SnapCenterサーバのインストールの準備

SnapCenter Software 5.0

NetApp
July 18, 2024

目次

SnapCenterサーバのインストールの準備

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。ワークグループとドメインの両方の場合、インストールに使用するユーザーには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を持つ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、Active Directoryドメインと信頼に関するMicrosoftの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と、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更新プログラムを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 英語版、ドイツ語版、日本語版、簡体字中国語版のみがサポートされています。 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"。
最小CPU数	4コア

項目	要件
最小RAM	8 GB MySQL Serverのバッファプールは、RAMの合計容量の20%を使用します。
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と同じドライブにSnapCenterリポジトリがある場合は、10 GBを使用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	• Microsoft .NET Framework 4.7.2以降 • Windows Management Framework（WMF）4.0以降 • PowerShell 4.0以降 用。 NET固有のトラブルシューティング情報。を参照してください。 "インターネットに接続されていないレガシーシステムでは、SnapCenter のアップグレードまたはインストールが失敗します"

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。

- ホストユーティリティ

  Host UtilitiesはFCとiSCSIをサポートしており、WindowsサーバでMPIOを使用できます。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、NetAppとWindows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とアプリケーション

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Amazon FSx for NetApp ONTAPをサポートしており、SnapCenterソフトウェア4.5 P1パッチリリースからデータを保護します。

  Amazon FSx for NetApp ONTAPを使用している場合は、データ保護処理を実行するために、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してください。

  Amazon FSx for NetApp ONTAP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は、さまざまなアプリケーションやデータベースの保護をサポートしています。

  サポートされているアプリケーションと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"。

- 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

  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

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"。

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1つの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に干渉し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	デフォルトポート
SnapCenterポート	8146（HTTPS）、URL _\https://server:8146_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	デフォルトポート
SnapCenter SMCore通信ポート	8145（HTTPS）、双方向、カスタマイズ可能 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。 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。"
MySQLのポート	3306（HTTPS）、双方向 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。 SnapCenterサーバからMySQLサーバへのセキュアな接続を確立できます。 "詳細" 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。"
Windowsプラグインホスト	135、445（TCP） ポート135と445に加えて、Microsoftが指定したダイナミックポート範囲もオープンにする必要があります。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。 サポートされ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" 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、インストール後に閉じることができます。

ポートのタイプ	デフォルトポート
LinuxまたはAIXプラグインホスト	22（SSH） 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。
SnapCenter Plug-ins Package for Windows 、SnapCenter Plug-ins Package for Linux 、SnapCenter Plug-ins Package for AIX	8145（HTTPS）、双方向、カスタマイズ可能 このポートは、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す。 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。 ポートをカスタマイズするには、またはを参照してください。 "ホストを追加してSnapCenter Plug-in for Microsoft Windowsをインストールする" "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。"
SnapCenter Plug-in for Oracle Database	27216、カスタマイズ可能 デフォルトのJDBCポートは、Oracleデータベースへの接続にOracle用プラグインで使用されます。 ポートをカスタマイズするには、を参照してください。 "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。"
SnapCenter 用のカスタムプラグイン	9090 （ HTTPS ）、固定 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す。ファイアウォールの例外は必要ありません。 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。

ポートのタイプ	デフォルトポート
ONTAPクラスタまたはSVMの通信ポート	443（HTTPS）、bidirectional80（HTTP）、bidirectional 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 のスペルチェックポート	3instance_number13または3instance_number15、HTTPまたはHTTPS、双方向、カスタマイズ可能 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、ポート番号は13で終わります。MDC以外の場合、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	認証が正しく機能するために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については、Microsoftのドキュメントを参照してください。 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には、を参照してください "プラグインホストの変更"。

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、仮想マシンのデータ保護を実現するために複数のライセンスが必要です。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。

ライセンス	必要な場合
SnapCenter Standard（コントローラベース）	FAS、AFF、オールSANアレイ（ASA）に必要 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に含まれています。SnapManager Suiteライセンスをお持ちの場合は、SnapCenter Standardライセンスの使用権も取得できます。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。 SnapCenterは、Data Protection Bundleの一部としても提供されます。A400以降を購入済みの場合は、Data Protection Bundleを購入する必要があります。
SnapCenter Standard（容量ベース）	ONTAP SelectトCloud Volumes ONTAPニヒツヨウ Cloud Volumes ONTAPまたはONTAP Selectをご利用の場合は、SnapCenterの管理データに基づいて容量ベースのライセンスをTB単位で購入する必要があります。SnapCenterには、容量ベースのSnapCenter Standard 90日間試用版ライセンスがデフォルトで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。
SnapMirrorまたはSnapVault	ONTAP SnapCenterでレプリケーションが有効になっている場合は、SnapMirrorまたはSnapVaultのいずれかのライセンスが必要です。
SnapRestore	バックアップのリストアと検証に必要です。 フライマリストレエシシステム • リモート検証を実行し、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には、SnapMirrorデスティネーションシステムに必要です。

