



SnapCenter

サーバをインストールする準備をします

SnapCenter Software 4.9

NetApp
March 20, 2024

目次

SnapCenter サーバをインストールする準備をします	1
ドメインとワークグループの要件	1
スペースとサイジングの要件	1
SANホストの要件	2
サポートされるストレージシステムおよびアプリケーション	3
サポートされているブラウザ	3
接続とポートの要件	4
SnapCenter ライセンス	7
クレデンシャルの認証方式を指定します	10
ストレージ接続およびクレデンシャル	11
多要素認証 (MFA)	12

SnapCenter サーバをインストールする準備をします

ドメインとワークグループの要件

SnapCenter サーバは、ドメインまたはワークグループ内のシステムにインストールできます。インストールに使用するユーザには、ワークグループとドメインの両方の場合に、マシンに対する管理者権限が必要です。

Windows ホストに SnapCenter Server プラグインと SnapCenter プラグインをインストールするには、次のいずれかを使用する必要があります。

- * Active Directory ドメイン *

ローカル管理者の権限を持つドメインユーザを使用する必要があります。ドメインユーザは、Windows ホストのローカル管理者グループのメンバーである必要があります。

- * ワークグループ *

ローカル管理者の権限があるローカルアカウントを使用する必要があります。

ドメイントラスト、マルチドメインフォレスト、およびクロスドメイントラストはサポートされていますが、クロスフォレストドメインはサポートされません。詳細については、Microsoft の Active Directory ドメインと信頼関係に関するドキュメントを参照してください。



SnapCenter サーバをインストールしたあとに、SnapCenter ホストが配置されているドメインを変更しないでください。SnapCenter サーバをインストールした時点のドメインから SnapCenter サーバホストを削除して、SnapCenter サーバをアンインストールしようとする、アンインストール処理は失敗します。

スペースとサイジングの要件

SnapCenter サーバをインストールする前に、スペースとサイジングの要件を十分に理解しておく必要があります。また、利用可能なシステムおよびセキュリティの更新も適用する必要があります。

項目	要件
オペレーティングシステム	Microsoft Windows の場合 サポートされているのは、英語版、ドイツ語版、日本語版、簡体字中国語版のオペレーティングシステムのみです。 サポートされているバージョンの最新情報については、 を参照してください "NetApp Interoperability Matrix Tool で確認できます" 。

項目	要件
最小 CPU 数	4 コア
最小 RAM	8 GB  MySQL Server のバッファプールでは、RAM の合計の 20% が使用されます。
SnapCenter サーバソフトウェアおよびログ用のハードドライブの最小容量	4 GB  SnapCenter サーバがインストールされているドライブに SnapCenter リポジトリがある場合は、10GB にすることを推奨します。
SnapCenter リポジトリ用のハードドライブの最小容量	6 GB  メモ： SnapCenter リポジトリがインストールされているドライブに SnapCenter サーバがある場合は、10GB にすることを推奨します。
必要なソフトウェアパッケージ	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.2以降 • Windows Management Framework (WMF) 4.0 以降 • PowerShell 4.0 以降

SANホストの要件

SnapCenter ホストが FC / iSCSI 環境に配置されている場合、ONTAP ストレージへのアクセスを有効にするために、システムに追加のソフトウェアのインストールが必要になることがあります。

SnapCenter には、Host Utilities と DSM は含まれていません。SnapCenter ホストが SAN 環境に配置されている場合は、次のソフトウェアのインストールと設定が必要になることがあります。

- Host Utilities のことです

Host Utilities は FC および iSCSI をサポートしており、Windows サーバ上で MPIO を使用することができます。詳細については、を参照してください "[Host Utilities のマニュアル](#)"。

- Microsoft DSM for Windows MPIO

このソフトウェアは Windows MPIO ドライバと連携して、ネットアップと Windows のホストコンピュータ間の複数のパスを管理します。

ハイアベイラビリティ構成には DSM が必要です。



ONTAP DSM を使用していた場合は、Microsoft DSM に移行する必要があります。詳細については、を参照してください ["ONTAP DSM から Microsoft DSM への移行方法"](#)。

サポートされるストレージシステムおよびアプリケーション

サポートされるストレージシステム、アプリケーション、およびデータベースを確認しておく必要があります。

- SnapCenter では、データを保護するために ONTAP 8.3.0 以降がサポートされています。
- SnapCenter は、ONTAP ソフトウェア 4.5 P1 パッチリリースからデータを保護するために、NetApp SnapCenter 用の Amazon FSX をサポートしています。

NetApp ONTAP に Amazon FSX を使用している場合、データ保護処理を実行するには、SnapCenter サーバホストプラグインを 4.5 P1 以降にアップグレードする必要があります。

NetApp ONTAP の Amazon FSX の詳細については、を参照してください ["Amazon FSX for NetApp ONTAP のドキュメント"](#)。

- SnapCenter では、さまざまなアプリケーションやデータベースの保護がサポートされます。

サポートされているアプリケーションおよびデータベースの詳細については、を参照してください ["NetApp Interoperability Matrix Tool で確認できます"](#)。

- SnapCenter 4.9 P1以降では、Amazon Web Services (AWS) のSoftware-Defined Data Center (SDDC) 環境上のVMware Cloudで、OracleとMicrosoft SQLのワークロードの保護がサポートされます。

詳細については、を参照してください ["VMware Cloud on AWS SDDC環境でNetApp SnapCenterを使用してOracleやMS SQLのワークロードを保護"](#)。

