

## Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [はじめに](#)
- [Dell Management Console のインストール、アンインストール、およびアップグレード](#)
- [Dell OpenManage IT Assistant の検出設定の移行](#)
- [Dell Management Console への移行](#)
- [Dell Management Console のユーザーインターフェイス](#)
- [検出とインベントリ設定の設定](#)
- [Dell OpenManage Server Administrator ソリューションの導入](#)
- [ジョブおよびタスクの管理](#)
- [ハードウェアの設定タスク](#)
- [電源監視](#)
- [監視と警告](#)
- [Dell パッチ管理ソリューション](#)
- [レポート](#)
- [仮想化](#)
- [インベントリの属性](#)

---

## メモおよび注意

 **メモ:** コンピュータ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:** 手順に従わないと、ハードウェアの損傷やデータの損失につながる可能性があることを示しています。

---

本書の内容は予告なく変更されることがあります。  
© 2011 すべての著作権は Dell Inc. にあります。

Dell Inc. の書面による許可のない複製は、いかなる形態においても厳重に禁じられています。

本書に使用されている商標: Dell, DELL, ログ, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™ および EqualLogic™ は Dell Inc. の商標です。Microsoft®, Windows®, Microsoft® .NET Framework 3.5, Microsoft Internet Explorer® および Windows Server® は米国およびその他の国々における Microsoft Corporation の商標または登録商標です。Altiris®, Symantec™ および Notification Server™ は米国およびその他の国々における Symantec Inc. の商標または登録商標です。Brocade, Itrapid, および McData は Brocade Communications Systems, Inc. の商標です。

商標または製品の権利を主張する事業体を表すためにその他の商標および社名が使用されていることがあります。それらの商標や会社名は、一切 Dell Inc. に帰属するものではありません。

2011 - 06

---

[目次に戻る](#)

[目次に戻る](#)

## 仮想化

### Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [サポートされている仮想オペレーティングシステム](#)
- [仮想サーバーのサポートされている機能](#)
- [ESXi 設定](#)
- [Dell Management Console 設定](#)
- [注意点](#)

Dell Management Console では、仮想化サーバーを検出できます。また、ホストサーバーのハードウェアインベントリおよび正常性の監視もサポートします。

Dell Management Console の All Devices(すべてのデバイス)ツリーの Servers(サーバー)ノードの下に、物理ホストおよび仮想マシンが表示されます。

All Devices(すべてのデバイス)ツリーに `virtual_machine_to_host`(ホストする仮想マシン)関連付けを表示するには、新しいグループを作成します。

各仮想マシンはこのノードの下に表示されます。ホストを 1 つ選択すると、このサーバーで実行されているすべての仮想マシンが右ペインに表示されます。

ハードウェアインベントリは、Summary(概要)→Hardware Summary(ハードウェア概要)の Resource Manager(リソースマネージャ)に表示されます。

---

## サポートされている仮想オペレーティングシステム

- 1 Classic ESX
- 1 Embedded ESX
- 1 HyperV

---

## 仮想サーバーのサポートされている機能

- 1 検出
- 1 ホストと仮想マシンの関連付け
- 1 ハードウェアインベントリ

## 検出

ゲストマシンおよびホストマシンは、ネットワーク上で別々に検出されます。

 **メモ:** 仮想サーバーの検出後に仮想マシンを追加すると、Dell 管理コンソールではゲストとホストの関連付けは行われません。この問題を解決するには、仮想サーバーを再検出します。

### Classic ESX

Dell Management Console では、VMware SNMP エージェントを使用してホストデバイスを検出します。

ホストを検出する場合の前提条件は次のとおりです。

- 1 サーバーで SNMP サービスを有効にする
- 1 検出タスクで使用される接続プロファイルで SNMP を有効にする

### HyperV

Dell Management Console では、WMI プロバイダを使用してホストデバイスを検出します。

ホストを検出する場合の前提条件は次のとおりです。

- 1 サーバーで WMI サービスを有効にする
- 1 検出タスクで使用される接続プロファイルで WMI を有効にする

### Embedded ESX

Dell Management Console では、VMware によって提供された CIM プロバイダを使用してホストデバイスを検出します。

ホストを検出する場合の前提条件は次のとおりです。

- 1 サーバーで WSMAN サービスを有効にする
- 1 検出タスクで使用される接続プロファイルで WSMAN を有効にする

## ホストと仮想マシンの関連付け

- 1 仮想ホストサーバーは、これらのホストサーバーで実行されているハイパーバイザオペレーティングシステムに基づいて識別されます。
- 1 仮想ホストサーバーは、Virtual Host (仮想ホスト)ノードの All Devices (すべてのデバイス)ツリーに表示されます。
- 1 サーバーで実行されている仮想マシンは、ネットワーク上で個別に検出されます。
- 1 ホストで実行されているホストと仮想マシンの間の関連付けは、検出後に仮想マシンの MAC アドレス、IP アドレス、および UUID を使用して作成されます。
- 1 左ペインのホストサーバーをクリックすると、ホストに関連付けられている仮想マシンが右ペインに表示されます。

## インベントリ

### Classic ESX

ハードウェアインベントリは、Dell OpenManage Server Administrator SNMP エージェントを使用して表示されます。

Classic ESX サーバーのインベントリを開始する場合の前提条件は次のとおりです。

- 1 Server Administrator がサーバーにインストールされている
- 1 サーバーで SNMP サービスが有効になっている
- 1 インベントリタスクで使用される接続プロファイルで SNMP が有効になっている

### HyperV

ハードウェアインベントリは、Server Administrator SNMP または WMI エージェントを使用して表示されます。

HyperV サーバーのインベントリを開始する場合の前提条件は次のとおりです。

- 1 Server Administrator がサーバーにインストールされている
- 1 サーバーで SNMP または WMI サービスが有効になっている
- 1 インベントリタスクで使用される接続プロファイルで SNMP または WMI、もしくはその両方が有効になっている

### Embedded ESX

ハードウェアインベントリは、VMware によって提供される CIM プロバイダを使用して表示されます。情報は、WSMAN プロトコルを使用して収集されます。

Embedded ESX サーバーのインベントリを開始する場合の前提条件は次のとおりです。

- 1 サーバーで WSMAN サービスが有効になっている
- 1 インベントリタスクで使用される接続プロファイルで WSMAN が有効になっている

---

## ESXi 設定

### CIM OEM プロバイダの有効化

ESXi サーバーから(Dell Management Console モニタで報告される)正常性情報を受信するには、CimOemProvidersEnabled 構成設定を有効にします(値 1 に設定)。そして、ESXi インストール後の初回時に管理エージェントを再起動します。

CIM OEM プロバイダを有効にするには、次の手順を実行します。

1. RCLI ツールを VMware ウェブサイト [vmware.com/go/remotecli/](http://vmware.com/go/remotecli/) からダウンロードしてインストールします。
2. リモートの Windows または Linux サーバーから次の VMware RCLI コマンドを実行します。

```
vicfg-advcfg.pl --server <IP アドレス> --username <user_name> --password <パスワード> --set 1 Misc.CimOemProvidersEnabled
```

- ESXi サーバーのダイレクトコンソールユーザーインターフェイス(DCUI)から管理エージェントを再起動するか、サーバーを再起動します。

 **メモ:** VI クライアント(Configuration(設定)→ Software(ソフトウェア)→ Advanced Settings(詳細設定)→ Misc(その他)→ Enable OEM Providers(OEM プロバイダの有効化))を使用して CimOemProvidersEnabled プロパティを設定することもできます。

## Dell Management Console 設定

### セキュアな導入モード - HTTPS を使用した WSMAN への接続

ESXi サーバーでセキュアモードで実行されている WS-MAN に接続するには、Dell Management Console で次の設定が必要です。

- Credential Manager を使用してWS-MAN 資格情報が作成されている。

ESXi サーバーのすべてに同じユーザー名およびパスワードが設定されている場合、必要な資格情報は 1 つだけです。

- WS-MAN プロトコルを使用する接続プロファイルが有効になっていて、次の設定が適用されている。

- 手順 1 で説明されているように資格情報が作成されている。
- セキュアなモードが選択されている。
- ESXi サーバーの HTTPS サービス向けに定義されたポート番号が Secure port(セキュアポート)テキストボックスに表示されている。デフォルトで、この値は 443 です。
- SSL 証明書ファイルが ESXi サーバーからダウンロードされた SSL 証明書(自己署名)をポイントしている。複数の SSL 証明書を Dell Management Console 接続プロファイルにインポートするには、本項の手順を参照してください。

 **メモ:** 複数の ESXi サーバーの(デフォルトでインストールされている)自己署名証明書が接続プロファイルにインポートされた 1 つの証明書を統合されていて、資格情報がすべての ESXi サーバー全体である場合、同じ接続プロファイルを使用して複数の ESXi サーバーを検出できます。

 **メモ:** 同じ資格情報を使用する ESXi サーバーでは、接続プロファイルの Trusted Site(信頼済みサイト)オプションを有効にすることで、1 つの接続プロファイルを使用して複数の ESXi サーバーを検出できます。ESXi 証明書を接続プロファイルにインポートする必要はありません。

すべての ESXi サーバーに同じ CA が生成した証明書がある場合、個別の証明書ではなくその CA 向けの証明書を Dell Management Console 接続プロファイルにインストールすれば十分です。

### 複数の SSL 証明書の Dell Management Console 接続プロファイルへのインポート手順

Dell Management Console では、接続プロファイルの一部として WS-MAN を(安全なモードで)設定する場合に、SSL 証明書をインポートできます。

HTTPS を介した WS-MAN を使用するデバイスを複数検出する必要がある場合、異なるサーバーから自己署名証明書(デフォルトでインストールされている)を含む 1 つのファイルを Dell Management Console 接続プロファイルにインポートできます。

複数の ESXi サーバーから取得した SSL 証明書を使用して複数の証明書を含むファイルを作成できます。そして、複数の証明書を含むファイルを接続プロファイルにインポートして、1 つの接続プロファイルを使用して複数の ESXi サーバーを検出できるようにします(前提:すべての ESXi サーバーの資格情報が同じ)。

次の手順では、(デフォルトでインストールされている)自己署名証明書について説明します。この手順は CA 署名証明書についても有効です。すべての ESXi サーバーに同じ CA が生成した証明書がある場合、CA 向けの証明書を Dell Management Console 接続プロファイルにインストールすれば十分なので、次の手順は省略できます。

#### 手順 1: VMware からのリモート CLI ツールのインストール

Windows コンピュータで VMware インフラストラクチャリモート CLI をダウンロードしてインストールします。

- インフラストラクチャリモート CLI ツールを VMware ウェブサイト [vmware.com/go/remotecli/](https://vmware.com/go/remotecli/) からダウンロードします。

このページの VMware インフラストラクチャリモート CLI のセクションにあるダウンロードリンクを探します。

- デフォルトの場所(たとえば、C:¥Program Files¥VMware¥VMware VI Remote CLI)にツールをインストールします。今後の手順では、デフォルトのインストールパスを仮定します。インストールパスを変更する場合は、次の手順でも適宜変更してください。
- コマンドウィンドウで次のコマンドを実行します。

```
Set path=%path%;"C:¥Program Files¥VMware¥VMware VI Remote CLI ¥Perl¥bin"
```

#### 手順 2: マルチ証明書ファイルの作成

- combinecerts.bat DOS バッチファイルを作成します。

2. 次のように combinecerts.bat ファイルを実行します。

```
combinecerts <ユーザー名> <パスワード> <サーバー IP リストファイル> <出力証明書ファイル> [create|append]
```

**ユーザー名:** ESXi サーバーにログインするために使用するユーザー名

**パスワード:** ユーザーのパスワード

**サーバー IP リストファイル:** 各行に 1 つの IP アドレスを含む ASCII ファイル(本書のサンプルファイルを参照してください)

**出力証明書ファイル:** すべての証明書を含めるファイルの名前

**create|append:**

**create:** スクリプトが新しい出力証明書ファイルを作成するようにします

**append:** スクリプトが新しい証明書を出力証明書ファイルに追加するようにします このパラメータが指定されていない場合、デフォルトは append です。

このバッチファイルを使用して、サーバー IP リストファイルにある 1 つの IP アドレスだけを指定して、create オプションを指定することで、ESXi サーバーから 1 つの証明書をインポートします。

## Combinecerts.bat DOS バッチファイル

次のテキストを combinecerts.bat というファイルにコピーします。

```
----- START OF DOS Batch File -----  
  
@echo off  
  
rem Usage: combinecerts <ユーザー> <パスワード> <サーバー IP リストファイル> <出力証明書ファイル> [create|append]  
  
rem (assuming same user and password for all servers)  
  
rem option "append" causes the script to append new certificates to the <出力証明書ファイル>.  
  
rem option "append" causes the script to append new certificates to the <出力証明書ファイル>.  
  
if "%5"=="create" (del /F /Q %4 2>NUL)  
  
for /f %%X in (%3) do (  
  
echo.  
  
echo.  
  
echo Importing certificate from server: %%X  
  
vifs.pl --server %%X --username %1 --password %2 --get /host/ssl_cert tmpcert.crt  
  
if not errorlevel 1 (type tmpcert.crt >> %4)  
  
del /F /Q tmpcert.crt 2>NUL  
  
)  
  
echo.  
  
----- END OF DOS Batch File -----
```

## Sample Servers IP list file Copy

```
----- START OF SAMPLE servers IP list file -----  
  
192.168.22.243  
192.168.11.45  
192.168.22.31  
192.168.22.65  
  
----- END OF SAMPLE "servers IP list file" -----
```

---

## 注意点

- 1 All Devices(すべてのデバイス)ツリーに表示されている仮想マシンを削除するには、まずグループにあるデバイスを削除してからグループを削除します。検出範囲にあるグループも削除します。削除しないと、検出サイクルのたびにグループが表示されます。
  - 1 仮想マシンの検出後にゲストを仮想マシンに追加すると、ゲストはホストに関連付けられません。ゲストをホストに関連付けるには、ホストを再検出します。
-

[目次に戻る](#)

[目次に戻る](#)

## インベントリの属性

Dell Management Console バージョン 2.0.2 ユーザーズガイド

この項では、Dell Management Console によるレポートの作成時に使用される属性を表示します。

表 B-1 サーバーおよび MD1000 ストレージのレポート用インベントリ属性

コンポーネント	属性
エージェント	AgentDescription
	AgentGlobalStatus
	AgentId
	AgentManufacturer
	AgentName
	AgentURL
	AgentVersion
コンタクト	ContactInformation
	ContactLocation
	ContactName
デバイス	DeviceAssetTag
	DeviceChassisServiceTag
	DeviceDescription
	DeviceLocation
	DeviceLocationInChassis
	DeviceManufacturer
	DeviceName
	DeviceSerialNumber
	DeviceServiceTag
	DeviceSystemId
	DeviceSystemModelType
ファームウェア	FirmwareChassisIndex
	FirmwareIndex
	FirmwareName
	FirmwareReleaseDate
	FirmwareType
FirmwareVersion	
ネットワーク	NICIPAddress
	NICMACAddress
	NICDescription
	NICManufacturer
	NICNetmask
	NICPingable
	NICTOECapable
	NICTOEEnable
BIOS	BIOSChassisIndex
	BIOSReleaseDate
	BIOSVersion
	BIOSName
	BIOSType
BIOSIndex	
オペレーティングシステム	OSTotalPhysicalMemory
	OSType
	OSRevision
	OSMajorVersion
	OSMinorVersion
	OSArchitecture
	OSVendor

	OSSPMajorVersion
	OSSPMinorVersion
メモリ	MemoryDeviceSize
	MemoryDeviceFormFactor
	MemoryDeviceManufacturerName
	MemoryDeviceSerialNumberName
	MemoryDeviceAssetTagName
	MemoryDeviceStatus
	MemoryDeviceType
	MemoryDevicePartNumberName
	MemoryDeviceFailureMode
	MemoryDeviceBankName
	MemoryDeviceIndex
	MemoryDeviceLocationName
	電源装置
PowerSupplyType	
PowerSupplyOutputWatts	
PowerSupplyStatus	
PowerSupplyState	
PowerSupplyRedundancyState	
PowerSupplyChassisIndex	
PowerSupplyIndex	
プロセッサ	ProcessorBrandName
	ProcessorFamily
	ProcessorSteppingName
	ProcessorCores
	ProcessorMaxSpeed
	ProcessorSlotNumber
	ProcessorStatus
	ProcessorCurrentSpeed
	ProcessorModelName
	ProcessorChassisIndex
FRU	FruIndex
	FruStatus
	FruState
	FruDeviceName
	FruManufacturer
	FruSerialNumber
	FruPartNumber
	FruRevision
	FruManufacturingDate
デバイスカード	DeviceCardAdapterSpeed
	DeviceCardManufacturer
	DeviceCardDescription
	DeviceCardSlotNumber
	DeviceCardDataBusWidth
	DeviceCardBusSpeed
DeviceCardSlotLength	
アレイディスク	ArrayDiskNumber
	ArrayDiskName
	ArrayDiskVendorName
	ArrayDiskState
	ArrayDiskStatus
	ArrayDiskModelNumber
	ArrayDiskSerialNumber
	ArrayDiskRevision
	ArrayDiskEnclosureId
	ArrayDiskChannel
	ArrayDiskLength

	ArrayDiskFreeSpace
	ArrayDiskUsedSpace
	ArrayDiskBusType
	ArrayDiskSpareState
	ArrayDiskTargetId
	ArrayDiskLUNId
	ArrayDiskPartNumber
コントローラ	ControllerNumber
	ControllerName
	ControllerVendor
	ControllerType
	ControllerState
	ControllerStatus
	ControllerFWVersion
	ControllerCacheSize
	ControllerPhysicalDeviceCount
	ControllerLogicalDeviceCount
	ControllerPartnerStatus
	ControllerMemorySize
	ControllerDriveChannelCount
	ControllerChargeCount
	ControllerDriverVersion
	ControllerPatrolReadState
エンクロージャ	EnclosureNumber
	EnclosureName
	EnclosureVendor
	EnclosureState
	EnclosureStatus
	EnclosureId
	EnclosureServiceTag
	EnclosureAssetTag
	EnclosureAssetName
	EnclosureProductId
	EnclosureType
	EnclosureChannelNumber
	EnclosureBackplanePartNum
	EnclosureSCSIId
	EnclosurePartNumber
	EnclosureSerialNumber
EMM	EMMNumber
	EMMName
	EMMRevision
	EMMVendor
	EMMState
	EMMPartNumber
	EMMFWVersion
	EMMStatus
仮想ディスク	VirtualDiskNumber
	VirtualDiskName
	VirtualDiskDeviceName
	VirtualDiskState
	VirtualDiskStatus
	VirtualDiskLength
	VirtualDiskWritePolicy
	VirtualDiskReadPolicy
	VirtualDiskCachePolicy
	VirtualDiskLayout
	VirtualDiskStripeSize
	VirtualDiskTargetId

所有者	PurchaseCost
	WayBillNumber
	InstallationDate
	PurchaseOrderNumber
	PurchaseDate
	SigningAuthorityName
	OriginalMachineConfigurationExpensed
	OriginalMachineConfigurationVendorName
	CostCenterInformationVendorName
	UserInformationUserName
	ExtendedWarrantyStartDate
	ExtendedWarrantyEndDate
	ExtendedWarrantyCost
	ExtendedWarrantyProviderName
	OwnershipCode
	CorporateOwnerName
	HazardousWasteCodeName
	DeploymentDurationUnitType
	TrainingName
	OutsourcingProblemDescription
	OutsourcingServiceFee
	OutsourcingSigningAuthority
	OutsourcingProviderFee
	OutsourcingProviderServiceLevel
	InsuranceCompanyName
	BoxAssetTagName
	BoxSystemName
	BoxCPUSerialNumberName
	DepreciationDuration
	DepreciationDurationUnitType
	DepreciationPercentage
	DepreciationMethod
	RegistrationRegistered

表 B-2 EMC および MD3000 ストレージのレポート用インベントリ属性

コンポーネント	属性
アレイディスク	ArrayDiskNumber
	ArrayDiskName
	ArrayDiskLength
	ArrayDiskBusType
	ArrayDiskLUNId
	ArrayDiskPartNumber
	ArrayDiskUserCapacity
	ArrayDiskVendorName
	ArrayDiskState
	ArrayDiskModelNumber
	ArrayDiskSerialNumber
	ArrayDiskRevision
	ArrayDiskChannel
	ArrayDiskEnclosureId
コントローラ	ControllerNumber
	ControllerName
	ControllerMemorySize
	ControllerDriveChannelCount
	ControllerChargeCount
	ControllerSPAReadCacheSize
	ControllerSPAWriteCacheSize

	ControllerSPBReadCacheSize
	ControllerSPBWriteCacheSize
	ControllerCachePageSize
	ControllerVendor
	ControllerSPAReadCachePolicy
	ControllerSPAWriteCachePolicy
	ControllerSPBReadCachePolicy
	ControllerSPBWriteCachePolicy
	ControllerFWVersion
	ControllerCacheSize
	ControllerPhysicalDeviceCount
	ControllerLogicalDeviceCount
	ControllerType
	ControllerNumberOfPorts
エンクロージャ	EnclosureNumber
	EnclosureName
	EnclosureType
	EnclosurePartNumber
	EnclosureSerialNumber
	EnclosureVendor
	EnclosureLocationOfManufacture
	EnclosureServiceTag
	EnclosureProductId
	EnclosureNumberOfFanPacks
	EnclosureNumberOfControllers
	EnclosureNumberOfDisks
	EnclosureId
	EnclosureAssetTag
ストレージグループ	StorageGroupIndex
	StorageGroupLUNId
	StorageGroupName
	StorageGroupHostName
仮想ディスク	VirtualDiskNumber
	VirtualDiskName
	VirtualDiskStripeSize
	VirtualDiskTargetId
	VirtualDiskStripeElementSize
	VirtualDiskLUNId
	VirtualDiskDeviceName
	VirtualDiskLength
	VirtualDiskWritePolicy
	VirtualDiskReadPolicy
VirtualDiskLayout	
ソフトウェアエージェント	SoftwareType
	SoftwareVersion
	SoftwareDescription

表 B-3 テープライブラリのレポート用インベントリ属性

コンポーネント	属性
コンタクト	ContactInformation
	ContactLocation
	ContactName
デバイス	DeviceAssetTag
	DeviceDescription
	DeviceManufacturer
	DeviceName
	DeviceSerialNumber

	DeviceServiceTag
	DeviceSystemModelType
ファームウェア	FirmwareName
	FirmwareVersion
ネットワーク	NICIPAddress
	NICMACAddress
	NICDescription
テープデバイス	TapeDriveCleaningRequired
	TapeDriveFirmwareVersion
	TapeDriveIndex
	TapeDriveModel
	TapeDriveMotionHrs
	TapeDriveSerialNumber
	TapeDriveType
	TapeDriveVendor
テープライブラリ	TapeLibraryFirmwareVersion
	TapeLibraryScsiId
	TapeLibrarySerialNumber
	TapeLibrarySlotCount
	TapeLibraryVendor
	TapeLibraryDriveCount
	TapeLibraryModel

表 B-4 FC およびイーサネットスイッチのレポート用インベントリ属性

コンポーネント	属性
コンタクト	ContactInformation
	ContactLocation
	ContactName
デバイス	DeviceAssetTag
	DeviceDescription
	DeviceManufacturer
	DeviceName
	DeviceSerialNumber
	DeviceServiceTag
	DeviceSystemModelType
ファームウェア	FirmwareName
	FirmwareVersion
ネットワーク	NICIPAddress
	NICMACAddress
	NICDescription

表 B-5 KVM のレポート用インベントリ属性

コンポーネント	属性
コンタクト	ContactInformation
	ContactLocation
	ContactName
デバイス	DeviceAssetTag
	DeviceDescription
	DeviceManufacturer
	DeviceName
	DeviceSerialNumber
	DeviceServiceTag
	DeviceSystemModelType
ファームウェア	FirmwareName
	FirmwareVersion
ネットワーク	NICIPAddress

	NICMACAddress
	NICDescription

表 B-6 DRAC のレポート用インベントリ属性

コンポーネント	属性
コンタクト	ContactInformation
	ContactLocation
	ContactName
デバイス	DeviceAssetTag
	DeviceDescription
	DeviceManufacturer
	DeviceName
	DeviceSerialNumber
	DeviceServiceTag
	DeviceSystemModelType
ファームウェア	FirmwareName
	FirmwareVersion
ネットワーク	NICIPAddress
	NICMACAddress
	NICDescription

表 B-7 CMC のレポート用インベントリ属性

コンポーネント	属性
コンタクト	ContactInformation
	ContactLocation
	ContactName
デバイス	DeviceAssetTag
	DeviceDescription
	DeviceManufacturer
	DeviceName
	DeviceSerialNumber
	DeviceServiceTag
	DeviceSystemModelType
ファームウェア	FirmwareName
	FirmwareVersion
ネットワーク	NICIPAddress
	NICMACAddress
	NICDescription

表 B-8 プリンタのレポート用インベントリ属性

コンポーネント	属性
プリンタサプライ	PrinterSupplyIndex
	PrinterSupplyDescription
	PrinterSupplyType
	PrinterSupplyLevel
	PrinterSupplyMaxLevel
プリンタの給紙トレイ	PrinterInputIndex
	PrinterInputName
	PrinterInputVendorName
	PrinterInputModel
	PrinterInputDescription

	PrinterInputMaxCapacity
プリンタの排紙トレイ	PrinterOutputIndex
	PrinterOutputName
	PrinterOutputVendorName
	PrinterOutputModel
	PrinterOutputDescription
	PrinterOutputMaxCapacity
プリンタカバーエントリー	PrinterCoverIndex
	PrinterCoverDescription
	PrinterCoverStatus
エージェント	AgentDescription
	AgentGlobalStatus
	AgentId
	AgentManufacturer
	AgentName
	AgentVersion
コンタクト	ContactInformation
	ContactLocation
	ContactName
デバイス	DeviceLocation
	DeviceSystemModelType
ファームウェア	FirmwareChassisIndex
	FirmwareIndex
	FirmwareName
	FirmwareReleaseDate
	FirmwareType
	FirmwareVersion
ネットワーク	NICIPAddress
	NICMACAddress
	NICDescription

表 B-9 電源のインベントリ属性

コンポーネント	属性
電源監視 (xx0x および xx1x サーバー向け)	PeakAmperage PeakPowerWatts PeakPowerBTUH PeakAmperageStartTime PeakAmperageTime PeakPowerStartTime PeakPowerTime
電力バジェット (xx0x および xx1x サーバー向け)	PeakHeadroomWatt IdlePowerWatt MaxPotentialPowerWatt CapValueWatt PeakHeadroomBTUhr IdlePowerBTUhr MaxPotentialPowerBTUhr CapValueBTUhr
電源プロファイル	ProfileSetting



[目次に戻る](#)

## Dell OpenManage IT Assistant の検出設定の移行

Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [IT Assistant の検出設定のインポート](#)
- [データベース移行のユーザーインターフェース](#)
- [IT Assistant の検出設定を移行する前の注意点](#)

Dell OpenManage IT Assistant を使用したことがない、または検出範囲を Dell Management Console に移行しない場合は、本項を省略してください。

IT Assistant を既にお使いの場合は、検出範囲を Dell Management Console に移行する方法を理解するために、本項をお読みください。

Dell Management Console では、IT Assistant 8.0 以降の検出設定情報を移行できます。

---

### IT Assistant の検出設定のインポート

次の検出設定を IT Assistant データベースから Dell Management Console に移行できます。

- 1 除外範囲
  - 1 包括範囲
  - 1 包括範囲に関連付けられているプロトコル情報:
    - SNMP:再試行、タイムアウト、および読み取りコミュニティストリング
-  **メモ:** Dell Management Console には書き込みコミュニティストリングがないため、書き込みコミュニティストリングは移行されません。
- ICMP:再試行とタイムアウト
  - Dell|EMC NaviCLI:ユーザー名とパスワード
  - IPMI:再試行、タイムアウト、ユーザー名、パスワード、および KG キー
  - CIM:ドメイン名、ユーザー名、およびパスワード。ドメイン名が設定されていない場合は、localhost が使用されます。
  - Dell PowerVault MD ストレージアレイプロトコルの有効 / 無効の情報
- 1 検出スケジュールの情報

---

### データベース移行のユーザーインターフェース

Home(ホーム)→ Dell Management Console Portal(Dell Management Console ポータル)をクリックして、データベース移行リンクにアクセスできます。Dell Enterprise Management Quick Start(Dell Enterprise Management クイックスタート)ウェブパーツの **Getting Started(スタートガイド)** タブで、**Migrate Dell OpenManage IT Assistant Discovery Settings(Dell OpenManage IT Assistant の検出設定の移行)** をクリックします。

---

### IT Assistant の検出設定を移行する前の注意点

- 1 Dell Management Console のデータベースに検出範囲を移行できるのは、IT Assistant 8.0 以降のみです。
  - 1 先に Dell Management Console 2.0 へ移行してから、Dell Management Console 2.0.2 にアップグレードする必要があります。
  - 1 データベースの移行プロセスを開始したら、その移行をキャンセルしたり、停止したりすることはできません。
  - 1 リモート IT Assistant データベースからやデータベースの名前付きインスタンスからデータを移行することもできます。ローカルシステムとリモートデータベースの間の接続が機能していることを確認してください。
  - 1 検出範囲を移行する前に、Dell Management Console システムへの負荷を低減するために、各検出タスクに使用されるスレッドの数を減らすことができます。デフォルト値の 40 を変更するには、**Settings(設定)**→ **All Settings(すべての設定)** に移動します。右ペインの **Settings(設定)**→ **Discovery and Inventory(検出とインベントリ)**→ **Network Discovery Settings(ネットワーク検出設定)** で、デフォルト値を変更します。
- 移行後、ネットワーク検出設定を変更するときは、各検出タスクを選択して編集する必要があります。詳細については、[検出のパフォーマンス](#)を参照してください。

### リモートデータベース

リモートデータベースを指定する場合は、ローカルシステムとリモートデータベースの間の接続が機能していることを確認します。リモートデータベース接続を有効にするには、[SQL Server 2005 または 2008 Express へのリモート接続の有効化](#)を参照してください。IT Assistant データベースの場所と認証モードを設定します。

- 1 Microsoft Windows 認証 - ユーザー名とパスワードを IT Assistant と Dell Management Console の間で同じにします。
- 1 Mixed/SQL 認証 - IT Assistant データベースの管理者 SQL ログイン資格情報を入力します。入力した SQL ログイン資格情報は、有効にされ、リモートデータベースに対して適切なサニパーロールとユーザーマッピングが設定されている必要があります。

IT Assistant は、データベースを Windows 認証モードでのみ作成します。SQL 認証を使用するには、認証モードを変更します。詳細については、[SQL Server 認証と Windows 認証の有効化](#)を参照してください。

IT Assistant は、リモートデータベースのデフォルトインスタンスをサポートしています。IT Assistant のデータベースを名前付きインスタンスで設定している場合は、名前付きインスタンスをサーバー名とともに指定します(たとえば、MyServer/NamedInstance)。

## SQL Server 2005 または 2008 Express へのリモート接続の有効化

デフォルトでは、SQL Server はリモートデータベースに自動接続しません。手動で接続を有効にする必要があります。Microsoft Windows の ODBC Data Source Administrator ツールを使用して、リモートデータベースの接続を確認します。最初にリモート接続を有効にせずにリモート SQL Server へ接続すると、エラーが表示されます。

このエラーを解決するには、次の作業を実行します。

1. SQL Server 上で SQL Server と Windows の両方の認証モードを有効にします。
1. TCP/IP プロトコルを使用してリモート接続を有効にします。

## SQL Server 認証と Windows 認証の有効化

SQL Server 認証と Windows 認証を有効にするには、次の手順を実行します。

1. ローカル SQL Server 上で SQL Server Management Studio Express を使用して、Windows 認証ユーザー資格情報で SQL Server にログインします。SQL Server への認証には、Windows アカウントが使用されます。
2. Object Explorer (オブジェクトエクスプローラ)で、インスタンス名を右クリックし、Properties (プロパティ)を選択します。
3. 左ペインで、Security (セキュリティ)を選択し、サーバー認証を SQL Server and Windows Authentication mode (SQL Server 認証モードと Windows 認証モード)に変更します。
4. 変更を反映するために、インスタンス名を再度右クリックし、Restart (再起動)を選択して SQL Server サービスを再起動します。

## リモート接続の有効化

リモート接続を有効にするには、次の手順を実行します。

1. SQL Server Surface Area Configuration を開きます。
2. Surface Area Configuration for Services and Connections (サービスと接続の SQL Server Surface Area Configuration)を選択します。
3. 左ペインで、SQL Server インスタンス → Database Engine (データベースエンジン) → Remote Connections (リモート接続)と展開します。
4. 右側で、Local and remote connections (ローカル接続およびリモート接続) → Using both TCP/IP and named pipes (TCP/IP および名前付きパイプを使用する)を選択します。
5. 左側で、SQL Server Browser (SQL Server ブラウザ) → Service (サービス)を選択します。
6. 右側で、スタートアップの種類が Disable (無効化)の場合、Automatic (自動)に変更し、Apply (適用)をクリックします。
7. Start (開始)をクリックしてサービスを起動し、OK をクリックします。
8. SQL Server 認証モードを使用してリモートシステムから SQL Server にログインします。

## IT Assistant 8.x からの検出情報の移行

1. Dell Management Console をインストールします。
2. Dell Management Console を起動します。
3. Home (ホーム) → Dell Management Console Portal (Dell Management Console ポータル)をクリックします。
4. Dell Enterprise Management Quick Start (Dell Enterprise Management クイックスタート)ウェブページの Getting Started (はじめに)タブで、Migrate Dell OpenManage IT Assistant Discovery Settings (Dell OpenManage IT Assistant の検出設定の移行)をクリックします。

IT Assistant Discovery Settings Migration (IT Assistant の検出設定の移行)ページが表示されます。

5. **Discovery Settings Migration** (検出設定の移行) ウェブパーツで、**Launch Migration Wizard** (移行ウィザードの起動) をクリックします。
6. ウィザードの最初のページでは、IT Assistant データベースへ接続するために必要なパラメータを入力します。  
ローカルの、またはリモートに設定された IT Assistant データベースを指定できます。  
IT Assistant がデータベースの名前付きインスタンス上に設定されている場合は、その情報を **Database Server Name** (データベースサーバー名) に指定します。  
たとえば、`MyITAssistant¥MyNamedInstance` を指定します。  
必要な認証モードを選択します。  
**Next** (次へ) をクリックします。
7. 2 番目のページには、前のペインで指定した IT Assistant データベースから取得された検出範囲が表示されます。  
**Include Range** (包括範囲) リストボックスに、IT Assistant から取得されたすべての有効な包括範囲が表示されます。  
 **メモ:** サブ範囲が包括範囲内で無効になっている場合、サブ範囲は Dell Management Console へ移行されません。  
**Exclude Range** (除外範囲) リストボックスに、IT Assistant から取得されたすべての除外範囲が表示されます。  
詳細情報 (プロトコルおよび関連する設定) を表示するには、**Include Range** (包括範囲) リストボックスから各包括範囲を選択します。  
**Next** (次へ) をクリックします。
8. ウィザードの 3 番目のページには、IT Assistant の移行スケジュールの情報が表示されます。  
ただし、移行タスクをすぐに実行する場合は、**Now** (今すぐ) を選択し、**Next** (次へ) をクリックします。
9. ウィザードの最後のページは、情報のみのペインです。  
**Finish** (完了) をクリックして移行を開始します。