ライセンス	必要な場合
FlexClone	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。 フライマリストレシシステムトセカンタリストレシシステム • セカンダリバックアップからクローンを作成するには、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	• LUNのiSCSIまたはFCライセンス • SMB共有用のCIFSライセンス • NFSタイプのVMDK用のNFSライセンス • VMFSタイプのVMDK用のiSCSIまたはFCライセンス ソースボリュームを使用できない場合に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。
SnapCenter Standardライセンス（オプション）	セカンダリデスティネーション 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 Standard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で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。

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、またはを参照してください "SnapCenter Standardコントローラベースライセンスを追加" "SnapCenter Standard容量ベースライセンスを追加"。

Single Mailbox Recovery（SMBR）ライセンス

SnapCenter Plug-in for Exchangeを使用してMicrosoft Exchange Serverデータベースおよびsingle Mailbox Recovery（SMBR）を管理する場合は、SMBR用の追加ライセンスが必要です。このライセンス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

クレデンシャルで使用される認証方法は、アプリケーションや環境に応じて異なります。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に使用するクレデンシャルとデータ保護処理に使用するクレデンシャルをそれぞれ1組ずつ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。

信頼されていないドメイン認証

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に対するWindows認証は、Windowsクレデンシャルの作成時に実行されるのではなく、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完了し、リソースを更新する必要があります。SQL Server認証は、SQL Serverでのスケジュール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 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、AIXホストを追加し、SnapCenter Plug-ins Package for AIXをSnapCenter GUIからリモートで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）認証が無効になっている場合は、Oracleデータベースで処理を実行するためにOracleデータベース認証が必要になります。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インスタンスにアクセスする必要があり、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は、Oracle ASM認証が必要です。そのため、Oracle ASMの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ユーザを作成しておく必要があります。

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た場合は、RMANカタログ認証を追加する必要があります。

ストレージ接続とクレデンシャル

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サーバと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 *

  ストレージ接続により、SnapCenter ServerプラグインとSnapCenterプラグインはONTAPストレージにアクセスできます。これらの接続の設定には、AutoSupportおよび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。ユーザ名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、ユーザ名に完全なadmin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の権限を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。

タスクの内容

- 同じAD FSで他のアプリケーションが設定されている場合、SnapCenterはSSOベースのログインをサポートします。一部のAD FS構成では、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"。

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サーバと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にする必要があります。
- SnapCenterサーバ用に許可された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）中に自己署名証明書が再作成されないようにすることで、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ファイルの生成"。

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. FQDN >/FederationMetadata/2007-06/FederationMetadata.xmlからAD FSフェデレーションメタデータファイルをダウンロードし "https://<host ます。
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パラメータには、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ホストにコピーして、SnapCenterをクライアントエンティティとして設定します。
7. コマンドレットを使用して、SnapCenterサーバのMFAを有効にします `Set-SmMultiFactorAuthentication` 。
8. （オプション）コマンドレットを使用して、MFAの設定ステータスと設定を確認します `Get-SmMultiFactorAuthentication` 。
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. Permissionsウィザードで、次の手順を実行します。
      i. [追加]*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。

       SnapCenterが、指定した表示名の証明書利用者として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. [ルールの追加]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. [Endpoints]、[Identifiers]、および[Signature]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メタデータの更新

アップグレード、CA証明書の更新、DRなど、AD FSサーバで変更があった場合は、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. FQDN >/FederationMetadata/2007-06/FederationMetadata.xmlからAD FSフェデレーションメタデータファイルをダウンロードし "https://<host ます。"
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で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メタデータの更新

ADFSサーバで修復、CA証明書の更新、DRなどの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。

      証明書利用者信頼のユーザ定義名が表示されます。

   c. 多要素認証（MFA）を有効にします。

      を参照して "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、コマンドレットを使用して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` 。
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]*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、ユーザ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	値
付与タイプ	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す。

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1つのフィールドで拡張し、ベアラ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、[Username]テキストボックスにユーザ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、ユーザ名とロール名を使用して、API実行のためにユーザを認証します。

   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/RST 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. コマンドレットを使用して、MFAの設定ステータスと設定を確認します `Get-SmMultiFactorAuthentication` 。
- 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	値
要求されたURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	投稿
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"、"SCConfigFileP ath"：null、"IsRestApiMFAEnabled"：true 、"IsCliMFAEnabled"：false、 "ADFSHostName" ：" win-adfs-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	値
要求されたURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	取得
応答本文	{"MFAConfiguration"： {"IsGuiMFAEnabled " ：false、"ADFSConfigFilePath"："C ：\\ADFS_METADATA\\abc.xml"、"SCConfigFileP ath"：null、"IsRestApiMFAEnabled"：true 、"IsCliMFAEnabled"：false、 "ADFSHostName" ：" win-adfs-sc49.winscedom2.com}

著作権に関する情報

商標に関する情報