サポートされているブラウザ

SnapCenter ソフトウェアは、複数のブラウザで使用できます。

- クロム

v66 を使用している場合、SnapCenter GUI の起動に失敗することがあります。

- Internet Explorer の略

IE 10 以前のバージョンを使用している場合、SnapCenter UI が正しくロードされません。IE 11 にアップグレードする必要があります。

- デフォルトレベルのセキュリティのみがサポートされています。

Internet Explorer のセキュリティ設定を変更すると、ブラウザの表示に重大な問題が発生します。

◦ Internet Explorer の互換表示を無効にする必要があります。

- Microsoft Edge の場合

サポートされているバージョンの最新情報については、を参照してください "[NetApp Interoperability Matrix Tool](#) で確認できます"。

接続とポートの要件

SnapCenter サーバとアプリケーションまたはデータベースのプラグインをインストールする前に、接続とポートの要件が満たされていることを確認する必要があります。

- アプリケーションはポートを共有できません。

各ポートは、適切なアプリケーション専用にする必要があります。

- デフォルトのポートを使用しない場合は、インストール時にカスタムポートを選択できます。

プラグインポートは、インストール後にホストの変更ウィザードを使用して変更できます。

- 固定ポートの場合は、デフォルトのポート番号を受け入れる必要があります。

- ファイアウォール

◦ ファイアウォール、プロキシ、またはその他のネットワークデバイスが接続を妨げないようにしてください。

◦ SnapCenter のインストール時にカスタムポートを指定した場合は、プラグインホストに、SnapCenter Plug-in Loader のそのポート用のファイアウォールルールを追加する必要があります。

次の表に、各ポートとそのデフォルト値を示します。

ポートのタイプ	デフォルトのポート
SnapCenter ポート	8146 (HTTPS) 、 URL <code>_https://server:8146_</code> のように双方向、カスタマイズ可能 SnapCenter クライアント (SnapCenter ユーザ) と SnapCenter サーバ間の通信に使用されます。プラグインホストから SnapCenter サーバへの通信にも使用されます。 ポートをカスタマイズするには、を参照してください " インストールウィザードを使用してSnapCenterサーバをインストールします。 "

ポートのタイプ	デフォルトのポート
SnapCenter SMCORE の通信ポート	<p>8145（HTTPS）、双方向、カスタマイズ可能</p> <p>このポートは、SnapCenter サーバと SnapCenter プラグインがインストールされているホストの間の通信に使用されます。</p> <p>ポートをカスタマイズするには、を参照してください "インストールウィザードを使用してSnapCenterサーバをインストールします。"</p>
MySQL ポート	<p>3306（HTTPS）、双方向</p> <p>このポートは、SnapCenter と MySQL リポジトリデータベースの間の通信に使用されます。</p> <p>SnapCenter サーバから MySQL サーバへのセキュアな接続を作成できます。 "詳細はこちら。"</p> <p>ポートをカスタマイズするには、を参照してください "インストールウィザードを使用してSnapCenterサーバをインストールします。"</p>
Windows プラグインホスト	<p>135、445（TCP）</p> <p>ポート 135 および 445 に加え、Microsoft が指定したダイナミックポート範囲も開いている必要があります。リモートインストール操作では、このポート範囲を動的に検索する Windows Management Instrumentation（WMI）サービスを使用します。</p> <p>サポートされているダイナミックポート範囲については、を参照してください "Windows のサービス概要とネットワークポート要件"</p> <p>ポートは、SnapCenter サーバとプラグインをインストールするホストとの間の通信に使用されます。プラグインパッケージのバイナリを Windows プラグインホストにプッシュするには、プラグインホストでのみポートを開く必要があります。このポートはインストール後に閉じることができます。</p>

ポートのタイプ	デフォルトのポート
Linux または AIX プラグインホスト	<p>22 (SSH)</p> <p>ポートは、SnapCenter サーバとプラグインをインストールするホストとの間の通信に使用されます。プラグインパッケージのバイナリを Linux または AIX プラグインのホストにコピーするために SnapCenter で使用されます。これらのポートを開いておくか、ファイアウォールまたは iptables から除外しておく必要があります。</p>
SnapCenter Plug-ins Package for Windows、SnapCenter Plug-ins Package for Linux または SnapCenter Plug-ins Package for AIX のいずれかです	<p>8145 (HTTPS)、双方向、カスタマイズ可能</p> <p>ポートは、SMCore とプラグインパッケージがインストールされているホストの間の通信に使用されません。</p> <p>通信パスも、SVM 管理 LIF と SnapCenter サーバの間で開いている必要があります。</p> <p>ポートをカスタマイズするには、を参照してください "ホストを追加し、SnapCenter Plug-in for Microsoft Windows をインストールします" または "ホストを追加してLinuxまたはAIX用のSnapCenter Plug-insパッケージをインストールします。"</p>
SnapCenter Plug-in for Oracle Database	<p>27216、カスタマイズ可能</p> <p>デフォルトの JDBC ポートは、Oracle データベースに接続するためにプラグイン for Oracle で使用されません。</p> <p>ポートをカスタマイズするには、を参照してください "ホストを追加してLinuxまたはAIX用のSnapCenter Plug-insパッケージをインストールします。"</p>
SnapCenter 用のカスタムプラグイン	<p>9090 (HTTPS)、固定</p> <p>これはカスタムプラグインホストでのみ使用される内部ポートで、ファイアウォールの例外は不要です。</p> <p>SnapCenter サーバとカスタムプラグイン間の通信はポート 8145 を介してルーティングされます。</p>