## Dell Management Console に移行されたデータの表示

Dell Management Console に移行されたデータを表示するには、次の手順を実行します。

1. **Home** (ホーム) → **Discovery and Inventory** (検出とインベントリ) → **Network Discovery** (ネットワーク検出) をクリックします。
2. **Network Discovery Task Management** (ネットワーク検出タスク管理) ウェブパーツの **Available Tasks** (使用可能なタスク) タブで、移行されたさまざまなスキャングループ (検出タスク) を表示できます。  
移行された検出タスクは、**IT Assistant Migrated Discovery Task - <include range>** (IT Assistant から移行された検出タスク - <包括範囲>) として表示されます。  
**Task Runs** (タスクの実行) タブで、検出タスクの状態を表示できます。
3. 移行された検出タスクのプロトコルを表示するには、**Settings** (設定) → **All Settings** (すべての設定) → **Monitoring and Alerting** (監視と警告) → **Credential Settings** (資格情報の設定) → **Credentials Management** (資格情報管理) に移動します。  
移行された検出タスクの接続プロファイルを表示するには、**Settings** (設定) → **All Settings** (すべての設定) → **Monitoring and Alerting** (監視と警告) → **Protocol Management** (プロトコル管理) → **Connection profiles** (接続プロファイル) → **Manage Connection Profiles** (接続プロファイルの管理) に移動します。  
詳細については、[検出タスクの実行](#) および [インベントリタスクの結果の表示](#) を参照してください。

---

[目次に戻る](#)

[目次に戻る](#)

## 検出とインベントリ設定の設定

Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [検出ユーザーインターフェース](#)
- [検出設定を設定する前に](#)
- [接続プロファイルと資格情報管理](#)
- [検出タスクの作成](#)
- [新規組織ビューと組織グループの作成](#)
- [インベントリ設定の設定](#)

Dell Management Console では、デバイスの検出とインベントリ、ユーザーへの警告、ドライバ、BIOS、およびファームウェアのアップデートに加え、企業内の各システムにさまざまなタスクを実行することができます。管理対象システムには、サーバー、プリンタ、テープデバイス、ストレージデバイス、リモートアクセスカード搭載システム、Dell PowerConnect スイッチ、ラックが多いシステムで使用されるデジタルキーボード / ビデオ / マウス (KVM) スイッチなどが含まれます。

本項では、中小企業 (サーバー 50 台、クライアントシステム 200 台以上、スイッチ 10 台) のシステム管理者がどのように Dell Management Console の検出およびインベントリソリューションを使用できるかについて説明します。

このシナリオでは、ネットワーク環境の管理を担当する管理者が Dell Management Console を設定する方法を示します。

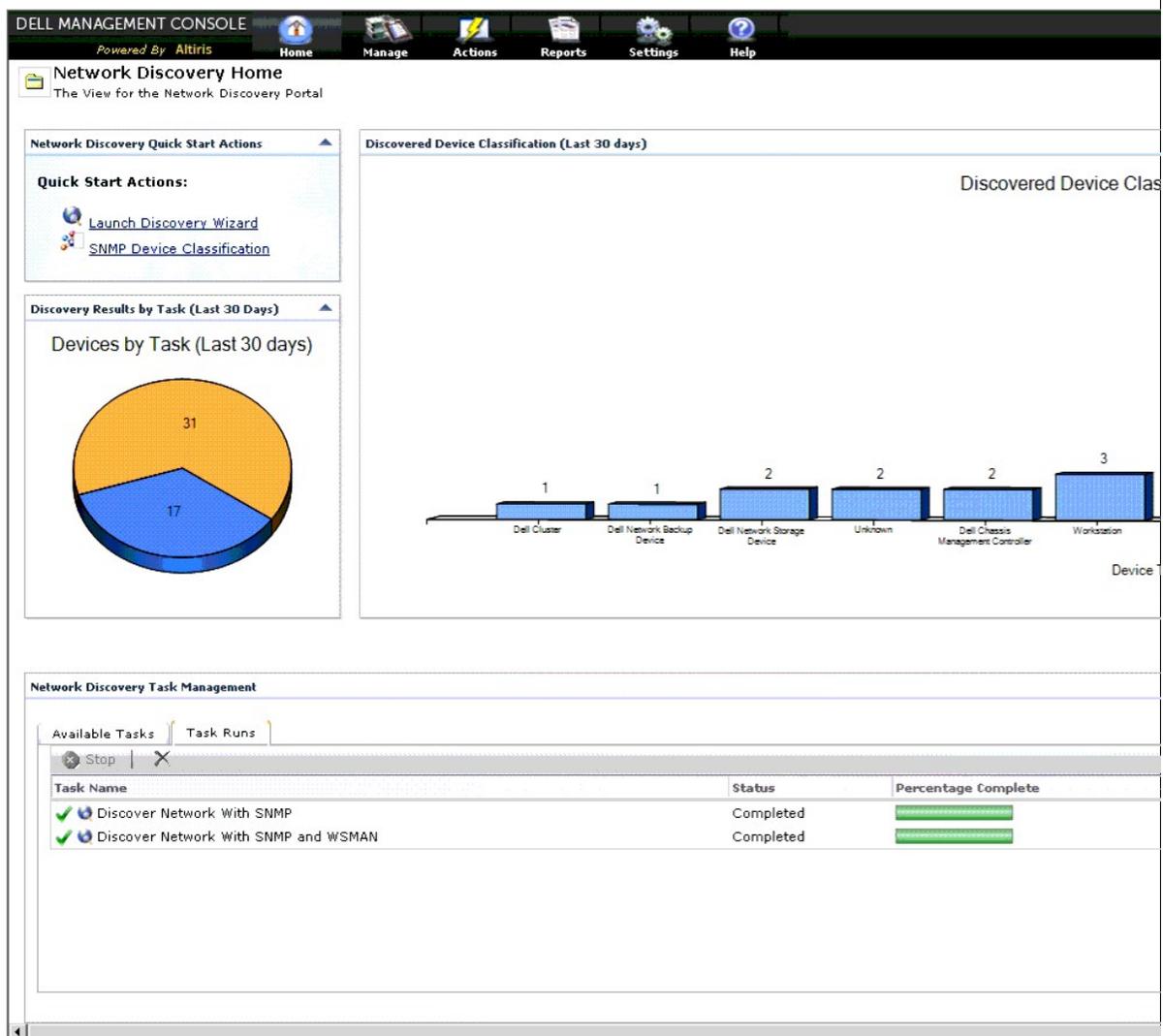
 **メモ:** これらのシナリオは、Dell Management Console の全機能を説明するものではありません。

---

## 検出ユーザーインターフェース

検出ポータルにアクセスするには、Home (ホーム) → **Discovery and Inventory** (検出とインベントリ) → **Network Discovery** (ネットワーク検出) の順にクリックします。

## 検出ユーザーインターフェースについて



Network Discovery Quick Start Actions (ネットワーク検出クイックスタートアクション) ウェブパーツは、ネットワークデバイスの検出設定を開始するのに適しています。

Network Discovery Task Management (ネットワーク検出タスク管理) ウェブパーツには、使用可能な検出タスクと実行されたタスクが表示されます。

Discovery Results by Tasks (タスク別の検出結果) ウェブパーツには、実行したタスクと、タスクによって検出されたデバイスの数が表示されます。

Discovered Device Classification (検出されたデバイスの分類) ウェブパーツには、検出された各種のデバイスが表示されます。たとえば、サーバー、プリンタ、テープ、スイッチなどです。

## 検出設定を設定する前に

Dell Management Console を使用して検出を設定する前に、ネットワークに基づいた基本的な決定を行う必要があります。特に、次について決定する必要があります。

- 1 検出するシステムのホスト名、IP アドレス、または IP サブネット範囲
- 1 デバイスと通信するために必要な資格情報 たとえば、WMI プロトコルを使用して Microsoft Windows システムを検出する場合は、Windows の資格情報を Dell Management Console に入力する必要があります。[資格情報の管理](#)を参照してください。
- 1 ネットワーク上のシステムとデバイス管理に必要なシステム管理プロトコル。表 6-1 にクイックレファレンスを示します。

プロトコルを管理するには、デバイスがサポートするシステム管理プロトコルに従って接続プロファイルを作成する必要があります。詳細については、[接続プロファイル](#)を参照してください。

## 接続プロファイルと資格情報管理

Credential Manager を使用すると、さまざまなプロトコルを介した接続に使用される機密データ、すなわち資格情報を暗号化し、保存することができます。

接続プロファイルとは、プロトコルとそれに対応する資格情報のセットのことで、論理的なセットとして設定、保存できます。このセットは、定義されているプロトコルを使用する際の参照として、検出、インベントリ、および監視ソリューションによって使用されます。

Dell Management Console では、デバイスとの通信に接続プロファイルが使用されます。認証が必要なデバイスを確認し、それらの資格情報のリストを準備しておきます。その後で、これらのデバイスの接続プロファイルを作成します。たとえば、ネットワーク上の 10 台のサーバーに個別の認証資格情報がある場合は、各システム用に個別の接続プロファイルを作成する必要があります。

## 資格情報の管理

Dell|EMC ストレージデバイスをネットワークに追加し、これらのデバイスを検出するには、検出ソリューションが Dell|EMC デバイスと通信するための資格情報を入力します。

1. Dell Management Console で、**Settings** (設定) → **All Settings** (すべての設定) の順にクリックします。
2. 左ペインで、**Settings** (設定) → **Monitoring and Alerting** (監視と警告) → **Credential Settings** (資格情報の設定) フォルダから **Credentials Management** (資格情報管理) を選択します。
3. 右ペインで、**Add Credentials** (資格情報の追加) をクリックします。
4. **Add Credentials** (資格情報の追加) ダイアログボックスで、**Credential Type** (資格情報タイプ) として **EMC Credentials** (EMC 資格情報) を選択します。
5. この資格情報の **Name** (名前) を入力します (例: emc-cred)。

Dell|EMC デバイスの **Username** (ユーザー名) と **Password** (パスワード) を入力し、**OK** をクリックします。

新しい資格情報が **Credential Management** (資格情報管理) ページに表示されます。

## 接続プロファイル

Dell Management Console では、デフォルトの接続プロファイルが提供されています。このプロファイルでは次のプロトコルが有効になっています。

- 1 HTTP
- 1 ICMP
- 1 SNMP V1 V2
- 1 SNMP Trap Sender
- 1 WMI

デフォルトの接続プロファイルをテンプレートとして参照し、ネットワークデバイスの検出に使用するプロトコルを含む新しい接続プロファイルを作成します。

## デフォルトの接続プロファイルの表示

デフォルトの接続プロファイルを表示するには、次の手順を実行します。

1. **Settings** (設定) → **All Settings** (すべての設定) の順にクリックします。
2. 左ペインで、**Settings** (設定) フォルダ → **Monitoring and Alerting** (監視と警告) → **Protocol Management** (プロトコル管理) → **Connection Profiles** (接続プロファイル) → **Manage Connection Profiles** (接続プロファイルの管理) の順に選択します。

デフォルトの接続プロファイルを編集してプロトコルを追加または削除します。

 **メモ:** デフォルトの接続プロファイルがすでに存在する場合でも、各プロトコル用に適切な資格情報を設定する必要があります。

## デフォルトの接続プロファイルの編集

**Default Connection Profile** (デフォルトの接続プロファイル) を編集するか、**Add Settings** (設定の追加) をクリックして新しい接続プロファイルを追加することができます。

1. **Manage Connection Profile** (接続プロファイルの管理) ページで、**Default Connection Profile** (デフォルトの接続プロファイル) を選択し、鉛筆アイコンの **edit** (編集) をクリックします。  
**Define Group Settings** (グループ設定の定義) ページに、デフォルトプロファイルに事前設定されているプロトコルが表示されます。
2. **Define Group Settings** (グループ設定の定義) ページで、**On** (オン) を選択して **IPMI** を有効にします。
3. 上矢印をクリックして、管理対象デバイスまたはデバイスグループの **IPMI** 資格情報を追加します。

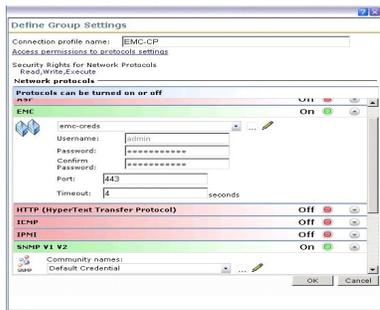
**メモ:** IPMI を正しく動作させるためには、管理対象デバイスの KG キーを入力する必要があります。デバイスの IPMI 資格情報プロフィールに KG キーを入力します。詳細については、[資格情報の管理](#)を参照してください。

- ネットワークデバイスで使用されない場合、他のプロトコル(HTTP、ICMP、SNMP Trap Sender など)は無効にします。  
多数のプロトコルがあるとデバイスの検出速度が低下するため、ネットワークの検出に不要なプロトコルは無効にすることを強くお勧めします。
- OK をクリックします。

## 新しい接続プロフィールの作成

ネットワークに Dell|EMC デバイスを追加する場合、デフォルトの接続プロフィールでは必要なシステム管理プロトコルが有効になっていないため、デフォルトの接続プロフィールは使用できません。EMC と SNMP が有効になっている新しい接続プロフィールを作成する必要があります (各種デバイスで必要とされる接続プロフィールについては、[表 6-1](#) を参照してください)。

- [デフォルトの接続プロフィールの表示](#)を参照してください。
- Manage Connection Profiles (接続プロフィールの管理) ページで、Add Settings (設定の追加) をクリックします。
- Define Group Settings (グループ設定の定義) ペインで、EMC プロトコルをオンにし、下矢印をクリックして EMC 資格情報を設定します。



- 接続プロフィール名 (例: EMC\_SNMP) を入力します。
- ドロップダウンリストから emc-cred を選択します ([資格情報の管理](#)を参照)。  
Dell Management Console は emc-cred の情報を取得してすべてのフィールドにデータを投入します。
- SNMP V1 V2 プロトコルを選択してオンにし、下矢印をクリックして SNMP 資格情報を設定してから OK をクリックします。

新しい接続プロフィールが Manage Connection Profiles (接続プロフィールの管理) ページに表示されます。

**表 6-1. 各種デバイスで必要とされるプロトコルと接続プロフィール**

デバイス	サポートされているシステム管理プロトコル	接続プロフィール用のプロトコル
対応 Microsoft Windows オペレーティングシステムを実行しているサーバー	SNMP、WMI、および IPMI	SNMP、WMI、または IPMI、あるいはこれらの組み合わせ
対応 Linux オペレーティングシステムを実行しているサーバー LINUX オペレーティングシステム	SNMP および IPMI	SNMP、または IPMI、あるいはこれらの組み合わせ
Dell PowerVault ストレージシステム	MD アレイ	MD アレイ
Dell PowerConnect スイッチ	SNMP	SNMP
テープ	SNMP	SNMP
プリンタ	SNMP	SNMP
Dell EMC	SNMP および Navisphere Secure CLI	SNMP および EMC
Remote Access Controller	SNMP	SNMP
デジタル KVM	SNMP	SNMP
Lifecycle Controller を実行しているサーバー	Web Services for Management (WS-MAN)	WS-MAN
Dell EqualLogic	SNMP	SNMP

## 検出タスクの作成

1. Home(ホーム) → Discovery and Inventory(検出とインベントリ) → Network Discovery(ネットワーク検出)の順にクリックします。
2. Network Discovery Home(ネットワーク検出のホーム)ページの Network Discovery Quick Start Actions(ネットワーク検出クイックスタートアクション)ウェブパーツで、Launch Discovery Wizard(検出ウィザードの起動)をクリックします。

Discover network devices(ネットワークデバイスの検出)ページが表示されます。

 **メモ:** Network Discovery Home(ネットワーク検出のホーム)ページの Available Tasks(使用可能なタスク)タブで、New(新規)をクリックして検出タスクを作成します。

3. 手順 1: Choose method of device discovery(デバイス検出方法の選択)で、Targeted network scan(ターゲットとなるネットワークのスキャン)を選択し、Next(次へ)をクリックします。

 **メモ:** ARP を選択した場合は、SNMP リクエストを受け入れるように設定されたルータの IP アドレスを入力します。

4. 手順 2: Enter network IP Ranges(ネットワーク IP 範囲の入力)で、Include(含める) → Custom Range(カスタム範囲)の順にクリックします。

カスタム範囲は、さまざまなサブネットを同時に定義するために使用されます。たとえば、サブネットマスクが 255.255.255.0 のカスタム範囲 10.94.\*.\* では、10.94.1.1 から 10.94.255.254 までの IP アドレスをスキャンします。

カスタム範囲が広くなるとデバイスの検出に非常に長い時間がかかるため、カスタム範囲の使用には注意が必要です。

5. Custom Range(カスタム範囲)ダイアログボックスで、次の情報を入力し、Next(次へ)をクリックします。

Custom range(カスタム範囲): 10.94.168.\*

Mask(マスク): 255.255.255.0

6. 手順 3: Select device communication protocol(デバイス通信プロトコルの選択)で、Default Connection Profile(デフォルトの接続プロファイル)を選択します。このプロファイルでは HTTP、ICMP、SNMP、WMI などのプロトコルが選択されています。

7. IPMI プロトコルを含めるように Default Connection Profile(デフォルトの接続プロファイル)を編集し、Next(次へ)をクリックします。

[デフォルトの接続プロファイルの編集](#)を参照してください。

8. 手順 4: Enter task name(タスク名の入力)で、Task name(タスク名)として Discover\_All と入力し、Next(次へ)をクリックします。

9. 手順 5: Choose when to run the discovery(検出実行時の選択)で、タスクのスケジュールを選択します。

要件に応じて、たとえば週に 1 回のようにネットワーク上のデバイスの検出をスケジュールします。

スケジュールを週に 1 回実行するには、次の手順を実行します。

Schedule(スケジュール): Shared Schedule(共有スケジュール)

Select Shared Schedule(共有スケジュールの選択): Weekly(毎週)

New(新規)をクリックします。

10. Create New Shared Schedule(新しい共有スケジュールの作成)ページで、スケジュールの名前と説明を入力します。

Add schedule(スケジュールの追加) → Scheduled Time(スケジュール時刻)の順に選択し、検索タスクの開始時刻として 0600 時を選択します。

No repeat(繰り返しなし)をクリックし、Repeat Schedule(繰り返しスケジュール)画面で Week(週単位)と Monday(月曜日)を選択します。

OK をクリックします。

11. Discover network devices(ネットワークデバイスの検出)ページで Finish(完了)をクリックします。

Discover\_All タスクが、Server Tasks(サーバータスク) → Network Tasks(ネットワークタスク)フォルダの下の Task Management Portal(タスク管理ポータル)に表示されません。

 **メモ:** 異なる認証資格情報を持つすべてのデバイスまたはデバイスのグループには、新しい接続プロファイルが必要になります。そのようなデバイスまたはデバイスグループには、それぞれ個別の検出タスクを作成し、適切な接続プロファイルにマップする必要があります。

## 検出タスクの実行

検出タスクを作成したら、Discover\_All タスクを実行できます。

1. Home(ホーム)→ Discovery and Inventory(検出とインベントリ)→ Network Discovery(ネットワーク検出)の順にクリックします。

Network Discovery Home(ネットワーク検出のホーム)ページが表示されます。

2. Network Discovery Task Management(ネットワーク検出タスク管理)ウェブパーツで、Available Tasks(使用可能なタスク)タブを選択します。
3. Discover\_All タスクを選択し、Run Now...(今すぐ実行...)をクリックします。

Dell OpenManage IT Assistant から移行された検出タスクも実行することができます。

検出タスクの移行の詳細については、[IT Assistant 8.x からの検出情報の移行](#)を参照してください。

デバイスの詳細を表示するには、ネットワークデバイスの検出後、インベントリタスクを作成し、実行します。詳細については、[すべてのシステムのインベントリを収集するためのインベントリタスクの作成](#)を参照してください。

## 検出されたデバイスの表示

検出タスクでメンバーを検出するには、検出するアドレスのリストに各クラスタメンバーの IP アドレスを含めます。

高可用性クラスタを検出すると、クラスタ名によってアクティブクラスタノードの名前が置き換えられることがあります。これを回避するには、検出範囲にクラスタ IP アドレスを含めないでください。

クラスタ IP アドレスが高可用性クラスタに関連する検出タスクに含まれる唯一の IP アドレスである場合は、現在のアクティブクラスタノードが検出され、その名前はクラスタの名前と同じになります。その結果、All Devices(すべてのデバイス)組織ビューの下の複数の場所にクラスタ名が表示されます。

- 1 高可用性クラスタの下に高可用性クラスタとして表示
- 1 クラスタの組織グループが選択された場合、リソースペインに、検出されたシステムとして表示
- 1 サーバーの組織グループが選択された場合、リソースペインに、検出されたシステムとして表示

モジュラーシャーシサーバーを検出すると 2 つのエントリが作成されます。1 つは Modular Servers(モジュラーサーバー)の下のシャーシサーバスタググループで、もう 1 つはこのグループの下にグループ化されたサーバーです。これらの 2 つのエントリを削除しても、Discovered Device Classification(検出されたデバイスの分類)棒グラフではモジュラーシャーシのエントリを引き続き使用できます。

Discovered Device Classification(検出されたデバイスの分類)棒グラフからモジュラーシャーシのエントリを削除するには、モジュラーシャーシの検出に使用される検出タスクを削除します。

モジュラーシャーシのエントリを削除するには、Dell Management Console で、Home(ホーム)→ Discovery and Inventory(検出とインベントリ)→ Network Discovery(ネットワーク検出)→ Available Task(使用可能なタスク)の順に選択し、モジュラーシャーシの検出に使用される検出タスクを削除します。

ただし、モジュラーシャーシサーバーを再検出しても、Discovered Device Classification(検出されたデバイスの分類)棒グラフの下にモジュラーシャーシのエントリはありません。

検出されたネットワークデバイスを表示するには、次の手順を実行します。

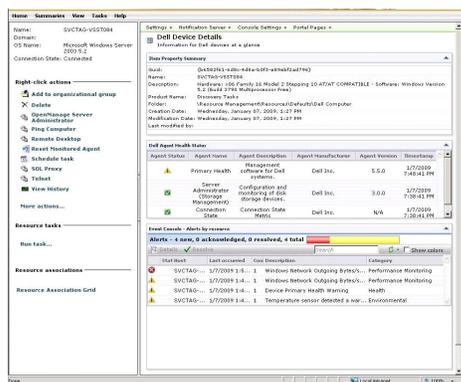
1. Manage(管理)→ All Devices(すべてのデバイス)の順にクリックします。
2. 左ペインで、サーバーを選択して、検出されたシステムを表示します。

Dell OpenManage Server Administrator がインストールされているサーバーはすべて、Resource Type(リソースタイプ) = Dell Computer(Dell コンピュータ)として検出されます。

他のリソースタイプの詳細については、[表 5-1](#)を参照してください。

3. システムを選択し、ダブルクリックして詳細を表示します。

このシステムの Resource Manager(リソースマネージャ)ページが表示されます。



 **メモ:** 検出されたデバイスの正常性が normal (正常) の場合、**Dell Agent Health Status** (Dell エージェントの正常性状態) ウェブパーツにプライマリ正常性メトリックが表示されるまで少し時間がかかります。正常性メトリックの詳細については、[表 11-9](#) を参照してください。

## 注意事項

1. **All Devices** (すべてのデバイス) ツリーに表示されている仮想マシン、モジュラーシステム、またはクラスタを削除する必要がある場合は、まずグループのデバイスを削除してからグループを削除します。検出範囲からもグループを削除します。そうしない場合は、検出サイクルごとにグループが表示されます。

## リソースマネージャ

**Resource Manager** (リソースマネージャ) ページには、画面の右ペインに 2 つのウェブパーツがあります。

**Item Property Summary** (項目のプロパティのサマリ) ウェブパーツには、検出されたデバイスの一般情報が含まれています。

**Dell Agent Health Status** (Dell エージェントの正常性状態) ウェブパーツには、デバイスに関連付けられているすべてのエージェントが表示されます。このウェブパーツは、Server Administrator、Storage Management、Remote Access Controller などの管理エージェントの状態を提供します。この情報は SNMP または WMI プロトコルを使用して取得されます。

エージェントの正常性状態は、監視ソリューションによって生成されたイベントによって決定されます。詳細については、[監視と警告](#) を参照してください。検出後、リソースマネージャには検出されたエージェントの状態が表示されます。監視ソリューションが 1 つ、または複数の管理対象エージェントから発信される警告を開始すると、エージェントの状態は Critical (重要)、Warning (警告)、または Undetermined (不明) に変更されます。

 **メモ:** すべてのエージェントがすべてのデバイスで使用できるとは限りません。たとえば、Storage Management Service Remote Access Controller がシステムにインストールされていない場合、これらのコンポーネントに関するエージェント情報は表示されません。エージェントがないということは、適切なソフトウェアがインストールされていないか、ハードウェアが適切に有効化されていないことを示します。

また、デバイスタイプが異なれば、表示されるエージェントも異なります。

エージェントの状態は、監視されているデバイスに関して受信した正常性タイプの警告に直接関連しています。たとえば、デバイスの Primary Health (基本正常性) が警告または重要と表示された場合は、対応する正常性警告が **Event Console** (イベントコンソール) ウェブパーツに表示されます。

イベントコンソールを使用すれば、システム、ソフトウェア、プリンタ、およびその他のデバイスを監視するために個別のツールを維持する必要性を減らすことができます。イベントコンソールは SNMP トラップとその他の状態メッセージを収集し、それらを 1 つの場所に表示します。すべての状態メッセージは共通のフォーマットに変換され、このフォーマットによって、Dell Management Console データベース内の影響を受けるリソースに各受信メッセージがリンクされます。これらのフォーマットされたメッセージは、警告と呼ばれます。

イベントコンソールでは、FC スイッチ、イーサネットスイッチ、または EMC アレイからトラップが生成されると、デバイスの IP アドレスが表示されます。ただし、そのデバイスが Dell Management Console で検出済みの場合でも、デバイスの名前は表示されません。

イベントコンソールは、次の方法で警告を処理できるルールベースのトリガーシステムも提供します。

1. 特定の警告に対応してタスクサーバーのタスクを起動する。

一部のデバイスで検出の起動タスクが使用可能な場合:

1. 特定の警告が警告データベースに保存されないようにする。
1. 別の管理システムに警告を転送する。

イベントコンソールの詳細については、[Help](#) (ヘルプ) → [Context](#) (コンテキスト) から Symantec のマニュアルを参照してください。

**Resource Manager** (リソースマネージャ) 画面の左側で、デバイスに関する基本情報とデバイスの接続状況を確認できます。接続状況には、デバイスがオンラインかどうかが表示されます。

**Right-click actions** (右クリックアクション) のセクションでは、デバイス上で実行できるアクションのセットが表示されます。このアクションのリストはコンテキスト依存で、表示されるアクションは、調べているデバイスのタイプ (システム、帯域外デバイス、プリンタなど) によって異なります。

イベントコンソールでは、複数回受け取ったイベントに対して感嘆符が表示されます。これは以前のリリースとは異なる表示で、繰り返し受信され、即時のアクションが必要な警告をより良く表示するために追加されました。

**Monitor portal** (監視ポータル) ページで **Monitored Resources By Status** (状態別監視対象リソース) ウェブパーツからイベントコンソールを開いた場合、監視ソリューションに関連した警告だけが表示されます。すべての SNMP 警告を表示するには、[Manage Event Console](#) (イベントコンソールの管理) リンクを選択します。

Dell Management Console、イベントコンソールに同じイベントが一定の順序および間隔で送信された場合、イベントのソース、重要度、およびカテゴリが同じでも、イベントカウントが更新されるかわりに複数回表示される場合があります。

## 検出ログ

検出ログでは、検出タスクの状態を確認することができます。ログは、検出の問題のトラブルシューティングを行う際に役立つデータを提供します。デフォルトでは、Dell Management Console はログエントリを保存しません。

検出ログを有効にするには、次の手順を実行します。

 **メモ:** 多数のデバイスを検出する場合、検出ログを有効にすると Dell Management Console のパフォーマンスに影響を及ぼす可能性があります。

1. **Settings** (設定) → **All Settings** (すべての設定) の順にクリックします。
2. 左ペインで、**Discovery and Inventory** (検出とインベントリ) フォルダ → **Discovery Log Settings** (検出ログの設定) と選択します。
3. 右ペインで、**Change Settings** (設定の変更) をクリックします。

4. **Enable discovery logging** (検出ログを有効にする) を選択し、検出ログの保存場所へのパスを入力して **Save Settings** (設定の保存) をクリックします。
5. ブラウザウィンドウを閉じ、Altiris Object Host Service を再起動します。

## 検出のパフォーマンス

Dell Management Console の検出タスクのパフォーマンスを管理するために、検出タスクを作成する前に各検出タスクに必要なスレッド数を設定することができます。

1. **Settings** (設定) → **All Settings** (すべての設定) の順にクリックします。
2. 右ペインで、**Settings** (設定) → **Discovery and Inventory** (検出とインベントリ) → **Network Discovery Settings** (ネットワーク検出設定) の順にクリックします。
3. 右ペインで、**Maximum number of threads per discovery task** (検出タスクごとの最大スレッド数) を変更します。  
この値は、作成したすべての検出タスクに適用されます。

検出タスクの作成後にデフォルト値を変更するには、次の手順を実行します。

1. **Home** (ホーム) → **Discovery and Inventory** (検出とインベントリ) → **Network Discovery** (ネットワーク検出) の順にクリックします。  
**Network Discovery Home** (ネットワーク検出のホーム) ページが表示されます。
2. **Network Discovery Task Management** (ネットワーク検出タスク管理) ウェブパーツの **Available Tasks** (使用可能なタスク) タブで、スレッド数を変更するタスクを選択します。  
鉛筆アイコンの **edit** (編集) ボタンをクリックします。
3. **Edit Discovery Task** (検出タスクの編集) ペインで、**Advanced** (詳細設定) をクリックします。
4. **Maximum number of threads per discovery task** (検出タスクごとの最大スレッド数) を変更して **OK** をクリックします。

## 警告開始検出

警告開始検出を使用すると、Dell Management Console によって管理されないデバイスを、警告またはトラップを介して検出できます。

ネットワーク内にある管理対象外デバイスのトラップ送信先を Dell Management Console システムの IP アドレスに設定します。これらのデバイスが Dell Management Console システムに非同期的にトラップを送信すると、各トラップは個々の検出プロセスを開始し、そのプロセスによりトラップの送信元ノードが検出されます。

この機能はデフォルトでは無効になっています。

 **メモ:** Dell は、この機能を有効にする時には注意を払うことを推奨しています。管理対象外デバイスから多数の警告を受信すると、Dell Management Console が反応しなくなる原因となる場合があります。

## 検出のトラブルシューティング

検出に関する問題のトラブルシューティングを行うには、次のツールのいずれか、または全部を使用します。

- 1 Dell トラブルシューティングツール
- 1 ネットワーク検出ログ
- 1 Altiris Log Viewer
- 1 その他のトラブルシューティングツール

Dell トラブルシューティングツールは Dell Management Console とともにインストールされており、[en.community.dell.com/dell-groups/dell-management-console/m/dell\\_management\\_console-mediagallery/default.aspx](https://en.community.dell.com/dell-groups/dell-management-console/m/dell_management_console-mediagallery/default.aspx) から入手できます。このツールを使用すると、接続の問題の原因を見つけることができます。詳細については、上記リンクで入手可能な [readme](#) を参照してください。

検出関連の問題のトラブルシューティングについては、[en.community.dell.com/groups](https://en.community.dell.com/groups) にある『Dell Management Console - Trouble shooting Guide』を参照してください。

## ネットワーク検出ログ

[検出ログ](#) を参照してください。

## Altiris Log Viewer

Altiris Log Viewer を表示するには、次の手順を実行します。

1. Dell Management Console がインストールされているシステムで、**Start**(スタート)ボタンをクリックします。
2. **Programs**(すべてのプログラム)→ **Symantec**→ **Diagnostics**(診断)→ **Altiris Log Viewer**(Altiris Log Viewer)の順に選択します。  
**Altiris Log Viewer**(Altiris Log Viewer)が表示されます。

## その他のトラブルシューティングツール

- 1 IPMI 接続性ツール  
例: pmish.exe, ipmitool.exe
- 1 SNMP MIB ブラウザ  
例: MG-SOFT MIB ブラウザ
- 1 ネットワークプロトコルアナライザ  
例: Wireshark

---

## 新規組織ビューと組織グループの作成

1. **Manage**(管理)→ **Organizational Views and Groups**(組織ビューと組織グループ)の順にクリックします。
2. 左ペインで、**New Organizational Views**(新規組織ビュー)を右クリックし、**New**(新規)→ **Organizational View**(組織ビュー)と進みます。
3. **New Organizational View**(新規組織ビュー)を右クリックし、**New**(新規)→ **Organizational Group**(組織グループ)の順に選択します。  
このグループにデバイスを追加し、グループに適切な役割を割り当てることができます。

---

## インベントリ設定の設定

Dell Management Console のインベントリソリューションは、さまざまなプロトコルを使用して、ネットワーク上のデバイスからインベントリ情報を収集することを可能にします。

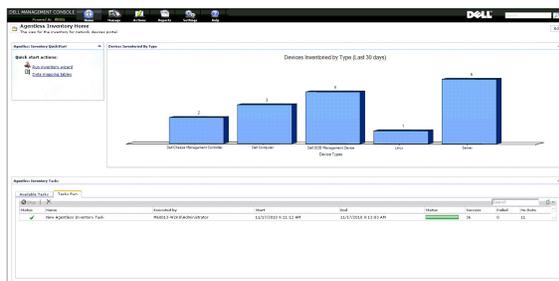
**メモ:** Server Administrator がインストールされている Dell システムは、インベントリタスクを有効にし、システムに関する具体的な詳細レポートを返します。

また、Dell Management Console では MIB をインポートして受信 SNMP トラップをフォーマットすることもできます。ただし、MIB をインポートしてデータクラスにマップし、新しいデバイスにエージェントレスインベントリを拡張することはできません。この機能には、Symantec の Altiris Inventory Solution のライセンスが必要です。

**メモ:** Dell Management Console では、エージェントベースとは Altiris Agent がターゲットシステムにインストールされていることを意味し、エージェントレスとは Dell システム管理エージェント(Dell OpenManage Server Administrator)がターゲットシステムにインストールされていることを意味します。

インベントリポータルにアクセスするには、**Home**(ホーム)→ **Discovery and Inventory**(検出とインベントリ)→ **Agentless Inventory**(エージェントレスインベントリ)の順にクリックします。

## インベントリユーザーインターフェースについて



**Agentless Inventory Quick Start**(エージェントレスインベントリクイックスタート)ウェブパーツは、ネットワークデバイスのインベントリ情報の設定と表示を開始するのに適しています。

**Agentless Inventory Tasks**(エージェントレスインベントリクイックスター)ウェブパーツには、使用可能なインベントリタスクと実行されたタスクが表示されます。

## すべてのシステムのインベントリを収集するためのインベントリタスクの作成

検出されたシステムのインベントリを収集し、情報をリソースマネージャに表示するには、次の手順を実行します。

1. **Home**(ホーム) → **Discovery and Inventory**(検出とインベントリ) → **Agentless Inventory**(エージェントレスインベントリ)の順にクリックします。  
**Agentless Inventory Home**(エージェントレスインベントリのホーム)ページが表示されます。
2. **Agentless Inventory QuickStart**(エージェントレスインベントリクイックスタート)ウェブパーツで、**Run inventory wizard**(インベントリウィザードの実行)をクリックします。  
**Agentless Inventory Task Creation**(エージェントレスインベントリタスクの作成)ページが表示されます。
3. 手順 1:**Choose devices to inventory**(インベントリを収集するデバイスの選択)で、たとえばネットワーク上の Dell PowerEdge システムのインベントリだけを収集する場合は、**Choose devices**(デバイスの選択)を選択し、**Choose a group package**(グループパッケージの選択)ドロップダウンメニューから **Servers**(サーバー)を選択して、**Next**(次へ)をクリックします。
4. 手順 2:**Inventory network task name**(インベントリネットワークタスク名)で、同種のさまざまなタスクを区別しやすいように固有の名前(Dell Server Inventory Task)を入力し、**Next**(次へ)をクリックします。
5. 手順 3:**Schedule**(スケジュール)で、このタスクの作成後にスケジュールを実行するために **Now**(今すぐ)を選択し、**Finish**(完了)をクリックします。  
  
このタスクを後で実行するように日付と時刻を指定し、これを繰り返しタスクにすることもできます。  
  
エージェントレスインベントリタスクが作成され、**Agentless Inventory Tasks**(エージェントレスインベントリのタスク)セクションの下の **Agentless Inventory Home**(エージェントレスインベントリのホーム)ページに表示されます。

