CHAPTER 12

ポリシーの導入

この章では、ACE Web Application Firewall にポリシーを導入する方法について説明します。内容は次のとおりです。

導入の概要

コンソールで設定を変更し、これらの変更を保存すると、ACE Web Application Firewall Manager で使用中のポリシーに変更を反映することになります。変更は、使用中のポリシーが ACE Web Application Firewall Manager から導入されるまで Firewall で反映されません。

ポリシーを導入すると、ポリシーが ACE Web Application Firewall Manager から ACE Web Application Firewall Manager の管理ドメイン内のすべての ACE Web Application Firewall に送信されます。導入後は、ACE Web Application Firewall によってポリシーのルールと動作が適用されます。

開発設定または評価設定で、変更の効果をテストするためなどにポリシーを頻繁に導入したいことがよくあります。ただし、実稼動設定では、導入はポリシーがテストおよび検証された後にだけ行う必要があります。必要な場合は、導入プロセスを制御するために承認ベースの導入機能を有効にできます。

たとえば、ACE Web Application Firewall Manager のドメインに最近追加された Firewall にポリシーを個別に導入できます。ただし、一般的に、特定のドメイン内のすべての Firewall は同じポリシーを持つ必要があります。

導入プロセスは複数の手順で行われます。

1. ACE Web Application Firewall Manager がポリシーの基本的な確認を行い、設定エラーと他の問題を探します。
2. ACE Web Application Firewall Manager がポリシーをコンパイルし、実行のために ACE Web Application Firewall のネイティブ形式に変換します。
3. ACE Web Application Firewall Manager がタイムスタンプと ID コードをポリシーに追加し、アーカイブに保存します。
4. ACE Web Application Firewall Manager がポリシーを ACE Web Application Firewall に送信します。

5. ACE Web Application Firewall はポリシーを受け入れ、サービスを一時的に停止し、新しいポリシーを適用するようサービスを再設定し、サービスを再起動します。

導入の成功を検証する最後の手順として、[System Management] ページで I/O プロセスのステータスを確認することを推奨します。ポリシーに問題がある場合は、http-server プロセスまたは reactor プロセスが再起動されないことがあります。Firewall ステータス設定の I/O プロセスの表ですべてのプロセスが実行されていることを確認できます。

これらの手順が正常に完了したら、ACE Web Application Firewall は新しいポリシーを適用します。

ポリシーを導入できるユーザ

ポリシーを導入するには（または、承認ベースの導入が有効な場合に導入するポリシーを承認するには）、ユーザが適切な権限を持っている必要があります。ユーザは特に、次の条件を満たす必要があります。

- Administrator ユーザまたは Operations ロールを持つ Privileged ユーザ
- Shared サブポリシーと、導入するサブポリシーにアクセス可能

また、承認ベースの導入が有効な場合は、ポリシーまたはサブポリシー自体が導入のために承認されている必要があります。Administrator ユーザは常にポリシーを導入および承認できます。Operations ロール ユーザは、導入に関係するサブポリシーと Shared ポリシーにアクセスできる場合にポリシーを導入できます。導入のためにポリシーを承認するには、「任意のサブポリシー」へのアクセスが必要です。

承認ベースの導入の場合、Shared ポリシーにアクセスできないユーザはポリシー変更の承認を実際の導入を行う管理者に要求します。

ポリシーの導入

ポリシーを導入すると、現在使用中のポリシーの変更が ACE Web Application Firewall で反映されます。Administrator ユーザと Operations ロールを持つ Privileged ユーザは Web コンソールでポリシー変更を導入できます。

また、Administrator 承認ベースの導入を Web コンソールで有効にすることもできます。有効な場合は、特定のユーザだけがポリシーを承認または導入できます。承認ベースの導入を有効にした状態でポリシーを導入する手順は、これらの標準的な導入手順に似ています（ただし、手順がいくつか追加されます）。詳細については、「承認ベースの導入」（P.12-5）を参照してください。

承認ベースの導入がアクティブでない場合は、次の手順に従ってポリシーを導入します。

ステップ 1　`Administrator` ユーザまたは `Operations` ロールを持つ `Privileged` ユーザとして Web コンソールにログインしている状態で、アクティブなサブポリシーを導入するポリシーに設定します（ポリシーにサブポリシーが含まれる場合）。

