ADFS/IdS のトラブルシューティングと一般的な問題

目次

概要

Cisco 識別サービス（ID）とブラウザによる Active Directory フェデレーション サービス（AD FS）間のセキュリティ アサーション マークアップ言語（SAML）相互対話は（SSO）ログイン フローの単一サインのコアです。 この資料はそれらを解決する推奨 処置と共に Cisco IDS および AD FS の設定にデバッグ関する問題で、助けます。

Cisco IdS 導入モデル

製品	導入
UCCX	共存
PCCE	CUIC（Cisco Unified Intelligence Center）と LD（ライブ データ）の共存
UCCE	2k 導入用の CUIC と LD の共存。 4k および 12k 導入用のスタンドアロン。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco Unified Contact Center Express（UCCX）リリース 11.5、Cisco Unified Contact Center Enterprise リリース 11.5、Packaged Contact Center Enterprise（PCCE）リリース 11.5（該当する場合）
- Microsoft Active Directory：Windows サーバ上にインストールされた AD
- IdP（識別プロバイダ） - Active Directory フェデレーション サービス（AD FS）バージョン 2.0/3.0

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

トラスト 関係が Cisco IDS と AD FS の間で（詳細については、UCCX および UCCE のためによくあるここに参照して下さい）確立された後、管理者は Cisco IDS と AD FS 間の設定がうまく働くようにするために識別サービス管理の Settings ページのテスト SSO 設定を実行すると期待されます。 テストが失敗した場合、問題を解決するために与えられるこのガイドで適切なアプリケーションおよび推奨事項を使用して下さい。

デバッグで便利である場合もあるログおよびアプリケーション

アプリケーション/ログ	詳細	ツールをどこ
Cisco IDS ログ	Cisco IDS ロガーは Cisco IDS で発生したエラーを記録 します。	Cisco IDS ロ RTMT を使用 さい、ガイト 以下の事項に す。 ログを、
Fedlet ログ	Fedlet ログはあらゆる SAML エラーについてのより多くの詳細を説明します Cisco IDS で起こす	Fedlet ログを Fedlet ログの

Cisco IDS API メトリック	API メトリックがに検知 し、Cisco IDS 返す API がかもしれないおよび要求の数をことができます Cisco IDS によって処理される工ラー検証するのに使用する	fedlet ログは API メトリッ 以下の事項に す これは別個の に注意して下 はこの資料の AD FS マシン よび**サービス** Control Pane ビューア**およ** Windows 20 リティ\管理_ 見るためにウ 見つけるか検 これらはため 推奨される S 1. バイオ オリン 2. SAML 3. SAML
AD FS のイベント ビューアー	イベントを表示する割り当てユーザはシステムをログオンします。 SAML 応答を送信 するを SAML 要求/処理している間ここに記録される AD FS のエラー。	
SAML ビューア	SAML ビューアは Cisco IDS from/to 返される応答および SAML 要求の検知で助けます。 このブラウザ アプリケーションは要求および応答 SAML の分析に非常に役立ちます。	

デバッグ オプションの流れ図

SSO 認証のためのさまざまなステップはそのステップの失敗の発生時に各ステップのイメージと共におよびデバッグ成果物で説明されます。

この表は方法の詳細をブラウザの SSO の各ステップで失敗を識別する説明したものです。 どのようにできなさいか異なるツール彼らはデバッグで同様に規定 されます助け。

ステップ	ブラウザの失敗を識別する方法	ツール/ログ
Cisco IDS による AuthCode 要求処理	失敗の場合には、ブラウザは SAML エンドポイントか AD FS にリダイレクトされません、クライアントID かリダイレクト URL は無効であることを示す JSON エラーは Cisco IDS によって示されています。	Cisco IDS ログは authcode 要求を示します。 Cisco IDS API メトリック-処理さ
Cisco IDS による SAML 要求 開始	障害の間に、ブラウザは AD FS にリダイレクトされないし、Error ページ/メッセージは Cisco IDS によって表示されます。	Cisco IDS ログは例外があるか、示します。 Cisco IDS API メトリック-処理さ
AD FS による SAML 要求処理	この要求を処理するどの障害でも Login ページの代りに AD FS サーバによって表示される Error ページという結果に終ります。	AD FS のイベント ビューアーは要ます。 SAML ブラウザ プラグイン- SAM。
AD FS による SAML 応答の送信	有効な資格情報が入った後応答を返すどの障害でも AD FS サーバによって表示される Error ページという結果に終ります。	AD FS のイベント ビューアー-要す。
Cisco IDS によって処理する SAML 応答	Cisco IDS はエラー原因および素早いチェック ページとの 500 エラーを示します。	AD FS のイベント ビューアー- A SAML 応答を返す場合エラーを示 SAML ブラウザ プラグイン- SAM って間違っているものを識別する Cisco IDS ログ-エラー/例外が処理 Cisco IDS API メトリック-処理さ

Cisco IDS による Authcode 要求処理

Cisco IDS に関する限りでは、SSO ログオンの開始点は SSO によって有効に される アプリケーションからのオーソリゼーション・コードのための要求です。 API 要求の検証はそれが登録されていたクライアントからの要求であるかどうか確認するために行われます。 Cisco IDS の SAML エンドポイントにリダイレクトされるブラウザの正常な検証結果。 要求の検証のどの失敗でも送返されるエラー page/JSON（ JavaScript オブジェクト 表示法 ）という結果に Cisco IDS に終ります。

このプロセスの間に見つけられるよくある エラー

1. できていないクライアント登録

問題の要約	Login 要求はブラウザの 401 エラーと失敗します。
エラー メッセージ	**ブラウザ:** このメッセージとの 401 エラー: {" error ": 「invalid_client」、「error_description」: 「無 **Cisco IDS ログ:** 2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] com.cisco.ccbu.ids IdSConfigImpl. fb308a80050b2021f974f48a72ef9518a5e7ca69 2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoi com.cisco.ccbu.ids IdSOAuthEndPoint.java:45 - AUTH org.apache.oltu.oauth2.common.exception.OAuthProblemException: invalid_client ClientId org.apache.oltu.oauth2.common.exception.OAuthProblemException.error(OAuthProblemExcepti com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequestParams(IdSAuthor com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequiredParameters(IdSA org.apache.oltu.oauth2.as.request.OAuthRequest.validate(OAuthRequest.java:63)
考えられる原因	Cisco IDS とのクライアント登録は完了しませんでした。
推奨処置	Cisco IDS マネジメント コンソールにナビゲートし、クライアントが登録に成功される 。 そうでなかったら、それから SSO を続行する前にクライアントを登録して下さい。

