SupportAssist Enterprise バージョン 4.0

ユーザーズ ガイド

DELL EMC

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その危険を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

2020 - 01

Rev. A03

目次

1

概要

SupportAssist Enterprise は、Dell EMC サーバー、ストレージ、およびネットワーキング デバイスのテクニカル サポートを自動化するアプリケーションです。SupportAssist はお使いのデバイスを監視し、発生する可能性のあるハードウェアの問題をプロアクティブに検知します。サービス契約に応じて、SupportAssist は監視対象デバイスで検出された問題に対するサポートリクエストの作成も自動化します。

メモ: この文書では、ローカルシステムとは SupportAssist Enterprise が導入されているサーバーを指し、リモートデバイスとはお使いの環境内の他のデバイスを指します。

ハードウェアの問題が検出されると、SupportAssist は問題のトラブルシューティングに必要なシステム状態情報を自動的に収集するか、または収集はデバイス自体によって自動的にバックエンドに送信されます。収集されたシステム情報は、テクニカル サポートがより高度で個別化された効率的なサポートを提供するために役立ちます。SupportAssist の機能には、問題の解決に役立つテクニカル サポートからのプロアクティブな対応も含まれます。

また、SupportAssist は、OpenManage Enterprise を使用して管理しているデバイスで発生するハードウェアの問題を監視することができます。

トピック：

SupportAssist Enterprise の仕組み

SupportAssist Enterprise がセットアップされ、デバイスが正しく設定されている場合、SupportAssist はハードウェアイベントがデバイスで発生するたびにアラートを受信します。アラートはさまざまなポリシーを使ってフィルターされ、そのアラートが新しいサポートケースの作成、または既存のサポートケースのアップデートに十分であるかどうかが判断されます。それらに値するアラートは、サポートケースの作成、または既存サポートケースのアップデートを行うために、バックエンドにセキュアに送信されます。サポートケースが作成またはアップデートされた後、SupportAssist はデバイスからシステム情報を収集してそれをバックエンドに送信します。また、アラートが生成されたときに、一部のデバイスは情報をバックエンドに直接送信します。テクニカル サポートは、システム情報を使用して問題をトラブルシューティングし、適切なソリューションを提供します。

メモ: SupportAssist のケースの自動作成とシステム情報収集機能を体験するには、登録を完了する必要があります。

メモ: SupportAssist は、監視対象デバイスから受け取ったアラートすべてに対してサポートケースを作成するわけではありません。サポートケースが作成されるのは、対象がアクティブなサービス契約のあるデバイスで、なおかつデバイスから受け取ったアラートのタイプと件数がサポートケース作成に対してデルが定義した条件と一致した場合のみです。

メモ: SupportAssist は、サポートケース、デバイスステータス、ネットワーク接続性ステータスなどに関する自動 E メール通知を送信します。さまざまな E メール通知についての情報は、「電子メール通知のタイプ」を参照してください。

SupportAssist Enterprise によって収集されるシステム情報

SupportAssist Enterprise は、管理対象ハードウェアおよびソフトウェア デバイスの構成情報と使用情報を継続的に監視します。Dell EMC は、このプログラムに関連してお客様の個人ファイル、Web 閲覧履歴、Cookie などの個人情報にアクセスまたは収集することを想定していませんが、誤って収集または表示された個人システム情報は Dell.com/privacy でご覧いただける Dell プライバシーポリシーに従って処理されます。

収集されたシステム情報ログに暗号化されている情報には、次のカテゴリのデータが含まれています。

- **ハードウェアとソフトウェアのインベントリ** — 取り付けられたデバイス、プロセッサ、メモリ、ネットワークデバイス、使用状況、およびサービスタグ
- **サーバに対するソフトウェア設定** — オペレーティングシステム、およびインストールされたアプリケーション

- **設定情報** — インタフェース、VLAN、データセンターブリッジング (DCB)、スパニングツリー、およびスタッキング
- **ID 情報** — システム名、ドメイン名、および IP アドレス
- **イベントデータ** — Windows イベントログ、コアダンプ、およびデバッグログ

SupportAssist によって収集されたシステム情報にアクセスして表示することもできます。収集したシステム情報の表示については、「[デバイス] ページからコレクションを表示」を参照してください。

デフォルトでは、SupportAssist は、デバイスのサービス契約に関係なく、すべてのデバイスからシステム情報を収集し、そのシステム情報を安全にバックエンドに送信します。システム情報収集は一度にデバイス 1 台ずつ、**環境設定** ページで指定された事前定義済みの収集開始日時に基づいて実行されます。

メモ: 会社のセキュリティ ポリシーによって収集システム情報の一部を社内ネットワーク外へ送信することが制限されている場合、お使いのデバイスから特定システム情報の収集を除外するように、SupportAssist を設定することができます。特定のシステム情報の収集を除外する方法については、「ID 情報の収集を有効化または無効化」および「システム情報の収集を有効化または無効化」を参照してください。

Dell EMC サービス契約で使用できる SupportAssist Enterprise 機能

次の表では、ProSupport、ProSupport Plus、ProSupport Flex for Data Center、または ProSupport One for Data Center サービス契約で使用できる SupportAssist Enterprise 機能を比較しています。

メモ: 登録を完了することは、お使いの Dell EMC デバイスで SupportAssist Enterprise のメリットをすべて受けるための前提条件です。SupportAssist Enterprise の登録の詳細については、「SupportAssist Enterprise の登録」を参照してください。

表 1. SupportAssist Enterprise の機能と Dell サービス契約

SupportAssist Enterprise の機能	説明	Basic Hardware	ProSupport	ProSupport Plus、ProSupport Flex for Data Center、または ProSupport One for Data Center
ハードウェア障害のプロアクティブな検知	SupportAssist Enterprise は、監視対象デバイスで発生するハードウェアイベントのアラートを受信し、そのアラートがハードウェア障害を示すものかどうかをプロアクティブに判断します。	✓	✓	✓
ハードウェア障害の予測検知*	監視対象デバイスから収集されたシステム情報のインテリジェントな分析は、将来発生する可能性のあるハードウェアの問題を予測するために使用されます。	✗	✗	✓
システム情報の自動収集	不具合のトラブルシューティングに必要なシステム情報は、監視対象デバイスから自動的に収集され、DEll EMC バックエンドに安全に送信されます。	✓	✓	✓
サポートケースの自動作成	ハードウェア障害がプロアクティブまたは予測的に検出された場合、テクニカル サポートでサポート ケースが自動的に作成されます。	✗	✓	✓
自動電子メール通知	サポート ケースまたは問題に関する E メール通知は、会社の一次および二次連絡先に自動的に送信されます。	✗	✓	✓
テクニカルサポートからのプロアクティブな対応	テクニカルサポート担当者がサポートケースについてプロアクティブに連絡し、問題を解決するお手伝いをします。	✗	✓	✓
プロアクティブ部品発送	収集されたシステム情報の分析後に、テクニカル サポート担当者が不具合の解決には部品の交換が必要であると判断した場合、	✗	✓	✓

SupportAssist Enterprise の機能	説明	Basic Hardware	ProSupport	ProSupport Plus、ProSupport Flex for Data Center、または ProSupport One for Data Center
	SupportAssist Enterprise で設定した発送プリファランスに基づいて交換パーツが発送されます。			

メモ: SupportAssist Enterprise は、Dell EMC Basic Hardware サービス契約を持つデバイスでもハードウェアの問題を検知します。ただし、Basic Hardware サービス契約を持つデバイスに対しては、サポートケースが自動的に作成されません。

* ハードウェア障害の予測検知は、PowerEdge RAID Controller (PERC) シリーズ 5 からシリーズ 10 までを搭載する、第 12 世代以降の PowerEdge サーバのバッテリ、ハードドライブ、バックプレーン、およびエキスパンダにのみ適用されます。ハードウェア障害の予測検知は、自動定期収集とシステム情報のアップロードが SupportAssist Enterprise で有効になっている場合にのみ使用可能です。

2

SupportAssist Enterprise のダウンロード

SupportAssist Enterprise は、OVF と VHD の形式で使用できます。お使いの Hypervisor に応じて、必要な形式をダウンロードして導入することができます。SupportAssist Enterprise をダウンロードするには、ビジネス エンタープライズ アカウントを持っている必要があります。ビジネス エンタープライズ アカウントを使用すると、他の関連するソフトウェアのダウンロードおよび SupportAssist Enterprise で使用可能なサポート ページにアクセスすることもできます。

ビジネス エンタープライズ アカウントを持っていない場合は、SupportAssist Enterprise のダウンロード時にアカウントを作成することができます。また、既存のアカウントをビジネス エンタープライズ アカウントにアップグレードすることもできます。

トピック：

SupportAssist Enterprise のダウンロード

前提条件

ビジネス エンタープライズ アカウントを持っている必要があります。ビジネス エンタープライズ アカウントを持っていない場合は、ビジネス エンタープライズ アカウントの作成と SupportAssist Enterprise のダウンロードを参照してください。既存のアカウントをビジネス エンタープライズ アカウントにアップグレードして SupportAssist Enterprise をダウンロードするには、「ビジネス エンタープライズ アカウントへのアップグレードと SupportAssist Enterprise のダウンロード」を参照してください。

手順

1. https://www.dell.com/SAE-v4 に移動します。
2. **[ログイン]** をクリックします。
   「**サインイン**」ページが表示されます。
3. E メール アドレスとパスワードを入力して**サイン イン**をクリックします。
   「Dell EMC SupportAssist Enterprise バージョン 4.0 - Virtual Edition」ページに、SupportAssist Enterprise をダウンロードしてアクセス キーを生成するためのリンクが表示されます。
4. **[キーの生成]** をクリックします。
   「**キーの生成**」ページがデバイスのサイト詳細とともに表示されます。
5. 必要なサイトを選択します。
6. 4 桁の PIN を入力して、**キーの生成**をクリックします。
   アクセスキーが生成され、E メール アドレスに送信されます。
7. **完了** をクリックします。

   メモ: アクセス キーと PIN は 7 日間有効です。アクセス キーと PIN を使用して SupportAssist Enterprise の登録を完了します。
8. **ファイルのダウンロード** をクリックします。

タスクの結果

SupportAssist Enterprise のパッケージがダウンロードされます。

ビジネス エンタープライズ アカウントの作成と SupportAssist Enterprise のダウンロード

手順

1. https://www.dell.com/SAE-v4 に移動します。
2. **[ログイン]** をクリックします。
   「**サインイン**」ページが表示されます。
3. **[アカウントの作成]** セクションで、必要な詳細を入力し、**[アカウントの作成]** をクリックします。
4. 確認メールが E メール アドレスに送信されます。E メールの **[E メールの検証]** リンクをクリックします。
   OTP が E メール アドレスに送信され、OTP の検証プロセスを完了するようプロンプトが出されます。
5. OTP を入力して、**[送信]** をクリックします。
   アカウントが検証され、ビジネス エンタープライズ アカウントを作成するプロセスが開始されます。
6. バックエンドに組織プロファイルが存在しない場合は、ビジネス エンタープライズ アカウントを作成するようプロンプトが出されます。次の手順を実行します。
   a) **[Dell EMC 製品またはサービスを所有しています]** を選択し、**[次へ]** をクリックします。
   b) 組織の資格情報を入力し、**[次へ]** をクリックします。
      ビジネス エンタープライズ アカウントが作成されます。
   c) **[ログイン]** をクリックして、ビジネス エンタープライズ アカウントの E メール アドレスとパスワードを入力し、**[サインイン]** をクリックします。
      SupportAssist Enterprise をダウンロードし、アクセス キーを生成するリンクが表示されます。
7. バックエンドに組織プロファイルが存在する場合、組織を選択するようプロンプトが出されます。次の手順を実行します。
   a) 組織の国および連絡先の詳細を入力します。
   b) 使用する言語を選択します。
   c) **送信** をクリックします。
   d) 表示された結果から組織を選択し、**[送信]** をクリックします。
      ビジネス エンタープライズ アカウントが作成されます。
8. **[キーの生成]** をクリックします。
   「**キーの生成**」ページがデバイスのサイト詳細とともに表示されます。
9. 必要なサイトを選択します。
10. 4 桁の PIN を入力して、**キーの生成**をクリックします。
    アクセスキーが生成され、E メール アドレスに送信されます。
11. **完了** をクリックします。

    メモ: アクセス キーと PIN は 7 日間有効です。アクセス キーと PIN を使用して SupportAssist Enterprise の登録を完了します。
12. **ファイルのダウンロード** をクリックします。

タスクの結果

SupportAssist Enterprise のパッケージがダウンロードされます。

ビジネス エンタープライズ アカウントへのアップグレードと SupportAssist Enterprise のダウンロード

手順

1. https://www.dell.com/SAE-v4 に移動します。
2. **[ログイン]** をクリックします。
   「**サインイン**」ページが表示されます。
3. E メール アドレスとパスワードを入力して**サイン イン**をクリックします。
   「Dell EMC SupportAssist Enterprise バージョン 4.0 - Virtual Edition」ページに、SupportAssist Enterprise をダウンロードしてアクセス キーを生成するためのリンクが表示されます。
4. **[ビジネス アカウントの登録]** をクリックします。

5. バックエンドに組織プロファイルが存在しない場合は、ビジネス エンタープライズ アカウントを作成するようプロンプトが出されます。次の手順を実行します。
   a) **[Dell EMC 製品またはサービスを所有しています]** を選択し、**[次へ]** をクリックします。
   b) 組織の資格情報を入力し、**[次へ]** をクリックします。
      ビジネス エンタープライズ アカウントが作成されます。
   c) **[ログイン]** をクリックして、ビジネス エンタープライズ アカウントの E メール アドレスとパスワードを入力し、**[サインイン]** をクリックします。
      SupportAssist Enterprise をダウンロードし、アクセス キーを生成するリンクが表示されます。
6. バックエンドに組織プロファイルが存在する場合、組織を選択するようプロンプトが出されます。次の手順を実行します。
   a) 組織の国および連絡先の詳細を入力します。
   b) 使用する言語を選択します。
   c) **送信** をクリックします。
   d) 表示された結果から組織を選択し、**[送信]** をクリックします。
      ビジネス エンタープライズ アカウントが作成されます。
7. **[キーの生成]** をクリックします。
   「**キーの生成**」ページがデバイスのサイト詳細とともに表示されます。
8. 必要なサイトを選択します。
9. 4 桁の PIN を入力して、**キーの生成**をクリックします。
   アクセスキーが生成され、E メール アドレスに送信されます。
10. **完了** をクリックします。

    メモ: アクセス キーと PIN は 7 日間有効です。アクセス キーと PIN を使用して SupportAssist Enterprise の登録を完了します。
11. **ファイルのダウンロード** をクリックします。

タスクの結果

SupportAssist Enterprise のパッケージがダウンロードされます。

3

SupportAssist Enterprise の導入

Dell EMC SupportAssist Enterprise は、ハイパーバイザー上に導入し、リソースを管理してダウンタイムを最小限に抑えるためのアプライアンスとして提供されています。VMware vSphere または Microsoft Hyper-V を使用してアプライアンスを導入することができます。この章では、導入の前提条件と最小要件についても説明します。

トピック：

SupportAssist Enterprise の導入および使用のための最小要件

次の項では、SupportAssist Enterprise を導入および使用するためのハードウェア、ソフトウェア、およびネットワークの最小要件を説明します。

ハードウェア要件

SupportAssist Enterprise の導入および使用のためのハードウェア要件は、次の内容に応じて異なります。

- 監視するデバイスの数
- システム情報のみの収集、またはシステム情報の監視と収集の両方で使用する SupportAssist Enterprise の機能

次の表は、SupportAssist Enterprise を導入するサーバー上のハードウェアの最小要件の概要を提供します。

表 2. SupportAssist Enterprise の導入および使用のためのハードウェア要件

デバイス	監視	システム情報の収集	プロセッサ	インストールされているメモリ（RAM）	ハードドライブ（空きスペース）
50 以下	はい	はい	4 コア	16 GB	140GB：シン プロビジョニング
50 ~ 4250	はい	はい	8 コア	16 GB	140GB：シン プロビジョニング

メモ: 環境内にある 100 台を超えるデバイスの監視には、指定されたハードウェア要件を満たすサーバーに SupportAssist Enterprise を導入することをお勧めします。100 台を超えるデバイスからの定期的なコレクションは、監視サーバーのプロセッサーやメモリーの使用率が高くなる可能性があります。リソースを他のアプリケーションと共有している場合、このようにリソース使用率が高くなると、監視サーバ上で実行されている他のアプリケーションに影響する可能性があります。

メモ: SupportAssist Enterprise を仮想環境に導入すると、プロセッサー、メモリー、I/O などのシステムのハードウェア リソースが仮想マシン間で共有されます。したがって、SupportAssist Enterprise が導入されている仮想マシンでは、より多くのハードウェア リソースを利用できます。パフォーマンスを最適化するには、SupportAssist Enterprise のハードウェア要件に従い、専用のプロセッサーとメモリを VM に割り当ててください。

共有、予約、制限設定を使用して VM に割り当てられるプロセッサー リソースの量を変更するには、次を参照してください。

- **ESX については、docs.vmware.com で、VMware vSphere ドキュメントの「CPU リソースの割り当て」を参照してください。**
- **Hyper-V については、msdn.microsoft.com で、「Hyper-V CPU スケジューリング」のブログ記事を参照してください。**
- **その他の仮想環境については、個別のマニュアルを参照してください。**

次の表には、複数のデバイス収集を実行するために SupportAssist Enterprise が動作するサーバのハードウェア最小要件の概要が記載されています。

表 3. 複数のデバイス収集を実行するためのハードウェア要件

デバイス	プロセッサ	インストールされているメモリ（RAM）	ハードドライブ（空きスペース）
デバイス 30 台以下	4 コア	16 GB	10GB
デバイス 50 台以下	4 コア	16 GB	40GB
デバイス 100 台以下	8 コア	16 GB	60 GB
デバイス 300 台以下	8 コア	16 GB	100GB

メモ: 導入、システムメンテナンス、コンサルティングの目的で複数のデバイス収集を実行すると、不規則な間隔でシステムリソースの利用率が高くなる可能性があります。

ソフトウェア要件

次のセクションでは、SupportAssist Enterprise を導入および使用するための Web ブラウザーとハイパーバイザーの要件について説明します。

ウェブブラウザ要件

SupportAssist Enterprise ユーザーインタフェースを表示するには、次のウェブブラウザのいずれかが必要です。

- Internet Explorer 10 以降
- Mozilla Firefox 31 以降
- Google Chrome 59 以降
- Microsoft Edge 38 以降

メモ: ウェブブラウザでトランスポート層セキュリティ（TLS）バージョン 1.1 以降が有効にされている必要があります。

メモ: Internet Explorer を使用して SupportAssist Enterprise を開きます。

- **セキュリティ タブで、アクティブスクリプト を有効にします。**
- **詳細設定 タブで、Web ページのアニメーションを再生する を有効にします。**

Hypervisor の要件

SupportAssist Enterprise を導入するには、次のいずれかの Hypervisor が必要です。

- VMware vSphere バージョン：
  - vSphere ESXi 6.5
  - vSphere ESXi 6.0
- Microsoft Hyper-V のサポート対象：
  - Windows Server 2012
  - Windows Server 2016

ネットワーク要件

SupportAssist Enterprise を導入するサーバーのネットワーク要件は、次のとおりです。

- インターネット接続 - 標準 1 GbE 以上のネットワーク。
- サーバーは次の宛先に接続して、**[グローバル サーバーとエンタープライズ サーバー]** への接続性を確保する必要があります。
  - **https://esrs3.emc.com**
  - **https://esrs3-core.emc.com**
  - **https://esrs3-dr.emc.com**
  - **https://esrs3-coredr.emc.com**
  - **https://esr3gduprd01.emc.com**

- **https://esr3gduprd02.emc.com**
- **https://esr3gduprd03.emc.com**
- **https://esr3gduprd04.emc.com**
- **https://esr3gduprd05.emc.com**
- **https://esr3gduprd06.emc.com**
- **https://esr3ghoprd01.emc.com**
- **https://esr3ghoprd02.emc.com**
- **https://esr3ghoprd03.emc.com**
- **https://esr3ghoprd04.emc.com**
- **https://esr3ghoprd05.emc.com**
- **https://esr3ghoprd06.emc.com**
- **https://esr3gscprd01.emc.com**
- **https://esr3gscprd02.emc.com**
- **https://esr3gscprd03.emc.com**
- **https://esr3gscprd04.emc.com**
- **https://esr3gscprd05.emc.com**
- **https://esr3gscprd06.emc.com**
- **https://esr3gckprd01.emc.com**
- **https://esr3gckprd02.emc.com**
- **https://esr3gckprd03.emc.com**
- **https://esr3gckprd04.emc.com**
- **https://esr3gckprd05.emc.com**
- **https://esr3gckprd06.emc.com**
- **https://esr3gckprd07.emc.com**
- **https://esr3gckprd08.emc.com**
- **https://esr3gckprd09.emc.com**
- **https://esr3gckprd10.emc.com**
- **https://esr3gckprd11.emc.com**
- **https://esr3gckprd12.emc.com**
- **https://esr3gspprd01.emc.com**
- **https://esr3gspprd02.emc.com**
- **https://esr3gspprd03.emc.com**
- **https://esr3gspprd04.emc.com**
- **https://esr3gspprd05.emc.com**
- **https://esr3gspprd06.emc.com**

- ローカルシステムが以下の接続先に接続できること。
  - **https://downloads.dell.com/*** - Dell OpenManage Server Administrator(OMSA)のダウンロード、および新しい SupportAssist Enterprise リリース情報、ポリシー ファイル、および製品サポート ファイルの受け取り時に使用します。

    メモ: downloads.dell.com ページでは、ダウンロードエクスペリエンスを向上させるために Akamai のサードパーティーベンダーが使用されています。
  - **https://sa-is.us.dell.com/***- TechDirect の統合に使用します。

    メモ: 登録時は、SupportAssist Enterprise は http://www.dell.com に接続を試み、https://www.dell.com にリダイレクトされることで、インターネットの接続を確認します。

次の表は、デバイスからシステム情報を監視し収集するためのネットワーク帯域幅の要件です。

表 4. ネットワーク帯域幅の要件

デバイス	監視	システム情報の収集	LAN の帯域幅*	WAN の帯域幅**
1	いいえ	はい	10 Mbps	5 Mbps
20	はい	はい	0.5 Gbps	10 Mbps
100 以下	はい	はい	0.5 Gbps	10 Mbps
300 以下	はい	はい	0.5 Gbps	10 Mbps
1000 以下	はい	はい	1 Gbps	20 Mbps
4000 以下	はい	はい	1 Gbps	20 Mbps

* 単一サイト内のデバイスのシステム情報を監視し収集するために必要なネットワーク帯域幅です。

** 複数のサイトにわたって分散されたデバイスのシステム情報を監視し収集するために必要なネットワーク帯域幅です。

Hyper-V での SupportAssist Enterprise の導入

前提条件

仮想マシンの仮想ディスクをホストする場所に、VHD ファイルが存在している必要があります。

手順

1. Hyper-V マネージャーを起動します。
2. **[アクション]** > **[新規]** > **[仮想マシン]** をクリックします。
   「新しい仮想マシン ウィザード」ウィンドウが表示されます。
3. **「開始する前に」**ページで、**[次へ]** をクリックします。
4. **「連絡先および配送先」**ページで、次を実行し、**[次へ]** をクリックします。
   a) 仮想マシンの名前を入力します。
   b) デフォルトでは、仮想マシンは `C:\ProgramData\Microsoft\Windows\Hyper-V` に格納されています。仮想マシンを別の場所に保存するには、**[仮想マシンを別の場所に保存]** を選択し、**[参照]** をクリックしてフォルダーを選択します。
5. **「世代の指定」**ページで、**[世代]** を選択し、**[次へ]** をクリックします。

   メモ: SupportAssist Enterprise は第 2 世代をサポートしていません。
6. メモリの**「割り当て」**ページで、起動メモリーを入力し、**[次へ]** をクリックします。

   メモ: 入力する必要がある最小起動メモリは 16384MB です。
7. **「ネットワークの設定」**ページで、**[接続]** リストからネットワーク アダプターを選択し、**[次へ]** をクリックします。
8. **「仮想ハード ディスクの接続」**ページで、**[既存の仮想ハード ディスクを使用]** を選択し、**[参照]** をクリックして VHD ファイルを選択し、**[次へ]** をクリックします。
9. **「サマリー」**ページに表示されている詳細を確認し、 **[完了]** をクリックします。
   仮想マシンが作成され、**[仮想マシン]** リストに表示されます。
10. 仮想マシンを右クリックして **[開始]** をクリックし、仮想マシンの電源をオンにします。
11. 仮想マシンを右クリックして、**[接続]**をクリックします。
    最初の起動プロセスが開始し、「YaST2」ウィンドウが表示されます。
12. 「YaST2」ウィンドウで、次の手順を実行します。
    a) **「ライセンス契約」**ページで、使用条件に同意し、F10 キーを押します。
    b) 地域とタイムゾーンを選択し、F10 キーを押します。
    c) root パスワードを入力し、F10 キーを押します。

       メモ: 複雑な root パスワードを使用することをお勧めします。パスワードには、少なくとも 1 つの大文字、1 文字の小文字、1 つの数字、1 つの特殊文字を含む 8 文字以上を指定できます。

       メモ: 導入後に初めて SupportAssist Enterprise にログインするには、この root パスワードを使用します。
    d) 管理者ユーザー名を入力し、F10 キーを押します。

       メモ: このユーザー名を使用して、root 認証情報を使用してログインした後、SupportAssist Enterprise にログインします。

    最初の起動処理が完了しました。ただし、導入プロセスを完了するには、ネットワーク設定を構成する必要があります。
13. ネットワーク設定を構成するには、次の手順を実行します。
    a) root 資格情報を使用して仮想マシンにログインし、`yast` を実行します。
    b) 「Yast Control Center」ページで、**[システム]** > **[ネットワーク設定]**に移動し、F10 キーを押します。
    c) F4 キーを押して、ネットワーク設定を編集します。
    d) 固定 IP アドレス、サブネット マスク、ホスト名を入力し、F10 キーを押します。

       メモ: SupportAssist Enterprise は、動的ホスト構成プロトコル (DHCP) をサポートしていません。
    e) ホスト名、ドメイン名、サーバー、およびドメイン検索情報を入力し、F10 キーを押します。
    f) デフォルトの IPv4 と IPv6 ゲートウェイの情報を入力し、F10 キーを押します。
    g) F9 キーを押して、「YaST2」ウィンドウを閉じます。

メモ: SupportAssist Enterprise ユーザー インターフェイスにログインするまで、10～15 分待機します。

VMware vSphere での SupportAssist Enterprise の導入

手順

1. サポート サイトから OVF ファイルをダウンロードして、VMware vSphere クライアントがアクセスできる場所にファイルを解凍します。
2. 右ペインで、**[VM の作成/登録]** をクリックします。
   「新しい仮想マシン」ウィンドウが表示されます。
3. **[作成タイプの選択]** ページで、**[OVF または OVA ファイルからの仮想マシンの導入]** を選択し、**[次へ]** をクリックします。
4. **「OVF および VMDK ファイルの選択」**ページで、仮想マシンの名前を入力し、OVF と VMDK ファイルを選択して、**[次へ]** をクリックします。
   「ストレージの場所」ページが表示されます。
5. ホストで使用可能なデータストアが複数ある場合は、**「ストレージの選択」**ページにそれらのデータストアが表示されます。仮想マシン（VM）ファイルを保存する場所を選択し、**[次へ]** をクリックします。
6. **「ライセンス契約」**ページで、使用許諾契約書を読み、 **[同意する]** をクリックして、**[次へ]** をクリックします。
7. **「導入オプション」**ページで、次の手順を実行します。
   a) **[ネットワーク マッピング]** リストから、導入テンプレートで使用する必要があるネットワークを選択します。
   b) **[ディスク プロビジョニング]** の場合は、 **[シン]** を選択します。
   c) **次へ** をクリックします。
8. **「追加の設定」**ページで、次の詳細を実行し、**[次へ]** をクリックします。
   - ドメイン名サーバー
   - ホスト名
   - デフォルトゲートウェイ
   - Network IPV4 および IPV6
   - タイムゾーン
   - root パスワード

     メモ: **複雑な root パスワードを使用することをお勧めします。パスワードには、少なくとも 1 つの大文字、1 文字の小文字、1 つの数字、1 つの特殊文字を含む 8 文字以上を指定できます。**

     メモ: **導入後に初めて SupportAssist Enterprise にログインするには、この root パスワードを使用します。**
   - ESRS Web 管理者ユーザー名
9. **「完了の準備」**ページで、表示された詳細を確認し、 **[完了]** をクリックします。
   導入が完了し、仮想マシンの電源がオンになると、メッセージが表示されます。

   メモ: **SupportAssist Enterprise ユーザー インターフェイスにログインするまで、10～15 分間待機する必要があります。**

4

SupportAssist Enterprise をお使いになる前に

SupportAssist Enterprise は、お使いのデバイスに対する Dell EMC のテクニカル サポートを自動化します。必要に応じて、1 つ以上のデバイスに SupportAssist Enterprise を導入してセットアップすることで、テクニカル サポートを自動化できます。

トピック：

SupportAssist Enterprise ユーザーインターフェイスを開く

手順

リモート システムから SupportAssist Enterprise にアクセスするには、Web ブラウザーを開き、次のように入力します。`https://<SupportAssist Enterprise がデプロイされているサーバーの IP アドレスまたはホスト名>: 5700/SupportAssist`

たとえば、https://10.25.35.1:5700/SupportAssist などです。

メモ: アドレスを入力する際は、SupportAssist の S と A を必ず大文字で入力してください。

- Internet Explorer を使用している場合は、メッセージ「**この Web サイトのセキュリティ証明書に問題があります**」が表示されます。SupportAssist Enterprise を開くには、**この Web サイトを続行します (推奨されません)** をクリックします。
- Mozilla Firefox を使用している場合は、次のメッセージが表示されます：「**この接続は信頼されません**」。SupportAssist Enterprise を開くには、**私はリスクを理解しています** をクリックしてから **例外を追加** をクリックします。**セキュリティの例外の追加** ウィンドウで **セキュリティの例外の確認** をクリックします。

SupportAssist Enterprise へのログイン

このタスクについて

SupportAssist Enterprise を導入して最初の起動設定を完了したら、ネットワーク内の任意のシステムから SupportAssist にログインできます。初めてログインするときは、ルート認証情報を入力し、管理者アカウントを作成してから SupportAssist Enterprise を登録してください。SupportAssist Enterprise を登録したら、管理者アカウントの認証情報を使用してログインできます。

手順

1. **https://<SAE IP>:5700/SupportAssist** に移動します。<SAE IP>は、SupportAssist Enterprise を導入した仮想マシンの IP アドレスです。
2. **ユーザー名** ボックスに `root` と入力します。
3. パスワードを入力します。

   メモ: SupportAssist Enterprise の導入時に、root アカウントに入力したのと同じパスワードを入力する必要があります。
4. **サインイン** をクリックします。
   ライセンス契約 ページが表示されます。
5. 利用規約を読み、**同意** をクリックします。

管理者アカウントの作成 ページが表示されます。

6. 次の手順を実行します。
   a) 管理者アカウントのユーザー名とパスワードを入力します。

   メモ: 管理者アカウントのユーザー名は大文字と小文字が区別され、導入時に設定されたものと同じである必要があります。

   b) **[管理者としてログイン]** をクリックします。

   SupportAssist Enteprise **のセットアップおよび設定** ウィザードの **ようこそ** ページが表示されます。

次の手順

SupportAssist Enterprise を登録します。登録せずに SupportAssist Enterprise を使用することはできません。「SupportAssist Enterprise の登録」を参照してください。

SupportAssist Enterprise の登録

このタスクについて

SupportAssist Enterprise に管理者としてログインした後、利点を十分に活用するには、SupportAssist Enterprise を登録する必要があります。SupportAssist を登録しない場合、ハードウェアの問題についてデバイスを監視したり、システム情報を自動的に収集したりすることはできません。

手順

1. **ようこそ** ページで **次へ** をクリックします。
   プロキシ設定 ページが表示されます。
2. お使いのシステムがプロキシ サーバー経由でインターネットに接続している場合は、次の手順を実行します。
   a) **プロキシサーバを使用する** を選択します。
   b) ホスト名または IP アドレスおよびポート番号を入力します。
   c) プロキシ サーバーに認証が必要な場合は、**[認証が必要]** を選択します。
   d) プロキシサーバーのユーザー名とパスワードを入力します。
   e) **接続テスト**をクリックしてプロキシ設定を確認します。
3. **次へ** をクリックします。
   認証 ページが表示されます。
4. SupportAssist Enterprise パッケージのダウンロード中に生成されたアクセス キーと PIN を入力します。
   アクセス キーと PIN を持っていない場合は、https://www.dell.com/SAE-v4 に移動して、新しいアクセス キーと PIN を作成します。
5. **次へ** をクリックします。
   連絡先 ページが表示されます。
6. 一次連絡先情報を入力します。

   メモ: SupportAssist Enterprise の登録後は、[設定] > [連絡先情報] ページから一次連絡先情報のアップデートに加え、二次連絡先情報の入力を行うこともできます。一次連絡先が使用できない場合、Dell EMC は二次連絡先を通して会社に連絡します。一次および二次連絡先の両方に有効な E メールアドレスが設定されている場合は、両方の連絡先に E メールを送信します。

7. **次へ** をクリックします。
   「Dell EMC **サーバーのパーツの交換設定 (オプション)**」ページが表示されます。
8. Dell EMC にご使用のサーバーの交換パーツを自動的に配送してもらう場合は、**[交換パーツを自動的に出荷する]** を選択し、一次および二次配送連絡先情報を入力します。

   メモ: 「連絡先」ページに入力された一次連絡先情報をコピーする場合は、[一次配送連絡先] セクションの上に表示されているリンクをクリックします。

9. **次へ** をクリックします。
   「**サマリー**」ページが表示され、一次連絡先およびパーツ発送情報の詳細が表示されます。
10. **終了** をクリックします。
    サイト正常性ページが表示されます。

次の手順

SupportAssist Enterprise から E メール通知を受信するように SMTP 設定を構成します。「SMTP サーバーを設定」を参照してください。

管理者パスワードのリセット

前提条件

SupportAssist Enterprise が導入されているサーバーへの root アクセス権限を持っている必要があります。

手順

1. root 認証情報を使用して、セキュア シェル (SSH) 経由でアプライアンスにログインします。
2. `docker exec -it esrsde-app bash` を実行します。
3. `cd /opt/esrs/webuimgmt-util` に移動します。
4. `.passwordAdmin.sh` を実行します。
   パスワードをリセットするようプロンプトが出されます。
5. 新しいパスワードを入力します。
6. 新しいパスワードを再入力します。

タスクの結果

新しい管理者アカウントのパスワードが保存されます。

SupportAssist Enterprise 製品情報

「About」ページには、SupportAssist Enterprise の製品情報、ホストの詳細、およびセットアップの詳細が表示されます。グローバル ページのメンテナンス モードを有効化または無効化したり、SupportAssist アプリケーションを「About」ページからオフライン モードに設定したりすることができます。メンテナンスモードの詳細については、「メンテナンス モードの概要」を参照してください。オフラインモードの詳細については、「オフライン モードの概要」を参照してください。

