

ADFS/IdS トラブルシューティングおよびよくある問題

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[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](#)

[デバッグ オプションの流れ図](#)

[Cisco IDS による Authcode 要求処理](#)

[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](#)
- [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](#)

[Cisco IDS による SAML 要求 開始](#)

[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](#)

[AD FS による SAML 要求処理](#)

[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 認証を持っていない AD FS。](#)

[AD FS によって送信 する SAML 応答](#)

[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](#)

[Cisco IDS によって処理する SAML 応答](#)

[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 認証は最新ではありません。](#)
- [2. Cisco IDS および AD FS クロックは同期化されません。](#)
- [3. AD FS の間違っ た署名アルゴリズム \(SHA256 vs SHA1 \)](#)
- [4. 正しく設定されない発信クレーム ルール](#)
- [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](#)
- [6. 正しく設定されないカスタム クレーム ルール](#)
- [7. AD FS への余りにも多くの要求。](#)
- [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。](#)

[関連情報](#)

概要

Cisco 識別 サービス (ID) とブラウザによるアクティブ ディレクトリ 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 のコンフィギュレーションにデバッグ関する問題で、助けます。

Cisco IDS 配置モデル

[製品 (Product)] 導入

UCCX	共存する
PCCE	CUIC (Cisco Unified Intelligence Center) および LD (ライブ データ) の共存 2k 配備のための CUIC および LD の共存。
UCCE	4k および 12k 配備のためにスタンドアロン。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Contact Center Express (UCCX) リリース 11.5 か Cisco Unified Contact Center Enterprise リリース 11.5 または適当 Packaged Contact Center Enterprise (PCCE) リリース 11.5。
- Microsoft Active Directory - Windows サーバでインストールされる AD
- IdP (識別プロバイダ) - アクティブ ディレクトリ 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。

このドキュメントの情報は、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、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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 セットアップ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

Cisco IDS ログ Cisco IDS ログガーは Cisco IDS で発生したエラーを記録します。

ツールをどこ
Cisco IDS ログ
さい。RTM
る方法の情報
[して下さい](#)
以下の事項に
Cisco 識別サ
Cisco 識別サ

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
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エラー検証するのに使用する
AD FS のイベント ビューア	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。

Fedlet ログを
。Fedlet ログの
る同じです。
fedlet ログは
API メトリッ
さい。
以下の事項に
Cisco 識別サ
これは別個の
れます。以
saml_metrics
はこの資料の
AD FS マシ
>Applications
>AdDFS 2.0
Control Pane
2008、起動
ス>管理ツ
Windows 20
テムおよびセ
起動させて下
見るためにウ
ビューアをと
これらはため
る使用できる
です
1. [バイオ](#)
[を使用](#)
[ラグイ](#)
2. [SAML](#)
3. [SAML C](#)

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 カリダイレクト 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ログイン ページの代わりに AD FS サーバによって表示する Error ペ	AD FS のイベント ビューアは要す。

ージという結果に終わります。

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する Error ページという結果に終わります。

AD FS のイベント ビューア-要求

Cisco IDS によっ
て処理する SAML
応答

Cisco IDS はエラーの理由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- AD I
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済みの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 に終わります。

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。

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)
```

**エラー メッセ
ージ**

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」
リダイレクト Uri」 }

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
アプリケーションは Cisco 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
この問題はユーザが Cisco IDS に登録されていない代替ホスト名にアクセスした場合起
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
用されているクライアン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

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。Cisco IDS と AD FS 間の相互対話の開始はこのステップで引き起こされます。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 間の信頼確立は完了していませんでした。 Cisco IDS マネジメントコンソールにナビゲートし、ID が Not Configured の状態にあるか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下さい。 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わります:

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 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 認証を持っていない AD FS。

問題の要約	その代りログイン 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

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.ProcessRequestMessage Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.CreateCreateErrorMessageRequest CreateErrorMessageRequest Microsoft.IdentityServer.Protocols.Saml.Contract.SamlContractUtility.CreateSamlMessage
```