## MIB のインポート

管理情報ベース(MIB)のインポート機能では、次を行うことができます。

1. MIB トラップの定義をインポートして受信トラップを分類する。
1. MIB オブジェクトをインポートしてインベントリ機能を拡張する。

ただし、MIB オブジェクトのインポートとインベントリ機能の拡張は、Symantec が提供する有料ライセンスです。

MIB インポートを実行するには、次の手順を実行します。

1. Dell Management Console で、**Settings**(設定) → **All Settings**(すべての設定) → **Monitoring and Alerting**(監視と警告) → **SNMP MIB import Browser**(SNMP MIB インポートブラウザ) → **MIB Browser**(MIB ブラウザ)の順に選択します。
2. 右上のペインから **Import MIB file**(MIB ファイルのインポート) → **Browse**(参照)の順に選択し、必要な MIB ファイルを選択して **Apply**(適用)を選択します。
3. MIB ファイルは、**iso** → **org** → **dod** → **internet**(インターネット) → **private**(プライベート) → **enterprises**(エンタープライズ)にあります。

## カスタム組織グループ内の選択されたデバイスのインベントリを収集するためのインベントリタスクの作成

複数の組織グループを作成したら、[新規組織ビューと組織グループの作成](#)を参照してください。Dell|EMC デバイスのインベントリだけを収集できます。

1. **Home**(ホーム) → **Discovery and Inventory**(検出とインベントリ) → **Agentless Inventory**(エージェントレスインベントリ)の順にクリックして **Agentless Inventory Home**(エージェントレスインベントリのホーム)ページを表示します。
2. **Agentless Inventory QuickStart**(エージェントレスインベントリクイックスタート)ウェブパーツで、**Run inventory wizard**(インベントリウィザードの実行)をクリックします。  
**Agentless Inventory Task Creation**(エージェントレスインベントリタスクの作成)ページが表示されます。
3. 手順 1:**Choose devices to inventory**(インベントリを収集するデバイスの選択)で、たとえばネットワーク上の Dell|EMC デバイスのインベントリだけを収集する場合は、**Choose devices**(デバイスの選択)を選択し、**Choose a group package**(グループパッケージの選択)ドロップダウンメニューから **Servers**(サーバー)を選択します。
4. Dell|EMC デバイスを除くすべてのデバイスをクリアし、**Next**(次へ)をクリックします。
5. 手順 2:**Inventory network task name**(インベントリネットワークタスク名)で、同種のさまざまなタスクを区別しやすいように固有の名前(Dell Server Inventory Task)を入力し、**Next**(次へ)をクリックします。
6. 手順 3:**Schedule**(スケジュール)で、このタスクの作成後にスケジュールを実行するために **Now**(今すぐ)を選択し、**Finish**(完了)をクリックします。このタスクを後で実行するように日付と時刻を指定し、これを繰り返しタスクにすることもできます。

## タスクの進行状況と詳細の表示

インベントリタスクの進行状況を表示するには、次の手順を実行します。

1. **Home**(ホーム) → **Discovery and Inventory**(検出とインベントリ) → **Agentless Inventory**(エージェントレスインベントリ)の順にクリックして **Agentless Inventory Home**(エージェントレスインベントリのホーム)ページを表示します。
2. **Agentless Inventory Tasks**(エージェントレスインベントリのタスク)ウェブパーツで、**Tasks Run**(タスク実行)タブを選択します。  
タスクの状態と進行状況が表示されます。
3. **Agentless Inventory Tasks**(エージェントレスインベントリのタスク)ウェブパーツで、**Available Tasks**(使用可能なタスク)タブを選択します。  
すべての使用可能なインベントリタスクが表示されます。
4. タスクの追加詳細情報を表示するために、タスクインスタンスをダブルクリックします。  
新しいウィンドウにタスクの詳細が表示されます。

## インベントリタスクの結果の表示

1. **Manage**(管理) → **All Devices**(すべてのデバイス)の順にクリックします。
2. 左ペインで、**All Devices**(すべてのデバイス)ツリーを展開し、**Servers**(サーバー)を選択します。  
検出されたシステムは、右ペインに、**Resource Type**(リソースタイプ)が **Dell Computer**(Dell コンピュータ)として表示されます。
3. インベントリの詳細を表示するシステム名をダブルクリックします。
4. **Resource Manager Home**(リソースマネージャのホーム)ページで、**Summaries**(サマリ) → **Hardware Summary**(ハードウェア概要)の順にクリックします。  
システムのインベントリ情報が表示されます。Hardware Summary(ハードウェア概要)を表示するには、ターゲットシステムに **Server Administrator** をインストールし、システムを **Dell Computer**(Dell コンピュータ)として分類します。

---

[目次に戻る](#)

[目次に戻る](#)

## ハードウェアの設定タスク

Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [ハードウェアの設定タスクについて](#)
- [ハードウェアの設定タスクユーザーインターフェイスについて](#)

Dell Management Console には、一組のハードウェアの設定タスクが用意されており、これらのタスクを使ってサーバーハードウェア設定を迅速に行うことができます。これらのタスクを利用すると、Dell PowerEdge システムで共通の BIOS 設定および共通のベースボード管理コントローラ(BMC)設定を行うことができます。

## ハードウェアの設定タスクについて

ハードウェアの設定タスクは、システムの BIOS タスクと同じ機能を提供します。Hardware Configuration Tasks(ハードウェアの設定タスク)の **Advanced**(詳細設定)ペインで設定を変更する場合、タスクを正常に実行するには、Admin(管理者)パスワードを再入力する必要があります。

Advanced(詳細設定)の設定とハードウェアの設定パラメータの詳細については、『Dell Management Console のオンラインヘルプ』を参照してください。

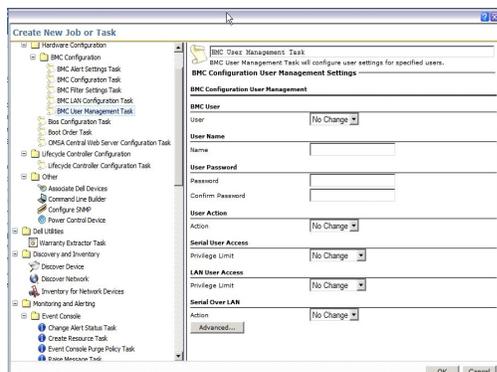
ハードウェアの設定タスクを使用して、次の設定を行うことができます。

- 1 BIOS Configuration Task(BIOS 設定タスク) - フロントパネル LCD 設定、メモリ冗長性設定、キーボード Numlock 設定、ネットワークインタフェースコントローラ(NIC)設定、およびシステムセキュリティ設定を行うには、このタスクを実行します。
- 1 BMC Configuration(BMC の設定) - このタスクには、次の 5 つのサブタスクがあります。
  - BMC Alert Settings Task(BMC アラート設定タスク) - プラットフォームイベント警告ポリシーおよび警告の宛先を設定するには、このタスクを実行します。
  - BMC Configuration Task(BMC の設定タスク) - LAN チャネルアクセス、シリアル設定パラメータ、およびターミナルノード設定などの共通の BMC パラメータを設定するには、このタスクを実行します。
  - BMC Filter Settings Task(BMC フィルタ設定タスク) - プラットフォームイベントフィルタ(PEF)設定を行うには、このタスクを実行します。温度プローブエラーなどの所定の PEF イベントに対しては、サーバーの電源オフや再起動などの適切な措置を設定できます。
  - BMC LAN Configuration Task(BMC LAN 設定タスク) - Dell PowerEdge システムで LAN およびシリアルオーバー LAN(SOL)パラメータを設定するには、このタスクを実行します。
  - BMC User Management Task(BMC ユーザー管理タスク) - 指定のユーザーに対してユーザー設定を行うには、このタスクを実行します。
- 1 Boot Order Task(起動順序タスク) - 管理対象システムのプライマリデバイスの起動順序を変更するには、このタスクを実行します。
- 1 Central Web Server Configuration Task(Central Web Server の設定タスク) - Dell OpenManage Server Administrator がインストールされている管理対象システムに Central Web Service の URL 起動ポイントを設定するには、このタスクを実行します。
- 1 Lifecycle Controller Configuration Task(Lifecycle Controller の設定タスク) - Lifecycle Controller の設定を行うには、このタスクを実行します。
- 1 Server Task(サーバータスク) - Health Monitor Email Task(正常性監視電子メールタスク) - 事前に選択したデバイスの正常性の状態について電子メールによる警告を送信するには、このタスクを実行します。
- 1 Create New Task(新規タスクの作成)

## ハードウェアの設定タスクユーザーインターフェイスについて

Jobs and Tasks(ジョブとタスク)ポータルページにアクセスするには、**Manage**(管理)→ **Jobs and Tasks**(ジョブとタスク)をクリックします。

Dell Tasks(Dell タスク)フォルダの下に **Hardware Configuration**(ハードウェアの設定)フォルダが表示されます。



## ハードウェアの設定タスクの作成

ハードウェアの設定タスクを作成するには、[ジョブとタスクモジュールの使用](#)を参照してください。

**Job and Tasks Status**(ジョブおよびタスクの状態) ウェブパーツで、Dell Management Console のポータルページからタスクを表示できます。タスクをダブルクリックすると、その **Output Properties**(出力プロパティ)が表示されます。

詳細については、『[オンラインヘルプ](#)』を参照してください。

---

[目次に戻る](#)

[目次に戻る](#)

# Dell Management Console のインストール、アンインストール、およびアップグレード

Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [インストール要件](#)
- [Dell Management Console のアンインストール](#)
- [最新バージョンの Dell Management Console へのアップグレード](#)
- [HTTPS の有効化](#)
- [トラブルシューティング](#)
- [パフォーマンス調整](#)

Dell Management Console は、Symantec モジュラーアーキテクチャを使用して、ユーザーのニーズに合わせた最適なソリューションを提供します。Dell Management Console は、Symantec インフラストラクチャを基盤としており、その主要テクノロジーを利用してタスクの実行、ソフトウェアの展開、およびネットワーク上のデバイスの検出と在庫管理を実現します。

Symantec Installation Manager (SIM) は、Dell Management Console のインストーラです。SIM インストーラにより、管理ステーションに SIM がインストールされます。Dell Management Console は SIM のインストールオプションとして提供されます。

## インストール要件

推奨されるハードウェア構成については、[推奨される最小構成](#)を参照してください。

Dell Management Console をインストールする管理ステーションには、ソフトウェアに関する次の前提条件があります。

## Dell Management Console の前提条件

Dell Management Console をインストールする前に、管理ステーションに Microsoft .NET Framework 3.5 をインストールする必要があります。

 **メモ:** 前提条件となるソフトウェアが管理ステーションにインストールされていない場合、SIM (『Dell Management Console DVD』に収録) によって前提条件がスキャンされ、前提条件をインストールするためのリンクが表示されます。これらのリンクを使用して前提条件となるソフトウェアをダウンロードおよびインストールしてから、Dell Management Console をインストールします。

## インストール準備完了の前提条件

- 1 Microsoft Windows Server 2008 R2 (64 ビット)
- 1 Microsoft ASP .NET Framework
- 1 Microsoft Silverlight 3.0
- 1 Microsoft SQL Express 2008、SQL Express 2005、SQL Server 2005、SQL Server 2008 SP1、または SQL Server 2008 R2
- 1 8 GB 以上の空きディスク容量。10 GB の空きディスク容量が推奨されます
- 1 Internet Information Services 7.0 以下
- 1 Microsoft Internet Explorer バージョン 8.0 以下
- 1 インターネット接続

 **メモ:** インターネットにアクセスできない場合は、インターネット接続のあるシステムに SIM をインストールしてインストールパッケージを作成します。SIM を起動し、**Create installation package** (インストールパッケージの作成) をクリックして、Dell Management Console の最新バージョンを選択します。これにより、インストールパッケージが作成されます。Dell Management Console をインストールするサーバーに、インストールパッケージをコピーします。

インストールの前提条件の詳細については、『Support Information Matrix for Dell Management Console』を参照してください。

## その他の考慮事項

- 1 管理ステーションを Windows Domain Controller として設定しないでください。
- 1 ターミナルサービスを利用して Dell Management Console をインストールする場合は、そのインストールがコンソールセッションを介していることを確認します。例えば、mstsc/console が挙げられます。
- 1 (強く推奨) 管理ステーションに HyperText Transfer Protocol over Secure Socket Layer (HTTPS) をインストールして設定し、有効にします。
- 1 このリリースの Dell Management Console にアップグレードする場合は、SIM を使用します。最新のアップデートを取得するには、SIM をインターネットに接続する必要があります。SIM のアップデートや、使用可能なその他の重要アップデートが必要になる場合があります。推奨されるアップデートおよび任意のアップデートは、Updates (アップデート) セクションに表示されます。
- 1 SSL を適用せずに Dell Management Console をインストールした場合に、Altiris Agent が SSL モードを使用していると、検出タスクを実行したときにエラーメッセージが表示されます。解決するには、Dell Management Console と Altiris Agent が SSL モードで動作するように設定します。セキュアなウェブページ [kb.altiris.com](#) の **Configuring Notification Server to use SSL knowledge base content** の項を参照してください。
- 1 Dell Management Console バージョン 1.1 または 1.1.x からこのリリースの Dell Management Console にデータベースを移行する場合は、[Dell Management Console への移行](#)を参照してください。

## Dell 管理コンソールのインストール

Dell Management Console は、『Dell Management Console DVD』からインストールすることも、[Support.dell.com](http://Support.dell.com) から自己解凍式実行ファイルをダウンロードしてインストールすることもできます。また、Welcome(ようこそ)画面に表示されるリンクを使用して依存関係をインストールできます。

1. 『Dell Management Console』DVDを DVD ドライブに挿入します。インストールプログラムが自動的に起動しない場合は、DVD のルートフォルダに移動して **setup.exe** をダブルクリックします。

または

**Support.dell.com** から自己解凍式ファイルをダウンロードします。ダウンロードしたファイルをダブルクリックして必要なパスに展開し、OK をクリックします。プログラムが開始されない場合は、展開したフォルダに移動し、**setup.exe** をダブルクリックします。

Dell Management Console の Welcome(ようこそ)ダイアログボックスが表示されます。

 **メモ:** 前述の前提条件がインストールされていない場合は、Welcome(ようこそ)画面で Minimum System Requirement(最小システム要件)をクリックします。各前提条件をクリックしてリンクを開き、インターネットを通じてソフトウェアをダウンロードします。

2. Welcome(ようこそ)画面で **Install Dell Management Console** (Dell Management Console のインストール)を選択します。

マシンを再起動して表示されるポート数を増やすように求めるメッセージが表示されます。Yes(はい)を選択します。

システムが再起動したら、インストーラを実行します。インストーラによって、システム上の Microsoft .NET Framework がスキャンされます。.NET がインストールされていない場合、.NET Framework をインストールするように求められます。

依存関係の欠落がなければ、**Symantec Installation Manager Setup**(Symantec Installation Manager のセットアップ)ダイアログボックスが表示されます。

3. **Next(次へ)**をクリックします。
4. エンドユーザーライセンス契約に同意し、**Next(次へ)**をクリックします。
5. **Destination Folder**(宛先フォルダ)ダイアログボックスで、Dell Management Console をインストールするフォルダを参照し、**Begin Install**(インストールの開始)をクリックします。
6. インストールが完了したら、**Automatically launch Symantec Installation Manager**(Symantec Installation Manager を自動的に起動)を選択し、**Finish(完了)**をクリックします。

Symantec Installation Manager(SIM)が自動的に起動します。

 **メモ:** ホットフィックス、パッチ、および付加価値プラグインソリューションのトライアルバージョンをダウンロードするには、インターネットアクセスが必要です。

 **メモ:** ネットワークでインターネットアクセス用にプロキシサーバーを使用している場合、インターネットに接続するには、SIM のプロンプトにプロキシの詳細を入力します。

7. **Symantec Installation Manager** のメインダイアログボックスで、**Install new products**(新製品のインストール)を選択します。SIM を最新バージョンにアップデートするように要求されたら、**Update Now**(今すぐアップデート)をクリックして OK をクリックします。表示されるすべてのインストール画面に、必要な詳細を入力します。

8. **Install New Products**(新製品のインストール)ダイアログボックスで、**Dell Management Console** を選択して **Next(次へ)**をクリックします。

各種のフィルタを選択できます。その他のコンポーネントを確認し、インストールするには、**show all available versions**(使用可能なすべてのバージョンを表示する)を選択します。

9. **Optional Installs**(オプションインストール)ダイアログボックスの Available features(使用可能な機能)から、インストールする機能を選択します。

Dell Management Console バージョン 1.1 または 1.1.x からこのリリースの Dell Management Console にデータベースを移行する場合は、**Install Migration Wizard Components for migration Dell Management Console data**(Dell Management Console データの移行用に移動ウィザードコンポーネントをインストールする)を選択します。

**Next(次へ)**をクリックします。

10. エンドユーザーライセンス契約に同意し、**Next(次へ)**をクリックします。

**Install Readiness Check**(インストール準備状態のチェック)ダイアログボックスに、依存関係と推奨事項が表示されます。

11. 欠落している依存関係がある場合は、提供されるリンクを使用してオンラインで必要条件をインストールします。

 **メモ:** .Net 証明書および SQL 最大メモリ構成についてインストール準備状態をチェックしてください。

**Check install readiness again**(インストールの準備状態を再チェックする)をクリックし、**Next(次へ)**をクリックします。

12. **Dell Management Console Configuration**(Dell Management Console の設定)ダイアログボックスに、ローカル管理者の資格情報を入力します。

電子メール情報を設定している場合は、テストメールの送信によって設定を検証できます。

13. **Next**(次へ)をクリックします。

14. **Database Configuration**(データベースの設定)ダイアログボックスに、Symantec 管理コンソールで使用される Microsoft SQL Server の詳細を入力します。

Symantec Installation Manager を移行に使用する場合、つまり、Dell Management Console バージョン 1.1 または 1.1.x からこのリリースの Dell Management Console に復元されたデータベースを使用する場合、**Database name**(データベース名)から **Use existing**(既存を使用)を選択し、リストから復元データベースを選択して **Next**(次へ)をクリックします。

データベース移行方法を使用している場合は、**Next**(次へ)をクリックします。

15. **Review Installation Details**(インストールの詳細の確認)ダイアログボックスで、**Begin Install**(インストールの開始)をクリックします。

Dell Management Console がインストールされます。

Product Licensing(製品ライセンス)ダイアログボックスが表示されます。

16. **Product Licensing**(製品ライセンス)ダイアログボックスで、**Next**(次へ)をクリックします。

Installation Complete(インストールの完了)ダイアログボックスが表示されます。

17. Installation Complete(インストールの完了)ダイアログボックスで、**Finish**(完了)をクリックします。

Dell Client Manager への Dell Management Console のインストールについては、『Symantec Management Platform Installation Guide』を参照してください。

## インストール後の注意点

- 1 Dell Management Console をインストールした後で、オペレーティングシステムと Symantec 管理コンソールのパスワードを変更する場合は、必ずオペレーティングシステムのパスワードを変更する前に、Symantec 管理コンソールのパスワードを変更してください。

ただし、オペレーティングシステムのパスワードを Notification Server のパスワードよりも前に変更した場合は、次のコマンドを使用して Notification Server のパスワードを変更できます。

```
aexconfig /svcid user:<username (domain, machine%user)> password:<password>
```

 **メモ:** aexconfig コマンドは、Altiris/Notification server/bin フォルダの下で使用できます。

- 1 Dell Management Console をインストールした後で、システムのホスト名を変更し、Dell Management Console を起動しようとすると、サーバーの例外が表示されます。

この問題のトラブルシューティングについては、Dell Management Console の『オンラインヘルプ』で **Symantec Management Server Error** の項を参照してください。

---

## Dell Management Console のアンインストール

Dell Management Console をアンインストールするには、次の手順を実行します。

1. **Add or Remove Programs**(プログラムの追加と削除)に移動し、Symantec Platform and Solutions(Symantec プラットフォームおよびソリューション)ウィザードを実行します。
2. **Symantec Platform and Solutions**(Symantec プラットフォームおよびソリューション)コンポーネントを選択し、**Uninstall**(アンインストール)をクリックします。

Dell Management Console がアンインストールされます。

『Dell Management Console』DVDから Dell Management Console をアンインストールすることもできます。

1. 『Dell Management Console』DVDを挿入します。
2. **Dell Management Console**(Dell Management Console)ダイアログボックスで、**Install Dell Management Console**(Dell Management Console のインストール)を選択します。
3. **Install Products**(製品のインストール)ダイアログボックスが表示されるまで、インストールウィザードを先に進めます。
4. Dell Management Console オプションを選択し、**Uninstall**(アンインストール)をクリックします。

Dell Management Console がアンインストールされます。

 **メモ:** Dell Management Console をアンインストールしても、Dell Management Console データベースはアンインストールされません。

---

## 最新バージョンの Dell Management Console へのアップグレード

Dell Management Console の初期バージョンからこのバージョンにアップグレードすることはできません。このバージョンは、Windows Server 2008 R2 64 ビットまたは Windows Server 2008 R2 64 ビット SP1 オペレーティングシステムにインストールする必要があります。このバージョンのリリースは、32 ビットから 64 ビットバージョンの Dell Management Console へのアップ

ブグレードをサポートしていません。

32 ビットオペレーティングシステムにインストールできる最新バージョンの Dell Management Console へのアップグレードについては、[support.dell.com/manuals](https://support.dell.com/manuals) を参照してください。

---

## HTTPS の有効化

Dell Management Console をインストールした後、リモートデスクトップ機能および RAC Telnet 機能を使用するには、HTTPS を有効にします。

HTTPS を有効にするには、次の手順を実行します。

1. **デスクトップ** から **Start** (スタート) → **Run** (ファイル名を指定して実行) を選択します。
2. **Run** (ファイル名を指定して実行) で、`inetmgr` と入力します。  
Internet Information Services Manager が表示されます。
3. 右側のペイン (中央) でサーバー (ホスト名が表示されます) を選択し、**Server Certificates** (サーバー証明書) をダブルクリックします。
4. 右側のペインで **Create Self-Signed Certificate** (自己署名証明書の作成) をクリックします。
5. ウィザードに名前を入力し、**OK** をクリックします。
6. ホスト名の下側のペインで、**Sites** (サイト) ツリーを展開して **Default Web Site** (デフォルトウェブサイト) をクリックします。
7. **Actions** (アクション) の下の右側のペインで、**Bindings...** (バインド) → **Add** (追加) をクリックし、**HTTPS** タイプを選択します。
8. **SSL Certificate** (SSL 証明書) の下から、作成した証明書を選択します。
9. **中央** ペインで **SSL Settings** (SSL 設定) をクリックし、**Require SSL** (SSL 必須) を選択します。

 **メモ:** Dell Management Console のインストール時に HTTPS を有効にするには、インストールの準備状態のチェック完了後に表示されるページで、**Use SSL to access the Management Platform** (SSL を使用して管理プラットフォームにアクセスする) を選択します。  
Dell Management Console を開くときは、URL に LOCALHOST ではなくシステムホスト名が含まれていることを確認してください。LOCALHOST が含まれていると、証明書エラーが発生し、右クリック操作が機能しません。  
また、右クリック操作のレジストリキーファイルがレジストリに入っていることを確認してください。

---

## トラブルシューティング

トラブルシューティングの詳細については、『オンラインヘルプ』を参照してください。

---

## パフォーマンス調整

Dell Management Console にリモートデータベースを設定した場合に、Dell Management Console のパフォーマンスを最適化するには、[en.community.dell.com/dell-groups/dell-management-console/m/dell\\_management\\_console-mediagallery/default.aspx?PageIndex=3](https://en.community.dell.com/dell-groups/dell-management-console/m/dell_management_console-mediagallery/default.aspx?PageIndex=3) からダウンロードできるホワイトペーパーを参照してください。

---

[目次に戻る](#)

[目次に戻る](#)

## はじめに

### Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [このリリースの新機能](#)
- [Dell Management Console の使用開始前に](#)
- [その他の必要マニユアル](#)
- [Symantec Management Platform 7.1 セキュリティモデル 33271](#)

Dell Management Console は、一対多システム管理アプリケーションで、強化された検出機能、インベントリ機能、監視機能、パッチ アップデート機能、および報告機能を提供します。

Dell Management Console は、ウェブベースのグラフィカル ユーザー インターフェイス (GUI) であり、基本的なハードウェア管理用の拡張可能なモジュラー コンソールに加え、資産管理、高度なセキュリティ、コンプライアンスなどの高度な機能も提供します。Dell Management Console は、ネットワーク環境の管理ステーションにインストールできます。

Dell Management Console は、デルサポートサイト [support.jp.dell.com](http://support.jp.dell.com) からダウンロードできる無償のソフトウェアです。ただし、無償の永続ライセンスを取得するには、デルウェブサイト [dell.com/openmanage/register](http://dell.com/openmanage/register) に登録する必要があります。登録すると、30 日の試用期間後も Dell Management Console を引き続き使用できます。Dell Management Console は、Symantec Server Management Suite など様々な Symantec プラグインをサポートしています。

 **メモ:** Symantec Inc. は Altiris Inc. を買収したため、本書には Altiris と Symantec への参照が含まれている場合があります。

## このリリースの新機能

このリリースでは、次の機能を使用できます。

- 1 オペレーティングシステムのサポート - Dell Management Console は、Windows 2008 R2(64 ビット)および Windows 2008 R2(64 ビット)SP1 オペレーティングシステムにインストールできます。
- 1 設定 - わかりやすい手順の説明にアクセスして Dell Management Console を設定し、デバイス、監視の設定、SNMP 警告、および Dell パッチの検出およびインベントリ作成を行うことができます。また、Dell テックセンターおよびデル FAQ のリンクでも詳細情報にアクセスできます。
- 1 コンソールモード - 基本コンソールモードおよび標準コンソールモードを使用できます。基本コンソールモードでは基本機能に迅速にアクセスでき、標準コンソールモードでは Dell Management Console で使用できるすべての機能にアクセスできます。基本コンソールモードで使用できる機能は、Configuration(設定)、switch to Standard Console(標準コンソールへの切り替え)、Dell Management Console Portal(Dell Management Console ポータル)、Discovery and Inventory(検出とインベントリ)、Events and Alerts(イベントとアラート)、All Devices(すべてのデバイス)、および Help(ヘルプ)があります。
- 1 保証サポートサイトを開き、現在の保証情報を表示します。
- 1 サーバーモデル番号とシステム出荷日が記載された保証レポートを取得します。
- 1 LifeCycle Controller 1.4 によって提供されるインベントリ情報を取得します。
- 1 仮想マシン (VMware ESX 4.1 または Microsoft Hyper-V 2008) に Dell Management Console をインストールします。
- 1 統合トラブルシューティングツールを使用して、Dell Management Console でサポートされている各種プロトコルの検出関連問題を診断します。

## Dell Management Console の使用開始前に

Dell Management Console をインストールし、設定するには、次のプロセスを考慮してください。

- 1 Dell Management Console インストールの計画 - 次の要件に基づいてインストールを計画します。
  - 1 ネットワークの規模
    - 1 管理するネットワークデバイスと、それらのネットワークデバイスとの通信に必要なプロトコル。たとえば、Simple Network Management Protocol(SNMP)、Windows Management Interface(WMI)、Web Services for Management(WS-MAN)、または Intelligent Platform Management Interface(IPMI)プロトコルなど。デバイスと必要なプロトコルの詳細については、[表 6-1](#) を参照してください。
    - 1 監視する属性 たとえば、デバイスの正常性のみを管理することも、デバイスの正常性とパフォーマンスを管理することもできます。
    - 1 多数のサイトへの階層化ソフトウェア展開。詳細については、[Help\(ヘルプ\) → Documentation Library\(マニュアルライブラリ\)](#) または [Help\(ヘルプ\) → Context\(コンテキスト\)](#) から入手できる Symantec のマニュアルを参照してください。

詳細については、[Dell Management Console のインストール計画](#)を参照してください。

- 2 Dell Management Console のインストール - 『Dell Management Console DVD』またはデルウェブサイト [dell.com/openmanage](http://dell.com/openmanage) から Dell Management Console をインストールできます。Dell Management Console のインストールの詳細については、[Dell Management Console のインストール、アンインストール、およびアップグレード](#)を参照してください。
- 3 Dell Management Console の設定準備 - Dell Management Console およびネットワークデバイスの設定には、計画を行うことが最も重要です。次の詳細の設定を計画してください。
  - 1 検出タスク。たとえば、IP アドレス、サブネット、ホスト名、およびカスタム範囲などの包括範囲と除外範囲を定義します。
  - 1 ネットワーク上デバイスのタイプ (Dell デバイスおよび Dell 製ではないデバイスの両方)。
  - 1 デバイスのセキュリティ。
  - 1 接続プロファイルと資格情報。詳細については、[接続プロファイルと資格情報管理](#)を参照してください。

4. 次の順序に従った Dell Management Console の設定 (Dell Management Console の設定手順については、[設定ページ](#)を参照してください)。
  - a. 検出タスク - 検出するネットワークデバイスのグループを定義します。
  - b. エージェントの展開 - Altiris Agent を展開してから、Dell OpenManage エージェントである Dell OpenManage Server Administrator (OMSA) をターゲットサーバーに展開します。
  - c. インベントリ - メモリ、プロセッサ、電源装置、組み込みデバイス、およびソフトウェアとファームウェアのバージョンなどのインベントリ情報を収集します。詳細については、[インベントリ設定の設定](#)を参照してください。
  - d. ネットワークデバイスの整理 - 組織または地理的位置に基づいてネットワークデバイスを整理できます。
  - e. ステータスポーリングの設定 - すべての検出されたデバイスについて電源および接続の正常性をチェックします。これによりデバイスが正常に動作しているか、異常な常態か、電源が切れているかを判断します。詳細については、[監視と警告](#)を参照してください。
  - f. イベント管理および警告 - プロトコルを設定します。
  - g. 管理情報ベース (MIB) - ネットワークに Dell 以外のデバイスが存在する場合は、それらのデバイスから受信したトラップを認識できるように、適切な MIB をインポートします。詳細については、[MIB のインポート](#)を参照してください。
  - h. パフォーマンスおよび正常性の監視 - ネットワークデバイスの正常性とパフォーマンスをリアルタイムで監視します。
  - i. パッチ管理 - Altiris Agent または LC 対応パッチアップデートを使用して、1 つのシステムまたはシステムのグループに一度にアップデートを展開します。
  - j. タスク - システムのグループを設定します。
  - k. レポート - レポート結果を Dell Management Console で表示する方法を選択し、レポートのデフォルトビューを設定します。

## Dell Management Console のインストール計画

本項では、Dell Management Console のインストールを計画する際に生じる可能性のある疑問点について回答しています。

### Dell Management Console をインストールするための基本的なハードウェア要件は何ですか？

特定の Dell Management Console の展開およびネットワーク環境によっては、推奨設定以上のプロセッサ速度、メモリ容量、およびハードウェアドライブ容量をお勧めします。

### 推奨される最小構成

- 1 Microsoft Windows Server 2008 R2 (64 ビット)
- 1 4 つ以上のプロセッサコア
- 1 RAM - 4 GB
- 1 DVD ドライブ
- 1 Microsoft .NET Framework バージョン 3.5、3.5 SP1、または 4.0

 **メモ:** Microsoft .NET Framework バージョン 4.0 は、システムにバージョン 3.5 または 3.5 SP1 が存在する場合にのみサポートされます。

- 1 Microsoft Silverlight 3.0
- 1 Windows Internet Information Services バージョン 7.0
- 1 Microsoft SQL Express 2008、SQL Express 2005、SQL Server 2005 SP1、SQL Server 2005 SP2、SQL Server 2005 SP3、SQL Server 2008 SP1、または SQL Server 2008 R2
- 1 (推奨)規模の大きい環境の場合、リモートデータベース、8 個以上のプロセッサコア、および 8 GB 以上のメモリ空き容量が使用可能であることを推奨
- 1 Windows Internet Explorer バージョン 7.0 または 8.0 (32 ビットのみ)

詳細については、[DellTechCenter.com](#) を参照してください。

### どのシステム管理プロトコルをインストールまたは有効にすればよいか？

一般に、選択するプロトコルは、モニターするシステムと、そのシステムがサポートするそれぞれのエージェントプロトコルによって決定されます。監視するシステムに、Simple Network Management Protocol (SNMP)、Windows Management Interface (WMI)、Web Services for Management (WS-MAN)、または Intelligent Platform Management Interface (IPMI) プロトコルを使用するエージェントが存在する場合、これらのプロトコルを Dell Management Console に設定します。

Dell Management Console では、必要なプロトコルが含まれるように **Connection Profile** (接続プロファイル) を設定できます。Dell Management Console は、**Connection Profile** (接続プロファイル) に定義されたプロトコルを使用して、ネットワーク上のデバイスに接続します。

### サブネットで複数のシステム管理プロトコルを使用している場合、どのように 管理下システムの IP アドレス を整理したらよいか？

可能な限り、同一のシステム管理プロトコルを使用するシステムを、連続したサブネットにグループ化します。この方法は、Dell Management Console の検出範囲を作成する際の管理の容易性を向上させます。

### 監視ネットワークのパフォーマンスは、監視対象の属性によって決まりますか？

はい。監視するデバイスの属性によって、必要なリソースが決定されます。たとえば、システムの正常性だけを監視するには、推奨される最小ハードウェア構成で十分です。ただし、構成は、監視するシステムの数によって異なります。

システムの正常性とパフォーマンスを監視するには、推奨設定以上の構成をお勧めします。[推奨される最小構成](#)を参照してください。

世界各地にある管理システムを使用した多層化ネットワークを利用しています。これは Dell Management Console のインストール方法にどのように影響しますか？

世界各地に管理ステーションが存在する場合、Dell Management Console のインストール方法に影響が及びます。詳細については、階層化インフラストラクチャに関する Symantec のマニュアルを参照してください。Symantec のマニュアルは、Help(ヘルプ)→ Documentation Library(マニュアルライブラリ)で入手できます。

## Dell Management Console の設定計画

Dell Management Console をインストールした後は、設定計画を立てる必要があります。Dell Management Console の設定手順については、[Configuration\(設定\)ページ](#)を参照してください。

ネットワークに Dell デバイスと Dell 製ではないデバイスが存在しています。これらのデバイスは別々に設定すべきですか？

はい。監視する Dell 製ではないデバイス用に適切な MIB をインポートする必要があります。Dell 製ではないデバイス用の MIB をインポートすると、それらのデバイスに関する SNMP 警告を受信できるようになります。

Dell Management Console を使用するために設定するセキュリティオプションには何がありますか？

役割ベースのセキュリティについて、Help(ヘルプ)→ Documentation Library(マニュアルライブラリ)で入手できる Symantec のマニュアルを参照してください。

Dell OpenManage IT Assistant から移行しています。検出範囲を Dell Management Console に移行するにはどうすればよいですか？

IT Assistant からの検出設定の移行については、[IT Assistant の検出設定のインポート](#)を参照してください。

使用する機能に対して必要な特別設定はありますか？

任意の機能またはすべての機能を要件に応じて設定できます。各機能を適切に動作させるために、管理対象デバイスに展開する必要があるエージェントについては、[表 1-1](#) を参照してください。

表 1-1. エージェントによってサポートされている機能

機能	エージェントなし	Dell OpenManage Server Administrator	Altiris エージェント
Discovery(検出)	IPMI、WMI、または SNMP を使用して検出	リソースマネージャの詳細なハードウェア概要に必要	不要
Inventory(インベントリ)	IPMI、WMI、または SNMP を使用した基本インベントリ	リソースマネージャの詳細なハードウェア概要に必要	不要
Monitoring Health(正常性の監視)	IPMI * を使用した帯域外正常性の監視	SNMP 経由のエージェントベースの正常性監視に必要	不要
Events(イベント)および Alerting(警告)	基本的な IPMI プラットフォームイベントラップ(PET)のみ	包括的なハードウェアイベントに必要	不要
Hardware configuration task(ハードウェアの設定タスク)	-	必須	不要
Deploying the Dell Agent(Dell エージェントの展開) - Server Administrator	-	-	必須
Patch(firmware/drivers/BIOS)Management(パッチ(ファームウェア/ドライバ/BIOS)管理)	-	-	必須
Monitor Operating System Performance(オペレーティングシステムのパフォーマンスの監視)	WMI/IPMI * を使用し、Windows エージェントレスで監視	IPMI * が有効 / 使用可能でない場合に必要	Linux で動作しているシステムに必要