SupportAssist のヘッダー領域で、**About** をクリックして SupportAssist Enterprise の製品情報を表示します。

ネットワーク接続性テスト

このページでは、SupportAssist Enterprise の機能に影響を与えるサーバーへの接続ステータスを確認およびテストできます。ネットワーク接続テストでは、SupportAssist Enterprise が使用するポートは確認されません。

デフォルトでは、SupportAssist Enterprise は毎日午後 11 時 (SupportAssist Enterprise が導入されているサーバーでの時間) に依存リソースへの接続性を自動でテストし、**[ステータス]**列にその結果を表示します。依存リソースへの接続に不具合がある場合、E メールが一次および二次の連絡先に送信されます。また、依存サーバーに対する SupportAssist Enterprise 接続は、いつでもテストすることができます。

「ネットワーク接続性テスト」ページを表示するには、SupportAssist Enterprise ヘッダー領域で、***ユーザー名***をクリックし、**[ネットワーク接続性のテスト]**をクリックします。

次の表には、**ネットワーク接続テスト** ページに表示される情報が記載されています。

表 5. ネットワーク接続性テスト

行	説明
Test	テストできる依存ネットワークサーバーの種類を表示します。利用できるオプションは次のとおりです。 · **インターネット接続性** · **SMTP Server (SMTP サーバ)** · **グローバル サーバとエンタープライズ サーバ**
説明	各テストの目的を説明します。
ステータス	接続性ステータスを示すアイコンとメッセージを表示します。次のようなステータスがあります。

行	説明
	• **未設定**（SMTP サーバーテストのみに該当）- SMTP サーバーが SupportAssist Enterprise で設定されていません。社内で SMTP サーバーが使用されている場合は、SupportAssist Enterprise で **[SMTP 設定]**を行うことをお勧めします。「SMTP サーバーを設定」を参照してください。 • **進行中** - 接続性テストが進行中です。 • **接続済み** - 接続性テストに成功しました。 • **エラー** - 接続性テストに失敗しました。 **メモ: エラー のステータスがリンクとして表示され、そのリンクをクリックして問題の説明および解決のための手順を表示できます。**
最後の検証	接続性ステータスを最後に検証した日付と時刻を表示します。日付と時刻は、SupportAssist Enterprise が導入されているサーバーごとに表示されます。

SupportAssist Enterprise のテスト

SupportAssist Enterprise のテスト ページでは、SupportAssist Enterprise で特定のタスクを実行できるかどうかを検証できます。

次の表には、「**SupportAssist Enterprise のテスト**」ページに表示される情報が記載されています。

表 6. SupportAssist Enterprise のテスト

行	説明
Test	テスト可能な SupportAssist の機能
説明	テストの目的
ステータス	テストのステータスを示すアイコンとメッセージ
最後の検証	システムが最後に検証された日時

ケース作成機能をテスト

このタスクについて

[ケース作成] 機能をテストして、サポート ケースを自動的に作成する実際のアラートの前にサポート ケースの作成が機能していることを確認します。

手順

1. SupportAssist Enterprise のヘッダー領域で ***ユーザー名*** をクリックし、**[SupportAssist Enterprise のテスト]**をクリックします。**SupportAssist Enterprise のテスト** ページが表示されます。
2. **ケースの作成** を選択します。
3. **接続性のテスト** をクリックします。
   次のいずれかのステータスが表示されます。
   - **未検証** - サポート ケース作成タスクがテストされていません。
   - **進行中** - サポート ケース作成テストが進行中です。
   - **ケースを作成する準備ができました** - SupportAssist Enterprise でサポート ケースを作成できます。
   - **ケースを作成できません** - SupportAssist Enterprise はサポート ケースを作成できません。

SupportAssist サービス ステータス

SupportAssist Enterprise の一部として実行されている複数の RESTful およびコア サービスがあります。「**サービス ステータス**」ページに、これらのサービスとそのステータスがリストされます。

SupportAssist Enterprise ヘッダー領域で、***ユーザー名***リンクをクリックし、次に **[サービス ステータス]** をクリックして「**サービス ステータス**」ページを表示します。

次の表で、**[サービス ステータス]** ページに表示される情報について説明します。

表 7. サービス ステータス

行	説明
サービス	RESTful またはコア サービスの名前
ステータス	サービスのステータスを示すアイコン。次のいずれかが表示されます。 .  – サービスが実行中のとき .  – サービスが停止したとき .  – サービスが無効になったとき
説明	サービスの目的

SupportAssist Enterprise の評価

SupportAssist Enterprise には、監視とシステム情報収集機能の評価を有効または無効にすることができる、複数の設定があります。

監視機能の評価

SupportAssist Enterprise で一部の特定のデバイスまたはすべてのデバイスの監視を無効にすることができます。

特定のデバイスの監視を無効にすると、SupportAssist Enterprise では、そのデバイスから受信したアラートを処理しません。したがって、そのデバイスでハードウェアの問題が発生した場合でも、SupportAssist Enterprise は自動的にサポートケースを開きません特定のデバイスのモニタリングを無効にする手順については、「デバイス監視の有効化または無効化」を参照してください。

デバイスをメンテナンスモードにすると、特定のデバイスの監視を一時的に無効にすることができます。デバイスをメンテナンスモードにすると、SupportAssist Enterprise は計画されたメンテナンスアクティビティの実行中にそのデバイスから受信したアラートを処理しません。デバイスをメンテナンス モードにする手順については、「デバイスレベルのメンテナンスモードの有効化または無効化」を参照してください。

必要に応じて、すべてのデバイスをメンテナンスモードにすることによって SupportAssist Enterprise で全デバイスの監視を無効にすることができます。すべてのデバイスをメンテナンス モードにする手順については、「グローバルレベルのメンテナンスモードの有効化または無効化」を参照してください。

システム情報の収集機能評価

デフォルトでは、SupportAssist Enterprise によって定期的にすべてのデバイスからシステム情報が自動的に収集され、サポートケースが作成されたときにもデータは自動的に収集されます。収集されたシステム情報はデルにセキュアに送信されます。SupportAssist Enterprise がデバイスから収集したシステム情報については、「SupportAssist Enterprise によって収集されるシステム情報」を参照してください。

また、SupportAssist Enterprise によって収集されたシステム情報を表示することもできます。収集したデータの表示については、「収集の表示」を参照してください。

社内のセキュリティポリシーのため、収集されたシステム情報の社内ネットワーク外への送信が一部制限される場合は、SupportAssist Enterprise にある次の設定オプションを使用できます。

- すべてのデバイスからの ID 情報の収集を無効にすることができます。「ID 情報の収集を有効化または無効化」を参照してください。
- 特定のデバイスからのソフトウェア情報とシステムログの収集を無効にすることができます。「システム情報の収集を有効化または無効化」を参照してください。
- すべてのデバイスからのシステム情報の定期収集を無効にすることができます。「システム情報の定期収集を有効化または無効化」を参照してください。

- サポートケース作成時におけるシステム情報の自動収集を無効にすることができます。「サポート ケース作成時のシステム情報の自動収集を有効化または無効化」を参照してください。
- 収集のアップロードを防ぐこともできます。「収集された情報の自動アップロードを有効化または無効化」を参照してください。

メモ: ほとんどの場合、SupportAssist Enterprise によって収集されたシステム情報の全部または一部は、テクニカルサポートが不具合を正しく診断して適切な解決方法を提供するために必要となります。SupportAssist Enterprise のメリットを最大限に活用するためには、すべてのシステム情報収集オプションを有効にする必要があります。

5

サイト正常性

SupportAssist Enterprise では、デバイスの全体的なサイト正常性、接続性、ステータスを表示できます。サイト正常性には、サイトの最も重要な問題を識別して優先度をつけることができる、主要な接続結果情報が含まれます。

次の表で、**サイト正常性** ページに表示される情報について説明します。

表 8. サイト正常性

フィールド	説明
	進行中のアクティブなリモート セッションの数
	進行中のアクティブな Connect Home セッションの数
	SupportAssist Enterprise によって呼び出された REST API コールの数。
	SRS 仮想エンジンのステータス。次のステータスが表示されます。 • ✓ — 接続済 • ✗ — 切断
概要 メモ: **[概要] セクションは、SupportAssist Enterprise でデバイスを追加した後でのみ表示されます。SupportAssist Enterprise にデバイスが追加されていない場合は、デバイスを追加したり、複数のデバイスを検出したり、アダプターをセットアップしたりするリンクが表示されます。**	以下の状況におけるデバイス数のグラフィック表示。状況をクリックすると、**状況の詳細** セクションに追加の詳細を表示できます。 • **管理対象** — クリックすると、デバイスタイプに従って監視対象デバイスの数が表示されます。 • **ステージング** — クリックすると、グループ内のデバイスの問題と解決策が表示されます。 • **管理対象外** — クリックすると、サポート対象外、無効、およびオフラインのデバイスの数が表示されます。 • **非アクティブ** — クリックすると、非アクティブなデバイスの数が表示されます。
現在の SupportAssist の概要	SupportAssist Enterprise によって監視されているデバイスの数と未解決のサポートケースの数。 **管理対象デバイス** をクリックして **デバイス** ページを表示します。**ケース** をクリックして **ケース** ページを表示します。
デバイス検証	SupportAssist Enterprise で検出または追加されたデバイスの総数とサイト全体のインベントリ検証ステータスが表示されます。次のステータスが表示されます。 • ✓ **成功** - 接続性、収集機能、監視機能のテストが正常に行われたデバイスの数。 • ⛔ **失敗** - 接続性、収集機能、監視機能のテストが正常に行われなかったデバイスの数。 サイトインベントリの検証では、デバイスの合計数が SupportAssist Enterprise で追加または検出されたデバイスの合計数と一致しない場合があります。この差異はインベントリ検証が次の検証をサポートしていないために発生します。

フィールド	説明
	· アダプタ経由で SupportAssist Enterprise に追加されたデバイス · SNMP の手動設定を必要とするデバイス(ネットワークデバイスなど)
ネットワーク リソース	以下のネットワークリソースへの SupportAssist Enterprise 接続の状況は次のとおりです。 · **Dell EMC Enterprise サーバー** · **Dell EMC グローバル アクセス サーバー** · **SMTP Server (SMTP サーバ)**

6

デバイスの追加

デバイスの追加により、SupportAssist Enterprise でお使いの Dell デバイスのための Dell EMC テクニカル サポートからのサポートを自動化するための準備をします。SupportAssist Enterprise を使用してハードウェアの問題を監視したりお使いのデバイスからシステム情報を収集したりするには、SupportAssist Enterprise にお使いのデバイスを追加する必要があります。

SupportAssist Enterprise に追加できるデバイス タイプとデバイス モデルの詳細なリストについては、*SupportAssist Enterprise バージョン 4.0 Support Matrix*（ ）を参照してください。

メモ: デフォルトでは、SupportAssist コンポーネントは第 14 世代 PowerEdge サーバで使用できます。SupportAssist の自動サポート機能を受信するために、サーバで SupportAssist コンポーネントを登録できます。iDRAC が SupportAssist Enterprise に追加されると、SupportAssist コンポーネントが自動的に無効になりますが、SupportAssist Enterprise を介して自動サポート機能を使用できます。

メモ: IPv4 および IPv6 でアドレスデバイスの追加とシステム情報収集がサポートされています。

デバイスがドメインの一部である場合は、その DNS（Domain Name System）を正しく構成して、**デバイス** ページでホスト名を表示する必要があります。

トピック：

デバイスの追加方法

次のいずれかの方法で、SupportAssist Enterprise にデバイスを追加できます。

- 単一デバイスの追加 — デバイスの詳細を入力して各デバイスを個別に追加します
- デバイス検出ルールの作成 — 特定の IP アドレス範囲に基づいてデバイスを追加します。検出ルールの詳細については、「デバイス検出ルールの作成」を参照してください。
- アダプタの設定 — OpenManage Enterprise が管理するインベントリおよび追加デバイスに行います。アダプターのセットアップの詳細については、「アダプタ」を参照してください。
- デバイスで利用可能なユーザーインターフェイスを使用して、REST プロトコルを介して SupportAssist にデバイスを追加します。

SupportAssist を使用して監視できるデバイスの種類とモデルについては、「デバイスタイプと適用可能なデバイス」を参照してください。

デバイスタイプと適用可能なデバイス

SupportAssist Enterprise デバイスを追加するときは、適切なデバイス タイプを選択する必要があります。次の表に、特定のデバイスタイプを選択することで追加できるデバイスを一覧表示します。

メモ: SupportAssist Enterprise は、サポートされているデバイス タイプのすべてのモデルと互換性があるとは限りません。サポートされているデバイス タイプおよび対応するモデルのリストについては、 の『*SupportAssist Enterprise Version 4.0 Support Matrix*』(SupportAssist Enterprise バージョン 4.0 サポート マトリックス) を参照してください。

表 9. デバイス タイプ

デバイスタイプ	追加できるデバイス
シャーシ	• PowerEdge M1000e • PowerEdge VRTX • PowerEdge FX2/FX2s • PowerEdge MX7000
データ保護	• AppSync[1] • Avamar[3] • CloudBoostAppliance[1] • DPA[1] • DataDomain[3] • iDPA • DPAppliance[1] • EMCeCDM[1] • Networker[1] • PowerPath[1] • RecoverPoint[2] • UCC[1]
iDRAC	第 12 世代以降の PowerEdge サーバ メモ: iDRAC を追加するには、サーバの iDRAC の IP アドレスを入力する必要があります。
ネットワーク	• PowerConnect • Force10 • Dell Networking • Networking ワイヤレスコントローラモビリティシリーズ • その他のサポート対象ネットワーキングデバイス (Brocade および Cisco)
サーバー / ハイパーバイザー	実行中の第 9 世代以降の PowerEdge サーバーは次のとおりです。 • Linux • VMware ESX または VMware ESXi • Citrix XenServer • Oracle Virtual Machine メモ: サーバー / ハイパーバイザー を追加するには、サーバーのオペレーティング システムの IP アドレスを入力する必要があります。
ソフトウェア	• VMware 用 HIT キット / VSM • vCenter
仮想マシン	• Linux
ハイパーコンバージド インフラストラクチャー	• WebScale • VCEVision[1] • VSPEXBLUE/VXRail[1] • VxRackFlex[1] • VXRackSDDC[1]
データ ストレージ	• Fluid File System (FluidFS) • Storage PS Series と FluidFS

デバイスタイプ	追加できるデバイス
	・ Storage MD Series と FluidFS ・ Storage SC Series と FluidFS ・ ピアストレージ（PS）/ EqualLogic ・ Storage PS Series アレイ ・ PowerVault ・ Storage MD Series アレイ ・ Storage ME4 Series アレイ ・ Storage Center（SC）/ Compellent ・ Storage SC Series ソリューション ・ Atmos[2] ・ Celerra[2] ・ Centera[2] ・ Clariion[2] ・ CloudArray[1] ・ CloudIQ-CLTR[1] ・ CustManageSta[2] ・ DL3D[2] ・ DLm3[2] ・ DLm4[3] ・ DLm[2] ・ DSSD[1] ・ EDL-Engine[2] ・ ElasticCloudStorage[3] ・ Isilon[3] ・ Isilon-SD[1] ・ ScaleIO[1] ・ Symmetrix[2] ・ Unity[1] ・ VMAX3[3] ・ VNXe[2] ・ VNX[2] ・ ViPR[3] ・ ViPRSRM[1] ・ XtremIO[3] ・ Connectrix[3] ・ Switch-Brocade-B[3] ・ Switch-Cisco[2]

- 1 - RESTful プロトコルを使用して、デバイスから直接 SupportAssist Enterprise にデバイスを追加する必要があります。
- 2 - デバイスは SupportAssist Enterprise ユーザーインターフェイスから追加できます。
- 3 - デバイスは、SupportAssist Enterprise ユーザーインターフェイスから、および RESTful プロトコルを使用して追加できます。SupportAssist ユーザーインターフェイスからこのデバイスを追加した場合、そのデバイスでは限られた SupportAssist の機能のみが有効になります。接続の構成については、モデルとバージョンの製品構成ドキュメントを参照してください。

シャーシの追加

前提条件

- デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。
- デバイスでポート 22、161、および 443 が開いている必要があります。
- SSH サービスがデバイスで実行されている。

このタスクについて

ハードウェアの問題についてシャーシを監視し、システム情報を収集できます。追加できるシャーシモデルのリストについては、「デバイスタイプと適用可能なデバイス」を参照してください。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイス タイプ** リストから、**シャーシ** を選択します。
4. 適切なフィールドにデバイスのホスト名、または IP アドレスを入力します。

   メモ: デバイスのホスト名を入力することをお勧めします。ホスト名を使用できない場合、デバイスの IP アドレスを入力できます。
5. 必要に応じて、**名前** ボックスにデバイスの名前を入力します。

   入力した名前は、SupportAssist Enterprise でデバイスを表す際に使用されます。名前を入力しない場合、デバイスを表すために IP アドレスまたはホスト名が使用されます。
6. シャーシに関連している可能性のある別のサポートされているデバイス タイプを検出または追加するには、**詳細な検出を実行する** チェック ボックスを選択します。「詳細な検出」を参照してください。
   資格情報プロファイル リストが表示されます。
7. 次のいずれかの手順を実行してください。
   - 詳細な検出が有効の場合は、デバイスとそれに関連するデバイス タイプに割り当てる資格情報プロファイルを選択します。新しい資格情報プロファイルを作成するには、**新しいプロファイルを作成** をクリックし、次に**作成**をクリックします。「認証情報プロファイルの作成」を参照してください。
   - 詳細な検出が有効ではない場合は、**アカウント認証情報**リストからデバイスに割り当てる認証情報アカウントを選択します。新しいアカウントの資格情報一式を作成するには、**新しいアカウントを作成する**をクリックし、次に**作成**をクリックします。「アカウント資格情報の追加」を参照してください。
8. デバイスで発生する可能性のあるハードウェアの問題を SupportAssist Enterprise が監視しない場合は、**監視を有効にする** オプションをオフにします。
9. **次へ** をクリックします。
   SupportAssist Enterprise でデバイスが識別されるまで、**デバイスを検出しています** ページが表示されます。

   デバイスが正常に検出された場合は、**デバイスグループを割り当て（オプション）** ページが表示されます。それ以外の場合、適切なエラーメッセージが表示されます。
10. 必要に応じて、**他のグループの割り当て**リストから、デバイスを割り当てるデバイス グループを選択します。

    デバイスグループを選択しない場合、デバイスは **デフォルト** デバイスグループに割り当てられます。**デフォルト** デバイス グループについては、「事前定義されたデバイスグループ」を参照してください。
11. **終了** をクリックします。
    デバイスがデバイスインベントリに追加され、**サマリ** ページが表示されます。
12. **OK** をクリックします。
    デバイス ページが表示されます。

次の手順

注意: デバイスがアラートを転送するように設定されていない場合、SupportAssist Enterprise はデバイスで発生する可能性があるハードウェアの問題を検知できません。

デバイスで発生する可能性があるハードウェアの問題の監視に関してのみ、デバイスが SNMP トラップ(アラート)を SupportAssist Enterprise が導入されているサーバーに転送するように設定されていることを確認します。アラート転送を設定する方法については、「Web インターフェイスを使用したシャーシのアラート送信先を手動設定」を参照してください。

デバイスが **ステージング** グループに追加されたことを示すメッセージが表示された場合：

1. デバイスを追加するための前提条件がすべて満たされていることを確認します。
2. デバイスでインベントリ検証を実行します。「インベントリ検証を手動で開始」を参照してください。

データ保護デバイスの追加

前提条件

デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイス タイプ** リストから、**データ保護**を選択します。
4. **モデル タイプ** リストから、必要なモデルを選択します。
5. 適切なフィールドにデバイスの IP アドレスとシリアル番号を入力します。
6. **拡張機能** リストからデバイスの拡張機能を選択します。
7. **次へ** をクリックします。
   サマリー ページには、デバイスの詳細が表示されます。

   メモ: 特定の種類のデバイスは、デバイス インベントリに追加され、検証された後に限り デバイス ページに表示されます。この処理は最大 24 時間かかることがあります。
8. **OK** をクリックします。
   デバイス ページが表示されます。

iDRAC の追加

前提条件

- デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。
- デバイスは第 12 世代以降の Dell PowerEdge サーバ (iDRAC7 以降) である必要があります。PowerEdge サーバーの世代の識別については、「PowerEdge サーバー シリーズの特定」を参照してください。
- デバイスがプロキシ サーバー経由でインターネットに接続されている場合は、ポート 161 および 443 がプロキシ サーバーのファイアウォールで開いている必要があります。
- iDRAC7 または iDRAC8 を追加するには、iDRAC に Enterprise または Express ライセンスがインストールされている必要があります。iDRAC9 を追加するには、iDRAC に Basic、Enterprise、または Express ライセンスがインストールされている必要があります。Enterprise または Express ライセンスの購入およびインストール方法についての情報は、で『*iDRAC User's Guide*』(iDRAC ユーザーズガイド) の「Managing Licenses」(ライセンスの管理) を参照してください。

このタスクについて

SupportAssist Enterprise はハードウェアの問題を監視し、デルサーバからシステム情報を収集することができます。次の手順を実行して、第 12 世代以降の Dell PowerEdge サーバを追加することができます。デバイスの追加中に、SupportAssist Enterprise でデバイスの SNMP を自動的に設定することが可できます。SNMP の設定は、デバイスから SupportAssist Enterprise にアラートを転送するために必要です。

メモ: デフォルトでは、SupportAssist コンポーネントは第 14 世代 PowerEdge サーバで使用できます。SupportAssist の自動サポート機能を受信するために、サーバで SupportAssist コンポーネントを登録できます。iDRAC が SupportAssist Enterprise に追加されると、SupportAssist コンポーネントが自動的に無効になりますが、SupportAssist Enterprise を介して自動サポート機能を使用できます。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイス タイプ** リストから、**iDRAC** を選択します。
4. 適切なフィールドにデバイスのホスト名、または IP アドレスを入力します。

メモ: **デバイスのホスト名を入力することをお勧めします。ホスト名を使用できない場合、デバイスの IP アドレスを入力できます。**

5. 必要に応じて、**名前** ボックスにデバイスの名前を入力します。

   入力した名前は、SupportAssist Enterprise でデバイスを表す際に使用されます。名前を入力しない場合、デバイスを表すために IP アドレスまたはホスト名が使用されます。

6. **[アカウントの資格情報]**リストから、デバイスに割り当てるアカウントの資格情報を選択します。新しいアカウントの資格情報を作成するには、**[新しいアカウントを作成する]** を選択し、**[作成]**をクリックします。「アカウント資格情報の追加」を参照してください。

7. SupportAssist Enterprise でデバイスにて発生する可能性があるハードウェアの問題を監視する場合は、**モニタリングを有効にする** および **SNMP の設定** チェックボックスを選択します。

   SupportAssist Enterprise がデバイスで発生する可能性のあるハードウェアの問題を監視するには、SupportAssist Enterprise が導入されているサーバーに SNMP トラップ (アラート) を転送するようにデバイスを設定する必要があります。この要件を満たすために、SupportAssist Enterprise は SNMP トラップ (アラート) 転送を自動的に設定できます。アラートを転送するように SupportAssist Enterprise で自動的にデバイスを設定できるようにするには、**[SNMP の設定]**オプションが選択されている必要があります。アラート転送を設定するタスクは、デバイスが正常にデバイスインベントリに追加された後に開始されます。

   メモ: **アラートの転送を手動で設定する場合は、SNMP の設定 チェックボックスをオフにします。**

8. **次へ** をクリックします。
   SupportAssist Enterprise でデバイスが識別されるまで、**デバイスを検出しています** ページが表示されます。

   デバイスが正常に検出された場合は、**デバイスグループを割り当て (オプション)** ページが表示されます。それ以外の場合、適切なエラーメッセージが表示されます。

9. 必要に応じて、**他のグループの割り当て** リストから、デバイスを割り当てるデバイスグループを選択します。

   デバイスグループを選択しない場合、デバイスは **デフォルト** デバイスグループに割り当てられます。**デフォルト** デバイス グループについては、「事前定義されたデバイスグループ」を参照してください。

10. **終了** をクリックします。

    メモ: **SNMP の設定 オプションを選択した場合は、デバイスの追加にしばらく時間がかかる場合があります。**

    デバイスがデバイス インベントリに追加され、**サマリー** ページが表示されます。

11. **OK** をクリックします。

    注意: **SupportAssist Enterprise が導入されているサーバーにアラートを転送するようにデバイスの SNMP 設定が構成されていない場合、SupportAssist Enterprise はデバイスで発生する可能性のあるハードウェアの問題を監視できません。**

    デバイスが適切なステータスで、デバイスインベントリに追加されます。SupportAssist Enterprise が SNMP 設定を構成しているとき、デバイスには **SNMP の設定** ステータスが表示されます。SNMP の設定が完了すると、デバイスのステータスが、**[成功]**になります。SNMP の設定中に問題が発生した場合は、**デバイス** ページに適切なステータスが表示されます。

    メモ: **デバイスにエラー ステータス が表示される場合は、エラーリンクをクリックして、問題の説明と可能な解決手順を表示します。SNMP の設定を再試行するには、デバイス概要 ペインにある タスク リストを使用することができます。**

次の手順

任意で、オペレーティング システムの詳細を使用して SupportAssist Enterprise でサーバを追加することができます。このケースでは、SupportAssist Enterprise は、アラートとオペレーティング システムおよび iDRAC の両方からのシステム情報のコレクションを自動的に相関させます。手順については、「サーバまたはハイパーバイザーの追加」を参照してください。SupportAssist Enterprise がデバイス情報を相関させる方法の詳細については、「デバイスの相互関係」を参照してください。

デバイスが **ステージング** グループに追加されたことを示すメッセージが表示された場合：

1. デバイスを追加するための前提条件がすべて満たされていることを確認します。
2. デバイスでインベントリ検証を実行します。「インベントリ検証を手動で開始」を参照してください。

ネットワーキング デバイスの追加

前提条件

- デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。
- ポート 22 と 161 がデバイス上で開いている必要があります。

- SSH サービスと SNMP サービスがデバイス上で実行されている必要があります。

このタスクについて

ハードウェアの問題についてネットワーキング デバイスを監視し、システム情報を収集できます。追加できるネットワーキング デバイスのリストについては、「デバイスタイプと適用可能なデバイス」を参照してください。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイスタイプ** リストから、**ネットワーキング** を選択します。
4. 適切なフィールドにデバイスのホスト名、または IP アドレスを入力します。

   メモ: デバイスのホスト名を入力することをお勧めします。ホスト名を使用できない場合、デバイスの IP アドレスを入力できます。
5. 必要に応じて、**名前** ボックスにデバイスの名前を入力します。

   入力した名前は、SupportAssist Enterprise でデバイスを表す際に使用されます。名前を入力しない場合、デバイスを表すために IP アドレスまたはホスト名が使用されます。
6. シャーシに関連している可能性のある別のサポートされているデバイス タイプを検出または追加するには、**詳細な検出を実行する** チェック ボックスを選択します。「詳細な検出」を参照してください。
   資格情報プロファイル リストが表示されます。
7. 次のいずれかの手順を実行してください。
   - 詳細な検出が有効の場合は、デバイスとそれに関連するデバイス タイプに割り当てる資格情報プロファイルを選択します。新しい資格情報プロファイルを作成するには、**新しいプロファイルを作成** をクリックし、次に**作成**をクリックします。「認証情報プロファイルの作成」を参照してください。
   - 詳細な検出が有効ではない場合は、**アカウント認証情報**リストからデバイスに割り当てる認証情報アカウントを選択します。新しいアカウントの資格情報一式を作成するには、**新しいアカウントを作成する**をクリックし、次に**作成**をクリックします。「アカウント資格情報の追加」を参照してください。
8. デバイスで発生する可能性のあるハードウェアの問題を SupportAssist Enterprise が監視しない場合は、**監視を有効にする** オプションをオフにします。

   SupportAssist Enterprise がデバイスを監視できるのは、デバイスの SNMP 設定が SupportAssist Enterprise に SNMP トラップ(アラート) を転送するように構成されている場合のみです。アラート転送を設定する手順については、「ネットワーク デバイスのアラート送信先を手動設定」を参照してください。
9. **次へ** をクリックします。
   SupportAssist Enterprise でデバイスが識別されるまで、**デバイスを検出しています** ページが表示されます。

   デバイスが正常に検出された場合は、**デバイスグループを割り当て (オプション)** ページが表示されます。それ以外の場合、適切なエラーメッセージが表示されます。
10. 必要に応じて、**他のグループの割り当て**リストから、デバイスを割り当てるデバイス グループを選択します。

    デバイスグループを選択しない場合、デバイスは **デフォルト** デバイスグループに割り当てられます。**デフォルト** デバイス グループについては、「事前定義されたデバイスグループ」を参照してください。
11. **終了** をクリックします。
    デバイスがデバイスインベントリに追加され、**サマリ** ページが表示されます。
12. **OK** をクリックします。
    デバイス ページが表示されます。

次の手順

注意: デバイスがアラートを転送するように設定されていない場合、SupportAssist Enterprise はデバイスで発生する可能性があるハードウェアの問題を検知できません。

デバイスで発生する可能性があるハードウェアの問題の監視に関してのみ、デバイスが SNMP トラップ(アラート)を SupportAssist Enterprise に転送するように設定されていることを確認します。アラート転送を設定する手順については、「ネットワーク デバイスのアラート送信先を手動設定」を参照してください。

デバイスが **ステージング** グループに追加されたことを示すメッセージが表示された場合 :

1. デバイスを追加するための前提条件がすべて満たされていることを確認します。
2. デバイスでインベントリ検証を実行します。「インベントリ検証を手動で開始」を参照してください。

サーバまたはハイパーバイザーの追加

前提条件

- デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。
- デバイスが Linux オペレーティングシステムを実行している場合には、次の要件があります。
  - SSH サービスがデバイスで実行されている。
  - SSH パスワード認証が有効化されている (デフォルトで有効)。
  - 解凍パッケージが SupportAssist Enterprise がインストールされているサーバーにインストールされている。
- デバイスで VMware ESXi、ESX、Oracle Virtual Machine または Citrix XenServer が実行されている場合 :
  - SSH サービスがデバイスで実行されている。
  - デバイスでポート 22 および 443 が開いている必要があります。
  - ESX および ESXi のみからシステム情報を収集する場合は、SFCBD および CIMOM が有効になっていることを確認してください。
- OMSA 通信のために、デバイスでポート 1311 が開いている。
- デバイスがプロキシサーバ経由でインターネットに接続されている場合は、プロキシ サーバーのファイアウォールで、ポート 161、22 (Linux を実行しているデバイスを追加する場合) および 1311 が開いている必要があります。
- デバイスに OMSA をインストールするための要件を確認します。詳細に関しては、 で、『Dell OpenManage Server Administrator インストールガイド』を参照してください。

このタスクについて

SupportAssist Enterprise はハードウェアの問題を監視し、Dell EMC サーバからシステム情報を収集することができます。次の手順を実行して、Linux サーバーまたはハイパーバイザーを追加することができます。デバイスを追加している間、SupportAssist Enterprise がデバイスで発生する可能性のあるハードウェアの問題を監視するために必要な次のタスクを自動的に実行できるようにすることができます。

- OMSA のインストール / アップグレード - デバイスで発生するハードウェアイベントに対するアラートの生成、またはデバイスからのシステム情報の収集には、OMSA が必要です。
- SNMP の設定 — デバイスから SupportAssist Enterprise にアラートを転送するには、SNMP の設定が必要です。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイス タイプ** リストから、**サーバー / ハイパーバイザー** を選択します。
4. 適切なフィールドにデバイスのホスト名、または IP アドレスを入力します。

   メモ: デバイスのホスト名を入力することをお勧めします。ホスト名を使用できない場合、デバイスの IP アドレスを入力できます。
5. 必要に応じて、**名前** ボックスにデバイスの名前を入力します。

   入力した名前は、SupportAssist Enterprise でデバイスを表す際に使用されます。名前を入力しない場合、デバイスを表すために IP アドレスまたはホスト名が使用されます。
6. シャーシに関連している可能性のある別のサポートされているデバイス タイプを検出または追加するには、**詳細な検出を実行する** チェック ボックスを選択します。「詳細な検出」を参照してください。
   資格情報プロファイル リストが表示されます。
7. 次のいずれかの手順を実行してください。
   - 詳細な検出が有効の場合は、デバイスとそれに関連するデバイス タイプに割り当てる資格情報プロファイルを選択します。新しい資格情報プロファイルを作成するには、**新しいプロファイルを作成** をクリックし、次に**作成**をクリックします。「認証情報プロファイルの作成」を参照してください。
   - 詳細な検出が有効ではない場合は、**アカウント認証情報**リストからデバイスに割り当てる認証情報アカウントを選択します。新しいアカウントの資格情報一式を作成するには、**新しいアカウントを作成する**をクリックし、次に**作成**をクリックします。「アカウント資格情報の追加」を参照してください。
8. SupportAssist Enterprise でデバイスにて発生する可能性があるハードウェアの問題を監視する場合は、**モニタリングを有効にする**、**SNMP の設定**および **OMSA のインストール / アップグレード**チェックボックスを選択します。

SupportAssist Enterprise がデバイスで発生する可能性があるハードウェアの問題を監視するには、次の依存関係を満たす必要があります。

- デバイスの SNMP 設定が SNMP トラップ (アラート) を SupportAssist Enterprise に転送するように設定されている必要があります。
- Dell OpenManage Server Administrator (OMSA) の奨励するバージョンがデバイスにインストールされている必要があります。

これらの依存関係を満たすため、SupportAssist Enterprise は SNMP トラップ (アラート) の転送を設定し、デバイスで自動的に OMSA をインストールまたはアップグレードできます。SupportAssist Enterprise の自動動作を有効化するには、次のようにします。

- アラートを転送するようにデバイスを設定し、**SNMP の設定** オプションが選択されていることを確認します。
- デバイスで OMSA をインストールまたはアップグレードするには、**OMSA のインストール / アップグレード** オプションが選択されていることを確認します。

アラート転送を設定し OMSA をインストールするタスクは、デバイスが正常にデバイスインベントリに追加された後に開始されます。

メモ: 両方のタスク (アラート転送の設定と OMSA のインストールまたはアップグレード) を手動で実行する場合は、SNMP の設定 と OMSA のインストール / アップグレード チェックボックスをオフにします。

9. **次へ** をクリックします。
SupportAssist Enterprise でデバイスが識別されるまで、**デバイスを検出しています** ページが表示されます。

   デバイスが正常に検出された場合は、**デバイスグループを割り当て (オプション)** ページが表示されます。それ以外の場合、適切なエラーメッセージが表示されます。

10. 必要に応じて、**他のグループの割り当て** リストから、デバイスを割り当てるデバイス グループを選択します。
   デバイスグループを選択しない場合、デバイスは **デフォルト** デバイスグループに割り当てられます。**デフォルト** デバイス グループについては、「事前定義されたデバイスグループ」を参照してください。

