日本語抄訳

RCA - 複数の Microsoft サービスおよび Azure Active Directory と連携したアプリケーションでの認証エラー (Tracking ID SM79-F88)

影響の概要:

2020 年 9 月 28 日の 21:25 UTC（日本時間 9 月 29 日 AM 6：25）から 2020 年 9 月 29 日の 00:23 UTC（日本時間 9 月 29 日 AM 9：23）の間で Azure Active Directory (Azure AD) を認証基盤として利用するすべての Microsoft およびサードパーティのアプリケーション、サービスの認証処理でエラーが生じた可能性があります。Azure AD B2C を使用して認証を行うアプリケーションも影響を受けました。

事象発生時点で Azure AD を利用したクラウド サービスで認証済みでなかったユーザーは、問題の影響を受けた可能性がより高く、平均して以下に示すような可用性の値で複数の認証リクエストが失敗していた可能性があります。これらの値は、さまざまな顧客とワークロードの情報を元に集計されました。

- ヨーロッパ: 事象発生期間中の成功率 81 %。
- アメリカ: 事象発生期間中の成功率は 17 %、緩和直前には 37 % に改善。
- アジア: 事象発生期間中の最初の 120 分間の成功率は 72 %。業務時間のピークが始まるころの可用性は最低で 32 % に低下。
- オーストラリア: 事象発生期間中の成功率は 37 %。

2020 年 9 月 29 日 00:23 UTC（日本時間 9 月 29 日 AM 9：23）までに、大多数のお客様のサービスは通常の運用可能な状態に復旧しましたが、その後も認証リクエストの失敗が散発的に発生しており、02:25 UTC（日本時間 AM 11：25）まで影響が生じていた可能性があります。

事象開始時刻前に認証を行っていたユーザーは、アクセスしているアプリケーションやサービスに依存しますが、この問題による影響を受けた可能性は低い状態でした。

仮想マシン、仮想マシンのスケールセット、および Azure Kubernetes サービスのマネージド アイデンティティ サービスには回復機能が備えられており、事象発生期間中にも平均 99.8 % の可用性を保ちました。

根本原因:

9 月 28 日 21:25 UTC（日本時間 9 月 29 日 AM 6：25）に、内部の検証テスト リングを対象としたサービス アップデートが展開され、その結果、Azure AD のバックエンド サービスの起動時にクラッシュが発生しました。Azure AD バックエンド サービスのセーフ デプロイ プロセス（SDP）システムの潜在的なコード欠陥により、通常の検証プロセスを介さず本番環境にサービス アップデートが直接展開されました。

Azure AD は、世界中の複数のデータセンターにまたがる複数のパーティションを持つアクティブ・アクティブ構成で展開された地理的に分散したサービスであり、隔離境界を持ちます。通常、変更は最初に顧客データを含まない検証リングを対象にし、次に Microsoft のみのユーザーを含む内部リング、最後に本番環境を対象に展開されます。これらの変更は、数日かけて 5 つのリングに渡って段階的に展開されます。

今回のケースでは、潜在的な不具合により展開に使用するメタデータがシステムにより正しく認識されず、SDP システムが正しく検証テスト リングを展開先として設定できませんでした。その結果、すべてのリングが同時に展開先になりました。この不適切な展開により、サービスの可用性が低下しました。

影響が発生してから数分以内に、自動ロールバック システム（通常であれば影響度と影響の発生時間が限定されることが期待される）を使用して変更を元に戻す処置を行いました。しかし、SDP システムの潜在的な欠陥が展開メタデータを破損させていたため、手動のロールバック プロセスに頼らざるを得ず、問題を緩和するまでに大幅に時間を要する結果となりました。

緩和策

監視により、影響が発生してから数分以内にサービスの劣化を検知し、直ちにトラブルシューティングを開始しました。以下の対応を実施しました。

・ 問題は UTC 21:25（日本時間 9 月 29 日 AM 6：25）に始まり、 5 分以内に監視システムで不健全な状態が検出され、直ちにエンジニアによる調査が開始されました。

・ その後 30 分間、問題のトラブルシューティングと並行して、顧客への影響を最小限に抑えるとともに問題回避を迅速化するための一連の手順が実施されました。これには、問題が緩和された後に予想される負荷を処理するために、Azure AD サービスの一部をスケールアウトし、バックアップの Azure AD 認証システムに特定のワークロードをフェイルオーバーしたことも含まれます。

・ 22:02 UTC（日本時間 9 月 29 日 AM 7：02）に、根本原因を特定し、修復を開始し、自動ロールバック メカニズムを開始しました。

・ SDP メタデータの破損が原因で自動ロールバックに失敗しました。22:47 UTC（日本時間 AM 7：47）に、SDP システムを利用せずにサービス構成を手動で更新するプロセスを開始し、23:59 UTC（日本時間 AM 8：59）までにすべての操作が完了しました。

・ UTC 00:23（日本時間 AM 9：23）までに、十分な数のバックエンドのサービス インスタンスが正常な状態に戻り、通常のサービス運用状態に回復しました。

・ いくつか残存する影響が生じていたすべてのサービス インスタンスは、02:25 UTC（日本時間 AM 11：25）までに復旧しました。

次のステップ:

今回の影響を受けましたお客様に深くお詫び申し上げます。このようなインシデントが将来的に発生しないよう、Microsoft Azure プラットフォームと当社のプロセスを改善するための措置を継続的に講じています。今回のケースでは、対応策として以下が含まれます（ただし、これらに限定されません）。

以下は既に完了済みの内容となります。

- Azure AD バックエンド SDP システムの潜在的なコードの欠陥の修正。
- 破損から保護するために、最後の動作確認済み（last known-good）メタデータを復元できるように既存のロールバック システムを修正。
- ロールバック操作の訓練の範囲と頻度を拡大。

残りのステップは以下のとおりです。

- 今回特定された類似の問題を防ぐために、Azure AD サービスのバックエンド SDP システムに追加の保護機能を適用。

- 将来的に同様の問題が発生した場合の影響を大幅に軽減するため最優先事項として、すべての主要サービスへの Azure AD バックアップ認証システムの展開を早急に実施。
- 問題が生じてから 15 分以内に影響を受けた顧客に一報する Azure の顧客通知の仕組みに Azure AD に対応したシナリオを追加。

フィードバックのお願い:

Azure カスタマー・コミュニケーション・エクスペリエンスの向上のためのアンケートにご協力ください: https://aka.ms/AzurePIRSurvey