VPC 内のセキュリティグループは、最大 **2,000** のプライベート **IP** アドレスを含むことができます **(**プライマリ **ENI** およびセカンダリ **ENI** により共有**)**。 イントラネット間で **2,000** 以上のプライベート **IP** アドレスにアクセスする必要がある場合、異なるセキュリティグループに割り当て、セキュリティグループ間で相互アクセスを許可します。

・ セキュリティグループの設定の変更は、サービスの継続性に影響しません。
・ アウトバウンドパケットが許可されている場合、この通信間でのインバウンドパケットも許可されます。

詳しくは、「セキュリティグループの制限に関する *FAQ*」をご参照ください。

セキュリティグループルールの概要

セキュリティグループ内の **ECS** インスタンスでは、イントラネット間またはインターネット間の、インバウンドおよびアウトバウンドのアクセスの許可または禁止をするセキュリティグループルールを設定できます。

いつでもセキュリティグループルールを作成または削除できます。 変更した場合、更新されたセキュリティグループルールは自動的にセキュリティグループ上の **ECS** インスタンスに適用されます。

セキュリティグループルールの設定の際に、簡素なものであることの確認を推奨します。 たとえば、複数のセキュリィグループに対して **ECS** インスタンスを追加した場合、たくさんのルールがすぐにインスタンスに適用されます。これは、インスタンにアクセスした際の接続エラーの原因になります。

セキュリティグループルールの制限

ENI ごとのセキュリティグループルールの最大数 = 対象のインスタンスが結合できるセキュリィグループ数 × セキュリィグループごとのルールの最大数。

1 つのインスタンスのそれぞれの **ENI** は最大で **500** のセキュリィグループルールを持つことができます。 ここで、

・ デフォルトでは、それぞれのインスタンスを **5** つまでセキュリィグループを結合できます。

  ご利用のメンバーシップのレベルに応じて、制限を **10** または **16** に引き上げるために、チケットを起票し、サポートセンターへお問い合わせください。 ただし、セキュリィグループ数が増えると、**1** つのセキュリィグループで許可されたルールの数が減ります。

- それぞれのセキュリィグループは、100 個のセキュリィグループルールを持つことができ、これにはインバウンドルールとアウトバウンドルールの両方を含みます。

  セキュリィグループごとのルール数は、セキュリィグループのクォータに応じて 30、50、100 となります。

セキュリィグループ数に応じて、ルール数がどのように異なるかは、以下の表のようになります。

セキュリィグループ数	ルールの最大数
5 (デフォルト値)	100
10 (チケットを起票します)	50
16 (チケットを起票します)	30

例

デフォルトでは、ENI は 5 つのセキュリティグループまで結合でき、それぞれが最大で 100 個のルールを持つことができます。

ただし、ご利用のメンバーシップレベルで、それぞれの ENI が 10 個のセキュリィグループまで結合可能な場合、それぞれのセキュリィグループは最大で 50 個のルールを持つことができます。 これは、それぞれのインスタンスに関して、合計で 500 を超えるセキュリティグループルールを持つことができないためです。

さらに多くのセキュリティグループおよび、1 つのインスタンスに対するグループあたりのルール数が少なくても良い場合、上限を調整するため、チケットを起票し、サポートセンターへお問い合わせください。

1.2 アドバンストセキュリティグループの概要

ベーシックセキュリティグループに比べ、アドバンストセキュリティグループには、より多くの ECS インスタンスと ENI を含めることができます。また、無制限の数のプライベート IP アドレスを管理することもできます。 アドバンストセキュリティグループは VPC ネットワークに適用可能で、ルールを追加する仕組みが簡素化されています。 アドバンストセキュリティグループは、O&M 効率、ECS インスタンス仕様、コンピューティングノードの要件がより高いシナリオで使用可能です。

機能比較

ECS インスタンスまたは ENI をベーシックセキュリティグループとアドバンストセキュリティグループの両方に追加できないため、ネットワーク環境を計画する前に、2 つのセキュリティグ

ループタイプの機能の違いを理解しておくことを推奨します。 ベーシックセキュリティグループの詳細は、「セキュリティグループ」をご参照ください。

項目	ベーシックセキュリティグループ	アドバンストセキュリティグループ
すべてのインスタンスタイプをサポートしているか。	はい	いいえ。 **IPv6** インスタンスのみをサポートします。
VPC をサポートしているか。	はい	はい
クラシックネットワークをサポートしているか。	はい	いいえ
ルールのプライオリティを指定できるか。	はい	いいえ
他のセキュリティグループに付与されたアクセス権限か。	はい	いいえ
許可のセキュリティグループルールを手動で設定するか。	はい	はい
拒否のセキュリティグループルールを手動で設定するか。	はい	いいえ。 アドバンストセキュリティグループの場合、デフォルトですべてのアクセスリクエストは拒否されます。
サポートされる **ENI** の数	セキュリティグループ内の **ECS** インスタンスの数によって制限されます。	**50,000**
どのインスタンスタイプにも **ENI** をバインドできるか。	はい。 インスタンスネットワークタイプは **VPC** である必要があります。	いいえ。 **ENI** をバインドできるのは、**IPv6** をサポートするインスタンスタイプのみです。
プライベート **IP** アドレスの数	**2,000**	制限なし

制限

- **2019** 年 **5** 月 **30** 日より前に作成された **ECS** インスタンスをアドバンストセキュリティグループに追加することはできません。
- アドバンストセキュリティグループに追加できるのは、**IPv6** をサポートするインスタンスタイプのみです。 詳細は、「*#unique_4*」をご参照ください。

- **ECS** インスタンスと **ENI** には、セキュリティグループタイプに関して次の要件があります。
  - **ECS** インスタンスは、ベーシックセキュリティグループとアドバンストセキュリティグループの両方に追加できません。
  - **ENI** は、ベーシックセキュリティグループとアドバンストセキュリティグループの両方に追加できません。
  - **ENI** が **ECS** インスタンスにバインドされている場合、どちらも同じセキュリティグループタイプに属していなければなりません。

コンソール操作

ECS コンソールでは、次のようにアドバンストセキュリティグループを使用できます。

1. アドバンストセキュリティグループを作成します。 [セキュリティグループタイプ] を [アドバンストセキュリティグループ] に設定します。
2. アドバンストセキュリティグループに許可ルールを追加します。

   アドバンストセキュリティグループは、通信のホワイトリストに相当します。 許可ルールのみを作成でき、ルールにプライオリティ値を設定することはできません。 権限付与オブジェクトは、セキュリティグループではなく、**CIDR** ブロックでなければなりません。
3. *IPv6 をサポートする ECS インスタンスをアドバンストセキュリティグループに追加します。*

   ECS インスタンスは、ベーシックセキュリティグループとアドバンストセキュリティグループの両方に追加できません。
4. アドバンストセキュリティグループで **ENI** を使用するには、次の手順を実行します。
   a. **ENI** が既にベーシックセキュリティグループに追加されている場合、*#unique_8*により、**ENI** をアドバンストセキュリティグループに追加できます。
   b. *ENI を ECS インスタンスにバインドします。*
5. (オプション) アドバンストセキュリティグループを管理します。 たとえば、タグの追加、名前や説明の変更、アドバンストセキュリティグループの **ECS** インスタンスの管理などが可能です。

API 操作

1. *CreateSecurityGroup* を呼び出し、 `SecurityGroupType` を `enterprise` に設定します。

   セキュリティグループを作成する前に、**VPC** と **VSwitch** が作成されていることを確認してください。

2. *AuthorizeSecurityGroup* を呼び出して、アドバンストセキュリティグループへの受信トラフィックを許可するルールを追加します。 権限付与オブジェクトは、セキュリティグループではなく、**CIDR** ブロックでなければなりません。

   アドバンストセキュリティグループは、通信のホワイトリストに相当します。 **Policy** は、デフォルトで accept に設定されています.。 Priority は空白のままにできますが、IpProtocol、PortRange、SourcePortRange (オプション)、SourceCidrIp、DestCiderIp は指定する必要があります。
3. *AuthorizeSecurityGroupEgress* を呼び出して、送信ルールをアドバンストセキュリティグループに追加します。
4. *JoinSecurityGroup* を呼び出して、**VPC** タイプの **ECS** インスタンスをアドバンストセキュリティグループに追加します。
5. アドバンストセキュリティグループで **ENI** を使用するには、次の手順を実行します。
   a. **ENI** が既にベーシックセキュリティグループに追加されている場合、*ModifyNetworkInterfaceAttribute* を呼び出して、**ENI** をアドバンストセキュリティグループに追加します。
   b. *AttachNetworkInterface* を呼び出して、アドバンストセキュリティグループに追加されている **ENI** を **ECS** インスタンスにアタッチします。
6. (オプション) *DescribeSecurityGroups* を呼び出して、現在のリージョンに作成されているセキュリティグループのリストを表示します。

1.3 シナリオ

ここでは、**VPC** 接続およびクラシックネットワーク接続のいくつかのセキュリティグループのシナリオの詳細について説明します。

> 注:
> セキュリティグループの作成方法と対応するルールの詳細については、「セキュリティグループの作成」および「セキュリティグループルールの追加」をご参照ください。

- シナリオ *1:* イントラネット通信の有効化

  異なるアカウント、または異なるセキュリティグループに属するの **2** つのクラシックネットワークに接続された **ECS** インスタンス間でファイルをコピーするには、コピーする前にセキュリティグループルールを設定し、両インスタンス間でのイントラネット通信を有効にする必要があります。

- シナリオ 2: 指定された IP アドレスのみリモート接続を許可

  ECS インスタンスにハッカーがリモートからアクセスした場合、リモート接続のポートを変更し、指定された IP アドレスからのアクセスのみを許可するようにセキュリティグループルールを設定することができます。
- シナリオ 3: 特定の IP アドレスのみにインスタンスがアクセスすることを許可

  ECS インスタンスのセキュリティが侵害された場合、セキュリティグループルールを設定して特定の IP アドレスに対してのみインスタンスへのアクセスを許可することができます。
- シナリオ 4: ECS インスタンスへのリモート接続を許可

  ECS インスタンスへのリモートアクセスが必要な場合、対応するセキュリティグループルールを設定できます。
- シナリオ 5: HTTP または HTTPS サービスを介した ECS インスタンスへのアクセスを許可

  インスタンス上に Web サイトを構築する場合は、ユーザーがその Web サイトにアクセスできるようにセキュリティグループルールを設定できます。

シナリオ 1: イントラネット通信の有効化

セキュリティグループルールを使用して、次のように同じリージョンの異なるアカウント、または異なるセキュリティグループに属する ECS インスタンス間のイントラネット通信を有効にできます。

- ケース 1: 同じリージョンの同じアカウントに属するインスタンス
- ケース 2: 同じリージョンの異なるアカウントに属するインスタンス。

> 注:
> VPC 接続 ECS インスタンスの場合
>
> - インスタンスが 1 つの VPC 内にある場合は、イントラネット通信を有効にするようにそれらのセキュリティグループルールを設定できます。
> - インスタンスが異なる VPC 内にある場合、または同じリージョンの異なるアカウントに属している場合は、イントラネット通信を確立するために Express Connect を使用する必要があります。 詳細については、「異なるアカウントでの VPC 間のイントラネット接続の確立」をご参照ください。

ケース 1: 1 つのリージョンの 1 つのアカウントに属するインスタンス

同じリージョンで同じアカウントに属している 2 つのインスタンスが 1 つのセキュリティグループに属しているとき、デフォルトでイントラネット通信が有効になっています。 異なるセキュリ

ティグループに属している場合は、ネットワークタイプに応じてイントラネット通信を有効にするようにセキュリティグループルールを設定する必要があります。

・ **VPC**

インスタンスが **1** つの **VPC** にある場合は、それぞれのセキュリティグループにセキュリティグループ間の共有アクセスを許可するようにルールを追加します。 ルールは以下のとおりです。

NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	優先度	権限付与タイプ	権限付与オブジェクト
N/A	インバウンド	許可	必要なプロトコルの選択	必要なポート範囲の設定	**1**	セキュリティグループアクセス(このアカウントを許可)	インスタンスへのアクセスを許可するセキュリティグループ **ID** を選択

・ クラシックネットワーク

セキュリティグループ間で共有アクセスを許可するためのルールをそれぞれのセキュリティグループに追加します。 ルールは以下のとおりです。

NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	優先度	権限付与タイプ	権限付与オブジェクト
イントラネット	インバウンド	許可	必要なプロトコルの選択	必要なポート範囲の設定	**1**	セキュリティグループアクセス(このアカウントを許可)	インスタンスへのアクセスを許可するセキュリティグループ**ID**を選択

ケース **2:** 同じリージョンの異なるアカウントに属するインスタンス

以下の情報は、クラシックネットワーク接続 **ECS** インスタンスについてのみです。

セキュリティグループ間の共有アクセスを許可します。 例**:**

- ユーザー A は、プライベート IP アドレス A.A.A.A を持つ、インスタンス A という名前の、中国 (杭州) リージョンのクラシックネットワーク接続 ECS インスタンスを所有しています。セキュリティグループはグループAです。
- ユーザー B は、プライベート IP アドレス B.B.B.B を持つ、インスタンス B という名前の、中国 (杭州) リージョンのクラシックネットワーク接続 ECS インスタンスを所有しています。セキュリティグループはグループ B です。
- 次の表に示すように、インスタンス A からインスタンス B へのアクセスを許可するために、グループ A にルールを追加します。

NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
イントラネット	インバウンド	許可	必要なプロトコルの選択	必要なポート範囲の設定	セキュリティグループアクセス (他のアカウントを許可)	ユーザー B のアカウント ID とグループ B のセキュリティグループ ID を入力	1

- 次の表に示すように、インスタンス B からインスタンス A へのアクセスを許可するために、グループ B にルールを追加します。

NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
イントラネット	インバウンド	許可	必要なプロトコルの選択	必要なポート範囲の設定	セキュリティグループアクセス (他のアカウントを許可)	ユーザー A のアカウント ID とグループ A のセキュリティグループ ID を入力	1

 注：

インスタンスのセキュリティを保証するために、クラシックネットワーク接続セキュリティグループのイントラネットインバウンドルールを設定している場合は、[セキュリティグループアクセス] が [権限付与タイプ] の最優先になります。 [アドレスフィールドアクセス] を選択した場合は、**a.b.c.d/32**フォーマットの `/32` CIDR プレフィックスを持つ IP アドレスを入力する必要があります。 IPv4 のみがサポートされます。

シナリオ 2: **指定された** IP **アドレスのみリモート接続を許可**

指定したパブリック IP アドレスからインスタンスへのリモート接続を許可する場合は、次のルールを追加します。 この例では、指定された IP アドレスから TCP ポート 22 のインスタンスへのリモート接続が許可されています。

ネットワークタイプ	NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
VPC	**N/A**	インバウンド	許可	**SSH(22)**	**22/22**	アドレスフィールドアクセス	**1.2.3.4** など、アクセスを許可する **IP** アドレス	**1**
クラシックネットワーク	インターネット							

シナリオ 3: **特定の** IP **アドレスのみにインスタンスがアクセスすることを許可**

インスタンスから指定の**IP**アドレスにアクセスする場合は、次のルールをそのセキュリティグループに追加します。

1. 次のルールを追加して、すべてのパブリック IP アドレスへのアクセスをすべて削除します。 優先順位は、手順 2 のルールより低くなければなりません。

ネットワークタイプ	NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
VPC	**N/A**	インバウンド	不可	すべて	**-1/-1**	アドレスフィールドアクセス	**0.0.0.0/0**	**2**
クラシックネットワーク	インターネット							

2. 以下のルールを追加して、手順 1 よりも高い優先順位で、指定した IP アドレスへのアクセスを許可します。

ネットワークタイプ	NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
VPC	**N/A**	アウトバウンド	許可	必要なプロトコルの選択	必要なポート範囲の設定	アドレスフィールドアクセス	**1.2.3.4** などの指定のIPアドレスを入力	**1**
クラシックネットワーク	インターネット							

ルールを加えた後で、インスタンスに接続して特定の IP アドレスからインスタンスへ `ping` または `telnet` を試行します。 指定した IP アドレスからインスタンスにアクセスできる場合、ルールは正常に適用されています。

シナリオ 4: ECS **インスタンスへのリモート接続を許可**

次のような場合には、インスタンスに接続します。

・ ケース **1:** インターネットからインスタンスへのリモート接続を許可
・ ケース **2:** イントラネットからインスタンスへのリモート接続を許可

ケース **1:** インターネットからインスタンスへのリモート接続を許可

インターネットからインスタンスへのリモート接続を許可するには、ネットワークタイプとインスタンスのオペレーティングシステムに応じて次のルールを追加します。

- **VPC**

NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
N/A	インバウンド	許可	**Windows: RDP(3389)**	**3389/3389**	アドレスフィールドアクセス	任意のパブリック **IP** アドレスからのインターネットアクセスを許可するには、「**0.0.0.0/0**」と入力します。指定した **IP** アドレスからのインターネットアクセスを許可するには、「シナリオ 2」を参照	**1**
			Linux: SSH(22)	**22/22**			
			カスタム **TCP**	カスタマイズ			

・ クラシックネットワーク

NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
インターネット	インバウンド	許可	**Windows: RDP(3389)**	**3389/3389**	アドレスフィールドアクセス	任意のパブリック **IP** アドレスからのインターネットアクセスを許可するには、「**0.0.0.0/0**」と入力します。 指定した **IP** アドレスからのインターネットアクセスを許可するには、「シナリオ 2」を参照	**1**
			Linux: SSH(22)	**22/22**			
			カスタム **TCP**	カスタマイズ			

リモート接続用にポートをカスタマイズするには、「デフォルトのリモートアクセスポートの変更」をご参照ください。

ケース **2:** イントラネットからインスタンスへのリモート接続を許可

1 つのリージョンに属するが異なるアカウントに属するインスタンス間のイントラネット通信を有効にしていて、異なるセキュリティグループ内のインスタンスが互いに接続できるようにする場合は、必要に応じて次のルールを追加します。

・ プライベート IP アドレスがインスタンスに接続できるようにします。

- **VPC**

  イントラネット通信が *Express Connect* を使用して両方のアカウント間に構築されていることを確認し、 次のいずれかのルールを追加します。

NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
N/A	インバウンド	許可	**Windows: RDP(3389)**	**3389/3389**	アドレスフィールドアクセス	ピアインスタンスのプライベート IP アドレスを指定	**1**
			Linux: SSH (22)	**22/22**			
			カスタム TCP	カスタマイズ			

- クラシックネットワーク

  次のいずれかのルールを追加します。

NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
イントラネット	インバウンド	許可	**Windows: RDP (3389)**	**3389/3389**	アドレスフィールドアクセス	ピアインスタンスのプライベート IP アドレスを指定 インスタンスを保護するために、**a.b.c.d/32** 形式の `/32` CIDR プレフィックス を持つ IP アドレスのみが許可されます。	**1**
			Linux: SSH (22)	**22/22**			
			カスタム TCP	カスタマイズ			

- 1 つのアカウントのセキュリティグループ内のすべてのインスタンスが自分のインスタンスに接続できるようにするには、次の手順を実行します。
  - **VPC**

    イントラネット通信が *Express Connect* を使用して両方のアカウント間に構築されていることを確認し、次のいずれかのルールを追加します。

NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
N/A	インバウンド	許可	**Windows: RDP (3389)**	**3389/3389**	セキュリティグループアクセス (他のアカウントを許可)	ピアのアカウント ID とセキュリティグループ ID を入力	**1**
			Linux: SSH(22)	**22/22**			
			カスタム TCP	カスタマイズ			

  - クラシックネットワーク

    次のいずれかのルールを追加します。

NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
イントラネット	インバウンド	許可	**Windows: RDP (3389)**	**3389/3389**	セキュリティグループアクセス (他のアカウントを許可)	ピアのアカウント ID とセキュリティグループ ID を入力	**1**
			Linux: SSH(22)	**22/22**			
			カスタム TCP	カスタマイズ			

シナリオ 5: HTTP **または** HTTPS **サービスを介した** ECS **インスタンスへのアクセスを許可**

インスタンス上に **Web** サイトを構築し、ユーザーが **HTTP** または **HTTPS** でサイトにアクセスする場合、以下のいずれかのルールを追加します。

- **VPC**

  任意のパブリック IP アドレスからサイトのアクセスを許可するには、次のいずれかのルールを追加します。

NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
N/A	インバウンド	許可	HTTP(80)	80/80	アドレスフィールドアクセス	0.0.0.0/0	1
			HTTPS(443)	443/443			
			カスタム TCP	カスタマイズ、8080/8080 など			

- クラシックネットワーク

  すべてのパブリック IP アドレスが自分のサイトにアクセスできるようにするには、次のいずれかのルールを追加します。

NIC	ルールの方向	権限付与ポリシー	プロトコルタイプ	ポート範囲	権限付与タイプ	権限付与オブジェクト	優先度
インターネット	インバウンド	許可	HTTP(80)	80/80	アドレスフィールドアクセス	0.0.0.0/0	1
			HTTPS (443)	443/443			
			カスタム TCP	カスタマイズ、8080/8080 など			

注：

- `http://Public IP address` を使用してユーザーがインスタンスにアクセスできない場合、*TCP ポート 80 が正しく動作するかどうかをご確認ください*。

- **TCP** ポート **80** は、**HTTP** サービスのデフォルトポートです。 他のポートを使用したい場合は、**Web** サーバーの設定ファイル内のポートを変更します。

1.4 一般的な ECS インスタンスポートの紹介

一般的に使用される **ECS** インスタンスポートを次の表に示します。

ポート	サービス	説明
21	**FTP**	**FTP** サービスによって開かれたポートは、ファイルのアップロードとダウンロードに使用されます。
22	**SSH**	**SSH** ポートは、コマンドラインモードでのパスワードを使用した*Linux* インスタンスの接続に使用されます。
23	**Telnet**	**Telnet** ポートは、**Telnet** が **ECS** インスタンスにログインするために使用されます。
25	**SMTP**	**SMTP** サービスに対して開いているポートは、メールの送信に使用されます。 セキュリティ上の問題から、**ECS** インスタンスのポート **25** はデフォルトで制限されています。 「*TCP* ポート *25* の使用申請」を参照し、制限を解除します。
80	**HTTP**	**IIS**、**Apache**、**Nginx** などの **HTTP** サービスへのアクセスを提供します。 *TCP* ポート *80* が正しく動作するか確認することを推奨します。
110	**POP3**	**POP3** プロトコルに使用されているポートは、メールの送受信に使用されます。

143	**IMAP**	**IMAP (Internet Message Access Protocol)** プロトコルに使用されているポートは、メールの受信に使用されます。
443	**HTTPS**	このポートは、**HTTPS** サービスへのアクセスを提供するために 使用されます。**HTTPS** は、暗号化と安全なポートを介した伝送を提供するプロトコルです。
1433	**SQL Server**	**SQL Server** の **TCP** ポートは、**SQL Server** の外部サービスのために使用されます。
1434	**SQL Server**	**SQL Server** の **UDP** ポートは、**SQL Server** が使用する **TCP/IP** を返すために使用されます。
1521	**Oracle**	**Oracle** 通信ポート。 **Oracle SQL** で開放される必要があるポートは、**ECS** インスタンスにデプロイされます。
3306	**MySQL**	**MySQL** データベースが外部サービスを提供するポートです。
3389	**Windows Server Remote Desktop Services**	**Windows Server Remote Desktop Services** のポートは、*Windows* インスタンスの接続に使用されます。

8080	**Proxy port**	ポート **80** と同様に、ポート **8080** は**Web** ブラウジングを可能にするために **WWW** エージェントによって使用されます。 ポート **8080** を使用している場合、**Web** サイトにアクセス、またはプロキシサーバーを使用するには、**IP** アドレス **8080** の後に `:8080` を追加する必要があります。**Apache Tomcat** サービスをインストールする場合、デフォルトのサービスポートは **8080** です。
137、138、139	**NetBIOS protocol**	• **UDP** ポートのポート **137** および **138** は、近隣ネットワークを介したファイルの転送に使用されます。 • ポート **139** を介した接続は、**NetBIOS/smb** サービスを取得しようとします。 **NetBIOS** プロトコルは、**Windows** ファイル、プリンタ共有、および **samba** に使用されます。

アクセスができない一部のポート

問題**: ECS** インスタンスがポートのリッスンを試みたとき、他のポートは通常どおりアクセス可能であるのに対し、対象ポートはアクセスができない。

原因**:** ポート **135**、**139**、**444**、**445**、**5800**、**5900**、および関連ポートが危険度の高いポートであるとオペレーターによって判断されたため、デフォルトでブロックされます。

解決策**:** 使用ポートを別のポート番号に変更することを推奨します。

関連トピック

セキュリティグループを介してサービスポートを解放する方法の詳細については、「セキュリティグループルールの追加」をご参照ください。

1.5 セキュリティグループの作成

デフォルトセキュリティグループでは、デフォルトのルールは着信 **ICMP** トラフィックと **SSH** ポート **22**、**RDP** ポート **3389**、**HTTP** ポート **80**、および **HTTPS** ポート**443** への着信アクセスにのみ適用されます。 さらに、デフォルトのルールはセキュリティグループのネットワークタイプによって異なります。 インスタンスをデフォルトのセキュリティグループに追加したくない場合は、カスタマイズセキュリティグループを作成できます。

背景

各 **ECS** インスタンスは少なくとも **1** つのセキュリティグループに参加する必要があります。 詳細は、「セキュリティグループ」をご参照ください。

インスタンスを作成する前にセキュリティグループを作成しなかった場合は、デフォルトのセキュリティグループを使用できます。 詳細については、「デフォルトセキュリティグループルール」をご参照ください。

前提条件

VPC 用のセキュリティグループを作成する場合は、まず*VPC と vSwitch の作成*をする必要があります。

> 注：
> **VPC** を使用してセキュリティグループを作成する場合は、その **VPC** 内のさまざまな **vSwitch** とともにそのセキュリティグループを使用できます。 ただし、そのセキュリティグループを他の **VPC** で使用することはできません。