考えられる原因

依存パーティ信頼は確立されませんまたは Cisco IDS 認証は変更しましたが、同じは AD FS ではありません。

最新の Cisco IDS 認証との AD FS および Cisco IDS 間の信頼を確立して下さい。

推奨処置

Cisco IDS 認証が期限切れではないことを確認して下さい。Cisco 識別 サービス 管理のロードを表示できます。その場合、Settings ページの認証を再生して下さい。

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、[こちら](#)

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の 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失敗します。

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

。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:

推奨処置

[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 認証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 エラーと失敗します
失敗のステップ SAML 応答処理

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:

エラー メッセージ
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 IdSEndPoints-0
- com.sun.identity.saml2.common.SAML2Exception :
com.sun.identity.saml2.xmlsig.FMSigProvider.verify(FMSigProvider.java:331)
com.sun.identity.saml2.protocol.impl.StatusResponseImpl.isSignatureValid(StatusResponseImpl.java:196)
com.sun.identity.saml2.profile.SPACSUtills.getResponseFromPost(SPACSUtills.java:985)
com.sun.identity.saml2.profile.SPACSUtills.getResponse(SPACSUtills.java:196)
```

考えられる原因 Cisco IDS で利用可能であるものと IdP 認証が異なっているので失敗される SAML 応答。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>

推奨処置 そして識別 サービス Management ユーザインターフェイスによって Cisco IDS にそれをダウンロードして下さい。

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

ブラウザ:

このメッセージとの 500 エラー:

IdP 設定 エラー: 失敗される 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:status:Success
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 IdSSAMLA
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.SPACSUtills.processResponse(SPACSUtills.java:1050)
com.sun.identity.saml2.profile.SPACSUtills.processResponseForFedlet(SPACSUtills.java:2038)
com.cisco.ccbu.ids.auth.api.IdSSAMLAAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLA
com.cisco.ccbu.ids.auth.api.IdSSAMLAAsyncServlet.processSamlPostResponse(IdSSAMLA
com.cisco.ccbu.ids.auth.api.IdSSAMLAAsyncServlet.processIdSEndPointRequest(IdSSAMLA
com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269)
```

