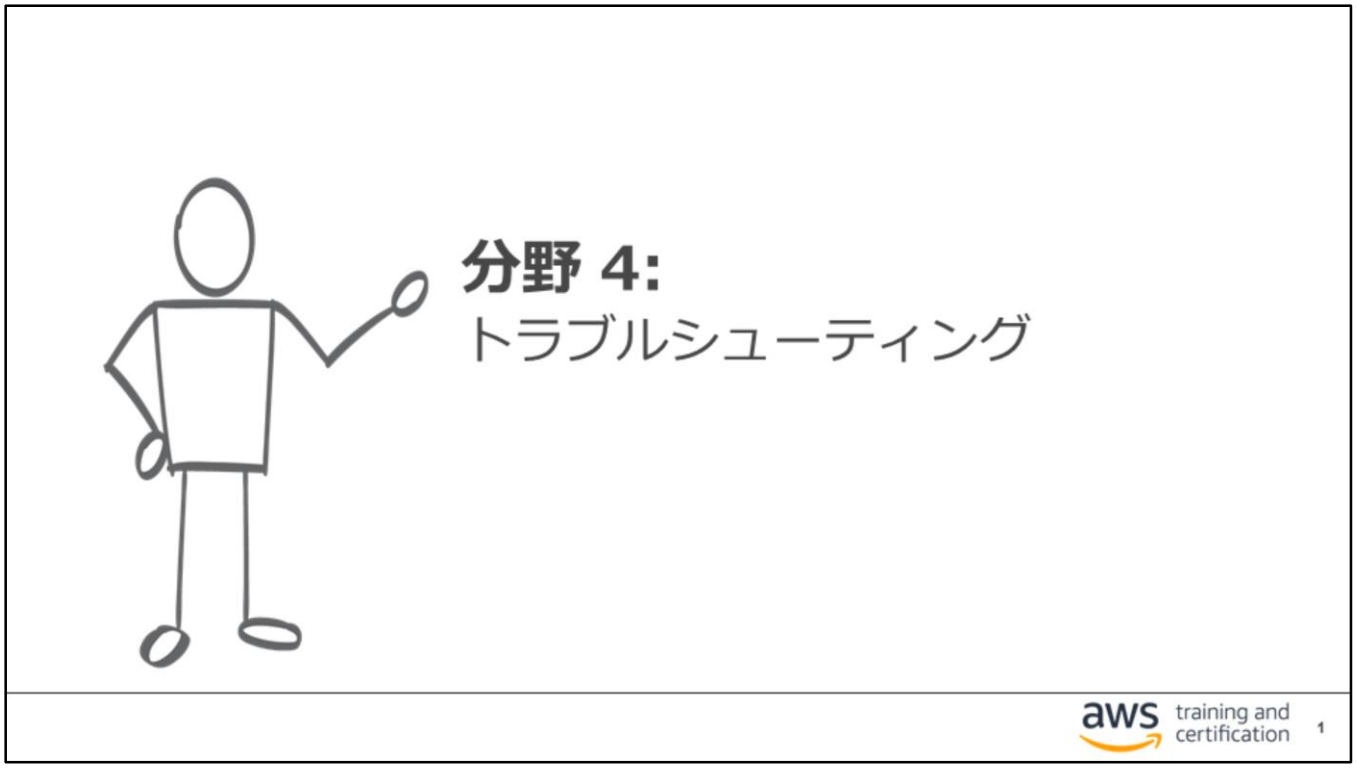


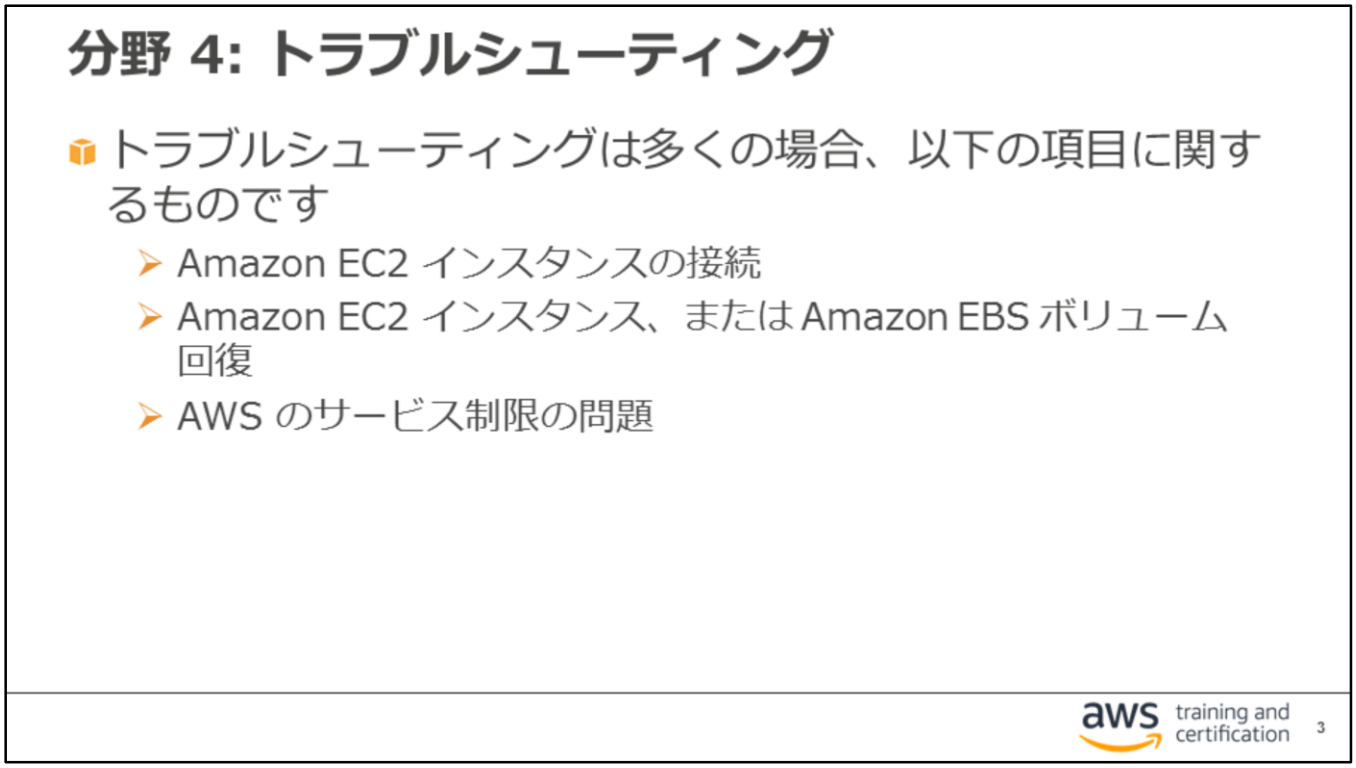
このセッションでは、分野4 トラブルシューティングの説明をしていきます。

本セッションでは一般的なトラブルシューティングシナリオをいくつか考察し、シナリオごとに問題例を一緒に考えていきます。

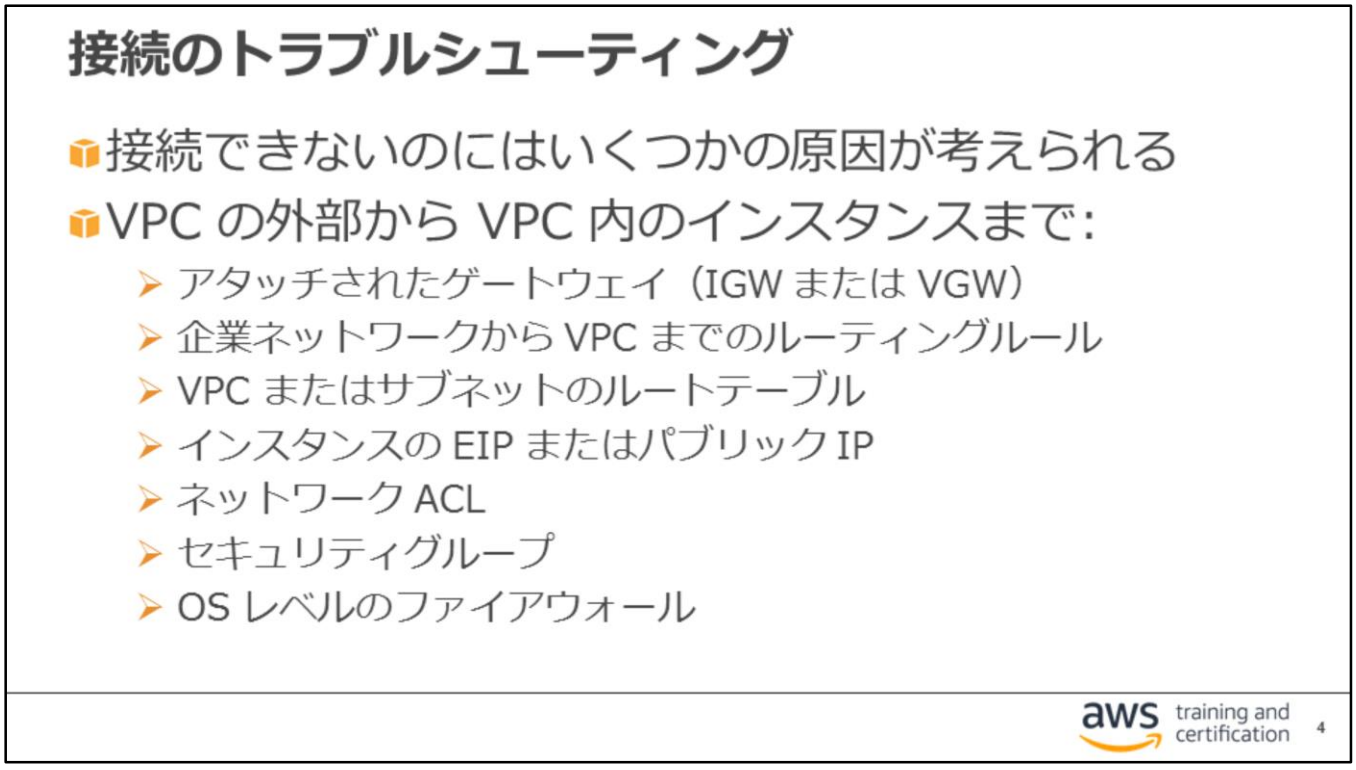
分野 4: トラブルシューティング

- 一般的なトラブルシューティングの情報および質問

この分野では、一般的なトラブルシューティングの情報や質問が出てきます。
それでは、いくつのシナリオを見ていきましょう。



トラブルシューティングで試験によく出るシナリオとして、3つの項目があります。
1つ目は、インスタンスの接続に関するトラブルシューティングです。Amazon EC2 インスタンスのSSH やHTTP といった特定ポートに接続する際に、接続できないという問題です。
2つ目は、Amazon EC2 インスタンスが応答しない、起動しないなどのトラブルシューティングや、Cドライブのようなルートボリュームの復旧に関するトラブルシューティングです。
3つ目は、Amazon EC2、Amazon S3、EBS、その他AWS サービスの制限に関する問題です。