2. IP アドレス/交替ホスト名を使用するユーザアクセス アプリケーション

問題の要約	Login 要求はブラウザの 401 エラーと失敗します。
エラー メッセージ	**ブラウザ:** このメッセージとの 401 エラー: {" error ": 「invalid_redirectUri」、「error_description」 IP アドレス/交替ホスト名を使用するユーザアクセス アプリケーション。
考えられる原因	SSO モードでは、アプリケーションが IP を使用してアクセスされれば、それははたらき IDS で登録されているホスト名によってアクセスする必要があります。 この問題はユー 代替ホスト名にアクセスした場合起こる場合があります。
推奨処置	Cisco IDS マネジメント コンソールにナビゲートし、同じがアプリケーションにアクセ トが正しいリダイレクト URLand に登録されているかどうか確認して下さい。

Cisco IDS による SAML 要求 開始

Cisco IDS の SAML エンドポイントは SSO によって基づくログオンで SAML の開始点フローしますです。 Cisco IDS と AD FS 間の相互対話の開始はこのステップで誘発されます。 ここの前提条件は IdP 対応するメタデータがこのステップのための Cisco IDS に成功するためにアップロードする必要があると同時に Cisco IDS がに接続するために AD FS を知るはずであることです。

このプロセスの間に見つけられるよくある エラー

1. Cisco IDS に追加されない AD FS メタデータ

問題の要約	Login 要求はブラウザの 503 エラーと失敗します。
エラー メッセージ	**ブラウザ:** このメッセージとの 503 エラー: {" error ": 「service_unavailable」、「error_description 「SAML メタデータ」は初期化されません}
考えられる原因	Idp メタデータは Cisco IDS で利用できません。 Cisco IDS と AD FS 間の信頼確立は完 しませんでした。 Cisco IDS マネジメント コンソールにナビゲートし、ID が**設定されなかった**状態にある どうか参照して下さい。
推奨処置	IdP メタデータがアップロードされるかどうか確認して下さい。 そうでなかったら、AD FS からダウンロードされる IdP メタデータをアップロードして さい。 詳細については[ここに]参照して下さい。

AD FS による SAML 要求処理

SAML 要求処理は SSO フローの AD FS の第一歩です。 Cisco IDS によって送信 される SAML 要求はこのステップの AD FS によって読まれ、検証され、解読されます。 この要求の正常な処理は 2 つのシナリオという結果に終ります:

1. それがブラウザの新しいログインである場合、AD FS は Login 形式を示します。それが既存のブラウザー セッションからの認証済みユーザの既に relogin である場合、AD FS は SAML 応答背部を直接送信 するように試みます。

   注: このステップのための主要な前提条件は AD FS のため応答パーティ信頼を設定してもらうことです。

このプロセスの間に見つけられるよくある エラー

1. Cisco 最新の ID の SAML 証明書を持っていない AD FS。

問題の要約	その代り Login ページを示さない AD FS は Error ページを示します。
エラー メッセージ	**ブラウザ** AD FS はこれへの Error ページ 類似したを示します: サイトにアクセスする問題がありました。 サイトに再度参照することを試みて下さい。 問題が持続する場合、このサイトの管理者に連絡し、問題点を明らかにするために参照 参照番号: 1ee602be-382c-4c49-af7a-5b70f3a7bd8e **AD FS イベント ビューアー** フェデレーション サービスは SAML 認証要求を処理している間エラーに出会いました。 **追加データ** `: Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificationFailedException: myuccx.cisco.com Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.Proc requestMessage Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.Create createErrorMessageRequest CreateErrorMessageRequest Microsoft.IdentityServer.Protocols.Saml.Contract.SamlContractUtility.CreateSamlMessage`
考えられる原因	依存当事者信頼は確立されませんまたは Cisco IDS 証明書は変更しましたが、同じは AD れません。
推奨処置	最新の Cisco IDS 証明書との AD FS および Cisco IDS 間の信頼を確立して下さい。 Cisco IDS 証明書が期限切れではないことを確認して下さい。 Cisco 識別のステータス を保守するのを表示できます。 その場合、Settings ページの証明書を再生して下さい。 詳細についてはメタデータを確立する方法で ADFS 及び Cisco IDS を渡って見ます、[こ]

AD FS によって送信 する SAML 応答

ADFS はブラウザによって Cisco IDS に戻ってユーザの認証に成功された後 SAML 応答を返します。 ADFS は成功か失敗を示すステータス スコードの SAML 応答背部を送信できます。 IF 形式認証は AD FS で有効に なりませんそれからこれが障害応答を示す。

このプロセスの間に見つけられるよくある エラー

1. 形式認証は AD FS で有効に なりません

問題の要約	ブラウザは NTLM ログオンを示し、次に正常にリダイレクトしないで Cisco IDS に失敗します。
失敗のステップ	SAML 応答の送信
エラー メッセージ	**ブラウザ:** ブラウザは NTLM ログオンを示しますが、正常なログインの後で、多くのリダイレクト敗します。
考えられる原因	Cisco IDS は AD FS で形式ベースの認証だけ、形式認証有効に なりませんサポートしま。
推奨処置	Enable 形式認証にどのようにで参照しなさいか詳細については: ADFS 2.0 形式認証設定 ADFS 3.0 形式認証設定

Cisco IDS によって処理する SAML 応答

このステージでは、Cisco IDS は AD FS から SAML 応答があります。 この応答は成功か失敗を示すステータス スコードが含まれている可能性があります。 AD FS からのエラー応答は Error ページに起因し、同じはデバッグされなければなりません。

正常な SAML 応答の間に、要求の処理はこれらの理由により失敗する場合があります:

- IdP 不正確な（AD FS）メタデータ。
- AD FS から期待された発信クレームを取得する失敗。
- Cisco IDS および AD FS クロックは同期化されません。

このプロセスの間に見つけられるよくある エラー

1. Cisco IDS の AD FS 証明書は最新ではないです。

問題の要約	Login 要求は invalidSignature としてエラー· コードのブラウザの 500 エラーと失敗しま
失敗のステップ	SAML 応答処理

エラー メッセージ	**ブラウザ:**
	ブラウザのこのメッセージとの 500 エラー:
	Error Code: invalidSignature
	メッセージ： 署名証明書は定義されるものがエンティティ メタデータで一致する。
	AD FS イベント ビューアー:
	エラーなし
	Cisco IDS ログ:
	`2016-04-13 12:42:15.896 IST(+0530) DEFAULT [IdSEndPoints-0] com.cisco.ccbu.ids IdSEndP`
	`- com.sun.identity.saml2.common.SAML2Exception :`
	`com.sun.identity.saml2.xmlsig.FMSigProvider.verify(FMSigProvider.java:331)`
	`com.sun.identity.saml2.protocol.impl.StatusResponseImpl.isSignatureValid(StatusResponse`
	`com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:985)`
	`com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196)`