ポートのタイプ	デフォルトのポート
ONTAP クラスタまたは SVM の通信ポート	443 (HTTPS)、双方向 80 (HTTP)、双方向 このポートは、SnapCenter サーバを実行するホストと SVM の間の通信に SAL (ストレージ抽象化レイヤ) で使用されます。現時点では、SnapCenter プラグインホストと SVM の間の通信に、SnapCenter for Windows プラグインホストの SAL でもポートが使用されています。
SnapCenter Plug-in for SAP HANA Database vCode スペルチェッカーポート	3instance_number13 または 3instance_number15、HTTP または HTTPS、双方向、カスタマイズ可能です マルチテナントデータベースコンテナ (MDC) のシングルテナントの場合は、ポート番号は 13 で終わり、MDC 以外の場合はポート番号は 15 で終わります。 たとえば、32013 はインスタンス 20 のポート番号で、31015 はインスタンス 10 のポート番号です。 ポートをカスタマイズするには、 を参照してください "ホストを追加し、プラグインパッケージをリモートホストにインストールする。"
ドメインコントローラの通信ポート	認証が適切に機能するために、Microsoft のマニュアルを参照して、ドメインコントローラのファイアウォールで開く必要があるポートを確認してください。 SnapCenter サーバ、プラグインホスト、またはその他の Windows クライアントがユーザを認証できるように、ドメインコントローラで Microsoft の必要なポートを開く必要があります。

ポートの詳細を変更する手順については、[を参照してください](#) "プラグインホストを変更します"。

SnapCenter ライセンス

SnapCenter では、アプリケーション、データベース、ファイルシステム、および仮想マシンのデータを保護するために、複数のライセンスが必要になります。インストールする SnapCenter ライセンスのタイプは、ストレージ環境および使用する機能によって異なります。

使用許諾	必要に応じて
SnapCenter 標準のコントローラベース	<p>FAS、AFF、オールSANアレイ（ASA）に必要</p> <p>SnapCenter Standard ライセンスはコントローラベースのライセンスで、Premium Bundle に含まれていません。SnapManager スイートのライセンスをお持ちの場合は、SnapCenter Standard のライセンスもご利用いただけます。FAS、AFF、またはASAストレージにSnapCenterの試用版をインストールする場合は、営業担当者に連絡してPremium Bundleの評価ライセンスを取得してください。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>SnapCenter は、データ保護バンドルの一部としても提供されます。A400以降を購入している場合は、データ保護バンドルを購入する必要があります。</p> </div>
SnapCenter - 容量ベース	<p>ONTAP Select および Cloud Volumes ONTAP で必要です</p> <p>Cloud Volumes ONTAP または ONTAP Select を使用している場合は、SnapCenter で管理するデータに基づいて、容量ベースのライセンスを 1TB 単位で購入する必要があります。デフォルトでは、SnapCenter には 90 日間の 100TB SnapCenter の標準容量ベースの試用版ライセンスが組み込まれています。その他の詳細については、営業担当者にお問い合わせください。</p>
SnapMirror または SnapVault	<p>ONTAP</p> <p>SnapCenter でレプリケーションを有効にする場合は、SnapMirror または SnapVault のライセンスが必要です。</p>
SnapRestore	<p>バックアップのリストアおよび検証に必要です。</p> <p>プライマリストレージシステム</p> <ul style="list-style-type: none"> • リモート検証に加えてバックアップからのリストアを実行するには、SnapVault デスティネーションシステムに必要です。 • リモート検証を実行する場合は、SnapMirror デスティネーションシステムに必要です。

使用許諾	必要に応じて
FlexClone	<p>データベースのクローニングおよび検証処理に必要です。</p> <p>プライマリストレージシステムおよびセカンダリストレージシステム。</p> <ul style="list-style-type: none"> セカンダリ SnapVault バックアップからクローンを作成する場合、SnapVault デスティネーションシステムに必要です。 セカンダリ SnapMirror バックアップからクローンを作成するには、SnapMirror デスティネーションシステムに必要です。
プロトコル	<ul style="list-style-type: none"> LUN 用の iSCSI または FC ライセンス SMB 共有の CIFS ライセンス NFS タイプの VMDK 用の NFS ライセンスです VMFS タイプの VMDK 用の iSCSI または FC ライセンス <p>ソースボリュームを利用できない場合に SnapMirror デスティネーションシステムからデータを提供するには、SnapMirror デスティネーションシステムに必要です。</p>
SnapCenter 標準ライセンス (オプション)	<p>セカンダリデスティネーション</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p> セカンダリデスティネーションに SnapCenter Standard ライセンスを追加することを推奨しますが、必須ではありません。セカンダリデスティネーションで SnapCenter 標準ライセンスが有効になっていない場合、フェイルオーバー処理の実行後に、SnapCenter を使用してセカンダリデスティネーションのリソースをバックアップすることはできません。ただし、クローニング処理と検証処理を実行するには、セカンダリデスティネーションに FlexClone ライセンスが必要です。</p> </div>



SnapCenter Advanced および SnapCenter NAS ファイルサービスのライセンスは廃止され、現在は提供されていません。

1 つ以上の SnapCenter ライセンスをインストールする必要があります。ライセンスの追加方法については、[を参照してください "SnapCenter の標準コントローラベースのライセンスを追加します"](#) または ["SnapCenter](#)

の Standard 容量ベースのライセンスを追加".