手順

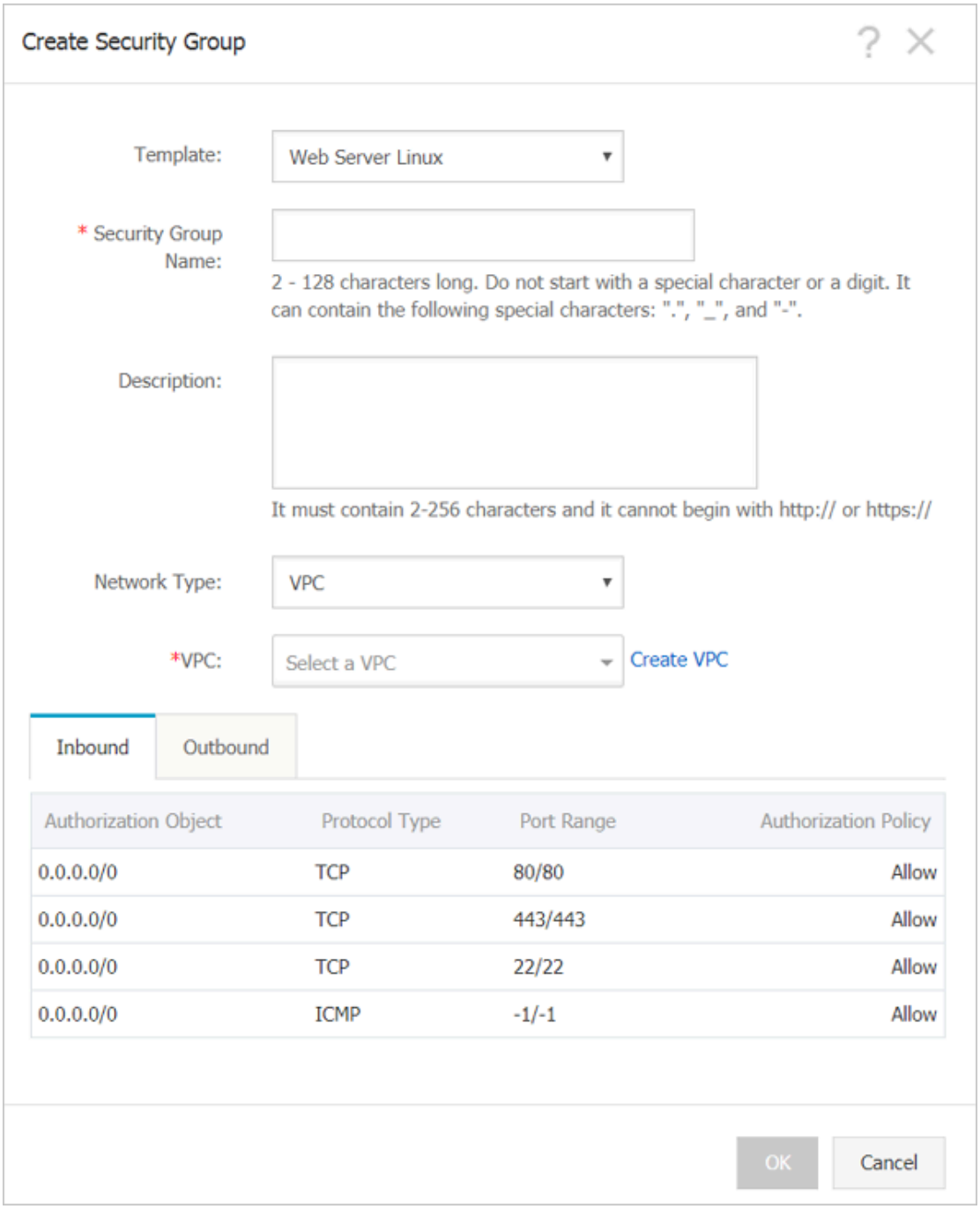
1. *ECS コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、 [ネットワークとセキュリティ] > [セキュリティグループ]を選択します。
3. リージョンを選択します。
4. [セキュリティグループの作成] をクリックします。
5. 表示された [セキュリティグループの作成] ダイアログボックスで、次の設定を行います。
   - テンプレート: セキュリティグループ内のインスタンスにデプロイされているサービスに応じてテンプレートを選択します。 テンプレートは、セキュリティグループルールの設定を

簡素化するように設計されています。 次の表は、テンプレートをさまざまなシナリオに適用する方法について説明しています。

シナリオ	テンプレート	説明
Web サービスは、セキュリティグループ内の **Linux** インスタンスにデプロイする必要があります。	**Web** サーバー **Linux**	デフォルトでは、**TCP** ポート **80/443/22** への着信アクセスと着信 **ICMP** トラフィックが許可されています。
Web サービスは、セキュリティグループ内の **Windows** インスタンスにデプロイする必要があります。	**Web** サーバー **Windows**	デフォルトでは、**TCP** ポート **80/443/3389** への着信アクセスと着信 **ICMP** トラフィックが許可されています。

特別な要件はありません	カスタム	セキュリティグループを作成したら、ビジネスニーズに応じてセキュリティグループルールを追加できます。 セキュリティグループルールを追加

- セキュリティグループ名**:** セキュリティグループの名前を入力します。
- 説明**:** セキュリティグループの説明を入力します。
- ネットワークタイプ**:**
  - **VPC** 用のセキュリティグループを作成するには、**[VPC]** を選択し、対象の **VPC** を選択します。
  - クラシックネットワーク用のセキュリティグループを作成するには、**[**クラシック**]** を選択します。



6. **[OK]** をクリックします。

ルールを追加せずに新しいセキュリティグループを作成した場合は、インターネットとイントラネットの両方にデフォルトのルールが適用されます。 具体的には、インバウンドアクセスが拒否されている間、アウトバウンドアクセスは許可されます。

API 操作

セキュリティグループを作成するために*CreateSecurityGroup*を呼び出すことができます。

次のステップ

- インターネットまたはイントラネットに基づく ECS インスタンスへのアクセスを制御するために、セキュリティグループルールを追加できます。 セキュリティグループのルールに共通に関連するポートについては、「共通の *ECS* インスタンスポートの概要」をご参照ください。 代表的なユースケースの詳細については、「セキュリティグループルールの代表的な適用例」をご参照ください。

1.6 セキュリティグループルールを追加

セキュリティグループの ECS インスタンスに対して、インターネットのアクセスまたはイントラネットのアクセスを有効あるいは無効にするセキュリティグループルールを追加できます。

- **VPC:** インバウンドトラフィックルールとアウトバウンドトラフィックルールを設定するだけで、インターネットやイントラネットに対して異なるルールを作る必要はありません。 VPC インスタンスへのインターネットアクセスは、プライベート NIC マッピングにより実現されます。 そのためインスタンス内にインターネットNICは表示されず、セキュリティグループにはイントラネットルールしか設定できません。 このルールはインターネットおよびイントラネットへのアクセスに適用されます。
- 従来のネットワーク**:** アウトバウンドとインバウンドのルールはインターネット、イントラネットそれぞれで設定しなければなりません。

ルールが設定されていない新しいセキュリティグループでは、インターネット経由であれイントラネット経由であれ、デフォルトでアウトバウンドトラフィックは許可され、インバウンドトラフィックは拒否されます。 従って、拒否するアウトバウンドトラフィックと許可するインバウンドトラフィックのルールのみ設定することを推奨します。

セキュリティグループルールの変更は、セキュリティグループのECSインスタンスに自動的に適用されます。

前提条件

セキュリティグループが作成されている必要があります。 詳細につきましては、「セキュリティグループを作成」 をご参照ください。

インスタンスに対し、どのインターネットあるいはイントラネットからの要求が、許可または拒否されるのかがわかります。

手順

1. *ECS* コンソールにログインします。

2. 左側のナビゲーションウィンドウで [ネットワークとセキュリティ] > [セキュリティグループ]の順で選択します。
3. ターゲットリージョンを選択します。
4. 承認規則を加えるセキュリティグループを見つけ、[操作] 列の [ルールを追加]をクリックします。
5. [セキュリティグループルール]で、[セキュリティグループルールを追加] をクリックします。

   注：
   あらゆるプロトコル、ICMP、GREに対してポートを有効または無効にする必要がない場合は、[クイックルール作成] を選択できます。

プロトコル	SSH	telnet	HTTP	HTTPS	MS SQL
ポート	22	23	80.	443	1433
プロトコル	Oracle	MySQL	RDP	PostgreSQL	Redis
ポート	1521	3306	3389	5432	6379

   注：
   各パラメーター構成の説明については、手順 6 をご参照ください。
6. ダイアログボックスで、以下のパラメーターを設定します。

   - NIC:
     - VPCに接続されたセキュリティグループに対しては、NIC を選択する必要はありません。

       注：

       ■ インスタンスがインターネットにアクセスできる場合、ルールはインターネットとイントラネットの両方に適用されます。

■ インスタンスがインターネットにアクセスできない場合、ルールはイントラネットでのみ適用されます。

- 従来のネットワーク接続されたセキュリティグループに対しては、インターネットかイントラネットを選択しなければなりません。

・ ルールディレクション:

- アウトバウンド: ECS インスタンスは、イントラネットかインターネットを介して別の ECS インスタンスにアクセスします。
- インバウンド: 別の ECS インスタンスは、イントラネットかインターネットを介してECSインスタンスにアクセスします。

・ 操作: 許可か禁止を選択します。

注 :
禁止ポリシーでは、データパケットが破棄され、応答も返されません。 承認ポリシー以外で 2 つのセキュリティグループルールが重複している場合、"禁止" が "許可" に優先します。

・ プロトコルタイプとポート範囲: ポート範囲の設定は選択されたプロトコルタイプに左右されます。 次の表は、プロトコルタイプとポート範囲の関係を示しています。

プロトコルタイプ	ポート範囲	シナリオ
すべて	-1/-1 として表示された場合、すべてのポートを意味します。 それを変更することはできません。	両方のアプリケーションが完全に相互信頼されているシナリオで使用されます。
すべての ICMP	-1/-1 として表示された場合、ポート制限がないことを意味します。 それを変更することはできません。	ping を用いてインスタンスネットワークの接続状況を検出するのに用いられます。
すべての GRE	-1/-1 として表示された場合、ポート制限がないことを意味します。 それを修正することはできません。	VPN サービスに使用されます。

カスタマイズ TCP カスタム UDP	カスタムポート範囲では、有効なポート値は 1～65535 で、有効なポート範囲形式は "開始ポート/終了ポート" です。 1 つのポートに対して妥当なポート範囲フォーマットを使用する必要があります。 たとえば、ポート 80 を指定するには 80/80 を使用します。	1 つまたは複数の連続ポートを許可または禁止するために使用できます。
SSH	22/22 として示されます。 ECS インスタンスに接続したら、ポート番号を変更できます。 詳細については、「デフォルトのリモートアクセスポートの変更」をご参照ください。	SSH は Linux インスタンスにリモート接続させるために使用されます。
TELNET	23/23 として表示されます。	Telnet を使用しリモートからインスタンスにログインするために使用されます。
HTTP	80/80 として表示されます。	インスタンスは、Web サイトまたは Web アプリケーションのサーバーとして使用されます。
HTTPS	443/443 として表示されます。	インスタンスは、HTTPS をサポートする Web サイトまたは Web アプリケーションのサーバーとして使用されます。
MS SQL	1433/1433 として表示されます。	インスタンスは MS SQL サーバーとして使用されます。
Oracle	1521/1521 として表示されます。	インスタンスは Oracle SQL サーバーとして使用されます。
MySQL	3306/3306 として表示されます。	そのインスタンスは MySQL サーバーとして使用されます。

RDP	**3389/3389** として表示されます。 **ECS** インスタンスに接続したら、ポート番号を変更できます。 詳細は、「デフォルトのリモートアクセスポートの変更」をご参照ください	**Windows** インスタンスにリモート接続するために使用されます。
PostgreSQL	**5432/5432** として表示されます。	インスタンスは **PostgreSQL** サーバーとして使用されます。
Redis	**6379/6379** として表示されます。	インスタンスは **Redis** サーバーとして使用されます。

注：

ポート **25** はデフォルトで制限されており、セキュリティグループルールでは開くことができません。 チケットを起票し*[TCP ポート 25 を開く]* を適用することが可能です。 サポートセンターへお問い合わせください。 詳細については、「共通 *ECS* インスタンスポートの紹介」をご参照ください。

- 承認タイプおよび承認オブジェクト：承認オブジェクトにより承認タイプの設定は影響されます。 次の表にそれらの関係を示します。

承認タイプ	承認オブジェクト
アドレスフィールドアクセス	**10.0.0.0** または **192.168.0.0/24** などの **IP** または **CIDR** ブロック形式を使用します。 **IPv4** アドレスのみがサポートされています。 **0.0.0.0/0** はすべての **IP** アドレスを示しています。

セキュリティグループアクセス	イントラネットアクセス専用 自分のアカウントまたは別のアカウントにあるセキュリティグループのインスタンスに、このセキュリティグループ内のインスタンスへのアクセスを承認します。 - このアカウントを承認する：自分のアカウントのセキュリティグループを選択します。 両方のセキュリティグループは同じVPCに属している必要があります。 - 別のアカウントを承認する：ターゲットセキュリティグループ ID とアカウント ID を入力します。 アカウント管理 > セキュリティ設定に関して、アカウントIDを取得することができます。 VPC 接続ネットワークインスタンスの場合、セキュリティグループアクセスはプライベート IP アドレスに対してのみ機能します。 インターネット IP アドレスへのアクセスを許可する場合、アドレスフィールドアクセスを使用します。

注：
従来のネットワークに接続しているセキュリティグループに対してイントラネットのインバウンドルールを構成している場合、インスタンスのセキュリティを保証するためには、セキュリティグループアクセスが承認タイプにとって最優先事項となります。[アドレスフィールドアクセス]を選択し、IP アドレスを CIDR 形式で入力する場合には、a.b.c.d/32 の形式で IP アドレスを入力します。 有効な CIDR プレフィックスは 32 のみです。

