



SAMLを使用する

SANtricity 11.7

NetApp
February 12, 2024

目次

SAMLを使用する	1
SAMLを設定する	1
SAMLのロールマッピングを変更する	6
SAMLサービスプロバイダファイルをエクスポートする	7

SAMLを使用する

SAMLを設定する

アクセス管理の認証を設定する場合、ストレージレイに組み込みのSecurity Assertion Markup Language (SAML) 機能を使用することができます。この設定により、アイデンティティプロバイダとストレージプロバイダの間の接続が確立されます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- ストレージレイの各コントローラのIPアドレスまたはドメイン名を確認しておく必要があります。
- IdP管理者がIdPシステムの設定を完了している必要があります。
- IdP管理者が、認証時に名前IDを返す機能がIdPでサポートされていることを確認しておく必要があります。
- IdPサーバとコントローラのクロックを同期しておきます（NTPサーバを使用するかコントローラのクロックの設定を調整します）。
- IdPのメタデータファイルをIdPシステムからダウンロードし、System Managerへのアクセスに使用するローカルシステムで使用できるようにしておきます。

このタスクについて

アイデンティティプロバイダ (IdP) は、ユーザにクレデンシャルを要求して認証されたユーザかどうかを確認するために使用される外部のシステムです。多要素認証にも対応し、Active Directoryなどの任意のユーザデータベースを使用するように設定できます。IdPの保守はセキュリティチームが行います。サービスプロバイダ (SP) は、ユーザの認証とアクセスを制御するシステムです。アクセス管理にSAMLを設定すると、ストレージレイがアイデンティティプロバイダに認証を要求するサービスプロバイダとして機能します。IdPとストレージレイの間の接続を確立するには、この2つのエンティティ間でメタデータファイルを共有します。その後、IdPのユーザエンティティをストレージレイのロールにマッピングします。最後に、接続とSSOログインをテストしたうえでSAMLを有効にします。



- SAMLとディレクトリサービス*。認証方式としてディレクトリサービスを使用するように設定されている状況でSAMLを有効にした場合、System ManagerではSAMLがディレクトリサービスよりも優先されます。あとでSAMLを無効にすると、元の設定に戻ってディレクトリサービスが使用されます。



- SAMLを編集および無効化しています。* SAMLを有効にすると、ユーザインターフェイスで無効にすることはできず、IdP設定を編集することもできません。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

SAML認証の設定は複数の手順からなる手順です。

手順1：IdPのメタデータファイルをアップロードする

ストレージレイにIdPの接続情報を提供するには、System ManagerにIdPのメタデータをインポートします。このメタデータは、IdPシステムが認証要求を正しいURLにリダイレクトし、受信した応答を検証するために必要です。コントローラが2台ある場合でも、アップロードするメタデータファイルはストレージレイ

に対して1つだけです。

手順

1. メニューを選択します。Settings [Access Management]。
2. SAML *タブを選択します。

設定手順の概要が表示されます。

3. アイデンティティプロバイダ (IdP) ファイルのインポート*リンクをクリックします。

アイデンティティプロバイダファイルのインポートダイアログボックスが開きます。

4. Browse *をクリックして、ローカルシステムにコピーしたIdPメタデータファイルを選択してアップロードします。

ファイルを選択すると、IdPのエンティティIDが表示されます。

5. [* インポート *]をクリックします。

手順2：サービスプロバイダのファイルをエクスポートする

IdPとストレージレイの間の信頼関係を確立するために、サービスプロバイダのメタデータをIdPにインポートします。このメタデータは、IdPがコントローラとの間の信頼関係を確立し、許可要求を処理するために必要になります。このファイルには、コントローラのドメイン名やIPアドレスなど、IdPがサービスプロバイダと通信するために必要な情報が含まれています。

手順

1. [サービスプロバイダファイルのエクスポート*]リンクをクリックします。

[Export Service Provider Files]ダイアログボックスが開きます。

2. コントローラのIPアドレスまたはDNS名を[コントローラA *]フィールドに入力し、[*エクスポート]をクリックしてメタデータファイルをローカルシステムに保存します。ストレージレイにコントローラが2台ある場合は、2台目のコントローラの Controller B *フィールドでこの手順を繰り返します。