\* IPMI は Dell PowerEdge x8xx サーバーまたはそれ以降のサーバーで使用できます。

Dell Management Console を使用して管理できるように管理対象デバイスを有効にするには、どうすればよいですか？

SNMP および WMI プロトコルを使用する Dell PowerEdge システムの場合、管理を最も容易にするために Dell OpenManage Server Administrator を管理対象システムにインストールする必要があります。

Dell Management Console でプロトコルおよび資格情報が正しく設定されていれば、サーバーではないその他のデバイスを管理できます。たとえば、ネットワークプリンタを管理する場合は、SNMP が有効化され、Dell Management Console の接続プロファイル設定でコミュニティストリングが定義されている必要があります。詳細については、[接続プロファイルと資格情報管理](#)を参照してください。

## その他の必要マニュアル

参照用として次のマニュアルにアクセスできます。

- 1 Symantec のマニュアルは、Help(ヘルプ)→ Documentation Library(マニュアルライブラリ)で入手できます。
  - Symantec のマニュアルには、Notification Server 7.1 のマニュアルが含まれます。
- 1 オンラインヘルプには、Help(ヘルプ)→ Context(コンテキスト)からアクセスできます。
- 1 デルサポートサイト [support.dell.com/manuals](http://support.dell.com/manuals) で、『Dell Management Console 向けサポート情報マトリクス』、『用語集』および『Readme』にアクセスできます。
- 1 メディアでは、次の情報にアクセスできます。
  - 『Readme』がリンクとして提供されます。

- 製品デモがリンクとして提供されます。
  - 1 Dell EqualLogic の詳細については、デルサポートサイト [support.dell.com/manuals](http://support.dell.com/manuals) で利用できる Dell EqualLogic のマニュアルを参照してください。
  - 1 その他のマニュアルは、Dell テックセンター [delltechcenter.com/page/Dell+Management+Console](http://delltechcenter.com/page/Dell+Management+Console) および [en.community.dell.com/groups/](http://en.community.dell.com/groups/) で入手できます。
  - 1 Navisphere CLI の最新のソフトウェアおよびユーザーマニュアルについては、[powerlink.emc.com](http://powerlink.emc.com) を参照してください。リンクは、Dell Management Console のインストールウィザードからも利用できます。
- 

## Symantec Management Platform 7.1 セキュリティモデル 33271

Symantec Management Platform 7.1 セキュリティモデルには、次の機能があります。

- 1 Symantec ロールは現在、Symantec Management Platform の内部エンティティです。(Windows ユーザーグループは作成されません)。
  - 1 Symantec ユーザーは、Symantec Management Platform の内部エンティティです。
  - 1 Symantec ロールには、その他の Symantec ロールおよび Symantec ユーザーを含めることができます。
  - 1 Symantec ユーザーは、Windows アカウントまたは内部 Symantec Management Platform アカウントにマッピングされます。
  - 1 Notification Server コンソールへのログオンは、Symantec Management Platform アカウントまたはマッピングされた Windows アカウントでのみ可能です。
- 

[目次に戻る](#)

[目次に戻る](#)

## Dell Management Console への移行

Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [Dell Management Console の移行に関する備考](#)
- [Dell Management Console バージョン 2.0 への移行](#)

本項では、32 ビット Windows 2003 R2 オペレーティングシステム用の Dell Management Console バージョンを今回の 64 ビット Windows 2008 R2 オペレーティングシステム用の Dell Management Console リリースに移行する方法について説明します。

 **メモ:** Dell Management Console 2.0 に移行してから、Dell Management Console 2.0.2 にアップグレードする必要があります (Dell Management Console 2.0.2 への直接移行はサポートされていません)。Windows Server 2008 R2(64 ビット)SP1 には直接移行できません。Dell Management Console 2.0.2 バージョンに移行してから、オペレーティングシステムを SP1 にアップグレードする必要があります。

### Dell Management Console の移行に関する備考

- 1 Dell Management Console バージョン 1.x を Dell Management Console バージョン 2.0 に移行した後の OpenManage 展開タスクについて、既存の OpenManage Server Administrator パッケージを使用すると、「The installation package could not be modified. (インストールパッケージを変更できませんでした。)」というエラーメッセージが表示されます。回避策として、移行後に Dell Management Console に保存および展開された OpenManage Server Administrator パッケージを使用してください。
- 1 [Symantec Installation Manager を使用した移行](#)またはデータベース移行方法を使用して、Dell Management Console バージョン 1.x から Dell Management Console バージョン 2.0 に移行する場合は次のとおりです。移行プロセスによって Dell Management Console 2.0 に存在しないソリューションがインポートされると、Notification Server アップグレードウィザードの「Unable to get product details for the specified product (Product Guide: ...) (指定された製品の製品詳細を取得できません(製品ガイド: ...))」というインポートエラーが Altiris Log Viewer に表示されます。回避策として、適切なソリューションが Dell Management Console バージョン 2.0 と共にインストールされていることを確認します。
- 1 Windows 2008 R2 サーバーにインストールされた Dell Management Console バージョン 2.0 の使用時に 64 ビットプラットフォーム対応の移行実行可能ファイル (Dell\_Migration\_Package\_\*\_x64.exe) を実行し、**NSUpgrade Setup**(NSUpgrade セットアップ)で **Repair**(修復)を選択すると、エラーメッセージが表示されます。回避策として、Upgrade(アップグレード)フォルダから 64 ビット移行実行可能ファイルを実行します。

### Dell Management Console バージョン 2.0 への移行

Dell Management Console バージョン 1.1.0 および 1.1.x から Dell Management Console バージョン 2.0 にデータベースを移行するには、次のいずれかの方法を使用できます。

- 1 Symantec Installation Manager
- 1 データベース移行方法

#### 必要条件

Symantec Installation Manager またはデータベースを使用して移行するには、次のものがが必要です。

- 1 Dell Management Console バージョン 1.1 のインストール
- 1 Dell Management Console バージョン 2.0 をインストールするための最小要件を満たすシステム。

### Symantec Installation Manager を使用した移行

Symantec Installation Manager を使用して Dell Management Console に移行するには、次の手順を実行します。

1. [Dell Management Console バージョン 1.1 または 1.1.x データベースのバックアップ](#)
2. [Dell Management Console バージョン 1.1 または 1.1.x データベースの復元](#)
3. [データベース所有者のセットアップ](#)
4. [Dell 管理コンソールのインストール](#)
5. [Symantec Installation Manager の移行方法に対するローカルまたはリモートの SQL Server の使用](#)
6. [NS アップグレードウィザードを使用した CM/KMS キーのエクスポートおよびインポート](#)

### データベースを使用した移行

データベースを使用して Dell Management Console に移行するには、次の手順を実行します。

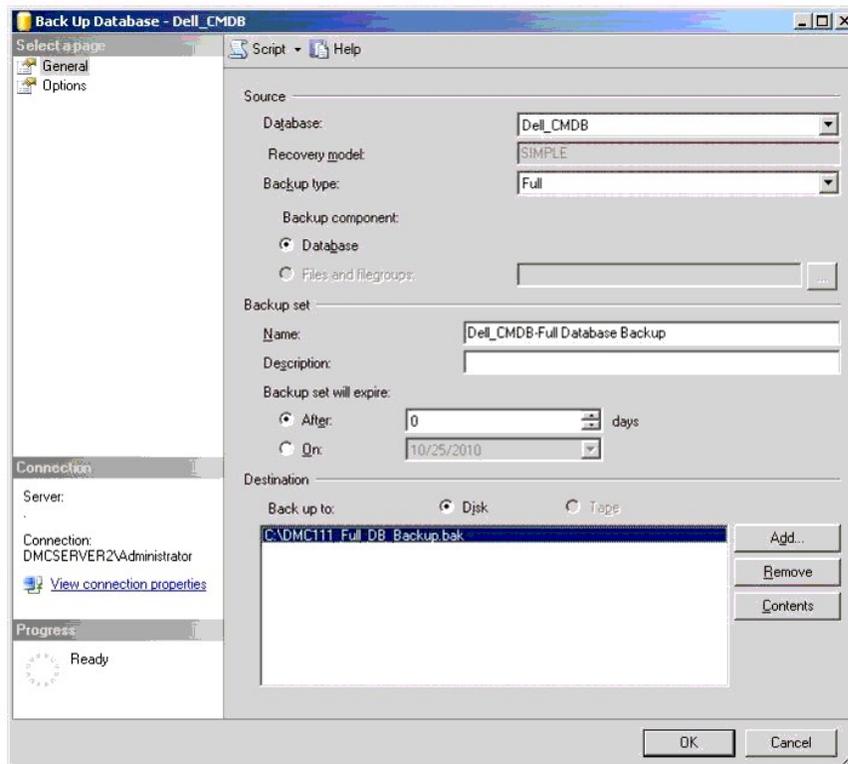
1. [Dell Management Console バージョン 1.1 または 1.1.x データベースのバックアップ](#)
2. [Dell Management Console バージョン 1.1 または 1.1.x データベースの復元](#)
3. [データベース所有者のセットアップ](#)
4. [Dell 管理コンソールのインストール](#)
5. [データベースの設定](#)
6. [NS アップグレードウィザードを使用した CM/KMS キーのエクスポートおよびインポート](#)

## Dell Management Console バージョン 1.1 または 1.1.x データベースのバックアップ

Dell Management Console バージョン 1.1 または 1.1.x データベースをバックアップするには、次の手順を実行します。

1. Microsoft SQL Server Management Studio で、Dell Management Console database(Dell Management Console データベース)を選択し、右クリックして Tasks(タスク)→ Back Up (バックアップ)と選択します。

Back Up Database(データベースのバックアップ)画面が表示されます。



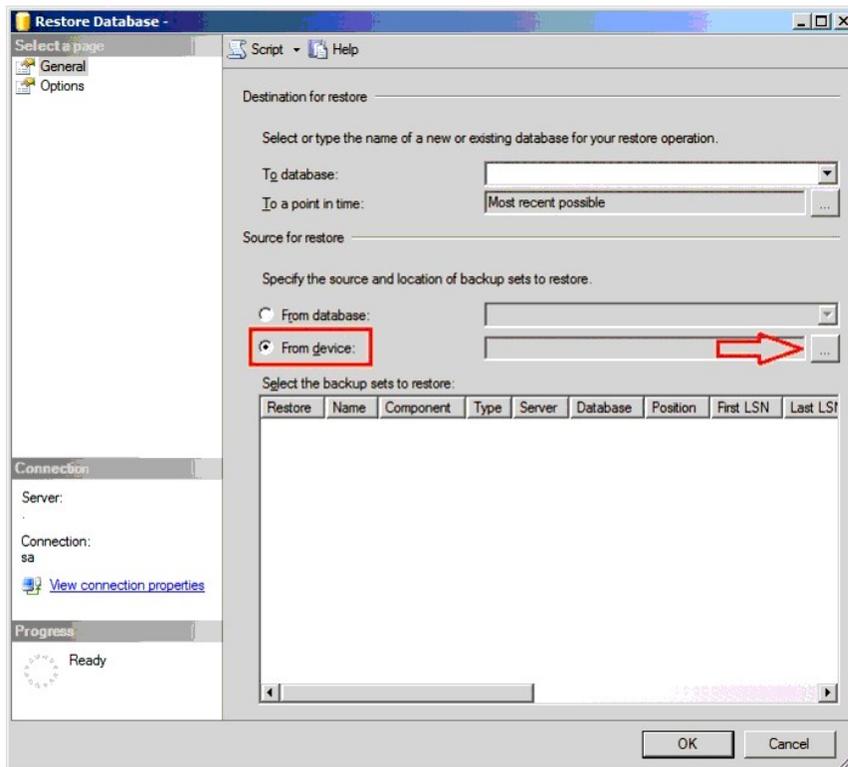
2. データベースバックアップファイルの場所を確認し、OK をクリックします。
3. database back-up result(データベースのバックアップ結果)で OK をクリックします。

## Dell Management Console バージョン 1.1 または 1.1.x データベースの復元

Dell Management Console バージョン 1.1 または 1.1.x データベースを復元するには、次の手順を実行します。

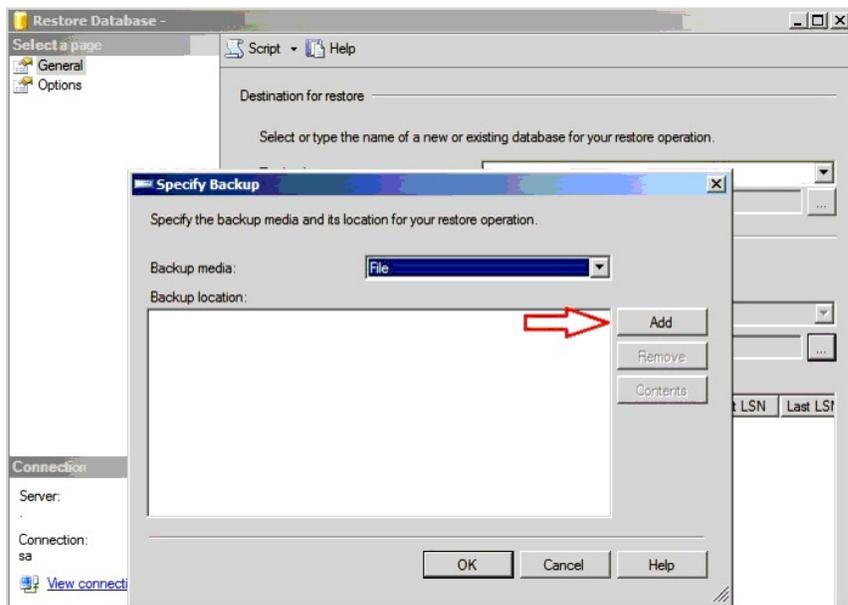
1. Microsoft SQL Server Management Studio で Database(データベース)を選択し、右クリックして Restore Database(データベースの復元)を選択します。

Restore Database(データベースの復元)画面が表示されます。

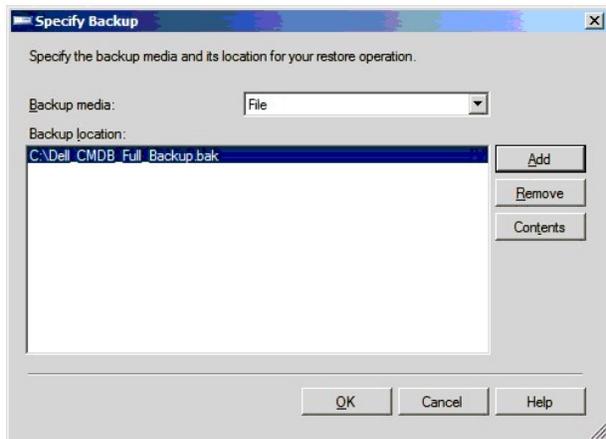


2. From device(デバイスから)を選択し、(...)をクリックします。

Specify Backup(バックアップの指定)画面が表示されます。



3. **Backup media** (バックアップメディア) ドロップダウンリストから **File** (ファイル) を選択し、**Add** (追加) をクリックします。
4. **Locate Backup File** (バックアップファイルの検索) で、Dell Management Console バージョン 1.1 または 1.1.x バックアップファイルを選択し、**OK** をクリックします。



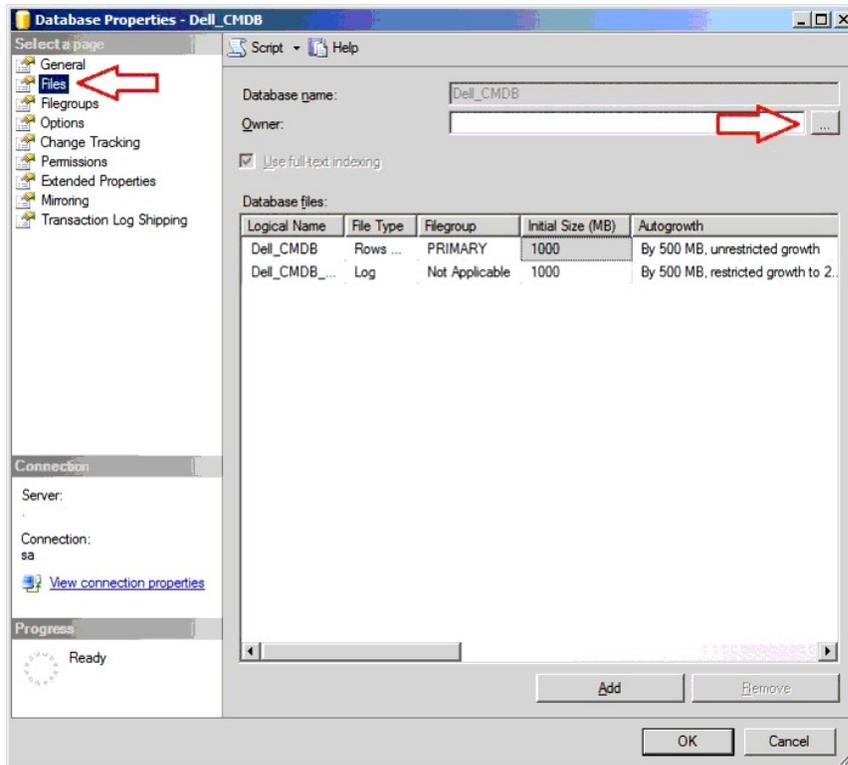
5. **Specify Backup** (バックアップの指定) 画面の **Backup location** (バックアップの場所) の下に選択したファイルが表示されます。**OK** をクリックします。
6. **Restore Database** (データベースの復元) で **OK** をクリックします。
7. **database back-up restore result** (データベースバックアップの復元結果) で **OK** をクリックします。

Dell Management Console が復元されます。

## データベース所有者のセットアップ

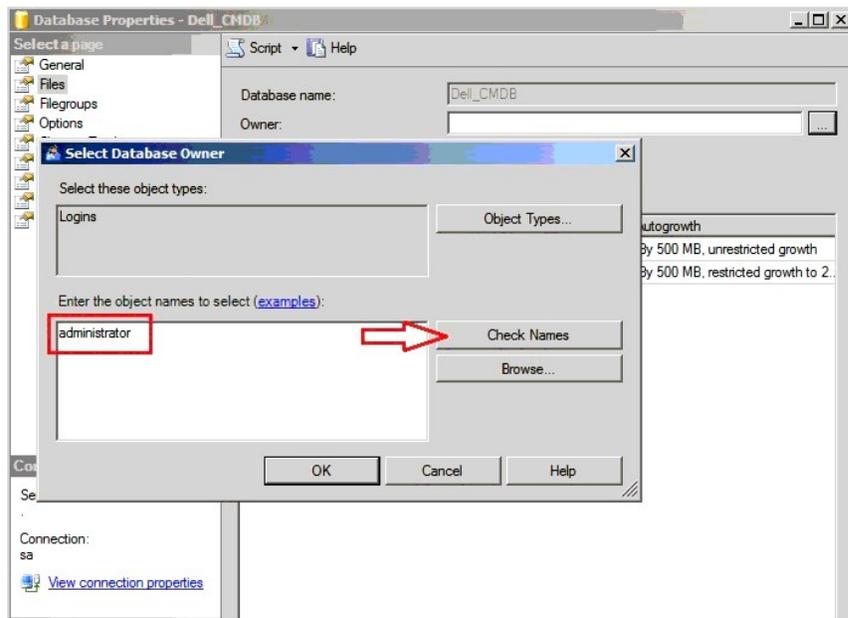
ローカル管理者アカウントをデータベース所有者としてセットアップするには、次の手順を実行します。

1. **Microsoft SQL Server Management Studio** で、Dell Management Console database (Dell Management Console データベース) を選択し、右クリックして **Properties** (プロパティ) を選択します。  
**Restore Properties** (データベースのプロパティ) 画面が表示されます。



2. Files(ファイル)をクリックしてから、(...)をクリックします。

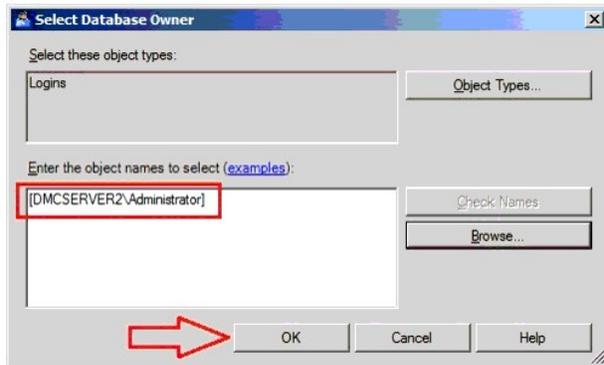
Select Database Owner(データベースの所有者の選択)画面が表示されます。



3. Check Names(名前の確認)をクリックします。

4. **Multiple Objects Found** (複数のオブジェクトが見つかりました) で、管理者ユーザーを選択し、**OK** をクリックします。
5. **object names** (オブジェクト名) の下で管理者ユーザーをチェックし、**OK** をクリックします。
6. **Database Properties** (データベースのプロパティ) で、**OK** をクリックします。

ローカル管理者アカウントがデータベース所有者として設定されました。



## Symantec Installation Manager の移行方法に対するローカルまたはリモートの SQL Server の使用

Dell Management Console バージョン 1.1 または 1.1.x データベースの移行に Symantec Installation Manager を使用する場合は、この方法を使用します。

Symantec Installation Manager の移行方法に SQL Server を使用するには、次の手順を実行します。**Database Configuration** (データベースの設定) の **SQL Server name** (SQL Server 名) に、SQL Server の名前または IP アドレスを入力し、**Use existing** (既存のものを使用) を選択した後、**Database name** (データベース名) から復元したデータベースを選択します。

## NS アップグレードウィザードを使用した CM/KMS キーのエクスポートおよびインポート

Altiris Notification Server 移行ウィザードを使用して CM/KMS キーをエクスポートするには、次の手順を実行します。

1. Dell Management Console 2.0 をインストールした後、`C:\Program Files\Dell\ysmgmt\dmcs\Symantec Installation Manager\Migration Package` から、32 ビット移行パッケージを Dell Management Console バージョン 1.1 または 1.1.x システムにコピーします。
2. Altiris Notification Server 移行ウィザードをインストールして、CM/KMS キーをデータストアファイル(.adb)にエクスポートします。
3. Altiris Notification Server 移行ウィザードを実行します。
4. **Export / Import Task Selection** (エクスポート / インポートタスクの選択) で、**Export data from an Altiris Notification Server to a file store** (データを Altiris Notification Server からファイルストアにエクスポート) を選択し、**Browse** (参照) をクリックしてファイルのエクスポート先を選択したら、**Next** (次へ) をクリックします。
5. **Exporter Configuration** (エクスポートの設定) で、**Next** (次へ) をクリックします。

データは、Dell Management Console 1.x システムのデータストアファイル(.adb)にエクスポートされます。

6. エクスポートされたデータストア(.adb)ファイルを Dell Management Console 1.x システムから Dell Management Console 2.0 システムにコピーして、CM/KMS キーをインポートします。このファイルは、`Program Files\Dell\ysmgmt\dmcs\Upgrade\Data` に作成されます。

Altiris Notification Server 移行ウィザードを使用して CM/KMS キーをインポートするには、次の手順を実行します。

1. Dell Management Console 2.0 がインストールされたシステムで、`C:\Program Files\Dell\ysmgmt\dmcs\Symantec Installation Manager\Migration Package` から Altiris Notification Server 移行ウィザードを実行します。
2. **Export / Import Task Selection** (エクスポート / インポートタスクの選択) で **Import data from a file store into an Altiris Notification Server** (データをファイルストアから Altiris Notification Server にインポート) を選択し、**Browse** (参照) をクリックして Dell Management Console 1.x システムから Dell Management Console 2.0 システムにコピーしたファイルを選択したら、**Next** (次へ) をクリックします。
3. **Importer Configuration** (インポートの設定) で、**Next** (次へ) をクリックします。

 **メモ:** Notification Server 移行ウィザードの Data Store (データストア) に表示されるデフォルトの場所を使用しないでください。

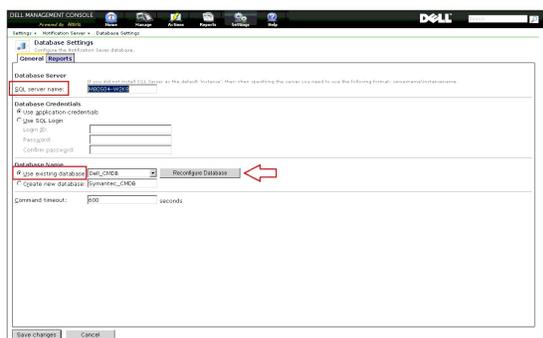
データストア(.adb)ファイルは、Dell Management Console 2.0 がインストールされたシステムにインポートされます。

## データベースの設定

データベースを設定するには、次の手順を実行します。

1. Dell Management Console から、**Settings**(設定)→**Notification Server**→**Database Settings**(データベース設定)を選択します。

**Database Settings**(データベースの設定)画面が表示されます。



2. バックアップおよび復元した Dell Management Console 1.1 または 1.1.1 データベースを選択し、**Reconfigure Database**(データベースの再設定)をクリックします。

 **メモ:** 500 MB のデータベースを再設定するには、30 分以上かかる場合があります。

3. データベースを再設定した後は、**Save Changes**(変更の保存)をクリックします。

## 移行後

移行が完了したら、次の操作を実行します。

1. Altiris Agent が管理対象システムにインストールされている場合、このエージェントは移行後に以前の Dell Management Console 1.x サーバーにアクセスしようとします。このため、これらの管理対象ノードでは、クライアントタスクやハードウェアアップデート(Dell バッチ)を実行できません。エージェントが現在のサーバーにアクセスできるようにするには、**Action**(操作)→**Agents/Plug-ins**(エージェント / プラグイン)→**Push Altiris Agent**(Altiris Agent のプッシュ)を選択し、Dell Management Console 2.x システムからそれぞれの管理対象ノードに Altiris Agent をプッシュします。
2. SNMP を設定します。たとえば、SNMP トラップ宛先アドレスは、特定のホストからパケットを受け入れます。
3. 移行後、Altiris Agent がインストールされていない管理対象ノードは、以前の Dell Management Console 1.x タスクサーバーに割り当てられます。このため、これらの管理対象ノードに対して Dell タスクを実行できません。管理対象ノードが現在のタスクサーバーにアクセスできるようにするには、**Settings Notification Server Task**(Notification Server の設定タスク)の **Settings**(設定)メニューから **Update Task Service Assignments**(タスクサービスの割り当てのアップデート)タスクを実行します。

 **メモ:** このタスクを手動で実行しない場合でも、デフォルトで毎日午前 2 時に実行されます。

4. カスタムプロキシが設定されている場合、Altiris Agent はタスクサーバーに登録されない可能性があります。登録を有効にするには、Internet Explorer ウェブブラウザで **Tools**(ツール)→**Internet Options**(インターネットオプション)→**Connections**(接続)→**LAN settings**(LAN の設定)を選択します。Advanced(詳細設定)をクリックし、Exceptions(例外)に次のアドレスを追加します。
  - 1 http://<localhost>/
  - 1 http://<Hostname of Dell Management Console system>
5. Dell Management Console 1.x サーバーで **DUP Catalog Import**(DUP カタログのインポート)と **Inventory Collector Import**(インベントリコレクタのインポート)が実行されている場合、関連するファイルは Dell Management Console 2.0 サーバーに移行されません。したがって、バッチ管理タスクは正常に機能しません。

移行後に、Dell Management Console 2.0 サーバーで **DUP Catalog Import**(DUP カタログのインポート)タスクと **Dell Inventory Collector Import**(Dell インベントリコレクタのインポート)タスクを実行してください。

[目次に戻る](#)

[目次に戻る](#)

## 監視と警告

### Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [監視について](#)
- [監視と警告のユーザーインターフェイス](#)
- [依存関係](#)
- [監視と警告ソリューションのライセンスに関する制限事項](#)
- [パフォーマンスの監視](#)
- [監視ポリシーの有効化](#)
- [メトリクスの変更](#)
- [パフォーマンスビューア](#)
- [正常性の監視](#)
- [OnDemand 監視](#)
- [クライアントアップデート自動化ポリシー](#)
- [異なるしきい値を持つ各種デバイスを監視するためのポリシーの複製](#)
- [サーバー監視警告の管理](#)

Dell Management Console は、ネットワーク上の管理対象デバイスと通信して、**正常性とパフォーマンス**のデータを収集します。監視と警告モジュールは、システムのリアルタイムの正常性、パフォーマンス、および電力消費を監視するための主要インターフェイスです。この機能では、Simple Network Management Protocol(SNMP)、Common Information Model(CIM)、および Intelligent Platform Management Interface(IPMI)などの各種プロトコルを使用して管理対象デバイスと通信します。

 **メモ:** Dell Management Console に監視と警告を設定すると、新規の設定がアクティブになるまで追跡は開始されません。

#### Dell OpenManage Storage Management に関する注意事項

- 1 サーバーに接続されたストレージのファームウェアが古い場合、Dell Management Console のストレージコントローラコンポーネントの状態に Warning(警告)状態が表示されます。ストレージコントローラコンポーネントの状態の詳細については、「OpenManage Server Administrator」を参照してください。
- 1 OpenManage Storage Management で仮想ディスクが削除されるか、物理ディスクが取り外されると、監視エージェントが再起動されたときや、デバイスセッションが更新されたときのみ、Dell Management Console で変更が反映されます(デフォルトでは、デバイスセッションは 1 時間に 1 回更新されます)。
- 1 管理情報ベース(MIB)では、コンポーネントとロールアップの状態がサポートされます。コンポーネント状態は、子要素のロールアップ状態のいずれとも別個に扱われる要素の状態です。ロールアップ状態は、要素とその子の最悪のケースの状態です。次に示すように、OpenManage Storage Management と Dell Management Console では、これらの状態が表示されるインターフェイスと要件が異なります。
  - OpenManage Storage Management ユーザーインターフェイスには、ロールアップ状態だけが表示されます。これは、考えられる問題を判断するために階層全体にドリルダウンすることなく、異常な状態であることを判断できるようにするために特に必要です。
  - Dell Management Console には、コンポーネント状態が表示されます。Dell Management Console は、フラットなビューでデバイスを監視し、そこでは異常な状態のコンポーネントをすべて一度に確認できます。いずれの要素のコンポーネント 状態も引き上げないようすることが非常に重要です。状態引き上げるとコンポーネントが不良と見なされることがありますが、状態の変化はロールアップ 状態によるものである可能性があります。したがって、Dell Management Console と OpenManage Server Administrator ユーザーインターフェイスのストレージドリルダウン状態は必ずしも一致しません。
- 1 さまざまな OpenManage のバージョンでサポートされるカウンタの違いによるエラーを防止するため、ハードウェアでサポートされる最新の OpenManage バージョンを使用してください。
- 1 別のインスタンスが異常な状況になると、1 つのカウンタのすべてのインスタンスが 1 つの警告を共有し、新しい警告は生成されません。たとえば、4 つの温度プローブがあり、1 つのプローブが警告状態になったために警告を受信した場合、別の温度プローブが警告状態になっても、新しい警告は生成されません。
- 1 プローブインスタンスの名前は、OpenManage Server Administrator ユーザーインターフェイスと Dell Management Console ユーザーインターフェイスで一致しない場合があります。

## 監視について

監視ソリューションを使用すると、監視ポリシーで定義されているエージェントベースまたはエージェントレスのインターフェイスを通じて、検出されたデバイスをリアルタイムで監視できます。

 **メモ:** Dell Management Console では、**エージェントベース**とは Altiris Agent がターゲットシステムにインストールされていることを意味し、**エージェントレス**とは Dell システム管理エージェント(Dell OpenManage Server Administrator)がターゲットシステムにインストールされていることを意味します。

 **メモ:** Symantec Inc. が Altiris Inc. を買収したため、本書では、Altiris と Symantec への参照が混用されていることがあります。

ポリシーは、ルールのセットと、それらのルールを実行するターゲットグループを定義します。ルールは、監視するデータと、警告を発する条件または何らかの措置を取る条件を定義します。メトリクスは、監視するデータ、およびデータを取得するポーリング間隔を定義します。Dell ポリシーは、Dell ハードウェアの正常性およびパフォーマンスを監視できるよう、メトリクス、ルール、およびポリシーを定義します。

 **メモ:** 監視ソリューションの詳細については、Symantec のユーザーズガイドを参照してください。

表 11-1. Dell ポリシーの説明

Dell ポリシー	説明	エージェントベース / エージェントレス	サポート範囲	デフォルト動作	デフォルトのポーリング間隔
Device Primary Health(デバイスのプライマリ正常性)	プライマリデバイスの正常性を監視します(Dell OpenManage Server Administrator は、この情報を Dell サーバーに提供します。その他すべてのデバイスについては、埋め込みエージェントがこの情報を提供します)。	エージェントレス	すべての Dell デバイス	有効	1 時間
Device Agent Health-Dell Remote Access Controller In-Band(デバイスエージェントの正常性 - 帯域内の Dell Remote Access Controller)	帯域内の Dell Remote Access Controller(DRAC)の正常性を監視します。	エージェントレス	DRAC 搭載の Dell サーバー	有効	1 時間

Device Agent Health-Dell OpenManage Storage Management(デバイスエージェントの正常性 - Dell OpenManage Storage Management)	Dell OpenManage Storage Management の正常性を監視します。	エージェントレス	Storage Management 搭載の Dell サーバー	有効	1 時間
Device Connection State(デバイス接続状態)	デバイス接続状態を監視します。	エージェントレス	すべての Dell デバイス	有効	1 時間
Performance Monitoring for Microsoft Windows(Microsoft Windows のパフォーマンス監視)	Windows パフォーマンスカウンタを監視します。	エージェントレス	サポート対象の Windows オペレーティングシステムを搭載した Dell サーバー	無効	2 分
Performance Monitoring for Linux(Linux のパフォーマンス監視)	Linux パフォーマンスカウンタを監視します。	エージェントベース	サポート対象の Windows オペレーティングシステムを搭載した Dell サーバー	無効	2 分
電源監視	Dell サーバーを監視します	エージェントレス	OpenManage Server Administrator 搭載の Dell サーバー	無効	1 時間

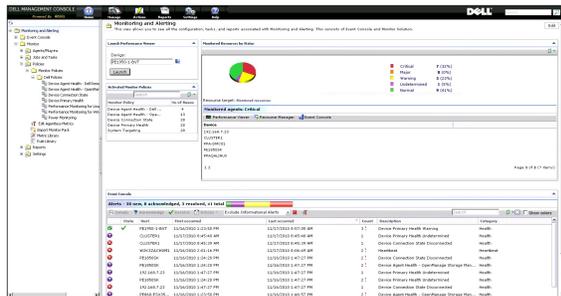
**メモ:** 正常性ポリシーはすべてデフォルトで有効になりますが、パフォーマンスと電力のポリシーは有効にする必要があります。履歴ビューおよびリアルタイムビューには、有効なポリシーだけが表示されます。

**メモ:** 監視のポーリング時間は、メトリクスベースで定義されます。ただし、ポリシーのすべてのメトリクスのデフォルトポーリング時間は同じです。

## 監視と警告のユーザーインターフェイス

監視と警告モジュールにアクセスするには、Home(ホーム)→Monitoring and Alerting(監視と警告)をクリックします。

### 監視と警告のユーザーインターフェイスについて



左側のペインには、Monitoring and Alerting(監視と警告)ツリーが表示されます。このツリーから Metrics Library(メトリクスライブラリ)、Rule Library(ルールライブラリ)、Reports(レポート)、および Settings(設定)のポリシーにアクセスできます。