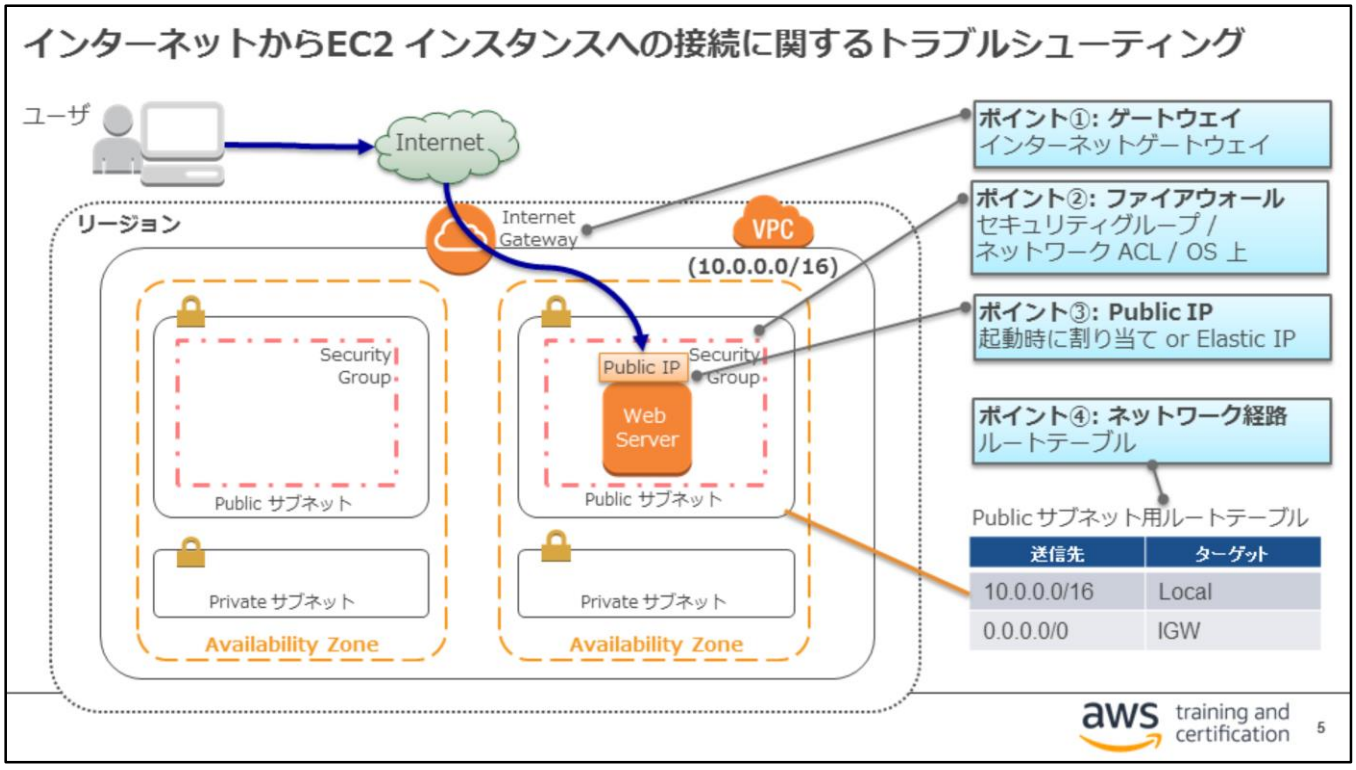


まず接続できないトラブルシューティングを見ていきます。
接続できない原因は複数ありますが、いくつか例を見ていきましょう。

まず、インターネットゲートウェイや仮想プライベートゲートウェイといったゲートウェイが、VPC にアタッチされているかどうかです。VPC 内では、インターネット接続にインターネットゲートウェイ が必要です。また、VPC にデータセンターから接続するには仮想プライベートゲートウェイが必要です。ゲートウェイの種類や役割を理解していることが必要です。

次は、VPC またはルートテーブルに適切なルートが定義されているかどうかです。特にVPC 内と外で通信をする場合は、適切なルートをルートテーブルに設定する必要があり、そのことを理解している必要があります。

最後は、Amazon EC2 インスタンスのポートに接続できるかどうかです。 これはネットワーク ACL やセキュリティグループ などのファイアウォールの仕組みで適切な許可がされているかどうかが確認するポイントとなります。

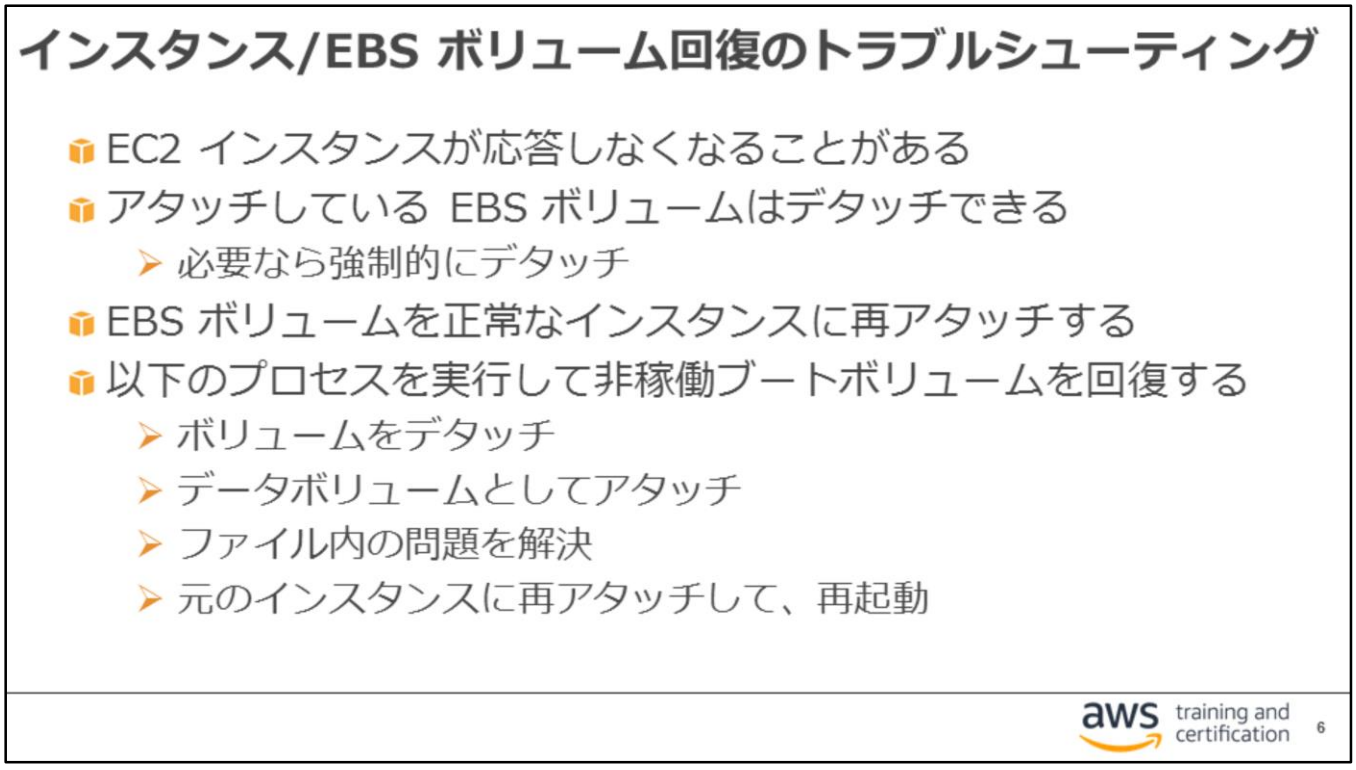


試験によく出る接続に関するトラブルシューティングの問題として、インターネットからEC2 インスタンスに接続できない場合の原因を特定するといった問題があります。
この問題では、VPC とEC2 インスタンスの構成において、4つのポイントを理解していることが重要となりますのでここでは重点的に解説します。