考えられる原因	Cisco IDS で利用可能であるものをと IdP 証明書が異なっているので停止する SAML 応

推奨処置	最新の AD FS メタデータをからダウンロードして下さい: https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml そして識別サービス Managament ユーザインターフェイスによって Cisco IDS にそれを して下さい。 詳細については、設定 Cisco IDS および AD FS を参照して下さい

2. Cisco IDS および AD FS クロックは同期化されません。

問題の要約	Login 要求はステータス スコードのブラウザの 500 エラーと失敗します: urn:oasis:names:tc:SAML:2.0:status:Success
失敗のステップ	SAML 応答処理

エラー メッセージ	**ブラウザ:**
	このメッセージとの 500 エラー:
	IdP Configuration エラー: 停止する SAML 処理
	ステータス スコードの IdP からの SAML assertion failed: urn:oasis:names:tc:SAML:2.0:
	定を確認し、もう一度試して下さい。
	Cisco IDS ログ
	`2016-08-24 18:46:56.780 IST(+0530) [IdSEndPoints-SAML-22]  com.cisco.ccbu.ids IdSSAMLAs`
	`com.sun.identity.saml2.common.SAML2Exception - SAML : SubjectConfirmationData`
	`com.sun.identity.saml2.common.SAML2Utils.isBearerSubjectConfirmation(SAML2Utils.java:76`
	`com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:609)`
	`com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050)`
	`com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAM`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncSe`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncS`
	`com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269)`
	`java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)`
	`java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615)`
	`java.lang.Thread.run(Thread.java:745)2016-08-24 18:24:20.510 IST(+0530) [pool-4-thread-`
	SAML ビューア:
	NotBefore および NotOnOrAfter フィールドを探して下さい
	<Conditions NotBefore="2016-08-28T14:45:03.325Z" NotOnOrAfter="2016-08-28T15:45

考えられる原因	Cisco IDS および IdP システムの時間は同期化からあります。
推奨処置	Cisco IDS および AD FS システムの時間を同期して下さい。 AD FS システムおよび Cis を使用して同期される時間であることを推奨します。

3. AD FS の間違った署名アルゴリズム (SHA256 vs SHA1)

問題の要約	Login 要求はステータス code:urn:oasis:names:tc:SAML:2.0:status:Responder のブラウ します AD FS イベント View Log のエラー メッセージ–間違ったシグニチャ Algorithm(SHA256
失敗のステップ	SAML 応答処理

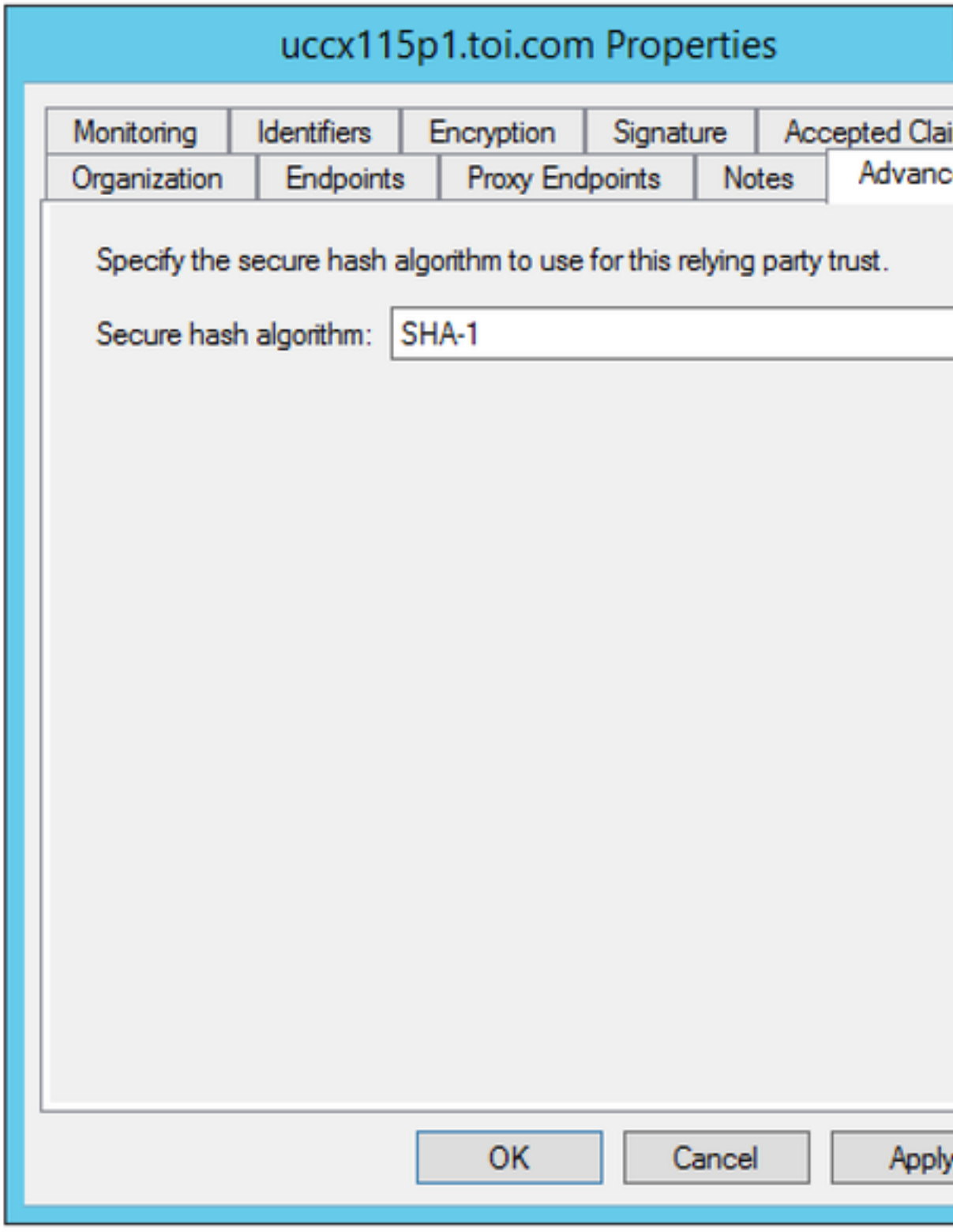
エラー メッセージ	**ブラウザ**
	このメッセージとの 500 エラー:
	IdP Configuration エラー: 停止する SAML 処理
	ステータス スコードの IdP からの SAML assertion failed: urn:oasis:names:tc:SAML:2.0:
	設定を確認し、もう一度試して下さい。
	AD FS イベント ビューアー:
	SAML 要求は期待された署名アルゴリズムと署名しません。 SAML 要求は署名アルゴリ
	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 と署名します。
	期待された署名アルゴリズムは http://www.w3.org/2000/09/xmldsig#rsa-sha1 です
	Cisco IDS ログ:
	`com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - com.sun.identity.saml2.common.SAML2E`
	`com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425)`
	`com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050)`

```
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAM
```