右側のペインには、ユーザーインターフェイスのウェブパーツが表示されます。このペインから、次のタスクを実行できます。

- 1 パフォーマンスビューを起動する。
- 1 アクティブ化したポリシーを表示する。
- 1 リソースを状態別に監視する。
- 1 現在受信済みの警告が表示されるイベントコンソールを表示する。

## 依存関係

監視と警告ソリューションは、さまざまな要因に依存しています。表 11-2 に、これらの要因の詳細を示します。

表 11-2. 監視ソリューションの依存関係

依存関係	説明
デバイスエージェント	正常性の監視では、プロトコル経由でデータを提供するために、監視下デバイス上にエージェントが必要です。たとえば Dell サーバーでは、サーバーを監視し、そのプ

	ライマリ正常性状態を取得するには、Server Administrator がインストールされている必要があります。同様に、プリンタには、その正常性を監視するため、SNMP をサポートする埋め込みエージェントが必要です。
プロトコルのサポート	Dell 監視メトリクスはスマートメトリクスであり、プロトコルに依存します。これらのメトリクスは、SNMP、WMI、WS-MAN、IPMI、NaviCII、Symbol、および Linux コマンドなどのプロトコルやインタフェースから 1 つまたは複数によるサポートを必要とします。 <a href="#">接続プロファイルと資格情報管理</a> を参照してください。
検出ソリューション	監視するデバイスは、検出され、Dell デバイスとして分類する必要があります。検出ソリューションは、エージェントバージョンおよび製造元のデータを収集します。このデータは、 <b>リソースマネージャ</b> ビューでエージェントの正常性を表示するときに使用されます。  <b>メモ:</b> デバイスは、検出で使用されたプロトコルのみによって監視できます。  <b>メモ:</b> デバイスを監視するには、デバイスが Dell デバイスとして分類されている必要があります。たとえば、 <b>Dell コンピュータ</b> や <b>Dell プリンタ</b> などです。
イベントソリューション	イベントコンソールには、Dell Management Console によって受信されたすべての SNMP トラップと監視警告が表示されます。 <b>Managed Resources by Status</b> (状態別の管理対象リソース)、 <b>Group View</b> (グループビュー)、および <b>Resource Manager Health View</b> (リソースマネージャ正常性ビュー) などの各種ウェブパーツでは、監視警告を使用してデバイスの正常性を計算します。また、SNMP トラップは「 <b>OnDemand 監視</b> 」機能も推進します。
レポートソリューション	レポートソリューションは、Dell の監視ベースのレポートをインストールします。
Dell Management Console のホームページ	ホームページには <b>Group Health View</b> (グループ正常性ビュー) があります。これは、デバイスの正常性状態を表示する主要インタフェースです。
Dell ライセンス	Dell ライセンスはデフォルトのライセンスであり、Dell デバイスを監視するために必要です。また、Dell ライセンスによって、既存のポリシーを制限付きでカスタマイズできます。ただし、新しいポリシーを作成することはできません。
無制限ライセンス	無制限ライセンスはフルライセンスであり、既存の監視ポリシーの完全な変更およびユーザー定義ポリシーの作成を行うことができます。このプラグインは Symantec から購入できます。
Altiris Agent for Linux	Linux パフォーマンスの監視に必要です。
Linux Monitor Agent	Linux パフォーマンスの監視に必要です。

## 監視と警告ソリューションのライセンスに関する制限事項

Dell Management Console には、監視と警告ソリューションで使用できる機能に影響を及ぼす制限付きのライセンスがあります。このライセンスを使用すると、Dell デバイスのみでポリシーを実行したり、ポリシーを制限付きで変更したりできます。

ただし、無制限ライセンスや追加の監視パックを購入すると、Dell ポリシーに設定されているすべての機能を利用できます。

### 制限付きの Dell ライセンス

このライセンスでは、次のタスクを実行できません。

- 1 メトリクスの作成。
- 1 ルールの作成。
- 1 メトリクスの複製。
- 1 次の例外を除くメトリクスまたはルールの変更。

メトリクスに対しては、次の操作を実行できます。

- 1 メトリクスのポーリング間隔の変更。
- 1 メトリクスタイムアウトの変更。
- 1 メトリクスの有効化または無効化。

ルールに対しては、次のタスクを実行できます。

- 1 ルールの条件の変更。
- 1 ルール値タイプの変更。
- 1 ルール値の変更。
- 1 ルールの繰り返し回数の変更。
- 1 ルールのオーバータイム値の変更。
- 1 ルールの状況属性の変更。
- 1 ルールのアクション属性の変更。
- 1 ルール、パック、およびカテゴリの有効化または無効化。
- 1 ルールの複製。

ポリシーに対しては、次のタスクを実行できます。

- 1 ポリシーターゲットの変更。
- 1 ポリシーに対するルールの追加または削除。

- 1 ポリシーの複製。

## パフォーマンスの監視

パフォーマンスの監視を利用すると、サポートされている Microsoft Windows および Linux のオペレーティングシステム全体で標準セットのパフォーマンスカウンタを監視できます。

## パフォーマンス監視の依存関係

表 11-3. パフォーマンス監視の依存関係

Dell ポリシー	エージェント / エージェントレス	サポート範囲	デフォルト動作	依存関係
Windows のパフォーマンス監視	エージェントレス	サポート対象の Windows オペレーティングシステムを搭載した Dell サーバー	無効	WMI プロトコル、Windows 2003 以降
Linux のパフォーマンス監視	Altiris Agent	サポート対象の Windows オペレーティングシステムを搭載した Dell サーバー	無効	glibc 2.2 以降、sysstat、Linux エージェント、および監視エージェント  <b>メモ:</b> 監視ソリューションの詳細については、Symantec のユーザーズガイドを参照してください。

## Linux パフォーマンス監視用の Sysstat のインストール

次のコマンドを入力して、このライブラリの rpm がすべてに Linux サーバーに存在することを確認してください。

```
rpm -qa | grep sysstat
```

rpm が存在する場合は、次のコマンドを実行してライブラリをインストールします。

```
rpm -i <package name>
```

ライブラリまたは rpm が Linux サーバーに存在しない場合は、次の場所からダウンロードしてください。

[pagesperso-orange.fr/sebastien.godard/](http://pagesperso-orange.fr/sebastien.godard/)

Linux オペレーティングシステムメディアで rpm を検索することもできます。

rpm を Linux サーバーにダウンロードし、前述のとおり rpm をインストールします。

 **メモ:** sysstat ソースはコンパイルしないことを強くお勧めします。

## パフォーマンスのメトリクス

パフォーマンスメトリクスは、Windows および Linux オペレーティングシステムと同じタイプのカウンタに基づいています。

表 11-4. パフォーマンスのメトリクス

メトリクス(合計カウン ト = 単純 + 複合)	説明
<b>CPU</b>	
%Kernel Utilization Time(%カーネル使用時間)	プロセスのスレッドが特権モードでコードを実行するときに費やした経過時間の割合をパーセントで示します。Windows システムサービスは呼び出されると、システム専用データにアクセスするために特権モードで実行されることがあります。これらのデータは、ユーザーモードで実行中のスレッドがアクセスできないように保護されます。システムの呼び出しは、明示的な場合と、またはページフォルトや割り込みのように暗黙的な場合があります。以前のオペレーティングシステムとは異なり、Windows では、ユーザー モードおよび特権モードの従来の保護に加え、プロセス境界を使用してサブシステムを保護します。Windows は、プロセスの特権時間だけでなく、その他のサブシステムプロセスに表示される可能性のある一部の作業をアプリケーションの代わりに実行します。
%プロセッサ使用時間	プロセッサが非アイドルのスレッドを実行するために費やす経過時間の割合をパーセントで示します。この値は、サンプリング期間においてアイドルスレッドがアクティブである期間を測定し、その期間をサンプリング期間から差し引くことによって計算されます (各プロセッサには、実行するスレッドがほかにない場合にサイクルを消費するアイドル状態のスレッドがあります)。このカウンタは、プロセッサのアクティビティを示す主要なインジケータです。
%User Utilization Time(%ユーザー使用時間)	プロセッサがユーザー モードで費やす経過時間の割合をパーセントで示します。ユーザーモードは、アプリケーション、環境サブシステム、および一体型サブシステム用に設計された制限付きの処理モードです。  また、特権モードは、オペレーティングシステムコンポーネント用に設計されており、ハードウェアおよびすべてのメモリに直接アクセスできます。オペレーティングシステムは、オペレーティングシステムサービスにアクセスするため、アプリケーションスレッドを特権モードに切り替えます。このカウンタには、平均ビジー時間がサンプリング時間の割合として表示されます。
<b>Logical Disk(論理ディスク)</b>	

Logical Disk Free Space(論理ディスクの空き領域)	選択した論理ディスクドライブの使用可能な空き領域の合計の割合をパーセントで示します。
Logical Disk IO/Sec(論理ディスク IO / 秒)	ディスク上の読み取りおよび書き込み操作の比率。
<b>Memory(メモリ)</b>	
% Page File Usage(%ページファイル使用率)	Memory\Committed Bytes の Memory\Commit Limit に対する比率です。コミットされたメモリとは、ディスクへの書き込みが必要になった時のためにページングファイルに領域が予約されている物理メモリです。Commit Limit は、ページングファイルのサイズによって決定します。ページングファイルが拡張されると、Commit Limit が増え、比率は小さくなります。このカウンタには、平均値ではなく現在の割合値だけが表示されます。
Available Memory(使用可能メモリ)	Memory\Available Bytes に報告されるバイト数ではなく、システムで実行中のプロセスに使用できる物理メモリのサイズをメガバイト数で示します。ゼロメモリ、空きメモリ、およびスタンバイメモリのリストに容量を追加することによって計算されます。空きメモリは使用可能なメモリです。ゼロメモリはゼロで埋められたメモリのページであり、以前のプロセスに使用されたデータが後続のプロセスで参照されないようにします。スタンバイメモリは、ディスクへのルート上でプロセスのワーキングセット(物理メモリ)から削除されたものの、再呼び出しが可能なメモリです。このカウンタには、平均値ではなく最後に観測された割合値だけが表示されます。
Pages IO/Sec(ページ IO/ 秒)	ハードページフォールトを解決するためにディスクから読み取られた、またはディスクに書き込まれたページの比率です。このカウンタは、システム全体の遅延を招くフォールトの主要インジケータです。Memory\Pages Input/ 秒と Memory\Pages Output/ 秒の合計です。ページ数がカウントされるので、カウントを変換することなく Memory\Page Faults/ 秒などの他のページカウントと比較できます。ファイルシステムキャッシュ内および非キャッシュのマップされたメモリ ファイル内のフォールトを解決するために取得されたページ(通常、アプリケーションが要求する)が含まれます。
<b>Network(ネットワーク)</b>	
Incoming Bytes/Sec(着信バイト数 / 秒)	フレーム文字を含め、各ネットワークアダプタを介して受信されるバイトの比率。Network Interface\Bytes Received/ 秒は、Network Interface\Bytes Total/ 秒のサブセットです。
Incoming Packets/Sec(着信バイト数 / 秒)	ネットワークインタフェースで受信されるパケットの比率です。
Outgoing Bytes/Sec(発信バイト数 / 秒)	フレーム文字を含め、各ネットワークアダプタを介して送信されるバイトの比率。Network Interface\Bytes Sent/ 秒は、Network Interface\Bytes Total/ 秒のサブセットです。
Outgoing Packets/Sec(発信バイト数 / 秒)	ネットワークインタフェースで送信されるパケットの比率です。
<b>Physical Disk(物理ディスク)</b>	
Average Access Time(平均アクセス時間)	ディスクの平均転送時間(秒単位)です。
Physical Disk IO/Sec(物理ディスク IO / 秒)	ディスク上の読み取りおよび書き込み操作の比率です。
<b>System(システム)</b>	
Context Switches/Sec(コンテキストスイッチ / 秒)	コンピュータ上のすべてのプロセッサがあるスレッドから他のスレッドに切り替わる場合の組み合わせの比率です。コンテキストスイッチは、実行中のスレッドが自発的にプロセッサを解放したとき、優先度の高い実行可能スレッドによって割り込まれたとき、または、Executive サービスやサブシステムサービスを使用するためにユーザーモードと特権(カーネル)モードを切り替えるときに発生します。これは、すべてのプロセッサ上で実行中のすべてのスレッドの Thread\Context Switches/ 秒の合計値で、切り替えの回数で計測されます。システムオブジェクトとスレッドオブジェクトには、コンテキストスイッチカウンタが存在します。このカウンタには、最新の 2 つサンプルで観測した値の差を、サンプル間隔の期間で割った値が表示されます。
Processor Queue Length(プロセッサキュー長)	プロセッサキュー内のスレッドの数です。ディスクカウンタとは異なり、このカウンタには実行中のスレッドではなく実行可能スレッドのみが表示されます。複数のプロセッサが搭載されたコンピュータでも、プロセッサ時間のキューは 1 つです。したがって、コンピュータに複数のプロセッサが存在する場合は、この値を、負荷を処理しているプロセッサの数で割る必要があります。負荷に応じて、1 つの持続されているプロセッサキューに対してスレッドが 10 未満であれば通常許容されます。
<b>メモ:</b> これらの定義は、Windows のパフォーマンス監視カウンタ用であり、Linux 用の定義は若干異なる場合があります。	

## パフォーマンス監視のしきい値

すべてのパフォーマンスカウンタには、デフォルトの警告と重要なしきい値があります。これらのしきい値を超えると、デバイスのロールアップ正常性に影響を及ぼす警告が生成されます。デバイスの正常性の変化は、**Group Health View**(グループ正常性ビュー)(Dell Management Console のポータルページ)で確認できます。

表 11-5. パフォーマンス監視のしきい値

メトリクス(合計カウント(単純+複合))	単位	警告しきい値	重要なしきい値	範囲
<b>CPU</b>				
%Kernel Utilization Time(%カーネル使用時間)	%	70	80	0~100
%プロセッサ使用時間	%	70	80	0~100
%User Utilization Time(%ユーザー使用時間)	%	70	80	0~100
<b>論理ディスク</b>				
<b>メモ:</b> これらのカウンタは、サポートされている Linux オペレーティングシステムを実行しているサーバーでは使用できません。				
Logical Disk Free Space(論理ディスクの空き領域)	%	20	10	0~100
Logical Disk IO/Sec(論理ディスク IO / 秒)	/ 秒	5	10	限定なし
<b>メモリ</b>				
% Page File Usage(%ページファイル使用率)	%	90	95	0~100

Available Memory(使用可能メモリ)	MB	50	20	限定なし
Pages IO/Sec(ページ IO/ 秒)	/ 秒	15	20	限定なし
<b>ネットワーク</b>				
Incoming Bytes/Sec(着信バイト数 / 秒)	バイト数 / 秒	1250000	1875000	限定なし
Incoming Packets/Sec(着信バイト数 / 秒)	パケット数 / 秒	1250	1875	限定なし
Outgoing Bytes/Sec(発信バイト数 / 秒)	バイト数 / 秒	1250000	1875000	限定なし
Outgoing Packets/Sec(発信バイト数 / 秒)	パケット数 / 秒	1250	1875	限定なし
<b>Physical Disk(物理ディスク)</b>				
Average Access Time(平均アクセス時間)	秒	1	2	限定なし
Physical Disk IO/Sec(物理ディスク IO / 秒)	/ 秒	5	10	限定なし
<b>システム</b>				
Context Switches/Sec(コンテキストスイッチ / 秒)*	/ 秒	100000	200000	限定なし
Processor Queue Length(プロセッサキュー長)		4	8	限定なし
*コンテキストスイッチは、サーバー間で異なる可能性があります。これらの値は状況に応じ、各自の判断で設定してください。				

## 監視ポリシーの有効化

- Monitoring and Alerting(監視と警告)ポータルページの左側のペインで、Monitor(監視)→Policies(ポリシー)→Monitor Policies(ポリシーの監視)→Dell Policies(Dell ポリシー)を選択し、変更するポリシーをクリックします。
  - Device Agent Health - Dell Remote Access Controller In-Band(デバイスエージェントの正常性 - 帯域内の Dell Remote Access Controller)を選択し、DRAC 搭載サーバーのエージェントの正常性を監視します。
  - Device Agent Health - OpenManage Storage Management(デバイスエージェントの正常性 - Dell OpenManage Storage Management)を選択し、OpenManage Storage Management デバイスのエージェントの正常性を監視します。
  - Performance Monitoring for Linux(Linux のパフォーマンス監視)を選択し、Linux システムのパフォーマンス監視を有効にします。
  - Performance Monitoring for Windows(Windows のパフォーマンス監視)を選択し、Windows システムのパフォーマンス監視を有効にします。
  - Device Primary Health(デバイスのプライマリ正常性)を選択し、デバイスの正常性を監視します。
  - Power Monitoring(電源監視)を選択し、電力消費の監視を有効にします。
- On/Off(オン / オフ)ドロップダウンをクリックし、On(オン)を選択します。
- Save Changes(変更の保存)をクリックします。
- クライアントポリシーの強制アップデートを実行して(またはデフォルトのポリシーアップデート期間を待って)変更を有効にします。[クライアントポリシーアップデートの強制](#)を参照してください。

## ポーリング設定の変更

- Monitoring and Alerting(監視と警告)ポータルページの左側のペインで、Monitor(監視)→Policies(ポリシー)→Metric Library(メトリクスライブラリ)を選択します。
- 間隔を変更するメトリクスを選択し、鉛筆アイコンをクリックして編集します。
- Polling Interval(ポーリング間隔)に秒単位の時間を入力し、OK をクリックします。
- クライアントポリシーの強制アップデートを実行して(またはデフォルトのポリシーアップデート期間を待って)変更を有効にします。詳細については、[クライアントポリシーアップデートの強制](#)を参照してください。

## ルールへのタスクの追加

- Monitoring and Alerting(監視と警告)ポータルページの左側のペインで、Monitor(監視)→Policies(ポリシー)→Rule Library(ルールライブラリ)を選択します。
- タスクを追加するルールを選択します。たとえば、Device Primary Health Critical(デバイスのプライマリ正常性が重要)を選択し、鉛筆アイコンをクリックして編集します。
- ルールの編集ダイアログボックスの Actions(アクション)セクションの Tasks(タスク)の下にある黄色い星印をクリックして、新しいタスクを追加します。
- 追加するタスクを選択します。たとえば、Send E-mail(電子メールの送信)などです。
- 右側のペインで、タスクと一緒に保存する適切な詳細を入力し、OK をクリックします。

- 追加したタスクが、このルールの一部として **Tasks** (タスク) リストの下に表示されることを確認します。
- Edit Rule** (ルールの編集) ダイアログで、**OK** をクリックします。
- クライアントポリシーの強制アップデートを実行して (またはデフォルトのポリシーアップデート期間を待って) 変更を有効にします。詳細については、[クライアントポリシーアップデートの強制](#)を参照してください。

---

## メトリクスの変更

メトリクスは変更できます。

メトリクスを編集するには、次の手順を実行します。

- Monitoring and Alerting** (監視と警告) ウェブポータルページから、**Monitor** (監視) → **Policies** (ポリシー) → **Edit Agentless Metrics** (エージェントレスメトリクスの編集) を選択します。
- Agentless Metrics** (エージェントレスメトリクス) で、編集するメトリクスを選択し、鉛筆アイコンをクリックします。
- ポーリング間隔とタイムアウトに必要なアップデートを行い、**OK** をクリックします。

 **メモ:** 複数のメトリクスを選択して、ポーリング間隔とタイムアウトをアップデートできます。

- クライアントポリシーの強制アップデートを実行して (またはデフォルトのポリシーアップデート期間を待って) 変更を有効にします。[クライアントポリシーアップデートの強制](#)を参照してください。

メトリクスルールを編集するには、次の手順を実行します。

- Monitoring and Alerting** (監視と警告) ポータルページから **Monitor** (監視) → **Policies** (ポリシー) → **Rule Library** (ルールライブラリ) を選択します。
- Agentless Metrics** (エージェントレスメトリクス) で、編集するメトリクスを選択し、鉛筆アイコンをクリックします。
- ポーリング間隔とタイムアウトに必要なアップデートを行い、**OK** をクリックします。
- クライアントポリシーの強制アップデートを実行して (またはデフォルトのポリシーアップデート期間を待って) 変更を有効にします。[クライアントポリシーアップデートの強制](#)を参照してください。

スマートメトリクスを編集するには、次の手順を実行します。

- Monitoring and Alerting** (監視と警告) ポータルページから **Monitor** (監視) → **Policies** (ポリシー) → **Metric Library** (メトリクスライブラリ) を選択します。
- Agentless Metrics** (エージェントレスメトリクス) で、編集するメトリクスを選択し、鉛筆アイコンをクリックします。
- メトリクス値とスマートキー値に必要なアップデートを行い、**OK** をクリックします。
- クライアントポリシーの強制アップデートを実行して (またはデフォルトのポリシーアップデート期間を待って) 変更を有効にします。[クライアントポリシーアップデートの強制](#)を参照してください。

---

## パフォーマンスビューア

パフォーマンスビューアは、パフォーマンスカウンタやその他の監視されているデータを表示するためのリアルタイムインタフェースを提供します。**Actions** (アクション) → **Monitor** (監視) → **Real-time...** (リアルタイム...) を選択し、デバイスを選択することによって、このデータをリアルタイムで表示できます。履歴データを表示するには、**Actions** (アクション) → **Monitor** (監視) → **Historical...** (履歴...) をクリックし、デバイスを選択します。

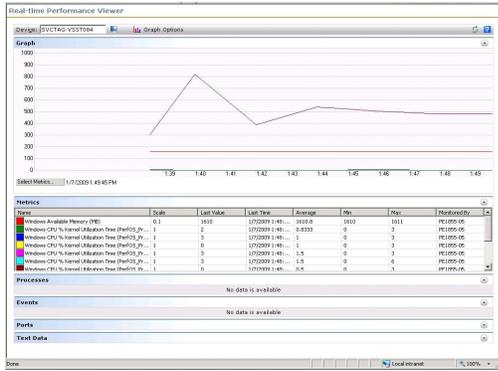
このインタフェースの起動と表示の詳細については、**Help** (ヘルプ) → **Documentation Library** (マニュアルライブラリ) にある Symantec のマニュアルを参照してください。

### Dell OpenManage Server Administrator に関するメモ

- パフォーマンスビューアで使用できる機能は、OpenManage Server Administrator で使用できる機能とは異なります。
- パフォーマンスビューアのグラフを起動すると、OpenManage Server Administrator メトリクスにデバイスのプライマリ正常性状態とデバイス接続状態が表示されます。その他の OpenManage Server Administrator メトリクスも値が 99 に設定された状態で起動します。

### Dell OpenManage Storage Management に関するメモ

- サーバーがストレージに接続され、すでに 2 つの仮想ディスクが作成されており、サーバーが Dell Management Console で検出されている場合、パフォーマンスビューアにはストレージ仮想ディスクコンポーネントの 2 つのプロープが表示されます。OpenManage Server Administrator を使用して別の仮想ディスクが作成された場合、それらの変更は監視サービスを再起動するか、デバイスを再検出した場合のみ Dell Management Console に表示されます。



## 正常性の監視

正常性の監視は、検出されたすべての Dell デバイスの正常性と接続状況を監視するための共通のインタフェースを提供します。正常性の監視には、プライマリデバイスの正常性、エージェントの正常性、およびデバイス接続状況が含まれます。デバイスの正常性は Symantec Notification Server に伝達され、Dell Management Console ホームページのロールアップビューに表示されます。また、デバイスの Resource Manager (リソースマネージャ)ポータルページのドリルダウンビューを介して、デバイスの正常性を表示することもできます。パフォーマンスビューにデバイス正常性を表示すると、Metrics (メトリクス) ウェブパーツに数値が表示されます。表 11-6 では、これらの値について説明します。

表 11-6. 最後の値の説明

値	状況
0	正常
10	不明
20	情報
30	警告
40	メジャー
50	重要
99	切断
1	電源オフ

**メモ:** デバイスが電源オフのときに帯域外インタフェースからデバイス状態を取得できる Dell Remote Access Controller (DRAC) などのデバイスを除き、ほとんどの場合は切断状態と電源オフ状態は区別できません。

正常性の監視ポリシーはすべてエージェントレスであり (デバイスへの Altiris Agent のインストールが不要)、デフォルトで有効になります。

ルールは、正常性状況のいずれかが変化したときに警告がトリガーされるように定義されています。

## 正常性の監視の依存関係

表 11-7. 正常性の監視の依存関係

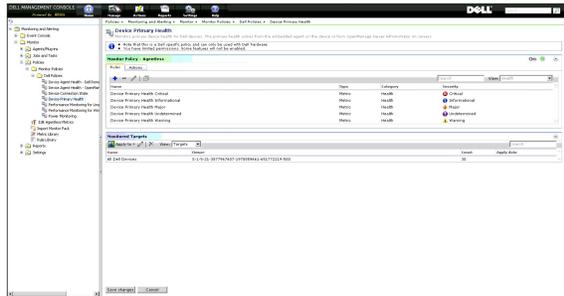
依存関係	説明
Dell OpenManage Server Administrator	Dell サーバーの正常性を管理するには、Server Administrator が必要です。また、Server Administrator をインストール中に、Storage Management と Dell Remote Access Controller をインストールするように選択できます。
SNMP	SNMP は、ほとんどのネットワークデバイスの監視に使用できる唯一のプロトコルです。
Navisphere CLI (NaviCLI)	EMC デバイスの正常性を監視するには、NaviCli が必要です。 Navisphere CLI の最新のソフトウェアおよびユーザーマニュアルについては、powerlink.emc.com を参照してください。
Symbol	Dell PowerVault MD 3000 アレイの正常性を監視するには、Symbol が必要です。
WMI、IPMI	これらのプロトコルは、サーバーの正常性を取得するために SNMP のほかに任意で使用できます。

## 正常性ポリシー

表 11-8. 正常性ポリシー

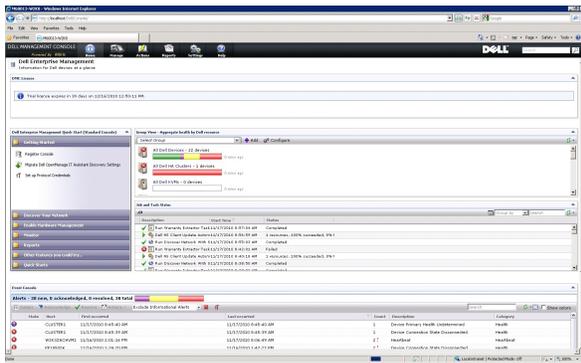
--	--

正常性ポリシー	説明
Device Primary Health(デバイスのプライマリ正常性)	デバイスの全体的な正常性
Device Connection State(デバイス接続状態)	デバイスがネットワークに接続されているかどうか
Agent Health-Storage Management(エージェントの正常性 - Storage Management)	ソフトウェアストレージコンポーネントの正常性
Agent Health-DRAC(エージェントの正常性 - DRAC)	リモートアクセスコントローラの正常性



## グループビュー

Group View(グループビュー)は、デバイスの正常性を表示するための主要インタフェースです。デバイスの正常性は、ハードウェア正常性の最悪のケースのロールアップであり、パフォーマンスの監視での警告基準に一致します。



この Group View(グループビュー)は、Dell 正常性監視ポリシーによって収集される正常性の値に基づいており、デバイスの正常性状態が変化するたびにリアルタイムでアップデートされます。このウェブページの右上隅にある更新コントロールを使用すると、更新間隔を指定できます。また、Refresh(更新)をクリックして正常性状態ビューをアップデートすることもできます。

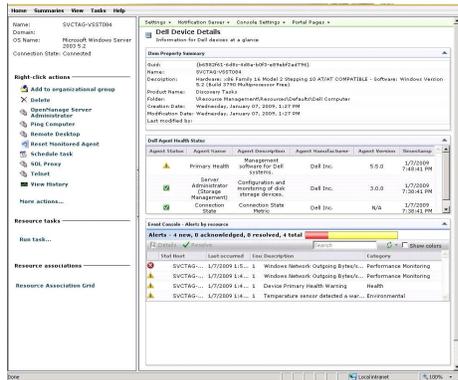
このウェブページは、デバイスクラスごとに棒グラフでロールアップ正常性を表示する複数の定義済みのグループで構成され、さらにすべての Dell デバイスの正常性をロールアップするサマリーグループも表示します。独自のカスタムグループを追加したり、このビューから既存のグループを削除したりすることもできます。

デバイスグループのタイトルまたはデバイスグループ棒グラフのセクションをクリックすると、新しいウィンドウが開き、デバイスの完全なリストまたは特定の状態にそれぞれ一致しているデバイスが表示されます。このウィンドウには、このグループのロールアップ状態に対する特定の要因とその他の詳細が表示されます。



All Dell Devices(すべての Dell デバイス)ウィンドウをクリックし、リソースマネージャを表示します。

## 正常性の監視のリソースマネージャビュー



**リソースマネージャ** は、デバイスの正常性に影響するデバイス固有の要因すべてに関する詳細ビューです。

Group Health View(グループ正常性ビュー)に表示されるように、プライマリ正常性、エージェントの正常性、および接続状況すべての組み合わせがデバイスの全体的な正常性を構成します。正常性状態の詳細は、**リソースマネージャ** から表示することも、**パフォーマンスビューア** に数値で表示することもできます(表 11-6 を参照)。

## Agent Health Status(エージェントの正常性状態)ウェブパーツ

このウェブパーツには、正常性が監視されているすべてのエージェントとその他の関連情報が表示されます。

## Connection State(接続状態)インジケータ

**リソースマネージャ** の左上隅にあるこのインジケータは、デバイスが接続された状態か、切断された状態かを示します。

## Event Console(イベントコンソール)ウェブパーツ

**リソースマネージャ** の Event Console(イベントコンソール)ウェブパーツには、このデバイスに固有のすべての警告が表示されます。監視ソリューションから受信したすべての警告は、このデバイスの全体的な正常性に影響を及ぼします。Event Console(イベントコンソール)の詳細については、オンラインヘルプを参照してください。

## 接続状態の監視

接続状態は、正常性の監視の一部であり、デバイスのロールアップ正常性に影響します。接続が失われると、デバイスのロールアップ正常性は重要と表示されます。

デバイスが **Disconnect**(切断)または **Connection lost**(接続消失)状態になると、Notification Server はデバイスと通信できません。この状態は次を意味します。

- 1 物理的な電力の損失
- 1 ネットワーク接続の損失
- 1 プロトコルの応答停止
- 1 エージェントの応答停止

非通信デバイスをトラブルシューティングする場合は、これらの可能性を考慮してください。

## 注意事項

- 1 Dell Management Console では、デバイスを検出し、監視するために同じプロトコルを使用します。たとえば、SNMP を含まないカスタム接続プロファイルを使用する場合、**リソースマネージャ** および **パフォーマンスビューア** にはパフォーマンスメトリクスも、次のような一部の正常性メトリクスも表示されません。
  - Device Agent Health-Dell OpenManage Storage Management(デバイスエージェントの正常性 - Dell OpenManage Storage Management)
  - Device Agent Health - Dell Remote Access Controller IB(In Band) (デバイスエージェントの正常性 - 帯域内の Dell Remote Access Controller)

## OnDemand 監視

OnDemand 監視を使用すると、SNMP 警告の受信時に、Notification Server がメトリクスを瞬時に収集することを可能にします。

この機能は、正常性に影響する可能性のある SNMP トラップをデバイスから受信したときに、デバイスの正常性をポーリングするために使用します。これによって、次のポーリング間隔に正常性がアップデートされるのを待つのではなく、ハードウェアの正常性が変化した時点で正確かつ効率的にデバイスの正常性をアップデートすることができます。

この機能を利用するには、管理対象システムの SNMP サービス設定で SNMP トラップの宛先に Dell Management Console システムの IP アドレスを入力します。

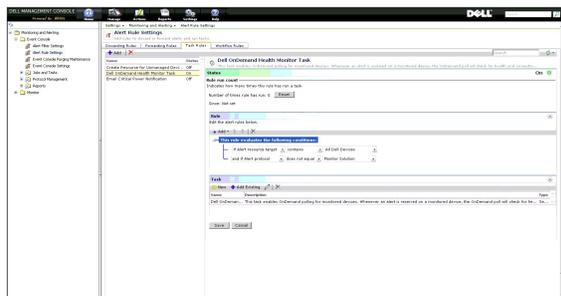
その他のデバイスタイプの場合、Dell Management Console システムにトラップを転送するための設定手順については、各デバイスのマニュアルを参照してください。

OnDemand 機能は、デフォルトで有効になっています。

 **メモ:** この機能はデバイスからの SNMP トラップに依存するので、この機能を利用するには、デバイスに SNMP 管理を設定する必要があります。

OnDemand タスクおよび警告ルールは、**Monitoring and Alerting** (監視と警告)ポータルページで確認できます。OnDemand 警告ルールでは、OnDemand タスクをトリガーするために必要な条件を定義し、この機能を有効にするかどうかを制御します。このルールは、左側のペインの **Monitoring and Alerting** (監視と警告) → **Event Console** (イベントコンソール) → **Alert Rule Settings** (警告ルール設定)の下に表示されます。右側のペインの **Task Rules** (タスクルール)タブで、**Dell OnDemand Health Monitor Task** (Dell OnDemand 正常性監視タスク)を選択します。

OnDemand タスクには、OnDemand 警告ルールがトリガーされたときにどのメトリクスをポーリングするかが定義されます。このタスクを表示するには、警告ルール内のタスクをダブルクリックするか、直接左側のペインの **Monitoring and Alerting** (監視と警告) → **Event Console** (イベントコンソール) → **Jobs and Tasks** (ジョブとタスク) → **Dell OnDemand Health Monitor Task** (Dell OnDemand 正常性監視タスク)を選択します。



## 特定のデバイスへの OnDemand ポーリングの強制

1. **Manage** (管理) → **All Devices** (すべてのデバイス)をクリックします。
2. 右側のペインで、OnDemand ポーリングを強制するデバイスを右クリックし、**Properties** (プロパティ)を選択します。
3. **Properties** (プロパティ) ページで **Guid** の値をコピーします。
4. **Home** (ホーム) → **Monitoring and Alerting** (監視と警告)をクリックします。
5. **Monitoring and Alerting** (監視と警告)ポータルページで、**Event Console** (イベントコンソール) → **Jobs and Tasks** (ジョブとタスク) → **Dell OnDemand Health Monitor Task** (Dell OnDemand 正常性監視タスク)をクリックします。
6. 右側のペインの **Task Status** (タスク状態) ウェブパーツで、**New Schedule** (新規スケジュール)をクリックします。
7. **New Schedule** (新規スケジュール) ダイアログボックスで、ポーリングを今すぐ行う、または後で実行するようにスケジュールできます。
8. **Monitored Resource** (監視下リソース) セクションの下に、手順 3 でコピーした GUID 値を貼り付けます。

 **メモ:** GUID に、スペースなどの余分な文字が含まれていないことを確認してください。

9. **Schedule** (スケジュール)をクリックします。

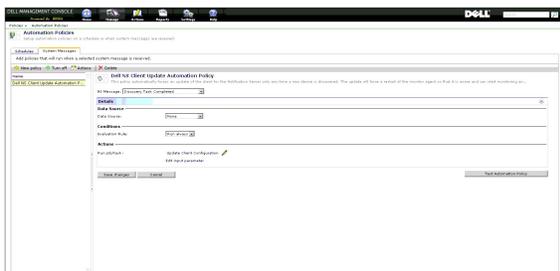
タスクが実行されると、正常性ビューに正常性のアップデートを表示できます。

## クライアントアップデート自動化ポリシー

クライアントポリシーのアップデートは、新しいデバイスが検出されたときや、監視ポリシー、メトリクス、またはルールがアップデートされたときに必要です。この機能を使用すると、新しいデバイスを検出するたびにクライアント ポリシーを自動的にアップデートできます。それによって、監視エージェントが再起動され、そのエージェントへのオープン接続が終了します。ただし、このポリシーでは、リモート監視エージェントのアップデート中に現在の監視プロセスへの短い中断が発生します。それでも、ポリシー、ルール、またはメトリクスの変更後には、クライアントアップデートを手動で強制する(詳細については [クライアントポリシーアップデートの強制](#)を参照してください)、または次回ポーリングされるクライアントのアップデートを待つ(デフォルトでは毎時間)必要があります。