「* Export」をクリックすると、サービスプロバイダのメタデータがローカルシステムにダウンロードされます。ファイルの保存先をメモします。

3. ローカルシステムで、エクスポートしたサービスプロバイダのメタデータファイルを探します。

コントローラごとにXML形式のファイルが1つあります。

4. IdPサーバで、サービスプロバイダのメタデータファイルをインポートして信頼関係を確立します。ファイルを直接インポートすることも、ファイルからコントローラの手動で入力することもできます。

手順3：ロールをマッピングする

System Managerに対する許可とアクセスをユーザに提供するには、IdPユーザ属性とグループメンバーシップをストレージレイの事前定義されたロールにマッピングする必要があります。

作業を開始する前に

- IdP管理者が、IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
- IdPのメタデータファイルをSystem Managerにインポートしておきます。
- 各コントローラのサービスプロバイダメタデータファイルをIdPシステムにインポートして信頼関係を確立しておきます。

手順

1. マッピングSystem Manager *の役割のリンクをクリックします。

ロールマッピング(Role Mapping)ダイアログボックスが開きます

2. IdPユーザの属性とグループを事前定義されたロールに割り当てます。1つのグループに複数のロールを割り当てることができます。

設定	説明
マッピング	ユーザー属性
マッピングするSAMLグループの属性（「member of」など）を指定します。	属性値
マッピングするグループの属性値を指定します。正規表現がサポートされます。これらの特殊正規表現文字はバックスラッシュでエスケープする必要があります。（\）正規表現パターンに含まれていない場合は、次のようになります。 \.[]{}()<>*+.=!?^\$	
ロール	<p>フィールド内をクリックし、属性にマッピングするストレージレイのロールを選択します。追加するロールを1つずつ選択する必要があります。MonitorロールはSystem Managerにログインするため必要なロールであり、他のロールと一緒に指定する必要があります。また、少なくとも1つのグループにSecurity Adminロールを割り当てる必要があります。</p> <p>各ロールの権限は次のとおりです。</p> <ul style="list-style-type: none"> • * Storage admin *--ストレージ・オブジェクト（ボリュームやディスク・プールなど）への読み取り/書き込みのフル・アクセス。セキュリティ構成へのアクセスはありません。 • * Security admin *--アクセス管理、証明書管理、監査ログ管理のセキュリティ構成へのアクセス、および従来の管理インターフェイス（SYMBOL）のオン/オフの切り替え機能。 • * Support admin *--ストレージレイのすべてのハードウェアリソース、障害データ、MELイベント、およびコントローラファームウェアアップグレードへのアクセス。ストレージオブジェクトやセキュリティ設定にはアクセスできません。 • * Monitor *--すべてのストレージオブジェクトへの読み取り専用アクセスが可能ですが、セキュリティ設定へのアクセスはありません。



Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System Managerは正常に動作しません。

- 必要に応じて、*別のマッピングを追加*をクリックして、グループとロールのマッピングをさらに入力します。



ロールのマッピングは、SAMLを有効にしたあとに変更できます。

- マッピングが終了したら、*保存*をクリックします。

手順4：SSOログインをテストする

IdPシステムとストレージレイが通信できることを確認するために、必要に応じてSSOログインをテストできます。このテストは、SAMLを有効にする最後の手順でも実行します。

作業を開始する前に

- IdPのメタデータファイルをSystem Managerにインポートしておきます。
- 各コントローラのサービスプロバイダメタデータファイルをIdPシステムにインポートして信頼関係を確立しておきます。

手順

1. [Test SSO Login*]リンクを選択します。

SSOクレデンシャルを入力するためのダイアログボックスが表示されます。

2. Security AdminとMonitorの両方の権限を持つユーザのログインクレデンシャルを入力します。

ログインのテストを実行している間、ダイアログボックスが開きます。

3. テストに成功したことを示すメッセージを確認します。テストに成功した場合は、SAMLを有効にする次の手順に進みます。

テストが正常に完了しない場合は、エラーメッセージに詳細が表示されます。次の点を確認してください。

- ユーザがSecurity AdminとMonitorの権限を持つグループに属していること。
- アップロードしたIdPサーバのメタデータが正しいこと。
- SPメタデータファイル内のコントローラのアドレスが正しいこと。