考えられる原因 AD FS は SHA-256 を使用するために設定されます。

推奨処置 署名および暗号化のために SHA-1 を使用するために AD FS をアップデートして下さい。

1. AD FS システムへの RDP。
2. 開いた AD FS コンソール。
3. **依存パーティ信頼を**選択し、『Properties』 をクリック して下さい
4. [Advanced] タブを選択します。
5. ドロップダウン リストから SHA-1 を選択して下さい。

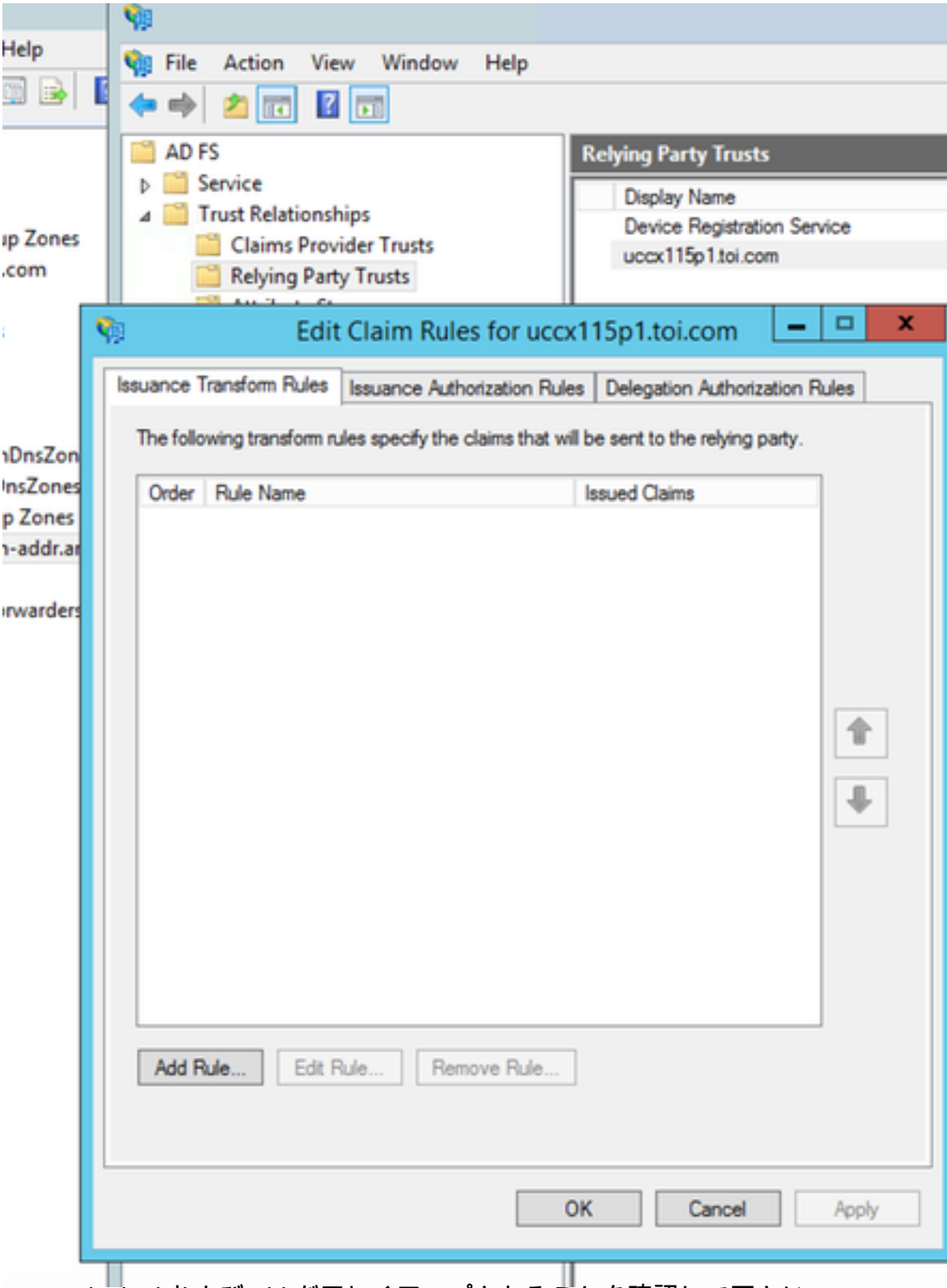


4. 正しく設定されない発信クレーム ルール

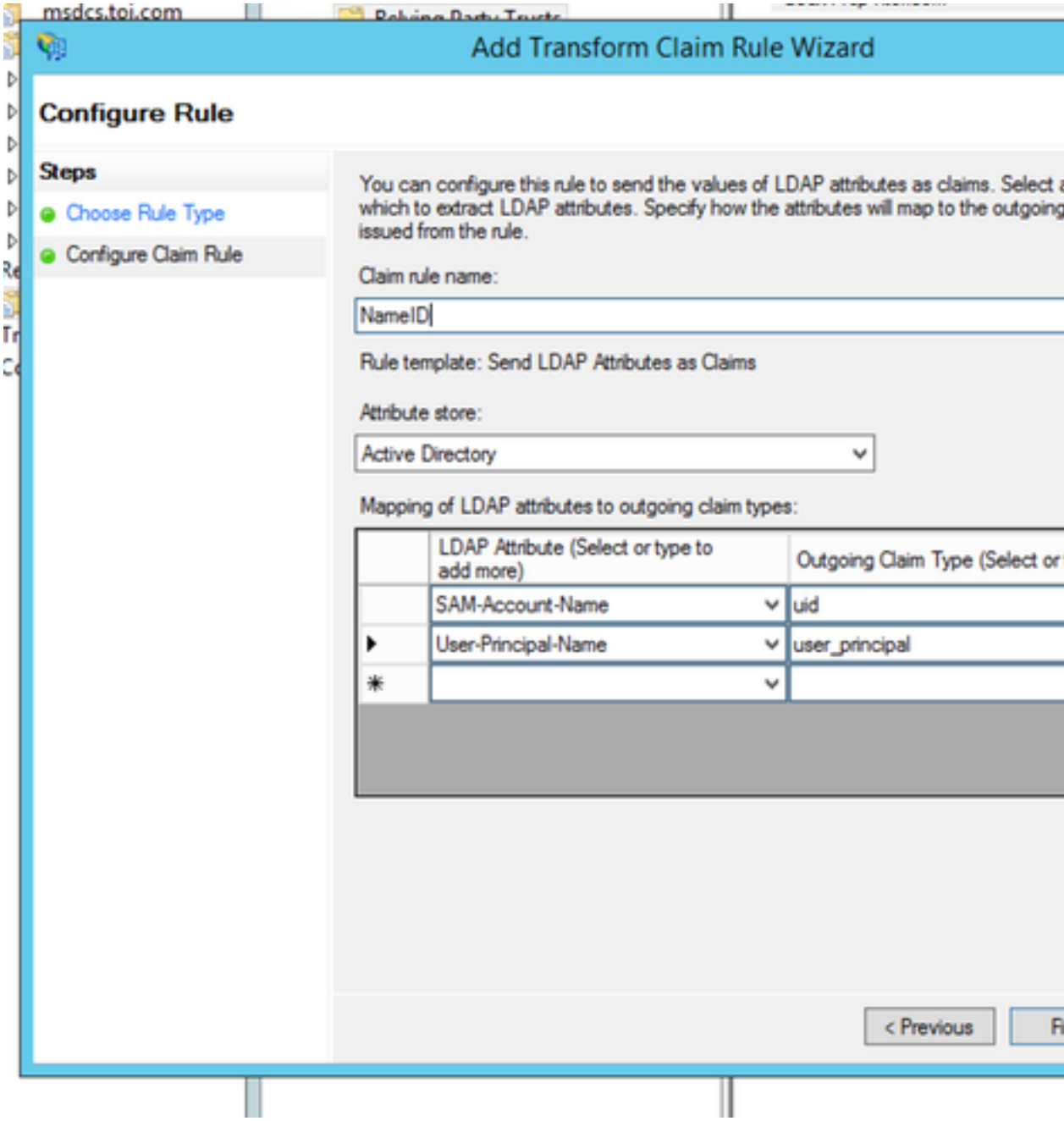
問題の要約	Login 要求はメッセージとのブラウザのエラーによって「SAML 応答からの検索ユーザ識 と失敗します。/Could SAML 応答からのない検索ユーザ プリンシパル」。 発信クレームで設定 されない uid および/または user_principal。
失敗のステップ	SAML 応答処理

エラー メッセージ	**ブラウザ:**
	このメッセージとの 500 エラー:
	IdP Configuration エラー: 停止する SAML 処理。
	SAML 応答からの検索ユーザ識別はできませんでした。/Could SAML 応答からのない検
	。
	AD FS イベント ビューアー:
	エラーなし
	Cisco IDS ログ:
	`com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - com.sun.identity.saml.common.SAMLExc`
	`retreive ID`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncServ`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncSer`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncS`

考えられる原因	必須発信クレームはクレーム ルールで（uid および user_principal）正しく設定されませ NameID クレーム ルールをまたは設定しないか、uid か user_principal 正しく設定されま NameID ルールが設定されなくてかまたは user_principal 正しくマップされなければ、こ プロパティであるので user_principal 取得されない Cisco IDS は示します。 uid が正しくマップされない場合、Cisco IDS は uid が取得されないことを示します。 AD FS クレーム ルールの下で、（か。ガイドする）「uid」マップする属性が定義され レーション ガイドおよび「user_principal のために」であることを確認して下さい。 1. AD FS システムへの RDP。 2. 依存パーティ信頼のためのクレーム ルールを編集して下さい。