- 優先度：値の範囲は 1～100 です。 値が小さいほど、優先度が高くなります。 詳細は、*ECS セキュリティグループルールの優先順位の説明*をご参照ください。

7. [OK] をクリックします。

セキュリティグループルールは、通常すぐに有効になります。

セキュリティグループルールを確認

ウェブサービスをインスタンス上にインストールし、セキュリティグループにルールを追加すると、全ての IP アドレスがインスタンスの TCP ポート 80 にインバウンドアクセスするようになります。 セキュリティルールを確認するには、インスタンス OS に応じて次の手順を実行します。

Linux インスタンス：

セキュリティグループ内の **Linux** インスタンスの場合は、次の手順に従ってセキュリティグループルールを

1. *#unique_21*確認します。
2. 次のコマンドを実行して、**TCP 80** がリッスンされているかどうかを確認します。

   ```
   netstat -an | grep 80
   ```

   次の結果が返されると、**TCP** ポート **80** の **Web** サービスが有効になります。

   ```
   tcp        0      0 0.0.0.0:80                  0.0.0.0:*
           LISTEN
   ```

3. 「http:// インスタンスのパブリック IP アドレス」を自分のブラウザに入力します。 アクセスが成功すると、ルールは有効になります。

Windows インスタンス：

セキュリティグループ内の **Windows** インスタンスの場合は、次の手順に従ってセキュリティグループルールを

1. *#unique_22*確認します。
2. **TCP** ポート**80** がインストールされているかどうかを確認するには、**CMD** を走らせ、以下のコマンドを使用します。

   ```
   netstat -aon | findstr：80
   ```

   次の結果が返されると、**TCP** ポート **80** の **Web** サービスが有効になります。

   ```
   TCP 0.5.0.0: 80 0.5.0.0: 0 listening 1172
   ```

3. 「http:// インスタンスのパブリック IP アドレス」を自分のブラウザに入力します。 アクセスが成功したら、ルールは有効になります。

ECS セキュリティグループルールの優先順位の説明

セキュリティグループルールの優先度の値は **1**～**100** となります。 数字が小さいほど、優先度が高くなります。

ECS インスタンスは異なるセキュリティグループに属することができます。 その結果、インスタンスには、同じプロトコルタイプ、ポート範囲、承認タイプ、および承認オブジェクトを持つ複数のセキュリティグループルールが含まれることがあります。 優先度と承認ポリシーによりルールは影響を受けます。

・ 複数のルールが同じ優先度を持つ場合、禁止ルールが許可ルールを上回ります。

- 複数のルールが異なる優先度を持つ場合、承認ポリシーの設定にかかわらず高い優先度を持つルールが最初に有効になります。

関連トピック

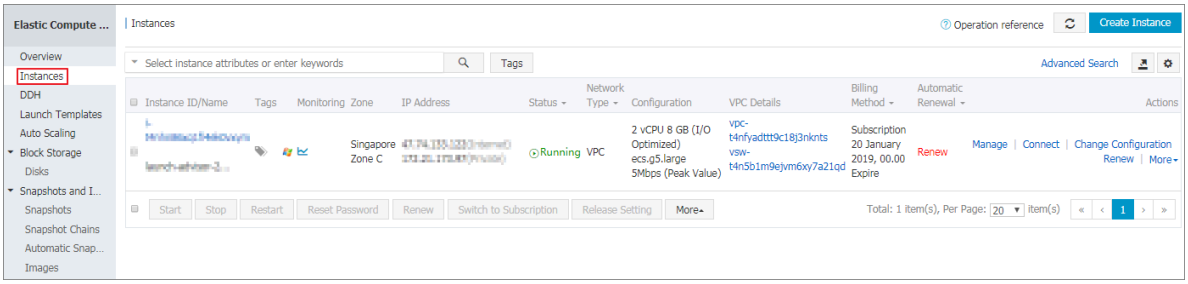
- セキュリティグループ *FAQ*
- セキュリティグループ
- *#unique_23*
- *ECS* セキュリティグループルールの優先順位の意味と一致の順序

1.7 セキュリティグループにインスタンスを追加

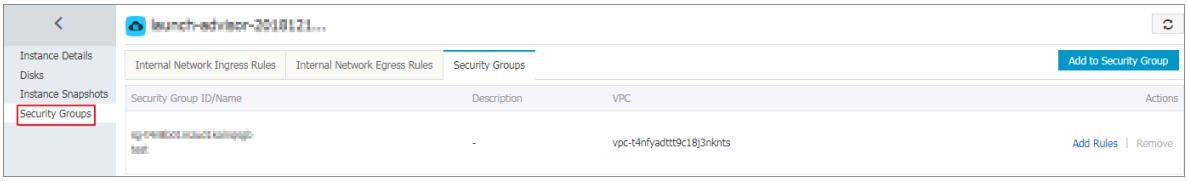
ECS コンソールでは、**1** つ以上のセキュリティグループにインスタンスを追加できます。 各**ECS** インスタンスはセキュリティグループに **5** つまで加えることができます。

手順

1. *[ECS コンソール]* にログインします。
2. 左側のナビゲーションウィンドウで、[インスタンス] をクリックします。

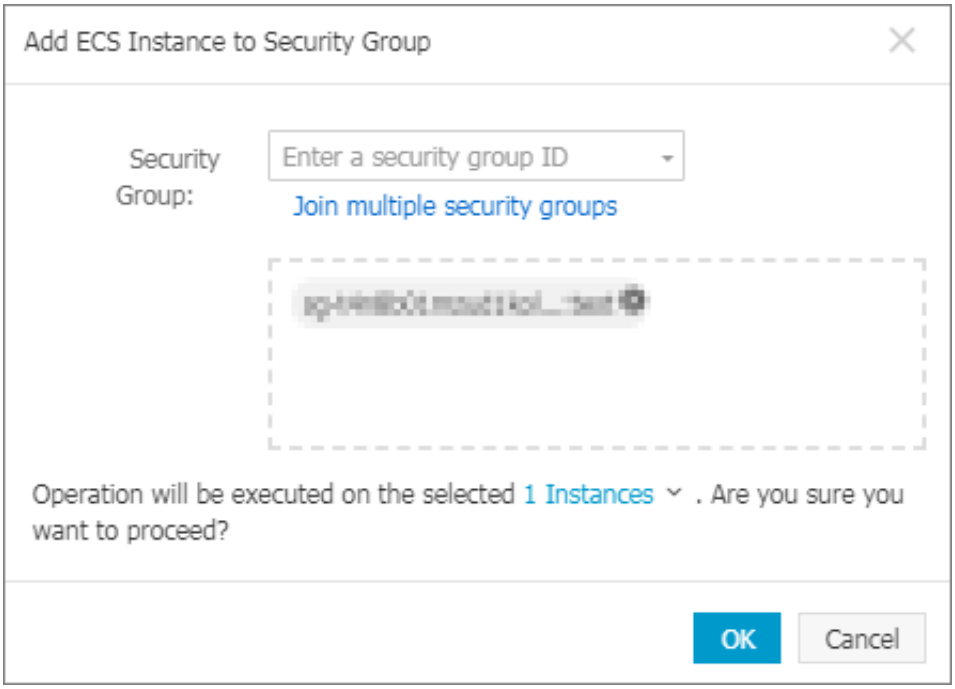


3. リージョンを選択します。
4. ターゲットインスタンスを選択します。 インスタンスの詳細ページに行くには、インスタンス名を選択するかインスタンスの右にある [管理] をクリックします。
5. 左側のナビゲーションウィンドウで [セキュリティグループ] をクリックします。

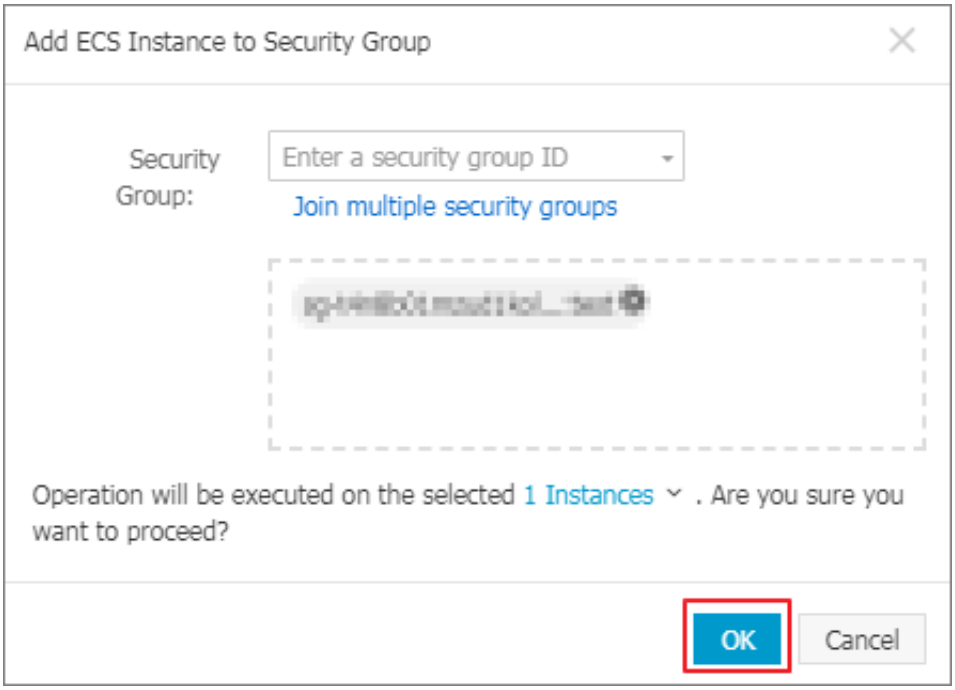


6. [セキュリティグループに追加] をクリックします。

7. 加えたいセキュリティグループを選択します。 複数のセキュリティグループに参加する時は、セキュリティグループを選択し、[複数のセキュリティグループに参加] をクリックします。 選択したセキュリティグループを示す選択ボックスが表示されます。



8. **[OK]** をクリックします。



インスタンスがセキュリティグループに追加されると、そのセキュリティグループのルールが自動的にインスタンスに適用されます。

2 キーペア

2.1 SSH キーペア

SSH キーペアの概要

SSH キーペア (以下、キーペア) は、セキュリティ保護された認証方法で、**Alibaba Cloud** により提供され、お使いの **Linux** インスタンスへのリモートログインに利用されます。 ユーザー名とパスワードを使用した認証方法に代わるものです。

キーペアは、公開鍵と秘密鍵で構成されます。 非対称の暗号化機能により、公開鍵がデータの暗号化に使われれ、ローカルクライアントは秘密鍵を使ってデータを解読します。

Linux ECS インスタンスは公開鍵を保存します。 **SSH** コマンドの入力または、他のツールから、秘密鍵を使用してインスタンスに接続します。 セキュリティを保証するため一度 **SSH** キーペアが有効化されると、**ECS** によりユーザー名とパスワードによる認証は無効化されます。

メリット

典型的なユーザー名とパスワードによる認証に比べて、**SSH** キーペアは以下のようなメリットがあります。

高いセキュリティ

SSH キーペアを使った **Linux** インスタンスへのログインは、セキュリティおよび信頼性がより高くなります。

- キーペアは、パスワードクラッキングを標的とした総当たり攻撃(ブルートフォースアタック)を防ぎます。
- たとえ公開鍵が悪意を持って取得されたとしても、複雑な **RSA** 暗号化により秘密鍵は推測されることはありません。

使いやすさ

- **ECS** コンソールおよびローカルクラインアントで、設定したキーペアによりインスタンスにリモートでログインできます。つまり、ログインの度にパスワードを入力する必要はありません。
- 複数の **ECS** インスタンスを管理する場合は、この方法を推奨します。

制限

SSH キーペアの利用には、以下のような制限があります。

- **Linux** インスタンスのみへ適用
- **Alibaba Cloud** による **2048-bit RSA** キーペアの作成のみのサポート
  - **Alibaba Cloud** がキーペアの公開鍵を保持します。
  - キーペアの作成後、秘密鍵をダウンロードし、セキュリティ保護された状態で保存する必要があります。
  - 秘密鍵は、非暗号化の **PEM** でエンコードされた `PKCS#8` 形式です。
- それぞれの **Alibaba Cloud** アカウントでリージョンごとに最大 **500** のキーペアを保有可能
- 一度に **Linux** インスタンスに対して **1** つの **SSH** キーペアのみ追加可能。 キーペアがすでにお使いのインスタンスに追加されている場合、新しいキーペアが、これまで使用していたキーペアに置き換えられます。
- **Linux** インスタンスのライフサイクルの間、いつでも **SSH** キーペアを追加、または削除が可能。 キーペアを追加または削除した後、変更が適用されるように「インスタンスの再起動」を行う必要があります。
- **Generation I** の **I/O** 最適化インスタンスを除く、任意の「インスタンスタイプファミリー」のすべてのインスタンスが、**SSH** キーペアをサポート

SSH キーペアの作成

SSH キーペアの作成には、以下のどちらかの方法を利用できます。

- **ECS** コンソールでの *SSH* キーペアの作成

> 注：
> **ECS** コンソールでキーペアを作成したら、後で使用するために秘密鍵をすぐにダウンロードし、セキュリティ保護された状態で保存します。 **ECS** インスタンスに対して **SSH** キーペア認証が有効化された場合、キーペアの秘密鍵以外で **ECS** インスタンスにログインできません。

