ケーススタディ

digicert

Digicert Trust Lifecycle Manager による多様なワークロードのセキュアな証明書管理の自動化

エグゼクティブサマリー

組織名 : デジサート
業種 : テクノロジー
本部 : ユタ州リーハイ

主なビジネス要件 :

- 会社の仮想マシン（VM）上の電子証明書を効率的に管理する
- 証明書をプロビジョニングして多様なワークロードにインストールするために必要な多くのステップを合理化する
- 証明書ライフサイクル管理（CLM）のすべてのプロセスを自動化する

ソリューション :

- DigiCert Trust Lifecycle Manager

主な利点 :

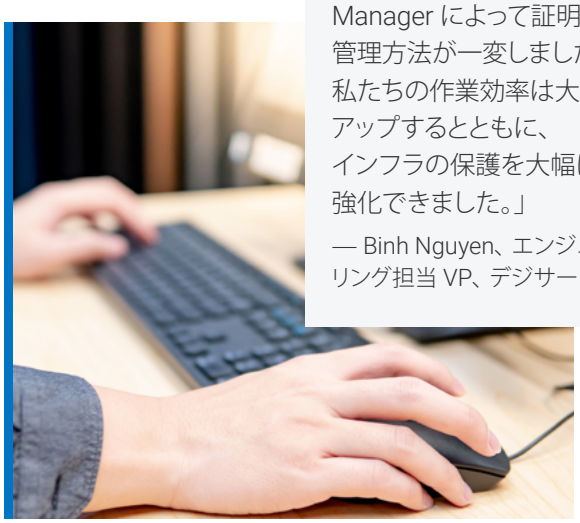
- 構成テンプレートを使用することで、SRE チームは DigiCert Trust Lifecycle Manager の自動登録機能を活用し、証明書のプロビジョニングとインストールの時間を数時間から数分に短縮できる
- 自動化により、証明書管理を合理化し、証明書のエラーや有効期限切れに起因する機能停止やビジネス中断の可能性を下げる
- サードパーティプラットフォーム、クラウド、デバイスとすぐに統合し、エンドツーエンドの証明書ライフサイクル管理を行うことにより、ビジネスの拡大に伴う IT 部門の負担を大幅に軽減する

要件

分散する IT 環境でホストのセキュリティと可用性を効率的に管理

デジサートの SRE（Site Reliability Engineering）チームは、デジサートのグローバル IT インフラストラクチャの連続稼働率とパフォーマンスに責任を負っています。このレベルの可用性を確実に維持するために、SRE チームは、米国、ヨーロッパ、日本にある同社のデータセンターを支えている数千台の仮想マシン（VM）に格納された電子証明書を管理する必要があります。

「しかし、これらの VM のワークロードのアイデンティティとして使用される証明書が増加するにつれて、すべての証明書の管理はますます大変な作業になっていました」と、デジサートのエンジニアリング担当バイスプレジデントの Binh Nguyen は述べています。「証明書の管理は以前からずっと大変な作業でしたが、使用する証明書が増え続ける中、他の手を借りずに証明書に意識を向け続けることはほぼ不可能です」と、Nguyen は続けます。「1 つの証明書をプロビジョニングしてインストールするのに数時間かかることがありました。なぜなら、非常に多くのステップが必要だったからです。」



「DigiCert Trust Lifecycle Manager によって証明書の管理方法が一変しました。私たちの作業効率は大幅にアップするとともに、インフラの保護を大幅に強化できました。」

— Binh Nguyen、エンジニアリング担当 VP、デジサート

これまで、証明書登録は面倒で時間のかかる作業でした。証明書署名リクエスト（CSR）が承認されて証明書が発行された後、チームは証明書を手動でダウンロードしてターゲットホストにインストールする必要がありました。複数ステップのプロセスはターゲットに応じて異なっていました。その後、証明書をテストしなければなりませんでした。証明書ごとにステップを繰り返さなければならず、各ステップでヒューマンエラーのリスクが高まっていました」と、Nguyen は述べています。「私たちはこれらのプロセスを自動化する方法を必要としていました。インフラストラクチャの保護に PKI を使用している他の企業と同様、期限切れの証明書に起因する機能停止を免れているにすぎなかったからです」

ソリューション

DigiCert Trust Lifecycle Manager が VM の証明書ライフサイクル管理（CLM）を変革

Nguyen にとって、DigiCert Trust Lifecycle Manager の登場はタイムリーでした。Trust Lifecycle Manager により、数千台の VM とそれらがサポートするワークロードの保護に使用されるすべての証明書が可視化されました。そして、証明書ライフサイクル管理に伴う多様なプロセスを合理化する方法がもたらされました。さらに、Trust Lifecycle Manager には、証明書調達の迅速化と、証明書の期限切れや設定ミスに起因する機能停止の防止を目的とした豊富な自動化機能が提供されており、プロセス内で緊密に連携していました。

「DigiCert Trust Lifecycle Manager によって証明書の管理方法が一変しました。「私たちの作業効率は大幅にアップするとともに、インフラスの保護を大幅に強化できました」と、Nguyen は述べています。