Single Mailbox Recovery (SMBR) ライセンス

SnapCenter Plug-in for Exchange を使用して Microsoft Exchange Server データベースと Single Mailbox Recovery (SMBR) を管理している場合は、SMBR のライセンスが追加が必要です。SMBR の場合は、ユーザのメールボックスに基づいて別途購入する必要があります。

NetApp®Single Mailbox Recoveryは、2023年5月12日に販売終了 (EOA) になりました。詳細については、を参照してください "[CPC-00507](#)". NetAppは、2020年6月24日に導入されたマーケティング用パーツ番号を通じて、メールボックスの容量、メンテナンス、サポートを購入したお客様をサポート対象期間中も引き続きサポートします。

NetApp Single Mailbox Recoveryは、Ontrackが提供するパートナー製品です。Ontrack PowerControlsには、NetApp Single Mailbox Recoveryと同様の機能が用意されています。お客様は、新しいOntrack PowerControlsソフトウェアライセンスとOntrack PowerControlsメンテナンスおよびサポートの更新をOntrackから (licensingteam@ontrack.com経由で) 調達し、2023年5月12日のEOA日以降にメールボックスをきめ細かくリカバリできます。

クレデンシャルの認証方式を指定します

クレデンシャルは、アプリケーションや環境に応じて異なる認証方式を使用します。クレデンシャルで認証されたユーザは、SnapCenter の処理を実行できます。プラグインのインストール用とデータ保護処理用に 1 組のクレデンシャルを作成する必要があります。

Windows 認証

Windows 認証方式は、Active Directory に照らして認証します。Windows 認証の場合、Active Directory は SnapCenter の外部で設定されます。SnapCenter の認証に追加の設定は必要ありません。Windows クレデンシャルは、ホストの追加、プラグインパッケージのインストール、ジョブのスケジュール設定などのタスクを実行する際に必要になります。

信頼されないドメイン認証です

SnapCenter では、信頼されていないドメインに属するユーザとグループを使用して Windows クレデンシャルを作成できます。認証を成功させるには、信頼されていないドメインを SnapCenter に登録する必要があります。

ローカルワークグループ認証

SnapCenter では、ローカルのワークグループユーザとグループを使用して Windows クレデンシャルを作成できます。ローカルワークグループのユーザとグループの Windows 認証は、Windows クレデンシャルの作成時には行われませんが、ホストの登録やその他のホスト処理が実行されるまで保留されます。

SQL Server 認証

SQL 認証方式は、SQL Server インスタンスに照らして認証します。つまり、SnapCenter で SQL Server インスタンスが検出されている必要があります。そのため、SQL クレデンシャルを追加する前に、ホストの追加とプラグインパッケージのインストールを行って、リソースを更新しておく必要があります。SQL Server

認証は、SQL Server でのスケジュールの設定やリソースの検出などの処理を実行する際に必要になります。

Linux 認証

Linux 認証方式は、Linux ホストに照らして認証します。Linux 認証は、SnapCenter の GUI からリモートで Linux ホストを追加して SnapCenter Plug-ins Package for Linux をインストールする最初のステップで必要になります。

AIX 認証

AIX 認証方式は、AIX ホストに照らして認証します。AIX 認証は、SnapCenter の GUI からリモートで AIX ホストを追加して SnapCenter Plug-ins Package for AIX をインストールする最初のステップで必要になります。

Oracle データベース認証

Oracle データベース認証方式は、Oracle データベースに照らして認証します。データベースホストでオペレーティングシステム（OS）認証が無効な場合、Oracle データベースに対して処理を実行するには、Oracle データベース認証が必要です。そのため、Oracle データベースのクレデンシャルを追加する前に、Oracle データベースで sysdba 権限を持つ Oracle ユーザを作成しておく必要があります。

Oracle ASM 認証

Oracle ASM 認証方式は、Oracle Automatic Storage Management（ASM）インスタンスに照らして認証します。Oracle ASM 認証は、Oracle ASM インスタンスにアクセスする際、データベースホストでオペレーティングシステム（OS）認証が無効になっている場合に必要になります。したがって、Oracle ASM クレデンシャルを追加する前に、ASM インスタンスで SYSASM 権限を持つ Oracle ユーザを作成する必要があります。

RMAN カタログ認証

RMAN カタログ認証方式は、Oracle Recovery Manager（RMAN）カタログデータベースに照らして認証します。外部のカタログメカニズムを設定し、データベースをカタログデータベースに登録している場合は、RMAN カタログ認証を追加する必要があります。

ストレージ接続およびクレデンシャル

データ保護処理を実行する前に、ストレージ接続をセットアップし、SnapCenter サーバおよび SnapCenter プラグインで使用するクレデンシャルを追加する必要があります。

- * ストレージ接続 *

ストレージ接続を使用すると、SnapCenter サーバおよび SnapCenter プラグインから ONTAP ストレージにアクセスできるようになります。この接続のセットアップには、AutoSupport 機能と Event Management System（EMS；イベント管理システム）機能の設定も含まれます。

- * 資格情報 *

- ドメイン管理者または管理者グループの任意のメンバー

ドメイン管理者、または SnapCenter プラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。Username フィールドの有効な形式は次のとおりです。