11. **終了** をクリックします。
デバイスがデバイスインベントリに追加され、**サマリ** ページが表示されます。

12. **OK** をクリックします。

注意: デバイスの SNMP が設定されておらず、デバイスに OMSA がインストールされていない場合、SupportAssist Enterprise はデバイスで発生する可能性があるハードウェアの問題を監視できません。

メモ: OMSA のインストールは、CentOS、Oracle Virtual Machine、および Oracle Enterprise Linux を実行しているデバイス上ではサポートされません。これらのデバイスを デバイスタイプ で サーバ / ハイパーバイザー として追加したときは、SupportAssist Enterprise では、システム情報を収集してアップロードすることのみ可能です。SupportAssist Enterprise でこれらのデバイスのハードウェアの問題を監視できるようにするには、これらのデバイスを デバイス タイプ で iDRAC として選択して追加します。「iDRAC の追加」を参照してください。

デバイスが適切なステータスで、デバイスインベントリに追加されます。

- SupportAssist Enterprise が SNMP 設定を構成しているとき、デバイスには  **SNMP の設定** ステータスが表示されます。
- SupportAssist Enterprise が OMSA 設定を構成しているとき、デバイスには  **OMSA のインストール中** ステータスが表示されます。

OMSA のインストールと SNMP の設定が完了すると、デバイスのステータスが、  **成功** に変わります。SNMP の設定または OMSA のインストール中に問題が発生した場合は、**デバイス** ページに適切なステータスが表示されます。

メモ: デバイスに  が表示される場合は、エラーリンクをクリックして、問題の説明と可能な解決手順を表示します。OMSA のインストールまたは SNMP の設定を再試行するには、デバイス概要 ペインにある [タスク] リストを使用します。

次の手順

オプションで、iDRAC の詳細を使用して SupportAssist Enterprise にサーバーを追加します。このケースでは、SupportAssist Enterprise は、アラートとオペレーティング システムおよび iDRAC の両方からのシステム情報のコレクションを自動的に相関させます。「iDRAC の追加」を参照してください。SupportAssist Enterprise がデバイス情報を相関させる方法の詳細については、「デバイスの相互関係」を参照してください。

ソフトウェアの追加

前提条件

デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。

このタスクについて

SupportAssist Enterprise は、以下の管理および監視ソフトウェアからのみシステム情報を収集できます。

- VMware vCenter
- VMware 向け Host Integration Toolkit (HIT Kit/Virtual Storage Manager)

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイス タイプ** リストから、**ソフトウェア** を選択します。
4. **ソフトウェア タイプ** リストから、ソフトウェア タイプを選択します。
5. 適切なフィールドにデバイスのホスト名、または IP アドレスを入力します。

   メモ: デバイスのホスト名を入力することをお勧めします。ホスト名を使用できない場合、デバイスの IP アドレスを入力できます。
6. 必要に応じて、**名前** ボックスにデバイスの名前を入力します。
   入力した名前は、SupportAssist Enterprise でデバイスを表す際に使用されます。名前を入力しない場合、デバイスを表すために IP アドレスまたはホスト名が使用されます。
7. **アカウントの認証情報**リストから、デバイスに割り当てるアカウント認証情報を選択し、**次へ**をクリックします。新しいアカウントの資格情報一式を作成するには、**新しいアカウントを作成する**をクリックし、次に**作成**をクリックします。「アカウント資格情報の追加」を参照してください。
   - 認証情報アカウントを選択した場合、SupportAssist Enterprise がデバイスを認識するまで、**[デバイスを検出しています]** ページが表示されます。デバイスが正常に検出された場合は、**デバイスグループを割り当て (オプション)** ページが表示されます。それ以外の場合、適切なエラーメッセージが表示されます。
   - **新しいアカウントを作成する** をクリックすると、**アカウント資格情報の追加** ウィンドウが表示されます。「アカウント資格情報の追加」を参照してください。
8. 必要に応じて、**他のグループの割り当て**リストから、デバイスを割り当てるデバイス グループを選択します。
   デバイスグループを選択しない場合、デバイスは **デフォルト** デバイスグループに割り当てられます。**デフォルト** デバイス グループについては、「事前定義されたデバイスグループ」を参照してください。
9. **終了** をクリックします。
   デバイスがデバイスインベントリに追加され、**サマリ** ページが表示されます。
10. **OK** をクリックします。
    デバイス ページが表示されます。

次の手順

デバイスが **ステージング** グループに追加されたことを示すメッセージが表示された場合：

1. デバイスを追加するための前提条件がすべて満たされていることを確認します。
2. デバイスでインベントリ検証を実行します。「インベントリ検証を手動で開始」を参照してください。

仮想マシンの追加

前提条件

- SupportAssist Enterprise が導入されているサーバーから仮想マシンをホストするシステムに到達可能である必要があります。
- 追加する仮想マシンは VMware ESX、ESXi、Microsoft Hyper-V 上に作成する必要があります

このタスクについて

SupportAssist Enterprise は、仮想マシンからのみシステム情報を収集できます。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイスタイプ**リストから、**仮想マシン**を選択します。
4. 適切なフィールドにデバイスのホスト名、または IP アドレスを入力します。

   メモ: デバイスのホスト名を入力することをお勧めします。ホスト名を使用できない場合、デバイスの IP アドレスを入力できます。
5. 必要に応じて、**名前** ボックスにデバイスの名前を入力します。
   入力した名前は、SupportAssist Enterprise でデバイスを表す際に使用されます。名前を入力しない場合、デバイスを表すために IP アドレスまたはホスト名が使用されます。
6. **アカウントの認証情報**リストから、デバイスに割り当てるアカウント認証情報を選択し、**次へ**をクリックします。新しいアカウントの資格情報一式を作成するには、**新しいアカウントを作成する**をクリックし、次に**作成**をクリックします。「アカウント資格情報の追加」を参照してください。
   - 認証情報アカウントを選択した場合、SupportAssist Enterprise がデバイスを認識するまで、**[デバイスを検出しています]** ページが表示されます。デバイスが正常に検出された場合は、**デバイスグループを割り当て (オプション)** ページが表示されます。それ以外の場合、適切なエラーメッセージが表示されます。
   - **新しいアカウントを作成する** をクリックすると、**アカウント資格情報の追加** ウィンドウが表示されます。「アカウント資格情報の追加」を参照してください。
7. 必要に応じて、**他のグループの割り当て**リストから、デバイスを割り当てるデバイス グループを選択します。
   デバイスグループを選択しない場合、デバイスは **デフォルト** デバイスグループに割り当てられます。**デフォルト** デバイス グループについては、「事前定義されたデバイスグループ」を参照してください。
8. **終了** をクリックします。
   デバイスがデバイスインベントリに追加され、**サマリ** ページが表示されます。
9. **OK** をクリックします。
   デバイス ページが表示されます。

ハイパーコンバージド インフラストラクチャ デバイスの追加

前提条件

デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。

このタスクについて

SupportAssist Enterprise を使用すると、データ ストレージ デバイスからシステム情報を監視および収集できます。ただし、システム情報収集機能は、Web スケール モデルでのみ使用可能です。追加できるハイパーコンバージド インフラストラクチャー デバイスのモデルについては、「デバイスタイプと適用可能なデバイス」を参照してください。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイス タイプ** リストから、**ハイパーコンバージド インフラストラクチャ** を選択します。
4. **モデル タイプ** リストから、必要なモデルを選択します。
   適切なフィールドが表示されます。
5. **[Web スケール]** アプライアンスを追加するには、「ウェブスケール ソリューションの追加」を参照してください。

6. 他のモデルを追加する場合は、次の手順を実行します。
   a) 適切なフィールドにデバイスの IP アドレスとシリアル番号を入力します。
   b) **拡張機能** リストからデバイスの拡張機能を選択します。
   c) **次へ** をクリックします。
   サマリー ページには、デバイスの詳細が表示されます。
   メモ: 特定の種類のデバイスは、デバイス インベントリに追加され、検証された後に限り デバイス ページに表示されます。この処理は最大 24 時間かかることがあります。
7. **OK** をクリックします。
   デバイス ページが表示されます。

ウェブスケール ソリューションの追加

前提条件

- デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。
- デバイスでポート 9440 および 22 が開いている必要があります。
- Web スケールのソリューションでは、システム情報を収集するために、ファームウェア バージョン 4.x 以降がデバイスにインストールされている必要があります。

このタスクについて

SupportAssist Enterprise では、ハードウェアの問題を監視し、Web スケールのハイパーコンバージド アプライアンスからのシステム情報を収集できます。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイス タイプ** リストから、**ハイパーコンバージド インフラストラクチャ** を選択します。
4. **ソリューション / モデル タイプ** リストから、**Web スケール** を選択します。
5. 適切なフィールドにデバイスのホスト名、または IP アドレスを入力します。
   メモ: デバイスのホスト名を入力することをお勧めします。ホスト名を使用できない場合、デバイスの IP アドレスを入力できます。
6. 必要に応じて、**名前** ボックスにデバイスの名前を入力します。
   入力した名前は、SupportAssist Enterprise でデバイスを表す際に使用されます。名前を入力しない場合、デバイスを表すために IP アドレスまたはホスト名が使用されます。
7. シャーシに関連している可能性のある別のサポートされているデバイス タイプを検出または追加するには、**詳細な検出を実行する** チェック ボックスを選択します。「詳細な検出」を参照してください。
   資格情報プロファイル リストが表示されます。
8. 次のいずれかの手順を実行してください。
   - 詳細な検出が有効の場合は、デバイスとそれに関連するデバイス タイプに割り当てる資格情報プロファイルを選択します。新しい資格情報プロファイルを作成するには、**新しいプロファイルを作成** をクリックし、次に**作成**をクリックします。「認証情報プロファイルの作成」を参照してください。
   - 詳細な検出が有効ではない場合は、**アカウント認証情報**リストからデバイスに割り当てる認証情報アカウントを選択します。新しいアカウントの資格情報一式を作成するには、**新しいアカウントを作成する**をクリックし、次に**作成**をクリックします。「アカウント資格情報の追加」を参照してください。
9. 必要に応じて、**他のグループの割り当て**リストから、デバイスを割り当てるデバイス グループを選択します。
   デバイスグループを選択しない場合、デバイスは **デフォルト** デバイスグループに割り当てられます。**デフォルト** デバイス グループについては、「事前定義されたデバイスグループ」を参照してください。
10. **終了** をクリックします。
    デバイスがデバイスインベントリに追加され、**サマリ** ページが表示されます。
11. **OK** をクリックします。
    デバイス ページが表示されます。

次の手順

デバイスが **ステージング** グループに追加されたことを示すメッセージが表示された場合：

1. デバイスを追加するための前提条件がすべて満たされていることを確認します。
2. デバイスでインベントリ検証を実行します。「インベントリ検証を手動で開始」を参照してください。

データ ストレージ デバイスの追加

前提条件

デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。

このタスクについて

SupportAssist Enterprise を使用すると、データ ストレージ デバイスからシステム情報を監視および収集できます。システム情報は必要に応じて展開後に収集できます。ただし、システム情報収集機能は、データ ストレージ デバイス内の次のモデルでのみ使用可能です。

- Storage PS Series（旧 EqualLogic）アレイ
- Storage SC Series
- Fluid File System（FluidFS）ネットワーク接続ストレージ（NAS）デバイス
- Storage MD Series アレイ

追加できるデータ ストレージ デバイスのリストについては、デバイスタイプと適用可能なデバイスを参照してください。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイス タイプ** リストから、**データ ストレージ**を選択します。
4. **モデル タイプ** リストから、必要なデータ ストレージ モデルを選択します。
   適切なフィールドが表示されます。
5. **[Peerstorage (PS) / Equallogic]** デバイスを追加するには、「EqualLogic PS Series ストレージアレイの追加」を参照してください。
6. **[Storage Center (SC) /Compellent]** デバイスを追加するには、「Compellent SC シリーズストレージソリューションの追加」を参照してください。
7. **[Fluid File System (Fluid FS)]** デバイスを追加するには、「Fluid File System NAS デバイスの追加」を参照してください。
8. **[PowerVault]** デバイスを追加するには、「PowerVault ストレージ アレイの追加」を参照してください。
9. 他のモデルを追加する場合は、次の手順を実行します。
   a) 適切なフィールドにデバイスの IP アドレスとシリアル番号を入力します。
   b) **拡張機能** リストからデバイスの拡張機能を選択します。
   c) **次へ** をクリックします。
   サマリー ページには、デバイスの詳細が表示されます。

   メモ: 特定の種類のデバイスは、デバイス インベントリに追加され、検証された後に限り デバイス ページに表示されます。この処理は最大 24 時間かかることがあります。
10. **OK** をクリックします。
    デバイス ページが表示されます。

EqualLogic PS Series ストレージアレイの追加

前提条件

- デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。
- デバイスでポート 21、22、および 161 が開いている必要があります。
- SSH および SNMP サービスがデバイスで実行されている必要があります。

このタスクについて

SupportAssist Enterprise は、Storage PS Series（以前の EqualLogic）アレイからのシステム情報のみを収集できます。Storage PS Series デバイスを追加することで、オンデマンドおよび導入後にシステム情報を収集することができます。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイス タイプ** リストから、**データ ストレージ**を選択します。
4. **モデルタイプ** リストから、**ピアストレージ（PS）/EqualLogic** を選択します。
5. 適切なフィールドにデバイスのホスト名、または IP アドレスを入力します。

   メモ: デバイスのホスト名を入力することをお勧めします。ホスト名を使用できない場合、デバイスの IP アドレスを入力できます。
6. 必要に応じて、**名前** ボックスにデバイスの名前を入力します。

   入力した名前は、SupportAssist Enterprise でデバイスを表す際に使用されます。名前を入力しない場合、デバイスを表すために IP アドレスまたはホスト名が使用されます。
7. シャーシに関連している可能性のある別のサポートされているデバイス タイプを検出または追加するには、**詳細な検出を実行する** チェック ボックスを選択します。「詳細な検出」を参照してください。
   資格情報プロファイル リストが表示されます。
8. 次のいずれかの手順を実行してください。
   - 詳細な検出が有効の場合は、デバイスとそれに関連するデバイス タイプに割り当てる資格情報プロファイルを選択します。新しい資格情報プロファイルを作成するには、**新しいプロファイルを作成** をクリックし、次に**作成**をクリックします。「認証情報プロファイルの作成」を参照してください。
   - 詳細な検出が有効ではない場合は、**アカウント認証情報**リストからデバイスに割り当てる認証情報アカウントを選択します。新しいアカウントの資格情報一式を作成するには、**新しいアカウントを作成する**をクリックし、次に**作成**をクリックします。「アカウント資格情報の追加」を参照してください。
9. **次へ** をクリックします。
   SupportAssist Enterprise でデバイスが識別されるまで、**デバイスを検出しています** ページが表示されます。

   デバイスが正常に検出された場合は、**デバイスグループを割り当て（オプション）** ページが表示されます。それ以外の場合、適切なエラーメッセージが表示されます。
10. 必要に応じて、**他のグループの割り当て** リストから、デバイスを割り当てるデバイスグループを選択します。

    デバイスグループを選択しない場合、デバイスは **デフォルト** デバイスグループに割り当てられます。**デフォルト** デバイス グループについては、「事前定義されたデバイスグループ」を参照してください。
11. **終了** をクリックします。
    デバイスがデバイスインベントリに追加され、**サマリ** ページが表示されます。
12. **OK** をクリックします。
    デバイス ページが表示されます。

次の手順

デバイスが **ステージング** グループに追加されたことを示すメッセージが表示された場合：

1. デバイスを追加するための前提条件がすべて満たされていることを確認します。
2. デバイスでインベントリ検証を実行します。「インベントリ検証を手動で開始」を参照してください。

Compellent SC シリーズストレージソリューションの追加

前提条件

- デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。
- デバイスでポート 443 が開いている必要があります。
- REST サービスがデバイスで実行されている必要があります。
- システム情報を収集するには、SC Series ストレージソリューション 7.1 以前を搭載する Compellent デバイス向け Dell Compellent Enterprise Manager アプリケーションで SupportAssist を有効にする必要があります。

このタスクについて

SupportAssist Enterprise でシステム情報を収集できるのは、Storage SC Series ソリューションからのみです。Storage SC Series デバイスを追加することで、オンデマンドおよび導入後にシステム情報を収集することができます。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイス タイプ** リストから、**データ ストレージ**を選択します。
4. **モデルタイプ** リストから、**Storage Center (SC) /Compellent** を選択します。
5. 適切なフィールドにデバイスのホスト名、または IP アドレスを入力します。

   メモ: デバイスのホスト名を入力することをお勧めします。ホスト名を使用できない場合、デバイスの IP アドレスを入力できます。
6. 必要に応じて、**名前** ボックスにデバイスの名前を入力します。

   入力した名前は、SupportAssist Enterprise でデバイスを表す際に使用されます。名前を入力しない場合、デバイスを表すために IP アドレスまたはホスト名が使用されます。
7. **アカウントの認証情報**リストから、デバイスに割り当てるアカウント認証情報を選択し、**次へ**をクリックします。新しいアカウントの資格情報一式を作成するには、**新しいアカウントを作成する**をクリックし、次に**作成**をクリックします。「アカウント資格情報の追加」を参照してください。
   - 認証情報アカウントを選択した場合、SupportAssist Enterprise がデバイスを認識するまで、**[デバイスを検出しています]** ページが表示されます。デバイスが正常に検出された場合は、**デバイスグループを割り当て (オプション)** ページが表示されます。それ以外の場合、適切なエラーメッセージが表示されます。
   - **新しいアカウントを作成する** をクリックすると、**アカウント資格情報の追加** ウィンドウが表示されます。「アカウント資格情報の追加」を参照してください。
8. 必要に応じて、**他のグループの割り当て**リストから、デバイスを割り当てるデバイス グループを選択します。

   デバイスグループを選択しない場合、デバイスは **デフォルト** デバイスグループに割り当てられます。**デフォルト** デバイス グループについては、「事前定義されたデバイスグループ」を参照してください。
9. **終了** をクリックします。
   デバイスがデバイスインベントリに追加され、**サマリ** ページが表示されます。
10. **OK** をクリックします。
    デバイス ページが表示されます。

次の手順

デバイスが **ステージング** グループに追加されたことを示すメッセージが表示された場合：

1. デバイスを追加するための前提条件がすべて満たされていることを確認します。
2. デバイスでインベントリ検証を実行します。「インベントリ検証を手動で開始」を参照してください。

Fluid File System NAS デバイスの追加

前提条件

- デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。
- デバイスでポート 22 および 44421 が開いている必要があります。
- SSH サービスがデバイスで実行されている。

このタスクについて

SupportAssist Enterprise は、Dell Fluid File System (FluidFS) ネットワーク接続ストレージ (NAS) デバイスからシステム情報のみを収集できます。FluidFS NAS デバイスを追加することで、オンデマンドおよび導入後にシステム情報を収集することができます。追加できる Fluid File Systems (FluidFS) のリストについては、「デバイスタイプと適用可能なデバイス」を参照してください。

手順

1. **デバイス** > **デバイスを表示** に移動します。

デバイス ページが表示されます。

2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイス タイプ** リストから、**データ ストレージ**を選択します。
4. **モデル タイプ** リストから、**Fluid File System（FluidFS）** を選択します。
5. 適切なフィールドにデバイスのホスト名、または IP アドレスを入力します。

   メモ: デバイスのホスト名を入力することをお勧めします。ホスト名を使用できない場合、デバイスの IP アドレスを入力できます。
6. 必要に応じて、**名前** ボックスにデバイスの名前を入力します。
   入力した名前は、SupportAssist Enterprise でデバイスを表す際に使用されます。名前を入力しない場合、デバイスを表すために IP アドレスまたはホスト名が使用されます。
7. **アカウントの認証情報**リストから、デバイスに割り当てるアカウント認証情報を選択し、**次へ**をクリックします。新しいアカウントの資格情報一式を作成するには、**新しいアカウントを作成する**をクリックし、次に**作成**をクリックします。「アカウント資格情報の追加」を参照してください。
   - 認証情報アカウントを選択した場合、SupportAssist Enterprise がデバイスを認識するまで、**[デバイスを検出しています]** ページが表示されます。デバイスが正常に検出された場合は、**デバイス グループを割り当て（オプション）** ページが表示されます。それ以外の場合、適切なエラーメッセージが表示されます。
   - **新しいアカウントを作成する** をクリックすると、**アカウント資格情報の追加** ウィンドウが表示されます。「アカウント資格情報の追加」を参照してください。
8. 必要に応じて、**他のグループの割り当て**リストから、デバイスを割り当てるデバイス グループを選択します。
   デバイスグループを選択しない場合、デバイスは **デフォルト** デバイスグループに割り当てられます。**デフォルト** デバイス グループについては、「事前定義されたデバイスグループ」を参照してください。
9. **終了** をクリックします。
   デバイスがデバイスインベントリに追加され、**サマリ** ページが表示されます。
10. **OK** をクリックします。
    デバイス ページが表示されます。

次の手順

デバイスが **ステージング** グループに追加されたことを示すメッセージが表示された場合：

1. デバイスを追加するための前提条件がすべて満たされていることを確認します。
2. デバイスでインベントリ検証を実行します。「インベントリ検証を手動で開始」を参照してください。

PowerVault ストレージ アレイの追加

前提条件

- デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。
- デバイスでポート 2463 が開いている必要があります。

このタスクについて

SupportAssist Enterprise は、Storage MD Series アレイからシステム情報のみを収集できます。Storage MD Series デバイスを追加することで、オンデマンドおよび導入後にシステム情報を収集することができます。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   単一デバイスの追加ウィンドウが表示されます。
3. **デバイス タイプ** リストから、**データ ストレージ**を選択します。
4. **モデル タイプ** リストから、**PowerVault** を選択します。
5. 適切なフィールドにデバイスのホスト名、または IP アドレスを入力します。

   メモ: デバイスのホスト名を入力することをお勧めします。ホスト名を使用できない場合、デバイスの IP アドレスを入力できます。

6. 必要に応じて、**名前** ボックスにデバイスの名前を入力します。
   入力した名前は、SupportAssist Enterprise でデバイスを表す際に使用されます。名前を入力しない場合、デバイスを表すために IP アドレスまたはホスト名が使用されます。
7. シャーシに関連している可能性のある別のサポートされているデバイス タイプを検出または追加するには、**詳細な検出を実行する** チェック ボックスを選択します。「詳細な検出」を参照してください。
   資格情報プロファイル リストが表示されます。
8. 次のいずれかの手順を実行してください。
   - 詳細な検出が有効の場合は、デバイスとそれに関連するデバイス タイプに割り当てる資格情報プロファイルを選択します。新しい資格情報プロファイルを作成するには、**新しいプロファイルを作成** をクリックし、次に**作成**をクリックします。「認証情報プロファイルの作成」を参照してください。
   - 詳細な検出が有効ではない場合は、**アカウント認証情報**リストからデバイスに割り当てる認証情報アカウントを選択します。新しいアカウントの資格情報一式を作成するには、**新しいアカウントを作成する**をクリックし、次に**作成**をクリックします。「アカウント資格情報の追加」を参照してください。
9. **次へ** をクリックします。
   SupportAssist Enterprise でデバイスが識別されるまで、**デバイスを検出しています** ページが表示されます。
   デバイスが正常に検出された場合は、**デバイス グループを割り当て（オプション）** ページが表示されます。それ以外の場合、適切なエラーメッセージが表示されます。
10. 必要に応じて、**他のグループの割り当て**リストから、デバイスを割り当てるデバイス グループを選択します。
    デバイス グループを選択しない場合、デバイスは **デフォルト** デバイス グループに割り当てられます。**デフォルト** デバイス グループについては、「事前定義されたデバイス グループ」を参照してください。
11. **終了** をクリックします。
    デバイスがデバイス インベントリに追加され、**サマリ** ページが表示されます。
12. **OK** をクリックします。
    デバイス ページが表示されます。

次の手順

デバイスが **ステージング** グループに追加されたことを示すメッセージが表示された場合：

1. デバイスを追加するための前提条件がすべて満たされていることを確認します。
2. デバイスでインベントリ検証を実行します。「インベントリ検証を手動で開始」を参照してください。

複製によるデバイスの追加

前提条件

- デバイスは SupportAssist Enterprise が導入されているサーバーから到達可能である必要があります。
- デバイスで必要なネットワーク ポートが開いている必要があります。

このタスクについて

追加したデバイスと同じ種類のデバイスを追加します。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. 追加するデバイスと同じタイプのデバイスを選択します。
   デバイス概要 ペインが表示されます。
3. **複製** をクリックします。
   デバイスの複製 ウィザードが表示されます。
4. 適切なフィールドにデバイスのホスト名、または IP アドレスを入力します。

   メモ: デバイスのホスト名を入力することをお勧めします。ホスト名を使用できない場合、デバイスの IP アドレスを入力できます。
5. 必要に応じて、**名前** ボックスにデバイスの名前を入力します。
   入力した名前は、SupportAssist Enterprise でデバイスを表す際に使用されます。名前を入力しない場合、デバイスを表すために IP アドレスまたはホスト名が使用されます。

6. **アカウントの認証情報**リストから、デバイスに割り当てるアカウント認証情報を選択し、**次へ**をクリックします。新しいアカウントの資格情報一式を作成するには、**新しいアカウントを作成する**をクリックし、次に**作成**をクリックします。「アカウント資格情報の追加」を参照してください。
   - 認証情報アカウントを選択した場合、SupportAssist Enterprise がデバイスを認識するまで、**[デバイスを検出しています]** ページが表示されます。デバイスが正常に検出された場合は、**デバイスグループを割り当て (オプション)** ページが表示されます。それ以外の場合、適切なエラーメッセージが表示されます。
   - **新しいアカウントを作成する** をクリックすると、**アカウント資格情報の追加** ウィンドウが表示されます。「アカウント資格情報の追加」を参照してください。
7. 必要に応じて、**他のグループの割り当て**リストから、デバイスを割り当てるデバイス グループを選択します。
   デバイスグループを選択しない場合、デバイスは **デフォルト** デバイスグループに割り当てられます。**デフォルト** デバイス グループについては、「事前定義されたデバイスグループ」を参照してください。
8. **終了** をクリックします。
   デバイスがデバイスインベントリに追加され、**サマリ** ページが表示されます。
9. **OK** をクリックします。
   デバイス ページが表示されます。

次の手順

デバイスが **ステージング** グループに追加されたことを示すメッセージが表示された場合：

1. デバイスを追加するための前提条件がすべて満たされていることを確認します。
2. デバイスでインベントリ検証を実行します。「インベントリ検証を手動で開始」を参照してください。

デバイスデータのエクスポート

このタスクについて

このオプションを使用して、「**デバイス**」ページから次の詳細情報を CSV ファイルに保存します。

- ホスト名または IP アドレス
- シリアルナンバー
- サービスタグ
- モデル
- 導入ステータス
- 保守性ステータス

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. をクリックします。
   デバイスの詳細が CSV ファイルで保存されます。

デバイスの削除

このタスクについて

何らかの理由でデバイスを監視しない場合は、SupportAssist Enterprise から 1 つ以上のデバイスを削除できます。

メモ: デバイスの削除では、SupportAssist Enterprise ユーザーインタフェースからデバイスが削除されるだけです。デバイスの機能には影響はありません。

メモ: アダプタ経由でインベントリ済みで SupportAssist Enterprise に追加されたデバイスは、削除できません。これらのデバイスは、アダプタが削除されるか、デバイスがシステム管理コンソールから削除された際に、SupportAssist Enterprise から自動的に削除されます。

メモ: RESTful プロトコルを使用して SupportAssist Enterprise にデバイスを追加する場合は、デバイスのユーザー インターフェイスからそのデバイスを無効にして SupportAssist Enterprise からそのデバイスを削除する必要があります。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. 削除するデバイスを選択します。
3. をクリックします。
   デバイス削除の確認 ウィンドウが表示されます。
4. **はい** をクリックします。
   デバイスが **デバイス** ページから削除されます。

   メモ: デバイスが削除されると、収集のパージタスクにより収集したシステム情報が削除されるまでは、そのデバイスから収集したシステム情報は削除されません。収集のパージタスクは、30 日以上前のシステム情報収集および、過去 30 日間における最新の 5 つの収集よりも古いシステム情報収集だけを削除します。

デバイス

デバイス ページには追加したデバイスと、各デバイスの SupportAssist Enterprise の機能のステータスが表示されます。デフォルトのビューに追加したすべてのデバイスが表示されます。

次の表に、**デバイス** ページに表示されるオプションと、**デバイス** ページに表示されるデバイス用に自動的に生成されたインベントリ情報を示します。

表 10. デバイスページ

オプション / 列	説明
	アカウントのサイト ID を表示します
検索基準 リスト	表示されているデータの特定のカテゴリで検索します
検索語句	検索キーワードを入力します **メモ: 検索を実行するには 3 文字以上入力する必要があります。**
更新	ページに表示されているデータを更新します。
表示方法	デバイスを（リスト）ビューまたは（関連付け）ビューで表示します
登録 ID	導入された SupportAssist Enterprise アプライアンスの登録 ID
シリアル番号	導入された SupportAssist Enterprise アプライアンスのシリアル番号
	進行中のアクティブなリモート セッションの数
	進行中のアクティブな Connect Home セッションの数
	SupportAssist Enterprise によって呼び出された REST API コールの数
	SRS VE のステータス。次のステータスが表示されます。 ・ — 接続済 ・ — 切断
	デバイスを追加します
	デバイスの種類に応じて、名前、アカウント認証情報、または IP アドレスをアップデートします
	デバイスを削除
	デバイスの詳細を CSV ファイルに保存します
収集の開始	単一のデバイス収集、または複数のデバイス収集を開始します
収集目的 リスト	複数のデバイス収集を実行するための目的を選択します

オプション / 列	説明
認証情報プロファイルの割り当て リスト	デバイスに認証情報を割り当てます
インベントリの検証	デバイス インベントリの検証
チェックボックス	デバイス固有のタスクを実行する単一または複数のデバイスを選択します。SupportAssist Enterprise で開始する次のタスクが進行中の場合、このチェックボックスは無効になっています。 • SNMP 設定 • OMSA のインストールまたはアップグレード • システムイベントログのクリア • 自動サポート ケース作成直後および手動で開始したコレクションが進行中のシステム情報のコレクション • インベントリ検証
名前 /IP アドレス	以下の情報が表示されます。 • デバイス名 - デバイスに入力した情報に応じて名前、ホスト名、シリアル番号、または IP アドレスを表示します。 • コレクションのステータス - コレクションが発生した場合に、プログレスバーと対応するメッセージが表示され、コレクションのステータスが示されます。表示される可能性があるコレクションのステータス メッセージは次のとおりです。 • 手動で開始したコレクションの場合: **メモ: 手動で開始したコレクションが進行中の場合、 がプログレス バーの隣に表示されます。必要に応じて をクリックして、コレクションをキャンセルします。** **メモ: SupportAssist Enterprise がデバイスからシステム情報を収集している場合のみ、コレクションをキャンセルできます。収集されたシステム情報がバックエンドに送信されている間は、コレクションをキャンセルすることはできません。** • **コレクションの開始** • **コレクションが進行中** • **コレクションの送信** • **コレクションのキャンセル** • ハードウェアの問題が検出されたことによりサポートケースが作成され、自動で開始したコレクションの場合: • **サポートケースのコレクションの開始** • **サポートケースのコレクションが進行中** • **サポートケースのコレクションの送信** **メモ: Dell Basic サービス契約を持つデバイスでハードウェアに関する問題が検知された場合は、自動コレクションが開始されます。ただし、そのデバイスでサポートケースは作成されません。** • デフォルトまたは設定済みの収集スケジュールに基づいた、自動定期コレクションの場合 : • **定期コレクションの開始** • **定期コレクションが進行中** • **定期コレクションの送信** **メモ: インスタンスによっては、あるデバイス上でコレクションが実行中 (手動) に、他のコレクション (定期) が開始されることがあります。このような状況の場合、コレクションのステータスは次の優先順位に従って表示されます。** ◆ **手動コレクション** ◆ **サポートケースのコレクション** ◆ **定期コレクション** • メンテナンス モード - デバイスがメンテナンスモードの場合、メンテナンス モード アイコン が表示されます。
モデル	デバイスのモデル (PowerEdge M820 など)

オプション / 列	説明
ステータス	インベントリ検証のステータス。ステータスは次のように分類することができます。 • **成功** - デバイスのインベントリ検証が正常に完了しました。 • **失敗** - デバイスのインベントリ検証が失敗しました。 • **進行中** - デバイスのインベントリ検証を実行中です。 • インベントリの検証がデバイスでまだ開始されていない場合、ステータスは表示されません。 次のデバイスまたはデバイス モデルでは、デバイス概要ペインの **[接続性のモニタリング]** および **[検証ステータス]** フィールドにそれぞれ **[オンライン]** および **[接続]** ステータスが表示されている場合にのみ、**[成功]** ステータスが表示されます。 • データ保護 • **[PeerStorage (PS) / Equallogic]**、**[STORAGE Center (SC) /Compellent]**、**[Fluid File System (Fluid FS)]**、**[PowerVault]** 以外のデータ ストレージ デバイス • **[Web スケール]** 以外のハイパー コンバージド デバイス

絞り込みの条件 ペインでは、次のフィルタを使用して表示されているデバイスのリストを絞り込むことができます。

- **デバイスタイプ**
- **注意が必要**
  - **ステージング** - ステータスアイコンと**ステージング** グループに存在するデバイス数のロールアップ回数を表示します。
  - **非アクティブ** - ステータスアイコンと**非アクティブ** グループに存在するデバイス数のロールアップ回数を表示します。
- **インベントリ検証**
  - **成功** - ステータスアイコンと正常に検証されたデバイス数のロールアップ回数を表示します。
  - **失敗** - ステータスアイコンと正常に検証されなかったデバイス数のロールアップ回数を表示します。
- **グループ**
  - **デフォルト** - すべてのデバイスが表示されます。
  - カスタム作成グループも表示されます。
- **コレクションホスト**
- **追加されるデバイス**

デバイス ページでは、操作に基づいて次のペインも表示します。

- デバイス概要ペイン - 単一のデバイスが選択された場合のみ表示されます。「デバイス概要 ペイン」を参照してください。
- 複数のデバイス コレクション ペイン - 複数のデバイス コレクションが進行中の場合に表示されます。「複数のデバイス収集 ペイン」を参照してください。

デバイス概要 ペイン

デバイスの概要ペインには、デバイスの詳細情報が表示されます。このペインを使用して、デバイスで特定の操作を実行できます。このペインは、**デバイス** ページで単一のデバイスを選択している場合にのみ表示されます。

次の表は、次のデバイスまたはデバイス モデルのデバイスの概要ペインに表示されるフィールドについての説明です。

- サーバーまたはハイパーバイザー
- iDRAC
- シャーシ
- ネットワーク
- PeerStorage (PS) または EqualLogic
- Storage Center (SC) / Compellent
- Fluid File System (FluidFS)
- PowerVault