推奨処置	



3. user_principal および uid が正しくマップされることを確認して下さい



5. 発信クレーム ルールは連合させた AD FS で正しく設定されません

問題の要約	Login 要求はメッセージとのブラウザのエラーによって「SAML 応答からの検索ユーザ識 った 500 と失敗します。 またはできませんでした SAML 応答からの検索ユーザ プリン AD FS が連合させた AD FS である時。
失敗のステップ	SAML 応答処理

エラー メッセージ	**ブラウザ**
	このメッセージとの 500 エラー:
	IdP Configuration エラー: 停止する SAML 処理
	SAML 応答からの検索ユーザ識別はできませんでした。/SAML 応答からの検索ユーザ フ
	できませんでした。
	AD FS イベント ビューアー:
	エラーなし
	Cisco IDS ログ:
	`com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - com.sun.identity.saml.common.SAMLExc`
	`SAML retreive ID`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncServ`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncSer`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncS`

考えられる原因 連合させた AD FS で抜ける可能性があるより多くの設定が必要となりましたあります。

推奨処置 連合させた AD の AD FS 設定が設定 Cisco IDS の**連合させた AD FS** および AD FS の**マ設定のための**セクションによってされるかどうか確認して下さい

6. 正しく設定されないカスタム クレーム ルール

問題の要約 Login 要求はメッセージとのブラウザのエラーによって「SAML 応答からの検索ユーザ識と失敗します。/Could SAML 応答からのない検索ユーザ プリンシパル」。
発信クレームで設定 されない uid および/または user_principal。

失敗のステップ SAML 応答処理

エラー メッセージ
ブラウザ
このメッセージとの 500 エラー:
ステータス スコードの IdP からの SAML assertion failed: 壷: オアシス: 名前: tc: **SAML:2.0:status:Requester/urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy**. Id
一度試して下さい。