- NETBIOS_USERNAME_
 - _ ドメイン FQDN\ ユーザ名 _
 - Username@UPN
- ローカル管理者（ワークグループのみ）

ワークグループに属するシステムの場合は、SnapCenter プラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザアカウントに昇格された権限がある場合、またはホストシステムでユーザアクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザアカウントを指定できます。

Username フィールドの有効な形式は、*username* です

- 個々のリソースグループのクレデンシャル

個々のリソースグループのクレデンシャルを設定していて、ユーザ名にフル管理者権限がない場合は、少なくともリソースグループとバックアップ権限をユーザ名に割り当てる必要があります。

多要素認証（MFA）

多要素認証（MFA）を管理します。

Active Directory フェデレーションサービス（AD FS）サーバと SnapCenter サーバで多要素認証（MFA）機能を管理できます。

多要素認証（MFA）を有効にする

SnapCenter サーバの MFA 機能は、PowerShell コマンドを使用して有効にできます。

このタスクについて

- SnapCenter は、他のアプリケーションが同じ AD FS で構成されている場合に SSO ベースのログインをサポートします。AD FS の構成によっては、AD FS セッションの持続性に応じて、セキュリティ上の理由から SnapCenter でユーザ認証が必要になる場合があります。
- コマンドレットで使用できるパラメータとその説明は、を実行して確認できます `Get-Help command_name`。または、を参照することもできます "[SnapCenter ソフトウェアコマンドレットリファレンスガイド](#)"。

作業を開始する前に

- Windows Active Directory フェデレーションサービス（AD FS）がそれぞれのドメインで稼働している必要があります。
- Azure MFA、Cisco Duo など、AD FS がサポートする多要素認証サービスが必要です。
- SnapCenter および AD FS サーバのタイムスタンプは、タイムゾーンに関係なく同じである必要があります。
- SnapCenter サーバの認証済み CA 証明書を取得して設定します。

CA証明書は、次の理由で必須です。

- 自己署名証明書はノードレベルで一意であるため、ADFS-F5通信が切断されないようにします。
- スタンドアロン構成またはハイアベイラビリティ構成でのアップグレード、修復、またはディザスタリカバリ（DR）の実行時に、自己署名証明書が再作成されないようにしてMFAの再設定を回避します。
- IP-FQDNの解決を保証します。

CA証明書の詳細については、を参照してください "[CA 証明書 CSR ファイルを生成します](#)"。

手順

1. Active Directoryフェデレーションサービス（AD FS）ホストに接続します。
2. AD FSフェデレーションメタデータファイルをからダウンロードします "<https://<host Fqdn>/FederationMetadata/2007-06/FederationMetadata.xml>」を参照してください。
3. ダウンロードしたファイルをSnapCenter サーバにコピーしてMFA機能を有効にします。
4. PowerShellを使用して、SnapCenter 管理者ユーザとしてSnapCenter サーバにログインします。
5. PowerShellセッションを使用して、_New-SmMultifactorAuthenticationMetadata-path_cmdletを使用して、SnapCenter MFAメタデータファイルを生成します。

pathパラメータでは、SnapCenter サーバホストにMFAメタデータファイルを保存するパスを指定します。

6. 生成されたファイルをAD FSホストにコピーし、SnapCenter をクライアントエンティティとして設定します。
7. を使用して、SnapCenter サーバのMFAを有効にします Set-SmMultiFactorAuthentication コマンドレット。
8. （オプション）を使用して、MFAの設定のステータスと設定を確認します Get-SmMultiFactorAuthentication コマンドレット。
9. Microsoft管理コンソール（MMC）に移動し、次の手順を実行します。
 - a. [ファイル>*スナップインの追加と削除*]をクリックします。
 - b. [スナップインの追加と削除] ウィンドウで、[Certificates] を選択し、[Add] をクリックします。
 - c. [証明書] スナップインウィンドウで、[Computer account] オプションを選択し、[完了 *] をクリックします。
 - d. [コンソールルート] > [証明書-ローカルコンピューター] > [個人] > [証明書] の順にクリックします。
 - e. SnapCenter にバインドされているCA証明書を右クリックし、すべてのタスク>*秘密鍵の管理*を選択します。
 - f. 許可ウィザードで、次の手順を実行します。
 - i. [追加（Add）] をクリックします。
 - ii. [場所]*をクリックし、該当するホスト（階層の最上位）を選択します。
 - iii. 「場所」ポップアップウィンドウで「* OK」をクリックします。
 - iv. [オブジェクト名]フィールドに「IIS_IUSRS」と入力し、[名前の確認]をクリックして、[OK]をクリ

ックします。

チェックが正常に終了したら、* OK *をクリックします。

10. AD FSホストで、AD FS管理ウィザードを開き、次の手順を実行します。
 - a. [証明書利用者信頼 (Rel証明書利用者信頼)]>[証明書利用者信頼の追加 (Add Rel証明書利用者信頼)]>[開始]
 - b. 2番目のオプションを選択してSnapCenter MFAメタデータファイルを参照し、*次へ*をクリックします。
 - c. 表示名を指定し、*次へ*をクリックします。
 - d. 必要に応じてアクセス制御ポリシーを選択し、*[Next]*をクリックします。
 - e. 次のタブでデフォルトに設定を選択します。
 - f. [完了]をクリックします。