表 11. デバイス概要 ペイン

フィールド	説明
タスク リスト	• **システム イベント ログのクリア** — システム イベント ログ (SEL) または組み込みシステム管理 (ESM) ログをクリアします。

フィールド	説明

	• **ケースの確認** — デバイスにサポート ケースがないかどうかを確認します。
	• **詳細な検出を実行** - デバイスとそれに関連するデバイス タイプを検出します。
	• **メンテナンスモード**
	  • **有効** - デバイスをメンテナンス モードにします。
	  • **無効** - デバイスを通常モードにします。
	• **依存関係**
	  • **OMSA のインストール/アップグレード** - デバイスに OMSA をインストールまたはアップグレードします。
	  • **SNMP の設定** - デバイスの SNMP 設定を設定します。

ホスト名 / IP アドレス	デバイスのホスト名または IP アドレス。
モデル	デバイスのモデル (PowerEdge M820 など)。
サービスタグ	Dell EMC がデバイスを認識できる一意の英数字 ID。
監視	• **有効** - デバイスに発生する可能性のあるハードウェアの問題の監視を有効にします。 • **無効** - デバイスに発生する可能性のあるハードウェアの問題の監視を無効にします。
ソフトウェアバージョン	デバイスにインストールされているファームウェアのバージョン。
ディスプレイ名	デバイスに指定されている名前。
デバイスタイプ	デバイスのタイプ (サーバーなど)。
コレクション リスト	コレクションの履歴を含むリスト。リストから日付と時刻を選択して、収集されたシステム情報を表示します。 **コレクションなし**は、デバイスから実行されたコレクションがないときに表示されます。
次にスケジュールされている収集	次にスケジュールされているコレクションの日付と時刻。
最後のデバイスのジョブステータス	デバイスでの SupportAssist Enterprise 機能のステータスと、そのステータスが生成された日付と時刻。ステータスは次のように分類することができます。 **情報ステータス** • ✓ **OK** - デバイスは SupportAssist Enterprise 機能に対応するように正しく設定されています。 • **OMSA のインストール** — Dell OpenManage Server Administrator (OMSA) のアップグレードまたはインストールが進行中です。 • **SNMP を設定中** — デバイスの SNMP の設定が進行中です。 • **システム イベント ログのクリア** — システム イベント ログのクリアが進行中です。 • ✓ **システム イベント ログのクリア** - システム イベント ログが正常にクリアされました。 • **デバイスの再検証** — SupportAssist Enterprise がデバイスの動作条件および認証情報を検証しています。

フィールド	説明
	警告ステータス • **OMSA がインストールされていません** - デバイス上に OMSA がインストールされていません。 • **SNMP が設定されていません。OMSA が最新ではありません** — デバイスの SNMP が設定されておらず、デバイスにインストールされている OMSA バージョンが SupportAssist Enterprise 用に推奨されている OMSA バージョンより前のバージョンになっています。 • **SNMP が設定されていません** — デバイスの SNMP が設定されていません。 • **OMSA の新バージョンが使用可能です** — デバイスにインストールできる新しいバージョンの OMSA が使用可能です。 • **OMSA がインストールされ、追加されたデバイスが再起動されます** — デバイスへの OMSA のインストールを完了します。変更を有効にするには、デバイスを再起動します。 **エラーステータス** • **デバイスを設定できません** — デバイスが特定の動作条件を満たしていないため、SupportAssist Enterprise は、**ステージング** グループ内のデバイスに配置されました。**ステージング** グループの詳細については、「事前定義されたデバイスグループ」を参照してください。 • **SNMP を設定できません** — SupportAssist Enterprise は、デバイスの SNMP トラップ送信先を設定できません。 • **SNMP の設定を検証できません** - SupportAssist Enterprise は iDRAC の SNMP 設定を検証できません。 • **OMSA をインストールできません** - OMSA のインストールを完了できませんでした。 • **OMSA はサポートされていません** - OMSA のインストールはサポートされていません。 • **デバイスに到達できません** - SupportAssist Enterprise はデバイスと通信できません。 • **認証に失敗しました** - SupportAssist Enterprise はデバイスにログインできません。 • **システム情報を収集できません** - SupportAssist Enterprise はデバイスからシステム情報を収集できません。 • **システム情報を収集するためのストレージ スペースが不足しています** - SupportAssist Enterprise が導入されているサーバーには、デバイスからシステム情報を収集するために十分な容量がありません。 • **コレクションをエクスポートできません** - SupportAssist Enterprise は、収集したシステム情報を処理できません。 • **システム情報を送信できません** - SupportAssist Enterprise は、収集されたシステム情報をバックエンドに送信できません。

フィールド	説明
	• **システム イベント ログのクリアに失敗しました** - SupportAssist Enterprise はシステム イベント ログまたはデバイス上の組み込みシステム管理ログをクリアすることができません。 • **メンテナンス モード** - アラート ストームのため、SupportAssist Enterprise はデバイスを自動メンテナンス モードに設定しました。デバイスがメンテナンスモードになっている間、新しいサポートケースは作成されません。詳細については、「メンテナンス モードの概要」を参照してください。 • **認証情報が提供されていません** - デバイスのユーザー名とパスワードが入力されていません。 • **認証情報が正しくありません** - デバイスに入力したユーザー名またはパスワードが正しくありません。 **メモ: エラー ステータスはリンクとして表示できるため、それをクリックすると問題の説明および解決のための手順を表示できます。**
オペレーティングシステム	デバイスにインストールされているオペレーティングシステム。
Software（シャーシ、ネットワーク、およびその他のデバイス用）	デバイスにインストールされているファームウェアのバージョン。
iSM（iDRAC 用）	デバイスにインストールされている iSM のバージョン。
OMSA（サーバ用）	デバイスにインストールされている OMSA のバージョン。
重複	すでに追加されているデバイスと同じタイプのデバイスを追加します。
デバイスインベントリ検証	以下が表示されます: • 定期インベントリ検証が最後に実行された日付と時刻。 • インベントリの検証タイプ。インベントリ検証テストのステータスも表示されます。 検証テストが失敗した場合、エラーメッセージが表示されます。

次の表は、次のデバイス タイプのモデルのデバイスの概要ペインに表示されるフィールドの説明です。

- データ保護
- Web スケール以外のすべてのハイパーコンバージド インフラストラクチャのデバイス モデル。
- Peer Storage（PS）/EqualLogic、Storage Center（SC）/Compellent、Fluid File System（FluidFS）、および PowerVault 以外のすべてのデータ ストレージ デバイスのモデル。

表 12. デバイス概要 ペイン

フィールド	説明
ホスト名 / IP アドレス	デバイスのホスト名または IP アドレス。
シリアル	デバイスのシリアル番号。
モデル	デバイスのモデル（PowerEdge M820 など）。
接続性モニタリング	デバイスの接続ステータス。
導入ステータス	SupportAssist Enterprise に追加後のデバイスのステータス。次のステータスが表示されることがあります。 • **管理対象** - デバイスが SupportAssist Enterprise によって正常に追加されて監視されています。

フィールド	説明
	• **管理対象外** - デバイスは SupportAssist Enterprise に追加されています。 • **追加保留中** - デバイスはバックエンドからの検証を待機中です。このステータスの場合、デバイスはハードウェア問題について監視されていません。 • **削除保留中** - デバイスは SupportAssist Enterprise からの削除承認を待機中です。 • **未登録** - SupportAssist Enterprise へのデバイスの追加が開始しました。 • **検証エラー** - SupportAssist Enterprise へのデバイスの追加中にエラーが発生しました。
デバイス ステータスの設定	オフライン モードでデバイスを配置できます。オフライン モードの詳細については、「オフライン モードの概要」を参照してください。
Dell EMC のルール	デバイスとバックエンドとの間のファイル転送のための権限を設定できます。
検証ステータス	以下が表示されます: • 接続テストと監視テストが最後に実施された日付と時刻。 • 実行されたテストのステータス。

7

Device grouping（デバイスのグループ化）

SupportAssist Enterprise には 2 つの定義済みのデバイスグループ（**デフォルト** および **ステージング**）があり、追加するデバイスの管理に役立ちます。要件に応じて カスタムデバイスグループを作成して特定のデバイスをグループとして管理することもできます たとえば、以下の情報に基づいたデバイスが含まれるデバイスグループを作成できます。

- デバイスタイプ（サーバ、ストレージ、またはネットワーク）
- デバイスの管理者（管理者グループ）
- 組織または事業ユニット（マーケティング、経営、財務、など）
- デバイスの物理的場所（送付先住所）
- アラートまたは通知（デバイスで問題が検知された場合に通知されるべき個人）

デバイスのグループ化機能は、次のデバイスまたはデバイス モデルでは使用できません。これらのデバイスを**デフォルト**グループからカスタム デバイス グループに移動することはできません。

- データ保護
- **[PeerStorage（PS）/ Equallogic]**、**[STORAGE Center（SC）/Compellent]**、**[Fluid File System（Fluid FS）]**、**[PowerVault]** 以外のデータ ストレージ デバイス
- **[Web スケール]** 以外のハイパー コンバージド デバイス

デバイスグループを作成した後、以下のことができるようになります。

- デバイスグループにデバイスを追加またはデバイスグループからデバイスを削除します。
- デバイスグループの連絡先情報およびパーツ発送情報を設定します。
- デバイスグループ詳細を編集、またはデバイスグループを削除します。

メモ: デバイスのグループ化は、SupportAssist Enterprise の監視機能および自動ケース作成機能には影響しません。

メモ: デバイス グループに設定された連絡先情報およびパーツ発送情報は、「設定」ページで設定されたデフォルトの資格情報、連絡先情報およびパーツ発送情報を上書きします。たとえば、デバイスグループを作成し、デバイスグループのプライマリ連絡先を設定した場合、デバイスグループに含まれている任意のデバイスに関する問題に対する SupportAssist Enterprise の通知すべてがそのデバイスグループに割り当てられたプライマリ連絡先に送信されます。

トピック：

事前定義されたデバイスグループ

SupportAssist Enterprise で使用可能な事前定義されたデバイスグループは次のとおりです。

- **デフォルト** グループ — **デフォルト** グループに割り当てられたデバイスが含まれます。デフォルトでは、デバイスを他のグループに割り当てないかぎり、正常に検出されたすべてのデバイスがこのグループに割り当てられます。
- **ステージング** グループ — 特定の要件を満たしていないために、それらを追加しようとしたときに部分的にのみ検出されたデバイスが含まれます。このグループのデバイスは、要件が満たされた後で再検証した際に、自動的に **デフォルト** グループに移動されます。SupportAssist Enterprise 機能は、このグループ内のデバイスには使用できません。通常、デバイスは、次のケースでステージング グループに追加されます。
  - サーバで、iDRAC に必要なライセンスがインストールされていない
  - Compellent デバイスでは、Dell Compellent Enterprise Manager アプリケーションで SupportAssist が有効にされていない
  - デバイスを追加するための前提条件が満たされていない

デバイス グループの作成

このタスクについて

SupportAssist でデバイスを追加した後、デバイスを別のグループにグループ化できます。連絡先情報、希望連絡時間、連絡方法、グループ内のデバイスのパーツ発送情報を指定できます。

メモ: デバイス グループ パーツの発送先情報は、[連絡先情報] ページで指定したデフォルトのパーツ発送先情報を上書きします。問題の解決にパーツの交換が必要な場合は、ユーザーの同意の下交換用パーツがデフォルトのパーツ発送先住所ではなく、デバイスグループのパーツ発送先住所に送付されます。

メモ: テクニカルサポートの担当者が、サポートケースの解決には、使用中の環境でパーツを交換する必要があると判断した場合に、ユーザーの同意の下、事前に入力してある住所に交換パーツが発送されます。

手順

1. **デバイス** > **デバイス グループの管理**に移動します。
   デバイスグループ ページが表示されます。
2. **グループの作成** をクリックします。
   デバイス グループの作成 ウィンドウの **グループと連絡先の情報** ページが表示されます。
3. **グループの詳細** セクションに、名前と説明を入力します。
4. **連絡先情報** を選択します。
   連絡先情報のフィールドが有効になります。
5. 次の手順を実行します。
   a) 連絡先の種類を選択します。
   b) 名、姓、電話番号、代替電話番号、およびメール アドレスを入力します。
   c) ご希望の連絡方法、連絡時間帯、タイムゾーンを選択します。

   メモ: 連絡先情報 ページに表示されている連絡先情報をコピーするには、連絡先の種類を選択し、連絡先情報 チェック ボックスの下に表示されているリンクをクリックします。
6. **次へ** をクリックします。
   パーツ発送プリファランスのセットアップ (オプション) ページが表示されます。
7. **発送先住所の入力** を選択します。
   一次および二次発送連絡先セクションのフィールドが有効になります。
8. 次のいずれかを選択します。
   - **パーツ発送のみ** - 交換用ハードウェア パーツのみを指定した住所に発送する場合に選択します。
   - **オンサイト サービスによるパーツ発送** - 発送されたハードウェア パーツをオンサイトの技術者が交換する場合に選択します。
9. 一次および二次連絡先を入力します。

   メモ: 「グループおよび連絡先の情報」ページで入力された連絡先情報をコピーするには、[一次配送連絡先] セクションの上に表示されているリンクをクリックします。
10. ご希望の連絡時間帯、国または地域、タイムゾーンを選択し、交換部品を発送する必要がある場所に発送情報を入力します。
11. **発送メモ** ボックスに発送固有の情報を入力します。
12. **作成** をクリックします。
    デバイス グループが作成され、**デバイス グループ** ページに表示されます。

デバイスグループ内のデバイスの管理

前提条件

すでにデバイスグループが作成されていることを確認します。「デバイス グループの作成」を参照してください。

このタスクについて

デバイスグループを作成したら、そのグループにデバイスを追加または削除できます。

メモ: デバイスは 1 つのデバイスグループにのみ含めることができます。

メモ: **既存のグループ間でデバイスを移動することはできません。**

手順

1. **デバイス** > **デバイス グループの管理**に移動します。
   デバイスグループ ページが表示されます。
2. デバイスグループを選択します。
3. **グループ処置の選択** リストで、**デバイスの管理** を選択します。
   デバイスの管理 ウィンドウが表示されます。
4. デバイスグループにデバイスを追加するには、**グループ解除済のデバイス** ペインでデバイスを選択し、 > をクリックします。
   選択したデバイスは **現在のグループ内のデバイス** ペインに移動します。
5. デバイスグループからデバイスを削除するには、**現在のグループ内のデバイス** ペインでデバイスを選択して、 < をクリックします。
   選択したデバイスが **デフォルト** グループに移動され、**グループ解除済のデバイス** ペインに表示されます。
6. **保存** をクリックします。

   メモ: **相関するデバイスのリストを 1 つでも含めたり除外したりすると、別の関連するリストも自動的に含まれたり除外されたりします。デバイスの相互関係の詳細に関しては、「デバイスの相互関係」を参照してください。**

デバイス グループの編集

このタスクについて

連絡先情報、ご希望の連絡方法および時間帯、デバイス グループのパーツの発送先情報を更新することができます。デバイス グループの連絡先情報をアップデートすると、SupportAssist Enterprise は、デバイス グループの連絡先に通知を送信できます。

手順

1. **デバイス** > **デバイス グループの管理**に移動します。
   デバイスグループ ページが表示されます。
2. デバイスグループを選択します。
3. **グループ処置の選択** リストで、**グループの編集** を選択します。
   [デバイス グループの作成] ウィンドウの **[グループと連絡先の情報]** ページが表示されます。
4. **[グループの詳細]** セクションの必要な詳細、プライマリ連絡先情報、セカンダリ連絡先情報を更新します。
5. **次へ** をクリックします。
   パーツ発送プリファランスのセットアップ (オプション) ページが表示されます。
6. 必要なプライマリとセカンダリの配送先情報と配送先住所の詳細を更新します。
7. **アップデート** をクリックします。
   デバイス グループの詳細が更新されます。

デバイスグループの削除

このタスクについて

お好みに合わせてデバイスグループを削除することができます。デバイス グループの削除では、デバイス グループと連絡先の情報のみが削除されます。グループを削除すると、デバイスは自動的に**デフォルト**グループに移動します。SupportAssist によって自動的に作成された**デフォルト**および**ステージング**グループは削除できません。

手順

1. **デバイス** > **デバイス グループの管理**に移動します。
   デバイスグループ ページが表示されます。
2. デバイス グループを選択して、**削除** をクリックします。
   グループを削除するかどうかを確認するメッセージが表示されます。
3. **はい** をクリックします。
   グループが削除され、グループ内のデバイスが**デフォルト**グループに移動します。

8

デバイス検出ルールの管理

デバイス検出ルールにより 1 つまたは複数の IP アドレスの範囲内に存在するデバイスを検出および追加できます。デバイス検出ルールを作成することにより、複数のデバイスを追加しやすくなり、各デバイスを個別に追加する労力を軽減します。

トピック：

デバイス検出ルールの作成

このタスクについて

検出ルールを作成することで、IP アドレスの範囲またはホスト名に基づいてデバイスを検出および追加できます。検出ルールを作成する際、デバイスに適用する必要がある資格情報プロファイルを選択できます。デバイス検出ルールを作成した後は、ルールを直ちに実行するか、スケジュールに基づいてデバイスを検出することができます。

手順

1. **デバイス** に移動して、**Manage Rules for Device Discovery（デバイス検出ルールを管理）** をクリックします。
   検出ルールの管理 ページが表示されます。
2. **Create Discovery Rule（検出ルールの作成）** をクリックします。
   デバイス検出ルールの作成 ウィンドウが表示されます。
3. 検出ルールの名前を入力します。
4. **認証情報プロファイル** リストから、次のいずれかを実行します。「認証情報プロファイルの作成」を参照してください。
   - IP アドレス範囲内にあるデバイス タイプのアカウント資格情報を含む資格情報プロファイルを選択します。
   - 新しい資格情報プロファイルを作成するには、**新しいプロファイルを作成** を選択し、**作成** をクリックします。「認証情報プロファイルの作成」を参照してください。
5. IP アドレス範囲を使用してデバイスを検出するには、次の手順を実行します。
   a) **IP アドレス / 範囲** を選択します。
   b) 検出対象デバイスの IP アドレスまたは IP アドレスの範囲を入力します。

      メモ: 次のいずれかの形式で、異なる IP アドレスの範囲を最大 5 つ追加できます。

      - **10.34.*.***
      - **10.34.1-10.***
      - **10.34.*.1-10**
      - **10.34.1-10.1-10**
      - **10.34.1.1/24**

      メモ: 入力した IP アドレスの範囲が互いに重複しないようにします。

      メモ: Classless-Inter Domain Routing（CIDR）表記で入力された IP アドレスでは（たとえば 10.34.1.1/24）、サブネット マスク エントリが考慮されません。

   c) 複数の IP アドレス範囲を追加するには、**アドレス範囲の追加** をクリックし、次にデバイスの IP アドレスの範囲を入力します。
   d) IP アドレス範囲のサブネット マスクを入力します。

      メモ: デフォルトでは、サブネットマスク値は 255.255.255.0 です。

6. ホスト名または IP アドレスを使用してデバイスを検出するには、次の手順を実行します。

a) **デバイス** を選択します。
b) デバイスのホスト名または IP アドレスを次の形式のコンマ区切り値として入力します。

- 10.34.10.2, 10.34.10.3, 10.34.10.22
- hostname1, hostname2, hostname3
- 10.34.10.22, hostname2, 10.34.10.24

7. 次のいずれかを選択します。
   - **今すぐ実行** - デバイスをすぐに検出します。
   - **1 回実行** - 指定された日付と時刻にデバイスを検出します。
   - **再実行** - 定期的な間隔でデバイスを検出するスケジュールを設定します。
8. **次へ** をクリックします。
   デバイスの検出 ウィンドウが表示されます。資格情報プロファイルに含まれるデバイス タイプに基づいて、自動的にデバイス タイプが選択されます。
9. 必要に応じて、検出しないデバイス タイプをクリアします。
10. **構成設定**セクションで、プリファランスに基づいて次のオプションをクリアします。
    - **詳細な検出を実行** - デバイスとそれに関連するデバイス タイプを検出します。「詳細な検出」を参照してください。
    - **監視を有効化** - SupportAssist Enterprise が、検出されたデバイスで発生する可能性があるハードウェア問題を検知できるようにします。
    - **このデバイスからアラートを受信するよう SNMP を設定** - 検出されたデバイスの SNMP　設定をアラート (SNMP トラップ) が SupportAssist Enterprise に転送されるように自動的に設定します。
    - **最新バージョンの OMSA をインストール** – SupportAssist Enterprise が、検出されたサーバーに最新バージョンの OMSA または iDRAC Service Module (iSM) をインストールできるようにします。システム情報を収集し、デバイスからアラートを生成するには、OMSA または iSM が必要です。
11. **デバイスの追加** をクリックする
    検出ルールが追加され、**検出ルールの管理** ページに表示されます。**今すぐ実行** を選択した場合、デバイスの検出が開始されます。

デバイス検出ルールの編集

このタスクについて

必要に応じて検出ルールを編集できます。

メモ: デバイスの検出を実行中は検出ルールを編集できません。

手順

1. **デバイス** に移動して、**Manage Rules for Device Discovery (デバイス検出ルールを管理)** をクリックします。
   検出ルールの管理 ページが表示されます。
2. 編集する検出ルールを選択し、**編集** をクリックします。
   デバイス検出ルールの編集 ウィンドウが表示されます。
3. IP アドレス範囲を使用してデバイスを検出するには、次の手順を実行します。
   a) **IP アドレス / 範囲** を選択します。
   b) 検出対象デバイスの IP アドレスまたは IP アドレスの範囲を入力します。

   メモ: 次のいずれかの形式で、異なる IP アドレスの範囲を最大 5 つ追加できます。

   - **10.34.*.***
   - **10.34.1-10.***
   - **10.34.*.1-10**
   - **10.34.1-10.1-10**
   - **10.34.1.1/24**

   メモ: 入力した IP アドレスの範囲が互いに重複しないようにします。

   メモ: Classless-Inter Domain Routing (CIDR) 表記で入力された IP アドレスでは (たとえば 10.34.1.1/24)、サブネット マスク エントリが考慮されません。

   c) 複数の IP アドレス範囲を追加するには、**アドレス範囲の追加** をクリックし、次にデバイスの IP アドレスの範囲を入力します。

d) IP アドレス範囲のサブネット マスクを入力します。

メモ: デフォルトでは、サブネットマスク値は 255.255.255.0 です。

4. ホスト名または IP アドレスを使用してデバイスを検出するには、次の手順を実行します。
   a) **デバイス** を選択します。
   b) デバイスのホスト名または IP アドレスを次の形式のコンマ区切り値として入力します。
      - 10.34.10.2, 10.34.10.3, 10.34.10.22
      - hostname1, hostname2, hostname3
      - 10.34.10.22, hostname2, 10.34.10.24
5. **次へ** をクリックします。
   デバイスの検出 ウィンドウが表示されます。
6. デバイスタイプと設定を選択またはクリアします。
7. **ルールの編集** をクリックします。
   検出ルールが更新されます。

デバイス検出ルールを削除

手順

1. **デバイス** に移動して、**Manage Rules for Device Discovery (デバイス検出ルールを管理)** をクリックします。
   検出ルールの管理 ページが表示されます。
2. 削除する検出ルールを選択し、**削除** をクリックします。
   デバイス検出ルールの削除 ウィンドウが表示されます。
3. **はい** をクリックします。
   検出ルールが削除されます。

デバイス検出ルールの実行

このタスクについて

検出ルールを作成したら、いつでもそのルールを実行してデバイスを検出できます。

手順

1. **デバイス** に移動して、**Manage Rules for Device Discovery (デバイス検出ルールを管理)** をクリックします。
   検出ルールの管理 ページが表示されます。
2. 実行する検出ルールを選択し、**今すぐ実行** をクリックします。
   検出ルールに関連付けられているデバイスはすぐに検出されます。

メモ: 検出ルールにより検出されたが、後で到達できないデバイスは 非アクティブ ステータスに移動します。検出ルールが 3 回連続して実行された後もデバイスが 非アクティブ ステータスになると、そのデバイスは自動的に削除されます。

9

デバイス資格情報の管理

SupportAssist Enterprise は、デバイスを追加しシステム情報を収集するために、デバイスの資格情報を必要とします。

次の方法のいずれかを使用して、デバイスに資格情報を入力または割り当てることができます。

- デバイスを追加中
- **編集** オプションの使用により
- アカウントの資格情報または資格情報プロファイルの割り当てにより

トピック：

アカウントの資格情報

アカウント資格情報は、特定のデバイスタイプの資格情報で構成されます。アカウントの資格情報は、SupportAssist Enterprise がデバイスに接続し、システム情報を収集する際に使用されます。環境内のデバイスタイプの数に応じて、アカウント資格情報を 1 つ、または複数作成する必要があります。

アカウント資格情報の追加

このタスクについて

デバイスを追加するか、デバイスに適用できる資格情報プロファイルを作成するには、アカウントの資格情報が必要です。必要に応じて、お使いの環境の各デバイス タイプ用にアカウントの資格情報を作成することができます。

手順

1. **デバイス** > **資格情報の管理** > **アカウントの資格情報** に移動します。
   アカウントの資格情報の管理 ページが表示されます。
2. **資格情報の追加** をクリックします。
   アカウントの資格情報の追加 ウィンドウが表示されます。
3. アカウントの資格情報の一意の名前を入力します。
4. **デバイスタイプ** リストから、デバイスのタイプを選択します。
5. 選択したデバイス タイプの資格情報を入力します。

   メモ: 入力した資格情報には管理者権限が必要です。

   - **サーバ / ハイパーバイザー** デバイスを選択した場合は、**オペレーティング システム タイプ** リストでオペレーティング システムを選択し、該当するフィールドにデバイスのユーザー名とパスワードを入力します。

     入力するユーザー名とパスワードには、ルート権限または sudo ユーザー権限が必要です。sudo ユーザーのユーザー名とパスワードを入力する場合は、その sudo ユーザーが SupportAssist Enterprise に設定されていることを確認します。sudo ユーザーの設定方法については、「Linux を実行するサーバー上の SupportAssist Enterprise の sudo アクセスを設定」を参照してください。
   - シャーシ、**Fluid File System (FluidFS)**、**iDRAC**、または **Storage Center (SC) /Compellent** の各デバイスを選択した場合は、適切なフィールドにデバイスのユーザー名とパスワードを入力します。
   - **ソフトウェア**では、**ソフトウェアタイプの選択** リストからソフトウェアのタイプを選択し、適切なフィールドにユーザー名とパスワードを入力します。
   - **ソリューション** デバイスの場合、適切なフィールドに SSH と REST の資格情報を入力します。
   - **ネットワーク** デバイスを選択した場合は、適切なフィールドにユーザー名、パスワード、およびコミュニティ文字列を入力し、デバイスのパスワードを有効にします。

     メモ: コミュニティ文字列は次のネットワークデバイスに必要です。

- **PowerConnect ファミリ 28xx および X シリーズ**
- **Cisco**
- **ワイヤレスコントローラ**

メモ: 有効なパスワードは、ネットワークデバイスに有効なパスワードが設定されている場合にのみ必要です。

- **Peer Storage (PS) /EqualLogic** デバイスを選択した場合は、適切なフィールドにデバイスのユーザー名、パスワード、およびコミュニティ文字列を入力します。

メモ:

- **アカウントの認証情報は、Storage ME4 Series デバイスを追加するために必須です。**
- **アカウントの認証情報は、Storage MD Series デバイスを追加する際には必要ありません。**

6. **保存** をクリックします。
アカウントの資格情報が **アカウントの資格情報の管理** ページに表示されます。

アカウント資格情報の編集

このタスクについて

必要に応じてアカウントの資格情報を編集します。たとえば、関連するデバイス タイプの資格情報に変更があった場合は、アカウント資格情報を編集する必要があります。

メモ: デバイスタイプの変更はサポートされません。

メモ: アカウント資格情報の名前の編集は、アカウント資格情報がデバイスに割り当てられていない場合にのみ可能です。

手順

1. **デバイス** > **資格情報の管理** > **アカウントの資格情報** に移動します。
アカウントの資格情報の管理 ページが表示されます。
2. 編集するアカウント資格情報を選択し、**編集** をクリックします。
アカウントの資格情報の編集 ウィンドウが表示されます。
3. 必要に応じて資格情報を更新します。
4. **アップデート** をクリックします。
アカウント資格情報が更新されます。アカウント資格情報が割り当てられているデバイスが再検証されます。

アカウントの資格情報の再割り当て

手順

1. **デバイス** > **デバイスを表示** に移動します。
デバイス ページが表示されます。
2. デバイスを選択し、[**編集**] をクリックします。
アカウントの編集 ウィンドウが表示されます。
3. **アカウントの資格情報** リストからアカウント資格情報を選択します。

メモ: 選択したデバイス タイプに対してすでに作成したアカウント資格情報のみがアカウント資格情報リストに表示されます。

4. 次のいずれかの手順を実行してください。
   - デバイスが**デフォルト**グループに属している場合は、[**保存**] をクリックします。
   - デバイスが**ステージング**グループに属している場合は、[**再検証**] をクリックします。

アカウント資格情報の削除

前提条件

削除するアカウント資格情報は、デバイスに割り当てないでください。

手順

1. **デバイス** > **資格情報の管理** > **アカウントの資格情報** に移動します。
   アカウントの資格情報の管理 ページが表示されます。
2. 削除するアカウント資格情報を選択し、**削除** をクリックします。
   アカウント資格情報の削除 ウィンドウが表示されます。
3. **はい** をクリックします。

資格情報プロファイル

資格情報プロファイルは、さまざまなデバイスタイプのアカウント資格情報のコレクションです。資格情報プロファイルを使用することで、各デバイスの資格情報を手動で入力する代わりに、デバイスに資格情報のセットを適用することができます。

認証情報プロファイルの作成

このタスクについて

認証情報プロファイルを作成すると、デバイスに認証情報を割り当てることができます。

手順

1. **デバイス** > **資格情報の管理** > **資格情報プロファイル** に移動します。
   資格情報プロファイルの管理 ページが表示されます。
2. **プロファイルの作成** をクリックします。
   資格情報プロファイルの作成 ウィンドウが表示されます。
3. **名前** ボックスに、認証情報プロファイルの一意の名前を入力します。
4. プロファイルに含めるデバイスタイプを選択します。

   サーバ / ハイパーバイザ、**ソフトウェア**、および **ソリューション** では、+ をクリックしてデバイスタイプのリストを展開します。

   アカウント資格情報 リストが選択できます。
5. **アカウントの認証情報** リストから、デバイス タイプに割り当てるアカウント認証情報を選択します。

   メモ: デバイス タイプ用にアカウント認証情報を作成していない場合は、アカウントの認証情報には使用不可と表示されます。新しいアカウント認証情報を作成するには、アカウント認証情報の追加 をクリックします。アカウント認証情報の作成に関する詳細については、「アカウント資格情報の追加」を参照してください。
6. 認証情報プロファイルに含める各デバイス タイプのために、手順 4 および 5 を繰り返します。
7. **保存** をクリックします。
   資格情報のプロファイルが **資格情報プロファイルの管理** ページに表示されます。

認証情報プロファイルの編集

このタスクについて

必要に応じて、プロファイルの資格情報を更新できます。たとえば、資格情報プロファイルを編集して、新しいアカウントの資格情報を追加したり、デバイスタイプのアカウント資格情報を変更したりすることができます。

メモ: 認証情報プロファイルの名前のアップデートはサポートされません。

手順

1. **デバイス** > **資格情報の管理** > **資格情報プロファイル** に移動します。
   資格情報プロファイルの管理 ページが表示されます。
2. 編集する認証情報プロファイルを選択し、**編集** をクリックします。
   資格情報プロファイルの編集 ウィンドウが表示されます。
3. アカウント認証情報を編集するデバイス タイプを選択します。
   アカウント資格情報 リストが選択できます。
4. **アカウントの認証情報** リストから、デバイス タイプに割り当てるアカウント認証情報を選択します。
5. **アップデート** をクリックします。

認証情報プロファイルがアップデートされます。認証情報プロファイルが割り当てられているデバイスが再検証されます。

認証情報プロファイルの割り当て

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. **認証情報プロファイルの割り当て** リストから 1 つまたは複数のデバイスを選択し、認証情報プロファイルを選択します。
   認証情報プロファイルが選択したデバイスに割り当てられます。認証情報プロファイルが割り当てられているデバイスが再検証されます。

資格情報プロファイルに関連付けられたデバイスを表示

手順

1. **デバイス** > **資格情報の管理** > **資格情報プロファイル** に移動します。
   資格情報プロファイルの管理 ページが表示されます。
2. 資格情報プロファイルを選択します。
   資格情報プロファイルに関連付けられているデバイスが資格情報プロファイルの概要ペインに表示されます。

資格情報プロファイルの割り当てに要する概算時間

資格情報プロファイルの割り当ては、デバイスタイプ、デバイス数、ネットワーク帯域幅によって長くなる場合があります。

次の表は、資格情報プロファイルの割り当てに要する概算時間をデバイス数ごとに示しています。

表 13. デバイス数と資格情報プロファイルの割り当て時間

デバイス数	資格情報プロファイルの割り当てにかかる時間
5	3 分
50	15 分
100	30 分
1000	6 時間
1500	9 時間
2000	12 時間
3000	17 時間

認証情報プロファイルの削除

前提条件

削除する認証情報プロファイルは、デバイスに割り当てないでください。

手順

1. **デバイス** > **資格情報の管理** > **資格情報プロファイル** に移動します。
   資格情報プロファイルの管理 ページが表示されます。
2. 削除する認証情報プロファイルを選択し、**[削除]** をクリックします。
   資格情報プロファイルの削除 ウィンドウが表示されます。
3. **はい** をクリックします。

10

デバイスインベントリの検証

サイトインベントリの検証は、使用しているデバイスで、SupportAssist Enterprise の次の機能が使用可能かどうかを確認します。

- **接続ステータス** - デバイスにインターネット接続性があり、デバイスで必要なポートが開いているかどうかを確認します。デバイスに必要な資格情報が正しく かつ使用可能であることも確認します
- **コレクション機能ステータス** - デバイスでシステム情報を収集するための要件が満たされているかどうかを確認します。
- **監視ステータス** - OMSA の最新バージョンがサーバーにインストールされているかどうかを確認します。SNMP トラップ送信先と iDRAC トラップ送信先が設定されているかどうかも確認します

  メモ: 監視機能のテストは Linux、iDRAC でのみサポートされます。

インベントリの検証中に、デバイスのステータスが更新されます。

- 検証に成功すると、デバイスはデフォルトグループに移動します。
- 検証に失敗すると、デバイスはステージングまたは非アクティブグループに移動します。

メモ: インベントリの検証が進行している間、デバイスは無効にされます。デバイスの操作の状態を表示するには、マウスポインタをデバイス上に移動します。

メモ: サイト インベントリの検証テーブルのデバイスの合計数が、進行状況インジケータに表示されるデバイスの合計数と一致しない場合があります。進行状況インジケータのデバイスカウントは、インベントリの定期検証が開始されるとき、または SupportAssist Enterprise が新バージョンにアップグレードされるときに割り当てられる一方で、サイトインベントリ検証テーブルのデバイスカウントは、以下のときに更新されます。

