SnapCenter
サーバをインストールする準備をします
SnapCenter Software 4.8

NetApp
January 18, 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）を管理します。 . . . 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	• Microsoft .NET Framework 4.7.2以降 • Windows Management Framework （ WMF ） 4.0 以降 • PowerShell 4.0 以降 **NET**固有の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 "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"。 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"。

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"。

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 _\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	デフォルトのポート
SnapCenter SMCore の通信ポート	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 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作成できます。 "詳細はこちら。"
Windows プラグインホスト	135 、 445 （ TCP ） 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。 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" 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。
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。

ポートのタイプ	デフォルトのポート
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	8145 （ HTTPS ）、双方向、カスタマイズ可能 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、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。"
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 データベースに接続するためにプラグイン for Oracle 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 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。 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。
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。

ポートのタイプ	デフォルトのポート
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	FAS およびAFF に必要です 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 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 または AFF ストレージを使用した SnapCenter の試用版をインストールする場合は、営業担当者にお問い合わせください。 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。
SnapCenter - 容量ベース	ONTAP Select および Cloud Volumes ONTAP で必要です 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。
SnapMirror または SnapVault	ONTAP 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。
SnapRestore	バックアップのリストアおよび検証に必要です。 プライマリストレージシステム • 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	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。 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。 • 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	• 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 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。
SnapCenter 標準ライセンス（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 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。

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で必要です。 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）を管理します。

このトピックでは、Active Directoryフェデレーションサービス(AD FS)サーバーとSnapCenter サーバーで多要素認証(MFA)機能を管理する方法について説明します。

多要素認証（MFA）を有効にする

このトピックでは、Active Directoryフェデレーションサービス(AD FS)サーバーとSnapCenter サーバーでMFA機能を有効にする方法について説明します。

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"。

必要なもの

- 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 -Enable -Path` コマンドレット。

   pathパラメータでは、手順3でSnapCenter サーバにコピーされたAD FS MFAメタデータXMLファイルの場所を指定します。

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://<host fqdn>/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 -Disable` 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。

著作権に関する情報

商標に関する情報