ポリシーにサブポリシーが含まれる場合は、導入時にアクティブなサブポリシー内のアーティファクトだけが移動します。複数のサブポリシーから変更を導入する場合は、各サブポリシーを有効にし、サブポリシーから 1 つずつ導入する必要があります。

ステップ 2　ページ上部の [Deploy Policy] ボタンをクリックします。

リソースリロードが有効な場合は、[Step 1 of 4: URL Resource Refresh] ページが表示されます。このページでは、ポリシーが、URL の場所からロードされたすべてのリソース ファイル（証明書など）の最新バージョンを持っていることを確認できます。詳細については、「導入時の URL ベース リソースのリロード」（P.12-5）を参照してください。

リソースリロードが有効でない場合、ACE Web Application Firewall Manager は [Step 1 of 3: Review Changes] ページを表示します。このページには、現在のポリシーと、導入するポリシーとの違いがまとめられています。詳細については、「ポリシー変更を個別にロール バック」（P.12-4）を参照してください。

ステップ 3　[URL Resource Refresh] ページが表示されたら、[Reload Resources Now] ボタンをクリックし、変更された URL ベースのリソースをアップロードします。

ACE Web Application Firewall Manager は、導入するポリシーが使用するすべての URL ベースのリソースの新しいコピーを取得しようとします。この結果、[Review Changes] ページが表示されます。

（注）　URL ベースのリソースのリロードは、取り消すことができません。リソースの以前に保存されたバージョンに戻す必要がある場合は、[Reload Resources Now] ボタンをクリックする前にリソースの現在のバージョンのコピーを保存してください。

または、[Continue To Next Step] をクリックしてリソースのリロードを省略してください。

ステップ 4　[Continue to Next Step] ボタンをクリックして導入プロセスを続行します。

[Step 2 of 3: Basic Policy Review] ページに正常な導入を阻む条件が一覧表示されます。ページのリンクは、影響を受けたポリシー オブジェクトへのアクセスを提供するため、問題を修正するのに必要な変更を行うことができます。

新しいポリシーの導入を中止する場合は、[Exit To Policy Manager] ボタンをクリックします。

ステップ 5　表示されたコンパイルの警告やエラーを確認し、必要な場合は修正します。

ACE Web Application Firewall Manager は、導入されたポリシーの整合性を確保するために広範なコンパイル時ポリシー チェックを実行します。潜在的な各問題を解決したら、ACE Web Application Firewall Manager は [Basic Policy Review] ページから関連する警告を削除します。問題解決後に [Basic Policy Review] ページに戻るには、ブラウザの [Back] ボタンを使用します。または、[Deploy] ボタンをクリックして導入プロセスを再開します。

ステップ 6　[Basic Policy Review] ページで警告を解決したら、[Continue To Next Step] ボタンをクリックして導入プロセスを続行します。

[Compile and Deploy] ページが表示されます。ポリシーのコンパイル時に「Please wait」メッセージが数秒間表示されることがあります。コンパイルにより、ポリシーは ACE Web Application Firewall のネイティブ実行可能形式に変換されます。完了したら、ページには、タイムスタンプと ACE Web Application Firewall Manager により割り当てられた ID 番号を含む、コンパイルされたポリシーに関する情報が表示されます。

ステップ 7　[Policy Description] フィールドにこのポリシー バージョンの説明を入力します。

この説明は、コンソールでポリシーを記録するのに役に立ちます。これはポリシー履歴の [Description] カラムに表示されます。デフォルトでは、これは省略可能なフィールドです。ただし、ACE Web Application Firewall Manager の管理者は [Manager Settings] ページから必要な説明を作成できます。

ステップ 8　アドレスまたはホスト名の隣にあるボックスをオンにして、コンパイルされたポリシーを転送するアプライアンスを指定します。Firewall の out-of-date ステータスは、コンパイルされたポリシーが、現在導入されているポリシーと異なることを示します。

（注）　ポリシーをクラスタ内の一部のアプライアンスに導入することは可能ですが、すべてのアプライアンスに導入することはできません。確実な理由がない限り、この作業を行わないでください。これは、ACE Web Application Firewall の通常の導入方針ではありません。通常は、ポリシーを、該当するクラスタ内の ACE Web Application Firewall Manager により制御された Firewall のすべてに導入するか、あるいはまったく導入しません。