- **関連するデバイスの一部が詳細な検出プロセスの一部として検出される**
- **新規デバイスが SupportAssist Enterprise に追加される**

SupportAssist Enterprise に管理者としてログインし、**デバイス サイト インベントリ検証**にアクセスして**サイト インベントリ検証** ページを表示します。インベントリの検証機能は、次のデバイスに対してのみ使用できます。

- サーバ / ハイパーバイザー
- iDRAC
- シャーシ
- Fluid File System (Fluid FS)
- ネットワーク
- Storage Center (SC) / Compellent
- PowerVault
- ソフトウェア
- ウェブスケール ハイパー コンバージド アプライアンス

トピック：

インベントリ検証を手動で開始

このタスクについて

デバイスでインベントリ検証を実行して、デバイスのステータスを確認できます。インベントリの検証機能は、次のデバイスまたはデバイス モデルに対してのみ使用できます。

- サーバ / ハイパーバイザー
- iDRAC
- シャーシ
- データ ストレージ：

- Fluid File System (Fluid FS)
- Storage Center (SC) / Compellent
- PowerVault
- PeerStorage (PS) / EqualLogic

- ネットワーク
- ソフトウェア
- ハイパーコンバージド インフラストラクチャー :
  - Web スケール

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. つ以上のデバイスを選択して、**インベントリの検証**をクリックします。
   SupportAssist Enterprise により、デバイスの接続ステータスが確認されます。
   メモ: 正常に検証されたデバイスの数と、検証に失敗したデバイスの数を表示するには、サイトインベントリの検証 ページを参照してください。

自動インベントリ検証のスケジュール

このタスクについて

インベントリ検証はデフォルトでは毎月のランダムに決定された日の午後 11 時にスケジュールされます。必要な場合は 要件に応じてスケジュールを変更できます

手順

1. **設定** > **プリファランス** に移動します。
   プリファランス ページが表示されます。
2. **インベントリ検証を自動的に開始** セクションで、インベントリ検証を開始する日を選択します。
3. **適用** をクリックします。

サイトインベントリの検証

サイトインベントリの検証ページには、次のセクションが表示されます。

- 検証テストのステータス - インベントリ検証で実行されたテストのタイプを表示します。
- 進行状況インジケータ - インベントリ検証のステータスを示します。
- 履歴 - インベントリ検証テストの履歴が表示されます。

次の表に、「**サイトインベントリの検証**」ページの**[検証テスト]**セクションに表示される項目の情報を示します。

表 14. 検証テストのステータス

フィールド	説明
検証テスト	インベントリ検証で実行されたテストのタイプ。
成功	と正常に検証されたデバイス数のロールアップ回数。
失敗	と正常に検証されなかったデバイス数のロールアップ回数。
その他	ステータスアイコンと次のデバイス数のロールアップ回数を表示します。 - SupportAssist Enterprise によってサポートまたは監視されていない可能性があるデバイス - アダプタ経由で SupportAssist Enterprise に追加または検出されたデバイス - 接続性テストに失敗したデバイス

フィールド	説明
	· 監視を無効にしたデバイス

次の表に、**サイトインベントリの検証**ページの履歴セクションに表示される項目の情報を示します。

表 15. インベントリ検証の履歴

フィールド	説明
開始済み	定期インベントリ検証が開始された日時。
完了しました	定期インベントリ検証が完了した日時。
最後の更新	定期インベントリ検証が最後に実行された日時。

11

SupportAssist Enterprise のケース

SupportAssist によって監視されているデバイスで問題が検出されると、サポート ケースが自動的に作成されます。SupportAssist によって作成されたすべてのケースは、**ケース** ページに表示されます。

メモ: SupportAssist Enterprise は、監視対象デバイスから受け取ったアラートすべてに対してサポートケースを作成するわけではありません。サポートケースが作成されるのは、デバイスから受け取ったアラートのタイプと件数が、サポートケース作成に対して Dell EMC が定義した条件と一致した場合のみです。

SupportAssist Enterprise がインターネット経由で Dell サポート ケースおよびサービス契約のデータベースに接続すると、有効な サービスタグがあるサポート対象デバイスのサポートケース情報が自動的に利用可能になります。サポートケース情報が更新されるのは、次の状況下のみです。

- 「**ケース**」ページを開くとき。
- 「**ケース**」ページの **[更新]** をクリックするとき。
- 「**ケース**」ページを開いて、 Web ブラウザー ウィンドウを更新するとき。

利用可能なケース管理オプションを使用して、次のアクティビティを実行するようテクニカルサポートに要求することもできます。

- サポートケースに関連するアクティビティをサスペンド
- サポートケースに関連するアクティビティを再開
- サポートケースのクローズ

ケース管理オプションは、次のデバイスに対して SupportAssist Enterprise によって自動的に開かれたサポートケースにのみ適用されます。

- サーバ / ハイパーバイザー
- iDRAC
- シャーシ
- ネットワーク
- データ ストレージ :
  - PeerStorage (PS) / EqualLogic
  - PowerVault

SupportAssist Enterprise が未解決サポートケースアップデートを完了したあとは、**ケース** ページに現在のサポートケースが表示されます。「**ケース**」ページに表示されるフィールドおよび詳細の情報については、「ケース」を参照してください。

トピック :

特定のデバイスに対するサポートケースを表示

このタスクについて

SupportAssist Enterprise によって監視されている特定のデバイスの未解決のサポートケースを表示します。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. サポートケースをチェックするデバイスを選択します。
   デバイス概要 ペインが表示されます。

メモ: **デバイス ページで 1 台のデバイスが選択されている場合のみ、デバイス概要 ペインが表示されます。**

3. **タスク** リストから、**ケースの確認** を選択します。
   - デバイスにサポートケースがある場合、**ケース** ページが表示されます。デバイス上のすべてのサポートケースは、**ケース** ページの最上部に表示されます。
   - デバイスにサポートケースが存在しない場合、該当するメッセージが表示されます。
   - SupportAssist Enterprise がサポート ケース情報を取得できない場合は、メッセージが表示されます。

ケースアクティビティの 24 時間停止を要求する

このタスクについて

必要に応じて、サポート ケースに関連するアクティビティを 24 時間停止するようテクニカル サポートに要求できます。たとえば次のようなケースで、あるサポート ケースについてアクティビティを一時停止するよう、テクニカル サポートに要求する場合があります。

- テクニカルサポートのサポートを受けず、問題を解決したい場合
- 計画されたメンテナンス アクティビティ中に、Dell EMC からサポート ケースに関連する通知の受信を希望しない場合

メモ: **サポート ケースが SupportAssist で開かれた場合のみ、サポート ケースに関連するアクティビティを停止するようテクニカル サポートに要求できます。**

手順

1. **ケース** に移動し、**ケースの表示** をクリックします。
   ケース ページが表示されます。
2. **絞り込みの条件** ペインの、**ソースタイプ** リストで、**SupportAssist** を選択します。
   SupportAssist によって開かれたすべてのケースのリストが表示されます。
3. 一時停止するサポートケースを選択します。

   メモ: **ケースオプション リストは、選択したサポートケースが SupportAssist によって開かれた場合のみ有効になります。**

   メモ: **動作を 24 時間一時停止 オプションは、選択されたサポートケースの通知を一時停止するよう、以前に要求していた場合、無効になります。**
4. **ケースオプション** リストから、**動作を 24 時間一時停止** を選択します。
   通知を 24 時間一時停止 ウィンドウが表示されます。
5. オプションで、サポート ケースのアクティビティを一時停止するよう要求する理由を入力します。
6. **OK** をクリックします。
   ケースをアップデートしています というメッセージが表示されます。ケースが正常にアップデートされると、**ケースステータス** メッセージが表示されます。
7. **OK** をクリックします。
   サポートケースは **一時停止** ステータスを表示します。

   メモ: **SupportAssist Enterprise が要求を処理できない場合、該当するエラーメッセージが表示されます。このようなケースでは、ケース作成テストを実行してデルへの接続を検証できます。その後、操作を再試行します。**

サポートアクティビティの再開を要求

このタスクについて

以前に、サポートケースのアクティビティを一時停止するように要求していた場合、サポートケースのアクティビティを再開するようテクニカルサポートに要求できます。

手順

1. **ケース** に移動し、**ケースの表示** をクリックします。
   ケース ページが表示されます。
2. **絞り込みの条件** ペインの、**ソースタイプ** リストで、**SupportAssist** を選択します。
   SupportAssist Enterprise によって開かれたすべてのケースのリストが表示されます。
3. テクニカルサポートにケースの活動を再開させたいサポートケースを選択します。

メモ: **ケースオプション リストは、選択したサポートケースが SupportAssist Enterprise によって開かれた場合のみ有効になります。**

メモ: **動作を再開 オプションは、選択されたサポートケースの通知を一時停止するよう、以前に要求していた場合のみ有効になります。**

4. **ケースオプション** リストから **動作を再開** を選択します。
   動作を再開 ウィンドウが表示されます。
5. 必要に応じて、サポートケースのアクティビティの再開を要求する理由を入力します。
6. **OK** をクリックします。
   ケースをアップデートしています というメッセージが表示されます。ケースが正常にアップデートされると、**ケースステータス** メッセージが表示されます。
7. **OK** をクリックします。
   サポートケースは適切なステータスを表示します。

   メモ: **SupportAssist Enterprise が要求を処理できない場合、該当するエラーメッセージが表示されます。このようなケースでは、ケース作成テストを実行して Dell EMC への接続を検証できます。その後、再試行します。**

サポートケースを閉じる要求

このタスクについて

デバイスに関する不具合を解決した場合は、テクニカルサポートに対応するサポートケースを閉じるよう要求できます。

メモ: **サポートケースを SupportAssist Enterprise で開いた場合のみ、サポートケースを閉じるようにテクニカル サポートに要求できます。**

メモ: **終了 および クローズ依頼済 を除く任意のステータスのサポートケースを閉じるようにテクニカルサポートに要求できます。**

手順

1. **ケース** に移動し、**ケースの表示** をクリックします。
   ケース ページが表示されます。
2. **絞り込みの条件** ペインの、**ソースタイプ** リストで、**SupportAssist** を選択します。
   SupportAssist Enterprise によって開かれたすべてのケースのリストが表示されます。
3. 閉じるサポートケースを選択します。

   メモ: **ケースオプション リストは、選択したサポートケースが SupportAssist Enterprise によって開かれた場合のみ有効になります。**
4. **ケースオプション** リストから **閉じるよう要求** を選択します。
   このケースを閉じるように依頼 ウィンドウが表示されます。
5. オプションで、サポートケースを閉じるよう要求する理由を入力します。
6. **OK** をクリックします。
   ケースをアップデートしています というメッセージが表示されます。ケースが正常にアップデートされると、**ケースステータス** メッセージが表示されます。
7. **OK** をクリックします。
   サポートケースは **クローズ依頼済** ステータスを表示します。

   メモ: **サポートケースを閉じるように要求した後、サポートケースを閉じる前に、詳細情報を取得するためにテクニカルサポートが連絡する場合があります。**

   メモ: **SupportAssist Enterprise が要求を処理できない場合、該当するエラーメッセージが表示されます。このようなケースでは、ケース作成テストを実行して Dell EMC への接続を検証できます。その後、再試行します。**

ケース

ケース ページには、SupportAssist Enterprise に追加されたデバイスのサポートケースが表示されます。ProSupport、ProSupport Plus、データセンター向け ProSupport Flex、データセンター向け ProSupport One のサービス計画のあるデバイスでは、「**ケース**」ページには、ケースの作成方法に関係なく、ケースのステータスを表示します。デフォルトでは、表示されるサポートケースは、それぞれのデバイス名またはデバイスの IP アドレスの下にグループ化されます。グループヘッダーに表示される最終更新日時は、ケース情報がバックエンドから取得された前回の日時を示します。

次の表に、**ケース** ページに表示されるオプションとサポートケース情報を示します。

表 16. ケース ページ

列名	説明
検索基準 リスト	表示されているデータの特定のカテゴリでケースを検索します。
検索語句	検索キーワードを入力します。 **メモ: 検索を実行するには 3 文字以上入力する必要があります。**
ケースオプション リスト	要件に基づいて、SupportAssist Enterprise によって開かれたサポートケースを管理します。使用できるオプションは次のとおりです。 • **動作を 24 時間一時停止** - サポート ケースに関連するアクティビティを 24 時間中断するようテクニカル サポートに依頼します。テクニカル サポートは、24 時間後にサポートケースに関連するアクティビティを自動的に再開します。「ケースアクティビティの 24 時間停止を要求する」を参照してください。 • **動作を再開** - サポート案件に関連するアクティビティを再開するには、テクニカル サポートに依頼します。「サポートアクティビティの再開を要求」を参照してください。 **メモ: 動作を再開 オプションは、サポートケースに関連するアクティビティを一時停止するよう、以前に要求していた場合のみ有効です。** • **クローズ依頼** - テクニカル サポートに依頼してサポート ケースをクローズします。「サポートケースを閉じる要求」を参照してください。 このリストは、SupportAssist Enterprise が次のデバイスまたはデバイスモデルに対して開いたケースに対してのみ有効になります。 • サーバー / ハイパーバイザー • iDRAC • シャーシ • ネットワーク • PeerStorage (PS) / EqualLogic • PowerVault
更新	表示されているケースリストを更新します。
ケースを取得中	ケースがお使いのデバイスに存在している場合は、SupportAssist Enterprise の検証中に進捗インジケータが表示されます。
TechDirect	新しいウェブブラウザウィンドウで **Dell EMC TechDirect** ホームページが開きます。
チェックボックス	ケース管理アクションを実行するためのサポートケースを選択します。 **メモ: チェックボックスは、SupportAssist Enterprise により自動的に作成されたケースに対してのみ表示されます。**
名前 /IP アドレス	デバイスに指定されている情報に応じた名前、ホスト名、または IP アドレス。デバイス名はリンクとして表示され、このリンクをクリックすると **デバイス** ページが表示されます。
番号	サポートケースに割り当てられた数字の ID。
ステータス	サポートケースの現在の状態。サポートケースのステータスは、以下のいずれかです。 • **提出済み** — SupportAssist Enterprise がサポートケースを提出しました。 • **オープン** — テクニカル サポートは提出されたサポートケースへの対応を開始しました。 • **進行中** または **対応中** — テクニカル サポートはサポートケースに対応中です。 • **割り当て中** — サポートケースはまだテクニカル サポート担当者に割り当てられていません。 • **お客様による延期** — テクニカル サポートはお客様の要望でサポートケースを延期しました。 • **再オープン** — サポートケースは以前にクローズされており、再開されました。 • **一時停止** — テクニカル サポートは依頼に基づいてサポートケースに関連するアクティビティを 24 時間中断しました。 • **クローズ依頼済** — テクニカル サポートにサポートケースを閉じるよう依頼しました。 • **クローズ済** — サポートケースがクローズしています。 • **適用なし** — SupportAssist Enterprise によって不具合が検出されましたが、デバイスの保証または基本的なハードウェア保証の有効期限が切れているために、サポートケースが作成されませんでした。

列名	説明
	• **使用不可** — サポートケースのステータスを Dell から取得できませんでした。 • **不明** — SupportAssist Enterprise はサポートケースの状況を判別できません。
タイトル	次を特定するサポートケース名です。 • サポートケースの生成方法 • デバイスモデル • デバイスのオペレーティングシステム • アラート ID (存在する場合) • アラートの説明 (存在する場合) • 保証ステータス • 解決案の説明
開始日付	サポートケースの対応を開始した日時。
サービス契約	デバイスに適用される Dell EMC のサービス契約レベル。**サービス契約** 列には次のような内容が表示されます。 • **不明** — SupportAssist Enterprise はサービス契約を判別できません。 • **無効なサービスタグ** — デバイスのサービスタグが無効です。 • **サービス契約なし** — このデバイスは Dell EMC サービス契約の対象ではありません。 • **サービス契約期限切れ** — デバイスのサービス契約の期限が切れています。 • **ベーシック サポート** — お使いのデバイスは Dell EMC ベーシック ハードウェア サービスの契約対象です。 • **ProSupport** — お使いのデバイスは Dell EMC ProSupport のサービス契約対象です。 • **ProSupport Plus** — お使いのデバイスは Dell EMC ProSupport Plus のサービス契約対象です。 • **データ センター向け ProSupport Flex** — お使いのデバイスは Dell EMC ProSupport Flex for Data Center のサービス契約対象です。 • **データ センター向け ProSupport One またはデータ センター向け ProSupport Flex** - デバイスには Dell EMC データ センター向け ProSupport One、またはデータ センター向け ProSupport Flex サービス契約が適用されています。
サービス タグ/シリアル ナンバー	Dell EMC がデバイスを認識できる一意の英数字 ID。

メモ: 特定のデバイスのサポートケースを確認する場合、そのデバイスのサポートケースは、ケース ページの一番上の適切な行に青い境界線で表示されます。「特定のデバイスに対するサポートケースを表示」を参照してください。

絞り込みの条件 ペインでは、表示されているデバイスのリストを絞り込むことができます。デバイスタイプ、ケースステータス、サービス契約、またはソースタイプに基づいてリストを絞り込むことができます。

12

収集の表示

SupportAssist Enterprise は、追加した各デバイスからシステム情報を収集し、その情報をセキュアにバックエンドに送信します。通常、システム情報は次のように収集されます。

- 定期的 - **環境設定** ページで指定されている事前定義された収集開始日に応じて一定の間隔で収集されます。
- ケース作成時 - SupportAssist Enterprise によって認識された問題に対してサポートケースが作成されたときに収集されます。
- 手動 (オンデマンド) - テクニカル サポートが要請した場合、1 つ、または複数のデバイスからシステム情報の収集をいつでも開始できます。

メモ: デフォルトでは、SupportAssist Enterprise は登録が完了した後でのみ、システム情報を定期的およびケース作成時に収集します。登録の詳細については、「SupportAssist Enterprise の登録」を参照してください。

SupportAssist Enterprise を使用すると、複数のデバイスからシステム情報を収集し、Dell EMC に送信できます。複数のデバイスからのシステム情報の収集の詳細については、「複数のデバイスからシステム情報を手動で収集する」を参照してください。

手動で収集をバックエンドにアップロードすることや、SupportAssist で次のデバイスまたはデバイスモデルの収集を自動的に開始することができます。

- サーバー/ハイパーバイザー
- iDRAC
- シャーシ
- ネットワーク
- データ ストレージ :
  - PeerStorage (PS) または EqualLogic
  - PowerVault

次のデバイスまたはデバイス モデルの場合、収集はデバイスからバックエンドに直接送信され、収集の詳細が「**収集**」ページに表示されません。

- データ保護
- Web スケール以外のすべてのハイパーコンバージド インフラストラクチャ デバイスモデル。
- Peer Storage (PS) または EqualLogic、Storage Center (SC) または Compellent、Fluid File System (Fluid FS)、および PowerVault 以外のすべてのデータ ストレージ デバイスのモデル。

収集したシステム情報は、収集タスクを実行するアプリケーションをホストするサーバ上に保存されます。SupportAssist Enterprise によって実行される収集タスクは、SupportAssist Enterprise が導入されているサーバーに保存されます。**デバイス** または **収集** ページから SupportAssist Enterprise により実行される収集にアクセスできます。収集で利用できるシステム情報は、SupportAssist Enterprise で利用できる **設定ビューア** に表示されます。

メモ: 設定ビューア で表示できるのは、最近の 5 件のシステム情報のみです。30 日以上前のシステム情報および、過去 30 日間における最新の 5 つの収集よりも古いシステム情報は、自動的にパージされます。収集のパージ タスクは毎日午後 10 時に自動的に実行されます (SupportAssist Enterprise が導入されているサーバーの時刻)。

メモ: 設定ビューア は、Fluid File System (FluidFS) を使用してストレージデバイスから収集したシステム情報の表示をサポートしていません。

メモ: 英語版以外のオペレーティング システムを実行しているデバイスからの収集の場合は、設定ビューア で特定の属性が表示されない場合があります。

メモ: 「収集」ページには、過去 7 日間に収集されたシステム情報のみが表示されます。7 日以上経過した収集を表示するには、日付フィルターを使用して収集のリストを表示します。

トピック :

- [デバイス] ページからコレクションを表示
- 収集ページから収集を表示
- 設定ビューア
- サーバからの定期的な収集で報告されるアイテム
- 複数のデバイスの取集をダウンロードして表示する

[デバイス] ページからコレクションを表示

このタスクについて

デバイス概要ペインには、特定のデバイスに対して実行された収集が一覧されます。収集リストから、表示したいすべてのコレクションを選択できます。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. 収集を表示するデバイスを選択します。
   デバイス概要 ペインが表示されます。

   メモ: デバイスからコレクションが実行されていない場合、コレクション フィールドに コレクションなし と表示されます。
3. **収集** リストから、収集の日付と時刻を選択します。
   デバイスからコレクションが実行されていない場合、**コレクション** フィールドに **コレクションなし** と表示されます。
   デバイスがサーバの場合、**設定ビューア** は、新しく開かれた Web ブラウザウィンドウに表示されます。その他すべてのデバイス タイプおよび複数のデバイス コレクションでは、コレクションを .zip ファイルとして保存するように求められます。ダウンロードしたコレクションを表示するには、.zip ファイルを解凍して `index.html` ファイルをクリックします。

収集ページから収集を表示

このタスクについて

収集 ページは、正常に実行された収集をすべて一覧します。収集リストから、表示したいすべてのコレクションを選択できます。

手順

1. **コレクション** > **コレクションを表示** に移動します。
   収集 ページが表示されます。
2. 表示する収集を選択します。
   収集の概要 ペインが表示されます。
3. **表示** (サーバ収集の場合) または **ダウンロード** (他のすべてのデバイスタイプおよび複数のデバイス収集の場合) をクリックします。
   サーバからの収集の場合、**設定ビューア** は、新しく開かれた Web ブラウザウィンドウに表示されます。その他すべてのデバイスタイプおよび複数デバイスからの収集では、収集をダウンロードして ZIP ファイルとして保存します。ダウンロードしたコレクションを表示するには、.zip ファイルを解凍して `index.html` ファイルをクリックします。

設定ビューア

設定ビューア では、SupportAssist Enterprise がデバイスから収集したシステム情報を表示することができます。**Configuration Viewer (設定ビューア)** にタブ形式で情報が表示されます。収集されたシステム情報は、**設定ビューアを** でさまざまなカテゴリとサブカテゴリに分けられて表示されます。

構成ビューアが では **概要** カテゴリも表示されます。**概要** カテゴリを選択すると、次の内容が表示されます。

- システム情報を収集した時点の SupportAssist Enterprise のデータ収集設定
- 収集したシステム情報で検出されたエラーの概要
- デバイスに関する簡単な情報

Configuration Viewer (設定ビューア) は、次で構成されます。

- 上部ペイン - 収集データのさまざまなカテゴリとサブカテゴリがメニュー形式で表示されます。メニューの上にマウスポインタを移動して、サブ項目を表示することができます。**すべて展開** または **すべて折りたたむ** をクリックしてすべてのカテゴリを素早く展開したり、折りたたんだりすることができます。加えて、上部ペインには **Contacts (担当者)** タブと **Section Status (セクションステータス)** タブも表示されます。
  - **担当者** - ケースの詳細、SupportAssist Enterprise の登録時に入力したお客様情報、コレクションの詳細、アプリケーション情報を表示します。**担当者** タブはデフォルトのタブです。
  - **セクション ステータス** - 収集のセクション レベル情報の概要を表示します。このタブには、収集の各セクションのステータスと説明が表示されます。**セクション ステータス** に表示されるアイテムの数は、デバイスの構成に応じて異なります。

Section Status（セクションステータス）セクションには収集のカウント数とステータスも表示されます。使用可能なステータスは次のとおりです。

- **成功**
- **失敗**
- **警告**

- 下部ペイン - 収集の詳細が表示されます。下部ペインには、上部ペインで選択されたカテゴリまたはサブカテゴリで入手できる情報も表示されます。収集の詳細を表示するには、サブ項目のいずれかをクリックします。カテゴリをクリックすると、カテゴリが展開され、そのサブカテゴリが表示されます。下部ペインにはナビゲーショントレイルも含まれています。クリックすると、現在のトレイルを逆方向に移動できます。

収集の実行元のデバイスのタイプに応じて、複数デバイス設定ビューアには、デバイスタイプごとに次のタブが表示されます。

メモ: デバイスからの ID 情報のコレクションを無効にしている場合は、ホスト名や IP アドレスなどの ID 情報は収集されたシステム情報内でトークン化された値に置き換えられます。トークン化された値はトークン *n* として表示されます。たとえば、トークン 0、トークン 1、トークン 2 のようになります。

メモ: サーバーからのコレクションで報告される可能性のあるアイテムのリストについては、「サーバからの定期的な収集で報告されるアイテム」を参照してください。

メモ: 設定ビューア は、Fluid File System（FluidFS）を使用してストレージデバイスから収集したシステム情報の表示をサポートしていません。

ログの種類

設定ビューアを使って、SupportAssist Enterprise によって収集されたシステム情報から次の 2 種類のログにアクセスすることができます。

構造化されたログ	アプリケーションログ、組み込みサーバ管理（ESM）ログ、SMART ログ、イベントログが含まれます。**体系化ログ** カテゴリをクリックすると、設定ビューアに使用可能な体系化ログのリストが表示されます。リストにある構造化ログのいずれかをクリックして、新しいウェブブラウザウィンドウにログの詳細を表示できます。
非構造化ログ	リモートアクセスコントローラー（RAC）ログなど、システムファイルのスナップショットが含まれます。**非体系化ログ** カテゴリをクリックすると、設定ビューアに使用可能な非体系化ログのリストが表示されます。 **メモ: 非体系化ログは設定ビューア内に表示することはできません。非体系化ログを保存し、適切なアプリケーションを使って、ログの詳細を表示することのみ可能です。**

サーバからの定期的な収集で報告されるアイテム

サーバから収集されるシステム情報で報告されるアイテムは、以下によって異なります。

- SupportAssist Enterprise でデバイスの追加に使用する**デバイスタイプ**
- 収集の種類（手動、定期的、またはサポートケース）

サーバから定期的に収集されるシステム情報で報告されるアイテムの概要を次の表に示します。

メモ: サポートケースの作成で実行される収集および手動で開始された収集のシステム情報は、定期収集で収集されたシステム情報と比較するとより詳細になります。SupportAssist Enterprise によって収集されるアイテムの包括的なリストについては、で『*SupportAssist Enterprise Version 4.0 Reportable Items*』（SupportAssist Enterprise バージョン 4.0 報告可能アイテム）の文書を参照してください。

メモ: 定期コレクションのシステム情報により、Dell EMC はプロアクティブなファームウェア推奨、およびその他レポートによって、保守された状態の会社環境設定に対する見解を提供します。

表 17. サーバからの定期的な収集で報告されるアイテム

報告されるアイテム	デバイスタイプを サーバ / ハイパーバイザー として SupportAssist Enterprise に追加したデバイス		デバイスタイプを iDRAC として SupportAssist Enterprise に追加したデバイス
	OMSA はデバイスにインストールされています。	OMSA はデバイスにインストールされていません。	
メモリ	✓	✗	✓
メモリアレイ	✓	✗	✓
Memory Operating Mode (メモリ動作モード)	✓	✗	✗
メモリ冗長性	✓	✗	✗
スロット	✓	✗	✓
コントローラ	✓	✗	✓
コネクタ	✓	✗	✗
PCIe-SSD エクステンダー	✓	✗	✓
Enclosure	✓	✗	✓
アレイディスク	✓	✗	✓
イントルージョンスイッチ	✓	✗	✓
ハードウェアログ	✓	✗	✓
メインシャーシ	✓	✗	✓
追加情報	✓	✗	✓
モジュラーエンクロージャ情報	✓	✗	✓
ファームウェア	✓	✗	✓
プロセッサ	✓	✗	✓
ファン	✓	✗	✓
ファン冗長性	✓	✗	✓
温度	✓	✗	✓
電圧	✓	✗	✓
電源装置	✓	✗	✓
電源装置冗長性	✓	✗	✓

報告されるアイテム	デバイスタイプを サーバ / ハイパーバイザー として SupportAssist Enterprise に追加したデバイス		デバイスタイプを iDRAC として SupportAssist Enterprise に追加したデバイス
	OMSA はデバイスにインストールされています。	OMSA はデバイスにインストールされていません。	
ネットワーク	✓	✗	✓
IPv4 アドレス	✓	✗	✗
IPv6 アドレス	✓	✗	✗
ネットワークチームインタフェース	✓	✗	✗
インタフェースメンバー	✓	✗	✗
リモートアクセスデバイス	✓	✗	✓
DRAC 情報	✓	✗	✗
シリアルオーバー LAN 設定	✓	✗	✓
Ipv6 の詳細	✓	✗	✗
ユーザー設定	✓	✗	✓
ユーザー情報	✓	✗	✓
iDRAC ユーザー権限	✓	✗	✓
DRAC ユーザー特権	✓	✗	✗
シリアルポート設定	✓	✗	✓
NIC 設定	✓	✗	✓
コンポーネントの詳細	✓	✗	✓
コントローラの TTY ログ	✓	✗	✓
オペレーティングシステム	✓	✓	✗

メモ: iDRAC ファームウェアバージョン 2.00.00.00 以降がサーバにインストールされている場合にのみ、iDRAC からの収集でコントローラの TTY ログが利用できます。

複数のデバイスの取集をダウンロードして表示する

このタスクについて

実行した複数のデバイス収集で使用可能なシステム情報を表示します。複数のデバイス収集を表示するには、複数のデバイス収集をダウンロードし、ウェブブラウザを使用して、収集を開く必要があります。

手順

1. **コレクション** > **コレクションを表示** に移動します。

収集 ページが表示されます。

2. 表示する複数のデバイス収集を選択します。
   収集の概要 ペインが表示されます。
3. **ダウンロード**をクリックして、収集ファイルを保存します。
4. ファイルを解凍し、index.html ファイルを開きます。
   複数のデバイス設定ビューアが、新しいウェブブラウザウィンドウで開きます。デバイス タイプ メニューにアクセスして、各デバイスから収集されたシステム情報を表示できます。

13

収集の設定

SupportAssist Enterprise は、すべてのデバイスから定期的にシステム情報を自動収集します。また、SupportAssist Enterprise は、デバイスの不具合に対してサポートケースが作成された場合にも、デバイスからシステム情報を自動収集します。ご希望に応じて次の設定が可能です。

- サポート ケースの作成またはアップデート時における、システム情報の自動収集。「サポート ケース作成時のシステム情報の自動収集を有効化または無効化」を参照してください。
- システム情報の定期収集「システム情報の定期収集を有効化または無効化」を参照してください。
- ID 情報の収集。「ID 情報の収集を有効化または無効化」を参照してください。
- ソフトウェア情報とシステム ログの収集。「システム情報の収集を有効化または無効化」を参照してください。
- 収集の自動アップロード。「収集された情報の自動アップロードを有効化または無効化」を参照してください。

トピック：

システム情報収集の前提条件

- ローカルシステムには、収集したシステム情報を保存するのに十分なハード ドライブ容量が必要です。
- ローカルシステムとリモートデバイスは、ネットワークポートの要件を満たす必要があります。
- オペレーティング システムの IP アドレスまたはホスト名を使用して、サーバーを追加した場合（エージェントベースの監視）:
  - サーバに、理想的には Dell OpenManage Server Administrator（OMSA）がインストールされている必要があります。
  - サーバが Linux オペレーティングシステムを実行している場合には、次の要件があります。
    - SupportAssist Enterprise に入力したデバイス資格情報にはデバイスの管理者権限が必要です。
    - `/tmp` フォルダにリソース（ネットワーク共有、ドライブ、または ISO イメージ）をマウントする必要はありません。
    - OMSA がデバイスにインストールされている場合は、OpenSSL の最新バージョンを、デバイス上にもインストールする必要があります。OpenSSL の詳細については、オペレーティング システムのサポート Web サイトで「*OpenSSL CCS インジェクションの脆弱性（CVE-2014-0224）*」の解決策を参照してください。

    メモ: エージェントベースの監視のために追加したサーバーに OMSA がインストールされていない場合、デバイスから定期的に収集される情報にはストレージとシステムの詳細が含まれません。
- iDRAC IP アドレスを使って追加した場合（エージェントレス監視）、入力した iDRAC の資格情報には管理者権限が必要です。
- 収集したシステム情報をバックエンドにアップロードするため、ローカル システムにインターネット接続が必要です。
- ESX および ESXi のみからシステム情報を収集する場合は、SFCBD および CIMOM が有効になっていることを確認してください。

サポート ケース作成時のシステム情報の自動収集を有効化または無効化

このタスクについて

デフォルトでは、SupportAssist Enterprise はサポート ケースが作成されたときに、デバイスからシステム情報を自動収集し、その情報を安全にバックエンドに送信します。必要な場合は、希望に応じて自動収集を有効または無効にすることができます。

メモ: デバイス向けの ProSupport Plus、ProSupport Flex for Data Center、または ProSupport One for Data Center サービス契約のサポート、レポート、およびメンテナンス提供の利点を最大限に活用するためには、システム情報の自動収集を有効にする必要があります。

手順

1. **設定** > **プリファランス** に移動します。
   プリファランス ページが表示されます。
2. **システム状態情報を収集** セクションで、**新しいサポートケースが作成されたとき** を選択またはクリアします。

   メモ: デフォルトでは、このオプションが選択されています。
3. **適用** をクリックします。

システム情報の定期収集を有効化または無効化

このタスクについて

SupportAssist Enterprise は、デフォルトですべての監視対象デバイスから定期的にシステム情報の収集を開始し、それをバックエンドに送信します。収集の開始時刻は、毎月ユーザーが定義した日の午後 11 時です。必要な場合は、希望に応じてすべての監視対象デバイスからのシステム情報の定期収集を有効または無効にすることができます。

手順

1. **設定** > **プリファランス** に移動します。
   プリファランス ページが表示されます。
2. **[システム状態情報の収集]** セクションで、**[毎月 N 日の午後 11 時]** を選択またはクリアします。
3. **適用** をクリックします。

ID 情報の収集を有効化または無効化

このタスクについて

デフォルトでは、SupportAssist Enterprise は、ホスト ID およびネットワーク構成データが含まれる可能性のある、システム、ホスト、およびネットワーク デバイスの完全な構成スナップショットなどの ID 情報 (PII) を収集します。通常、不具合の正しい診断には、このデータのすべてまたは一部が必要となります。会社のセキュリティ ポリシーにより、会社のネットワーク外への ID データの送信が制限されている場合、SupportAssist Enterprise はそのようなデータを収集できなくすることができます。

デバイスからシステム情報を収集する際、以下の ID 情報をフィルタすることができます。

- ホスト名
- IP アドレス
- サブネットマスク
- デフォルトゲートウェイ
- MAC アドレス
- DHCP サーバ
- DNS サーバ
- プロセス
- 環境変数
- レジストリ
- ログ
- iSCSI データ
- Fibre Channel データ - ホストの World Wide Name (WWN) とポートの WWN