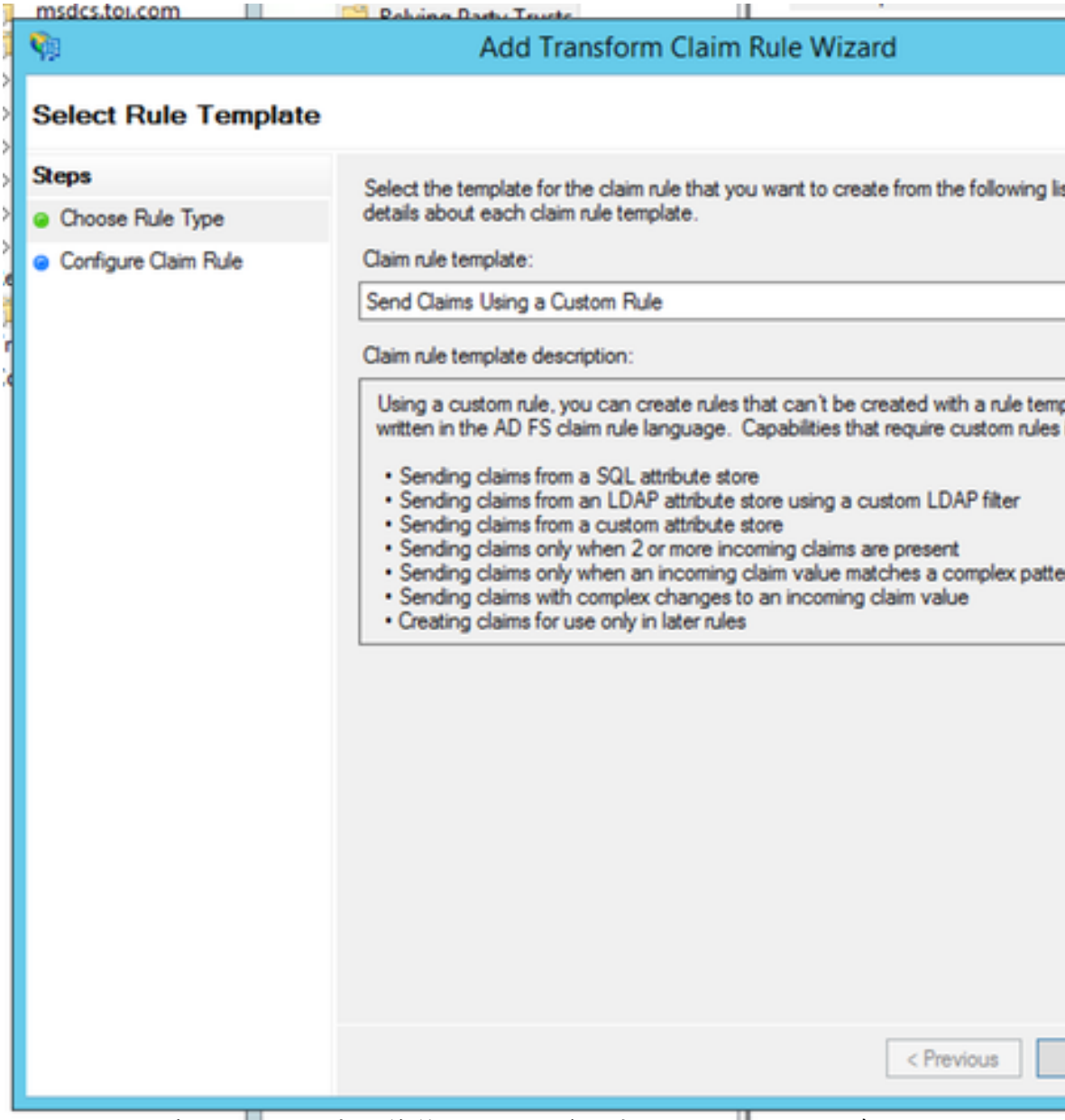
AD FS イベント ビューアー:
SAML 認証要求に満足することができなかった NameID ポリシーがありました。
要請人: myids.cisco.com
ネーム識別形式: urn:oasis:names:tc:SAML:2.0:nameid-format:transient
SPNameQualifier: myids.cisco.com
例外の詳細:
MSIS1000: SAML 要求は発行済みトークンによって満たされなかった NameIDPolicy が
求された NameIDPolicy: AllowCreate: 本当形式: urn:oasis:names:tc:SAML:2.0:nameid-fo
SPNameQualifier: myids.cisco.com。 NameID 実際のプロパティ: null を探します。
失敗されるこの要求。
ユーザのアクション
設定を設定するのに必須ネーム識別を出す AD FS 2.0 管理スナップインを使用して下さ
Cisco IDS ログ:

```
2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints-SAML-82] INFO com.cisco.ccbu.ids SAML2
: 1.: <samlp: Status> <samlp:  Value="urn:oasis:names:tc:SAML:2.0:status:Requester"> <s
Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy"> </samlp: StatusCode> </
</samlp: AuthnRequest  Status>: n/a 2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints-SA
com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:299 - com.sun.identity.saml2.common.SAML2Ex
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425)
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050)
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038
```

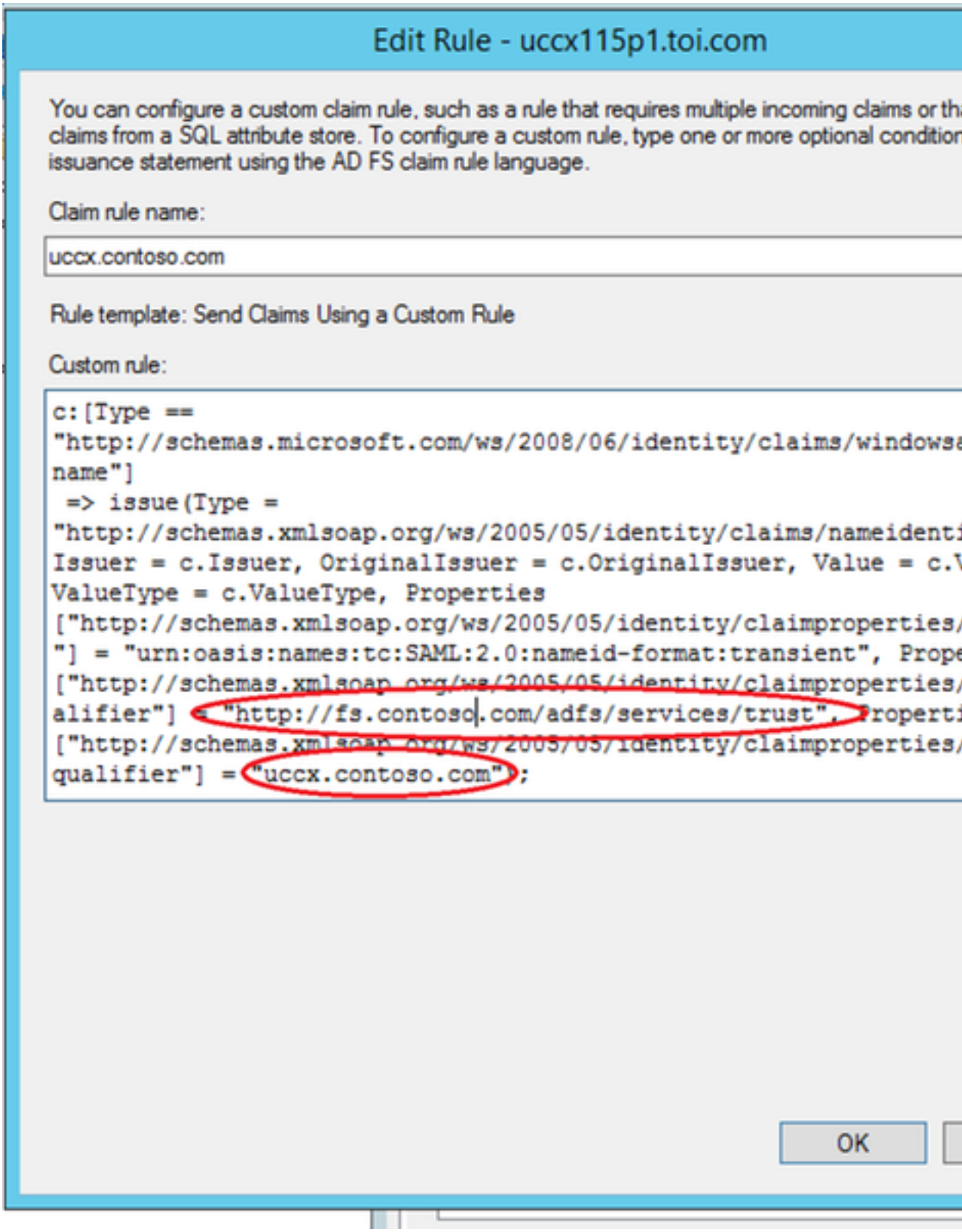
考えられる原因 カスタム クレーム ルールは正しく設定されません。
AD FS クレーム ルールの下で、（か。ガイドする）「uid」マップする属性が定義され
ション ガイドおよび「user_principal のために」であることを確認して下さい。