ステップ 9　[Deploy To Selected Firewalls] ボタンをクリックしてポリシーの導入を完了します。

ACE Web Application Firewall Manager は、選択されたアプライアンスにポリシーを送信します。選択されたアプライアンスで、ポリシーがネットワーク トラフィックに適用されます。

[Compile and Deploy] 画面が再び表示され、導入の結果が表示されます。以前に選択された各 Firewall に対して、[Status] カラムには [Up to Date] が表示され、[Deployed Policy Description] カラムには新しいポリシーの説明が表示され、[Deployed Policy Timestamp&ID] カラムにはポリシー ID と新しい導入のタイムスタンプが表示されます。

この時点で新しいポリシーは ACE Web Application Firewall で有効になります。

ポリシー変更を個別にロール バック

ポリシー バージョンによりカプセル化された変更は、いつでも個別にロール バックしたり、受け入れたりできます。次の手順に従ってください。

ステップ 1　コンソールで `Administrator` ユーザまたは `Operations` ロールを持つ `Privileged` ユーザとして、操作メニューで [Policy Manager] リンクをクリックします。

ステップ 2　Policy Manager の下部にあるポリシー履歴セクションで、確認するポリシー バージョンの隣にある [Roll Back] ボタンをクリックします。

[Roll Back To] 説明ページが表示されます。イタリック体の置き換え可能なテキストの代わりに、ポリシー履歴の指定されたポリシーのエントリの [Date Saved] カラムと [Description] カラムに表示されるテキストが表示されます。

ステップ 3　[Accept addition] チェックボックスまたは [Accept deletion] チェックボックスを必要に応じてクリックし、ポリシーへの個々の変更を受け入れるか、または拒否します。

[Accept addition] チェックボックスのチェックマークは、指定されたアクションの承認を示します。チェックマークを取り除くと、ラベルで指定されたアクションが拒否されます。

ステップ 4　[Save Changes] をクリックして変更を確認します。

[Policy Manager] ページが表示され、使用中のポリシーに、確認した内容が反映されます。この時点で、変更されたポリシーの管理承認を要求できます。また、適切な権限がある場合は、ポリシーを自分で導入することもできます。

導入時の URL ベース リソースのリロード

Firewall ポリシーには、URL で指定された場所からポリシーにロードされたリソース ファイルを含めることができます。一般的に、ACE Web Application Firewall は実行時にリモート リソースを取得しようとしません。代わりに、ACE Web Application Firewall はポリシーにリソースを格納します。ただし、ポリシーを導入するたびに、リソースが最初にポリシーにロードされたときに指定された URL にあるバージョンでリソースのコピーを更新できます。次の手順に従ってください。

ステップ 1　[Policy Manager] ページの [Review] セクションで [URL Resource Refresh] ボタンをクリックします。

[URL Resource Refresh] ページが表示されます。このページには、使用中のポリシーが使用する各ネットワークベースのリソースが、リソース、リソースのリロードの最終試行時刻、およびその試行の結果を提供する URL とともに一覧表示されます。

ステップ 2　[Reload Resources Now] ボタンをクリックします。

（注）　この操作は取り消すことができません。リソースの以前に保存されたバージョンに戻す必要がある場合は、[Reload Resources Now] ボタンをクリックする前にリソースの現在のバージョンを保存してください。

ACE Web Application Firewall Manager は、リストの各リソースの新しいコピーをダウンロードしようとします。時間が経つと、各試行のステータスを反映するよう [Last Reloaded] カラムと [Result] カラムが更新されます。

ステップ 3　[URL Resource Refresh] ページの下部にある [Continue To Next Step] ボタンをクリックします。

ACE Web Application Firewall Manager は URL で指定されたリソースを取得します。

承認ベースの導入

承認ベース（つまり、2 段階）の導入では、最初にポリシー開発者が、ポリシーに行われた変更の承認を要求します。管理者は変更を確認し、承認または拒否します。承認された変更は管理者が導入できます。

この機能が有効な場合、Privileged ユーザは通常どおりポリシーを編集できますが、Policy Manager の [Deploy] セクションはユーザが使用中のポリシー変更の管理承認を要求する [Submit] セクションに置き換えられます。

サブポリシー内から承認を要求する場合は、そのサブポリシー内からの変更だけが変更要求で示されます。複数のサブポリシーを使用しているユーザは、各サブポリシー内で承認を要求する必要があります。