ポイントの1つ目として、インターネットゲートウェイを作成し、VPC にアタッチされていることが確認ポイントになります。
2点目として、セキュリティグループやネットワークACL の設定で、通信を許可したいパケットが通るように構成されていることです。ファイアウォールに関してはOS上で設定している可能性もあります。
3点目として、EC2 インスタンスのパブリックIP アドレスが関連付けられていることです。パブリックIP アドレスの設定方法は、EC2 インスタンス起動時のパラメータでパブリックIP割り当てを有効にしておくか、EC2 インスタンス起動後に、Elastic　IP を EC2 インスタンスに関連付けることで実現できます。
4点目は、ネットワーク経路の設定です。Public サブネットのルートテーブルに、インターネットゲートウェイへの経路が定義されている必要があります。
この4点が適切に設定されているとインターネットからアクセスが可能となります。

試験問題では、この4つのどこかが設定不足であり、不足している箇所を特定する問題が出ます。
なお、本コースではこのスライドに挙げた各機能の詳細は説明しませんので、不明な機能がありましたら、試験前に確認してください。

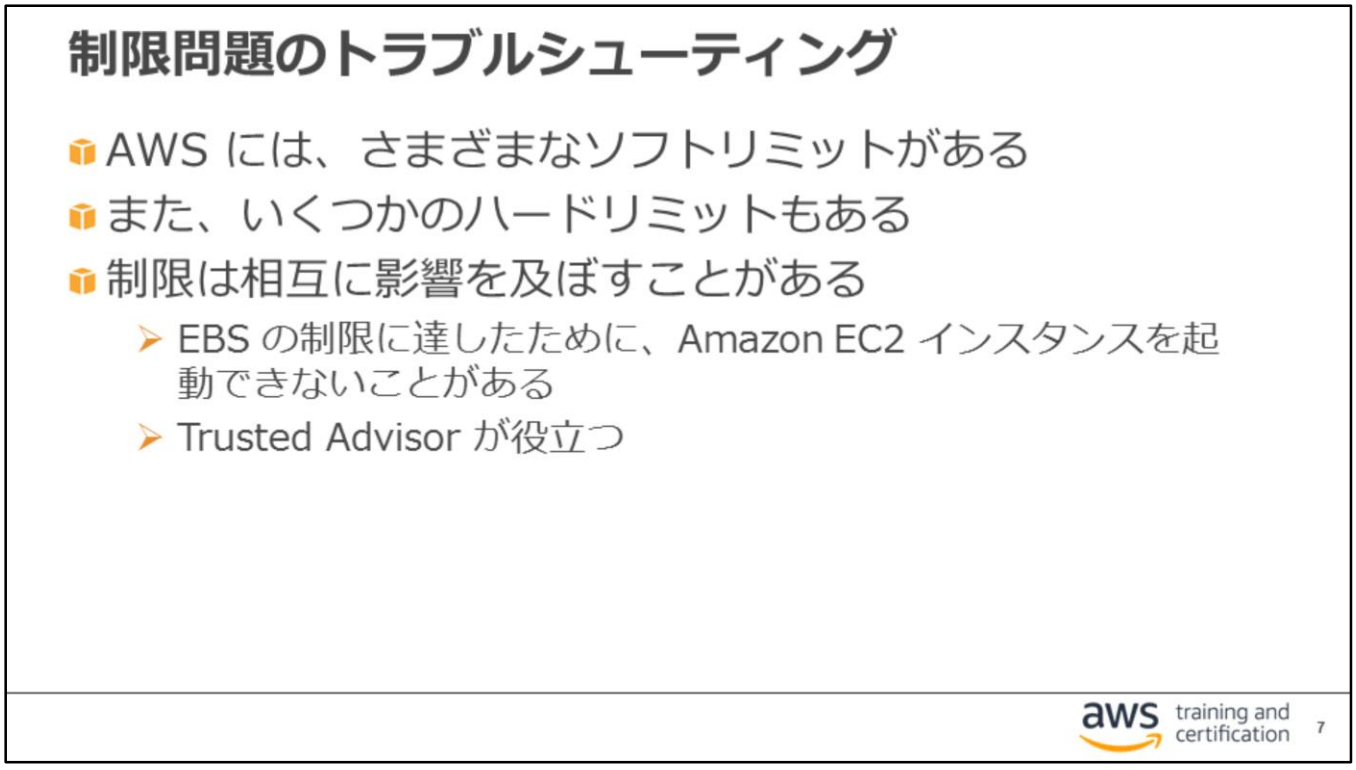
また、この設定は複雑ですので、机上だけの学習ではなく実際にAWS 上で設定をしてみることをおすすめします。



次は、インスタンス/EBS ボリューム回復のトラブルシューティングです。

複数の理由により Amazon EC2 インスタンスが応答しなくなることがあります。
例えば、Linuxのカーネルパラメータにおかしな設定をしてしまったとか、
Windowsのレジストリを不正に変更してしまったなどが挙げられます。
このような場合は、EC2 インスタンスを再起動しても回復しない可能性があります。その場合どのように回復すればよいか、その手順を理解している必要があります。