- 他のキーペアビルダーでSSHキーペアを作成し、ECSへ「キーペアをインポート」する

  以下ようなのキータイプがサポートされます。

  - **rsa**
  - **dsa**
  - **ssh-rsa**
  - **ssh-dss**
  - **ecdsa**
  - **ssh-rsa-cert-v00@openssh.com**
  - **ssh-dss-cert-v00@openssh.com**
  - **ssh-rsa-cert-v01@openssh.com**
  - **ssh-dss-cert-v01@openssh.com**
  - **ecdsa-sha2-nistp256-cert-v01@openssh.com**
  - **ecdsa-sha2-nistp384-cert-v01@openssh.com**
  - **ecdsa-sha2-nistp521-cert-v01@openssh.com**

関連する操作

- **SSH** キーペアがない場合、「*SSH* キーペアの作成」が行えます。
- 他のツールにより **SSH** キーペアが作成済みの場合、「*SSH* キーペアのインポート」が行えます。
- キーペアが必要ない場合、「*SSH* キーペアの削除」が行えます。
- **Linux ECS** インスタンスへのログインの **SSH** キーペアによる認証を有効化、または無効化する場合、「*SSH* キーペアの追加または削除」を行えます。
- 「*ECS* インスタンスの作成」の際に、**SSH** キーペアを割り当てることができます。
- 「*SSH* キーペアによるインスタンスにログイン」ができます。

3 アクセス制御 RAM

複数のクラウドサーバー **ECS** インスタンスを購入した場合、インスタンスを使用する必要がある組織内には複数のユーザーが存在します。 ユーザーがクラウドアカウントキーを共有すると、次の問題が発生します。

- キーは複数の人々によって共有されることにより、漏洩の危険性が高まります。
- ユーザーのアクセス権を制限することはできず、誤操作の可能性があるためにセキュリティ上のリスクが高まります。

アクセス制御 **RAM** (リソースアクセス管理) は、**Alibaba Cloud** によって提供されるリソースアクセス制御サービスです。 **RAM** により、 従業員、システム、アプリケーションなどのユーザーを一元的に管理し、ユーザーは自分の名前で、どのリソースにアクセスできるかを制御する権限を管理できます。

アクセス制御 **RAM** を使用すると、リソースに対するユーザーアクセス制御を管理できます。 たとえば、ネットワークセキュリティ制御を強化するために、グループに権限付与ポリシーを追加できます。 元の**IP**アドレスが企業ネットワークのものでない場合、ご自身の名前でリクエストされた**ECS** リソースへのアクセスは拒否されます。

以下のように、グループごとに異なる権限を設定できます。

- **Sysadmins** (システム管理者)**:** このグループには、**ECS** イメージ、インスタンス、スナップショット、セキュリティグループなどを作成および管理する権限が必要です。 グループメンバーにすべての **ECS** の実行を許可する権限付与ポリシーをこのグループに 割り当てました。
- **Developers** (開発者)**:** このグループは、インスタンスを使用する権限のみが必要です。 このグループでは、メンバー全員に **DescriptionInstances**、**StartInstance**、**StopInstance**、**CreateInstance**、および**DeleteInsance** を呼び出す 権限を付与するポリシーを 割り当てます。
- 開発者の職責が変わってシステム管理者になった場合は、開発者グループからシステム管理者グループに簡単に移行させることができます。

アクセス制御 **RAM** の詳細については、**RAM** のプロダクト資料をご参照ください。

4 インスタンス RAM ロール

4.1 インスタンス RAM ロールの概要

インスタンス **RAM (Resource Access Management)** ロールを使用すると、**ECS** インスタンスに対するロールベースのアクセス許可の権限を付与できます。

一時的な **STS (Security Token Service)** 認証情報を使用して、**ECS** インスタンスにロールを割り当て、そのインスタンスでホストされているアプリケーションが他のクラウドサービスにアクセスできるようにします。 これは **AccessKey** のセキュリティ保証に役立ち、インスタンスのきめ細かいアクセス制御の適用が可能です。

背景

一般に、**ECS** インスタンス内のアプリケーションは、**Alibaba Cloud** プラットフォーム上のさまざまなクラウドサービスにアクセスするために、**AccessKeyId** および **AccessKeySecret** を含む、プライマリアカウントまたは *RAM* ユーザーアカウントの **AccessKey** を使用する必要があります。

つまり、呼び出しを行うには、設定ファイルなどのインスタンスに直接 **AccessKey** を適用する必要があります。 ただし、**Alibaba Cloud** が呼び出し目的で **AccessKey** をインスタンスに書き込むと、**AccessKey** が誤って公開される可能性があります。アカウントとリソースのセキュリティを保証するために、**Alibaba Cloud** はインスタンス **RAM** ロールのサポートを提供します。

利点

インスタンス **RAM** ロールにより、次のことが可能になります。

- ロールを **ECS** インスタンスに関連付けます。
- **ECS** インスタンス内のアプリケーションからの **STS** 認証情報を使用して、他のクラウドサービス **(OSS**、**SLB**、および **ApsaraDB for RDS** など) に安全にアクセスします。
- 異なる **ECS** インスタンスに異なるポリシーを持つロールを割り当て、それらのインスタンスが他のクラウドサービスへの制限されたアクセスレベルを持つことで、きめ細かいアクセス制御が得られます。
- **RAM** ロールのポリシーのみを変更して **ECS** インスタンスのアクセス許可を維持します。つまり、**AccessKey** を変更する必要はありません。

価格

インスタンス **RAM** ロールの使用は無料です。

制限

インスタンス **RAM** ロールには、次の制限があります。

- インスタンス **RAM** ロールは **VPC** インスタンスにのみ適用されます。
- **ECS** インスタンスは、**1** つのインスタンス **RAM** ロールに対してのみ権限付与されます。

インスタンス RAM **ロールの使用方法**

インスタンス **RAM** ロールは、次のいずれかの方法で使用できます。

- *コンソールでのインスタンス RAM ロールの使用*
- *API 呼び出しによるインスタンス RAM ロールの使用*

参照

- **STS** をサポートするクラウドサービスの一覧については、「*RAM をサポートするクラウドサービス*」をご参照ください。
- 他のクラウドサービスにアクセスする方法については、「*インスタンス RAM ロールによる他のクラウドプロダクト API へのアクセス*」をご参照ください。

4.2 コンソールでのインスタンス RAM ロールの使用

制限

インスタンス **RAM** ロールには、次の制限があります。

- インスタンス **RAM** ロールは、**VPC** 接続インスタンスにのみ適用可能です。
- **ECS** インスタンスは、一度に **1** つのインスタンス **RAM** ロールに対してのみ権限付与されます。
- インスタンス **RAM** ロールを **ECS** インスタンスにバインドした後、**ECS** インスタンス内のアプリケーションから他のクラウドサービス **(OSS**、**SLB**、または **ApsaraDB for RDS** など) にアクセスする場合は、*#unique_44* を使ってインスタンス **RAM** ロールの権限付与の認証情報を取得する必要があります。 詳細は、「権限付与の認証情報を取得」をご参照ください。
- **RAM** ユーザーアカウントでインスタンス **RAM** ロールを使用している場合は、プライマリユーザーアカウントを使用して、*RAM ユーザーにインスタンス RAM ロールを使用する権限を付与する*必要があります。

前提条件

RAM サービスを有効化しておく必要があります。 有効化の方法を参照して、**RAM** サービスを有効化します。

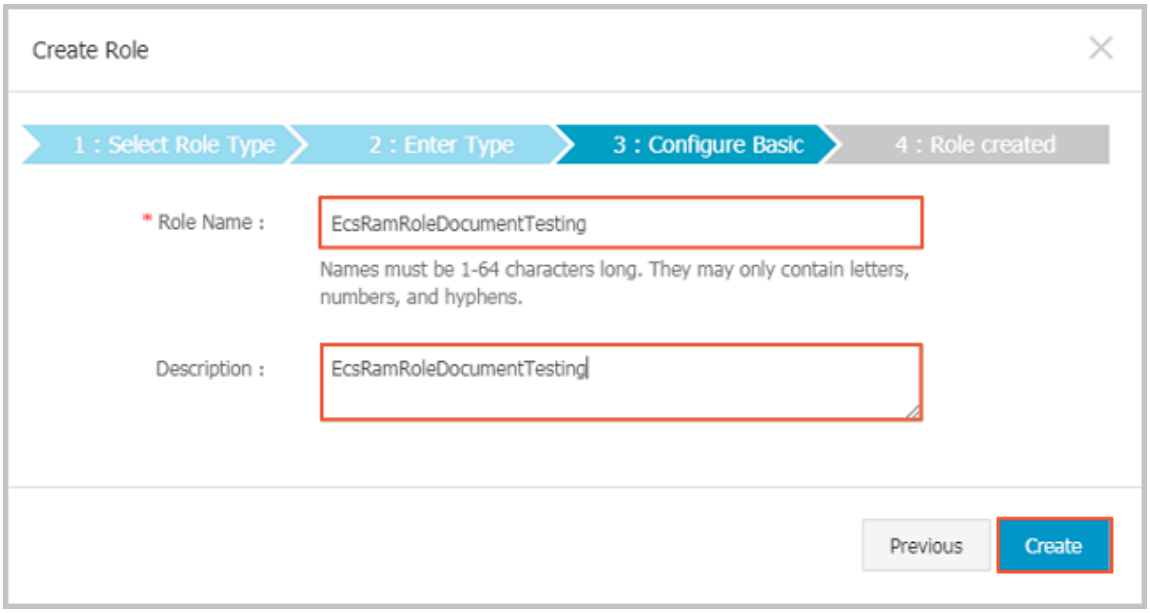
1. **インスタンス** RAM **ロールの作成**

   1. *RAM コンソール*にログインします。
   2. 左側のナビゲーションウィンドウで、[ロール] をクリックします。
   3. [ロールの作成] をクリックします。
   4. ダイアログボックスで、

      a. [ロールタイプ] で [サービスロール] を選択します。

      b. [タイプ] で [**Elastic Compute Service (ECS)**] を選択します。

      c. たとえば、「**EcsRamRoleDocumentTesting**」のように、ロール名と説明を入力します。



      d. [作成] をクリックします。

2. **インスタンス** RAM **ロールの権限付与**

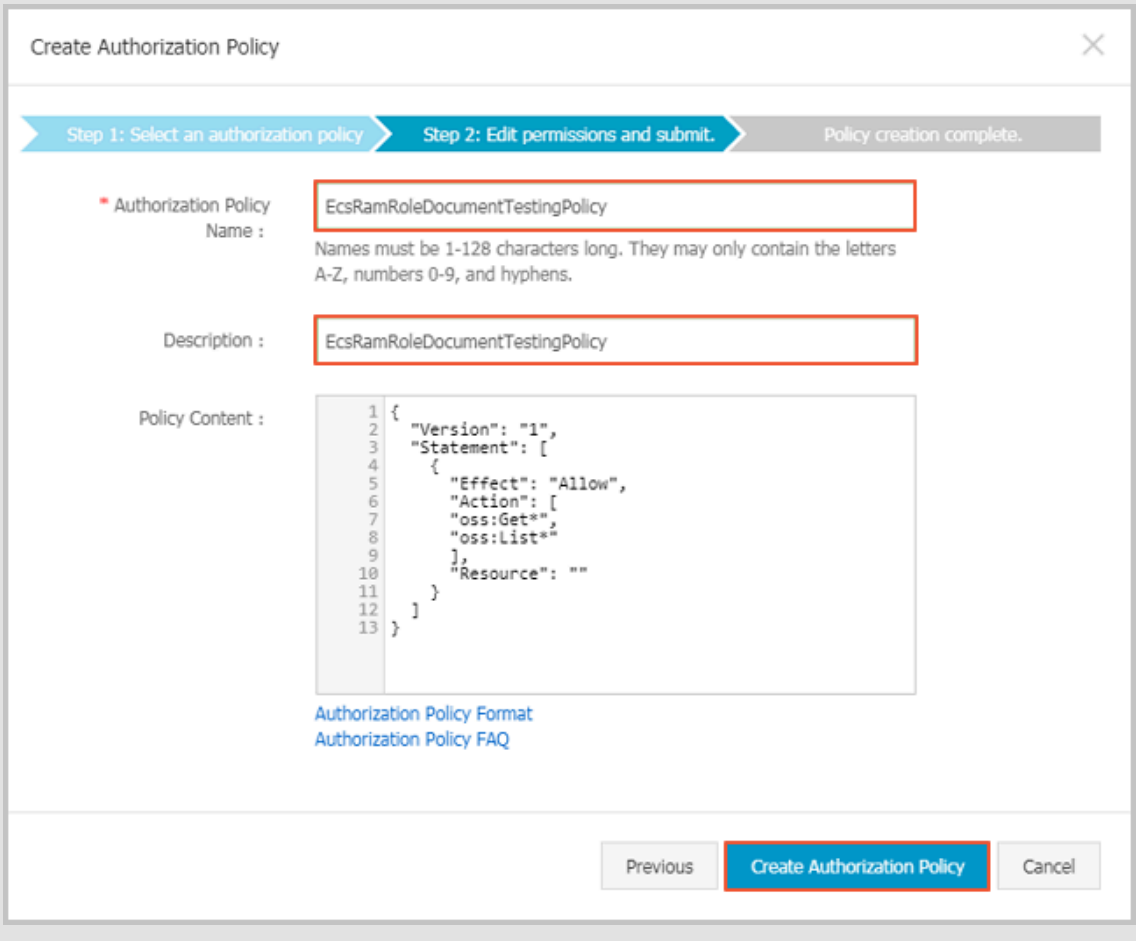
   1. *RAM コンソール*にログインします。
   2. 左側のナビゲーションウィンドウで、[ポリシー] をクリックします。
   3. [権限付与ポリシーの作成] をクリックします。