承認ベースの導入に適用される手順は次のとおりです。

- 承認ベースの導入の有効化
- 承認ステータスと要求の確認
- ポリシー変更の承認要求
- ポリシー変更の承認または拒否
- 承認されたポリシーの導入

承認ベースの導入の有効化

承認ベースの導入はデフォルトで無効になっています。有効にするには、次の手順に従います。

ステップ 1　ACE Web Application Firewall Manager Web コンソールで `Administrator` ユーザとして操作メニューで [System Management] リンクをクリックします。

ステップ 2　ACE Web Application Firewall Manager という見出しの右側にある [Manager Settings] というラベルのリンクをクリックします。

ステップ 3　一般設定領域で、[Workflow] 設定オプションを見つけ、[Use approval-based deployment] オプションを有効にします。

ステップ 4　[Save Changes] ボタンをクリックします。

[System Management] ページが表示されます。

ステップ 5　ACE Web Application Firewall Manager Web コンソールからログアウトします。

ステップ 6　**Operations** ロールの非管理ユーザとして ACE Web Application Firewall Manager Web コンソールにログインし、承認ベースの導入が有効であることを確認します。

ステップ 7　操作メニューで [Policy Manager] リンクをクリックします。

設定の変更に成功した場合は、[Deploy] セクションの代わりに [Submit] セクションが表示されます。

承認ステータスと要求の確認

承認ベースの導入が有効な場合は、この項で説明したように Manager Dashboard により、サブポリシー導入のステータスに関する追加情報が提供されます。

承認されたポリシー ステータス

Dashboard の上部にある [Approved Policy Status] セクションには、管理ユーザの承認を待っているポリシーの変更が一覧表示されます。

[Approved Policy Status] セクションは、承認ベースの導入が有効な場合にだけ表示されます。Dashboard のこのセクションを参照できるのは Privileged ユーザ（ポリシーを編集または導入できるユーザ）だけです。

このセクションには、ACE Web Application Firewall Manager にログインしているユーザ アカウントで利用可能なサブポリシーだけが表示されます。ユーザが「任意のサブポリシー」アクセス権を持っている場合は、このセクションにすべてのサブポリシーのステータスが同時に表示されます。その他の場合は、アクティブなサブポリシーのステータスだけが表示されます。別のサブポリシーの承認ステータスを確認するには、そのサブポリシーをアクティブなサブポリシーにする必要があります。

ACE Web Application Firewall Manager にログインしているアカウントが参照できる各サブポリシーに対して、このセクションには次の情報が一覧表示されます。

サブポリシーが最後に承認された日時

- 最後に承認されたバージョンが導入されているかどうか
- 新しいサブポリシーまたは変更されたサブポリシーの承認要求の日時
- 要求を最初に行った Web コンソール ユーザのユーザ名

ポリシー確認権限を持っている場合は、待機状態の各要求の隣に [Review] ボタンが表示されます。

アクティブなサブポリシーの承認要求ステータス

Dashboard の [Approval Request Status For] セクションには、アクティブなサブポリシーの変更に対する未処理の承認要求が一覧表示されます。

Dashboard のこのセクションを参照できるのは Privileged ユーザ（ポリシーを編集または導入できるユーザ）だけです。このセクションには、アクティブなサブポリシーのステータスだけが表示されます。別のサブポリシーのステータスを確認するには、そのサブポリシーをアクティブなサブポリシーにします。

このセクションには、各承認要求のステータスが一覧表示されます。ステータスの値は、次のいずれかになります。

- [Approved]：ポリシーのレビュー担当者が、サブポリシーの導入を承認しました。「任意のサブポリシー」アクセス権を持つ **Operations** ロールのユーザは、このポリシーを ACE Web Application Firewall に送信して適用できます。
- [Approval Requested]：ポリシーのレビュー担当者が、新しいサブポリシーまたは変更されたサブポリシーの導入を承認することをユーザが要求しました。サブポリシーを承認する前に、レビュー担当者はこのポリシーまたはサブポリシーと、ACE Web Application Firewall が現在適用しているポリシーまたはサブポリシーの違いを確認します。レビュー担当者は、最終的に ACE Web Application Firewall に導入されたポリシーが意図したように動作するよう各変更を個別に承認または拒否できます。
- [Rejected]：ポリシーのレビュー担当者が、新しいサブポリシーまたは変更されたサブポリシーを導入する権限を拒否しました。ポリシーの受け入れ拒否部分を変更した後で、再び承認を要求できます。