プロファイルを使用した自動登録の簡素化

SRE チームがまず行う必要があったのは、証明書の最初の CSR からインストール、テストまでの自動登録を合理化することでした。DigiCert Trust Lifecycle Manager には、電子証明書の発行、インストール、管理のための事前定義済みルールを提供する「プロファイル」という構成テンプレートが用意されているため、複雑なプロセスが簡素化されました。Trust Lifecycle Manager には、ウェブサーバーへの自動登録を実行するプロファイルなど一般的なプロファイルが多数用意されているため、Nguyen のチームは、設定プロセスが特に簡単であると感じました「私たちはターゲットシステムを一元的にモニタリングする、ACME エージェント用プロファイルを設定できました。期限切れ間近の証明書の更新に必要なすべてのステップはエージェントによって実行されるようになり、私たちは介入せずに済むようになりました」と、Nguyen は述べています。

ユーザーはまた、PKI の専門知識を必要としない DigiCert Trust Lifecycle Manager のわかりやすいテンプレートを使用して、プロファイルを作成できるようになりました。Trust Lifecycle Manager により、Nguyen のチームは、証明書のタイプ、有効期間、信頼の階層構造などのプロパティが定義された事前構成済みテンプレートを使用してプロファイルを作成し、ユースケースに必要な構成を適用できるようになりました。

DigiCert Trust Lifecycle Manager により、証明書の有効期間の構成も可能になりました。Nguyen は次のように述べています。「このようなアクションを構成するために PKI の高度な専門知識は不要です。CSR からインストール、置換まで、すべてのステップは Trust Lifecycle Manager によって実行されるからです。これらのプロセスには、それまで数時間かかっていましたが、わずか数分で完了できるようになりました。Trust Lifecycle Manager によって、すべてが自動化されるからです。」

検知から更新までの CLM を自動化

DigiCert Trust Lifecycle Manager は、プロファイルに加えて、組み込みの自動化アーキテクチャを備えており、Nguyen のチームは証明書ライフサイクル管理（CLM）のあらゆるプロセスを自動化できるようになりました。Nguyen は、Trust Lifecycle Manager の自動検知機能により、チームによる証明書の管理方法がいかに変化したかを強調しています。「チームにとって大きな負担が解消されました。VM 上のすべての証明書の追跡について心配する必要がなくなったからです」と、Nguyen は述べています。「証明書が元々どこで発行されたかにかかわらず、Trust Lifecycle Manager は証明書を検知してインベントリに追加するだけでなく、所有者、有効期限、セキュリティポリシーへの準拠状況を通知してくれます。」

さらによいことに、DigiCert Trust Lifecycle Manager の自動化アーキテクチャにより、Nguyen のチームは、人の介入なしに特定のアクションをトリガーする自動化ワークフローを作成できるようになりました。たとえば、Nguyen のチームは設定ミスや脆弱性が含まれている証明書や未承認の CA によって発行された証明書を自動的に失効するワークフローを作成しました。ワークフローでは、該当する証明書が CertCentral または DigiCert ONE CA Manager の承認済み証明書に置換されます。どちらであるかは、置換元の証明書のタイプに応じて決まります。

「効率化し、セキュリティを強化するとともに、信頼性を高める — それに優る成果はありません」

サードパーティのネットワークデバイスやワークロードとのシームレスな統合

最後に、DigiCert Trust Lifecycle Manager により、ロードバランサーやウェブサーバーなど、会社の VM がサポートしている多様なワークロードとシームレスに統合されました。Trust Lifecycle Manager では、SRE チームにとって複雑化や問題の増加につながり得る追加のスクリプトや他のプロセスを使用せずに、センサーとエージェントを介して、これらのネットワークデバイス上の証明書を確実に管理できるようになりました。「よくわからない証明書のせいで Apache サーバーが誤ってダウンすることはないとわかって大いに安心しました」と、Nguyen は述べています。

Nguyen はまた、DigiCert Trust Lifecycle Manager での証明書の管理と自動化の簡単さについても高く評価しました。管理対象は、会社のウェブサーバーとロードバランサーがサポートする多くのアプリケーションやマイクロサービスの ID として使用されるすべての証明書です。「これらのピースはそれぞれ、他のピースと連携するために、認証用の証明書を必要としています。それを考慮すると、作業は極めて複雑なのです。しかし、Trust Lifecycle Manager を使用することで、私たちはその作業から解放されました」と、Nguyen は述べています。

Nguyen のチームは、クラウドインスタンスの証明書を管理するために、DigiCert Trust Lifecycle Manager の展開をすでに開始しています。DigiCert Trust Lifecycle Manager には、堅牢な CLM とマネージド PKI の機能に加えて、必要に応じて起動される ICA（中間認証機関）を動的に作成する機能もあります。「Trust Lifecycle Manager は、私たちが必要とする俊敏性をもたらします。組織が拡大し続ける中、当社のインフラストラクチャはセキュアに維持されています」と、Nguyen は述べています。「効率化し、セキュリティを強化するとともに、信頼性を高める — それに優る成果はありません」

今すぐ DigiCert® Trust Lifecycle Manager をお試しになりたい方は、こちらからご連絡ください。