 **メモ:** この機能は、エージェントレスの監視のみに適用されます。

この機能を定義するタスクを確認するには、Manage(管理)→Automation Policies(自動化ポリシー)をクリックします。Automation Policies(自動化ポリシー)ページの System Messages(システムメッセージ)タブで、Dell NS Client Update Automation Policy(Dell NS クライアントアップデート自動化ポリシー)を選択します。



## クライアントポリシーアップデートの強制

クライアントポリシーアップデートは、デフォルトで毎時間行われます。

1. Notification Server の Windows ツールバーで、**Altiris Agent** アイコンを右クリックし、**Altiris Agent Settings**(Altiris Agent の設定)を選択します。
2. **Altiris Agent** ダイアログボックスで、**Send**(送信)をクリックしてから **Update**(アップデート)をクリックします。
3. **Configuration**(設定)セクションで、**requested**(要求)時間と **changed**(変更)時間が一致していること、またはアップデート後に **changed**(変更)時間が最近になっていることを確認します。

これは、設定が変更されているものの、変更を監視するためにエージェントのリセットが必要であることを示します。

監視エージェントをリセットするには、数分以上かかる場合があります(監視されるデバイスの数が増えると、所要時間も増えます)。リセット後、データが取得されると、**パフォーマンスビューア**でメトリクスが利用可能になります。

 **メモ:** 同じデバイスのメトリクスでも、同時に取得されないものがある場合があります。また、使用する接続プロファイルによって、表示されるメトリクスが異なります。接続プロファイルの詳細については、[新しい接続プロファイルの作成](#)および[デフォルトの接続プロファイルの編集](#)を参照してください。

## 異なるしきい値を持つ各種デバイスを監視するためのポリシーの複製

この手順は、2 以上のデバイスグループを異なるしきい値に対して同時に評価するポリシーまたはポリシーのサブセットを作成する場合のみ必要です。

メトリクスとルールはグローバルに定義されます。つまり、これらの値に対して変更を行うと、メトリクスまたはルールのすべての参照先に影響します。

デバイスまたはデバイスのグループに固有の変更を加え、別のデバイスグループに元の値が保持されるようにするには、メトリクスまたはルールを複製してから、元のメトリクスまたはルールではなく複製を参照する新しいポリシーを作成します。

### ルールの複製

1. **Monitoring and Alerting**(監視と警告)ポータルページの左側のペインで、**Monitor**(監視)→**Policies**(ポリシー)→**Rule Library**(ルールライブラリ)を選択します。
2. 変更するルールを右クリックし、**Clone**(複製)アイコンを選択します。  
ルールが複製されます。
3. 複製されたルールを選択します。
4. 変更するプロパティを修正し、**Save**(保存)をクリックします。
5. 変更するすべてのルールに対して、手順 1~4 を繰り返します。

### 元のポリシーの複製

1. **Monitoring and Alerting**(監視と警告)ポータルページの左側のペインで、複製するポリシーを選択します。
2. ポリシーを右クリックし、**Clone**(複製)を選択します。  
ポリシーが複製されます。

- 複製されたポリシーを選択します。
- ポリシー内の既存のルールをすべて選択し、- ボタンを使用して削除します。
- + ボタンを使用して、すべての新規ルールをポリシーに追加します。
- 新規のポリシー名を入力し、Apply to (適用先)ドロップダウンをクリックしてポリシーの新しいターゲットを選択します。

 **メモ:** 元のポリシーと重複しないターゲットを選択していることを確認してください。同じデバイスでマトリクスを 2 回監視すると、帯域幅の浪費につながります。

- On/Off (オン / オフ)ドロップダウンをクリックし、On (オン)を選択します。
- Save Changes (変更の保存)をクリックします。

クライアントポリシーの強制アップデートを実行して(またはデフォルトのポリシーアップデート期間を待つ)変更を有効にします。詳細については、[クライアントポリシーアップデートの強制](#)を参照してください。

---

## サーバー監視警告の管理

事前に選択したデバイスの正常性の状態に関する警告を特定のユーザーに電子メールで送信するよう、Dell Management Console を設定できます。

電子メールを送信するスケジュールを設定できます。定義済みコレクション内のデバイスの正常性状態の変更が、タスクによって監視されている正常性状態と一致する場合、次にタスクの実行がスケジュールされている時に指定されたユーザーに電子メールが送信されます。

タスクを作成し、警告を送信するための必要条件として、SMTP サーバーを追加し、設定する必要があります。[正常性監視電子メールタスクのスケジュール](#)を参照してください。

## 正常性監視電子メールタスクの表示

正常性監視タスクのリストを表示するには、Dell Management Console Portal (Dell Management Console ポータル) ページから、Dell Enterprise Management Quick Start (Dell Enterprise Management クイックスタート) → Quick Starts (クイックスタート) → Health Monitor Email Task (正常性監視電子メールタスク) を選択します。

## 正常性監視電子メール警告の受信

警告を受信するには、SMTP サーバーを設定し、正常性監視電子メールタスクを設定してから、正常性監視電子メールタスクをスケジュールします。

正常性監視電子メールタスクが完了すると、レポートが表示され、選択したユーザーに電子メールが送信されます。

正常性監視レポートには、参照できるデバイスが表示されます。このレポートでは、デバイスをクリックしてリソースマネージャのページを表示することができます。

## SMTP サーバーの設定

SMTP サーバーを設定するには、次の手順を実行します。

- Dell Management Console (Dell Management Console) から Settings (設定) → All Settings (すべての設定) → Notification Server → Notification Server Settings (Notification Server の設定) を選択します。
- Notification Server Settings (Notification Server の設定) ページの E-mail (電子メール) タブで、次の作業を行います。
  - SMTP Server Settings (SMTP サーバーの設定) 情報を入力します。
  - Default E-mail Addresses (デフォルト電子メールアドレス) 情報を入力します。
  - Send test e-mail (テストメールの送信) をクリックして設定をテストします。
- OK をクリックします。

## 正常性監視電子メールタスクの作成

サーバーの正常性に関する警告を受信するには、正常性監視電子メールタスクを次のように設定します。

Dell Management Console から、次のいずれかを実行します。

- Dell Management Console Portal (Dell Management Console ポータル) ページから、次の操作を実行します。
  - Dell Enterprise Management Quick Start (Dell Enterprise Management クイックスタート) ウェブパーツから、Quick Starts (クイックスタート) → New Health Monitor Email Task (新規の正常性監視電子メールタスク) を選択します。

- b. **E-mail information**(電子メール情報)ウェブパーツに、警告時にユーザーに送信する電子メール情報を入力します。警告条件は変更できます。警告条件を変更するには、『Dell Management Console のオンラインヘルプ』を参照してください。
1. **Jobs and Tasks Portal**(ジョブおよびタスクポータル)ページから、次の操作を実行します。
    - a. **Quick Start - Jobs and Tasks**(クイックスタート - ジョブおよびタスク)ウェブパーツで、**Create a new job or task**(ジョブまたはタスクの新規作成)を選択します。
    - b. **Create New Job or Task**(ジョブまたはタスクの新規作成)ページで、**Server Tasks Health Monitor E-mail Task**(サーバータスクの正常性監視電子メールタスク)を選択します。
    - c. **Server Tasks Health Monitor E-mail Task**(サーバータスクの正常性監視電子メールタスク)ページに、電子メール情報を入力します。警告条件は変更できます。警告条件を変更するには、『Dell Management Console のオンラインヘルプ』を参照してください。

## 正常性監視電子メールタスクのスケジュール

正常性監視電子メールタスクを選択した Dell デバイス上で実行するようにスケジュールできます。警告タスクは、**Jobs and Tasks Portal**(ジョブおよびタスクポータル)ページからスケジュールできます。

正常性監視電子メールタスクをスケジュールするには、次の手順を実行します。

1. **Dell Management Console Portal**(Dell Management Console ポータル)ページから、**Quick Starts**(クイックスタート)→ **Health Monitor Email Tasks**(正常性監視電子メールタスク)を選択します。
2. **Health Monitor Email Task**(正常性監視電子メールタスク)ページで、電子メールタスクを選択します。
3. **Task Status**(タスク状態)で、**New Schedule**(新規スケジュール)をクリックします。
4. タスクをスケジュールするには **Now**(今すぐ)をクリックします。特定の頻度や特定の日にタスクをスケジュールするには **Schedule**(スケジュール)を選択して、詳細を入力します。
5. 正常性監視電子メールタスクに電子メール条件を設定する際に、入力パラメータを指定するフィールドを選択した場合は、それらのフィールドが使用可能になります。使用可能なフィールドに、受信者の電子メール情報を入力します。
6. **Schedule**(スケジュール)をクリックします。
7. 完了したスケジュールをクリックして、正常性監視レポートを表示します。
8. レポート内のデバイスをクリックすると、**リソースマネージャ** のページが表示されます。

---

[目次に戻る](#)

[目次に戻る](#)

## 電源監視

Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [電源監視の依存関係](#)
- [電源監視のメトリクス](#)
- [電源監視のしきい値](#)
- [電源監視の管理](#)
- [グループメトリクス](#)

電源監視により、Dell サーバーの標準的な消費電力カウンタのセットを監視できます。ただし、対象となるサーバーで電源監視がサポートされている必要があります。

電源監視では、次の機能が提供されます。

- 1 Dell OpenManage によって収集されたメトリクスからデータを取得します。
- 1 デバイスの電力消費の傾向とデータをグラフィック形式で表示します。
- 1 SNMP と WMI プロトコルでデータにアクセスします。
- 1 電源監視は、OpenManage Server Administrator バージョン 5.3 以降がインストールされた yx0x サーバー、yx1x サーバー、および次の x9xx サーバーに限りサポートされます。
  - o 1950 MLK111
  - o 2950 MLK111

サポートされるサーバーの詳細に関しては、『Support Information Matrix for Dell Management Console』を参照してください。

サーバー名の形式 yxxx のうち、y はアルファベット(例えば R、T など)で、x は数字を示します。

- 1 電源装置あたりのアンペア数(A)、エネルギー消費量(KWh)などの単一のプローブ読み取り値を記録します。
- 1 総電力などの総合的な読み取り値を記録します。
- 1 リアルタイムの消費電力データ、消費電力データの履歴などのグラフを表示します。
- 1 各種消費電力メトリクスのレポートを生成します。

### Dell OpenManage Server Administrator に関連したメモ

- 1 一部のロールアップ状態については、OpenManage Server Administrator の状態と Dell Management Console に表示される状態が異なる場合があります。
- 1 Dell Management Console では、ロールアップの正常性として、常に最悪ケースのロールアップが示されます。したがって、デバイス上に重要状態があると、グローバルな正常性、つまり、グループビューと監視円グラフが常に重要状態になります。

例えば、電源装置の 1 つがサーバーから取り外されたとします。OpenManage Server Administrator では、全般的な正常性状態の表示は警告になり、電源冗長性状態の表示も警告になり、電源装置は重要として表示されます。リソースマネージャでも、正しい(OpenManage Server Administrator の状態と一致する)イベントが、警告として表示されます。一方、Dell Management Console サーバーの正常性状態は、**Monitored Resource by Status** (状態別監視対象リソース)円グラフにおいて重要(赤色)として表示されます。

### 電源監視に関連したメモ

- 1 パフォーマンスビューでは、現在、1 台のサーバーに関してのみリアルタイムの消費電力を表示できます。複数のサーバーの消費電力を確認するには、レポートを見る必要があります。
- 1 500 を超えるノードを管理している場合、電源監視を使用できません。500 以下のノードを管理するには、Dell Management Console 管理ステーションの次のシステム要件を満たす必要があります。
  - o 対応オペレーティングシステム。例えば、Microsoft Windows Server 2008 R2(64 ビット)など。
  - o 4 個以上のプロセッサコア
  - o RAM - 4 GB
  - o DVD ドライブ
  - o Microsoft .NET Framework バージョン 3.5、3.5 SP1、または 4.0

 **メモ:** Microsoft .NET Framework バージョン 4.0 は、システムにバージョン 3.5 または 3.5 SP1 が存在する場合に限りサポートされます。

- o Microsoft Silverlight 3.0
  - o Windows Internet Information Services バージョン 7.0
  - o Microsoft Internet Explorer 8.0
  - o Microsoft SQL Express 2008、SQL Express 2005、SQL Server 2005、SQL Server 2008 SP1、または SQL Server 2008 R2
  - o それより大規模な環境では、リモートデータベース、8 個以上のプロセッサコア、および 8 GB 以上のメモリ空き容量。
- 1 WMI プロトコルを使用して検出されたデバイスをインベントリした場合、**hardware Summary** (ハードウェア概要) ページの **Power supply information** (電源装置の情報) テーブルに **Power Supply Type** (電源装置タイプ) の値はありません。

---

## 電源監視の依存関係

電源監視には、次の依存関係があります。

表 10-1. 電源監視の依存関係

Dell ポリシー	エージェント / エージェントレス	サポート範囲	デフォルトの動作	依存関係
電源監視	エージェントレス	対応する電源監視が有効になっている Dell サーバー	無効	SNMP と WMI プロトコル

## 電源監視のメトリクス

次の消費電力のメトリクスを Dell サーバーで監視できます。

**メモ:** 使用不可または初期化中のメトリクスを表示するには、**Show unavailable/initializing metrics** (使用不可 / 初期化中のメトリクスの表示) チェックボックスを選択します。監視用に選択した数値メトリクスは、**Graph and Metrics** (グラフとメトリクス) から使用でき、選択したテキストメトリクスは **Text Data** (テキストデータ) から使用できます。このオプションを選択すると、監視エージェントが収集しようとしている他のメトリクスを表示できます。ただし、データが取得されるまで、それらのメトリクスを選択したり、グラフに表示したりすることはできません。

表 10-2. 電源監視のメトリクス

メトリック	説明
<b>エージェントレス数値メトリクス</b>	
Dell 電源 - 電源装置あたりのアンペア数 (アンペア)	電源装置のアンペア数をアンペア単位で監視する場合に選択します。
Dell 電源 - エネルギー消費量 (KWh)	エネルギー消費量をキロワット時単位で監視する場合に選択します。
Dell 電源 - エネルギー消費量 (BTU/hr)	エネルギー消費量を時間あたりのイギリス熱単位で監視する場合に選択します。
Dell 電源 - エネルギー消費量 (ワット)	エネルギー消費量をワット単位で監視する場合に選択します。
Dell 電源: 瞬間ヘッドルーム (BTU/時)	使用可能な瞬間ヘッドルームを時間あたりのイギリス熱単位で監視する場合に選択します。
Dell 電源: 瞬間ヘッドルーム (ワット)	使用可能な瞬間ヘッドルームをワット単位で監視する場合に選択します。
Dell 電源 - 電力消費量 (BTU/hr)	エネルギー消費量を時間あたりのイギリス熱単位で監視する場合に選択します。
Dell 電源 - エネルギー消費量 (ワット)	エネルギー消費量をワット単位で監視する場合に選択します。
<b>エージェントレステキストメトリクス</b>	
Dell 電源: エネルギー消費開始時間	エネルギー消費開始時間のテキストデータを表示する場合に選択します。

## 電源監視のしきい値

消費電力は、使用されているハードウェアに強く依存します。あるシステムで危機的な消費量であっても、別のシステムでは限界の範囲内に十分収まることもあります。便宜上、電源メトリクスに関するアラートをトリガーするためのルールが定義されていますが、ハードウェアとのこうした密接な結び付きがあるため、これらのルールのいずれかがトリガーするように監視されるハードウェアには固有の正しいしきい値を定義する必要があります。これは、デフォルト設定が実際のハードウェア値よりもはるかに高く設定されているためです。

## 電源監視の管理

消費電力監視で作業を行うには、電源監視ポリシーを有効にする必要があります。[監視ポリシーの有効化](#)を参照してください。

電源監視がアクティブになっていることを確認した後、使用可能な消費電力メトリクスを使用してデバイスの消費電力を監視できます。次の作業すべてを実行できます。

- リアルタイムデータを表示します。[電源監視メトリクスの管理](#)を参照してください。
- 履歴データを表示します。**Actions** (アクション) → **Monitor** (監視) → **Historical** (履歴) をクリックし、デバイスを選択します。
- 各種消費電力メトリクスのレポートを表示します。[レポート](#)の章を参照してください。

消費電力監視メトリクスのルールとアクションを変更できます。[メトリクスの変更](#)を参照してください。

## 電源監視メトリクスの管理

エージェントレス数値メトリクスとテキストメトリクスのリストから必要なメトリクスを選択して、デバイスの消費電力を監視できます。各種メトリクスに対し、定義されているルールとアクションを変更できます。

デバイスの消費電力を表示するには、次の手順を実行します。

- 次のいずれかを実行します。
  - Dell Management Console から、**Actions** (アクション) → **Monitor** (監視) → **Real-time** (リアルタイム) を選択します。

1. **Monitoring and Alerting (監視と警告)**ポータルページの **Launch Performance Viewer (パフォーマンスビューアの起動)**で、デバイスアイコンをクリックしてデバイスを選択し、**Launch (起動)**をクリックします。
1. **Monitoring and Alerting (監視と警告)**ポータルページの **Monitored Resources by Status (状態別監視対象リソース)**で、デバイスを選択し、**Performance Viewer (パフォーマンスビューア)**をクリックします。

**Real-time Performance Viewer (リアルタイムパフォーマンスビューア)** ページが **Registered Metrics (登録メトリクス)** ページとともに表示されます。

2. **Registered Metrics (登録メトリクス)** ページで、必要なメトリクスを選択し、**OK** をクリックします。詳細に関しては、[電源監視のメトリクス](#)を参照してください。

---

## グループメトリクス

この機能は、今後のバージョンの Dell Management Console で提供される予定です。グループメトリクスにより、データを効率的に収集できるインターフェースが提供されます。データを効率的に収集することにより、同じグループをスマートメトリクスレポートで表示する場合に比べて、レポートの計算が高速化されます。このインターフェースを使用すると、グループレベルでのしきい値も作成できます。すべてのグループメトリクスは、指定されたグループの値の合計を計算します。グループメトリクスは、常にターゲットを 1 つだけ持つことができ、このターゲットはポリシーターゲットと同じか、それに含まれている必要があります。いずれにしても、デフォルトは、検出時に自動的に決定される **All Devices with Power monitoring support (電源管理に対応したすべてのデバイス)** グループになります。

表 10-3. グループメトリクス

メトリクス	説明
Dell 電源 - グループエネルギー消費量 (KWh)	グループのエネルギー消費量を監視できます。
Dell 電源 - グループ瞬間ヘッドルーム (BTU/時)	グループの使用可能な瞬間ヘッドルームを時間あたりのイギリス熱単位で監視できます。
Dell 電源 - グループ瞬間ヘッドルーム (ワット)	グループの使用可能な瞬間ヘッドルームをワット単位で監視できます。
Dell 電源 - グループエネルギー消費量 (BTU/hr)	グループによって消費された電力を時間あたりのイギリス熱単位で監視できます。
Dell 電源 - グループ消費電力 (ワット)	グループによって消費された電力をワット単位で監視できます。

## グループメトリクスレポートの表示

グループメトリクスデータは、リアルタイムビューアや履歴ビューアで表示できません。このデータは、グループメトリクスレポートでのみ表示できます。

グループメトリクスを表示するには、Dell Management Console から、**Reports (レポート)** → **All Reports (すべてのレポート)** → **Group Metric Report (グループメトリクスレポート)** を選択します。

## グループメトリクスの管理

事前に定義されているグループメトリクスは、すべて電源監視ポリシーの一部です。これらのメトリクスは、スマートメトリクスと同じであり、同じ方法で変更されますが、1 つの重要な違いは、グループメトリクスのターゲットを指定するという点です。同様に、グループメトリクスの監視に使用されるルールは、スマートメトリクスのルールの場合と同じ方法で変更できます。メトリクスの監視とルールの詳細に関しては、[電源監視の管理](#)を参照してください。

---

[目次に戻る](#)

[目次に戻る](#)

## Dell パッチ管理ソリューション

Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [Dell パッチ管理ソリューションについて](#)
- [Altiris Agent 対応パッチ管理の前提条件](#)
- [Lifecycle Controller 対応パッチ管理の前提条件](#)
- [パッチ管理ソリューションのユーザーインターフェース](#)
- [DUP とシステムバンドル](#)
- [DUP カタログのインポート](#)
- [Dell インベントリコレクタツール](#)
- [Dell ベンダー設定ページ](#)
- [Dell アップデートパッケージのダウンロード](#)
- [パッチアップデートに対応した Linux Dell サーバーの検出](#)
- [パッチアップデートに対応した Windows Dell サーバーの検出](#)
- [パッチアップデートに対応した Lifecycle Controller 対応 Dell サーバーの検出](#)
- [Dell パッチ管理レポートへのアクセス](#)
- [コンプライアンスアセスメントタスク](#)
- [Dell ハードウェアアップデートの管理](#)
- [DUP のステー징と配布](#)
- [ロールアウトジョブ](#)
- [ロールバックレポート](#)
- [パッチ管理ソリューションのトラブルシューティング](#)

Dell パッチ管理ソリューションを使用すると、お使いの動作環境をスキャンして、対応する Dell PowerEdge システムが、BIOS、ドライバ、およびファームウェア用の Dell アップデートパッケージ (DUP) を適用するための最小パッチ要件を満たしているかどうか判定できます。また、このソリューションにより、DUP のダウンロードおよび配布が自動化されます。

Dell Management Console は、Lifecycle Controller を装備したサーバーのパッチアップデートをサポートしています。サポートされる最低限の Lifecycle Controller、およびパッチアップデートに必要な [Integrated Dell Remote Access Controller \(iDRAC\)](#) ファームウェアの詳細に関しては、『Support Information Matrix for Dell Management Console』を参照してください。

Lifecycle Controller を装備したサーバー上でパッチサーバーアップデートを実行するのに、Symantec Management Agent (旧称 Altiris Agent) は必要はありません。

Lifecycle Controller 対応のパッチサーバーアップデートでは、BIOS やファームウェア(またはその両方)、オペレーティングシステムのドライバパックなどのアプリケーション Dell アップデートパッケージ (APAC DUP)、および Unified Server Configurator (USC) の既存バージョンに関する情報を収集し、Dell サーバー内のさまざまなハードウェアコンポーネントに最新のアップデートを適用することが可能になります。また、必要なアップデートをスケジュールして導入することもできます。

アップデートが必要なシステムでは、『Dell Server Updates DVD』を使用するか、デルサポートサイトの [ftp.dell.com](http://ftp.dell.com) から該当する DUP をダウンロードします。

Dell パッチ管理に関連したメモ

- 1 ステーキングおよび配布中に Windows ターゲットとして選択されるサーバーでは (デフォルトの接続プロファイルを使用)、Apply Updates using Lifecycle Controller (Lifecycle Controller を使用してアップデートを適用) を優先するように選択していると、ロールアウトジョブが失敗します。この問題を解決するには、Lifecycle Controller ベースのアップデートに対し、Lifecycle Controller ベースのターゲットを使用します。
- 1 ステーキングおよび配布中に Windows ターゲットとして選択されるサーバーでは (適切な接続プロファイルを使用)、Apply Updates using Altiris Agent (Altiris Agent を使用してアップデートを適用) を優先するように選択していると、ロールアウトジョブが失敗します。この問題を解決するには、Altiris Agent ベースのアップデートに対し、ステージングおよび配布のウィザードで Windows ターゲットを使用します。
- 1 アップグレード後に再度ステージングする必要があります。Dell Management Console バージョン 1.1 へアップグレードすると、ステージングバンドルが削除されます。ステージングバンドルを取得するには、ステージングタスクを再度実行する必要があります。

ステージングタスクを実行するには、次の手順を実行します。

- a. Dell Management Console から、**Manage (管理)** → **Jobs and Tasks (ジョブとタスク)** → **System Jobs and Tasks (システムのジョブとタスク)** → **Software (ソフトウェア)** → **Patch Management for Dell Servers (Dell サーバーのパッチ管理)** → **Server (サーバー)** → **Download Software Update Package (ソフトウェアアップデートパッケージのダウンロード)** と選択します。
  - b. アップグレードの前にバンドルのステージングに使用したステージングタスクを選択し、そのステージングタスクを右クリックして **Start now (今すぐ開始)** を選択します。バンドルの再ステージングタスクが開始します。
- 1 サーバーで Altiris Agent 対応パッチアップデートと Lifecycle Controller 対応パッチアップデートの両方を同時にサポートするには、SNMP または WMI と WS-MAN プロトコルの含まれる接続プロファイルを使用してそのサーバーおよびそのサーバーの iDRAC を検出します。サーバーには、検出を実行する前に、OpenManage Server Administrator をインストールしておく必要があります。

サーバーを検出した後、Altiris Agent 対応パッチと Lifecycle Controller 対応パッチの前提条件を完了させます。

## Dell パッチ管理ソリューションについて

Dell パッチ管理ソリューションは、次を提供します。

- 1 個々のアップデート、およびシステムアップデートセットのアップデートのサポート。  
利便性と効率性のために、バンドルロールアウトジョブを作成することをお勧めします。単一の DUP とは違い、バンドルロールアウトジョブは、ソフトウェアアップデートセット全体 (バンドル) を配布します。
- 1 Lifecycle Controller を装備したサーバー上でのロールバックアップデートのサポート。前のアップデートに限りロールバックできます。
- 1 サポートされている Microsoft Windows オペレーティングシステムおよび Linux オペレーティングシステムを実行している Dell PowerEdge システムのサポート。
- 1 オペレーティングシステムに依存しない Lifecycle Controller 対応パッチアップデートを備えた Dell PowerEdge システムのサポート。
- 1 Dell システムを検出し、Dell サーバーをアップデートの受信に必要なレベルにアップデートするための単一サーバージョブのサポート。

## Altiris Agent 対応パッチ管理の前提条件

次の前提条件を完了しておく必要があります。

- 1 管理対象システムに Altiris Agent をインストールします。
- 1 ftp.dell.com または最新バージョンの Dell Server Update Utility から DUP カタログをインポートします。
- 1 インベントリコレクタをダウンロードします。
- 1 Getting Started (はじめに) ウェブパーツの設定セクションに示されるように、コンプライアンスアセスメントを実行します。

---

## Lifecycle Controller 対応パッチ管理の前提条件

適用可能な DUP は、Lifecycle Controller でサポートされる BIOS、ファームウェアアップデート、およびアプリケーション Dell アップデートパッケージ (APAC DUP) に限定されます。APAC DUP には、オペレーティングシステムのドライババック、32 ビット診断、Unified Server Configurator (USC) が含まれます。

次の前提条件を完了しておく必要があります。

- 1 対応サーバーには、必要なファームウェアバージョンの iDRAC6 Enterprise と USC が搭載されている必要があります。詳細に関しては、『Support Information Matrix for Dell Management Console』を参照してください。現在のバージョンの iDRAC にアップグレードした場合は、iDRAC を再検出する必要があります。

 **メモ:** iDRAC6 が設定されている必要があります。自動検出は、Dell Management Console でサポートされていません。

- 1 接続プロファイルで WS-MAN プロトコルを設定します。
- 1 Lifecycle Controller 対応サーバーの iDRAC 6 が DNS サーバーに登録されている必要があります。Dell Management Console サーバーと iDRAC6 に対するネットワーク通信は、それらのホスト名を使用して実行することが可能であるようにします。たとえば、Dell Management Console サーバーと iDRAC6 へ、それぞれのホスト名を使用して ping できる必要があります。
- 1 WS-MAN 接続プロファイルを使用して iDRAC 6 Enterprise を検出します。検出されたデバイスは、Dell サーバーに分類されている必要があります。
- 1 エージェントレスインベントリを使用して、検出されたデバイスの情報を収集します。
- 1 DUP カタログをダウンロードします。
- 1 Lifecycle Controller 対応サーバーのコンプライアンスアセスメントを実行します。

---

## パッチ管理ソリューションのユーザーインターフェイス

パッチ管理ソリューションのユーザーインターフェイス (UI) にアクセスするには、Home (ホーム) → Patch Management for Dell Servers Home (Dell サーバーのパッチ管理ホーム) を選択します。

### パッチ管理の開始前に

Getting Started Web (はじめにウェブ) パーツには、一般的な設定とパッチ管理プロセスの各項目へのリンクがあります。

#### 設定

- 1 Configure Proxy (プロキシの設定) (クリックすると、Notification Server Settings (Notification Server の設定) ページが表示されます。)
- 1 Download Updates Catalog (アップデートカタログのダウンロード) (クリックすると、DUP Catalog Import (DUP カタログのインポート) ページが表示されます。)
- 1 Download Inventory Collector (インベントリコレクタのダウンロード) (クリックすると、Dell Inventory Collector Import (Dell インベントリコレクタのインポート) ページが表示されます。)

 **メモ:** Dell Inventory Collector Import (Dell インベントリコレクタのインポート) ページは、Altiris Agent 対応パッチアップデートの場合にのみ必要です。

- 1 Solution Global Settings (ソリューショングローバル設定) (クリックすると、Dell Vendor Configuration (Dell ベンダー設定) ページが表示されます。)
- 1 Install Altiris Agent (Altiris Agent のインストール) (クリックすると、Altiris Agent Install (Altiris Agent のインストール) ページが表示されます。)

 **メモ:** Altiris Agent Install (Altiris Agent のインストール) ページは、Altiris Agent 対応パッチアップデートの場合にのみ必要です。

#### パッチプロセス

- 1 Run compliance check on (コンプライアンスチェックの実行)
  - Windows Servers (Windows サーバー) (クリックすると、Determine Windows Patchable Dell Servers Job (Windows のパッチ可能な Dell サーバーの判定ジョブ) ページが表示されます。)
  - Linux Servers (Linux サーバー) (クリックすると、Determine Linux Patchable Dell Servers Job (Linux のパッチ可能な Dell サーバーの判定ジョブ) ページが表示されます。)
  - Lifecycle Controller Enabled Servers (Lifecycle Controller 対応サーバー) (クリックすると、Compliance Assessment Task for Lifecycle Controller enabled Servers (Lifecycle Controller 対応サーバーのコンプライアンスアセスメントタスク) ページが表示されます。Lifecycle Controller 対応パッチの場合に必要です。)
- 1 Check applicable updates by computers (コンピュータごとの適用可能なアップデートの確認) (クリックすると、Hardware Update Compliance report (ハードウェアアップデートのコンプライアンスレポート) ページが表示されます。)

- 1 **Manage Updates** (アップデートの管理) (クリックすると、**Manage Dell Hardware Updates** (Dell ハードウェアアップデートの管理) ページが表示されます。)

**Identify Supported Servers Web** (サポートされているサーバーの識別ウェブ) パーツには、次の情報の含まれるレポートが表示されます。

- 1 **Identify servers that support automated updating** (自動アップデートをサポートするサーバーの識別) セクションには、次のレポートが含まれます。
  - **Computers scanned** (スキャンされたコンピュータ) : このレポートは、コンプライアンスチェックの完了時に生成されます。このレポートには、Dell Management Console によって検出されたサーバー (Lifecycle Controller または Symantec Management Agent を装備) を一覧表示する **Computers Evaluated for Dell Automated Patching Support** (Dell 自動パッチサポートのために評価されたコンピュータ) ページへのリンクが示されます。この一覧には、アップデートをサポートするサーバーが含まれています。
  - **Supported servers** (対応サーバー) : このレポートは、コンプライアンスチェックの完了時に生成されます。このレポートには、Altiris Agent 対応パッチアップデート、Lifecycle Controller 対応パッチアップデート、またはその両方をサポートするサーバーの一覧が含まれる **Computers Evaluated for Dell Automated Patching Support** (Dell 自動パッチサポートのために評価されたコンピュータ) ページへのリンクが示されます。
- 1 **Schedule or begin an identification scan** (識別スキャンのスケジュールまたは開始) セクションでは、対応オペレーティングシステム、サーバーモデル、および Altiris Agent が装備された Dell システムを検出できます。管理対象システム上に Altiris Agent がインストールされていない場合は、**Install Altiris Agent** (Altiris Agent のインストール) をクリックしてタスクを完了できます。

**Inventory Supported Servers** (対応サーバーのインベントリ) ウェブパーツには、インベントリが正常に実行された Dell システムの一覧を含むレポートが表示されます。一覧された Dell システムは、アップデートの受信準備ができていて、前提条件を満たしていない、インベントリを返さないのいずれかの状態になっています。インベントリスキャンをスケジュールまたは開始するには、次の作業を実行します。

- 1 パッチアップデートに対応した Windows オペレーティングシステムがインストールされている Dell サーバーを判定する場合は、**Windows Compliance Assessment Task** (Windows コンプライアンスアセスメントタスク) をクリックします。
- 1 パッチアップデートに対応した Linux オペレーティングシステムがインストールされている Dell サーバーを判定する場合は、**Linux Compliance Assessment Task** (Linux コンプライアンスアセスメントタスク) をクリックします。
- 1 パッチアップデートに対応した Lifecycle Controller 対応 Dell サーバーを判定する場合は、**Compliance Assessment Task for Lifecycle Controller enabled Servers** (Lifecycle Controller 対応サーバーのコンプライアンスアセスメントタスク) タスクをクリックします。

**Review update compliance of servers that are ready to receive updates** (アップデートの受信準備ができていないサーバーのアップデートコンプライアンスの確認) ウェブパーツでは、サポートされている Dell システムのコンプライアンスを表示し、アップデートを配布します。最新状態のサーバー、1 つまたは複数の推奨アップデートが適用されていないサーバー、1 つまたは複数のオプションのアップデートが存在するサーバー、1 つまたは複数の緊急アップデートが適用されていないサーバーが円グラフで示されます。円グラフの各セクションをクリックすると、適用可能なアップデートが配布されます。

Altiris Agent 対応パッチアップデートと Lifecycle Controller 対応パッチアップデート用の **Review Status of update tasks** (アップデートタスクのステータスの確認) ウェブパーツは、Altiris Agent 対応パッチ処理の個別アップデートまたはバンドルアップデートのロールアウトジョブのステータス、および Lifecycle Controller 対応サーバーのロールアウトジョブのステータスが表示されます。

---

## DUP とシステムバンドル

Dell アップデートパッケージ (DUP) は、システムコンポーネント (Dell システムの BIOS、ドライバ、ファームウェアなど) をアップデートするために設計されています。DUP を集めたものが、Dell システムアップデートの **セット** としてリリースされます。

パッチ管理ソリューションのインタフェースでは、システムアップデートセットは **バンドル** と呼ばれます。お使いの Dell システムには、個々の DUP を配布するのではなく、システムアップデートセットを配布することをお勧めします。DUP は DUP ロールアウトジョブを作成するために使用され、システムアップデートセットはバンドルロールアウトジョブを作成するために使用されます。

Altiris Agent 対応パッチアップデートを使用してシステムコンポーネントをアップデートする場合は、Symantec Management Agent をインストールしておく必要があります。このエージェントは、Lifecycle Controller 対応アップデートの場合には必要ありません。ただし、その場合には、システムコンポーネントのアップデートを完了させるために、Lifecycle Controller が使用可能になる必要があります。

Lifecycle Controller 対応パッチは Altiris Agent 対応パッチ管理でサポートされるすべてのアップデートをサポートするわけではないので、バンドルアップデートを実行するには、Altiris Agent 対応パッチの使用が推奨されます。

 **メモ:** デフォルトでは、Dell Management Console は、Lifecycle Controller 対応パッチアップデートよりも Altiris Agent 対応パッチを優先します。

Altiris Agent を使用してサーバーをアップデートするには、次の手順を実行します。

1. 接続プロファイルを作成し、設定します。
2. Altiris Agent 対応パッチアップデートを必要とする Dell システムを検出します。
3. ネットワーク接続またはインターネット設定を **Configure Proxy** (プロキシの設定) で設定します。
4. DUP カタログを **DUP Catalog Import** (DUP カタログのインポート) でインポートします。  
このリリースの Dell Management Console へアップグレードした場合は、DUP カタログを再インポートする必要があります。
5. **Download Inventory Collector** (インベントリコレクタのダウンロード) に示された URL から **Dell インベントリコレクタツール** をダウンロードします。
6. ベンダー情報を **Solution Global Settings** (ソリューショングローバル設定) で設定します。ftp.dell.com または Server Update Utility から DUP をダウンロードできます。
7. エージェントを **Altiris Agent Installation** (Altiris Agent のインストール) でインストールします。
8. Windows、Linux、またはその両方のコンプライアンスのコンプライアンスチェックを実行します。コンプライアンスチェック中にシステムインベントリ情報が収集されます。
9. レポートを使用してデータを表示し、**Hardware Update Compliance** (ハードウェアアップデートコンプライアンス) レポートから Altiris Agent 対応パッチアップデートを開始するか、