エラー メッセージ
エラーなし

```
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="2016-08-28T15:45:03.325Z">

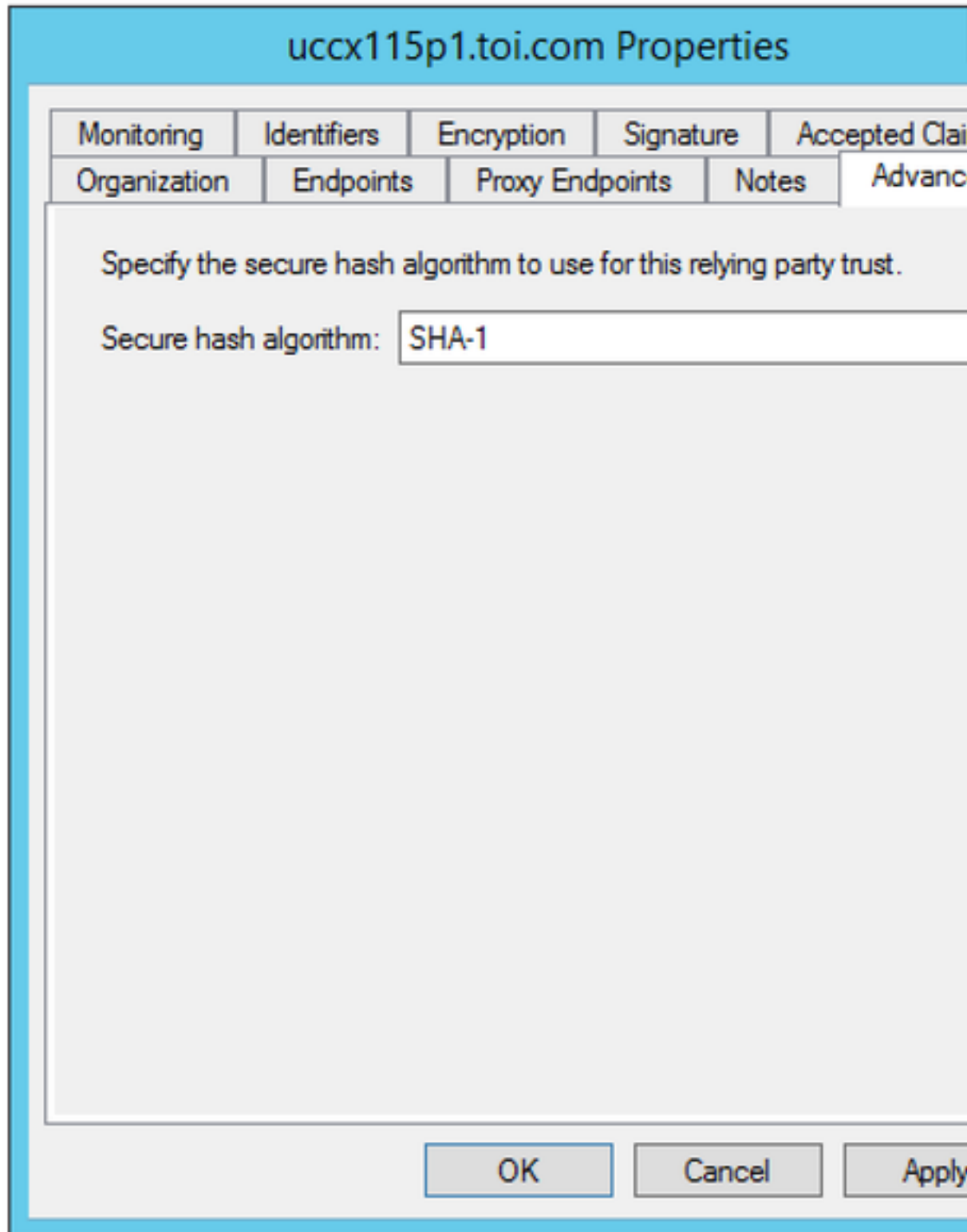
考えられる原因 Cisco IDS および IdP システムの時間は同期化からあります。

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 Cisco IDS 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 のブラウザ します
失敗のステップ	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) SAML 応答処理 ブラウザ このメッセージとの 500 エラー: IdP 設定 エラー: 失敗される 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。
エラー メッセージ	AD FS イベント ビューア: 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。 期待されたシグニチャ アルゴリズムは rsa-sha1 です Cisco IDS ログ: <pre>com.cisco.ccbu.ids.IdSSAMLAyncServlet.java:298 - SAML com.sun.identity.saml2.common. com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) com.sun.identity.saml2.profile.SPACUtils.processResponse(SPACUtils.java:1050) com.sun.identity.saml2.profile.SPACUtils.processResponseForFedlet(SPACUtils.java:2038) com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getMapFromSAMLResponse(IdSSAM</pre>
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。 署名および暗号化のために SHA-1 を使用するのために 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。

推奨処置



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」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」。
- 失敗のステップ** 発信クレームで設定 されない uid および/または user_principal。
SAML 応答処理
ブラウザ:
- エラー メッセージ** このメッセージとの 500 エラー:
IdP 設定 エラー: 失敗される SAML 処理。
SAML 応答からの検索ユーザ 識別子はできませんでした。/Could SAML 応答からのないル。

AD FS イベント ビューア:

エラーなし

Cisco IDS ログ:

```
com.cisco.ccbu.ids.IdSSAMLAyncServlet.java:294 - SAML com.sun.identity.saml.common.S
retrive ID
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.validateSAMLAttributes(IdSSAMLAyncServ
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncSer
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdEndPointRequest(IdSSAMLAyncS
```

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 が user_principal 正しく設定されま

考えられる原因 NameID ルールが設定されなくてかまたは user_principal 正しくマッピング されなければ

探す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 が正しくマッピング されない場合、Cisco IDS は uid が取得されないことを示します

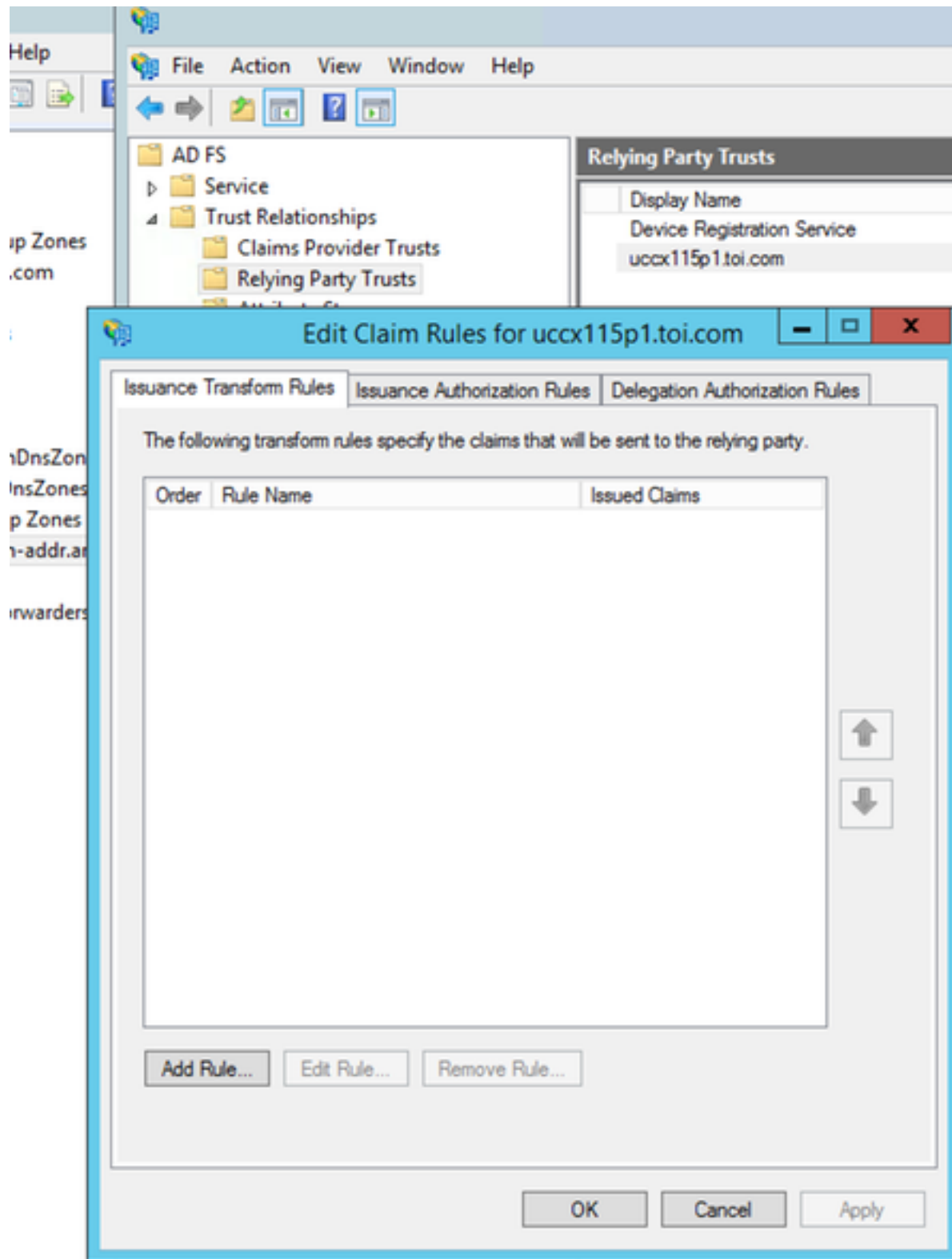
AD FS クレーム ルールの下で、(か。ガイドする) 「uid」マッピング する属性が定義

ギューレーション 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。

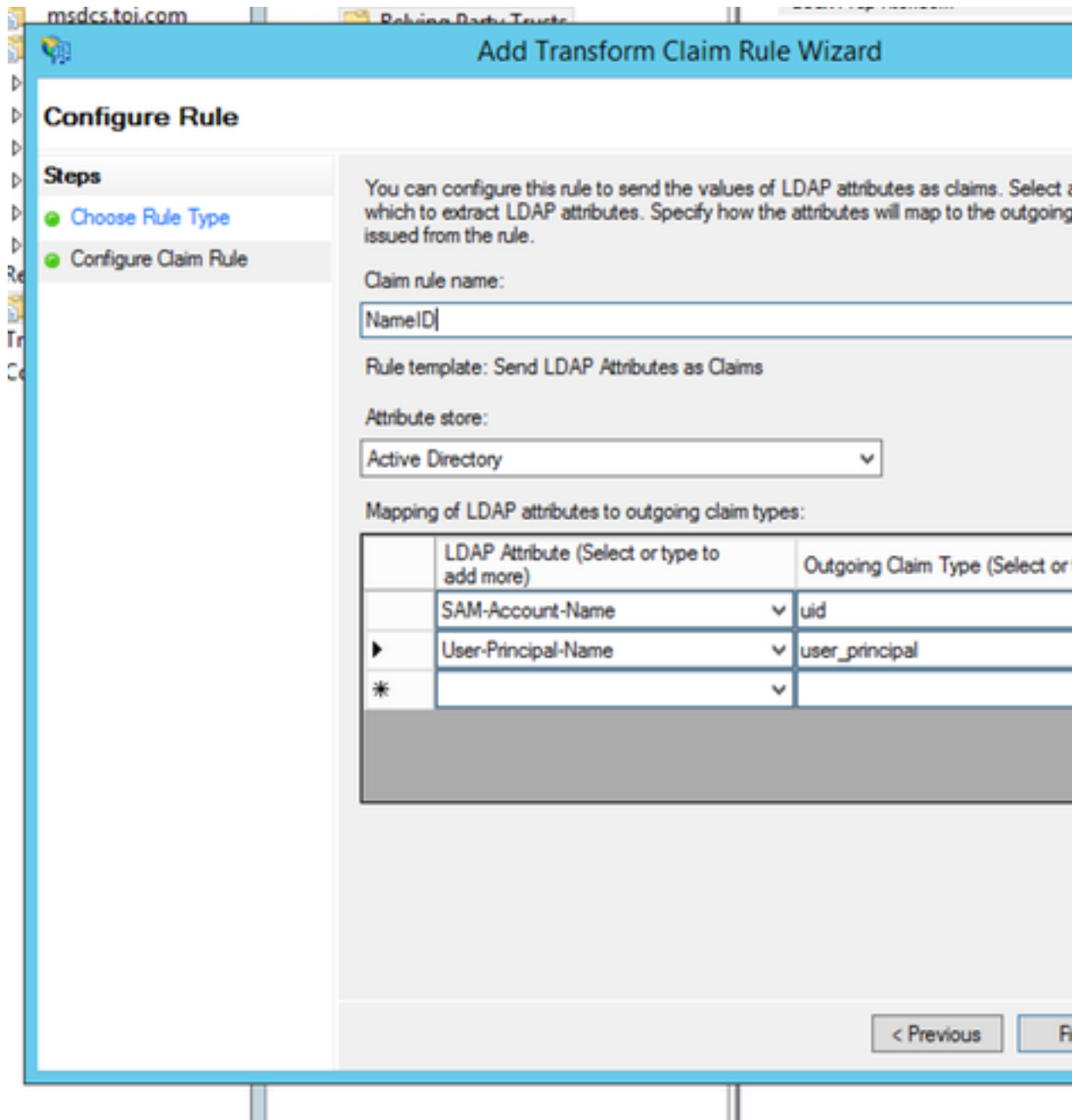
1. AD FS システムへの RDP。

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 が正しくマッピング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別子が見つからない」という 500 エラーで失敗します。またはできませんでした SAML 応答からの検索ユーザ識別子が見つからない 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

ブラウザ

このメッセージとの 500 エラー:

IdP 設定 エラー: 失敗される SAML 処理

SAML 応答からの検索ユーザ識別子はできませんでした。/SAML 応答からの検索ユーザ識別子はできませんでした。

エラー メッセージ

AD FS イベント ビューア:

エラーなし

Cisco IDS ログ:

```
com.cisco.ccbu.ids.IdSSAMLSyncServlet.java:294 - SAML com.sun.identity.saml.common.SAML retrieve ID
com.cisco.ccbu.ids.auth.api.IdSSAMLSyncServlet.validateSAMLAttributes(IdSSAMLSyncServlet)
com.cisco.ccbu.ids.auth.api.IdSSAMLSyncServlet.processSamlPostResponse(IdSSAMLSyncServlet)
com.cisco.ccbu.ids.auth.api.IdSSAMLSyncServlet.processIdEndPointRequest(IdSSAMLSyncServlet)
```

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コンフィギュレーションが必要となります。

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](#) のマシンの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と失敗します。/Could SAML 応答からの検索ユーザ プリンシパル」。

失敗のステップ 発信クレームで設定 されない uid および/または user_principal。

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: 壺: オアシス: 名前: tc:
SAML:2.0:status:Requester/urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy. l
一度試して下さい。

AD FS イベント ビューア:

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](#)

ネーム識別子 形式: urn:oasis:names:tc:SAML:2.0:nameid-format:transient

SPNameQualifier: [myids.cisco.com](#)

例外の詳細:

エラー メッセージ 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
求められた NameIDPolicy: AllowCreate: 本当形式: urn:oasis:names:tc:SAML:2.0:nameid-format:transient

SPNameQualifier: [myids.cisco.com](#). NameID 実際のプロパティ: ヌル。

この要求は失敗しました。

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子を出す AD FS 2.0 管理スナップインを使用して下

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 IdSSAMLSyncServlet.java:299 com.sun.identity.saml2.common.SAML2Exc
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425)
com.sun.identity.saml2.profile.SPACSTools.processResponse(SPACSTools.java:1050)
com.sun.identity.saml2.profile.SPACSTools.processResponseForFedlet(SPACSTools.java:2038
```