メモ: ID 情報の収集を無効にすると、社内ネットワークに関するデータの一部 (システムログを含む) がバックエンドに送信されません。これにより、お使いのデバイスで問題が発生した場合、テクニカル サポートで解決をすることが困難になる可能性があります。

メモ: お使いのデバイスにアクティブな ProSupport Plus、ProSupport Flex for Data Center、または ProSupport One for Data Center サービス契約があり、ID 情報の収集が無効になっている場合、デバイスについての一部の報告情報を受信しません。

メモ: デバイスからの ID 情報の収集を無効にしている場合、ホスト名や IP アドレスなどの ID 情報はトークン化された値に置き換えられます。トークン化された値はトークン *n* として表示されます。たとえば、トークン 0、トークン 1、トークン 2 のようになります。

手順

1. **設定** > **プリファランス** に移動します。
   プリファランス ページが表示されます。
2. デフォルトでは、**ID 情報設定**セクションの **Dell EMC に送信するデータに ID 情報を含める**チェックボックスはオンです。要件に応じて、チェックボックスをオンまたはオフにします。

   メモ: **ID 情報の収集を無効にすると、ログ、診断データ、およびサポート データの収集の設定は自動的に無効になります。したがって、自分のデバイスからバックエンドへ送信される収集には、特定カテゴリのデータが含まれません。**
3. **適用** をクリックします。

システム情報の収集を有効化または無効化

このタスクについて

デフォルトでは、SupportAssist Enterprise によって収集され、バックエンドに送信されるシステム情報には、ソフトウェア情報とシステム ログなどが含まれます。必要に応じて、すべてのデバイスからソフトウェア情報とシステムログの収集を除外するように、SupportAssist Enterprise を設定できます。

手順

1. **設定** > **プリファランス** に移動します。
   プリファランス ページが表示されます。
2. **収集データ設定**セクションで、各デバイス タイプで利用可能なオプションをオンまたはオフにします。

   メモ: **SupportAssist Enterprise により収集されるログの詳細については、 で『*SupportAssist Enterprise Version 4.0 Reportable Items*』の文書を参照してください。**
3. **適用** をクリックします。

収集された情報の自動アップロードを有効化または無効化

このタスクについて

デフォルトでは、システム状態情報が SupportAssist Enterprise によりデバイスから収集され、Dell EMC に送信されます。必要な場合は、収集の自動アップロードを無効化することができます。

メモ: **自動アップロード設定は、複数のデバイス収集には適用されません。**

手順

1. **設定** > **プリファランス** に移動します。
   プリファランス ページが表示されます。
2. **アップロード** で、**システム状態情報をデバイスから収集し Dell EMC に送信** オプションをオンまたはオフにします。
3. **適用** をクリックします。

14

SupportAssist Enterprise を使用したシステム情報の収集と送信

SupportAssist Enterprise では定期的に、およびケース作成時にも、デバイスからシステム情報を自動的に収集します。必要に応じて、いつでもシステム情報の収集と Dell EMC へのアップロードを手動で開始することもできます。システム情報の収集を開始する際は、単一または複数のデバイスから選択できます。

メモ: SupportAssist Enterprise がシステム情報を収集してバックエンドに送信することができるデバイスの詳細については、 にある『*SupportAssist Enterprise バージョン 4.0 サポート マトリックス*』を参照してください。

トピック：

システム情報を収集および送信するための SupportAssist Enterprise のセットアップ

このタスクについて

SupportAssist Enterprise を導入して登録すると、SupportAssist を使用してシステム情報を収集し、ローカル システムから送信できます。システム情報を収集し、リモート デバイスから送信するには、SupportAssist Enterprise に各リモート デバイスを追加する必要があります。

メモ: 次の手順は、SupportAssist Enterprise が導入されていない場合にのみ実行してください。SupportAssist をすでに導入している場合は、「特定のデバイスからシステム情報を手動で収集」手順に従って手動で収集を開始し、システム情報をバックエンドにアップロードします。

手順

1. SupportAssist Enterprise を導入します。
2. SupportAssist Enterprise を登録します。「SupportAssist Enterprise の登録」を参照してください。
   SupportAssist Enterprise を使用して、ローカルシステムからシステム情報を収集できるようになりました。
3. SupportAssist Enterprise に各リモートデバイスを追加します。

   メモ: OMSA を実行しているサーバーから収集されたシステム情報には、OMSA を実行していないサーバーから収集されたデータにはない追加的なトラブルシューティング情報が含まれます。したがって、SupportAssist Enterprise に追加したサーバーに OMSA をインストールすることをおすすめします。

   SupportAssist Enterprise を使用して、リモートデバイスからシステム情報を収集できるようになりました。

特定のデバイスからシステム情報を手動で収集

前提条件

SupportAssist Enterprise のセットアップが完了していることを確認します。「システム情報を収集および送信するための SupportAssist Enterprise のセットアップ」を参照してください。

このタスクについて

デバイスにサポート ケースが開始されたりアップデートされたりすると、SupportAssist Enterprise はシステム情報を自動的に収集して、バックエンドにアップロードします。必要に応じて、デバイスからのシステム情報の収集を手動で開始することもできます。

収集を手動で開始することができます。

- システム情報の自動収集およびアップロード中に問題が発生した場合
- テクニカル サポートから要求された場合

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. システム情報を収集するデバイスを選択します。
   収集の開始リンクが有効になります。
3. **収集の開始** をクリックします。
   [**デバイス**] ページの**名前/IP アドレス**列には、システム情報の収集とアップロードのステータスを示すプログレス バーとメッセージが表示されます。

   メモ: システム情報の収集をキャンセルする場合は、プログレス バーの隣に表示されている、 をクリックします。

   メモ: 収集が完了するまで、デバイスの選択に使用するチェックボックスは無効になります。したがって、収集が完了するまで、デバイスで他のタスクを開始することはできません。

複数のデバイスからシステム情報を手動で収集する

このタスクについて

複数のデバイスから収集したシステム情報を含むコレクション バンドルを作成およびアップロードします。

メモ: システム情報はステージンググループ内のデバイスから収集されません。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. システム情報を収集するデバイスを選択します。
   複数のデバイスを選択すると、**収集の開始**リンクは無効になります。
3. **収集目的**リストで収集の理由を選択します。
   収集の開始リンクが有効になります。
4. **収集の開始** をクリックします。
   複数のデバイス収集ウィンドウが表示されます。
5. オプションで、コレクション バンドルの名前、サポート ケース番号、およびテクニカル サポート エージェントの E メール アドレスを入力します。
6. SupportAssist Enterprise によりコレクション バンドルをバックエンドにアップロードする場合は、**収集のアップロード**チェックボックスが選択されていることを確認します。

   メモ: 収集のアップロードチェックボックスをオフにすると、コレクション バンドルは保存されますが、バックエンドにはアップロードされません。収集ページにより、後からコレクション バンドルをアップロードできます。
7. **OK** をクリックします。
   複数のデバイス収集 ペインに、収集の進行ステータスが表示されます。収集が正常に完了した場合は、**収集** ページに収集の詳細が表示されます。また、**収集** ページから複数のデバイス収集をダウンロードすることもできます。複数のデバイス収集の表示についての詳細は、「複数のデバイスの取集をダウンロードして表示する」を参照してください。

   メモ: 収集が完了するまで、デバイスで他のタスクを開始することはできません。

Upload Collection (コレクションのアップロード)

このタスクについて

収集 ページで利用可能な **アップロード** オプションを使用して、収集をバックエンドにアップロードします。次のケースで、収集のアップロードを選択できます。

- システム情報の収集には成功したが、アップロードに失敗した場合。
- 複数のデバイス収集を開始する際に、複数のデバイス収集をバックエンドにアップロードしないことを選択した場合。このような収集は、**収集** ページに `Never Uploaded` ステータスで表示される。
- 収集をバックエンドに再度アップロードする場合。

手順

1. **コレクション** > **コレクションを表示** に移動します。
   収集 ページが表示されます。
2. 1 つ以上のアップロードする収集を選択し、**アップロード** をクリックします。

   メモ: アップロードできる収集の合計サイズは 5 GB です。

   アップロードステータス列に、アップロードのステータスが表示されます。

切断されたサイトからの収集のアップロード

このタスクについて

インターネット接続が使用可能になると、SupportAssist Enterprise はお使いのデバイスから自動的にシステム情報を収集し、バックエンドに送信します。SupportAssist Enterprise が導入されているサーバーにインターネット接続がない場合は、収集した情報を手動でアップロードすることができます。

手順

1. デバイスから収集を実行します。「特定のデバイスからシステム情報を手動で収集」を参照してください。
2. SupportAssist Enterprise が収集を実行した場合
   - データ ストレージ、ネットワーク、または複数のデバイスのみの収集に関しては、[**収集**] ページで収集を選択し、[収集の概要] ペインで**ダウンロード**をクリックします。
   - 他のデバイス コレクションでは、`/var/lib/docker/volumes/saede_data/_data/reports` でコレクションの .ZIP ファイルにアクセスできます
3. 収集`.zip` ファイルをインターネットに接続されている別のシステムにコピー アンド ペーストします。
4. https://techdirect.dell.com/fileUpload/ に移動します。
   Dell EMC **テクニカルサポートのファイルアップロード**ページが表示されます。
5. デバイスのサービス タグを入力します。
6. 会社名、担当者名、サービスリクエスト番号、E メールアドレス、担当者の E メール、住所を入力します。

   メモ: サービス リクエスト番号がない場合は、テクニカル サポートに連絡して、サービス リクエストを開きます。
7. **ファイルの選択** をクリックして、収集 `.zip` ファイルを参照して選択します。
8. **送信** をクリックします。

複数のデバイス収集 ウィンドウ

複数のデバイスコレクションウィンドウでは、起動する複数のデバイスコレクションの詳細を入力できます。

次の表は、**複数のデバイス収集** ウィンドウに表示される項目についての説明です。

表 18. 複数のデバイス収集 ウィンドウ

フィールド	説明
収集名（オプション）	コレクションに割り当てる名前。
Dell EMC サポートリクエスト / ケース番号（オプション）	コレクションに関連付けるケースの識別子。
Dell EMC 技術者 E-メール（オプション）	テクニカルサポートの連絡先の E メールアドレスまたは名前。
プロジェクト ID（オプション）	プロジェクトの ID 情報。

フィールド	説明
Upload Collection（コレクションのアップロード）	• コレクションの完了後、このオプションを選択して、コレクションをバックエンドにアップロードします。 • ローカル システムにあるコレクションのみを保存する場合は、このオプションをクリアします。

複数のデバイス収集 ペイン

複数のデバイス収集ペインは、複数のデバイスからの収集が進行中である間、[**デバイス**] ページに表示されます。

複数のデバイス収集 ペインには、次のものが表示されます。

- コレクションのステータスを示すプログレスバー
- コレクションのステータスメッセージ
- 完了したコレクションの数とコレクションの合計数
- 収集に割り当てられた名前

メモ: 収集が完了すると、複数のデバイス収集ペインが自動的に閉じて、[収集] ページに収集の詳細が表示されます。

15

拡張機能

拡張機能を使用すると、Dell EMC OpenManage Enterprise などのシステム管理コンソールで管理しているデバイスのインベントリを行い、追加できます。

アダプターは、SupportAssist Enterprise で利用可能な拡張機能です。これは、SupportAssist とシステム管理コンソールの間のインターフェイスとして機能します。これにより、SupportAssist では各デバイスを個別に追加する代わりに、システム管理コンソールを使って管理している対応デバイスのインベントリおよびアラートの取得を行うことができます。デバイスの追加およびインベントリの後、SupportAssist はデバイスを監視してハードウェアに問題がないかを確認し、システム情報を収集してバックエンドにアップロードすることもできます。

システム管理コンソールによって管理されているデバイスのインベントリおよび追加を行うには、次の手順を実行します。

1. システム管理コンソールから追加するデバイスのアカウント認証情報を追加します。「アカウント資格情報の追加」を参照してください。
2. 追加するデバイスのタイプに応じて、1 つ、または複数の認証情報プロファイルを作成します。「認証情報プロファイルの作成」を参照してください。
3. SupportAssist Enterprise でアダプターを設定します。「アダプターのセットアップ」を参照してください。

トピック：

アダプターのセットアップ

前提条件

- OpenManage Enterprise を実行しているシステムの管理者権限が必要です。
- アカウント認証情報および認証情報プロファイルを作成し、それらにはアダプターによってインベントリが実行されているデバイスの認証情報が含まれている必要があります。「アカウント資格情報の追加」および「認証情報プロファイルの作成」を参照してください。

このタスクについて

アダプターをセットアップすると、OpenManage Enterprise などのシステム管理コンソールによって管理されているデバイスのインベントリを行うことができます。セットアップ中、SupportAssist Enterprise によって、SupportAssist Enterprise が実行されているシステムにアダプターが設定され、デバイスのインベントリが実行されます。

アダプターを介してのみ、インベントリを実行し、デバイスを追加することができます。

- yx2x ~ yx5x シリーズの PowerEdge サーバー iDRAC
- Linux、ESXi、HyperV を実行しているサーバ
- シャーシ
- Storage SC シリーズ デバイス (以前の Compellent)
- Dell EMC ネットワーキング デバイス—OS9 および OS10

  メモ: OS10 のサポートは、PowerEdge MX7000 スイッチのみに限定されています。
- OEM デバイス
- IOM デバイス
- PowerVault デバイス

メモ: 1 つの OpenManage Enterprise アダプターが複数の OpenManage Enterprise インスタンスからデバイスをインベントリし、追加できます。

手順

1. **拡張機能** > **アダプタの管理** に移動します。
   アダプタの管理 ページが表示されます。
2. **アダプターをセットアップ** をクリックします。
   アダプターのセットアップ ウィンドウが表示されます。
3. **アダプター タイプ** リストから、アダプター タイプを選択します。
4. 次の手順を実行します。
   a) 管理コンソールがインストールされているサーバーのホスト名または IP アドレスを入力します。
   b) 任意でアダプターの名前を入力します。
      入力した名前は SupportAssist Enterprise でアダプターを表す際に使用されます。名前を入力しない場合は、入力したホスト名または IP アドレスがアダプターを表す際に使用されます。
   c) ユーザー名とパスワードを入力します。

      メモ: パスワードは 50 文字を超えることはできません。
5. **認証情報プロファイル** リストから、アダプターによってインベントリが実行されるデバイスタイプのアカウント認証情報を持つプロファイルを選択します。
6. **デバイスインベントリのアップデート** リストから、アダプターを介してデバイスのインベントリのための希望の頻度を選択します。
7. **OK** をクリックします。
   アダプターの詳細概要ペインが表示され、OpenManage Enterprise によって管理されているデバイスのインベントリが SupportAssist Enterprise で実行されます。

次の手順

選択した認証情報プロファイルにインベントリを実行するデバイスの正しい認証情報が含まれる場合、そのデバイスは **デフォルト** グループに追加されます。認証情報が正しくないか使用できないデバイスは、**ステージング** グループに移されます。

メモ: デフォルトでは、アダプターを介して正常に追加されたデバイスでモニタリングが有効になります。

メモ: SupportAssist Enterprise の自動サポート機能は、ステージング グループに配置されているデバイスには使用できません。

ステージング グループに配置されているデバイスを追加するには：

1. **絞り込みの条件** ペインで **グループ** を展開し、**ステージング** を選択します。また、**絞り込みの条件** ペインの **追加されたデバイス** でアダプターを選択して、アダプターによってインベントリが実行されるデバイスを表示することもできます。必要に応じて、**検索基準** オプションを使用して、表示されているデバイスのリストをフィルタします。
2. 次のいずれかの手順を実行してください。
   - デバイスを選択し、選択したデバイスの認証情報を含む認証情報プロファイルを割り当てます。
   - デバイスを選択し、**編集** をクリックして認証情報アカウントを割り当てます。
3. 正しい認証情報プロファイルまたはアカウント認証情報をすべてのデバイスに割り当てるまで、手順 2 を繰り返します。

メモ: OpenManage Enterprise サービスが一時停止して再開されると、OpenManage Enterprise アダプターは、OpenManage Enterprise アダプターから SupportAssist Enterprise に追加されたデバイスの直近 12 時間以内に発生したアラートを取得します。

メモ: OpenManage Enterprise アダプターの同期後は、一部の iDRAC が SupportAssist Enterprise に表示されないことがあります。これは、OpenManage Enterprise から iDRAC のバージョンを取得できない場合に発生する可能性があります。

アダプタの編集

このタスクについて

以下のアダプタの詳細を更新できます。

- アダプタが設定されているサーバの資格情報
- インベントリの頻度
- ディスプレイ名

手順

1. **拡張機能** > **アダプタの管理** に移動します。
   アダプタの管理 ページが表示されます。
2. 編集するアダプタを選択し、**編集** をクリックします。
   アダプタの編集 ウィンドウが表示されます。
3. 必要な詳細を編集して、**更新** をクリックします。
   アダプタの詳細が更新されます。

アダプタの削除

このタスクについて

アダプタを削除すると以下が発生します。

- SupportAssist Enterprise ユーザーインタフェースからアダプタが削除されます
- アダプタに関連付けられたデバイスが削除されます
- アダプタアプリケーションがセットアップされたサーバから、そのアプリケーションがアンインストールされます

メモ: すべてのアダプタが SupportAssist Enterprise で削除された後にのみ、アダプタがインストールされたサーバーから、アダプタがアンインストールされます。

手順

1. **拡張機能** > **アダプタの管理** に移動します。
   アダプタの管理 ページが表示されます。
2. 削除するアダプタを選択し、**削除**をクリックします。
   アダプタを削除するかどうかを確認するメッセージが表示されます。
3. **はい** をクリックします。
   アダプタおよびそのアダプタ経由で SupportAssist Enterprise に追加したデバイスが、SupportAssist Enterprise から削除されます。

アダプタを同期

このタスクについて

アダプタは、アダプタのセットアップ中に選択した頻度に応じて、システム管理コンソールからデバイスの一覧表を自動的に作成します。デバイスの一覧表の作成は手動でもいつでも開始できます。

手順

1. **拡張機能** > **アダプタの管理** に移動します。
   アダプタの管理 ページが表示されます。
2. アダプタを選択します。
   アダプタの概要ペインが表示されます。
3. **今すぐ同期する** をクリックします。

アダプタ

アダプタは、SupportAssist Enterprise とシステム管理コンソールとの間でインターフェイスとして機能するアプリケーションです。

次の表は、[**アダプタ**] ページに表示される情報についての説明です。

表 19. アダプタ

フィールド	説明
アダプタのセットアップ	アダプターをセットアップします。「アダプターのセットアップ」を参照してください。
編集	アダプターの詳細を編集します。「アダプタの編集」を参照してください。

フィールド	説明
削除	アダプターを削除します。「アダプタの削除」を参照してください。
名前	アダプタに指定されている名前およびアダプタがセットアップされているサーバーのホスト名または IP アドレス。
タイプ	アダプタ タイプ
管理下デバイス	アダプタから追加されたデバイスの合計数。
コンソールバージョン	システム管理コンソールのバージョン。
ステータス	アダプタのステータス。アダプタのステータスは、以下のいずれかです。 · **接続済み** - SupportAssist はアダプタに正常に接続できます。 · **切断済み** - SupportAssist はアダプターに接続できません。 · **初期同期** - デバイスの初期インベントリが進行中。 · **定期同期** - デバイスの自動定期インベントリが進行中。 · **手動同期** - 手動で開始されたデバイスのインベントリが進行中。 · **接続が失われました** - SupportAssist を実行しているサーバーは、アダプターがセットアップされているサーバーに接続できません。 · **コピーが進行中** - アダプターのインストーラパッケージがシステムにコピーされています。 · **インストールが進行中** - アダプターのインストールが進行中です。 · **検証が進行中** - SupportAssist は、アダプターがアダプターをセットアップするための動作条件を満たしているかどうかを検証します。 · **設定が進行中** - SupportAssist がアダプターを設定しています。 · **サービスを開始しています** - SupportAssist がインストールされ、アダプターサービスが開始されています。 · **接続を待機しています** - SupportAssist はアダプターサービスの開始を待機しています。 · **接続が進行中** - SupportAssist はアダプターへの接続を試行しています。 · **プロファイルを割り当て中** - 認証情報プロファイルが、インベントリ対象のデバイスに適用されます。インベントリ対象デバイスの合計数と、プロファイルが適用されているデバイスの数も表示されます。

16

アクティブ セッション

テクニカル サポート エージェントがお使いのデバイスにリモートアクセスして、スクリプトの実行やファイルの転送を行う場合、処理の進行中はセッション情報が SupportAssist Enterprise に表示されます。

トピック：

アクティブ リモート セッション

アクティブ リモート セッションタブには、テクニカル サポートのエージェントによって実行されているトラブルシューティングまたはデバイス固有のタスクに関する情報が表示されます。

をクリックして、ページに表示されている詳細を更新します。をクリックして、表示する列を選択します。

次の表では、**アクティブ リモート セッション**タブに表示される情報について説明しています。

表 20. アクティブ リモート セッション

行	説明
開始時刻	リモートセッションが開始された日時。
モデル	デバイスのモデルです。
シリアルナンバー	デバイスのシリアル番号。
デバイス IP	デバイスの IP アドレス。
アプリケーション名	デバイスのリモートアプリケーション。
ポート	デバイスがアクセスされているポート。
ユーザー	セッションを開始したユーザーの名前。
所要時間（分）	セッションの期間（分単位で表示）。

アクティブ ファイル転送セッション

アクティブ ファイル転送セッションタブには、デバイスまたは SupportAssist Enterprise ユーザー インターフェイスから手動または自動でバックエンドに転送されているファイルの詳細が表示されます。ファイル転送が完了すると、詳細が**監査** > **ファイル転送** ページに表示されます。

をクリックして、ページに表示されている詳細を更新します。をクリックして、表示する列を選択します。

次の表は、**アクティブ ファイル転送セッション**タブに表示される情報について説明しています。

表 21. アクティブ ファイル転送セッション

行	説明
開始時刻	リモートセッションが開始された日時。
モデル	デバイスのモデルです。
シリアルナンバー	デバイスのシリアル番号。
ファイル名	転送されているファイルの名前。

行	説明
ファイル サイズ (kb)	転送されているファイルのサイズ。
転送タイプ	ファイル転送が開始されているチャネル。
転送レート (MiBs)	転送されているファイルのレート。
残り時間	ファイル転送を完了するまでの残り時間。
完了率	ファイル転送の進行状況。

アクティブ リモート スクリプト

アクティブ リモート スクリプトタブには、Managed File Transfer (MFT) サービスのリモート スクリプト機能を使用してデバイスとバックエンド間で転送されているファイルに関する情報が表示されます。ファイル転送が完了すると、詳細が**監査** > **リモート スクリプト** ページに表示されます。

をクリックして、ページに表示されている詳細を更新します。をクリックして、表示する列を選択します。

次の表は、**アクティブ リモート スクリプト**タブに表示される情報について説明しています。

表 22. アクティブ リモート スクリプト

行	説明
モデル	デバイスのモデルです。
シリアル ナンバー	デバイスのシリアル番号。
スクリプト名	使用されているスクリプトの種類 (たとえば PUT)。
リモート スクリプト ステータス	スクリプトのステータス。
開始時刻	スクリプトが開始された日時。
終了時刻	スクリプトが完了した日時。

アクティブ Connect Homes

アクティブ Connect Homes タブには、Connect Home サービスを使用してデバイスとバックエンド間で転送されているファイルの詳細が表示されます。このページには、転送中のファイルの総数と、ファイルの転送にかかる最大時間 (分単位) も表示されます。

ファイル転送が完了すると、転送の詳細が**監査** > **Connect Home** ページに表示されます。

をクリックして、ページに表示されている詳細を更新します。をクリックして、表示する列を選択します。

次の表は、**アクティブ Connect Homes** タブに表示される情報について説明しています。

表 23. アクティブ Connect Homes

行	説明
開始時刻	ファイル転送が開始された日時。
ファイル名	転送されたファイルの名前。
ファイル サイズ (kb)	転送されたファイルのサイズ。
年齢 (分)	ファイル転送にかかった時間。

17

SupportAssist Enterprise 設定の構成

設定タブでは、次の設定を行うことができます。

- システム情報の収集
- E メール通知
- SupportAssist Enterprise が導入されているサーバーのインターネット接続設定
- Policy Manager がインストールされているサーバーのインターネット接続設定
- SMTP サーバー
- ホームに接続
- 連絡先および配送先情報
- TechDirect との統合
- VMware Tools

トピック：

プロキシサーバを設定

SupportAssist Enterprise が導入されているサーバーがプロキシ サーバー経由でインターネットに接続されている場合は、SupportAssist Enterprise でプロキシを設定します。

手順

1. **設定** > **プロキシ設定** に移動します。
   プロキシ設定 ページが表示されます。
2. **プロキシ サーバを使用する** を選択します。

   メモ: SupportAssist Enterprise は Windows NT LAN Manager（NTLM）、および基本的なプロキシ認証プロトコルをサポートします。

   プロキシ サーバーのフィールドが有効になります。
3. プロキシ サーバーのホスト名/IP アドレスおよびポート番号を入力します。
4. プロキシ サーバーへの接続にユーザー名とパスワードが必要な場合は、**認証が必要** を選択します。

   メモ: ユーザー名とパスワードを入力しない場合、SupportAssist Enterprise は匿名ユーザーとしてプロキシ サーバーに接続します。

   ユーザー名とパスワードのフィールドは有効です。
5. ユーザー名とパスワードを入力します。
6. **[テスト]** をクリックします。
   SupportAssist Enterprise はプロキシ サーバーへの接続を確認し、接続ステータスを示すメッセージを表示します。
7. **適用** をクリックします。
   プロキシ設定が保存されます。

   メモ: プロキシ設定が保存されるのは、SupportAssist Enterprise がプロキシ サーバーに接続できる場合に限られます。

ポリシー マネージャー

ポリシー マネージャーは、次のデバイスに対する権限を設定できるようにするアプリケーションです。

- データ保護
- Web スケール以外のすべてのハイパーコンバージド インフラストラクチャ デバイスモデル。
- Peer Storage (PS) または EqualLogic、Storage Center (SC) または Compellent、Fluid File System (Fluid FS)、および PowerVault 以外のすべてのデータ ストレージ デバイスのモデル。

ポリシー マネージャーは、SupportAssist Enterprise が導入されているサーバーにはインストールされていないため、次のタスクを実行するように設定できます。

- デバイスへのリモートアクセスを制御する
- リモート接続とファイル転送の監査ログを維持する
- ポリシー マネージャーで実行されたアクセス管理操作

ポリシー マネージャーの操作と設定の詳細については、https://support.emc.com/products/37716_EMC-Secure-Remote-Services-Virtual-Edition/Documentation/にある『*EMC Secure Remote Services Policy Manager Operations Guide*』を参照してください。

ポリシー マネージャー設定の構成

このタスクについて

ポリシー マネージャーがインストールされているサーバーに SupportAssist Enterprise を接続できるように、インターネット接続の詳細を入力します。

手順

1. **設定** > **ポリシー マネージャー** に移動します。
   ポリシー マネージャー ページが表示されます。
2. **接続**セクションで、**リモート ポリシー マネージャーを有効にする**をオンにします。
3. ホスト名または IP アドレスおよびポート番号を入力します。

   メモ: ポートが SSL で保護されている場合、ポート番号は 8443 でなければなりません。ポートが SSL で保護されていない場合は、ポート番号を 8090 にする必要があります。
4. ポリシー マネージャーがインストールされているサーバーが SSL で保護されている場合は、**SSL を有効にする** を選択します。
5. **強度** リストから、暗号化の強度を選択します。
6. ポリシー マネージャーがインストールされているサーバーがプロキシ サーバーを介してインターネットに接続している場合は、次の手順を実行します。
   a) **カスタマー プロキシ サーバー** セクションで、**ポリシー マネージャーに対してのみプロキシ サーバーを有効にする** を選択します。
   プロキシの詳細フィールドが有効化されます。
   b) ホスト名または IP アドレスおよびポート番号を入力します。
   c) プロキシサーバーに認証が必要な場合は、**プロキシに認証が必要** をオンにします。
   ユーザー名とパスワードのフィールドは有効です。
   d) プロキシサーバーのユーザー名とパスワードを入力します。
7. **[テスト]** をクリックします。
   SupportAssist Enterprise はプロキシ サーバーへの接続を確認し、接続ステータスを示すメッセージを表示します。
8. **適用** をクリックします。
   設定が保存されます。

   メモ: プロキシ設定が保存されるのは、SupportAssist Enterprise がプロキシ サーバーに接続できる場合に限られます。

プリファランス

[プリファランス] ページでは、コレクション設定および E メール通知設定を構成できます。

次の表には、**SupportAssist Enterprise アプリケーション**ペインに表示されるオプションについての情報が記載されています。

表 24. SupportAssist Enterprise アプリケーション ペイン

セクション	説明
システム状態情報を収集する	• SupportAssist Enterprise が、午後 11 時にすべてのデバイスからシステム情報を自動的に収集可能な月日を選択します。 • サポート ケースが作成されたら、**新しいサポートケースが作成されたとき**を選択し、SupportAssist Enterprise がシステム情報を自動的に収集できるようにします。
アップロード	**デバイスから Dell EMC に収集されたシステム状態情報**を選択し、SupportAssist Enterprise が収集を自動的にバックエンドにアップロードできるようにします。
検証	毎月午後 11 時に各デバイスタイプから検証情報を自動的に取得するには、日付を選択します。
API インターフェイス	SupportAssist Enterprise の API インターフェイスを有効にするには、**SupportAssist Enterprise の API インターフェイスの有効化** を選択します。
ID 情報設定	**Dell EMC に送信するデータに ID 情報を含める**を選択し、SupportAssist Enterprise がシステム識別情報を他のデータとともにバックエンドに送信できるようにします。このチェックボックスをオフにすると、ログおよび診断データの収集が自動的に無効になります。
E メール設定	デバイスの新しいサポートケースが開かれたときに E メール通知を受信するには、**新しいサポートケースが開始されたときに E メール通知を受信する** を選択します。
希望の E メール用言語リスト	電子メール通知に使用する言語を選択します。
E メール通知	E メールで受信する通知を選択します。 • **アダプタ接続ステータス** • **接続性テスト** • **メンテナンスモード** • **デバイス検証ステータス** • **定期的なインベントリ検証** • **ステージングデバイスと非アクティブデバイス** • **自動発送の環境設定**

次の表には、**デバイスとネットワーク**ペインに表示されるオプションについての情報が記載されています。

表 25. デバイスおよびネットワーク ペイン

フィールド	説明
サーバー / ハイパーバイザー	• デバイスからソフトウェア関連情報を収集する**ソフトウェア**を選択します。 • デバイスからログを収集する**システムログ**を選択します。 • デバイスから SMART CTL ログを収集する **SMART ログ**を選択します。 **メモ: SupportAssist Enterprise により収集されるログの詳細については、 で『*SupportAssist Enterprise Version 4.0 Reportable Items*』の文書を参照してください。**
データ ストレージ : Fluid File System (FluidFS)	デバイスからログを収集する**ログ**を選択します。
データ ストレージ : Peer Storage (PS) /EqualLogic	• デバイスから診断情報を収集する**診断データ (診断収集)** を選択します。 • デバイスから Ping テスト結果を収集する**内部アレイ接続性テスト (Ping テスト)** を選択します。

フィールド	説明
データ ストレージ：PowerVault	デバイスからサポート データを収集する**サポート データ**を選択します。
ソフトウェア：VMware 向け HIT キット /VSM	デバイスからログを収集する**詳細ログ**を選択します。
ソリューション：Nutanix	デバイスからログを収集する**ログ**を選択します。
仮想マシン	デバイスからログを収集する**システム ログ**を選択します。

電子メール通知を設定

このタスクについて

SupportAssist Enterprise からの自動 E メール通知を有効または無効にし、さらに E メール通知に使用する言語も選択します。

手順

1. **設定** > **プリファランス** に移動します。
   プリファランス ページが表示されます。
2. **E メール設定**セクションでは、次の手順を行います。
   a) E メール通知を受信するイベントを選択します。

   メモ: サポート ケースの E メール通知を無効化すると、コレクションの進行中に送信された E メールと、コレクションがバックエンドに送信されたときに送信される E メールが無効になります。

   b) **希望の E メール言語**リストから、E メール通知を受信する言語を選択します。

   メモ: 新規サポート ケースが開かれたときに E メール通知を受信する を選択したときにのみこのリストは有効化されます。
3. **適用** をクリックします。

電子メール通知のタイプ

次の表は、SupportAssist Enterprise が送信する様々なタイプの E メール通知の一覧です。

表 26. 電子メール通知のタイプ

E メール通知のタイプ	電子メール通知が送信される時	電子メール通知の送信元
登録確認とようこそ電子メール	SupportAssist Enterprise の登録が正常に完了しました。	Dell EMC がホストする SupportAssist サーバー
ケースが作成されました	ハードウェア問題が検出され、その問題のサポート ケースが作成されました。	Dell EMC がホストする SupportAssist サーバー
ケースを作成できません	ハードウェア問題が検出されましたが、技術的な問題のためサポート ケースを作成できませんでした。	Dell EMC がホストする SupportAssist サーバー
システム情報を収集できません	デバイスに対するサポート ケースが自動的に作成されていますが、SupportAssist Enterprise がそのデバイスからシステム情報を収集できません。	Dell EMC がホストする SupportAssist サーバー
収集したシステム情報を送信できません	デバイスに対するサポート ケースが自動的に作成されていますが、SupportAssist Enterprise がそのデバイスから収集したシステム情報をバックエンドに送信できません。	Dell EMC がホストする SupportAssist サーバー
非アクティブ通知	SupportAssist Enterprise がどのデバイスも監視しておらず、過去 30 日間にデバイスが追加されていません。	Dell EMC がホストする SupportAssist サーバー