**Manage Updates** (アップデートの管理) で Altiris Agent 対応パッチアップデートを実行します。レポートを表示するには、**Check applicable updates by computers** (コンピュータごとの適用可能なアップデートの確認) をクリックします。

アップデートまたはバンドルをロールアウトするために Lifecycle Controller を使用してサーバーをアップデートするには、次の手順を実行します。

1. WS-MAN プロトコルを使用して接続プロファイルを作成し、設定します。
2. Lifecycle Controller 対応パッチアップデートを必要とする Dell システムを検出します。(WS-MAN 接続プロファイルを使用して iDRAC 6 Enterprise を検出します。検出されたデバイスは、Dell コンピュータに分類されている必要があります。エージェントレスインベントリを使用して、検出されたデバイスの情報を収集します。)
3. ネットワーク接続またはインターネット設定を **Configure Proxy** (プロキシの設定) で設定します。
4. DUP カタログを **DUP Catalog Import** (DUP カタログのインポート) でインポートします。
5. これらのシステムに対してエージェントレスインベントリを実行して、システムインベントリ情報を収集します。
6. Lifecycle Controller 対応サーバーのコンプライアンスアセスメントタスクを実行します。
7. レポートを使用してデータを表示し、**Hardware Update Compliance** (ハードウェアアップデートコンプライアンス) レポートから Lifecycle Controller 対応パッチアップデートを開始するか、**Manage Updates** (アップデートの管理) で Lifecycle Controller 対応パッチアップデートを実行します。レポートを表示するには、**Check applicable updates by computers** (コンピュータごとの適用可能なアップデートの確認) をクリックします。

Lifecycle Controller を使用してアップデートされたサーバーにロールバックを使用するには、次の手順を実行します。

1. レポートを表示するには、次のいずれかを実行します。
  1. **Reports** (レポート) → **All Reports** (すべてのレポート) → **Software** (ソフトウェア) → **Patch Management for Dell Servers** (Dell サーバーのパッチ管理) → **Hardware Update Compliance** (ハードウェアアップデートコンプライアンス) を選択します。
  1. **Patch Management for Dell Servers Home** (Dell サーバーのパッチ管理ホーム) ポータルページの **Getting Started** (はじめに) ウェブパーツ内で、**Check applicable updates by computers** (コンピュータごとの適用可能なアップデートの確認) をクリックします。
2. **Available Updates for Rollback** (ロールバックに使用可能なアップデート) レポート内のデータを表示します。
3. ステージングおよび配布のウィザードを使用して Lifecycle Controller 対応パッチロールバックを実行します。

---

## DUP カタログのインポート

**DUP Catalog Import** (DUP カタログのインポート) ページを使用して、ダウンロード可能な Dell ソフトウェア管理パッケージを取得します。

Altiris Agent 対応パッチアップデートまたは Lifecycle Controller 対応パッチアップデートのコンプライアンスアセスメントを実行して、管理対象システムに適用可能な DUP を確認します。

ステージングアクションまたはステージングと配布アクションを選択している場合にのみ、このアセスメントに基づいて、適用可能な DUP が Dell Management Console にダウンロードされます。最新の推奨 DUP を取得するには、カタログのダウンロードは欠かせません。

DUP カタログのインポートタスクでは、カタログのダウンロードを自動化できます。デルからリリースされる最新の DUP を確実に入手するために、このタスクを実行するスケジュールを指定します。

## Dell アップデートカタログのダウンロード

**Manage Dell Hardware Updates** (Dell ハードウェアアップデートの管理) ページに DUP カタログのインポートタスクを投入するために必要なソフトウェア管理リソースをダウンロードできます。

Dell アップデートカタログをダウンロードするには、次の手順を実行します。

1. **Home** (ホーム) メニューで、**Patch Management for Dell Servers Home** (Dell サーバーのパッチ管理ホーム) をクリックします。
2. **Getting Started** (はじめに) ウェブパーツの **Configuration** (設定) にある **Download Updates Catalog** (アップデートカタログのダウンロード) をクリックします。
3. 右ペインで、次のいずれかを選択します。
  1. **Dell site** (Dell サイト)
  1. **Local storage** (ローカルストレージ) (DUP がローカルに保存されている場合)
  1. **Only if modified** (変更されている場合のみ) は、アップデートされたファイルのみがダウンロードされるように、デフォルトで選択されています。それにより、不要なダウンロードが回避されます。
4. **Save Changes** (変更の保存) をクリックします。
5. **New Schedule** (新規スケジュール) をクリックして、タスクのスケジュールを指定します。 **Schedule Task** (タスクのスケジュール) ダイアログボックスで、タスクを実行するスケジュールを指定するか、**Now** (今すぐ) を選択してタスクをただちに実行します。

## Dell インベントリコレクタツール

Dell インベントリコレクタツールにより、現在のオペレーティングシステムとハードウェアファームウェアに関する情報を収集できます。Dell インベントリコレクタタスクは、Altiris Agent 対応パッチアップデートの場合にのみ必要です。

このツールにより、お使いの Dell システムでアップデートを受信可能かどうか判定されます。デルは、Dell サーバーに対し、オペレーティングシステムが Windows と Linux の場合でそれぞれ異なるツールを提供しています。これらのツールは、3 か月ごとにアップデートされ、公開されている Symantec のダウンロードポータルから .cab ファイルとしてダウンロードできます。なお、Dell インベントリコレクタタスクでは、各ツールが自動的にダウンロードされます。

Dell インベントリコレクタをダウンロードするには、次の手順を実行します。

1. Home(ホーム)メニューで、Patch Management for Dell Servers Home(Dell サーバーのパッチ管理ホーム)をクリックします。
2. Getting Started(はじめに)ウェブパーツの Configuration(設定)にある Download Inventory Collector(インベントリコレクタ)をクリックします。
3. 右ペインで、次のいずれかを選択します。
  1. Web URL: To(ウェブ URL:宛先)。Dell インベントリツールを solutionsam.com/imports/7\_0/Patch/Dell/dellinvtool\_windows.cab または solutionsam.com/imports/7\_0/Patch/Dell/dellinvtool\_linux.cab からダウンロードします。
  1. Local storage(ローカルストレージ) (.cab ファイルがローカルに存在する場合)
4. Save Changes(変更の保存)をクリックします。
5. New Schedule(新規スケジュール)をクリックして、タスクのスケジュールを指定します。Schedule Task(タスクのスケジュール)ダイアログボックスで、タスクを実行するスケジュールを指定するか、Now(今すぐ)を選択してタスクをただちに実行します。

## Dell ベンダー設定ページ

DUPs Update Preference Settings(DUP のアップデート優先設定)オプションでは、Altiris Agent 対応パッチアップデートが Lifecycle Controller 対応パッチアップデートよりも優先されるように設定されています。

1. Home(ホーム)メニューで、Patch Management for Dell Servers Home(Dell サーバーのパッチ管理ホーム)をクリックします。
2. Getting Started(はじめに)ウェブパーツの Configuration(設定)の下にある Solution Global Settings(ソリューショングローバル設定)をクリックします。
3. 右ペインにある Dell Vendor Configuration(Dell ベンダー設定)ページ 上で変更を行います。
4. Apply(適用)をクリックします。

このページを設定して、DUP 配布方法をセットアップします。設定の一部は、Rollout Job(ロールアウトジョブ)ウィザードでデフォルト値として使用されます。新規にダウンロードされるすべての DUP にデフォルトでこれらの設定が適用されます。これらの設定を変更しても、既存のソフトウェアアップデートタスクとパッケージは、これらのデフォルト値でアップデートされません。Manage Software Updates(ソフトウェアアップデートの管理)ページからパッケージを再作成することにより、それらを強制的にアップデートできます。

### General(全般)タブのオプション

オプション	説明
DUPs Download Verification(DUP のダウンロード検証)	すべての DUP がデルによって認定されていることを確認します。このオプションは、デフォルトでは選択されています。
DUPs Download Location(DUP のダウンロード場所)	DUP がデルの FTP サイトから直接ダウンロードされるように、デフォルトでデルの FTP サイトが選択されています。別の場所から DUP をダウンロードする場合は、Local storage(ローカルストレージ)をクリックし、その場所をフィールドに指定します。
DUPs Update Preference Settings(DUP のアップデート優先設定)	デフォルトでは、Apply updates using Altiris Agent(Altiris Agent を使用してアップデートを適用)に設定されています。Lifecycle Controller を優先するように設定するには、Apply updates using Lifecycle Controller(Lifecycle Controller を使用してアップデートを適用)を選択します。  <b>メモ:</b> Altiris agent と Lifecycle Controller のどちらを使用してもサーバーをアップデートできる場合、アップデートは優先設定に基づいて実行されます。
DUPs Distribution Options(DUP の配布オプション)	Windows オペレーティングシステム用、Linux オペレーティングシステム用、または Lifecycle Controller 用に配布された DUP を受信するように、ターゲットサーバーを指定します。

### Advanced(詳細)タブのオプション

オプション	説明
Package Defaults(パッケージデフォルト)	ソフトウェアアップデートパッケージを削除する頻度を決定できます。
Package distribution	Allow Package Server distribution(パッケージサーバー配布を許可) - パッケージサーバーがすべてのソフトウェアアップデートパッケージを処理する

(パッケージ配布)	<p>ように、デフォルトで選択されています。詳細に関しては、Symantec Management Platform のマニュアルを参照してください。</p> <p>Use alternate download location on Package Server(パッケージサーバー上の別のダウンロード場所を使用) - パッケージサーバーにパッケージをダウンロードするための別の場所を指定し、Windows オペレーティングシステムと Linux オペレーティングシステムを実行している Dell システム用にそれらの場所を指定できます。</p> <p>Use alternate download location on Package Server(パッケージサーバー上の別のダウンロード場所を使用) - パッケージサーバーにパッケージをダウンロードするための別の場所を指定し、Windows オペレーティングシステムと Linux オペレーティングシステムを実行している Dell システム用にそれらの場所を指定できます。</p>
-----------	---

#### Program(プログラム)タブのオプション

オプション	説明
Program Defaults (プログラムデフォルト)	<p>Run with rights(権限を指定して実行) - プログラムが System Account(システムアカウント)、Logged in User(ログインユーザー)、Specified User(指定ユーザー)アカウントのいずれかで実行されるかを指定します。Specified User(指定ユーザー)を選択する場合 - フィールドにユーザー名を指定します。このオプションは、Windows を実行しているシステム上でのみ適用可能です。</p> <p>Program can run(プログラムの実行可能条件) - プログラムが実行できる条件を指定します。選択肢には、Only when a user is logged on(ユーザーがログオンしている場合のみ)、Whether or not a user is logged on(ユーザーのログオンとは無関係)、および Only when no user is logged on(ログオンしているユーザーがいない場合のみ)があります。このオプションは、Windows を実行しているシステム上でのみ適用可能です。</p> <p>Minimum connection speed(最小接続速度) - Use Agent settings(エージェントの設定を使用)がデフォルトで選択されています。別の速度を指定することもできます。</p> <p>Terminate after(次の時間後に終了) - ソフトウェアアップデートタスクが終了させられるまでの時間を指定します。</p>
Agent Events(エージェントイベント)	<p>関連するイベントを管理対象システムから Dell Management Console システムへ送信するように設定します。</p>

## Dell アップデートパッケージのダウンロード

ftp.dell.com または Server Update Utility から DUP をダウンロードできます。DUP のダウンロード場所は、[Dell Vendor Configuration\(Dell ベンダー設定\)ページ](#)で設定できます。

## パッチアップデートに対応した Linux Dell サーバーの検出

DUP の受信準備のできている、Linux オペレーティングシステムを実行している対応 Dell システムをすべて検出できます。

Linux オペレーティングシステムを実行しているパッチアップデート対応 Dell システムを検出するには、次の手順を実行します。

1. Home(ホーム)メニューで、Patch Management for Dell Servers Home(Dell サーバーのパッチ管理ホーム)をクリックします。
2. Getting Started(はじめに)ウェブパーツの Run compliance check on(コンプライアンスチェックの実行)で Linux Servers (Linux サーバー)をクリックします。
3. Determine Linux Patchable Dell Servers Job(Linux のパッチ可能な Dell サーバーの判定ジョブ)ページで、Quick Run(クイック実行)をクリックし、サーバーを選択してジョブをただちに実行するか、Schedule(スケジュール)をクリックしてジョブを定期的に行うためのスケジュールを指定します。

## パッチアップデートに対応した Windows Dell サーバーの検出

DUP の受信準備のできている、Windows オペレーティングシステムを実行している Dell システムを検出できます。

Windows オペレーティングシステムを実行しているパッチアップデート対応 Dell システムを検出するには、次の手順を実行します。

1. Home(ホーム)メニューで、Patch Management for Dell Servers Home(Dell サーバーのパッチ管理ホーム)をクリックします。
2. Getting Started(はじめに)ウェブパーツの Run compliance check on(コンプライアンスチェックの実行)で Windows Servers (Windows サーバー)をクリックします。
3. Determine Windows Patchable Dell Servers Job(Windows のパッチ可能な Dell サーバーの判定ジョブ)ページで、Quick Run(クイック実行)をクリックし、サーバーを選択してジョブをただちに実行するか、Schedule(スケジュール)をクリックしてジョブを定期的に行うためのスケジュールを指定します。

## パッチアップデートに対応した Lifecycle Controller 対応 Dell サーバーの検出

Lifecycle Controller 対応パッチアップデートをサポートしている Dell サーバーを検出できます。

Lifecycle Controller を装備したパッチアップデート対応 Dell サーバーを検出するには、次の手順を実行します。

1. **Home**(ホーム)メニューで、**Patch Management for Dell Servers Home**(Dell サーバーのパッチ管理ホーム)をクリックします。
2. Dell Management Console から、デバイス検出ウィザードを使用して Dell サーバーを検出します。
3. Lifecycle Controller を装備している検出されたサーバー上で、エージェントレスインベントリウィザードを使用してインベントリを実行します。
4. **Getting Started**(はじめに)ウェブページの **Run compliance check on**(コンプライアンスチェックの実行)で**Lifecycle Controller Enabled Server**(Lifecycle Controller 対応サーバー)をクリックします。
5. **Compliance Assessment Task for Lifecycle Controller enabled Servers**(Lifecycle Controller 対応サーバーのコンプライアンスアセスメントタスク)ページで、Lifecycle Controller 対応パッチを実行するサーバーを選択し、**New Schedule**(新規スケジュール)をクリックして、ジョブを定期的に行うためのスケジュールを指定します。デフォルトでは、Lifecycle Controller を装備したすべての Dell サーバーが、このタスクに対して選択されています。

## Dell パッチ管理レポートへのアクセス

Altiris Agent 対応および Lifecycle Controller 対応のパッチ管理データをレポートで表示し、管理できます。

Dell パッチ管理レポートにアクセスするには、次の手順を実行します。

1. **Reports**(レポート)メニュー上で、**All Reports**(すべてのレポート)をクリックします。
2. 左ペインで、**Reports**(レポート)→ **Software**(ソフトウェア)→ **Patch Management for Dell Servers**(Dell サーバーのパッチ管理)をクリックします。
3. 必要なレポートの含まれるフォルダを選択します。

たとえば、**Dell Server Patching Inventory**(Dell サーバーパッチインベントリ)レポート、**Hardware Update Compliance**(ハードウェアアップデートコンプライアンス)レポート、**Update Installation Results**(アップデートインストール結果)レポートなどがあります。

## コンプライアンスアセスメントタスク

Lifecycle Controller 対応サーバー用のコンプライアンスアセスメントタスクは、アップデートカタログ内の使用可能なアップデートをサーバーに現在インストールされているアップデートと比較して、ターゲットサーバー内のさまざまなコンポーネントに対して適用可能なアップデートを決定します。このタスクには、インベントリの実行中に収集された情報とアップデートカタログ内に存在する情報に依存します。そのため、ターゲットサーバーに対するインベントリタスクの実行およびカタログのダウンロードをコンプライアンスアセスメントタスクの実行前に完了しておく必要があります。

コンプライアンスアセスメントタスクは、**Getting started**(はじめに)ウェブページ上のリンクをクリックし、スケジュールとターゲットサーバーの情報を選択することでスケジュールできます。コンプライアンスアセスメントタスクが正常に完了した後、ユーザーは、サーバー内の各種コンポーネントについてインストール済みアップデートのバージョンと使用可能なアップデートのバージョンが示されたさまざまなハードウェアコンプライアンスレポートを閲覧できます。

## Dell ハードウェアアップデートの管理

**Manage Dell Hardware Updates**(Dell ハードウェアアップデートの管理)ページでは、すべてのシステムアップデートセットを表示し、ステージングできます。DUP カタログファイル(.cab)は、[DUP カタログのインポート](#)タスクで [ftp.dell.com](http://ftp.dell.com) または『Dell Server Updates DVD』からダウンロードできます。システムアップデートセットをステージングする場合、関連する DUP が Dell Management Console システムにダウンロードされます。システムアップデートセットのすべての DUP のダウンロードが完了すると、それらの DUP をバンドルロールアウトジョブで配布する準備が整います。**Manage Dell Hardware Updates**(Dell ハードウェアアップデートの管理)ページで、ステージングおよび配布のタスクを作成できます。[ステージングおよび配布ウィザード](#)を参照してください。

Dell ハードウェアアップデートの管理ページで使用可能なオプション

オプション	説明
<b>Manage Bundles(バンドルの管理)</b> Manage Updates(アップデートの管理)	DUP のバンドルを配布するか(Manage Bundles(バンドルの管理))、個々の DUP を配布するか(Manage Updates(アップデートの管理))を選択できます。
<b>Filter by(次で絞り込み)</b>	システムのモデルまたは名前を絞り込めます。
<b>OS Type(OS タイプ)</b>	Windows、Linux、またはすべてのオペレーティングシステムタイプで絞り込めます。
<b>Group(グループ)</b>	組織グループ内で検索できます。
<b>Updates(アップデート)</b>	デフォルトですべてのアップデートを表示するか、適用可能なアップデートのみを表示できます。
<b>Severity(重要度)</b>	重要度レベルを選択してアップデートを絞り込めます。
<b>Stage and Distribute All Bundles(すべてのバンドルのステージングと配布)</b>	リストされているすべてのバンドルをステージングし、配布できます。
<b>Stage and Distribute Selected Bundles(選択したバンドルのステージングと配布)</b>	選択されたバンドルのみをステージングし、配布できます。
<b>Manage Selected Bundle(選択したバンドルの管理)</b>	バンドルを開いて、単一 DUP のロールアウトジョブを作成します。
<b>Bundle Name(バンドル名)</b>	システムアップデートセット(バンドル)の名前です。
<b>Release Date(リリース日)</b>	バンドルがリリースされた日です。
<b>Severity(重要度)</b>	バンドルの重要度レベルで、たとえば、 <b>Urgent</b> (緊急)などです。

Calendar(カレンダー)	From(開始日)と To(終了日)を指定でき、その期間にリリースされたバンドルが表示されます。
# of Computers(コンピュータの数)	影響を受ける Dell システムの数です。
# Updates(アップデートの数)	バンドル内の DUP の数です。
# Downloaded(ダウンロード済みの数)	関連するバンドルについてすでにダウンロードされた DUP の数です。

## DUP のステージングと配布

Manage Dell Hardware Updates(Dell ハードウェアアップデートの管理)ページからバンドルをステージングし、配布できます。このページには、使用可能なすべてのバンドルが一覧されています。バンドルをステージングする場合、関連するすべての DUP が Dell ウェブサイトの [ftp.dell.com](http://ftp.dell.com) から Dell Management Console システムにダウンロードされます。配布を選択することにより、選択したシステムに対してバンドルを導入およびアップデートできます。DUP は、ローカルストレージ([Dell Server Updates DVD]など)からダウンロードすることもできます。

DUP は、Dell システムタイプ、オペレーティングシステム、重要度、およびグループで絞り込みできます。

表示されているすべての DUP をステージングし、配布するには、次の手順を実行します。

1. Home(ホーム)メニューで、Patch Management for Dell Servers Home(Dell サーバーのパッチ管理ホーム)をクリックします。
2. Getting Started(はじめに)ウェブパーツから、Manage Updates (アップデートの管理)をクリックします。
3. 右ペインで、アップデートを適用するデバイスを選択し、次のいずれかを実行します。
  1. Stage and Distribute All Updates(すべてのアップデートのステージングと配布)を選択 - すべてのサーバーに対して適用可能なすべてのバンドルがステージングされ、個々の DUP が、サーバーの要件に基づいて、サーバー上にプッシュおよびインストールされます。
  1. Stage and Distribute Selected Updates(選択したアップデートのステージングと配布)を選択 - 選択したバンドルのみがステージングされ、個々の DUP が、サーバーの要件に基づいて、サーバー上にプッシュおよびインストールされます。
  1. Manage Selected Updates(選択したアップデートの管理)を選択 - バンドルから選択した DUP のみがステージングされ、選択された DUP がサーバー上にプッシュおよびインストールされます。

## ステージングおよび配布ウィザード

Stage and Distribute(ステージングと配布)ウィザードにより、ロールアウトジョブが作成されます。ロールアウトジョブは、Dell アップデートパッケージ(DUP)を管理対象システムに配布します。このウィザードは、該当するシステムに DUP のみをインストールするように、ターゲットを自動的に絞り込みます。

Altiris Agent 対応バッチと Lifecycle Controller 対応バッチの両方をサポートする Windows サーバーの場合、1 つのターゲットの下でのみアップデートされるようにサーバーを選択します。たとえば、Windows サーバーの Altiris Agent 対応バッチアップデートを使用して DUP またはバンドルを適用するには、そのサーバーが Windows ターゲットのみに追加される必要があります。

アップデートオプションは、選択されたターゲットに基づきます。

1. Windows Targets(Windows ターゲット)オプションは、レポートから Windows の DUP またはバンドルを選択した場合に使用できます。
1. Linux Targets(Linux ターゲット)オプションは、レポートから Linux の DUP またはバンドルを選択した場合に使用できます。
1. Lifecycle Controller Enabled Targets(Lifecycle Controller 対応ターゲット)オプションは、レポートから Windows の DUP またはバンドル、その両方、もしくはロールバックアップデートを選択した場合に使用できます。

表 12-1. ステージングと配布ウィザードのオプション

オプション	説明
Reboot Options(再起動オプション)	Reboot immediately(ただちに再起動) - DUP のインストール直後に再起動する場合に選択します。  Lifecycle Controller 対応サーバーの場合、Reboot immediately(ただちに再起動)オプションを有効にしなければ、再起動されるまでサーバーはアップデートしません。  Do not Reboot(再起動しない) - DUP のインストール後に再起動しない場合に選択します。
Installation Options(インストールオプション)	Silent(サイレント) - サイレントインストールを実行する場合に選択します。  Silent, allow downgrade(サイレント、ダウングレードを許可) - 古い DUP をインストールする場合に選択します。
Choose Connection Profile for Lifecycle Controller enabled Servers(Lifecycle Controller 対応サーバーの接続プロファイルの選択)	Connection profile(接続プロファイル) - 既存のプロファイルを選択および編集する場合に選択します。  New(新規) - 新しい接続プロファイルを作成する場合に選択します。  これは、Lifecycle Controller ベースのアップデートの場合にのみ必要です。選択した WS-MAN 接続プロファイルは、アップデートされるサーバーの検出に使用される接続プロファイルとは異なるものにできます。バッチに使用される WS-MAN 接続プロファイルには、Lifecycle Controller ベースのバッチを実行するために、ターゲットサーバーの iDRAC 上での Administrator 権限が必要です。
Schedule(スケジュール)	Now(今すぐ) - DUP をただちにインストールする場合に選択します。  Schedule(スケジュール) - DUP のインストールをスケジュールする場合に選択します。
Windows Targets(Windows ターゲット)	ロールアウトジョブを適用するターゲットを選択する場合に選択します。ターゲット内の適用可能なコンピュータのみが、ロールアウトジョブから DUP を受信します。
Lifecycle Controller Enabled Targets	ロールアウトジョブを適用するターゲットを選択する場合に選択します。適用可能なターゲットのみが、ロールアウトジョブから DUP を受

(Lifecycle Controller 対応ターゲット)	信します。
Linux Targets(Linux ターゲット)	ロールアウトジョブを適用するターゲットを選択する場合には選択します。ターゲット内の適用可能なコンピュータのみが、ロールアウトジョブから DUP を受信します。
Distribute Bundles List(配布バンドルのリスト)	ロールアウトジョブで配布される DUP バンドルのリストです。
Create(作成)	ウィザードを終了し、ステージングと配布のジョブを作成します。

## ロールアウトジョブ

ロールアウトジョブは、Dell アップデートパッケージを管理対象システムに配布することを可能にする一連のタスクで構成されます。

次のロールアウトジョブを表示できます。

### 1. DUP ロールアウトジョブ

DUP ロールアウトジョブは、単一の DUP を含み、Jobs and Tasks(ジョブとタスク) → System Jobs and Tasks(システムのジョブとタスク) → Software(ソフトウェア) → Patch Management for Dell Servers(Dell サーバーのパッチ管理) → Rollout Jobs(ロールアウトジョブ) → DUPs(DUPフォルダに保存されています)。

### 1. バンドルロールアウトジョブ

バンドルロールアウトジョブは、システムアップデートセット内のすべての DUP を含み、Jobs and Tasks(ジョブとタスク) → System Jobs and Tasks(システムのジョブとタスク) → Software(ソフトウェア) → Patch Management for Dell Servers(Dell サーバーのパッチ管理) → Rollout Jobs(ロールアウトジョブ) → Bundles(バンドル)フォルダに保存されています。

ロールアウトジョブは、サーバーコンポーネントのみを新しいバージョンにアップデートします。ロールアウトジョブは、ターゲットサーバーに現在インストールされているものよりも古いアップデートが含まれていると失敗します。その場合は、ダウングレードを強制的に実行するオプションがあります。

## ロールアウトジョブの作成

ロールアウトジョブは、管理対象システムにアップデートをインストールするために作成します。

DUP ロールアウトジョブを作成するには、次の手順を実行します。

1. **Manage(管理)** → **Software(ソフトウェア)** をクリックします。
2. 左ペインで、**Software(ソフトウェア)** → **Manage Dell Hardware Updates(Dell ハードウェアアップデートの管理)** をクリックします。
3. 右ペインで、バンドルを選択します。
4. **Manage Selected Updates(選択したアップデートの管理)** をクリックします。

選択したバンドル内のすべての DUP が表示されます。

5. 配布するアップデートを右クリックし、**Stage and Distribute Selected Updates(選択したアップデートのステージングと配布)** をクリックします。

 **メモ:** 複数の DUP を選択しても、Lifecycle Controller を使用してアップデートが実行される場合は単一のロールアウトジョブが作成されます。

6. DUP ロールアウトジョブの作成後、Jobs and Tasks(ジョブとタスク) → System Jobs and Tasks(システムのジョブとタスク) → Software(ソフトウェア) → Patch Management for Dell Servers(Dell サーバーのパッチ管理) → Server(サーバー)フォルダ内の **Stage and Distribute(ステージングと配布)** ジョブに表示されます。このジョブは、読み取り専用であり、ロールアウトジョブの進行状況を表示するために使用されます。ステージングと配布のタスクが完了した後、ロールアウトジョブが作成されます。

バンドルロールアウトジョブを作成するには、次の手順を実行します。

1. **Manage(管理)** → **Software(ソフトウェア)** をクリックします。
2. 左ペインで、**Software(ソフトウェア)** → **Manage Dell Hardware Updates(Dell ハードウェアアップデートの管理)** をクリックします。
3. 右ペインで、表内のバンドルを選択します。
4. **Stage and Distribute Selected Updates(選択したアップデートのステージングと配布)** をクリックします。

5. ステージングと配布のタスクが、Jobs and Tasks(ジョブとタスク) → System Jobs and Tasks(システムのジョブとタスク) → Software(ソフトウェア) → Patch Management for Dell Servers(Dell サーバーのパッチ管理) → Server(サーバー)フォルダ内の **Stage and Distribute(ステージングと配布)** ジョブに表示されます。このジョブは、読み取り専用であり、ロールアウトジョブの進行状況を表示するために使用されます。ステージングと配布のタスクが完了した後、ロールアウトジョブが作成されます。

6. バンドルロールアウトジョブの作成後、Jobs and Tasks(ジョブとタスク) → System Jobs and Tasks(システムのジョブとタスク) → Software(ソフトウェア) → Patch Management for Dell Servers(Dell サーバーのパッチ管理) → Rollout Jobs(ロールアウトジョブ) → Bundles(バンドル)フォルダに移動して、バンドルロールアウトジョブのステータスを表示します。

## ロールアウトジョブのステータスの表示

**アップデートのステージングと配布** ジョブは、DUP を処理し、個々の DUP またはバンドルアップデートのロールアウトジョブを作成します。

ロールアウトジョブの状態を表示する場合：

Dell Management Console で、次のいずれかを実行します。

- 1 **Manage (管理)** → **Jobs and Tasks (ジョブとタスク)** をクリックします。
- 1 **Patch Management for Dell Servers Home (Dell サーバーのパッチ管理ホーム)** をクリックします。ロールアウトジョブの状態が、**Review status of update tasks (アップデートタスクの状態の確認)** ウェブパーツに表示されます。

ロールアウトジョブを表示する場合：**Jobs and Tasks (ジョブとタスク)** → **System Jobs and Tasks (システムのジョブとタスク)** → **Software (ソフトウェア)** → **Patch Management for Dell Servers (Dell サーバーのパッチ管理)** → **Rollout Jobs (ロールアウトジョブ)** → **DUPs/Bundles (DUP/ バンドル)** を選択します。

## Lifecycle Controller 対応ロールアウトジョブ

Lifecycle Controller 対応ロールアウトジョブは、Altiris ジョブのインフラストラクチャをベースにしたジョブであり、Lifecycle Controller 対応パッチタスクすべてが含まれています。単一のロールアウトジョブを実行して、複数のアップデートを適用できます。

たとえば、**1** 個のアップデートが適用される場合、ロールアウトジョブには次のタスクが含まれます。

- 1 **1** 個の Lifecycle Controller 対応アップデート送信タスク
- 1 **1** 個の Lifecycle Controller 対応アップデート実行タスク
- 1 **1** 個の Lifecycle Controller 状態のポーリングタスク

Lifecycle Controller 対応ロールアウトジョブは、**Hardware Update Compliance (ハードウェアアップデートコンプライアンス)** レポートのひとつによって、**1** つ、または複数の DUP が管理対象システムに適用されるように選択した場合に作成されます。このジョブ内では、タスクごとに特定の機能があります。**アップデート送信** タスクでは、DUP が Dell Management Console からターゲット上の Lifecycle Controller にダウンロードされます。**アップデート実行** タスクでは、Lifecycle Controller が特定の DUP の適用を開始するようにします。**状態のポーリング** タスクでは、DUP の適用状態 (DUP の適用が正常に完了したかどうか) がチェックされます。アップデート後、ステータスメッセージが表示されます。

---

## ロールバックレポート

ロールバックレポートは、Lifecycle Controller 対応サーバー上で使用可能な、過去にインストールされた BIOS アップデートまたはファームウェアアップデートのバージョンのリストを表示します。ロールバックできるのは BIOS とファームウェアのみです。

次をロールバックすることはできません。

- 1 Universal Server Configurator (USC)
- 1 Dell Diagnostics アプリケーション
- 1 オペレーティングシステム (OS) のインストール用のドライバ

### ロールバックレポートの表示

- 1 レポートを表示するには、次のいずれかを実行します。
  - 1 **Reports (レポート)** → **All Reports (すべてのレポート)** → **Software (ソフトウェア)** → **Patch Management for Dell Servers (Dell サーバーのパッチ管理)** → **Hardware Update Compliance (ハードウェアアップデートコンプライアンス)** を選択します。
  - 1 **Patch Management for Dell Servers Home (Dell サーバーのパッチ管理ホーム)** ポータルページの **Getting Started (はじめに)** ウェブパーツ内で、**Check applicable updates by computers (コンピュータごとの適用可能なアップデートの確認)** をクリックします。
- 2 **Available Updates for Rollback (ロールバックに使用可能なアップデート)** レポート内のデータを表示します。

ロールバックレポート内で、次の作業を実行できます。

- 1 過去にインストールした BIOS またはファームウェアのバージョンにロールバックする場合：システムに適用するロールバックアップデートを選択し、**Rollback Selected Updates (選択したアップデートのロールバック)** をクリックします。
- 1 すべてのロールバックアップデートを適用する場合：**Rollback All Updates (すべてのアップデートのロールバック)** をクリックします。
- 1 ロールバックアップデートのバージョンをシステムに現在インストールされているバージョンと比較するには、**Installed Version (インストールバージョン)** フィールドと **Available Version (使用可能なバージョン)** フィールドに表示されているバージョンを比較します。
  - **Server (サーバー)** - ロールバックアップデートを適用可能なサーバーの名前を表示します。
  - **Device (デバイス)** - サーバー上でロールバックアップデートを適用可能なデバイスの名前を表示します。
  - **Type (タイプ)** - コンポーネントタイプ (BIOS または Firmware (ファームウェア)) を表示します。

---

## パッチ管理ソリューションのトラブルシューティング

トラブルシューティングの役に立つように、レポートおよび実行インスタンスの詳細情報にエラーコードが生成されます。

## Dell アップデートパッケージの終了コード

アップデートパッケージの実行後、終了コードが生成されます。それらは、Dell Update Execution Details(Dell アップデートの実行の詳細)レポートに表示されます。終了コードは、アップデートパッケージの実行後、実行結果を確認し、分析するのに役立ちます。

表 12-2. DUP 終了コード

値	メッセージ	説明
0	SUCCESSFUL	アップデートは正常に完了しました。
1	UNSUCCESSFUL	アップデート処理中にエラーが発生しました。アップデートは成功しませんでした。
2	REBOOT_REQUIRED	アップデートを適用するためにシステムを再起動してください。
3	DEP_SOFT_ERROR	次の原因が考えられます。 <ul style="list-style-type: none"><li>1 同じバージョンのソフトウェアにアップデートしようとした。</li><li>1 ソフトウェアの前のバージョンにダウングレードしようとした。</li></ul>
4	DEP_HARD_ERROR	必要なソフトウェアがシステムで見つかりませんでした。
5	QUAL_HARD_ERROR	アップデートパッケージを適用できません。 次の原因が考えられます。 <ul style="list-style-type: none"><li>1 オペレーティングシステムをアップデートパッケージがサポートしていない。</li><li>1 システムで検出されたデバイスとアップデートパッケージの互換性がない。</li></ul>
6	REBOOTING_SYSTEM	システムの再起動

## Windows Dell サーバー検出タスクの失敗エラーコード

次のエラーコードは、Windows Dell サーバー検出タスクが失敗したときに表示されます。これらのコードは、タスクの実行インスタンスの詳細情報内で見つかります。

表 12-3. Windows Dell サーバー検出タスクの失敗エラーコード

値	メッセージ	説明
10	Err_OK_IsDellServer	正常に実行されました。システムは Dell サーバーです。
11	Err_OK_IsNotDellServer	正常に実行されました。システムは Dell サーバーではありません。
12	Err_OK_IsNotSupportedDellServer	正常に実行されました。システムは Dell コンピュータですが、サポートされている Dell サーバーではないか、サポートされているオペレーティングシステムを使用していません。
-20	Err_EndofScript	現在、Err_EndofScript は使用されていません。
-21	Err_FileNotFound	サーバーリストファイル(DellServers.ini)が見つかりませんでした。
-22	Err_FailedStringSearch	現在、Err_EndofScript は使用されていません。
-24	Err_InvalidCmdArgument	コマンドライン引数に誤りがあります。空白、「/model」、または「/omsa」にする必要があります。
-25	Err_CantAccessWMI	WMIquery を実行できませんでした。インストールされていないか、稼動していません。