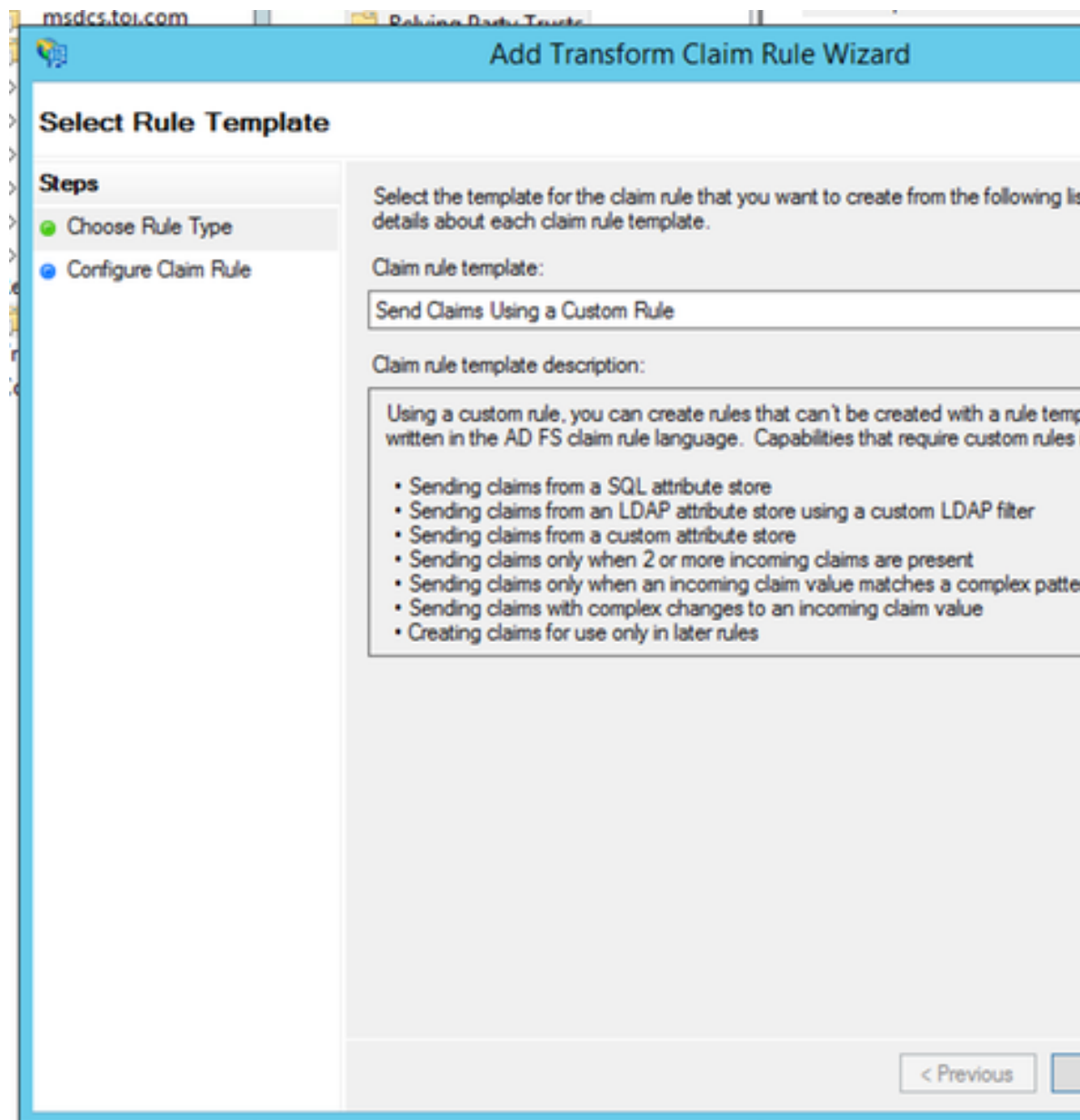
考えられる原因 カスタム クレーム ルールは正しく設定されません。

AD FS クレーム ルールの下で、(か。ガイドする) 「uid」 マッピング する属性が定義
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. 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つけられることを確認して下さい。

Edit Rule - uccx115p1.toi.com

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or the claims from a SQL attribute store. To configure a custom rule, type one or more optional condition issuance statement using the AD FS claim rule language.

Claim rule name:

uccx.contoso.com

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==  
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windows  
name"]  
=> issue(Type =  
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidenti  
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.V  
ValueType = c.ValueType, Properties  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/  
"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Prop  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/  
alifier"] = "http://fs.contoso.com/adfs/services/trust", Properti  
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/  
qualifier"] = "uccx.contoso.com";
```

OK

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 のブラウザ

失敗のステップ

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 へあるこ
SAML 応答処理
ブラウザ

エラー メッセージ

このメッセージとの 500 エラー:
IdP 設定 エラー: 失敗される 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:

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' 要求を持続しませんでした '16' 秒。 詳細に関しては管理者に連絡して下さい。

Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCookie

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 MSISIgn
</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.SPACUtils.processResponse(SPACUtils.java:1050)
com.sun.identity.saml2.profile.SPACUtils.processResponseForFedlet(SPACUtils.java:2038)
com.cisco.ccbu.ids.auth.api.IdSSAMLSyncServlet.getAttributesMapFromSAMLResponse(IdSSAM
```

考えられる原因 同じブラウザ 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:

1. AD FS Windows イベント ビューアをチェックして下さい。

推奨処置 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; : ArtifactResponse 2016-08-24 10:53:10.494 IST(+0530) [IdSEndPoint
com.cisco.ccbu.ids IdSSAMLSyncServlet.java:298 com.sun.identity.saml2.common.SAML2Exc
com.sun.identity.saml2.profile.SPACUtils.getResponseFromPost(SPACUtils.java:994)
com.sun.identity.saml2.profile.SPACUtils.getResponse(SPACUtils.java:196)
com.sun.identity.saml2.profile.SPACUtils.processResponseForFedlet(SPACUtils.java:2028)
com.cisco.ccbu.ids.auth.api.IdSSAMLSyncServlet.getAttributesMapFromSAMLResponse(IdSSAM
```

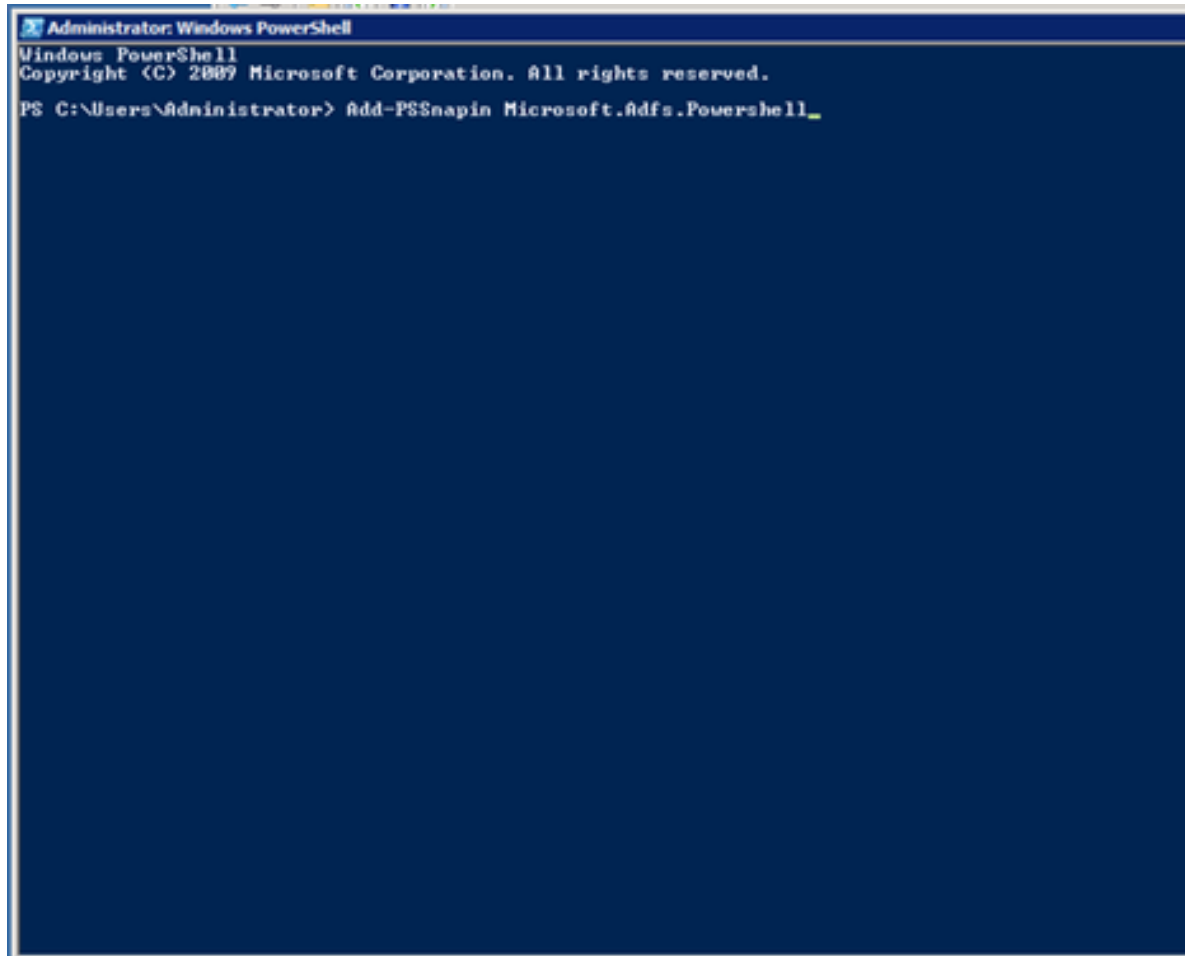
考えられる原因 AD FS はアサーションおよびメッセージに両方署名するために設定されません。

1. AD FS powershell コマンドを実行して下さい: **設定 されるADFSRelyingPartyTrust**
パーティ信頼 Identifier> - SamlResponseSignature 「MessageAndAssertion」

推奨処置 2. AD システムへの RDP。

3. Powershell を開いて下さい。

- 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。



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-PSSnapin Microsoft.Adfs.Powershell_
```

- ADFS 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

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-PSSnapin Microsoft.Adfs.Powershell
PS C:\Users\Administrator> Set-ADFSRelyingPartyTrust -TargetName uccx.contoso.com -SamlResponseSi
rtion"
```

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](#)