ポリシー変更の承認要求

承認ベースの導入が有効な場合、新しいサブポリシーまたは変更されたサブポリシーは変更が Administrator ユーザまたは Operations ロールを持つ Pivileged ユーザによって承認されるまで導入できません。

新しいサブポリシーまたは変更されたサブポリシーの承認を要求するには、次の手順に従います。

ステップ 1　承認される変更があるサブポリシーをコンソールでアクティブにし、ページ上部にある [Request Approval] ボタンをクリックします。

リソースリロードが有効な場合は、[Step 1 of 4: URL Resource Refresh] ページが表示されます。ポリシーを導入する前に、[Resource Refresh] ページを使用して、ポリシーが、リモートでホストされているすべてのリソース（URL から取得されたスキーマや証明書など）の最新バージョンを持っていることを確認できます。詳細については、「導入時の URL ベース リソースのリロード」（P.12-5）を参照してください。

リソースリロードが有効でない場合、ACE Web Application Firewall Manager は [Step 1 of 3: Review Changes] ページを表示します。このページには、現在のポリシーと、導入するポリシーとの違いがまとめられています。[Review Changes] ページの詳細については、「ポリシー変更を個別にロール バック」（P.12-4）を参照してください。

ステップ 2　[URL Resource Refresh] ページが表示されたら、[Reload Resources Now] ボタンをクリックして URL ベースのリソースをロードします。

ACE Web Application Firewall Manager は、導入するポリシーが使用するすべての URL ベースのリソースの新しいコピーを取得しようとします。完了したら、[Review Changes] ページが表示されます。

（注）　URL ベースのリソースのリロードは、取り消すことができません。リソースの以前に保存されたバージョンに戻す必要がある場合は、[Reload Resources Now] ボタンをクリックする前にリソースの現在のバージョンのバックアップ コピーをアーカイブしてください。

ステップ 3　[Continue to Next Step] ボタンをクリックします。

[Step 2 of 3: Basic Policy Review] ページが表示されます。このページには、変更されたポリシーによって引き起こされた可能性がある問題に関する警告が表示されます。

ステップ 4　警告を確認します。警告の原因となる問題を解決するか、現時点では警告を無視するかを選択できます。警告を解決するためにポリシーを変更する必要がある場合は、[Exit to Policy Manager] をクリックして承認プロセスを終了し、ポリシーを編集します。

完了したら、[Continue to Next Step] ボタンをクリックします。

ステップ 5　[Step 3 of 3: Submit Request] ページの [Description] フィールドに短い説明またはコメントを入力します。

説明は通常、管理者や他の開発者への送信で変更を特徴付けるために使用されます。説明は、policy-viewing 権限を持つすべてのユーザが参照できます。

ステップ 6　また、次のように要求の通知電子メールを送信することもできます。

a.　[Send e-mail notification of this approval request] ボタンをクリックします。

b.　[To e-mail address] フィールドに受信者のアドレスを入力します。

c.　[From e-mail address] フィールドに送信者の電子メール アドレスを入力します。通常、これは要求者のアドレスになります。

ステップ 7　[Submit Request] ボタンをクリックします。

承認要求が [Dashboard] ページに表示されます。Administrator ユーザまたは Operations ロールを持つ Privileged ユーザの場合、要求は Dashboard 上部の [Approved Policy Status] ペインに表示されます。Shared サブポリシーにアクセスできるユーザの場合、要求は [Approval Request Status for Shared] セクションに表示されます。

ポリシー変更の承認または拒否

Administrator ユーザまたは Operations ロールを持つ Privileged ユーザは、ポリシーの変更を確認および承認できます。変更されたポリシーを ACE Web Application Firewall に導入する前に変更要求が承認されている必要があります。

Manager Dashboard の [Approved Policy Status] セクションに、各サブポリシーの最後に提示された変更と最後に承認された変更が表示されます。各行には、サブポリシーの承認最終日、導入ステータス、および承認を待っている最後の変更が表示されます。すべての承認要求の完全なリストについては、[Policy Manager] ページの下部にあるポリシー履歴を参照してください。