指定した表示名の証明書利用者としてSnapCenter が反映されるようになりました。

11. 名前を選択し、次の手順を実行します。
 - a. [クレーム発行ポリシーの編集] をクリックします。
 - b. [ルール追加]をクリックし、[次へ]をクリックします。
 - c. クレームルールの名前を指定します。
 - d. 属性ストアとして「* Active Directory *」を選択します。
 - e. 属性として「* User-Principal-Name 」を選択し、発信クレームタイプとして「Name-ID *」を選択します。
 - f. [完了]をクリックします。
12. ADFSサーバで次のPowerShellコマンドを実行します。

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'  
-SigningCertificateRevocationCheck None
```

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'  
-EncryptionCertificateRevocationCheck None
```

13. メタデータが正常にインポートされたことを確認するには、次の手順を実行します。
 - a. 証明書利用者信頼を右クリックし、* Properties *を選択します。
 - b. [エンドポイント]、[識別子]、および[署名]フィールドに値が入力されていることを確認します
14. すべてのブラウザタブを閉じ、ブラウザを再度開いて既存またはアクティブなセッションCookieをクリアし、再度ログインします。

SnapCenter MFA機能は、REST APIを使用して有効にすることもできます。

トラブルシューティング情報については、を参照してください ["複数のタブで同時にログインを試行すると、MFAエラーが表示されます"](#)。

AD FS MFAメタデータを更新します

AD FSサーバでアップグレード、CA証明書の更新、DRなどの変更が行われた場合は、SnapCenter でAD FS MFAメタデータを更新する必要があります。

手順

1. AD FSフェデレーションメタデータファイルをからダウンロードします "<https://<hostfqdn>/FederationMetadata/2007-06/FederationMetadata.xml>"
2. ダウンロードしたファイルをSnapCenter サーバにコピーしてMFA設定を更新します。
3. 次のコマンドレットを実行して、SnapCenter 内のAD FSメタデータを更新します。

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. すべてのブラウザタブを閉じ、ブラウザを再度開いて既存またはアクティブなセッションCookieをクリアし、再度ログインします。

SnapCenter MFAメタデータを更新します

ADFSサーバで修復、CA証明書の更新、DRなどに変更があった場合は、AD FSでSnapCenter MFAメタデータを更新する必要があります。

手順

1. AD FSホストで、AD FS管理ウィザードを開き、次の手順を実行します。
 - a. [証明書利用者信頼]をクリックします。
 - b. SnapCenter 用に作成された証明書利用者信頼を右クリックし、*削除*をクリックします。

ユーザが定義した証明書利用者信頼の名前が表示されます。

- c. 多要素認証 (MFA) を有効にします。

を参照してください "[多要素認証を有効にします](#)".

2. すべてのブラウザタブを閉じ、ブラウザを再度開いて既存またはアクティブなセッションCookieをクリアし、再度ログインします。

多要素認証 (MFA) を無効にする

手順

1. MFAを無効にし、を使用してMFAを有効にしたときに作成された構成ファイルをクリーンアップします
Set-SmMultiFactorAuthentication コマンドレット。
2. すべてのブラウザタブを閉じ、ブラウザを再度開いて既存またはアクティブなセッションCookieをクリアし、再度ログインします。

REST API、PowerShell、SCCLIを使用して多要素認証 (MFA) を管理

MFAログインは、ブラウザ、REST API、PowerShell、およびSCCLIからサポートされます。MFAは、AD FSアイデンティティマネージャを介してサポートされます。GUI、REST API、PowerShell、SCCLIを使用して、MFAの有効化、MFAの無効化、およ

びMFAの設定を行うことができます。

AD FSをOAuth/OIDCとしてセットアップします

- Windows GUIウィザードを使用してAD FSを構成します*

1. Server Manager Dashboard > Tools > ADFS Management *に移動します。
2. >[アプリケーショングループ]*に移動します。
 - a. [アプリケーショングループ]を右クリックします。
 - b. を選択し、[アプリケーション名]*と入力します。
 - c. [サーバーアプリケーション]*を選択します。
 - d. 「*次へ*」をクリックします。

3. コピー*クライアントID*。

これはクライアントIDです。 。リダイレクトURLにコールバックURL（SnapCenterサーバURL）を追加します。 。 「*次へ*」をクリックします。

4. [Generate shared secret]*を選択します。

シークレット値をコピーします。これはクライアントの秘密です。 。 「*次へ*」をクリックします。

5. [概要]ページで、*[次へ]*をクリックします。

- a. [完了]ページで、*[閉じる]*をクリックします。

6. 新しく追加した*アプリケーショングループ*を右クリックし、*プロパティ*を選択します。

7. [アプリケーションのプロパティ]から*[アプリケーションの追加]*を選択します。

8. [アプリケーションの追加]*をクリックします。

[Web API]を選択し、*[Next]*をクリックします。

9. [Web APIの構成]ページで、前の手順で作成したSnapCenterサーバのURLとクライアント識別子を[識別子]セクションに入力します。

- a. [追加（Add）]をクリックします。

- b. 「*次へ*」をクリックします。

10. [Choose Access Control Policy]ページで、要件に基づいて制御ポリシーを選択し（[Permit Everyone and Require MFA]など）、*[Next]*をクリックします。