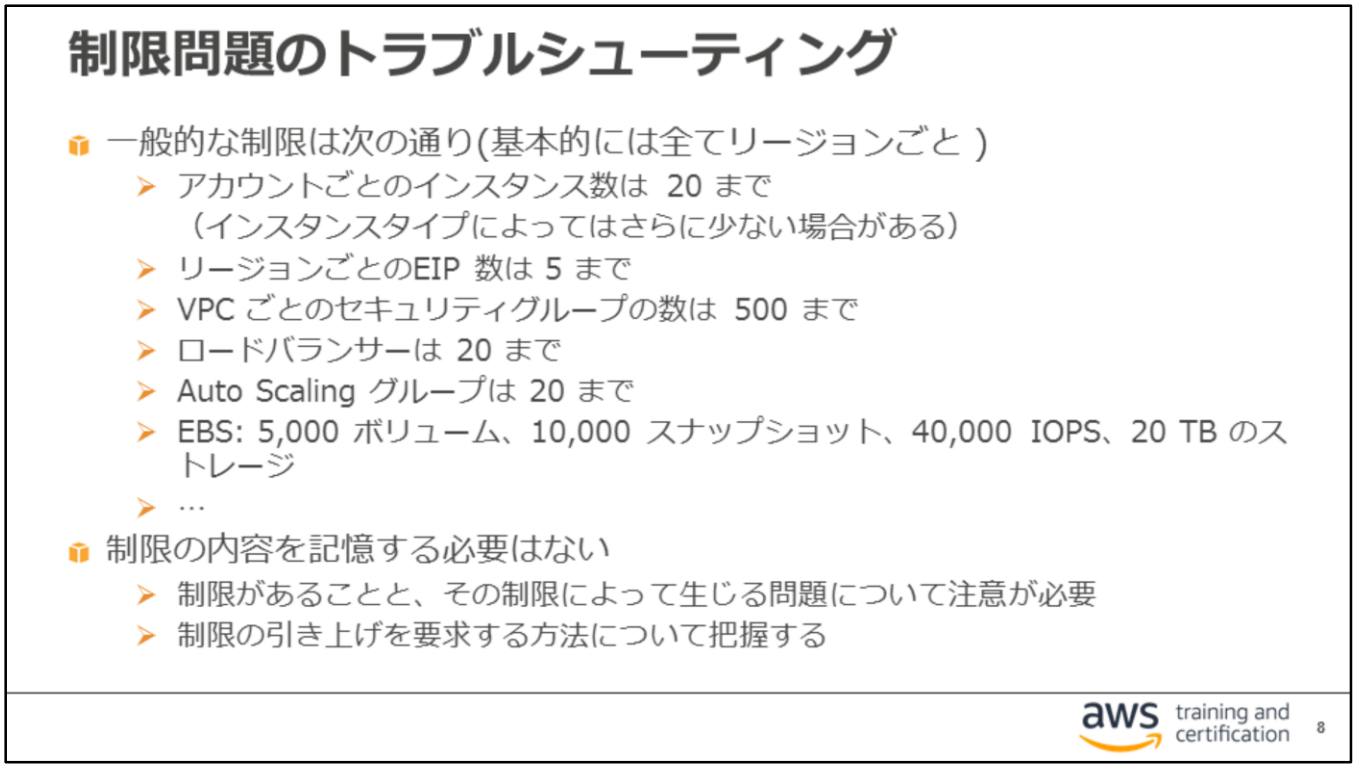
具体的には、次のような手順をとります。
まず、応答しないインスタンスからEBS ルートボリュームをデタッチします。
次に、そのボリュームを正常に稼働中の別のインスタンスにデータボリュームとしてアタッチし、マウントします。
データボリューム内を調べて設定の問題を修正し、ボリュームをアンマウントします。
修正したボリュームを元のインスタンスに再アタッチして、再起動します。



最後に知っておくべき内容は、制限に関する問題です。

AWS には様々なソフトリミットやハードリミットがあります。
ソフトリミットの例としては、S3 のバケットの数はデフォルトで100 個までなどです。ハードリミットの例としては、例えば、S3 のオブジェクトは最大 5 TB までなどです。
ソフトリミットは、制限緩和申請を挙げることで、制限を拡張することが可能です。

これらのリミットの具体的な数字を暗記する必要はありませんが、各サービスには、制限があるということを理解している必要があります。
また、制限は相互に影響を及ぼすことがあります。例えば、EBS の制限に達したために、EC2 インスタンスを起動できないなどです。
なお、使用量や制限を確認するには、Trusted　Advisor を利用すると便利です。



一般的な制限事項はここに書いてある通りです。ただ試験においては、制限の内容を暗記する必要はありません。

ただし、さまざまなサービスに制限があり、制限により問題が生じることがある点は覚えておいてください。

また、制限の引き上げを要求する方法については覚えておく必要があります。

例題

ルートテーブルをデフォルトに設定した既存の VPC が 1 つと、単一のサブネットで実行中の Linux インスタンスが複数あります。同じセキュリティグループを使用して、同じサブネット内で Amazon が提供する AMI から Windows インスタンスを起動します。Windows インスタンスは稼働中ですが、そのインスタンスには RDP 経由で接続することができません。ただし、SSH 経由で Linux インスタンスに接続し、そこから Windows インスタンスに Ping を実行できます。RDP 接続を実行できるようにするにはどのようにすべきですか?

1) Windows のファイアウォールルールを追加して、RDP を許可する必要がある。
2) ルーティングルールを、RDP トラフィックを許可するように設定する必要がある。
3) セキュリティグループルールを追加して、RDP トラフィックを許可する必要がある。
4) ネットワーク ACL 許可ルールを追加して、RDP トラフィックを許可する必要がある。

では、トラブルシューティングにおける例題を見てみましょう。この例題はEC2インスタンスに接続できないというトラブルシューティングの問題です。

次のページから解説します。

例題

ルートテーブルをデフォルトに設定した既存の **VPC** が 1 つと、単一のサブネットで実行中の **Linux** インスタンスが複数あります。**同じセキュリティグループ**を使用して、同じサブネット内で **Amazon が提供する AMI から Windows インスタンスを**起動します。Windows インスタンスは稼働中ですが、そのインスタンスには **RDP** 経由で**接続することができません。**ただし、SSH 経由で Linux インスタンスに接続し、そこから Windows インスタンスに Ping を実行できます。 RDP 接続を実行できるようにするにはどのようにすべきですか?