手順5：SAMLを有効にする

最後に、ユーザ認証用のSAMLの設定を完了します。このプロセスでは、SSOログインのテストも求められます。SSOログインのテストプロセスについては、前の手順で説明したとおりです。

作業を開始する前に

- IdPのメタデータファイルをSystem Managerにインポートしておきます。
- 各コントローラのサービスプロバイダメタデータファイルをIdPシステムにインポートして信頼関係を確立しておきます。
- 少なくともMonitorロールとSecurity Adminロールを1つずつマッピングしておきます。



- SAMLを編集および無効化しています。* SAMLを有効にすると、ユーザインターフェイスで無効にすることはできず、IdP設定を編集することもできません。SAMLの設定を無効にしたり編集したりする必要がある場合は、テクニカルサポートにお問い合わせください。

手順

1. [* SAML]タブで、[SAMLを有効にする]リンクを選択します。

[Confirm Enable SAML (SAMLを有効にする)]ダイアログボックスが開きます。

2. を入力します `enable` をクリックし、*[有効化]*をクリックします。
3. SSOログインのテスト用にユーザクレデンシャルを入力します。

結果

SAMLが有効になると、アクティブなセッションはすべて終了され、SAMLを使用したユーザの認証が開始されます。

SAMLのロールマッピングを変更する

アクセス管理にSAMLを設定している場合、IdPグループとストレージレイの事前定義されたロールとの間のロールマッピングを変更できます。

作業を開始する前に

- Security Adminの権限を含むユーザプロフィールでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- IdP管理者が、IdPシステムでユーザ属性とグループメンバーシップを設定しておく必要があります。
- SAMLを設定して有効にします。

手順

1. メニューを選択します。Settings [Access Management]。
2. SAML *タブを選択します。
3. [役割のマッピング]を選択します。

ロールマッピング(Role Mapping)ダイアログボックスが開きます

4. IdPユーザの属性とグループを事前定義されたロールに割り当てます。1つのグループに複数のロールを割り当てることができます。



SAMLが有効になっているときは権限を削除しないように注意してください。削除すると、System Managerにアクセスできなくなります。

フィールドの詳細

設定	説明
マッピング	ユーザー属性
マッピングするSAMLグループの属性 (「member of」など) を指定します。	属性値
マッピングするグループの属性値を指定します。	ロール



Monitorロールは、管理者を含むすべてのユーザに必要です。Monitorロールがないユーザの場合、System Managerは正常に動作しません。

5. 必要に応じて、* Add another mapping *をクリックして、グループとロールのマッピングをさらに入力します。
6. [保存 (Save)]をクリックします。

結果

このタスクを完了すると、アクティブなユーザセッションはすべて終了します。現在のユーザセッションのみが保持されます。

SAMLサービスプロバイダファイルをエクスポートする

必要に応じて、ストレージレイのサービスプロバイダのメタデータをエクスポートして、ファイルをアイデンティティプロバイダ (IdP) システムに再インポートすることができます。

作業を開始する前に

- Security Adminの権限を含むユーザプロファイルでログインする必要があります。そうしないと、アクセス管理機能は表示されません。
- SAMLを設定して有効にします。

このタスクについて

このタスクでは、コントローラからメタデータ (コントローラごとに1ファイル) をエクスポートします。このメタデータは、IdPがコントローラとの間の信頼関係を確立し、認証要求を処理するために必要になります。このファイルには、コントローラのドメイン名やIPアドレスなど、IdPで要求の送信に使用できる情報が含まれています。

手順

1. メニューを選択します。Settings [Access Management]。

2. SAML *タブを選択します。
3. 「書き出し」を選択します。

[Export Service Provider Files]ダイアログボックスが開きます。

4. 各コントローラについて、* Export (エクスポート) *をクリックしてメタデータファイルをローカルシステムに保存します。



各コントローラのドメイン名フィールドは読み取り専用です。

ファイルの保存先をメモします。

5. ローカルシステムで、エクスポートしたサービスプロバイダのメタデータファイルを探します。

コントローラごとにXML形式のファイルが1つあります。

6. IdPサーバから、サービスプロバイダのメタデータファイルをインポートします。ファイルを直接インポートすることも、ファイルからコントローラの手動で入力することもできます。
7. [* 閉じる *]をクリックします。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。