11. [アプリケーション権限の設定]ページでは、デフォルトでOpenIDがスコープとして選択されており、*[次へ]*をクリックします。

12. [概要]ページで、*[次へ]*をクリックします。

[完了]ページで、*[閉じる]*をクリックします。

13. [サンプルアプリケーションのプロパティ]ページで、*[OK]*をクリックします。

14. 承認サーバー(AD FS)によって発行され、リソースによって消費されることを意図したJWTトークン。

このトークンの「AUD」またはオーディエンス要求は、リソースまたはWeb APIの識別子と一致している必要があります。

15. 選択したWebAPIを編集し、コールバックURL（SnapCenterサーバURL）とクライアント識別子が正しく追加されていることを確認します。

ユーザー名を要求として提供するようにOpenID Connectを設定します。

16. サーバーマネージャの右上にある* Tools メニューの下にある AD FS Management *ツールを開きます。
 - a. 左側のサイドバーから* Application Groups *フォルダを選択します。
 - b. Web APIを選択し、* edit *をクリックします。
 - c. [発行トランスフォームルール]タブに移動します
17. [* ルールの追加 *] をクリックします。
 - a. [Claim rule template]ドロップダウンで、*[Send LDAP Attributes as Claims]*を選択します。
 - b. 「* 次へ *」 をクリックします。
18. [Claim rule]*の名前を入力します。
 - a. [属性ストア]ドロップダウンで*[Active Directory]*を選択します。
 - b. [LDAP Attribute]ドロップダウンで*を選択し、[O*utgoing Claim Type]*ドロップダウンで[UPN]*を選択します。
 - c. [完了] をクリックします。

PowerShellコマンドを使用してアプリケーショングループを作成します

PowerShellコマンドを使用して、アプリケーショングループ、Web APIを作成し、スコープと要求を追加できます。これらのコマンドは、自動スクリプト形式で使用できます。詳細については、<link to KB article>を参照してください。

1. 次のコマンドを使用して、AD FSに新しいアプリケーショングループを作成します。

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier  
-ApplicationGroupIdentifier $ClientRoleIdentifier
```

ClientRoleIdentifier アプリケーショングループの名前

redirectURL 許可後のリダイレクションの有効なURL

2. AD FSサーバアプリケーションを作成し、クライアントシークレットを生成します。

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"  
-ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL  
-Identifier $identifier -GenerateClientSecret
```

3. ADFS Web APIアプリケーションを作成し、使用するポリシー名を設定します。

```
$identifier = (New-Guid).Guid
```

```
Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
-Name "App Web API"
```

```
-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. クライアントIDとクライアントシークレットは1回しか表示されないため、次のコマンドの出力から取得します。

```
"client_id = $identifier"
```

```
"client_secret: "$($ADFSApp.ClientSecret)
```

5. AD FSアプリケーションにallatclaims権限とOpenID権限を付与します。

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
-ServerRoleIdentifier $identifier -ScopeNames @('openid')
```

```
$transformrule = @"
```

```
@RuleTemplate = "LdapClaims"
```

```
@RuleName = "AD User properties and Groups"
```

```
c:[Type ==
```

```
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer ==
```

```
"AD AUTHORITY"]
```

```
⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);
```

```
"@"
```

6. 変換ルールファイルを書き出します。

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii $relativePath = Get-Item .\issueancetransformrules.tmp
```

7. Web APIアプリケーションに名前を付け、外部ファイルを使用してその発行トランスフォームルールを定義します。

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier
```

```
$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile
```

```
$relativePath
```

アクセストークンの有効期限を更新します

アクセストークンの有効期限は、PowerShellコマンドを使用して更新できます。

- このタスクについて *
- アクセストークンは、ユーザー、クライアント、およびリソースの特定の組み合わせに対してのみ使用できます。アクセストークンは無効にすることはできず、有効期限が切れるまで有効です。
- デフォルトでは、アクセストークンの有効期限は60分です。この最小限の有効期限は十分であり、拡張されています。ビジネスクリティカルなジョブが継続的に発生しないように、十分な価値を提供する必要があります。
- ステップ *

アプリケーショングループWebAPIのアクセストークンの有効期限を更新するには、AD FSサーバで次のコマンドを使用します。

```
[+] Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"
```

AD FSからBearerトークンを取得します

RESTクライアント（Postmanなど）で以下のパラメータを入力する必要があります。ユーザークレデンシャルを入力するように求められます。さらに、ベアラートークンを取得するには、第2要素認証(あなたが持っているものとあなたがいるもの)を入力する必要があります。

[+] ベアラートークンの有効期間は、アプリケーションごとにAD FSサーバから設定できます。デフォルトの有効期間は60分です。

フィールド	価値
許可タイプ	承認コード
コールバックURL	コールバックURLがない場合は、アプリケーションのベースURLを入力します。
認証URL	[ADFS-domain-name]/ADFS/OAuth2/authorize
アクセストークンURL	[ADFS-domain-name]/ADFS/OAuth2/token
クライアント ID	AD FSクライアントIDを入力します
クライアントシークレット	AD FSクライアントシークレットを入力します
適用範囲	OpenID
クライアント認証	基本認証ヘッダーとして送信します

リソース	[詳細オプション]タブで、[コールバックURL]と同じ値を持つ[リソース]フィールドを追加します。この値は、JWTトークンでは「AUD」値として表示されません。
------	--

PowerShell、SCCLI、REST APIを使用してSnapCenterサーバでMFAを設定します

SnapCenter Serverでは、PowerShell、SCCLI、およびREST APIを使用してMFAを設定できます。

SnapCenter MFA CLI認証

PowerShellとSCCLIでは、既存のコマンドレット（Open-SmConnection）を「AccessToken」というもう一つのフィールドで拡張し、ベアートークンを使用してユーザを認証します。