1) Windows のファイアウォールルールを追加して、RDP を許可する必要がある。
2) ルーティングルールを、RDP トラフィックを許可するように設定する必要がある。
3) セキュリティグループルールを追加して、RDP トラフィックを許可する必要がある。
4) ネットワーク ACL 許可ルールを追加して、RDP トラフィックを許可する必要がある。

aws training and certification 10

この問題のポイントは、すでに起動しているLinux インスタンスと同じサブネットの中に、Windows　インスタンスを起動したが、RDPでアクセスできなかったので原因を特定するというトラブルシューティングの問題となります。
条件としては、Windows はAmazon が提供するAMI から起動されています。
SSH 経由でLinux には接続できており、Windows に対してLinux からPingを実行できるのでVPC内部の通信は正常にできていると考えられます。

それでは選択肢１から見ていきましょう。

「Windows のファイアウォールルールを追加して、RDP を許可する必要がある。」

これはどうでしょうか？

例題

ルートテーブルをデフォルトに設定した既存の **VPC** が 1 つと、単一のサブネットで実行中の **Linux** インスタンスが複数あります。**同じセキュリティグループ**を使用して、同じサブネット内で **Amazon が提供する AMI から Windows インスタンスを**起動します。Windows インスタンスは稼働中ですが、そのインスタンスには **RDP** 経由で**接続することができません。**ただし、SSH 経由で Linux インスタンスに接続し、そこから Windows インスタンスに Ping を実行できます。 RDP 接続を実行できるようにするにはどのようにすべきですか?

~~1) Windows のファイアウォールルールを追加して、RDP を許可する必要がある。~~
（Windows AMI は RDP を許可している）
2) ルーティングルールを、RDP トラフィックを許可するように設定する必要がある。
3) セキュリティグループルールを追加して、RDP トラフィックを許可する必要がある。
4) ネットワーク ACL 許可ルールを追加して、RDP トラフィックを許可する必要がある。

aws training and certification 11

選択肢 1 は正しくありません。Windows ファイアウォールが RDP トラフィックをブロックすることはありますが、このインスタンスは Amazon が提供する Windows AMI から起動されたので、OS が RDP を許可するように設定されています。

選択肢2を見てみましょう。「ルーティングルールを、RDP トラフィックを許可するように設定する必要がある。」
これはどうでしょうか？

例題

ルートテーブルをデフォルトに設定した既存の **VPC** が 1 つと、単一のサブネットで実行中の **Linux** インスタンスが複数あります。**同じセキュリティグループ**を使用して、同じサブネット内で **Amazon が提供する AMI から Windows インスタンスを**起動します。Windows インスタンスは稼働中ですが、そのインスタンスには **RDP** 経由で**接続することができません。**ただし、SSH 経由で Linux インスタンスに接続し、そこから Windows インスタンスに Ping を実行できます。 RDP 接続を実行できるようにするにはどのようにすべきですか?

~~1) Windows のファイアウォールルールを追加して、RDP を許可する必要がある。~~
（Windows AMI は RDP を許可している）
~~2) ルーティングルールを、RDP トラフィックを許可するように設定する必要がある。~~
（ルーティングルールが定義するのはパケットパスのみ）
3) セキュリティグループルールを追加して、RDP トラフィックを許可する必要がある。
4) ネットワーク ACL 許可ルールを追加して、RDP トラフィックを許可する必要がある。

aws training and certification 12

選択肢 2 も間違いです。ルーティングルールは、ネットワークトラフィックがサブネットで流れる経路を決定しますが、ポートまたはプロトコルによって通信が制限されるわけではありません。

選択肢３　はどうでしょうか？
「セキュリティグループルールを追加して、RDP トラフィックを許可する必要がある。」 です。

これは正しいように見えます。

選択肢 4 はどうでしょうか？
「ネットワーク ACL 許可ルールを追加して、RDP トラフィックを許可する必要がある。」

例題

ルートテーブルをデフォルトに設定した既存の **VPC** が 1 つと、単一のサブネットで実行中の **Linux** インスタンスが複数あります。**同じセキュリティグループ**を使用して、同じサブネット内で **Amazon が提供する AMI から Windows インスタンスを**起動します。Windows インスタンスは稼働中ですが、そのインスタンスには **RDP** 経由で**接続することができません。**
ただし、SSH 経由で Linux インスタンスに接続し、そこから Windows インスタンスに Ping を実行できます。 RDP 接続を実行できるようにするにはどのようにすべきですか?

~~1) Windows のファイアウォールルールを追加して、RDP を許可する必要がある。~~
（Windows AMI は RDP を許可している）
~~2) ルーティングルールを、RDP トラフィックを許可するように設定する必要がある。~~
（ルーティングルールが定義するのはパケットパスのみ）
3) セキュリティグループルールを追加して、RDP トラフィックを許可する必要がある。
~~4) ネットワーク ACL 許可ルールを追加して、RDP トラフィックを許可する必要がある。~~
（デフォルトのネットワーク ACL ではすべてが許可されている）

aws training and certification 13

選択肢4は除外できます。デフォルトのネットワーク ACL ではすべてのトラフィックが許可されており、許可ルールを追加で設定する必要性はないからです。

よって、この例題の正解は選択肢3ということになります。
セキュリティグループに、RDP の許可ルールを追加する必要があります。

この問題を解く際に、理解しておく必要があるのは、セキュリティグループはデフォルトではインバウンドの通信はすべて拒否されているということです。明示的に通したいポートを開放する必要があります。
今回の例題の構成では、Linux にはSSH でログインできるため、Linux 用に SSH ポート 22 は解放されていますが、
Windows からのアクセスに必要な RDP ポート 3389 が開いていない状況であったということが考えられます。

例題

Amazon EBS-Backed Amazon EC2 インスタンスで障害が発生し、応答しなくなりました。ルートボリュームに重要な情報があるため回復させる必要がありますが、あらゆる手段を試みてもインスタンスにログインできません。元の AMI にはアクセスできますが、ルートボリュームの最新のバックアップが利用できません。どうすればボリューム内の情報を回復できますか?