4. ダイアログボックスで、

   a. [権限付与ポリシーテンプレート] で [空白のテンプレート] を選択します。

   b. 権限付与ポリシー名とポリシーコンテンツを入力します。 この例では、" **EcsRamRoleDocumentTestingPolicy** " です。

   > 注：
   > 権限付与ポリシーを JSON 形式で記述する方法については、「ポリシー構文構造」をご参照ください。



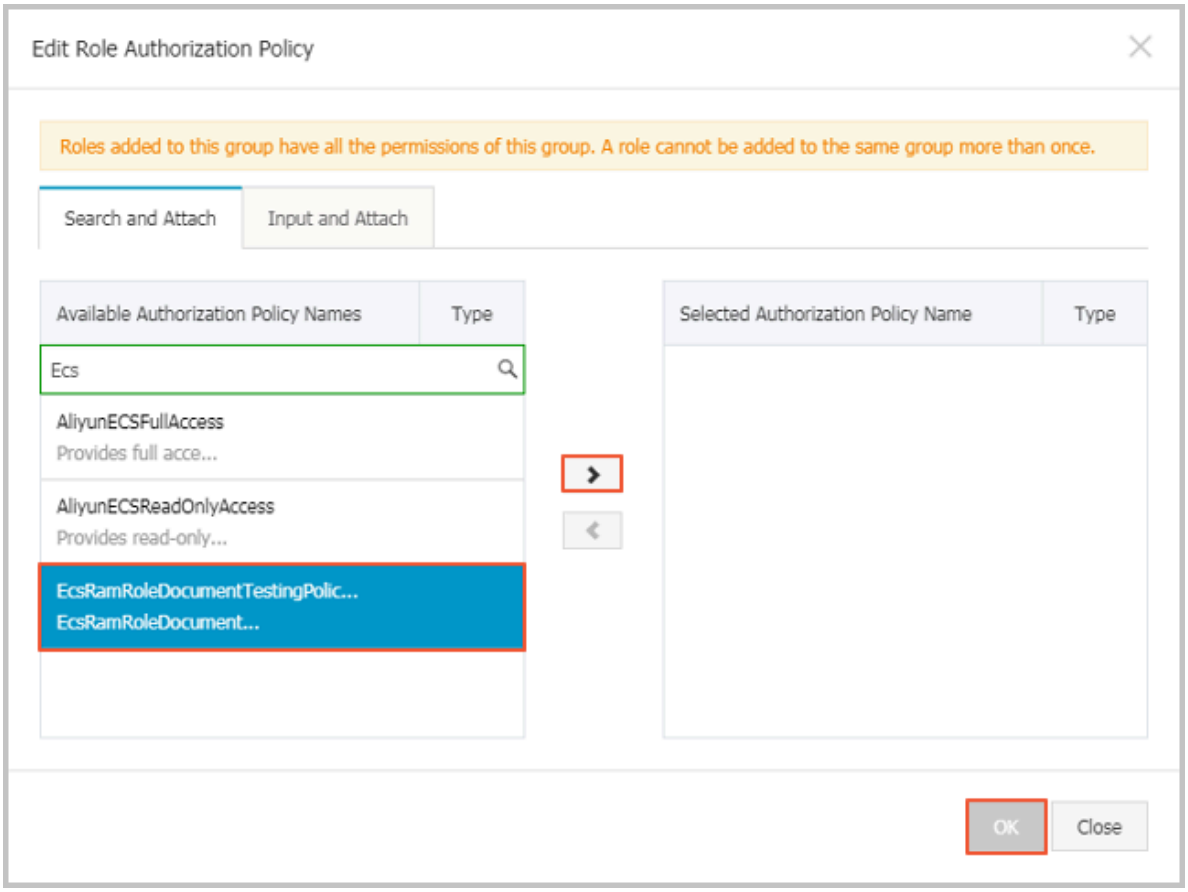
   c. [権限付与ポリシーの作成] をクリックします。

5. 左側のナビゲーションウィンドウで、[ロール] をクリックします。

6. たとえば、**EcsRamRoleDocumentTesting** のロールを選択し、[権限付与] をクリックします。

7. [権限付与ポリシー名] を入力して、ドロップダウンメニューから選択します。 この例では、**EcsRamRoleDocumentTestingPolicy** が選択されています。

8. [>] アイコンからポリシー名を選択し、[OK] をクリックします。



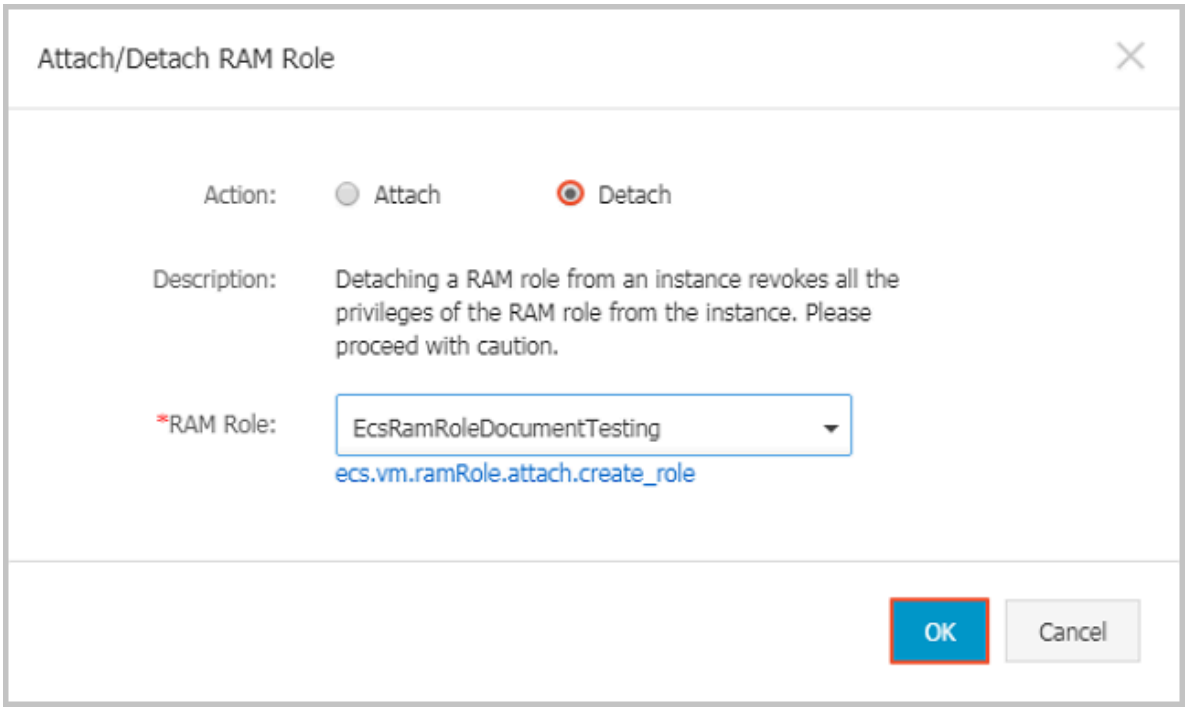
3. インスタンス RAM ロールのバインド

1. *ECS コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[インスタンス] をクリックします。
3. 対象のリージョンを選択します。
4. 対象の ECS インスタンスを検索し、[詳細] > [インスタンス設定] > [RAM ロールのバインド/バインド解除] の順に選択します。
5. "操作" から [バインド] を選択し、ロール (たとえば、EcsRamRoleDocumentTesting) を選択して [OK] をクリックします。

4. (オプション) インスタンス RAM ロールのバインド解除

1. *ECS コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[インスタンス] をクリックします。
3. 対象のリージョンを選択します。
4. 対象の ECS インスタンスを検索、[詳細] > [インスタンス設定] > [RAM ロールのバインド/バインド解除] の順に選択します。

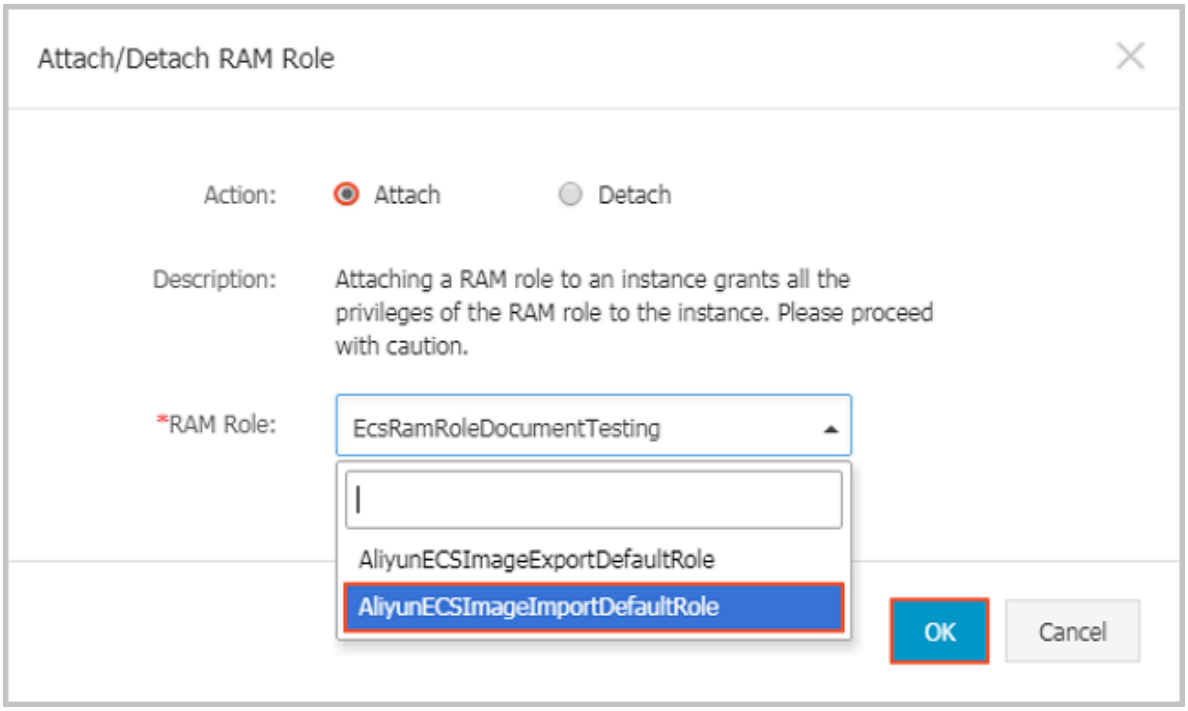
5. "操作" から [バインド解除] を選択し、[OK] をクリックします。



5. (オプション) インスタンス RAM のロールの置き換え

1. *ECS コンソール*にログインします。
2. 左側のナビゲーションウィンドウで、[インスタンス] をクリックします。
3. 対象のリージョンを選択します。
4. 対象の ECS インスタンスを検索し、[詳細] > [インスタンス設定] > R[AM ロールのバインド/バインド解除] の順に選択します。

5. "操作" から [バインド] を選択し、[RAM ロール] のリストで別のインスタンス RAM ロールを選択してから [OK] をクリックします。



6. (オプション) 権限付与の認証情報の取得

ECS インスタンスの内部アプリケーションにアクセスするには、(インスタンスのメタデータの一部である) インスタンス RAM ロールの STS 認証情報を取得して、ロールが権限付与されているアクセス許可とリソースにアクセスします。 認証情報は定期的に更新されます。 STS によってインスタンスにアクセスするには、次の手順を実行します。

1. ターゲット ECS インスタンスに接続します。
2. インスタンス RAM ロールの STS 資格情報を取得します。 この例では、EcsRamRoleDocumentTesting です。
   - Linux インスタンスの場合: `curl http://100.100.100.200/latest/meta-data/Ram/security-credentials/EcsRamRoleDocumentTesting` を実行します。
   - Windows インスタンスの場合: 「#unique_44」をご参照ください。
3. 認証情報を取得します。 戻り値の例は次のとおりです。

```
{
"AccessKeyId" : "XXXXXXXXX",
"AccessKeySecret" : "XXXXXXXXX",
"Expiration" : "2017-11-01T05:20:01Z",
"SecurityToken" : "XXXXXXXXX",
"LastUpdated" : "2017-10-31T23:20:01Z",
"Code" : "Success"
```

```
}
```

7. (**オプション**) RAM **ユーザーへのインスタンス** RAM **ロールの使用権限付与**

> 注：
> インスタンス **RAM** ロール機能を使用するための **PassRole** 許可を **RAM** ユーザーに与える必要があります。 **PassRole** 許可がなければ、**RAM** ユーザーは、付加されている権限付与ポリシーの権限を実行できません。

RAM コンソールにログインし、*RAM* ユーザーへの権限付与によって対象の **RAM** ユーザーに権限を付与をします。 以下は権限付与ポリシーの例です。

```
{
        "Version": "2016-10-17",
        "Statement": [
            {
            "Effect": "Allow",
            "Action": [
                "ecs: [ECS RAM Action]",
                "ecs: CreateInstance",
                "ecs: AttachInstanceRamRole",
                "ecs: DetachInstanceRAMRole"
            ],
            "Resource": "*"
            },
            {
        "Effect": "Allow",
        "Action": "ram:PassRole",
        "Resource": "*"
            }
        ]
}
```