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port <String>] [-RoleName <String>] [-AccessToken <string>]
```

上記のコマンドレットを実行すると、それぞれのユーザがSnapCenterコマンドレットを実行できるようにセッションが作成されます。

SnapCenter MFA REST API認証

REST <access token>クライアント(Postmanやswaggerなど)でBearerトークンを `_Authorization = Bearer _` の形式で使用し、ヘッダーにユーザRoleNameを指定すると、SnapCenterからの応答が成功します。

MFA REST APIワークフロー

MFAがAD FSで設定されている場合、REST APIを使用してSnapCenterアプリケーションにアクセスするには、アクセス (Bearer) トークンを使用して認証する必要があります。

- このタスクについて *
- Postman、Swagger UI、FireCampなど、任意のRESTクライアントを使用できます。
- アクセストークンを取得し、それを使用して以降の要求 (SnapCenter REST API) を認証し、あらゆる処理を実行します。
- 手順 *
- AD FS MFAを介して認証する場合*
 1. AD FSエンドポイントを呼び出してアクセストークンを取得するようにRESTクライアントを設定します。

ボタンを押してアプリケーションのアクセストークンを取得すると、AD FS SSOページにリダイレクトされ、ADクレデンシャルを入力してMFAで認証する必要があります。 1.[AD FS SSO]ページで、[ユーザー名]テキストボックスにユーザー名または電子メールを入力します。

[+] ユーザ名は、user@domainまたはdomain\userの形式で指定する必要があります。

1. [パスワード]テキストボックスにパスワードを入力します。

2. *ログイン*をクリックします。
3. [サインインオプション]*セクションで、認証オプションを選択し、（設定に応じて）認証します。
 - プッシュ：電話機に送信されるプッシュ通知を承認します。
 - QRコード: AUTH Pointモバイルアプリを使用してQRコードをスキャンし、アプリに表示される認証コードを入力します
 - ワンタイムパスワード: トークンのワンタイムパスワードを入力します。
4. 認証が成功すると、Access、ID、およびRefresh Tokenを含むポップアップが開きます。
アクセストークンをコピーし、SnapCenter REST APIでを使用して操作を実行します。
5. REST APIでは、ヘッダーセクションでアクセストークンとロール名を渡す必要があります。
6. SnapCenterは、AD FSからこのアクセストークンを検証します。
有効なトークンである場合、SnapCenterはそれをデコードし、ユーザー名を取得します。
7. SnapCenterは、ユーザー名とロール名を使用して、API実行のためにユーザーを認証します。
認証に成功した場合、SnapCenterは結果を返します。成功しなかった場合は、エラーメッセージが表示されます。

REST API、CLI、GUIのSnapCenter MFA機能を有効または無効にします

- GUI *
- 手順 *
 1. SnapCenter管理者としてSnapCenterサーバにログインします。
 2. >[グローバル設定]>[MultiFactorAuthentication（MFA）設定]*をクリックします
 3. インターフェイス（GUI/REST API/CLI）を選択してMFAログインを有効または無効にします。
- PowerShellインターフェイス*
- 手順 *
 1. PowerShellまたはCLIコマンドを実行して、GUI、REST API、PowerShell、SCCLIのMFAを有効にします。


```
Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled -IsCliMFAEnabled -Path
```

pathパラメータは、AD FS MFAメタデータXMLファイルの場所を指定します。

指定したAD FSメタデータファイルパスを使用して設定されたSnapCenter GUI、REST API、PowerShell、およびSCCLIのMFAを有効にします。

 1. を使用して、MFAの設定のステータスと設定を確認します Get-SmMultiFactorAuthentication コマンドレット。
- SCCLIインターフェイス*
- 手順 *

1. # sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true
-IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path
"C:\ADFS_metadata\abc.xml"
2. # sccli Get-SmMultiFactorAuthentication

• REST API *

1. GUI、REST API、PowerShell、SCCLIでMFAを有効にするには、次のPOST APIを実行します。

パラメータ	価値
要求されたURL	/api/4.9/settings/multifactorauthentication
HTTP メソッド	ポスト
リクエストボディ	{ "IsGuiMFAEnabled" : false、 "IsRestApiMFAEnabled" : true、 "IsCliMFAEnabled" : false、 "ADFSConfigFilePath" : "C :\ADFS_METADATA\abc.xml" }
応答本文	{ "MFAConfiguration" : { "IsGuiMFAEnabled" : false、 "ADFSConfigFilePath" : "C :\ADFS_METADATA\abc.xml"、 "SCConfigFilePath" : null、 "IsRestApiMFAEnabled" : true、 "IsCliMFAEnabled" : false、 "ADFSHostName" : " win-ads-sc49.winscedom2.com } }

2. 以下のAPIを使用してMFA構成のステータスと設定を確認します。

パラメータ	価値
要求されたURL	/api/4.9/settings/multifactorauthentication
HTTP メソッド	ゲット
応答本文	{ "MFAConfiguration" : { "IsGuiMFAEnabled" : false、 "ADFSConfigFilePath" : "C :\ADFS_METADATA\abc.xml"、 "SCConfigFilePath" : null、 "IsRestApiMFAEnabled" : true、 "IsCliMFAEnabled" : false、 "ADFSHostName" : " win-ads-sc49.winscedom2.com } }

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。