1) 障害が発生した Amazon EC2 インスタンスを削除してから、Amazon EBS ボリュームを回復する。
2) ルートボリュームのスナップショットを作成し、スナップショットから新しいインスタンスを起動する。
3) 元の AMI から新しいインスタンスを起動する。
4) ボリュームをデタッチし、別のインスタンスにデータボリュームとしてアタッチする。

では次の例題を見ていきましょう。こちらはEC2インスタンスのトラブルシューティングの例題です。

次のページから解説します。

例題

Amazon **EBS-Backed** Amazon **EC2 インスタンスで**障害が発生し、応答しなくなりました。ルートボリュームに重要な情報があるため回復させる必要がありますが、**あらゆる手段を試みても**インスタンスに**ログインできません**。元の AMI にはアクセスできますが、ルートボリュームの最新のバックアップが利用できません。どうすればボリューム内の**情報**を**回復**できますか?

1) 障害が発生した Amazon EC2 インスタンスを削除してから、Amazon EBS ボリュームを復旧する。
2) ルートボリュームのスナップショットを作成し、スナップショットから新しいインスタンスを起動する。
3) 元の AMI から新しいインスタンスを起動する。
4) ボリュームをデタッチし、別のインスタンスにデータボリュームとしてアタッチする。

それでは解説に移ります。この例題もよくあるシナリオです。
EC2 インスタンスに障害が発生してしまい、応答しないもしくはアクセスできない状況になったが、ルートボリュームから一部のデータを取り出す必要があるということになります。
その場合、どういった方法が取れるのかが問われています。

では、選択肢1を見てみましょう。
「障害が発生した Amazon EC2 インスタンスを削除してから、Amazon EBS ボリュームを復旧する。」

例題

Amazon **EBS-Backed** Amazon **EC2 インスタンスで**障害が発生し、応答しなくなりました。ルートボリュームに重要な情報があるため回復させる必要がありますが、**あらゆる手段を試みても**インスタンスに**ログインできません**。元の AMI にはアクセスできますが、ルートボリュームの最新のバックアップが利用できません。どうすればボリューム内の**情報**を**回復**できますか?

1) ~~障害が発生した Amazon EC2 インスタンスを削除してから、Amazon EBS ボリュームを復旧する。~~（削除と同時にルートボリュームが削除される）
2) ルートボリュームのスナップショットを作成し、スナップショットから新しいインスタンスを起動する。
3) 元の AMI から新しいインスタンスを起動する。
4) ボリュームをデタッチし、別のインスタンスにデータボリュームとしてアタッチする。

aws training and certification 16

選択肢 1 では解決できません。デフォルトの設定では、インスタンス削除と同時にルートボリュームも削除されますから、回復の対象となるボリュームが無くなってしまいます。
ただし、設定によりルートボリュームを残すことも可能です。今回はその条件が書いてないため、ロートボリュームも削除されてしまう可能性が大きいためほかの手段をとる方がより安全であるといえます。

選択肢2はどうでしょうか？
「ルートボリュームのスナップショットを作成し、スナップショットから新しいインスタンスを起動する。」

例題

Amazon **EBS-Backed** Amazon **EC2 インスタンスで**障害が発生し、応答しなくなりました。ルートボリュームに重要な情報があるため回復させる必要がありますが、**あらゆる手段を試みても**インスタンスに**ログインできません**。元の AMI にはアクセスできますが、ルートボリュームの最新のバックアップが利用できません。どうすればボリューム内の**情報**を**回復**できますか?

1) ~~障害が発生した Amazon EC2 インスタンスを削除してから、Amazon EBS ボリュームを復旧する。~~（削除と同時にルートボリュームが削除される）
2) ~~ルートボリュームのスナップショットを作成し、スナップショットから新しいインスタンスを起動する。~~（起動は AMI からのみ可能）
3) 元の AMI から新しいインスタンスを起動する。
4) ボリュームをデタッチし、別のインスタンスにデータボリュームとしてアタッチする。

選択肢 2 も間違いです。スナップショットからインスタンスを起動することはできません。AMI を作成する必要があります。
補足として、EBSのスナップショットからAMIを作成することは可能です。ただし、そもそもボリュームが破損していてこの操作では回復しない可能性があます。

では、選択肢3はどうでしょうか？
「元の AMI から新しいインスタンスを起動する。」

例題

Amazon **EBS-Backed** Amazon **EC2 インスタンスに**障害が発生し、応答しなくなりました。ルートボリュームに重要情報が入っているため復旧する必要がありますが、**あらゆる手段を試みても**インスタンスに**ログインできません**。元の AMI にはアクセスできますが、ルートボリュームの最新のバックアップが利用できません。どうすればボリューム内の**情報**を**復旧**できますか?

~~1) 障害が発生した Amazon EC2 インスタンスを削除してから、Amazon EBS ボリュームを復旧する。~~（削除と同時にルートボリュームが削除される）
~~2) ルートボリュームのスナップショットを作成し、スナップショットから新しいインスタンスを起動する。~~（起動は AMI からのみ可能）
~~3) 元の AMI から新しいインスタンスを起動する。~~（同一データではない）
4) ボリュームをデタッチし、別のインスタンスにデータボリュームとしてアタッチする。

aws training and certification 18

選択肢 3 は間違いです。元のAMI には障害が発生したインスタンスと同じデータは含まれていません。

よって、選択肢 4 が正解となります。
障害が発生したインスタンスからボリュームをデタッチし、正常なインスタンスにデータボリュームとしてアタッチします。

例題

VPC パブリックサブネットにアプリケーションをデプロイしました。複数の同じ EC2 アプリケーションインスタンスが正常に稼働し、インターネット経由でアクセスできます。ここで、同じ AMI およびセキュリティグループを使用して、同じサブネットに新たな Amazon EC2 インスタンスを起動し、アプリケーションをスケールすることにしました。ところが、新しいインスタンスにはインターネットからアクセスできないことがわかりました。どこを変更すれば、新しいインスタンスにインターネットからアクセスできるようになりますか?