E メール通知のタイプ	電子メール通知が送信される時	電子メール通知の送信元
接続性テストアラート	午後 11 時毎日(SupportAssist Enterprise が導入されているサーバーの日時)。 **メモ: テストアラート通知は、依存リソースへの接続性に問題が検出された場合にのみ送信されます。**	SupportAssist Enterprise アプリケーション
自動メンテナンスモード	デバイスから受け取ったアラート ストームのため、SupportAssist Enterprise がデバイスを自動的にメンテナンスモードにしました。	SupportAssist Enterprise アプリケーション
デバイスステータスアラート	午後 11 時毎日(SupportAssist Enterprise が導入されているサーバーの日時)。10 個未満のデバイスに問題がある場合、電子メールには問題および可能な解決手順に関する詳細が含まれます。10 個を超えるデバイスに問題がある場合、メールには問題の概要のみが含まれます。 **メモ: デバイスアラート通知は、デバイスのセットアップまたは設定に問題 (警告およびエラーステータス) がある場合にのみ送信されます。**	SupportAssist Enterprise アプリケーション
アダプターの問題	• アダプターの接続の問題が検知されてから 5 分以内。 • 問題が解決しない場合は、最初の E メールが送信されてから 6 時間後に別の E メール通知が送信されます。	SupportAssist Enterprise アプリケーション
アダプターによる通常の操作の再開	問題が検知されてから 6 時間以内に問題が解決された場合。	SupportAssist Enterprise アプリケーション
アダプターの未解決の問題に関する最終メッセージ	問題が検知されてから 6 時間以内に問題が解決されない場合。	SupportAssist Enterprise アプリケーション
インベントリ検証の概要	SupportAssist Enterprise は、自動サポート機能 (サポートケース/インシデントの作成およびシステム情報の収集) について、デバイス インベントリの検証を完了しました。	SupportAssist Enterprise アプリケーション
ステージングおよび**非アクティブ**グループのデバイスからのアラート	モニタリングおよび自動サポート リクエスト/インシデント作成機能がお使いのデバイスの一部に制限されていることが SupportAssist Enterprise で検出されました。	SupportAssist Enterprise アプリケーション
部品発送アドレスの検証	SupportAssist Enterprise がお使いのデバイスの 1 つでハードウェアの問題を検出しました。問題を解決するために部品を交換する必要があります。	SupportAssist Enterprise アプリケーション
部品を発送するアドレスの確認	交換部品の発送準備が完了しました。	SupportAssist Enterprise アプリケーション
管理者アカウントの状態	5 回失敗すると管理者アカウントはロックされます。アカウントのロックが解除されると、E メール通知も送信されます。	カスタマー定義の SMTP サーバー
アップデートが利用可能	Docker、オペレーティングシステムまたはアプリケーションの設定ファイル用のアップデートが利用可能です。	カスタマー定義の SMTP サーバー
リモートセッションのステータス	テクニカル サポートがデバイスのリモートセッションを開始または終了しました。	カスタマー定義の SMTP サーバー

E メール通知のタイプ	電子メール通知が送信される時	電子メール通知の送信元
ポリシーマネージャーのステータス	SupportAssist Enterprise は、ポリシーマネージャーがインストールされているサーバーに接続できません。	カスタマー定義の SMTP サーバー
ファイル転送のステータス	SupportAssist はバックエンドにファイルを送信できません。	カスタマー定義の SMTP サーバー
ファイル転送ステータス通知	SupportAssist Enterprise はアラートまたは収集ファイルをバックエンドに正常に送信しました。	カスタマー定義の SMTP サーバー
Connect Home フェールオーバーオプションのテストステータス	SupportAssist Enterprise は、[**Connect Home 設定 (送信)**] ページで設定された Connect Home のフェールオーバー方法をテストして、正常にファイルをバックエンドに転送しました。	カスタマー定義の SMTP サーバー
SMTP 設定のテスト	SupportAssist Enterprise は、[**SMTP 設定**] ページから接続をテストして、正常に SMTP サーバーに接続されました。	カスタマー定義の SMTP サーバー
SMTP 設定の保存	SupportAssist Enterprise は、[**SMTP 設定**] ページで設定された設定を正常に保存しました。	カスタマー定義の SMTP サーバー
ポリシーマネージャーの承認	ポリシーマネージャーは、お客様の承認を要求するように設定されています。たとえば、テクニカル サポートエージェントがデバイスでリモートセッションを開始したときに承認を求めるプロンプトを表示するようにポリシーマネージャーを設定した場合、E メールが送信されます。	カスタマー定義の SMTP サーバー

API インターフェイス設定の有効化または無効化

このタスクについて

REST API インターフェイスを有効にすると、お使いのデータ センターのツールおよびアプリケーションと SupportAssist Enterprise を統合できるようになります。詳細については、にある『*SupportAssist Enterprise Version 4.0 REST API Guide*』を参照してください。

メモ: デバイスの追加やシステム情報の収集など、10 個までの操作を並行して実行できます。操作ステータスと操作 ID のクエリを実行する前に、5 秒の最小遅延があることを確認してください。

手順

1. **設定** > **プリファランス** に移動します。
   プリファランス ページが表示されます。
2. **API インターフェイス**セクションで、要件に応じて **SupportAssist Enterprise の API インターフェイスを有効にします**をオンまたはオフにします。
3. **適用** をクリックします。

連絡先詳細情報

[**連絡先情報**] ページでは、プライマリおよびセカンダリの連絡先情報を表示および編集できます。交換部品の部品ディスパッチの自動化を有効または無効にすることもできます。

連絡先詳細情報を設定するには、「連絡先情報の設定」を参照してください。

パーツ発送プリファランスを設定するには、パーツ発送先のプリファランスの自動設定を参照してください。

連絡先情報の設定

SupportAssist Enterprise を登録した後に、一次および二次連絡先情報を入力またはアップデートします。一次連絡先が使用できない場合、Dell EMC は二次連絡先を通して会社に連絡します。一次および二次連絡先の両方に有効な電子メールアドレスが設定されている場合は、両方に SupportAssist Enterprise の電子メールを送信します。

手順

1. **設定** > **連絡先情報**に移動します。
2. 左ペインで、次の手順を実行します。
   a) 連絡先の種類を選択します。
   b) 名、姓、電話番号、代替電話番号、およびメール アドレスを入力します。
   c) ご希望の連絡方法、連絡時間帯、タイム ゾーンを選択します。
3. **適用** をクリックします。

パーツ発送先のプリファランスの自動設定

このタスクについて

発送のプリファランス設定と出荷情報を入力すると、Dell EMC はサーバーの交換用のパーツを発送することができます。登録時にプリファランスと配送先情報を入力すると、[**連絡先情報**] ページに情報が自動的に表示されます。必要に応じて、情報を編集することができます。

メモ: パーツディスパッチは、アクティブな ProSupport、ProSupport Plus、ProSupport One、ProSupport Flex のサービス資格のあるサーバーでのみ使用できます。

メモ: デバイスを別の場所に移動する場合は、発送プリファランスと配送先情報がアップデートされていることを確認します。

デフォルトでは、Dell EMC は自動的に交換パーツを発送します。ただし、交換パーツを自動的に受け取らない場合は、**交換パーツの自動配送を希望します**チェックボックスをオフにします。

手順

1. **設定** > **連絡先情報**に移動します。
2. 右ペインの**配送先一次連絡先**セクションで、次の手順を実行します。
   a) 姓、名、電話番号、E メール アドレスを入力し、タイム ゾーンを選択します。
      メモ: 左ペインから詳細をコピーするには、表示されたリンクをクリックします。
   b) 設定した配送連絡先の時間と国または地域を選択します。
   c) 以下の配送詳細を入力します。
   d) **発送メモ** セクションで、発送固有の関連情報を入力します。
3. **配送先二次連絡先**セクションに、名、姓、電話番号、および E メール アドレスを入力します。
   メモ: 左ペインから詳細をコピーするには、表示されたリンクをクリックします。
   メモ: 一次および二次連絡先の詳細は、一意にする必要があります。
4. **適用** をクリックします。

SupportAssist Enterprise からの TechDirect へのサインイン

手順

1. **設定** > **TechDirect ログイン**に移動します。
   TechDirect **統合** ページが表示されます。
2. **サインイン** をクリックします。
   「Dell **のアカウントにサインイン**」ウィンドウが表示されます。

3. E メールアドレスとパスワードを入力して**サインイン** をクリックします。
   OTP が表示されます。
   メモ: Web ブラウザー上の Dell EMC ポータルにすでにサイン インしている場合は、サイン イン アカウントの OTP が表示されます。同じアカウントへのサインインを続行するには、OTP を入力して送信 をクリックします。別のアカウントを使用してサインインする場合、Dell EMC ポータルからサインアウトしてから、再度サインインを試みます。
4. OTP を入力して、**適用** をクリックします。
   TechDirect アカウントが確認され、メッセージがページに表示されます。

SMTP サーバーを設定

このタスクについて

社内で SMTP サーバー (E メール サーバー) を使用している場合は、SMTP サーバーの設定を行うことをお勧めします。SMTP サーバーの設定を行うと、SupportAssist Enterprise は E メール通知を送信することができます。

メモ: SMTP サーバーでトランスポート層セキュリティ (TLS) バージョン 1.2 が有効になっている必要があります。

メモ: SMTP サーバーの設定はオプションです。

手順

1. **[設定]** > **[SMTP 設定]** に移動します。
   SMTP 設定 ページが表示されます。
2. オプションとして、**成功通知を有効化**を選択すると、アラート ファイルがバックエンドに送信されたときに E メールを受信します。
3. オプションとして、**デバイス接続通知を有効化**を選択すると、テクニカル サポート エージェントがデバイスに接続したときに E メールを受信します。
4. SMTP サーバーのホスト名/IP アドレスおよびポート番号を入力します。
5. SMTP サーバーが電子メールの送信に認証を必要とする場合は、**認証が必要です** を選択します。
6. ユーザー名とパスワードを入力します。
7. セキュアに E メール通知を送信するには、**SSL を使用する** を選択します。
8. **[テスト]** をクリックします。
   SupportAssist Enterprise では、SMTP サーバーへの接続を検証し、接続ステータスを示すメッセージを表示します。
9. **適用** をクリックします。

Connect Home 概要

アラートが生成されると、そのアラートファイルが Connect Home サービスを介して SupportAssist Enterprise に送信されます。ファイルは、以下のいずれかのリスナーサービスによって受信されます。

- HTTPS
- FTP (ファイル転送プロトコル)
- E メール (SMTP)

アラートファイルは圧縮され、次のいずれかの方法でバックエンドに送信されます。

- Managed File Transfer (MFT) - デフォルトでは、アラートファイルは MFT を介してバックエンドに送信されます。
- ESRS—MFT によるファイル転送が失敗した場合、ファイルは ESRS を介して送信されます。
- FTPS または E メール - MFT と ESRS の両方が使用できない場合、ファイルは FTPS または E メールを介してバックエンドにアップロードされます。ファイルは、Connect Home サービスに対して有効になっている場合にのみ、FTPS または E メールを介してアップロードされます。

Connect Home サービスには、次の設定を行うことができます。

- フェールオーバーの方法。「Connect Home のフェールオーバー方法の設定」を参照してください。
- E メール通知。「ホーム接続 E メール通知の設定」を参照してください。
- リスナーサービス。「Connect Home リスナーサービスの設定」を参照してください。
- 権限。「Connect Home の許可設定」を参照してください。

Connect Home のフェールオーバー方法の設定

このタスクについて

Connect Home のフェールオーバーの方法を有効にしてテストします。

メモ: デフォルトでは、ファイル転送を有効にする および フェールオーバー ESRS を有効にする 方法が有効になっています。これらの方法を無効にすることはできません。

手順

1. **[設定]** > **[ホーム接続]** に移動します。
   [ホーム接続の設定 (外部)] ページが表示されます。
2. **設定** タブをクリックします。
3. フェールオーバーの方法を選択します。

   メモ: E メール フェールオーバー方法を有効にするように SMTP 設定を行う必要があります。
4. **テスト** をクリックして、フェールオーバー方法を確認します。
5. **適用** をクリックします。

ホーム接続 E メール通知の設定

このタスクについて

REST が有効なデバイスからバックエンドにアラート ファイルが送信されたときに E メールを受信するように、Connect Home E メール通知を設定します。E メールとともにアラート データを受信するように選択できます。通知は、プライマリとセカンダリの E メール アドレスに送信されます。

手順

1. **[設定]** > **[ホーム接続]** に移動します。
   [ホーム接続の設定 (外部)] ページが表示されます。
2. **[詳細設定]** タブをクリックします。
3. **Connect Home 通知を設定**セクションで、次の手順を実行します。
   a) **[デバイス モデル]** リストから、必要なデバイス モデルを選択します。

      メモ: [デフォルト] を選択した場合、その設定がすべてのデバイス モデルに適用されます。
   b) **[成功通知の有効化]** を選択すると、アラート ファイルがバックエンドに送信されたときに E メールを受信します。
   c) **[コール ホーム データを含める]** 選択すると、アラート データを E メールの添付として受信します。
4. **適用** をクリックします。

Connect Home リスナーサービスの設定

このタスクについて

アラートが生成されると、SupportAssist Enterprise は次のいずれかのリスナーサービスを介してアラートの詳細を受け取ります。

- HTTPS
- FTP (ファイル転送プロトコル)
- 電子メール

デフォルトでは、すべてのサービスが有効になっています。必要に応じてサービスを無効にすることができます。

メモ: サービスを無効にする前に、どのデバイスでも該当のサービスを使用していないことを確認してください。

手順

1. **[設定]** > **[ホーム接続]** に移動します。
   [ホーム接続の設定 (外部)] ページが表示されます。
2. **[詳細設定]** タブをクリックします。

3. **Connect Home リスナー設定** セクションで、無効にするサービスをオフにします。
   サービスを無効化するかどうかを確認するメッセージが表示されます。
4. **OK** をクリックします。
   [詳細設定] タブが表示されます。
5. **適用** をクリックします。

Connect Home の許可設定

このタスクについて

デバイス、SupportAssist Enterprise、およびバックエンド間でファイルを送信するには、Connect Home サービスを有効にする必要があります。ただし、必要に応じてサービスを無効にすることができます。

手順

1. **[設定]** > **[ホーム接続]** に移動します。
   [ホーム接続の設定 (外部)] ページが表示されます。
2. **[詳細設定]** タブをクリックします。
3. **Connect Home の許可設定** セクションで、**Connect Home の無効化** を選択します。
   Connect Home を無効化するかどうかを確認するメッセージが表示されます。
4. **OK** をクリックします。
   [詳細設定] タブが表示されます。
5. **適用** をクリックします。

VMware Tools

VMware Tools は、仮想マシンのゲスト オペレーティング システムの性能を向上させ、仮想マシンの管理を向上させる一連のユーティリティーです。ゲスト オペレーティング システム に VMware Tools がインストールされていない場合、ゲストの性能に重要な機能が欠落してしまいます。VMware Tools をインストールすると、次の問題が解消または改善されます。

- 低解像度のビデオ
- 不十分な色深度
- ネットワーク スピードの誤った表示
- 制限されたマウスの動作
- ファイルのコピーアンドペーストおよびドラッグアンドドロップ不可
- サウンドの欠落

また、ゲスト オペレーティング システムの静止画スナップショットを取り、ゲスト オペレーティング システムの時刻とホストの時刻を同期させることもできます。

VMware Tools の設定

このタスクについて

仮想マシンの VMware Tools を有効または無効にします。VMware Tools の詳細については、「VMware Tools」を参照してください。

メモ: VMware tools は、SupportAssist Enterprise を VMware ESXi Hypervisor 上に導入している場合にのみ有効または無効にできます。

手順

1. **[設定]** > **[VMware Tools]** と移動します。
   [VMware Tools の設定] ページが表示されます。
2. 要件に応じて、**[有効]** または **[無効]** を選択します。
3. **適用** をクリックします。

18

監査の概要

SupportAssist Enterprise は、参照のために SupportAssist を使用して実行されたすべてのイベントとアクティビティを記録し、保存します。レコードは、**アクティビティ**、**Connect Home**、**ファイル転送**、**ファイル転送許可**、および**リモートスクリプト**監査に分類されます。

トピック：

アクティビティ

アクティビティ ページには、SupportAssist Enterprise によって呼び出された REST API コールの詳細（ユーザー認証、ファイルのアップロード、デバイスのシリアル番号の取得など）が表示されます。

絞り込み条件ペインから、特定の日付範囲、アクティビティタイプ、ユーザー、ソース、説明、またはステータスでログを検索できます。ログをクリックすると、[**追加詳細**] ペインに次の詳細情報が表示されます。

- **タイムスタンプ**
- **タイプ**
- **URL**
- **方法**

をクリックして、ページに表示されたデータを CSV ファイルに保存します。をクリックして、ページに表示されているデータを更新します。

次の表では、[**アクティビティ**] ページに表示される情報について説明します。

表 27. アクティビティ

行	説明
日付	アクティビティが実行された日時。
アクティビティ タイプ	実行されたアクティビティのタイプ（たとえば、 **esrsauth** など）
ユーザー	API コールを呼び出すために使用されたユーザーアカウントの名前。
ソース	アクティビティが実行されたシステムの IP アドレス。
説明	呼び出された API コールに関する詳細（たとえば、Get Policy Mgr Details ）。
ステータス	アクティビティのステータス。

Connect Home 監査

アラートがデバイスによって生成されると、アラートファイルが生成され、Connect Home サービスを通じてバックエンドに送信されます。そして、ファイルがフォーマットされ、バックエンドへの転送が要求されます。その後、ファイルは次のトランスポートタイプのいずれかを介してバックエンドに送信されます。

- Managed File Transfer（MFT）- バックエンドにファイルをアップロードするためのデフォルトの主要チャネルです。
- ESRS - MFT がファイルを送信できない場合、Connect Home は ESRS チャネルを介して自動的にファイルをバックエンドにアップロードします。
- FTPS または E メール - MFT と ESRS の両方が使用できない場合、ファイルは FTPS または E メールを介してバックエンドにアップロードされます。ファイルは、Connect Home サービスに対して有効になっている場合にのみ、FTPS または E メールを介してアップロードされます。「Connect Home のフェールオーバー方法の設定」を参照してください。

[Connect Home 監査] ページには、Connect Home サービスを介してバックエンドに転送されたファイルの詳細が表示されます。

絞り込みの条件ペインから、特定の日付範囲、ファイル名、トランスポートの種類、通知の種類、または結果でログを検索できます。ログをクリックすると、日付、モデル、シリアル番号などの詳細を表示できます。

をクリックして、ページに表示されたデータを CSV ファイルに保存します。をクリックして、ページに表示されているデータを更新します。

次の表は、[Connect Home 監査] ページに表示される情報について説明しています。

表 28. Connect Home 監査

行	説明
日付	ファイルが転送された日時。
ファイル名	転送されたファイルの名前。
トランスポートタイプ	ファイル転送に使用するトランスポートの種類。
通知タイプ	ファイル転送に使用される方式 (プライマリ、フェールオーバーなど)。
結果	ファイル転送のステータス (たとえば、**成功**)。
成功	• ファイルがバックエンドに転送された場合は、**1** が表示されます。 • ファイルがバックエンドに転送されなかった場合は、**0** が表示されます。
失敗	• ファイルがバックエンドに転送された場合は、**0** が表示されます。 • ファイルがバックエンドに転送されなかった場合は、**1** が表示されます。

ファイル転送監査

[**ファイル転送監査**] ページには、Managed File Transfer (MFT) トランスポート タイプを使用してバックエンドに転送されたファイルの詳細が表示されます。

をクリックして、ページに表示されているデータを更新します。

次の表には、[**ファイル転送監査**] ページに表示される情報が記載されています。

表 29. ファイル転送監査

行	説明
ソース	ファイルの転送元のデバイスモデル。
シリアルナンバー	デバイスのシリアル番号。
ファイル名	バックエンドに転送されたファイルの名前
ファイル サイズ (kb)	バックエンドに転送されたファイルのサイズ
開始時刻	ファイル転送が開始された日時。
終了時刻	ファイル転送が完了した日時。
転送レート	ファイルの転送レート。
残り時間	ファイル転送が進行中の場合、転送を完了するためにかかる残りの時間。
完了率	ファイル転送の進行状況をパーセント値で表示。

ファイル転送許可監査

SupportAssist Enterprise にデバイスを追加した後、デバイス概要ペインから次のファイル転送許可を有効または無効にすることができます。

- Dell EMC にファイルを転送
- Dell EMC からのファイル転送
- リモートでのスクリプト作成

ファイル転送許可は、次のデバイス タイプまたはデバイス モデルに対してのみ使用可能です。

- データ保護
- Web スケール以外のすべてのハイパーコンバージド インフラストラクチャ デバイスモデル。
- Peer Storage (PS) / EqualLogic、Storage Center (SC) / Compellent、Fluid File System (FluidFS)、および PowerVault 以外のすべてのデータストレージ デバイスモデル。

[**ファイル転送許可監査**] ページに、これらの許可で実行された変更に関する詳細が表示されます。をクリックして、ページに表示されたデータを CSV ファイルに保存します。をクリックして、ページに表示されているデータを更新します。

次の表では、[**ファイル転送許可監査**] ページに表示される情報について説明します。

表 30. ファイル転送許可監査

行	説明
製品シリアル番号	デバイスのシリアル番号。
製品ファミリ	デバイスのモデルです。
Dell EMC へ転送	• デバイスからバックエンドへのファイル転送が有効になっている場合は **TRUE** が表示されます。 • デバイスからバックエンドへのファイル転送が無効になっている場合は **FALSE** が表示されます。
Dell EMC から転送	• バックエンドからデバイスへのファイル転送が有効になっている場合は **TRUE** が表示されます。 • バックエンドからデバイスへのファイル転送が無効になっている場合は **FALSE** が表示されます。
リモートでのスクリプト作成	• デバイスに対してリモートスクリプティングが有効になっている場合は **TRUE** を表示します。 • デバイスに対してリモートスクリプティングが無効になっている場合は **FALSE** を表示します。
作成時刻	デバイスが SupportAssist Enterprise に追加された日時。
修正時刻	許可がアップデートされた日時。
ユーザー名	許可を変更する際に使用されるユーザー アカウントの名前。

リモート スクリプト監査

[**リモート スクリプト監査**] ページには、バックエンドからデバイスに転送されたファイルの詳細が表示されます。

をクリックして、ページに表示されたデータを CSV ファイルに保存します。をクリックして、ページに表示されているデータを更新します。

次の表は、[**リモート スクリプト監査**] ページに表示される情報について説明しています。

表 31. リモート スクリプト監査

行	説明
スクリプト リクエスト ID	使用されているスクリプトの識別名または番号。
モデル	デバイスのモデルです。
シリアルナンバー	デバイスのシリアル番号。
スクリプト名	ファイルの送信に使用されたスクリプトの名前 (たとえば PUT)。
リモート スクリプト ステータス	スクリプトのステータス。

行	説明
開始時刻	スクリプトが開始された日時。
終了時刻	スクリプトが完了した日時。

19

ログ

ダウンロードログ ページは SupportAssist サービスのログを表示しています。

- ConnectEMC
- REST サービス
- ESRS エージェント
- Apache
- SAE アプリケーションと REST サービス

ログファイルには、ログファイルが生成された日時がファイル名として含まれています。ログファイルは自動的に圧縮され、24 時間ごとに保存されます。ログファイルをクリックしてダウンロードプロセスを開始します。

メモ: ダウンロードログ ページには、過去 30 日間に実行されたサービスのログが表示されます。

20

メンテナンス モードの概要

メンテナンスモード機能は、SupportAssist Enterprise のアラート処理と自動ケース作成機能を一時停止するため、アラートストームまたは計画されたメンテナンスアクティビティ中に不要なサポートケースが作成されることを防ぎます。監視対象デバイスからアラートストームを受信した場合、SupportAssist Enterprise はデバイスを自動的にメンテナンスモードにします。また、計画されたメンテナンスアクティビティの前にメンテナンスモード機能を手動で有効にして、ケースの自動作成機能を一時停止することもできます。

メンテナンス モード機能は、次のデバイスまたはデバイス モデルの場合にのみ適用されます。

- サーバー/ハイパーバイザー
- iDRAC
- シャーシ
- ネットワーク
- データ ストレージ：
  - PeerStorage (PS) /EqualLogic
  - Storage Center (SC) / Compellent
  - Fluid File System (FluidFS)
  - PowerVault

次の項では、メンテナンスモード機能の詳細について説明します。

グローバルレベルのメンテナンスモード

グローバルレベルのメンテナンス モードでは、すべての監視対象デバイスがメンテナンス モードとなり、アラート処理と自動ケース作成が一時停止されます。このモードでは、黄色の **[メンテナンス モード]** のバナーがページ上部に表示されます。このモードを有効にして、ダウンタイムまたは定期メンテナンス アクティビティ間に不要なサポート ケースが作成されることを防ぐことができます。グローバルレベルのメンテナンス モードを有効にする手順については、「グローバルレベルのメンテナンスモードの有効化または無効化」を参照してください。

デバイスレベルのメンテナンスモード

デバイスレベルのメンテナンスモードは、特定のデバイスに対するアラート処理とケースの自動作成を一時停止します。その他すべての監視対象デバイスについては、SupportAssist Enterprise は引き続きアラートを処理し、アラートがケース作成の条件を満たす場合は、サポートケースを作成します。デバイスレベルのメンテナンスモードは、次のように実施されます。

- **自動化されたデバイスレベルのメンテナンスモード** - 1 時間の間に特定のデバイスから 10 件以上の有効なハードウェアアラートを受け取った場合、SupportAssist Enterprise はデフォルトでそのデバイスを自動的にメンテナンスモードにします。デバイスは 30 分メンテナンスモード状態となるので、そのデバイスのために追加のサポートケースを作成することなく問題を解決することができます。また、E メール通知が一次連絡先および二次連絡先に送信され、デバイスは、メンテナンス モード アイコン  を **デバイス** ページに表示します。30 分後、デバイスは自動的にメンテナンスモードから除外され、SupportAssist Enterprise はこのデバイスの通常のアラート処理に復帰します。必要に応じて、手動でメンテナンスモードを有効にすることで、問題が解決できるまでこのデバイスのメンテナンスモードを維持することができます。30 分経過する前に、デバイスを自動メンテナンスモードから除外することもできます。デバイスレベルのメンテナンス モードを有効または無効にする手順については、「デバイスレベルのメンテナンスモードの有効化または無効化」を参照してください。
- 手動による **デバイスレベルのメンテナンスモード** - デバイスに計画されたメンテナンスアクティビティがあり、SupportAssist Enterprise にサポートケースを自動作成させないようにするために、そのデバイスをメンテナンスモードにすることができます。メンテナンスモードに設定されている間、デバイスはメンテナンス モード アイコン  を **デバイス** ページに表示します。メンテナンスアクティビティの完了後、デバイスをメンテナンスモードから解除して、SupportAssist Enterprise がデバイスからのアラートの通常処理を再開できるようにします。デバイスレベルのメンテナンス モードを有効にする手順については、「デバイスレベルのメンテナンスモードの有効化または無効化」を参照してください。

グローバルレベルおよびデバイスレベルのメンテナンスモード機能は、次の例にあるように、互いに独立して動作します。例：

- デバイスが手動メンテナンスモードに設定されている場合、グローバルレベルのメンテナンスモードを有効にしてから無効化しても、デバイスは手動メンテナンスモードを引き続き維持します。

- デバイスが自動メンテナンスモードに設定されている場合、グローバルレベルのメンテナンスモードを有効にしてから無効化しても、デバイスは 30 分間自動メンテナンスモードを引き続き維持します。

トピック：

グローバルレベルのメンテナンスモードの有効化または無効化

手順

1. SupportAssist のヘッダー領域で、**About** をクリックします。
   About ページが表示されます。
2. **メンテナンスモード**セクションで、次のいずれかを実行します。
   - メンテナンスモードを有効にするには、**有効化** をクリックします。
   - メンテナンスモードがすでに有効の場合は、**無効に化** をクリックします。

   メンテナンス モードが有効になっていると、SupportAssist Enterprise ユーザー インターフェイスに**メンテナンスモード**バナーが表示されます。

デバイスレベルのメンテナンスモードの有効化または無効化

特定のデバイスに計画されたメンテナンスアクティビティがあり、SupportAssist Enterprise にそのデバイスからのアラートを処理させないようにするために、そのデバイスをメンテナンスモードにすることができます。メンテナンスアクティビティの完了後、デバイスをメンテナンスモードから解除して、SupportAssist Enterprise がデバイスからのアラートの処理を再開できるようにします。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. **デバイス** ページでデバイスを選択します。
   デバイス概要 ペインが表示されます。
3. **メンテナンスモード**で**タスク**リストから、要件に応じて、**有効**または**無効**を選択します。

   特定のデバイスでメンテナンス モードが有効になっている場合は、[**デバイス**] ページにデバイス名とともに  が表示されます。デバイスのメンテナンスモードを無効にする場合は、メンテナンスモードアイコンがデバイス名から削除されます。

21

オフライン モードの概要

オフライン モード機能は、SupportAssist Enterprise のアラート処理および自動ケース作成機能を一時停止します。これにより、計画的な保守作業中に不要なサポート ケースが作成されることを防ぎます。オフライン モード機能は、次のデバイスまたはデバイス モデルに適用されます。

- データ保護
- ハイパーコンバージド インフラストラクチャ

  メモ: オフライン モードは Web スケール モデルには適用されません。
- データ ストレージ

  メモ: オフライン モードは、Peer Storage (PS) / EqualLogic、Storage Center (SC) / Compellent、Fluid File System (Fluid FS)、および PowerVault には適用されません。

すべてのデバイスまたは特定のデバイスに対してオフライン モードを有効にできます。

トピック :

グローバル レベルのオフライン モードの有効化または無効化

手順

1. SupportAssist Enterprise のヘッダー領域で、**About** をクリックします。
   About ページが表示されます。
2. **設定詳細**セクションで、次のいずれかを実行します。
   - オフライン モードを有効にするには、**オフラインに設定**をクリックします。
   - デバイスが既にオフライン モードである場合は、**オンラインに設定**をクリックします。

デバイス レベルのオフライン モードの有効化または無効化

このタスクについて

特定のデバイスに計画されたメンテナンス アクティビティがあり、SupportAssist Enterprise にそのデバイスからのアラートを処理させないようにするために、そのデバイスをオフライン モードにすることができます。メンテナンス作業が完了したら、デバイスをオンラインに設定してデバイスからのアラートを処理できます。

デバイスに対してオフライン モードを有効または無効にします。デバイスをオフライン モードに設定すると、そのデバイスから生成されたアラートはケース作成のために処理されません。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. デバイスを選択します。
   デバイス概要 ペインが表示されます。
3. 次のいずれかの手順を実行してください。
   - デバイスをオフライン モードにセットするには、**オフラインに設定**をクリックします。

- デバイスが既にオフライン モードでセットされている場合は、**オンラインに設定**をクリックします。

22

SNMP の手動設定

デバイスの SNMP 設定（警告送信先）を設定すると、SupportAssist Enterprise でデバイスからの警告を確実に受信できます。SupportAssist Enterprise では、Dell EMC サーバーの SNMP 設定を自動で設定することができます。Dell EMC のシャーシおよびネットワーク デバイスについては、SNMP を手動で設定する必要があります。

トピック：

サーバーのアラート送信先を手動設定

デフォルトでは、サーバを追加するとき、サーバのアラート送信先を自動設定することを SupportAssist Enterprise に許可できます。自動 SNMP 設定に失敗した場合、次の方法を使用してデバイスの SNMP を設定できます。

- スクリプトファイルを実行する — SupportAssist Enterprise 導入フォルダにはスクリプトファイルが含まれており、これを使用してサーバーのアラート送信先を設定できます。
- 手動で SNMP を設定する - SNMP トラップサービスにアクセスすることで設定できます。

メモ: SupportAssist Enterprise の SNMP を設定 オプションを使用することで、アラート送信先の自動設定をいつでも再試行できます。SNMP の設定オプションについての詳細は、「SupportAssist Enterprise を使用した SNMP の設定」を参照してください。

Linux を実行するサーバーのアラート送信先の手動設定

Linux オペレーティング システムを実行するデバイスのアラート送信先を手動で設定するには、次の手順を実行します。

手順

1. コマンド `rpm -qa | grep snmp` を実行し、**net-snmp** パッケージがインストールされていることを確認します。
2. `cd /etc/snmp` を実行して snmp ディレクトリに移動します。
3. VI エディタ（**vi snmpd.conf**）で、**snmpd.conf** を開きます。
4. **snmpd.conf** で **# group context sec.model sec.level prefix read write notif** を検索し、**read**、**write**、**notif** の各フィールドの値が **all** となっていることを確認します。
5. **snmpd.conf** ファイルの末尾、**Further Information** の前に、次のフォーマットでエントリを追加します `Trapsink <IP address of the server where SupportAssist Enterprise is installed> <community string>`。たとえば、`trapsink 10.94.174.190 public` とします。
6. SNMP サービスを再起動します（`service snmpd restart`）。

Linux を実行するサーバーのアラート送信先をスクリプト ファイルを使用して手動設定する

前提条件

- Net-SNMP がシステムにインストールされている必要があります。
- デバイス上で、root 権限を持っていることを確認します。

スクリプトファイルは、以下のオペレーティングシステムを実行しているデバイスのみでサポートされています。

- Red Hat Enterprise Linux 5.5（32 ビットおよび 64 ビット）

- Red Hat Enterprise Linux 5.7 (32 ビットおよび 64 ビット)
- Red Hat Enterprise Linux 5.8 (32 ビットおよび 64 ビット)
- Red Hat Enterprise Linux 5.9 (32 ビットおよび 64 ビット)
- Red Hat Enterprise Linux 5.10 (32 ビットおよび 64 ビット)
- Red Hat Enterprise Linux 5.11 (32 ビットおよび 64 ビット)
- Red Hat Enterprise Linux 6.1 (64 ビット)
- Red Hat Enterprise Linux 6.2 (64 ビット)
- Red Hat Enterprise Linux 6.3 (64 ビット)
- Red Hat Enterprise Linux 6.4 (64 ビット)
- Red Hat Enterprise Linux 6.5 (64 ビット)
- Red Hat Enterprise Linux 6.7 (64 ビット)
- Red Hat Enterprise Linux 6.8 (64 ビット)
- Red Hat Enterprise Linux 7.0 (64 ビット)
- Red Hat Enterprise Linux 7.1 (64 ビット)
- Red Hat Enterprise Linux 7.2 (64 ビット)
- SUSE Linux Enterprise Server 10 SP 3 (32 ビットおよび 64 ビット)
- SUSE Linux Enterprise Server 10 SP 4 (32 ビットおよび 64 ビット)
- SUSE Linux Enterprise Server 11 (64 ビット)
- SUSE Linux Enterprise Server 11 SP 1 (32 ビットおよび 64 ビット)
- SUSE Linux Enterprise Server バージョン 11 SP2 (64 ビット)
- SUSE Linux Enterprise Server 11 SP3 (64 ビット)
- SUSE Linux Enterprise Server 11 SP4 (64 ビット)
- SUSE Linux Enterprise Server 12 (64 ビット)
- SUSE Linux Enterprise Server 12 SP1 (64 ビット)
- CentOS 7.0
- CentOS 6.0
- Oracle Linux 7.1
- Oracle Linux 6.7

手順

1. SupportAssist Enterprise が導入されているサーバー上で、`<SupportAssist Enterprise が導入されているドライブ>:/opt/dell/supportassist/scripts/` フォルダーを探します。
2. フォルダにあるスクリプトファイル (`LinuxSNMPConfig.sh`) をコピーし、デバイスの目的の場所 (`\root` など) にそれを貼り付けます。
3. ターミナルウィンドウを開き、ルート権限を持つユーザーとしてログインします。
4. 次の構文を使用して、デバイスで次のスクリプトファイルを実行します：`sh LinuxSNMPConfig.sh -d <IP address of the server where SupportAssist Enterprise is installed>`。たとえば、`sh LinuxSNMPConfig.sh -d 10.10.10.10` とします。

Web インターフェイスを使用した iDRAC のアラート送信先を手動設定

iDRAC のアラート送信先を手動で設定するには、次の手順を実行します。

手順

1. iDRAC ウェブインタフェースにログインします。
2. **概要** > **サーバ** > **アラート** に移動します。
3. **[アラート]** セクションで、**[有効]** オプションが選択されていることを確認します。
4. **[アラート フィルタ]** セクションで、次のオプションが選択されていることを確認します。
   - **システムの正常性**
   - **ストレージ**
   - **設定**
   - **メンテナンスモード**