ECS RAM Action パラメーターは、**RAM** ユーザーの特定の操作が許可されていることを示します。 詳細は、「権限付与ルール」をご参照ください。

参照

- 次のリンクをクリックして、*API* を呼び出してインスタンス *RAM* ロールを使用する方法を確認します。
- 次のリンクをクリックして、インスタンス *RAM* ロールを使用して、他のクラウドプロダクトにアクセスする方法を参照します。

4.3 API 呼び出しによるインスタンス RAM ロールの使用

制限

インスタンス **RAM** ロールには、次の制限があります。

- インスタンス **RAM** ロールは、**VPC** に接続されたインスタンスにのみ適用可能です。

- **ECS** インスタンスは、一度に **1** つの**RAM** ロールに対してのみ権限付与されます。
- インスタンス **RAM** ロールが **ECS** インスタンスにアタッチされた後、**ECS** インスタンス内のアプリケーションから他のクラウドサービス **(OSS**、**SLB**、または **ApsaraDB for RDS** など**)** にアクセスする場合は、*#unique_44*を使用してインスタンス **RAM** ロールの権限付与認証情報を取得する必要があります。 詳細は、「オンデマンド権限付与の認証情報の取得」をご参照ください。
- **RAM** ユーザーアカウントでインスタンス **RAM** ロールを使用している場合は、プライマリユーザーアカウントを使用して、*RAM ユーザーにインスタンス RAM ロールの使用権限を付与する*必要があります。

前提条件

RAM ユーザーアカウントを使用している場合は、インスタンス **RAM** ロールの権限を付与する必要があります。 「有効化の方法」を参照し、**RAM** サービスを有効化します。

1. **インスタンス** RAM **ロールの作成**

1. **CreateRole** *#unique_52* を呼び出し、インスタンス **RAM** ロールを作成します。
2. **RoleName** パラメーターを設定します。たとえば、**EcsRamRoleDocumentTesting** です。
3. `AssumeRolePolicyDocument` を以下のように設定します。

```
"Statement": [

"Action": "sts:AssumeRole",
"Effect": "Allow",
"Principal": {
"Service": [
"ecs.aliyuncs.com"

}


"Version": "1"
```

2. **インスタンス** RAM **ロールの権限付与**

1. **CreatePolicy** を呼び出して *#unique_53* 権限付与ポリシーを作成します。
2. **RoleName** パラメーターを設定します。たとえば、**"EcsRamRoleDocumentTestingPolicy"** に設定します。
3. 次のように `PolicyDocument` を設定します。

```
"Statement": [

"Action": [
"oss:Get*",
"oss:List*"
```

```
"Effect": "Allow",
"Resource": "*"


"Version": "1"
```

4. *AttachPolicyToRole* を呼び出し、ロールポリシーを承認します。
5. PolicyType をカスタムに設定します。
6. PolicyName パラメーターを設定します。たとえば、**"EcsRamRoleDocumentTestingPolicy"** です。
7. RoleName パラメーターを設定します。たとえば、**"EcsRamRoleDocumentTesting"** です。

インスタンス RAM **ロールのアタッチ**

1. *AttachInstanceRamRole* を呼び出し、インスタンス **RAM** ロールを **ECS** インスタンスにアタッチします。
2. RegionId パラメーターと InstanceIds パラメーターを設定して **ECS** インスタンスを 指定します。
3. RamRoleName パラメーターを設定します。たとえば、**"EcsRamRoleDocumentTesting"** です。

4. (**オプション**) **インスタンス** RAM **ロールのデタッチ**

1. *DetachInstanceRamRole* を呼び出し、インスタンス **RAM** ロールをデタッチします。
2. RegionId パラメーターと InstanceIds パラメーターを設定して **ECS** インスタンスを指定します。
3. RamRoleName パラメーターを設定します。たとえば、**"EcsRamRoleDocumentTesting"** です。

5. (**オプション**) **オンデマンド権限付与認証情報の取得**

ECS インスタンスの内部アプリケーションの場合は、インスタンスのメタデータであるインスタンス **RAM** ロールの **STS** 認証情報を取得して、ロールが権限付与されているアクセス許可とリソースにアクセスします。 認証情報は定期的に更新されます。 例

1. たとえば、**EcsRamRoleDocumentTesting** など、インスタンス **RAM** ロールの **STS** 認証情報を取得します。
   - **Linux** インスタンス: `curl http://100.100.100.200/latest/meta-data/Ram/security-credentials/EcsRamRoleDocumentTesting` を実行します。
   - **Windows** インスタンス: *#unique_44*を参照します。

2. 認証情報トークンを取得します。 リターン例

```
"AccessKeyId" : "XXXXXXXXX",
"AccessKeySecret" : "XXXXXXXXX",
"Expiration" : "2017-11-01T05:20:01Z",
"SecurityToken" : "XXXXXXXXX",
"LastUpdated" : "2017-10-31T23:20:01Z",
"Code" : "Success"
```

6. (**オプション**) **インスタンス** RAM **ロールを使用するための** RAM **ユーザーへの権限付与**

注：

インスタンス **RAM** ロール機能を使用するには **RAM**ユーザーに PassRole 許可を付与する必要があります。

RAM コンソールにログインし、手順に従って *RAM* ユーザーに権限付与します。 次に、**RAM** ユーザーに権限付与して権限付与を完了し、権限付与ポリシー例として以下のコードスニペットを参照します。

```
"Version": "2016-10-17",
"Statement": [

"Effect": "Allow",
"Action": [
"ecs: [ECS RAM Action]",
"ecs: CreateInstance",
"ecs: AttachInstanceRamRole",
"ecs: DetachInstanceRAMRole"

"Resource": "*"


"Effect": "Allow",
"Action": "ram:PassRole",
"Resource": "*"
```

[ECS RAM Action] パラメーターは、**RAM** ユーザーが特定のアクションの権限を付与されていることを示します。 「権限付与ルール」をご参照ください。

参照

- 次のリンクをクリックして、コンソールでインスタンス *RAM* ロールを使用する方法を参照します。
- 他のクラウドサービスにアクセスする方法については、「インスタンス *RAM* ロールによる他のクラウドプロダクト *API* へのアクセス」をご参照ください。

・ インスタンス **RAM** ロールに関連する **API** は以下が含まれます。

- *CreateRole*: インスタンス **RAM** ロールの作成
- *ListRoles*: インスタンス **RAM** ロールのリストの照会
- *CreatePolicy*: インスタンス **RAM** ロールポリシーの作成
- *AttachPolicyToRole*: インスタンス **RAM** ロールポリシーの権限付与
- *AttachInstanceRamRole*: インスタンス**RAM**ロールのアタッチ
- *DetachInstanceRamRole*: インスタンス**RAM**ロールのデタッチ
- *DescribeInstanceRamRole*: インスタンス **RAM** ロールの照会

5 Anti-DDoS Basic

「*Anti-DDoS Basic*」は無料の **DDoS (Distributed Denial of Service)** 保護サービスで、お使いの **ECS** インスタンス上のデータおよびアプリケーションを保護します。 **Alibaba Cloud Security** からのグローバルサービスとして、**Anti-DDoS Basic** により、一般的な **DDoS** 攻撃に対して **5 Gbit/s** の軽減容量が提供されます。 **ECS** インスタンスのインバウンドトラフィックが、**ECS** インスタンスタイプにより決められた制限を超えた場合、**Alibaba Cloud Security** が安定したパフォーマンスを維持するために帯域幅調整を有効化します。

Anti-DDoS Basic の作動方法

Anti-DDoS Basic が有効化されると、**Alibaba Cloud Security** がリアルタイムでインバウンドトラフィックを監視します。 **DDoS** 攻撃により引き起こされる大規模なトラフィックまたは通常とは異なるトラフックが観測された場合、**Alibaba Cloud Security** によりトラフィックが転送され、悪意のあるトラフィックを切断し、正常なトラフィックを **ECS** インスタンスに送ります。 この処理を "フロークリーニング" と呼びます。 詳しくは、「*Anti-DDoS Basic の仕様*」をご参照ください。

> 注 :
> **ECS** インスタンスに対し、**Anti-DDoS Basic** が有効化されると、インターネットからのインバウンドトラフィックが **5 Gbit/s** を超えた場合、グローバルクラスターのセキュリティ保護のため、**Alibaba Cloud Security** がそのようなトラフィックを受信するためにブラックホールを動作させます。 詳しくは、「*Alibaba Cloud ブラックホールポリシー*」をご参照ください。

フロークリーニングは、以下のような状況で動作します。

- インバウンドトラフィックで指定された攻撃が識別されたとき
- **ECS** インスタンスへのインバウンドトラフィックが指定されたしきい値を超えたとき

フロークリーニングの方法には、**ICMP** パケットのフィルタリング、ビットレートの制限および、パケットの転送レートの制限が含まれます。

そのため、**Anti-DDoS Basic** を使用の際は、以下のしきい値を設定する必要があります。

- **BPS** しきい値: インバウンドトラフィックが **BPS** しきい値を超えた場合、フロークリーニングが動作します。
- **PPS** しきい値: インバウンドパケット転送レートが **PPS** しきい値を超えた場合、フロークリーニングが動作します。

インスタンスタイプごとのクリーニングしきい値

それぞれのインスタンスタイプの設定により、フロークリーニングしきい値の最大値が決められています。 いくつかの「利用可能」および「順次停止」インスタンスタイプのフロークリーニングは、以下の表のようになります。

インスタンスタイプ	最大 BPS しきい値 (Mbit/s)	最大 PPS しきい値 (PPS)
ecs.g5.16xlarge	20,000	4,000,000
ecs.g5.22xlarge	30,000	4,500,000
ecs.g5.2xlarge	2,500	800,000
ecs.g5.4xlarge	5,000	1,000,000
ecs.g5.6xlarge	7,500	1,500,000
ecs.g5.8xlarge	10,000	2,000,000
ecs.g5.large	1,000	300,000
ecs.g5.xlarge	1,500	500,000
ecs.sn2ne. 14xlarge	10,000	4,500,000
ecs.sn2ne. 2xlarge	2,000	1,000,000
ecs.sn2ne. 4xlarge	3,000	1,600,000
ecs.sn2ne. 8xlarge	6,000	2,500,000
ecs.sn2ne.large	1,000	300,000
ecs.sn2ne.xlarge	1,500	500,000
ecs.c5.16xlarge	20,000	4,000,000
ecs.c5.2xlarge	2,500	800,000
ecs.c5.4xlarge	5,000	1,000,000
ecs.c5.6xlarge	7,500	1,500,000
ecs.c5.8xlarge	10,000	2,000,000
ecs.c5.large	1,000	300,000
ecs.c5.xlarge	1,500	500,000
ecs.sn1ne. 2xlarge	2,000	1,000,000
ecs.sn1ne. 4xlarge	3,000	1,600,000
ecs.sn1ne. 8xlarge	6,000	2,500,000
ecs.sn1ne.large	1,000	300,000
ecs.sn1ne.xlarge	1,500	500,000

インスタンスタイプ	最大 BPS しきい値 (Mbit/s)	最大 PPS しきい値 (PPS)
ecs.r5.16xlarge	20,000	4,000,000
ecs.r5.22xlarge	30,000	4,500,000
ecs.r5.2xlarge	2,500	800,000
ecs.r5.4xlarge	5,000	1,000,000
ecs.r5.6xlarge	7,500	1,500,000
ecs.r5.8xlarge	10,000	2,000,000
ecs.r5.large	1,000	300,000
ecs.r5.xlarge	1,500	500,000
ecs.re4.20xlarge	15,000	2,000,000
ecs.re4.40xlarge	30,000	4,000,000
ecs.se1ne. 14xlarge	10,000	4,500,000
ecs.se1ne. 2xlarge	2,000	1,000,000
ecs.se1ne. 4xlarge	3,000	1,600,000
ecs.se1ne. 8xlarge	6,000	2,500,000
ecs.se1ne.large	1,000	300,000
ecs.se1ne.xlarge	1,500	500,000
ecs.se1.14xlarge	10,000	1,200,000
ecs.se1.2xlarge	1,500	400,000
ecs.se1.4xlarge	3,000	500,000
ecs.se1.8xlarge	6,000	800,000
ecs.se1.large	500	100,000
ecs.d1ne. 2xlarge	6,000	1,000,000
ecs.d1ne. 4xlarge	12,000	1,600,000
ecs.d1ne. 6xlarge	16,000	2,000,000
ecs.d1ne. 8xlarge	20,000	2,500,000
ecs.d1ne. 14 x large	35,000	4,500,000
ecs.d1.2xlarge	3,000	300,000
ecs.d1.4xlarge	6,000	600,000
ecs.d1.6xlarge	8,000	800,000
ecs.d1.8xlarge	10,000	1,000,000