1) パブリックサブネット内に NAT インスタンスをデプロイする。
2) 新しいインスタンスのゲスト OS に、パブリック IP アドレスを設定する。
3) Elastic IP アドレスを新しいインスタンスに割り当てる。
4) サブネットのルートテーブルを、新しいインスタンスへのアクセスを許可するように変更する。

それでは、本セッションの最後の例題です。

次のページから解説します。

例題

VPC パブリックサブネットにアプリケーションをデプロイしました。複数の同じ**EC2 アプリケーションインスタンス**が正常に稼働し、インターネット経由で**アクセスできます**。ここで、同じ AMI およびセキュリティグループを使用して、**同じサブネット**に新たな Amazon **EC2 インスタンス**を起動し、アプリケーションをスケールすることにしました。ところが、**新しいインスタンスにはインターネットからアクセスできない**ことがわかりました。どこを変更すれば、新しいインスタンスにインターネットからアクセスできるようになりますか?

1) パブリックサブネット内に NAT インスタンスをデプロイする。
2) 新しいインスタンスのゲスト OS に、パブリック IP アドレスを設定する。
3) Elastic IP アドレスを新しいインスタンスに割り当てる。
4) サブネットのルートテーブルを、新しいインスタンスへのアクセスを許可するように変更する。

aws training and certification 20

この問題も接続性に関する問題で、特にインターネットからEC2 にアクセスする際のポイントを理解しているかが問われています。
設問文の中に次のような重要な情報があります。
まず、パブリックサブネットだということ。次に既存のインスタンスにはインターネットからアクセスできるが、新しいインスタンスにはアクセスできないことです。

この問題を解くには先ほどご紹介したインターネットからEC2 インスタンスにアクセスする際の4つの確認ポイントを理解していることが必要です。

では、選択肢1を見てみましょう。

「パブリックサブネット内に NAT インスタンスをデプロイする。」

例題

VPC パブリックサブネットにアプリケーションをデプロイしました。複数の同じ**EC2 アプリケーションインスタンス**が正常に稼働し、インターネット経由で**アクセスできます**。ここで、同じ AMI およびセキュリティグループを使用して、**同じサブネット**に新たな Amazon **EC2 インスタンス**を起動し、アプリケーションをスケールすることにしました。ところが、**新しいインスタンスにはインターネットからアクセスできない**ことがわかりました。どこを変更すれば、新しいインスタンスにインターネットからアクセスできるようになりますか?

~~1) パブリックサブネット内に NAT インスタンスをデプロイする。~~ (パブリックサブネット内のインスタンスが NAT インスタンスを使う必要はない)
2) 新しいインスタンスのゲスト OS に、パブリック IP アドレスを設定する。
3) Elastic IP アドレスを新しいインスタンスに割り当てる。
4) サブネットのルートテーブルを、新しいインスタンスへのアクセスを許可するように変更する。

aws training and certification 21

選択肢 1 は正しくありません。パブリックサブネット内のインスタンスが NAT インスタンスを使う必要はありません。パブリックサブネット内のインスタンスにインターネットからアクセスするために、パブリック IP と EIP を使用できます。

では、選択肢2を見てみましょう。

「新しいインスタンスのゲスト OS に、パブリック IP アドレスを設定する。」

例題

VPC パブリックサブネットにアプリケーションをデプロイしました。複数の同じ **EC2 アプリケーションインスタンス**が正常に稼働し、インターネット経由で**アクセスできます**。ここで、同じ AMI およびセキュリティグループを使用して、**同じサブネット**に新たな Amazon **EC2 インスタンス**を起動し、アプリケーションをスケールすることにしました。ところが、**新しいインスタンスにはインターネットからアクセスできない**ことがわかりました。どこを変更すれば、新しいインスタンスにインターネットからアクセスできるようになりますか?

1) ~~パブリックサブネット内に NAT インスタンスをデプロイする。~~（パブリックサブネット内のインスタンスが NAT インスタンスを使う必要はない）
2) ~~新しいインスタンスのゲスト OS に、パブリック IP アドレスを設定する。~~（プライベート IP を知っているのはホスト OS のみ）
3) Elastic IP アドレスを新しいインスタンスに割り当てる。
4) サブネットのルートテーブルを、新しいインスタンスへのアクセスを許可するように変更する。

aws training and certification 22

選択肢 2 は正しくありません。プライベート IP についてはOS が知っていますが、パブリック IP と EIP は、インスタンスの外側のVPC内部の NAT 構造です。

選択肢3はどうでしょうか？

「Elastic IP アドレスを新しいインスタンスに割り当てる。」

これは正しいように見えます。

続いて選択肢4はどうでしょうか？

「サブネットのルートテーブルを、新しいインスタンスへのアクセスを許可するように変更する。 」

例題

VPC パブリックサブネットにアプリケーションをデプロイしました。複数の同じ **EC2 アプリケーションインスタンス**が正常に稼働し、インターネット経由で**アクセスできます**。ここで、同じ AMI およびセキュリティグループを使用して、**同じサブネット**に新たな Amazon **EC2 インスタンス**を起動し、アプリケーションをスケールすることにしました。ところが、**新しいインスタンスにはインターネットからアクセスできない**ことがわかりました。どこを変更すれば、新しいインスタンスにインターネットからアクセスできるようになりますか?

1) ~~パブリックサブネット内に NAT インスタンスをデプロイする。~~（パブリックサブネット内のインスタンスが NAT インスタンスを使う必要はない）
2) ~~新しいインスタンスのゲスト OS に、パブリック IP アドレスを設定する。~~（ホスト OS が知っているのはプライベート IP のみ）
3) **Elastic IP アドレスを新しいインスタンスに割り当てる。**
4) ~~サブネットのルートテーブルを、新しいインスタンスへのアクセスを許可するように変更する。~~（ルートテーブルはサブネット全体に適用され、サブネット内の他のインスタンスは正常）

aws training and certification 23

選択肢 4 は正しくありません。ルートテーブルはサブネット全体に適用されますが、そもそもサブネット内の他のインスタンスは正常にアクセスできますので、ルートテーブルの問題ではありません。

よって、この例題は選択肢 3 が正解です。パブリックサブネットからインターネット経由で通信するには、インスタンスにパブリック IP または Elastic IP が必要です。それに加えて、インターネットゲートウェイ、ゲートウェイへの経路、適切なセキュリティグループ / ネットワークACL のルールも必要になります。

以上で、本セッションの説明は終了となります。

ありがとうございました。

[コピー禁止]