- アップデート
- 警告
- 重要

5. [アラートとリモート システム ログ設定] セクションで、[SNMP トラップ] 列のすべてのフィールドが選択されていることを確認します。
6. **SNMP と電子メールの設定** をクリックします。
7. **IP 送信先リスト** セクションで、**状態** オプションを選択してアラート送信先フィールドを有効にします。
   最大 8 つの送信先アドレスを指定できます。オプションの詳細については、「*iDRAC オンラインヘルプ*」を参照してください。
8. **送信先アドレス** フィールドに、SupportAssist Enterprise がインストールされているサーバの IP アドレスを入力します。
9. 該当するフィールドに iDRAC SNMP コミュニティ文字列 (Public) と SNMP アラートポート番号 (162 など) を入力します。
   オプションの詳細については、「*iDRAC オンラインヘルプ*」を参照してください。
   メモ: コミュニティ文字列の値は、iDRAC から送信される SNMP (簡易ネットワーク管理プロトコル) アラートトラップで使用されるコミュニティ文字列を示します。送信先のコミュニティ文字列が iDRAC コミュニティ文字列と同じであることを確認します。デフォルトのコミュニティ文字列は「Public」です。
10. **適用** をクリックします。
    アラート送信先が設定されます。
11. [SNMP トラップ形式] セクションで、[SNMP v1] または [SNMP v2] が選択されていることを確認し、[適用] をクリックします。

    iDRAC は、SupportAssist Enterprise がインストールされているサーバにアラートを転送するように設定されました。
    メモ: 他の方法を使用して iDRAC のアラート送信先を設定する方法については、の「IP アラート送信先の設定」を参照してください。

Web インターフェイスを使用したシャーシのアラート送信先を手動設定

前提条件

管理者権限で CMC ウェブインターフェイスにログインしている必要があります。

手順

1. システムツリーで **Chassis Overview (シャーシ概要)** に移動し、**Alerts (アラート)** > **Chassis Events (シャーシイベント)** の順にクリックします。
   Chassis Events (シャーシイベント) ページが表示されます。
2. **Chassis Event Filters Configuration (シャーシイベントフィルター設定)** セクションで、**Enable Chassis Event Alerts (シャーシイベントアラートを有効化)** オプションを選択して、アラートの生成を有効化します。
3. すべてのイベントに対してアラートを生成するには、**Chassis Event List (シャーシイベントリスト)** セクションのカラムヘッダーで **Enable Alert (アラートを有効化)** オプションを選択します。
4. システムツリーで **Chassis Overview (シャーシ概要)** に移動し、**Alerts (アラート)** > **Trap Settings (トラップ設定)** の順にクリックします。
   Chassis Event Alert Destinations (シャーシイベントアラートの送信先) ページが表示されます。
5. 次の手順を実行します。
   - **Destination (送信先)** フィールドに、SupportAssist Enterprise がインストールされているサーバの IP アドレスを入力します。
   - **Community String (コミュニティ文字列)** フィールドで、SupportAssist Enterprise がインストールされているサーバが属する有効なコミュニティ文字列を入力します。
     メモ: CMC は public としてデフォルトの SNMP コミュニティ文字列を使用します。より高いセキュリティを確保するため、デフォルトのコミュニティ文字列を変更し、空白以外の値を設定することをお勧めします。
   - **Enabled (有効化)** フィールドで、SupportAssist Enterprise がインストールされているサーバの IP アドレスに対応するチェックボックスを選択します。
6. **Apply (適用)** をクリックし、設定を保存します。
7. 宛先 IP アドレスが SNMP トラップを受信しているかどうかをテストするには、**Test SNMP Trap (SNMP トラップをテスト)** 列の **Send (送信)** をクリックします。

   IP アラートの送信先が設定されます。

ネットワーク デバイスのアラート送信先を手動設定

このタスクについて

メモ: ネットワークデバイスのアラート送信先を設定する手順は、ネットワークデバイスのタイプやモデルに応じて異なる場合があります。特定のネットワーク デバイス モデルのアラート設定に関する情報については、ネットワーク デバイス関連ドキュメントを参照してください。

手順

1. PuTTY などのターミナルエミュレータを使用して、ネットワークデバイスにログインします。
   ターミナルウィンドウが表示されます。
2. `configure` と入力し、Enter を押します。
3. `snmp-server host <SupportAssist Enterprise` がインストールされているサーバーの `IP` アドレス`> traps version 1` と入力します。
4. アラート送信先が正常に設定されたことを確認するには、`show running-config snmp` と入力して Enter を押します。
   デバイスに設定されているアラート送信先の一覧が表示されます。

23

SupportAssist Enterprise 機能の維持

一定期間にわたって会社の IT セットアップによって発生する変更により、SupportAssist Enterprise の設定またはアップデートが必要になることがあります。一定期間にわたって SupportAssist Enterprise 機能を維持するには、以下の対応が必要になる場合があります。

- デバイスの監視を有効にする。「デバイス監視の有効化または無効化」を参照してください。
- 会社のセキュリティ ポリシーまたはその他の理由のためにデバイス資格情報が変更された場合は、デバイスの資格情報（ユーザー名とパスワード）を編集する。「アカウント資格情報の編集」を参照してください。
- Dell OpenManage Server Administrator（OMSA）のような依存関係があるコンポーネントをインストールまたはアップグレードする。「SupportAssist Enterprise を使用した OMSA のインストールまたはアップグレード」を参照してください。
- デバイスの SNMP を設定する。「SupportAssist Enterprise を使用した SNMP の設定」を参照してください。
- 該当する場合、SupportAssist Enterprise のプロキシサーバの設定をアップデートする。「プロキシサーバを設定」を参照してください。
- 該当する場合、SupportAssist Enterprise の SMTP サーバ（メールサーバ）の設定をアップデートする。「SMTP サーバーを設定」を参照してください。
- 接続性テストを実行して SupportAssist Enterprise が依存関係のあるすべてのネットワーク リソースに接続できることを確認する。「ネットワーク接続性テスト」を参照してください。
- ケース作成テストを実行して SupportAssist Enterprise の自動ケース作成機能を確認する。「ケース作成機能をテスト」を参照してください。
- サーバのシステムイベントログをクリアする。「システムイベントログのクリア」を参照してください。
- SupportAssist Enterprise をアップグレードまたはアップデートする。「SupportAssist Enterprise のアップデート」を参照してください。

SupportAssist Enterprise によるデバイスの監視を行わない場合またはその他の理由によりデバイスを削除することもあります。「デバイスの削除」を参照してください。

トピック：

デバイス監視の有効化または無効化

このタスクについて

SupportAssist Enterprise が監視できるデバイスの場合は、デバイス追加中でも監視を有効にすることができます。必要に応じて、**デバイス** ページからいつでもデバイスの監視の有効 / 無効を切り替えることができます。デバイスにハードウェア問題が発生した際に SupportAssist Enterprise が自動的にサポートケースを作成できるようにするには、そのデバイスの監視を有効にする必要があります。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. 監視を有効または無効にするデバイスを選択します。
   [**デバイス**] ページの右側に [デバイス概要] ペインが表示されます。
3. **監視** で、必要に応じて **有効** または **無効** を選択します。

   メモ: SupportAssist Enterprise がデバイスを監視できるようにし、さらに監視の権限を付与するには、デバイスの SNMP も設定する必要があります。デバイスの SNMP 設定の手順については、「SupportAssist Enterprise を使用した SNMP の設定」および「SNMP の手動設定」を参照してください。

SupportAssist Enterprise を使用した OMSA のインストールまたはアップグレード

前提条件

ターゲットデバイスのシステムドライブへの読み書きアクセスが必要です。

このタスクについて

サーバーでハードウェアの問題を監視するには、Dell OpenManage Server Administrator（OMSA）エージェントがサーバーにインストールされ、実行している必要があります。OMSA がインストールされていないか、またはデバイスでのアップグレードが必要である場合は、**デバイス** ページの **ステータス** 列に該当するメッセージが表示されます。**OMSA のインストール / アップグレード** オプションを使用すると、デバイスで推奨されるバージョンの OMSA を自動的にダウンロードしてインストールすることができます。

メモ: SupportAssist Enterprise が奨励する OMSA バージョンは、PowerEdge サーバとサーバ上で実行されているオペレーティングシステムによって異なる場合があります。OMSA の推奨バージョンについての情報については、にある『*SupportAssist Enterprise バージョン 4.0 サポート マトリックス*』を参照してください。

メモ: SupportAssist Enterprise を使用することによる OMSA のインストールまたはアップグレードは、次のオペレーティング システムを実行しているサーバまたはハイパーバイザーではサポートされません。

- **Oracle Enterprise Linux**
- **CentOS**
- **Citrix XenServer**
- **VMware ESX または VMware ESXi**
- **Oracle Virtual Machine**
- **Debian 7.*x***
- **Debian 8.*x***
- **Ubuntu 14.*x***
- **Ubuntu 16.*x***
- **Ubuntu 18.*x***

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. OMSA のインストールまたはアップグレードを行うサーバを選択します。
   [**デバイス**] ページの右側に [デバイス概要] ペインが表示されます。
3. **タスク** リストから、**OMSA のインストール / アップグレード** を選択します。

   メモ: 選択したサーバで SupportAssist Enterprise が OMSA のインストールまたはアップグレードがサポートしていない場合、OMSA のインストール / アップグレード オプションが無効になっています。

   デバイス ページの **ステータス** 行に、OMSA のインストールまたはアップグレードのステータスが表示されます。

SupportAssist Enterprise を使用した SNMP の設定

前提条件

ターゲットデバイスのシステムドライブへの読み書きアクセスが必要です。

このタスクについて

SNMP を設定すると、デバイスのアラートの宛先が設定され、デバイスからのアラートが、SupportAssist Enterprise がインストールされているサーバーに転送されるようになります。デバイスの SNMP の設定が設定されていない場合は、**デバイス** ページのステータス列に適切なメッセージが表示されます。**SNMP の設定** オプションを使用して、デバイスの SNMP を自動的に設定できます。

メモ: SupportAssist Enterprise を使用した SNMP の構成は、次のオペレーティングシステムを実行しているデバイスまたはハイパーバイザではサポートされません。

- **Oracle Enterprise Linux**
- **VMware ESXi**
- **Oracle Virtual Machine**

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. SNMP を設定するデバイスを選択します。

   メモ: 選択したデバイス上で SupportAssist Enterprise が SNMP の設定をサポートしていない場合、SNMP の設定 オプションが無効になっています。

   [**デバイス**] ページの右側に [デバイス概要] ペインが表示されます。
3. **タスク** リストから、**SNMP の設定** を選択します。
   デバイス ページの **ステータス** 行に、SNMP 設定のステータスが表示されます。

システムイベントログのクリア

このタスクについて

システムイベントログ (SEL) またはハードウェアログ (組み込みシステム管理 (ESM) ログ) は Dell PowerEdge サーバの潜在的なハードウェア問題をレポートします。以下の状況において、SupportAssist Enterprise で使用可能な **[システム イベント ログのクリア]** オプションを使用して、SEL をクリアできます。

- 問題が解決した後でも、サーバ上にエラーメッセージが表示される。
- SEL フルエラーメッセージが表示される。

注意: SEL をクリアすると、サーバのイベント履歴が削除されます。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. システムイベントログをクリアするサーバを選択します。

   メモ: デバイスタイプをサーバーとして SupportAssist Enterprise に追加したデバイスに OMSA がインストールされていない場合、システムイベントログのクリアオプションは無効になります。

   [**デバイス**] ページの右側に [デバイス概要] ペインが表示されます。
3. **タスク**リストから、**システムイベントログのクリア**を選択します。
   SEL がデバイスからクリアされている間、デバイスには SupportAssist Enterprise の **システムイベントログをクリアしています**ステータスが表示されます。SEL がクリアされた後、デバイスには **システムイベントログをクリアしました**ステータスが表示されます。

詳細な検出を実行

前提条件

認証情報プロファイルがデバイスに割り当てられている必要があります。

このタスクについて

詳細な検出では、デバイスおよびそれに関連するデバイスタイプを検出できます。「詳細な検出」を参照してください。

手順

1. **デバイス** > **デバイスを表示** に移動します。
   デバイス ページが表示されます。
2. 詳細な検出を実行するデバイスを選択します。
   デバイス概要 ペインが表示されます。

3. **タスク** リストから、**詳細な検出を実行** を選択します。
   詳細な検出を実行 ウィンドウが表示されます。

   メモ: 詳細な検出がデバイスに適用されない場合、詳細な検出を実行 オプションは無効になります。

4. 認証情報プロファイルを選択し、**次へ** をクリックします。
   デバイスが再検証され、関連するデバイスが検出されます。

24

その他の役立つ情報

本章では、SupportAssist Enterprise を使用する際に必要となる場合がある追加情報を説明します。
トピック：

サーバでのハードウェア問題の監視

SupportAssist Enterprise では、次の方法を使用して Dell EMC サーバーを監視できます。

- **エージェントベースの監視** - この方法では、**デバイスタイプ** を **サーバー / ハイパーバイザー** として追加されたデバイスを監視するのに使用します。この方法では、エージェントはデバイスと SupportAssist Enterprise のインタフェースとして機能します。エージェントは、デバイスでハードウェアイベントが発生するたびにアラート（SNMP トラップ）を生成します。エージェントベース方式を使用したデバイスの監視では、SupportAssist Enterprise は Dell OpenManage Server Administrator（OMSA）エージェントに依存しています。OMSA エージェントは、インストールされているデバイスのさまざまなコンポーネントの正常性を監視するアプリケーションです。デバイスでハードウェアイベントが発生するたびにアラートを生成します。SupportAssist Enterprise はアラートを処理して、そのアラートがサポートケースを作成するために十分であるかどうかを判断します。エージェントベースの監視のためにデバイスを追加する手順については「サーバまたはハイパーバイザーの追加」を参照してください。

  メモ: SupportAssist Enterprise は、OMSA なしではエージェントベース方式でのデバイスの監視を行うことができません。

  メモ: OMSA のインストールは、特定のオペレーティングシステムではサポートされていない可能性があります。SupportAssist Enterprise は、エージェントレスの監視方式を使用した場合にのみ、このようなオペレーティングシステムを実行しているデバイスを監視することができます。エージェントベースの監視に対応したオペレーティングシステムの要件については、 にある『*SupportAssist Enterprise バージョン 4.0 サポート マトリックス*』を参照してください。
- **エージェントレス監視**—この方法は、iDRAC デバイスを監視するために使用されます。この方法では、デバイス上で使用できる iDRAC がデバイスと SupportAssist Enterprise 間のインターフェイスとして機能します。デバイスでハードウェアイベントが発生するたびに、iDRAC がアラートを生成します。SupportAssist Enterprise はアラートを処理して、そのアラートがサポートケースを作成するために十分であるかどうかを判断します。エージェントレス監視を実行するデバイスを追加する手順については、「iDRAC の追加」を参照してください。

  メモ: エージェントレス監視は、yx2x 以降の PowerEdge サーバ（iDRAC 7 以降）でのみサポートされています。

  メモ: iDRAC を、SNMP と IPMI を介してアラートを送信するように設定することができます。ただし、SupportAssist Enterprise は SNMP を介して送信されたアラートのみ受け付けることができます。SupportAssist Enterprise が iDRAC から送信されるアラートを受信するには、iDRAC ウェブコンソールの アラートとリモートシステムのログ設定 セクションで、すべての SNMP トラップ オプションを確実に選択してください。

エージェントベースの監視の利点

エージェントレス（iDRAC）方法で yx2x 以降の PowerEdge サーバを監視することもできますが、エージェントベース（OMSA）方法には次のメリットがあります。

- OMSA と iDRAC のアラート生成機能は異なります。yx3x 以降の PowerEdge サーバでは、OMSA と iDRAC のアラート生成機能はほぼ同一です。ただし、チップセットおよびソフトウェア RAID からのアラートは OMSA 経由でのみ利用可能です。
- オペレーティングシステムおよびソフトウェア コンポーネントのバージョンに関する推奨事項は、ProSupport Plus、ProSupport Flex for Data Center、または ProSupport One for Data Center のサービス契約を結んでいるデバイスが OMSA を通じて監視されている場合にのみ利用できます。
- OMSA は、nx9x から yx1x までの PowerEdge サーバをモニタリングするための唯一のオプションです。

OMSA の自動インストールまたは自動アップグレードのサポート

エージェントベース方式でデバイスを監視するには、デバイスに Dell OpenManage Server Administrator（OMSA）エージェントがインストールされ、実行している必要があります。OMSA エージェントは、インストールされているデバイスのさまざまなコンポーネントの正常性を監視するアプリケーションです。デバイスで OMSA がインストールおよび実行されていると、デバイス上でハードウェアイベントが発生するたびに OMSA エージェントがアラートを生成します。SupportAssist Enterprise はアラートを処理して、アラートがハードウェアの問題を示しているかどうかを識別します。OMSA の詳細については、Delltechcenter.com/OMSA にアクセスしてください。

メモ: SupportAssist Enterprise が奨励する OMSA バージョンは、PowerEdge サーバとサーバ上で実行されているオペレーティングシステムによって異なる場合があります。OMSA の推奨バージョンの情報については、にある『*SupportAssist Enterprise Version 4.0 Support Matrix*』を参照してください。

SupportAssist Enterprise には、推奨バージョンの OMSA をデバイス上に自動的にダウンロードしてインストールする機能があります。エージェントベースの監視用にサーバが追加されると、SupportAssist Enterprise はデフォルトでそのデバイスに推奨バージョンの OMSA がインストールされているかどうかを確認します。

- OMSA がデバイスにインストールされていない場合は、SupportAssist Enterprise が推奨バージョンの OMSA をデバイスにダウンロードしてインストールすることを確認するプロンプトを表示します。確認後、SupportAssist Enterprise がバックグラウンドで OMSA をダウンロードし、インストールします。OMSA インストールステータスは、**デバイス** ページの **ステータス** 列に表示されます。OMSA をインストールしないことを選択した場合、デバイスのステータスには **OMSA はインストールされていません** と表示されます。後で OMSA をインストールするには、[デバイス概要] ペインで **タスク** > **OMSA のインストール/アップグレード** オプションを使用できます。
- デバイスに OMSA がすでにインストールされている場合、SupportAssist Enterprise は、その OMSA のバージョンが SupportAssist Enterprise 用の推奨バージョンと一致するかどうかを検証します。既存の OMSA バージョンが推奨バージョンでなく、OMSA の推奨バージョンへの直接アップグレードがサポートされる場合は、SupportAssist Enterprise がデバイスでの OMSA のダウンロードとアップグレードを確認するプロンプトを表示します OMSA のアップグレードステータスは、**デバイス** ページの **ステータス** 列に表示されます。OMSA をアップグレードしないことを選択した場合、デバイスのステータスには **OMSA の新しいバージョンが使用可能です** と表示されます。後で OMSA をアップグレードするには、[デバイス概要] ペインの **タスク** > **OMSA のインストール/アップグレード** オプションを使用します。

  メモ: OMSA のバージョン *n* への直接アップグレードがサポートされるのは、2 つ前の OMSA バージョン *(n-2)* からのみです。直接アップグレードがサポートされていない場合、デバイスに OMSA を手動でダウンロードしてアップグレードする必要があります。たとえば、OMSA バージョン 7.0 がデバイスにすでにインストールされているが、OMSA の推奨バージョンが 7.4 であるという場合、OMSA バージョン 7.0 を手動で 7.2 にアップグレードする必要があります。OMSA バージョン 7.2 へのアップグレード後、デバイス概要 ペインの More Tasks(その他のタスク)> Install/Upgrade OMSA(OMSA のインストール / アップグレード) オプションを使用して、OMSA バージョン 7.4 にアップグレードすることができます。または、手動で OMSA バージョン 7.4 をダウンロードして、アップグレードすることもできます。

メモ: SupportAssist Enterprise を有効化または使用して OMSA のインストールまたはアップグレードをする場合は、ダウンロードされた OMSA のパッケージは SupportAssist Enterprise インストールフォルダに保持されます。以前の操作で互換性のあるバージョンの OMSA がすでにダウンロードされている場合、SupportAssist Enterprise はこれを再度ダウンロードしません。この状況下では、SupportAssist Enterprise はすでにダウンロードされたバージョンの OMSA を使用して、デバイスで OMSA のインストールまたはアップグレードを行うのみとなります。

メモ: OMSA のダウンロードに要する時間は、インターネットのダウンロード速度とネットワークの帯域幅によって異なります。

デバイスで推奨バージョンの OMSA がインストールおよび実行されている場合、デバイスのステータスには、✓**成功**と表示されます。

メモ: SupportAssist Enterprise を使用した OMSA の自動インストールは、Citrix XenServer、VMware ESXi、または ESX を実行しているデバイス上ではサポートされません。SupportAssist Enterprise がこれらのデバイス上でハードウェアの不具合が検知されるようにするには、手動で OMSA をダウンロードしてインストールしてください。

SNMP の自動設定のサポート

SupportAssist Enterprise がデバイスを監視できるようにするには、SupportAssist Enterprise が導入されているサーバーにアラート (SNMP トラップ) が転送されるようにデバイスを設定する必要があります。SNMP を設定すると、デバイスのアラート宛先が設定され、デバイスからのアラートが、SupportAssist Enterprise が導入されているサーバーに転送されるようになります。SupportAssist Enterprise により、SupportAssist Enterprise を導入しているサーバーにデバイスがアラートを転送できるように、デバイスの SNMP を自動的に設定することができます。デバイスの追加時またはそれ以降、SupportAssist Enterprise によってデバイスの SNMP を設定できます。SNMP 設定のステータスは、**[デバイス]** ページの **[ステータス]** 列に表示されます。SupportAssist Enterprise がデバイスの SNMP を設定しているとき、デバイスには、**SNMP を設定しています。**ステータスが表示されます。[デバイスの概要] ペインにある **[タスク]** > **[SNMP の設定]** オプションを使用しても、いつでもデバイスの SNMP を自動的に設定できます。

メモ: SupportAssist Enterprise でデバイスの SNMP を自動設定できる場合、デバイスのアラートの宛先は SupportAssist Enterprise が導入されているサーバーの IP アドレスに設定されています。

詳細な検出

詳細な検出機能により、プライマリデバイスに関連付けられているその他のデバイスを検出し、追加することができます。詳細な検出を実行するには、検出タスクの資格情報プロファイルを割り当てる必要があります。プライマリデバイスの検出中またはプライマリデバイスが検出された後に詳細な検出を実行する選択できます。

メモ: 詳細な検出では、全体の検出プロセスの時間が増加する可能性があります。

次の表には、プライマリデバイスと詳細検出によって検出されたその関連デバイスがリストされています。

表 32. プライマリデバイスと詳細検出によって検出されたその関連デバイス

プライマリデバイス	詳細検出によって検出された関連デバイス
シャーシ	• iDRAC* • Networking スイッチ
Storage PS Series グループ	• Storage PS Series メンバー • Storage PS Series FluidFS
Storage MD Series エンクロージャ	• JBOD
ネットワーク - 管理スイッチ	• メンバースイッチ
ウェブスケール統合型アプライアンス	• コントローラ VM • ノード (iDRAC / ESX)

* シャーシの詳細な検出では、iDRAC (モジュラーサーバ) の検出は、iDRAC 7 以降でのみサポートされます。

メモ: シャーシの詳細な検出では、シャーシに関連するネットワークデバイスも検出されます。ただし、システム情報を収集できるのは、SupportAssist Enterprise でサポートされるネットワークデバイスからのみです。サポート対象のネットワーキング デバイス リストについては、 にある『*SupportAssist Enterprise バージョン 4.0 サポート マトリックス*』を参照してください。

デバイスの相互関係

ホスト オペレーティング システムの IP アドレスとデバイスの iDRAC IP アドレスの両方を使用して、SupportAssist Enterprise でサーバーを追加 (検出) できます。このような場合、**[デバイス]**ページには、同じデバイスに対して 2 つの異なるリストが表示されます。SupportAssist Enterprise は、オペレーティング システムと iDRAC の両方を介してデバイスからアラートを受信します。ただし、

運用上の目的で、SupportAssist Enterprise は、オペレーティング システムの IP アドレス iDRAC とデバイスの IP アドレスを相互に関連づけ、デバイスを 1 つのデバイスと見なします。デバイスが関連づけられている場合、予想される動作は次のとおりです。

- オペレーティング システムと iDRAC から送信されたアラートは関連づけられ、デバイスのサービスタグに対してサポート ケースが作成されます。
- システム情報が収集されると、両方のリストの**[デバイス]**ページに同じステータスが表示されます。
- 手動で開始された収集のシステム情報の場合 - システム情報は、**[デバイス]**ページの選択したデバイス リストを介して収集されます。たとえば、オペレーティング システムのリストが選択されている場合は、オペレーティング システムを介してシステム情報が収集されます。ただし、SupportAssist Enterprise がオペレーティング システムの IP アドレスを使用してデバイスに接続できない場合、システム情報は iDRAC を介して収集されます。
- 定期収集およびケース作成の場合 - システム情報は通常、オペレーティング システムを介して収集されます。ただし、SupportAssist Enterprise がオペレーティング システムの IP アドレスを使用してデバイスに接続できない場合、システム情報は iDRAC を介して収集されます。

関連付けビュー

デバイス ページでは、デバイスリストを表示する次の 2 つのビュータイプをサポートします。

- デフォルトのビュー - リストとして使用可能なすべてのデバイスを表示
- 関連付けビュー - その関連付けに基づいてグループとして使用可能なすべてのデバイスを表示。このビューでは、プライマリデバイスとそれにグループとして関連するデバイスを表示できます

次の表では、関連付けビューでデバイスのグループ化をリストします。

表 33. 関連付けビューでのデバイスのグループ化

プライマリデバイス	関連するデバイス
サーバ	• iDRAC • vCenter
シャーシ	• iDRAC* • Networking スイッチ
Storage PS Series グループ	• Storage PS Series メンバー • Storage PS Series FluidFS
Storage MD Series エンクロージャ	JBOD
ネットワーク - 管理スイッチ	メンバースイッチ
ウェブスケール統合型アプライアンス	• コントローラ VM • iDRAC

* iDRAC7 以降のみがシャーシ ノードの下に表示されます。

メモ: 関連ビューに表示される次のデバイスでは、システム情報の収集を開始できません。

- **JBOD**
- **Storage PS Series メンバー**
- **スタックスイッチ**
- **IP アドレス 0.0.0.0 で SupportAssist Enterprise のリストにあるデバイス**

接続されたストレージデバイスのハードウェア問題の検知

SupportAssist Enterprise は、PowerEdge サーバーの監視に加えて、サーバーに接続された Storage MD Series アレイから受信したアラートを処理することもできます。接続されたストレージ デバイスからのアラート生成は、サーバーにインストールされた OpenManage Storage Services(OMSS) アプリケーションを介して行われます。SupportAssist Enterprise でサーバへの OMSA の自動インストールを許可すると、デフォルトで OMSS もインストールされます。OMSA を手動でダウンロードしてサーバにインストールする場合は、OMSS もインストールしてください。そうしないと、SupportAssist Enterprise は接続されたストレージ デバイスで発

生する可能性のあるハードウェア問題を検知できません。接続されたストレージデバイスでハードウェア問題が検知されると、SupportAssist Enterprise は関連するサーバのサポートケースを自動的に作成します。

OEM デバイスのサポート

Dell EMC OEM 対応デバイス (再ブランド化またはノンブランド化された Dell EMC ハードウェアのいずれか) が追加された場合は、元の名前ではなく、再ブランド化された名前で分類されます。アラート処理やケースの自動作成 (サポート インシデント時に ProSupport Plus、ProSupport Flex for Data Center、ProSupport One for Data Cente サービスのいずれかとしてサポート レベルが検証された場合) といった Dell EMC の標準デバイスで利用できるすべての機能は、OEM 対応デバイスで利用できます。OEM デバイスによっては、SupportAssist Enterprise ユーザー インターフェイスで、モデル名が空白になっている場合があります。

ケースの自動作成は Dell EMC エンタープライズ テクニカル サポートを通じてサポートされており、他のサポート ケース サービス リクエスト管理システムでは利用できません。

カスタムソリューション用に変更された他のシステムと同様に、SupportAssist Enterprise の機能をすべて検証して、それらの変更が正しく動作するようにすることをお勧めします。

SupportAssist Enterprise アプリケーション ログへのアクセス

このタスクについて

SupportAssist Enterprise は、システムイベントとログメッセージを次の場所に保存します。

- Var ログ
- 導入ログフォルダ : `/var/lib/docker/volumes/saede_logs/_data`

新しいログファイルは、システムに設定されているタイムゾーンに基づいて毎日午後 11 時 59 分に作成され、ログフォルダに保存されます。ログファイルには、当日のログ情報が含まれています。毎日の終わりに、ログファイルは `application.log <yyyymmdd の日付形式>` という名前に変更されます。2 日以上経過すると、ログファイルは自動的に圧縮されます。これにより、アラートが発生した日付で保存されたログファイルを正確に識別できます。たとえば、ログファイルは次のように表示されます。

- **地域**
- `application.log.`*20171101*
- `application.log.` *20171102* `.zip`
- `application.log.` *20171103* `.zip`

ログファイルは 30 日後にストレージからパージされます。

ログファイルには、`log4j.xml` ファイル内の次の値 (またはそれ以上) に対応するログメッセージが含まれています (FATAL、ERROR、WARN、INFO、DEBUG、特別な値 OFF および ALL)。`log4j.xml` ファイルは `/opt/dell/supportassist/config` で利用可能です。`log4j.xml` ファイル内の ERROR の値は、FATAL が ERROR よりも高いレベルであるため、FATAL および ERROR エラーのログメッセージを生成します。

SupportAssist Enterprise ユーザーインターフェイスからログをダウンロードするには、SupportAssist Enterprise にログインして **ログ** > **ダウンロードログ** に移動します。詳細については、「ログ」を参照してください。

PowerEdge サーバー シリーズの特定

PowerEdge サーバーは、*xnxx* または *yxnx* シリーズのサーバーとして表されます。ここでは次のようになります。

- *x* は 0 ~ 9 の数値を示します。
- *n* はサーバーのシリーズを示します。
- *y* はアルファベットの M、R、および T を示します。アルファベットは、次の通りサーバーのタイプを示します。M=モジュラー、R=ラック、T=タワー

次の表では、PowerEdge サーバーのさまざまなシリーズとサーバー モデルの表示についての情報を記載します。

表 34. PowerEdge サーバーの例

サーバーのシリーズ	サーバーモデルの表示	サーバーモデルの例
9 世代	PowerEdge *x*9*xx*	PowerEdge 2900

サーバーのシリーズ	サーバーモデルの表示	サーバーモデルの例
		PowerEdge 6950
10 世代	PowerEdge *yx*0*x*	PowerEdge M600 PowerEdge R300 PowerEdge T105
11 世代	PowerEdge *yx*1*x*	PowerEdge M610 PowerEdge R310 PowerEdge T110
12 世代	PowerEdge *yx*2*x*	PowerEdge M620 PowerEdge R620 PowerEdge T620
13 世代	PowerEdge *yx*3*x*	PowerEdge M630 PowerEdge R630 PowerEdge R730 PowerEdge FC630 PowerEdge T320
14 世代	PowerEdge *yx*4*x*	PowerEdge R740 PowerEdge T640 PowerEdge M640 PowerEdge R7415 DSS 9620
15 世代	PowerEdge *yx*5*x*	

イベント ストームの処理

SupportAssist Enterprise はイベント ストームの状況をインテリジェントに処理し、60 分のタイムスパン内に 1 つのデバイスから最大で 9 つの異なるアラートを許可します。ただし、デバイスから 10 個以上の個別のアラートを受信した場合、SupportAssist Enterprise は自動的にデバイスをメンテナンス モードに設定します。メンテナンス モードでは、デバイスからのアラートはそれ以上処理されなくなるため、不要なサポート ケースを作成せずにインフラストラクチャを変更できます。メンテナンス モードで 30 分が経過すると、SupportAssist Enterprise は自動的にデバイスをメンテナンス モードから解除し、デバイスの通常のアラート処理を再開します。メンテナンス モードの詳細については、メンテナンス モードの概要を参照してください。

Linux を実行するサーバー上の SupportAssist Enterprise の sudo アクセスを設定

Linux オペレーティング システムでは、sudo アクセス権を持つユーザーには、特定のコマンドを実行するための管理者権限が付与される場合があります。sudo ユーザーの資格情報を使用して SupportAssist Enterprise でリモート デバイスを追加した場合、SupportAssist Enterprise がデバイスからシステム情報を監視および収集するためには、次の手順を実行する必要があります。

前提条件

root 権限を持つユーザとしてリモートデバイスにログインしていることを確認します。

手順

1. ターミナルウィンドウを開きます。

2. ユーザー用のホーム ディレクトリ パスを設定します - `useradd user_name -d /home` と入力し Enter を押します。
3. `/etc/sudoers` ファイルを開きます。
4. 感嘆符 (!) を Requiretty 行に挿入します。たとえば、`!requiretty` などです。
5. お好みに合わせて、次のうち 1 つを追加します。
   - `%root ALL=(ALL) NOPASSWD: ALL` - ルート グループ内のすべてのユーザーに許可を付与します。
   - `user_name ALL=(ALL) NOPASSWD: ALL` - 特定のユーザーのみに許可を付与します。
6. `/etc/sudoers` ファイルを保存します。

SupportAssist Enterprise のアップデート

SupportAssist Enterprise では、SupportAssist Enterprise にログインしたときに利用可能なアップデートがあるかどうかを確認します。

SupportAssist Enterprise バージョン 4.0 以降を導入した場合は、次のアップデートについてバナーが表示されます。

- ドッカーのアップデート - バックエンド コンポーネントの修正またはアップデートを含みます
- オペレーティング システムまたは JRE アップデート - オペレーティング システムに対する SUSE からのアップデートを含みます
- 設定のアップデート - デバイス設定およびポリシーファイルのアップデートを含みます

メモ: SupportAssist Enterprise バージョン 2.x から SupportAssist Enterprise バージョン 4.0 以降にアップデートするには、SupportAssist Enterprise を手動でダウンロードして導入する必要があります。「SupportAssist Enterprise のダウンロード」および「SupportAssist Enterprise の導入」を参照してください。

バナーに次のオプションが表示されます。

- **今すぐダウンロード** - クリックすると、アップデートがローカル フォルダにダウンロードされます。
- **今すぐアップデート** - ダウンロードが完了した後に表示されます。クリックしてダウンロードしたアップデートをインストールします。

  メモ: Docker またはオペレーティング システムのアップデート中に、SupportAssist Enterprise からログアウトします。アップデートが完了すると、SupportAssist Enterprise サービスは自動的に再起動されます。
- **後で通知する** - クリックしてバナーを閉じます。バナーは SupportAssist Enterprise に再度ログインするまで表示されません。
- **詳細情報** - アップデートに関する詳細を提供します。