インスタンスタイプ	最大 BPS しきい値 (Mbit/s)	最大 PPS しきい値 (PPS)
ecs.d1-c8d3.8xlarge	10,000	1,000,000
ecs.d1.14xlarge	17,000	1,800,000
ecs.d1-c14d3.14xlarge	17,000	1,400,000
ecs.i2.xlarge	1,000	500,000
ecs.i2.2xlarge	2,000	1,000,000
ecs.i2.4xlarge	3,000	1,500,000
ecs.i2.8xlarge	6,000	2,000,000
ecs.i2.16xlarge	10,000	4,000,000
ecs.i1.xlarge	800	200,000
ecs.i1.2xlarge	1,500	400,000
ecs.i1.4xlarge	3,000	500,000
ecs.i1-c10d1.8xlarge	6,000	800,000
ecs.i1-c5d1.4xlarge	3,000	400,000
ecs.i1.14xlarge	10,000	1,200,000
ecs.hfc5.large	1,000	300,000
ecs.hfc5.xlarge	1,500	500,000
ecs.hfc5.2xlarge	2,000	1,000,000
ecs.hfc5.4xlarge	3,000	1,600,000
ecs.hfc5.6xlarge	4,500	2,000,000
ecs.hfc5.8xlarge	6,000	2,500,000
ecs.hfg5.large	1,000	300,000
ecs.hfg5.xlarge	1,500	500,000
ecs.hfg5.2xlarge	2,000	1,000,000
ecs.hfg5.4xlarge	3,000	1,600,000
ecs.hfg5.6xlarge	4,500	2,000,000
ecs.hfg5.8xlarge	6,000	2,500,000
ecs.hfg5.14xlarge	10,000	4,000,000
ecs.c4.2xlarge	3,000	400,000
ecs.c4.4xlarge	6,000	800,000
ecs.c4.xlarge	1,500	200,000

インスタンスタイプ	最大 BPS しきい値 (Mbit/s)	最大 PPS しきい値 (PPS)
ecs.ce4.xlarge	1,500	200,000
ecs.cm4.4xlarge	6,000	800,000
ecs.cm4.6xlarge	10,000	1,200,000
ecs.cm4.xlarge	1,500	200,000
ecs.gn5-c28g1.14xlarge	10,000	4,500,000
ecs.gn5-c4g1.xlarge	3,000	300,000
ecs.gn5-c4g1.2xlarge	5,000	1,000,000
ecs.gn5-c8g1.2xlarge	3,000	400,000
ecs.gn5-c8g1.4xlarge	5,000	1,000,000
ecs.gn5-c28g1.7xlarge	5,000	2,250,000
ecs.gn5-c8g1.8xlarge	10,000	2,000,000
ecs.gn5-c8g1.14xlarge	25,000	4,000,000
ecs.gn5i-c2g1.large	1,000	100,000
ecs.gn5i-c4g1.xlarge	1,500	200,000
ecs.gn5i-c8g1.2xlarge	2,000	400,000
ecs.gn5i-c16g1.4xlarge	3,000	800,000
ecs.gn5i-c28g1.14xlarge	10,000	2,000,000
ecs.gn4-c4g1.xlarge	3,000	300,000
ecs.gn4-c8g1.2xlarge	3,000	400,000
ecs.gn4-c4g1.2xlarge	5,000	500,000
ecs.gn4-c8g1.4xlarge	5,000	500,000
ecs.gn4.8xlarge	6,000	800,000
ecs.gn4.14xlarge	10,000	1,200,000
ecs.ga1.xlarge	1,000	200,000
ecs.ga1.2xlarge	1,500	300,000
ecs.ga1.4xlarge	3,000	500,000
ecs.ga1.8xlarge	6,000	800,000
ecs.ga1.14xlarge	10,000	1,200,000
ecs.f1-c28f1.7xlarge	5,000	2,000,000
ecs.f1-c8f1.2xlarge	2,000	800,000

インスタンスタイプ	最大 BPS しきい値 (Mbit/s)	最大 PPS しきい値 (PPS)
ecs.f2-c28f1.14xlarge	10,000	2,000,000
ecs.f2-c28f1.7xlarge	5,000	1,000,000
ecs.f2-c8f1.2xlarge	2,000	400,000
ecs.f2-c8f1.4xlarge	5,000	1,000,000
ecs.t5-c1m1.2xlarge	1,200	400,000
ecs.t5-c1m1.large	500	100,000
ecs.t5-c1m1.xlarge	800	200,000
ecs.t5-c1m2.2xlarge	1,200	400,000
ecs.t5-c1m2.large	500	100,000
ecs.t5-c1m2.xlarge	800	200,000
ecs.t5-c1m4.2xlarge	1,200	400,000
ecs.t5-c1m4.large	500	100,000
ecs.t5-c1m4.xlarge	800	200,000
ecs.t5-lc1m1.small	200	60,000
ecs.t5-lc1m2.large	400	100,000
ecs.t5-lc1m2.small	200	60,000
ecs.t5-lc1m4.large	400	100,000
ecs.t5-lc2m1.nano	100	40,000
ecs.ebmg4.8xlarge	10,000	4,500,000
ecs.ebmg5.24xlarge	10,000	4,500,000
ecs.sccg5.24xlarge	10,000	4,500,000
ecs.xn4.small	500	50,000
ecs.mn4.small	500	50,000
ecs.mn4.large	500	100,000
ecs.mn4.xlarge	800	150,000
ecs.mn4.2xlarge	1,200	300,000
ecs.mn4.4xlarge	2,500	400,000
ecs.n4.small	500	50,000
ecs.n4.large	500	100,000
ecs.n4.xlarge	800	150,000

インスタンスタイプ	最大 BPS しきい値 (Mbit/s)	最大 PPS しきい値 (PPS)
ecs.n4.2xlarge	1,200	300,000
ecs.n4.4xlarge	2,500	400,000
ecs.n4.8xlarge	5,000	500,000
ecs.e4.small	500	50,000
ecs.sn1.medium	500	100,000
ecs.sn1.large	800	200,000
ecs.sn1.xlarge	1,500	400,000
ecs.sn1.3xlarge	3,000	500,000
ecs.sn1.7xlarge	6,000	800,000
ecs.sn2.medium	500	100,000
ecs.sn2.large	800	200,000
ecs.sn2.xlarge	1,500	400,000
ecs.sn2.3xlarge	3,000	500,000
ecs.sn2.7xlarge	6,000	800,000
ecs.sn2.13xlarge	10,000	120,000

関連する操作

デフォルトでは、**ECS** インスタンスが作成されると、作成した **ECS** インスタンスに対して **Anti-DDoS Basic** が有効化されます。 以下が可能となります。

- フロークリーニング用のしきい値の設定。 **ECS** インスタンスの作成後、デフォルトで、インスタンスタイプによる最大しきい値が **Anti-DDoS Basic** に使用されます。 ただし、いくつかのインスタンスタイプで **BPS** しきい値はセキュリティに対して必要以上の設定になっています。 そのため、ニーズに応じてしきい値を設定する必要があります。 詳しくは、**Anti-DDoS Basic** ドキュメントの「*DDoS の基本保護設定*」をご参照ください。
- フロークリーニングのキャンセルは推奨しません。 **ECS** インスタンスへのインバウンドトラフィックがクリーニングしきい値を超えた場合、通常の業務トラフィックを含むトラフィックがクリーニングされます。 業務の割り込みを避けるため、フロークリーニングをキャンセルできます。 詳しくは、「フロークリーニングのキャンセル方法」をご参照ください『』。

 警告：

フロークリーニングをキャンセルした、または **ECS** インスタンスへのインバウンドトラフィックが **5 Gbit/s** を超えた場合、すべてのトラフィックがブラックホールへ転送されます。

6 セキュリティFAQ

セキュリティグループとは何ですか？

セキュリティグループとは、**1** つ以上の **ECS** インスタンスに対してネットワークアクセスを実装する仮想ファイアウォールです。 セキュリティの分離の重要な手段として、セキュリティグループはクラウド上のセキュリティドメインを論理的に分離させます。

各 **ECS** インスタンスは、少なくとも **1** つのセキュリティグループに属している必要があります。 **ECS** インスタンスを作成する際、セキュリティグループを指定する必要があります。 同じセキュリティグループにあるインスタンスは相互に通信できますが、異なるセキュリティグループにあるインスタンスは、デフォルトでは他のインスタンスから分離されています。 セキュリティグ

ループルールを設定して、2 つのセキュリティグループ間の相互アクセスを許可することができます。 詳細は、「セキュリティグループ概要」をご参照ください。

ECS インスタンスを作成するときにセキュリティグループを選択する必要があるのはなぜですか？

ECS インスタンスを作成するときは、セキュリティグループを選択して、アプリケーション環境内でセキュリティドメインを分割し、適切なネットワークセキュリティの分離をするためにセキュリティグループルールを設定する必要があります。

セキュリティグループを作成していないリージョンの ECS コンソールで ECS インスタンスを作成すると、該当のインスタンスは自動的にデフォルトのセキュリティグループに割り当てられます。 デフォルトのセキュリティグループからインスタンスを削除し、新しいセキュリティグループに追加することを推奨します。

セキュリティグループを作成する前に ECS インスタンスを作成する場合はどうすればよいですか？

ECS インスタンスを作成する前にセキュリティグループを作成しなかった場合は、デフォルトのセキュリティグループが使用可能です。 デフォルトのセキュリティグループは、一般的なポート (TCP ポート 22、ポート 3389 等) へのアクセスを許可します。 詳細については、「セキュリティグループの概要」の「デフォルトのセキュリティグループ」セクションをご参照ください。

セキュリティグループにインスタンスを追加すると、ルールの数が制限を超えているというプロンプトが表示されるのはなぜですか？

ECS インスタンス (プライマリ ENI) に関連付けることができるセキュリティグループルールの最大数 = インスタンスを追加できるセキュリティグループの最大数 × 各セキュリティグループのルールの最大数

[ルールの数が制限を超えています] というプロンプトが表示された場合、インスタンスに関連付けられているセキュリティグループルールの数が上限を超えています。 別のセキュリティグループを選択することを推奨します。

VPC の各セキュリティグループに含めることができる ECS インスタンスの最大数を調整した場合、それ以降に作成したセキュリティグループに対してのみ有効になりますか？

いいえ。調整前と調整後に VPC に作成したすべてのセキュリティグループに対して有効になります。

VPC で ECS インスタンスのパブリックセキュリティグループルールを設定できないのはなぜですか？

VPC のインスタンスは、内部 NIC マッピングを介した場合にのみパブリックネットワークにアクセスすることができます。このため、インスタンスではパブリック NIC が非表示になります。したがって、インスタンスが属するセキュリティグループの内部ルールのみ設定をすることがで

きます。 設定するセキュリティグループルールは、内部ネットワークとパブリックネットワークの両方に適用されます。

TCP ポート 25 にアクセスできないのはなぜですか？

TCP ポート 25 は、デフォルトのメールサービスポートです。 セキュリティ上の理由から、ECS インスタンスのポート 25 はデフォルトで無効になっています。 メール送信には、ポート 465 を使用することを推奨します。 その他の適用シナリオについては、「シナリオ」をご参照ください。

ポート 80 にアクセスできないのはなぜですか？

「*TCP ポート 80 が正常に機能しているか確認する*」をご参照ください。

セキュリティグループにいくつかの内部セキュリティグループルールが自動的に追加されたのはなぜですか？

次のいずれかの理由によって、セキュリティグループにルールが自動的に追加される場合があります。

- DMS (データ管理サービス) にアクセスしました。
- Alibaba Cloud DTS (データ送信サービス) を使用してデータを移行しました。 DTS IP アドレスに関連付けられているルールは、セキュリティグループに自動的に追加されます。

セキュリティグループに優先度 110 のルールがあるのはなぜですか？

優先度 110 のルールがあるセキュリティグループルールはシステムによって作成されたデフォルトルールです。 デフォルトルールの優先度は、手動で追加されたセキュリティグループルールの優先度よりも必ず低くなります。 セキュリティグループルールを手動で追加する場合、優先度を 1 ～ 100 の範囲内で値を設定できます。

セキュリティグループルールが正しく設定されていない場合はどうしたらよいですか？

セキュリティグループルールが正しく設定されていない場合、このルールに関連付けられた ECS インスタンスは、内部ネットワークを介して他のデバイスと通信することはできません。 例：

- SSH を使用して Linux ECS インスタンスにリモートでアクセスしたり、RDP (リモートデスクトッププロトコル) を使用して Windows ECS インスタンスにアクセスすることはできません。
- ECS インスタンスのパブリック IP アドレスは `ping` することはできません。
- ECS インスタンスによって提供される Web サービスには、HTTP または HTTPS を介してアクセスすることはできません。

・ このルールに関連付けられた ECS インスタンスは、内部ネットワークを介して他の ECS インスタンスと通信することはできません。

セキュリティグループのインバウンドルールとアウトバウンドルールは別々にカウントされますか？

いいえ。セキュリティグループのインバウンドルールとアウトバウンドルールは合わせてカウントされます。 各セキュリティグループに合計 100 件以上のインバウンドルールとアウトバウンドルールを設けることはできません。 詳細については、*#unique_73*をご参照ください。

セキュリティグループに追加できるルールの最大数を調整できますか？

いいえ。各セキュリティグループには最大 100件までのセキュリティグループルールを含めることができます。 ECS インスタンスの各 ENI は、デフォルトで最大 5 つのセキュリティグループに追加することができます。 したがって、ECS インスタンスの各 ENI は、最大 500 件のセキュリティグループルールに関連付けることができ、大抵のシナリオにおけるニーズを満たします。

各セキュリティグループのルールの最大数に到達後、さらにセキュリティグループルールを追加する必要がある場合は、次の手順に沿って操作します。

1. 冗長なルールが存在するか確認してください。 または、チケットを起票して Alibaba Cloud のテクニカルサポートにお問い合わせください。
2. 冗長ルールが存在する場合は、削除をしてから新しいセキュリティグループルールを追加します。 冗長ルールが存在しない場合は、新たなセキュリティグループを作成し、新しいセキュリティグループルールを追加します。