ポリシー導入の権限がある場合は、[Review] ボタンが、承認を待っている最後の要求の隣に表示されます。[Review] ボタンをクリックすると、ACE Web Application Firewall Manager はそのサブポリシーに影響を与える待機状態のすべての変更を一度に承認または拒否できる 1 つのサブポリシーとして扱いします。変更を個別に承認または拒否する場合は、「ポリシー変更を個別にロール バック」（P.12-4）を参照してください。

アクティブなサブポリシーへのすべての変更を受け入れたり、拒否したりするには、次の手順に従います。

ステップ 1　コンソールで Administrator ユーザまたは Operations ロールを持つ Privileged ユーザとして、Dashboard の [Approved Policy Status] セクションの、承認または拒否されるポリシーについて説明している行の右側にある [Review] ボタンをクリックします。

ステップ 2　[Review Approval Request] ページで次のようにポリシーを承認または拒否します。

- すべての変更を承認するには、[Approve Changes] ボタンをクリックします。
- すべての変更を拒否するには、[Reject Changes] ボタンをクリックします。
- 承認要求が待機状態のまま変更を行わずに終了するには、[Cancel Review] ボタンをクリックします。

[Dashboard] ページが表示されます。[Approved Policy Status] 領域と [Approval Request Status] 領域に選択の結果が反映されます。

ポリシー認証プロセスでは、管理者がポリシー全体を受け入れたり、拒否したりできます。承認後は、Policy Manager でロール バック プロセスを使用して特定の承認に影響を与えることができます。詳細については、「ポリシー変更を個別にロール バック」（P.12-4）を参照してください。

承認されたポリシーの導入

ポリシー承認要求が送信され、承認されると、Administrator ユーザまたは Operations ロールを持った Privileged ユーザは要求でカプセル化された変更を導入できます。

サブポリシーがポリシーに存在する場合は、導入時に、アクティブなサブポリシー（Shared を含む）内のアーティファクトだけが移動します。複数のサブポリシーから変更を導入する場合は、各サブポリシーを有効にし、サブポリシーから 1 つずつ導入する必要があります。

承認ベースの導入が有効な場合にポリシーを導入するには、次の手順に従います。

ステップ 1　Web コンソールで、[Deploy Approved Policy] ボタンをクリックしてポリシーをコンパイルし、適用のために ACE Web Application Firewall に送信します。

[Step 2 of 3: Basic Policy Review] ページに承認ステータスが一覧表示されます。ポリシー送信に対する類似のページが表示されますが、送信後にポリシーが変更された場合は [Basic Policy Review] ページが再び表示されることがあります。

ステップ 2　ACE Web Application Firewall Manager ですべての警告を確認し、解決します。

ポリシーはすでに承認されているため、変更できません。ポリシーをそのまま導入したくない場合は、[Exit to Policy Manager] ボタンをクリックして、導入を中止します。この場合は、Policy Manager でポリシーを編集し、承認のために再送信できます。

ステップ 3　承認されたポリシーに満足な場合は、[Continue To Next Step] ボタンをクリックして導入プロセスを続行します。

[Compile and Deploy] 画面に「Please wait」というメッセージが表示され、ポリシーがコンパイルされ、ACE Web Application Firewall のネイティブ実行可能形式に変換されます。完了したら、「This policy is compiled and can now be deployed」というメッセージと、このポリシーをロードおよび適用する ACE Web Application Firewall アプライアンスを指定できるコントロールが表示されます。

ステップ 4　このポリシーを受け取る各 Firewall アプライアンスの隣にあるチェックボックスをクリックします。

（注）　ポリシーをクラスタ内の一部の Firewall に導入することは可能ですが、すべてには導入できません。確実な理由がない限り、この作業を行わないでください。通常は、ポリシーをクラスタ内のすべての Firewall に導入するか、あるいはまったく導入しません。

ステップ 5　[Deploy To Selected Firewalls] ボタンをクリックしてポリシーの導入を完了します。

ACE Web Application Firewall Manager は選択された Firewall にポリシーを送信します。Firewall はポリシーを受け取り、ポリシーを適用するよう再設定されます。[Compile and Deploy] 画面に導入の結果が表示されます。[Timestamp&ID] カラムにポリシー ID と新しい導入のタイムスタンプが反映されます。

新しいポリシーはこの時点で有効になります。