1. AD FS システムへの RDP。
2. カスタム クレーム ルールのためのクレーム ルールを編集して下さい。

推奨処置



3. AD FS および Cisco IDS 完全修飾ドメイン名が与えられることを確認して下さい。



7. AD FS への余りにも多くの要求。

問題の要約	Login 要求はステータス code:urn:oasis:names:tc:SAML:2.0:status:Responder のブラウ します AD FS イベント View Log のエラー メッセージは余りにも多くの要求が AD FS へある
失敗のステップ	SAML 応答処理
エラー メッセージ	**ブラウザ** このメッセージとの 500 エラー: IdP Configuration エラー: 停止する SAML 処理 ステータス スコードの IdP からの SAML assertion failed: urn:oasis:names:tc:SAML:2.0: 設定を確認し、もう一度試して下さい。

AD FS イベント ビューアー:
Microsoft.IdentityServer.Web.InvalidRequestException:
MSIS7042: **同じクライアント ブラウザ セッションはの '6' 要求を持続しますしました '16' 秒。 詳細に関しては管理者に連絡して下さい。**
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionC
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse
(MSISSignInResponse 応答)

```
XML: <Event xmlns= " http://schemas.microsoft.com/win/2004/08/events/event"> <System>
2.0" Guid="{20E25DDB-09E5-404B-8A56-EDAE2F12EE81}"/> <EventID>364</EventID> <Version>0<
<Level>2</Level> <Task>0</Task> <Opcode>0</Opcode> <Keywords>0x8000000000000001</Keywor
04-19T12:14:58.474662600Z"/> <EventRecordID>29385</EventRecordID> <Correlation Activity
4DD5-B3B6-0565AC17BFFE}"/> <Execution ProcessID="2264" ThreadID="392"/> <Channel>AD FS
<Computer>myadfs.cisco.com</Computer> <Security UserID="S-1-5-21-1680627477-1295527365-
</System> <UserData> <Event xmlns:auto-ns2=" http://schemas.microsoft.com/win/2004/08/e
http://schemas.microsoft.com/ActiveDirectoryFederationServices/2.0/Events"> <EventData>
>Microsoft.IdentityServer.Web.InvalidRequestException <TimeCreated: MSIS7042:    '16'
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCookie(
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse MSISSig
</EventData> </Event> </UserData> </Event>
```

Cisco IDS ログ

```
2016-04-15 16:19:01.220 EDT(-0400) DEFAULT  [IdSEndPoints-1] com.cisco.ccbu.ids IdSEndP
com.sun.identity.saml2.common.SAML2Exception :
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425)
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050)
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAM
```

考えられる原因 同じブラウザー セッションから AD FS に来る余りにも多くの要求があります。
これは本番で一般的に起こるはずではないです。 しかしこれに出会えば、できます:

推奨処置
1. AD FS Windows イベント ビューアーをチェックして下さい。
2. 依存パーティ信頼 設定を再確認して下さい。 詳細については、設定 Cisco IDS お
   下さい
3. Relogin。

8. AD FS はアサーションおよびメッセージに両方署名するために設定されません。

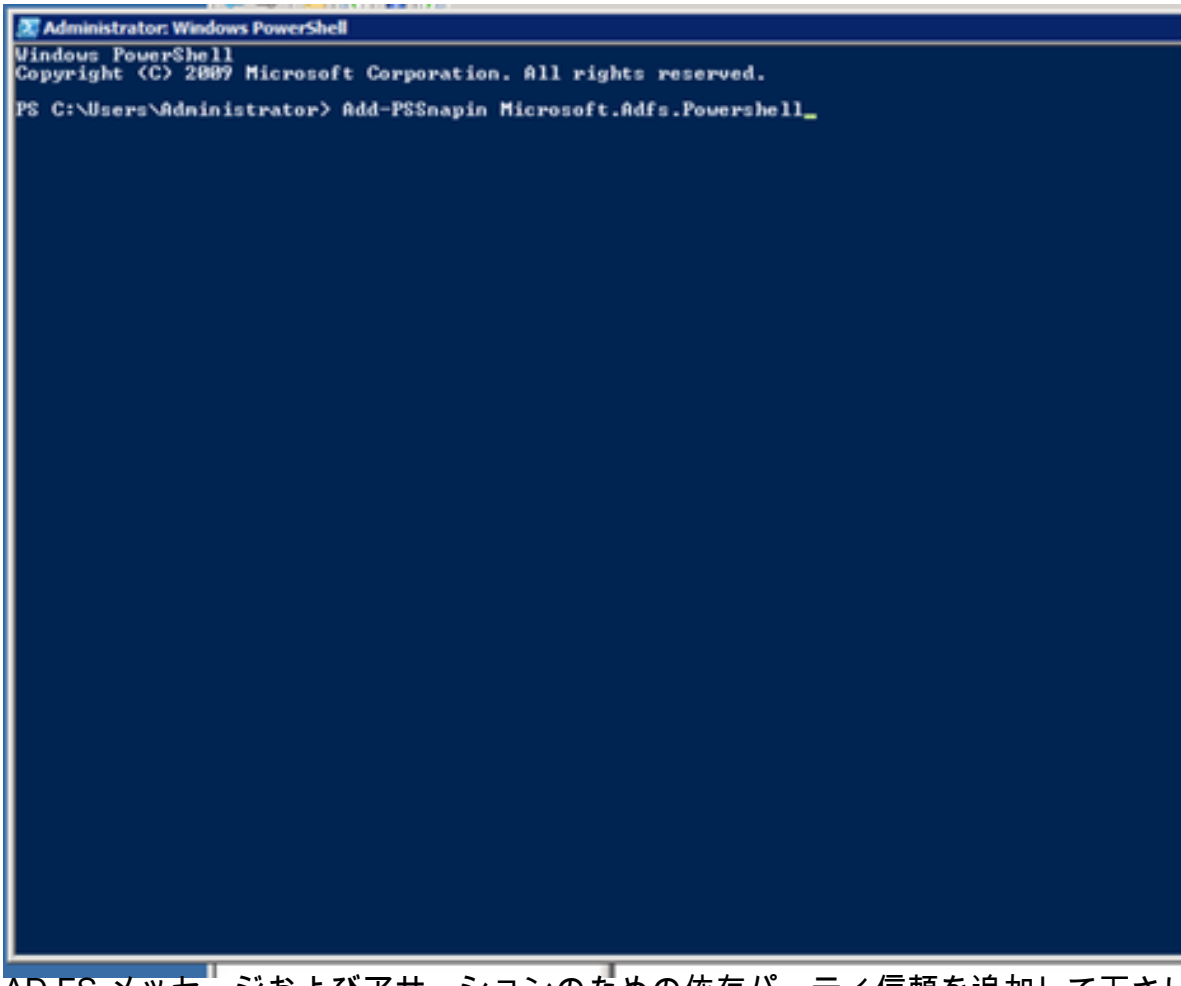
問題の要約 Login 要求はエラー· コードのブラウザの 500 エラーと失敗します: invalidSignature
失敗のステップ SAML 応答処理
ブラウザ
このメッセージとの 500 エラー:
Error Code: invalidSignature
メッセージ： ArtifactResponse の無効なシグニチャ。
エラー メッセージ **Cisco IDS ログ:**

```
2016-08-24 10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] INFO saml2error.jsp saml2err
invalidSignature; message: ArtifactResponse  2016-08-24 10:53:10.494 IST(+0530) [IdSEnd
com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - com.sun.identity.saml2.common.SAML2Ex
com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:994)
com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196)
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2028
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAM
```

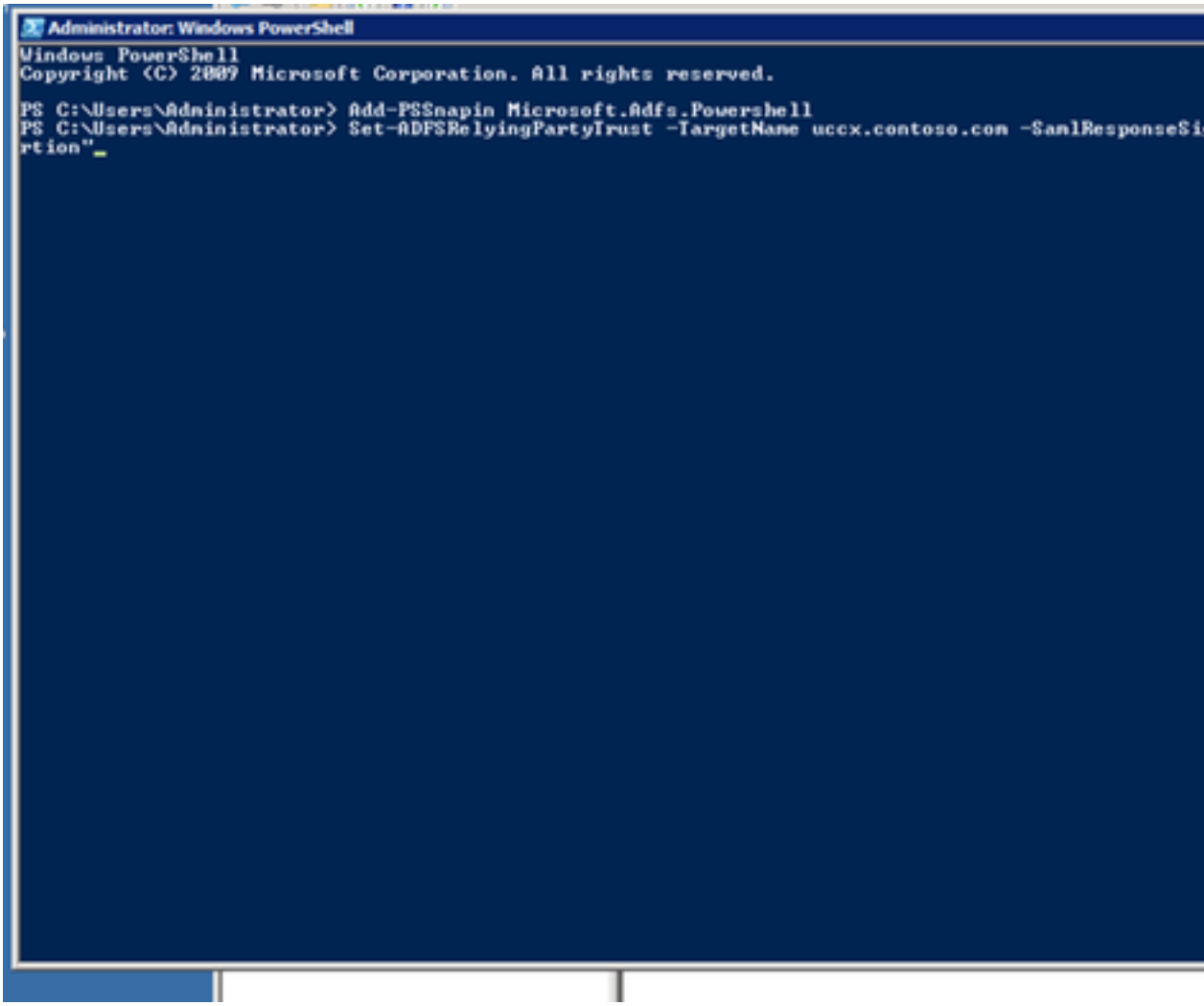
考えられる原因 AD FS はアサーションおよびメッセージに両方署名するために設定されません。

推奨処置
1. AD FS powershell コマンドを実行して下さい: **セットADFSRelyingPartyTrust - Tar
   ティ信頼 Identifier> - SamlResponseSignature 「MessageAndAssertion」**
2. AD システムへの RDP。
3. **Powershell を**開いて下さい。

4. 現在のセッションへの Add ウィンドウ PowerShell スナップ ins。 コマンドレット
追加の一部分として既にインストールされているので ADFS 3.0 を使用している場
とならないかもしれません。



5. AD FS メッセージおよびアサーションのための依存パーティ信頼を追加して下さい



関連情報

これは技術情報に説明がある識別プロバイダの設定と関連しています:

- https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX.html
- テクニカル サポートとドキュメント – Cisco Systems