## Linux Dell サーバー検出タスクの失敗エラーコード

次のエラーコードは、Linux Dell サーバー検出タスクが失敗したときに表示されます。これらのコードは、タスクの実行インスタンスの詳細情報内で見つかります。

表 12-4. Linux Dell サーバー検出タスクの失敗エラーコード

値	メッセージ	説明
7	RPM_VERIFY_FAILED	RPM 検証に失敗しました。
10	Err_OK_IsDellServer	正常に実行されました。システムは Dell サーバーです。
11	Err_OK_IsNotDellServer	正常に実行されました。システムは Dell サーバーではありません。
12	Err_OK_IsNotSupportedDellServer	正常に実行されました。システムは Dell コンピュータですが、サポートされている Dell サーバーではないか、サポートされているオペレーティングシステムを使用していません。
21	Err_FileNotFound	障害。サーバーリストファイル(DellServers.ini)が見つかりませんでした。ファイル名は SupportedDellServers.txt に指定されているものと

		異なります。
24	Err_InvalidCmdArgument	障害。コマンドライン引数に誤りがあります。
25	Err_CantAccessDMI	DMIquery を実行できませんでした。

---

[目次に戻る](#)

[目次に戻る](#)

## レポート

### Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [レポートモジュールについて](#)
- [レポートのユーザーインターフェイス](#)
- [SQL レポートの作成](#)
- [Dell コンピュータレポートの作成](#)
- [Dell レポートの編集](#)
- [レポートの実行](#)
- [レポートの保存](#)
- [レポートの表示](#)
- [メトリックレポート](#)
- [グループメトリックレポートの表示](#)
- [レポートの設定 - カスタムターゲットグループ](#)

Dell Management Console のレポートモジュールにより、事前定義されたレポートを表示したり、Dell Management Console によって検出および監視されたさまざまなデバイス上で収集されるデータに対してカスタムレポートを作成したりできます。

事前定義されたレポートは、デバイス固有であり、CSV(スプレッドシート)形式、XML 形式、および HTML 形式で保存できます。

レポートモジュールを使用して、レポートを表示します。各レポートは、収集された情報を処理して次の情報を表示します。

- 1 実行されたタスクおよび成功または失敗したタスク
- 1 所有されている資産、その場所、およびその所有者

 **メモ:** レポートで入手できるデータは、リアルタイムのデータではなく、タイムラグが存在します。

レポートに関連したメモ

- 1 電力バジェットおよび電源プロファイルの情報は、次のプラットフォームではサポートされていません。
  - o R805(Dell OpenManage 5.5、OpenManage 6.1、または OpenManage 6.2)
  - o R905(OpenManage 6.1 または OpenManage 6.2)

したがって、電力バジェットおよび電源プロファイルの情報は、インベントリ(SNMP 検出)と電力バジェットレポートで利用できません。

---

## レポートモジュールについて

レポートモジュールを使用して、デバイスに関連したインベントリ、監視、およびパフォーマンスの詳細情報を表示します。

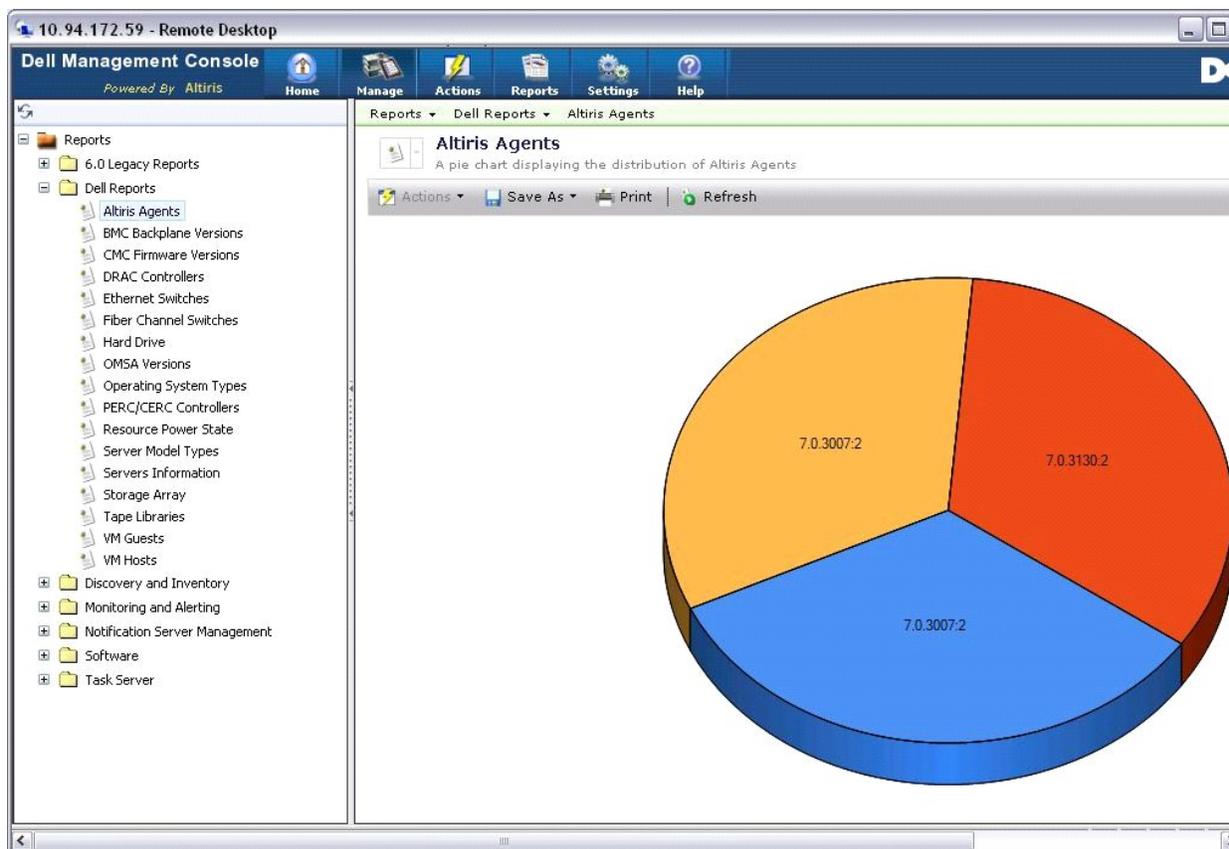
Dell Management Console レポートバックで既に提供されているさまざまなレポートを実行できます。また、シンプルなウィザードベースの手順に従ってカスタムレポートを作成することもできます。カスタムレポートは、非常にシンプルにすることも、SQL タイプのクエリを含めてより複雑なレポートにすることもできます。詳細に関しては、Symantec のユーザーガイドを参照してください。

---

## レポートのユーザーインターフェイス

Reports(レポート)ポータルページにアクセスするには、Reports(レポート)→ All Reports(すべてのレポート)を選択します。

## レポートのユーザーインターフェイスの説明



左ペインに、Reports (レポート) ツリーが表示されます。このツリーから、事前定義された Dell レポートにアクセスできます。

Dell Reports (Dell レポート) をクリックします。事前定義された Dell レポートとそれらの説明が右ペインに表示されます。

事前定義された各 Dell レポートは、右ペインに選択したレポートがグラフィック形式で表示されます。右ペインから、次の作業を実行できます。

- 1 表示されているレポートを別の形式 (例えば XML など) で表示します。
- 1 表示されているレポートをエクスポートします。
- 1 表示されているレポートを、特にウェブパーツとして保存します。[レポートの保存](#) を参照してください。
- 1 表示されているレポートを印刷します。

レポートの詳細情報を取得するには、円グラフ内の任意の場所をクリックします。

**メモ:** システムが新たに検出されても、その接続状態データはリソース接続状態レポートにすぐには表示されません。

## SQL レポートの作成

ニーズを満たすレポートが見つからない場合は、新しいレポートを作成し、目的に合った形式でデータを表示できます。

例えば、お使いのネットワーク上のサーバー上に存在するオペレーティングシステムに関するレポートが必要であるとします。

1. 左ペインの Reports (レポート) ツリーで、Reports (レポート) を右クリックし、New (新規) → Report (レポート) → SQL Report (SQL レポート) を選択します。
2. New SQL Report (新規 SQL レポート) ページの Data Source (データソース) タブで、次を入力します。
 

```
select [OS Name] from DiscoveredMachines
```
3. Apply (適用) をクリックします。
 

レポートに、それぞれ検出されたシステム上のオペレーティングシステムが表示されます。

## Dell コンピュータレポートの作成

Dell コンピュータレポートを新規に作成するには、次の手順を実行します。

1. **Reports**(レポート)ポータルページで、**Reports**(レポート)を右クリックし、**New**(新規)→**Report**(レポート)→**Computer Report** (コンピュータレポート)を選択します。
2. **Data Source**(データソース)タブの **Query**(クエリ)サブタブで、**Base Query**(基本クエリ)を選択し、**Base Resource Type**(基本リソースタイプ)ドロップダウンメニューから **Dell Computer**(Dell コンピュータ)を選択します。

 **メモ:** このドロップダウンメニューから、他の Dell レポートを作成することもできます。

3. **Fields**(フィールド)サブタブで、**Add**(追加)をクリックして属性を含めます。すべての Dell 属性については、[インベントリの属性](#)を参照してください。

 **メモ:** すべての Dell 属性にプレフィクスとして **Dell Computer** または **Dell Management Console** が付きます。

4. **Save changes**(変更の保存)をクリックします。

選択した属性がすべて含まれている表形式のレポートが表示されます。

詳細なレポートについては、**Help**(ヘルプ)→**Document Library**(マニュアルライブラリ)から利用可能な Symantec のマニュアルを参照してください。

---

## Dell レポートの編集

すべての Dell レポートは、デフォルトで読み取り専用になっています。そのため、レポートを編集するには、最初にこれらのレポートの複製を作成します。

---

## レポートの実行

左ペインで、レポートを選択します。選択したレポートが、右ペインに表示されます。

レポートによっては、パラメータを入力できます。これらのレポートパラメータを使用して、選択または入力した値に基づいてレポートを絞り込みます。

 **メモ:** "%" 記号はワイルドカードであり、ゼロ個以上の任意の文字列と一致します。

---

## レポートの保存

レポートを複数の形式で保存できます。例えば、HTML ファイル、XML ファイル、CSV、またはウェブパーツとして保存できます。

上記のレポートをウェブパーツとして保存する場合は、次の手順を実行します。

1. **New SQL Report**(新規 SQL レポート)ページの **Save As**(名前を付けて保存)ドロップダウンメニューから、**Web part**(ウェブパーツ)を選択します。
2. **Save As Web part**(ウェブパーツとして保存)ダイアログボックスで、新しいレポートの名前を入力します。
3. ウェブパーツのサイズを選択し、**Save**(保存)をクリックします。

レポートは、**Settings**(設定)→**Console Settings**(コンソールの設定)の **Web Parts**(ウェブパーツ)メニューにある **Web Parts**(ウェブパーツ)フォルダに保存されます。

このウェブパーツを Dell Management Portal(Dell 管理ポータル)ページに追加するには、[Dell Management Console ポータルページの変更](#)を参照してください。

---

## レポートの表示

L1/L2 ユーザー役割でログインした場合、レポートでは次の右クリックオプションが使用できません。

- 1. **Export**(エクスポート)
- 1. **View As XML**(XML で表示)
- 1. **Security**(セキュリティ)

レポートを表示するには、次の手順を実行します。

1. Dell Management Console から、**Reports**(レポート)→**All Reports**(すべてのレポート)→**Dell Reports**(Dell レポート)を選択します。
2. 表示するレポートをクリックします。

---

## メトリックレポート

デバイスグループのメトリックを監視するために、次のレポートを使用できます。

- 1 ピーク電力 - デバイスのピーク消費電力値に関する情報を提供します。時間、単位などの詳細な情報も含まれます。
- 1 電力バジェット - デバイスの電力バジェット、ヘッドルーム、アイドル電力などに関する情報を提供します。

ピーク電力レポートと電力バジェットレポートは、表形式で表示されます。

- 1 スマートメトリックレポート - この機能は、今後のバージョンの Dell Management Console で提供される予定です。デバイスのメトリック値の経時的な傾向に関する情報を提供します。期間、デバイス、およびメトリックを選択することにより、詳細情報をグラフィック形式で表示できます。グラフ上のポイントをクリックすることにより、テーブルをドリルダウンして各デバイスの値を表示できます。このグラフは、スマートメトリックデータから作成されます。Dell Management Console を使用して多数のデバイスを管理している場合は、グループメトリックレポートを使用すると、グループデータに関してははるかに速い応答が得られます。そのため、可能であれば、グループの表示にグループメトリックレポートを使用することをお勧めします。あるいは、スケジュールオプションを使用して夜間にレポートを実行し、朝にはデータに容易にアクセスできるようにすることもできます。

スマートメトリックレポートでは、電源監視とパフォーマンスモニターのメトリックのみがサポートされます。

スマートメトリックレポートでは、Windows オペレーティングシステムのサーバーでは WM 接続プロファイルについて、Linux オペレーティングシステムのサーバーでは SNMP 接続プロファイルについて、パフォーマンスモニターメトリックがサポートされます。

なお、スマートメトリックレポートでは、正常性メトリックはサポートされません。

- 1 グループメトリックレポート:この機能は、今後のバージョンの Dell Management Console で提供される予定です。グループのメトリック値の経時的な傾向に関する情報を提供します。期間とグループメトリックを選択することにより、詳細情報をグラフィック形式で表示できます。グラフ上のポイントをクリックすることにより、テーブルをドリルダウンして、そのポイントを構成する各デバイスの値を表示できます。このグラフは、グループメトリックデータから作成されます。

---

## グループメトリックレポートの表示

カスタムグループについてグループメトリックレポートのグラフを表示するには、次の手順を実行します。

1. Dell Management Console から、**Manage (管理)** → **Organizational Views and Groups (組織ビューと組織グループ)** を選択します。
2. **Organizational Views (組織ビュー)** ページで、新規の組織ビューを作成します。
3. 新規に作成した組織ビューの下でグループを作成します (例えば、group-report)。
4. この新規に作成したグループの下でサーバーを追加します。
5. 電源監視ポリシーを有効にします。
6. 電源監視ポリシーの **Monitored Targets (監視ターゲット)** の下で、**Apply to (適用先)** → **Resources (リソース)** をクリックします。
7. リソースの追加ウィザードで、ルールを追加し、**Then (次を行う) 条件ドロップダウンリスト** で、**exclude resources not in (次に含まれないリソースを除外)**、**Group (グループ)**、手順 3 で作成したグループレポートを選択します。

8. **Update results (結果のアップデート)** をクリックし、**Save as (名前を付けて保存)** をクリックして、名前 (例えば GM) を入力し、**OK** をクリックします。

 **メモ:** ルール設定を保存しないと、グラフは表示されません。

9. **Monitoring and Alerting (監視と警告)** ページから、**Metric Library (メトリックライブラリ)** を選択します。
10. **Metric Library (メトリックライブラリ)** 内に存在するグループメトリックに対して、**Target as (ターゲット)** を選択し、**Apply to (適用先)? Quick apply (すぐに適用)** をクリックし、グループ (GM) を選択します。

---

## レポートの設定 - カスタムターゲットグループ

カスタムグループを含むターゲットシステムのグループメトリックレポートを表示するには、レポート設定を設定する必要があります。

カスタムターゲットグループレポートを表示するには、次の手順を実行します。

1. Dell Management Console ポータルの **Group View - Aggregate Health by Dell Resource (グループビュー - Dell リソースごとの総合的な正常性)** で、**Configure (設定する)** をクリックします。
2. カスタムフィルタを定義し、グループを選択します。
3. Dell デバイスの **filter (フィルタ)** を選択し、両方のフィルタの最初のドロップダウンで **exclude resources not in (次に含まれないリソースを除外)** を選択し、**Update result (結果のアップデート)** をクリックします。

カスタムグループとそれに属するデバイスが表示されます。

4. **Save As** (名前を付けて保存)をクリックし、ファイルを保存し、**OK** をクリックします。

5. 既存のフィルタを上書きするには、リストからフィルタを選択し、**OK** をクリックします。

これで、このフィルタを監視モジュールで使用できるようになりました。

6. **Home** (ホーム) → **Monitoring and Alerting** (監視と警告) で、**Monitor** (監視) → **Policies** (ポリシー) → **Dell Policies** (Dell ポリシー) → **Power Monitoring** (電源監視) (あるいは変更する任意の他の特定のポリシーまたは複製ポリシー) を選択します。

7. **Monitor Targets** (ターゲットの監視) ウェブパーツで、定義したフィルタを選択し、デフォルトのフィルタを削除します。

上記の手順により、このフィルタで指定されるターゲットに対してデータ収集が有効になります。

8. メトリックライブラリで、メトリックターゲットをアップデートします。メトリックは、上記のポリシーによって使用されます。必要なメトリックを編集し、上記のポリシーで使用されるのと同じフィルタを追加し、変更を保存します。

9. 監視エージェントをリセットします。

10. アップデートポリシーを実行して、監視エージェントによる (監視ソリューションのために保存された) 最新の変更を収集します。

ポーリングサイクルが完了したら、グラフを表示できます。

---

[目次に戻る](#)

[目次に戻る](#)

## Dell OpenManage Server Administrator ソリューションの導入

Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [導入ソリューションについて](#)
- [Deploy Dell OpenManage Server Administrator ユーザーインターフェース](#)
- [依存関係](#)
- [その他](#)
- [Server Administrator タスクの導入](#)

Dell Management Console の導入ソリューションは、Dell OpenManage IT Assistant のソフトウェアアップデート機能と似た機能を提供します。

### 導入ソリューションについて

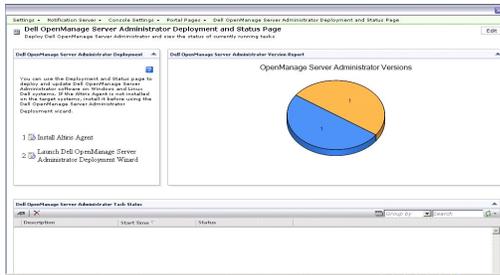
この導入ソリューションは、Dell OpenManage エージェント(OpenManage Server Administrator)のターゲットシステムへのインストールに役に立ちます。Dell Management Console は、このエージェントと通信して、ターゲットシステムの状態および正常性を提供します。Server Administrator の詳細については、デルサポートサイト([dell.support.com](http://dell.support.com))で入手できる『Dell OpenManage Server Administrator ユーザーズガイド』を参照してください。

導入タスクには、ソフトウェアパッケージの選択、スケジュールの指定、およびソフトウェアパッケージを適用するシステムの指定が含まれます。Windows および Linux オペレーティングシステムには特別なパッケージがあります。

### Deploy Dell OpenManage Server Administrator ユーザーインターフェース

Discover Your Network(ネットワークの検出)タブの Dell Enterprise Management Quick Start(Dell Enterprise Management クイックスタート)ウェブパーツにある Dell Management Console(Dell Management Console)ポータルページ上の **Deploy Dell OpenManage Server Administrator**(Dell OpenManage Server Administrator の導入)リンクにアクセスできます。

### Deploy Dell OpenManage Server Administrator ユーザーインターフェースの理解



### 依存関係

Dell Management Console から Server Administrator を導入するには、Altiris Agent がターゲットシステムに存在し、Dell Management Console システムに登録されている必要があります。

### その他

Server Administrator パッケージ(Microsoft Windows の場合は `sysmgmt.msi`、サポートされている Linux オペレーティングシステムの場合は `.tar.gz` および対応する `.sign` ファイル)を『システム管理ツールおよびマニュアル DVD』、『Dell サーバーアップデート DVD』またはデルサポートサイト([support.jp.dell.com](http://support.jp.dell.com))から取得します。

Server Administrator パッケージは、デフォルトでは、共有ライブラリフォルダに作成されます。このパッケージには、**Manage**(管理)→**All Resources**(すべてのリソース)からアクセスできます。

### Server Administrator タスクの導入

ソフトウェアアップデートには、ソフトウェアアップデートタスクの作成および管理対象システムへの Server Administrator エージェントの導入が含まれます。

OpenManage Server Administrator を導入する前に、Altiris Agent が管理対象システムにインストールされていることを確認する必要があります。Altiris Agent を管理対象システムにインストールするには、[Altiris Agent の管理対象ノードへのプッシュ](#)を参照してください。

Dell Management Console では、管理を行うために Dell システムに Server Administrator をシステムにインストールする必要があります。ソフトウェアアップデートタスクを使用して、Server Administrator バージョン 5.3 以降をインストール、またはバージョン 5.3 にアップグレードします。

 **メモ:** このタスクでは、Server Administrator バージョン 4.3 以降がすでにターゲットシステムにインストールされている場合にのみアップグレードが行えます。

 **メモ:** Server Administrator をターゲットシステムからアンインストールするには、デルサポートサイト([support.jp.dell.com](http://support.jp.dell.com))の『Dell OpenManage Server Administrator ユーザーズガイド』を参照してください。

## Altiris Agent の管理対象ノードへのプッシュ

Altiris Agent を管理対象ノードにプッシュするには、次の手順を実行します。

1. Dell Management Console を起動します。
2. Dell Management Console から、次のいずれかを実行します。
  1. **Actions(アクション)→ Agents/Plug-ins(エージェント / プラグイン)→ Push Altiris Agent(Altiris Agent のプッシュ)**にナビゲートします。
  1. **Dell Management Console Portal**(Dell Management Console ポータル)ページの **Dell Enterprise Management Quick Start**(Dell Enterprise Management クイックスタート)ウェブパーツで、**Discover Your Network**(ネットワークの検出)→ **Deploy Dell OpenManage Server Administrator**(Dell OpenManage Server Administrator の導入)を選択して、**Dell OpenManage Server Administrator Deployment and Status**(Dell OpenManage Server Administrator の導入および状態)ページで、**Install Altiris Agent**(Altiris Agent のインストール)をクリックします。
3. **Select Computers**(コンピュータの選択)ボタンをクリックします。
4. Altiris Agent をプッシュまたはインストールするコンピュータを選択して、**OK** をクリックします。
5. **Install Altiris Agent**(Altiris Agent のインストール)をクリックし、Altiris Agent をインストールするための資格情報を提供して、**Proceed With Install**(インストールを続行する)をクリックします。

## 管理ステーションからの Server Administrator パッケージの削除

既存の Server Administrator パッケージを Dell Management Console システムから削除するには、次の手順を実行します。

1. **Manage(管理)→ All Resources**(すべてのリソース)をクリックします。
2. Dell OpenManage コンポーネントを検索して、同じ Dell OpenManage バージョンの **Software componen**(ソフトウェアコンポーネント)、**release**(リリース)、**package**(パッケージ)および**product**(製品)を削除します。

検索フィールドに Dell と入力して、Dell OpenManage Server Administrator によりインポートされたパッケージを表示できます。

## エージェント導入タスクの作成

Windows および Linux オペレーティングシステムを使用している場合、2 つのエージェント導入タスクを作成する必要があります。1 つは、Server Administrator を対応 Microsoft Windows システムに導入するタスクで、もう 1 つは、Server Administrator を対応 Linux オペレーティングシステムに導入するタスクです。

1. **Home(ホーム)→ Dell Management Console Portal**(Dell Management Console ポータル)をクリックします。  
**Dell Enterprise Management** ページが表示されます。
2. **Dell Enterprise Management Quick Start**(Dell Enterprise Management クイックスタート)ウェブパーツで、**Discover Your Network**(ネットワークの検出)タブをクリックします。
3. **Deploy Dell OpenManage Server Administrator**(Dell OpenManage Server Administrator の導入)をクリックします。  
**Dell OpenManage Server Administrator Deployment and Status**(Dell OpenManage Server Administrator の導入および状態)ページが表示されます。  
 **メモ:** Server Administrator を導入する前に Altiris Agent をインストールします。エージェントを Server Administrator の導入に使用される Symantec Notification Server に登録します。ひとつのシステムのエージェントをプッシュし、別のシステムから Server Administrator をプッシュすると、タスクが失敗します。Altiris Agent のインストールの詳細については、Symantec マニュアルを参照してください。
4. **Launch Dell OpenManage Server Administrator Deployment Wizard**(Dell OpenManage Server Administrator の導入ウィザードの起動)をクリックします。
5. 手順 1 では、**Dell OpenManage Server Administrator Deployment**(Dell OpenManage Server Administrator の導入)ページのソフトウェアパッケージを選択すると、次のオプションから選択できるようになるので、オプション選択後、**Next**(次へ)をクリックします。
  1. **新規ソフトウェア配布パッケージを CD から作成する。**

これを選択して、Server Administrator インストーラをローカルシステム、CD/DVD またはネットワークロケーションからアップロードします。

 **メモ:** このオプションを選択した場合、パッケージは、今後の使用のために Symantec ソフトウェアライブラリに作成されます。

1. **既存のソフトウェア配布パッケージを選択する。**

パッケージがすでにインポートされている場合は、それを再使用できます。

 **メモ:** Server Administrator バージョン 4.3 以降がすでにターゲットシステムにインストールされている場合にのみ、このタスクをアップグレードに使用します。

Server Administrator の導入には追加のパラメータを指定することができます。パラメータの詳細については、デルサポートサイト([support.jp.dell.com](http://support.jp.dell.com))の『Dell OpenManage Server Administrator ユーザーズガイド』を参照してください。

6. ウィザードの 2 番目のページで、要件に応じて、Windows または Linux パッケージを選択して、Next (次へ) をクリックします。

a. 次のいずれかのオプションを使用して、ターゲットシステムを選択します。

- **Quick Add (すぐに追加):** システム名をこのフィールドに入力します。このオプションは、ターゲットシステムの数が少ない場合に便利です。
- **Add (追加):** 検出されたシステムのリストからコンピュータを追加します。このオプションは、ターゲットシステムの数の中程度の場合に便利です。

Select Computer (コンピュータの選択): ページが表示されます。

- **Add Groups (グループの追加):** このオプションは、ターゲットシステムの数が多い場合に便利です。

b. Server Administrator を導入するシステムを選択して、OK をクリックします。

7. ウィザードの 3 番目のページで、導入スケジュールおよび実行時間オプションを選択します。

Now (今すぐ実行) をクリックして、Deploy Dell OpenManage Server Administrator (Dell OpenManage Server Administrator の導入) をクリックします。

 **メモ:** メンテナンス時間外でスケジュールされている場合でもタスクを実行する場合、Override Maintenance window on target (ターゲットでのメンテナンス時間帯の上書き) オプションを選択します。メンテナンス時間帯の詳細については、『オンラインヘルプ』を参照してください。

ソフトウェアアップデートタスクは、タスク作成後すぐに実行されます。

ターゲットシステムに Adaptec コントローラがある場合、エージェント導入タスクにより、システムの再起動が要求されます。

システムを再起動するには、Reboot the target system if required (必要に応じてターゲットシステムを再起動する) オプションを選択します。

Server Administrator を対応 Linux オペレーティングシステムがインストールされたシステムに導入する場合は、新規タスクを作成します。Server Administrator を Linux システムに導入する場合、対応する署名ファイルを指定する必要があります。このファイルは、『Dell サーバーアップデート DVD』にあります。

Server Administrator MSI (Windows の場合) または tar.gz (Linux の場合) を初めてアップロードする場合、Server Administrator ソフトウェアアップデートパッケージが作成されます。2 回目以降のエージェント導入タスクでは、このパッケージを再使用して、Server Administrator を別の Dell システムに導入できます。

## タスク詳細の表示

タスクが実行されると、状態が、Dell OpenManage Server Administrator Task Status (Dell OpenManage Server Administrator タスク状態) ウェブパーツの Dell OpenManage Server Administrator Deployment and Status (Dell OpenManage Server Administrator の導入および状態) ページに表示されます。

タスクインスタンスをダブルクリックして、タスクの詳細を表示します。

後で行われるようにスケジュールされているタスクは、Dell OpenManage Server Administrator Task Status (Dell OpenManage Server Administrator タスク状態) ウェブパーツからタスクをダブルクリックして、スケジュールを変更します。

## ソフトウェアライブラリのデフォルトロケーションの変更

ライブラリフォルダのロケーションを変更する場合、次の手順を実行します。

1. ソフトウェアパッケージを保存するフォルダを選択します。
2. フォルダをネットワークで共有して、書き込み許可をシステム管理者だけに提供します。
3. Settings (設定) → All Settings (すべての設定) をクリックします。
4. 左ペインで、Settings (設定) → Software (ソフトウェア) → Software Catalog and Software Library Settings (ソフトウェアカタログおよびソフトウェアライブラリ設定) → Software Library Configuration (ソフトウェアライブラリ設定) を選択します。
5. 右ペインで、Dell Management Console への新しい共有ライブラリロケーションを提供します。



[目次に戻る](#)

## ジョブおよびタスクの管理

Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [ジョブおよびタスクユーザーインターフェイス](#)
- [ジョブとタスクモジュールの使用](#)

タスクは、システムで実行するアクションです。

Dell Management Console では、ハードウェアの設定やターゲットデバイスの電源リセットなどのタスクを実行できます。これらのタスクは、タスクを実行する場所に基づいて次のように分類されます。

- 1 クライアントタスク: クライアントタスクは、タスクサーバーを介してリモートコンピュータで実行されます。クライアントタスクでは、常に、サーバーとクライアントのセット間の通信が行われます。例として、Altiris 電源制御タスクが挙げられます。
- 1 タスクサーバー タスク: タスクサーバータスクは、Symantec 管理コンソール またはタスクサーバーがインストールされているシステムで実行できます。すべてのリモートタスクサーバーは、Symantec 管理コンソール に登録する必要があります。例として、コマンドラインビルダタスクが挙げられます。タスクサーバータスクは、クライアントタスクと似ていますが、管理外のシステム (つまり、Altiris Agent がインストールされていないシステム) でも実行できます。タスクサーバーの詳細については、『オンラインヘルプ』または Symantec マニュアルを参照してください。

タスクサーバーでは、タスクを複数のジョブで再使用したり、必要に応じてタスクのクローンを作成して変更したりできます。

- 1 サーバータスク: サーバータスクは、Symantec 管理コンソール で実行されます。サーバータスクでは、タスクの必要性に応じて、クライアントのセットとの通信が行われることがあります。例として、ネットワーク検出タスクが挙げられます。

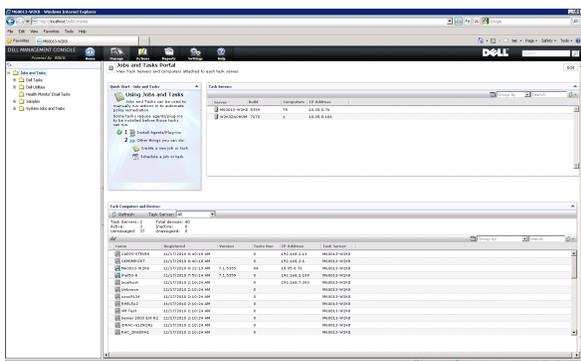
ジョブは、特定のシーケンスで複数のタスクを実行する 1 つのタスクです。たとえば、互いにジョブをネストすることで、状況に応じて異なる事前条件チェックを実行するという、複雑な例もあります。ジョブ作成の詳細については、オンラインヘルプを参照してください。

電源制御タスクは、NAS システムにインストールされている Windows 2008 Storage Server でタスクが実行される場合、正しいステータスを返さないことがあります。このタスクは、実際には電源制御処理を完了します。これは、管理下 NAS ディレクトリに直接ログインすることで確認できます。

## ジョブおよびタスクユーザーインターフェイス

Jobs and Tasks(ジョブとタスク)ポータルページにアクセスするには、Manage(管理)→ Jobs and Tasks(ジョブとタスク)をクリックします。

## ジョブとタスクユーザーインターフェイス



右ペインの Quick Start - Jobs and Tasks(クイックスタート - ジョブおよびタスク)ウェブパーツは、タスクソリューションを開始するのに適した場所です。このウェブパーツを使用して、新しいタスクおよびジョブを作成して、スケジュールできます。

Task Computer and Devices(タスクコンピュータおよびデバイス)ウェブパーツには、各タスクサーバーに割り当てられたデバイスのリストが表示されます。タスクサーバーのデバイスをソートしたり、デバイスを右クリックしてデバイスで実行されるタスクを確認したりできます。

Task Servers(タスクサーバー)ウェブパーツには、Symantec 管理コンソールに登録されているすべてのタスクサーバーが表示されます。

左ペインでは、サンプルのジョブおよびタスクを表示できます。

 **メモ:** サンプルタスクは、読み取り専用のタスクで、実行だけが可能です。

最初の Dell タスクを作成するときに、Dell Management Console により、Dell Task(Dell タスク)フォルダが Jobs and Tasks(ジョブとタスク)ルートフォルダ下に作成されます。

## ジョブとタスクモジュールの使用

Jobs and Tasks Portal(ジョブおよびタスクポータル)を表示するには、Manage(管理)→Jobs and Tasks(ジョブとタスク)をクリックします。タスク管理ソリューション(Create New Task(新規タスクの作成)ページ)では、タスクがツリー構造で表示され、フォルダにまとめられています。Dell タスクは、Dell Tasks(Dell タスク)フォルダ下にまとめられます。

タスクは、30 分ごと、毎時、営業時間内、毎日、毎週、毎月、またはカスタム定義間隔で実行するようにスケジュールできます。共有スケジュールを使用すると、時間、開始日および終了日や、たとえば、毎日、一度、毎週、毎月、ログイン時、システム起動時などの繰り返し実行を指定できます。

タスクは、1 台または複数のデバイスや 1 つまたは複数のコレクションで実行できます。スケジュールされるタスクでは、入力される資格情報は、タスクがユーザー操作なしで実行できるように保存されます。

Dell Management Console には、シャットダウン(デバイスの電源制御)、ウェイクアップ(電源制御)、コマンドライン(スクリプトの実行)およびリモートコマンドライン(コマンドラインビルダ)のサンプルタスクが事前に定義されています。これらのサンプルタスクは、実行したり、タスクパラメータを適切に設定して変更したりできます。

 **メモ:** Run Script(スクリプトの実行)タスクを実行する前に、Altiris Agent を管理下システムにインストールします。

Create New Task(新規タスクの作成)ページの Dell Tasks(Dell タスク)フォルダの下にリストされるすべてのタスク(Associate Dell Devices(Dell デバイスの関連付け)タスクを除く)は、サーバーおよびクライアントジョブの一部として追加できます。

Associate Dell Devices(Dell デバイスの関連付け)タスクは、サーバージョブだけに追加できます。

すべての Dell タスクの詳細については、『オンラインヘルプ』を参照してください。

## タスクのスケジュール

シャットダウンタスクをシステムのグループで、たとえば、6 月を除く、毎月第 3 土曜日の午後 6 時にスケジュールするには、次のように実行します。

1. Manage(管理)→Jobs and Tasks(ジョブとタスク)をクリックして、Jobs and Tasks Portal(ジョブおよびタスクポータル)を表示します。
2. Jobs and Tasks Quick Start(ジョブおよびタスクのクイックスタート)ウェブパーツで、Create a new job or task(ジョブまたはタスクの新規作成)をクリックします。
3. Create New Task(新規タスクの作成)ページで、Power Control Device(デバイスの電源制御)タスクを選択します。

4. Shut down(シャットダウン)を選択して、OK をクリックします。

Power Control Device - Shut down(デバイスの電源制御 - シャットダウン)タスクが作成され、Task Server Tasks(タスクサーバータスク)→Dell Tasks(Dell タスク)フォルダの下に表示されます。

5. Power Control Device - Power Off(デバイスの電源制御 - 電源オフ)タスクを左ペインの Jobs and Tasks(ジョブとタスク)ツリーから選択します。

詳細は、右ペインに表示されます。

6. Task Status(タスクステータス)ペインで、New Schedule(新規スケジュール)を選択して、Schedule Task(タスクのスケジュール)ページで次のように設定します。

Schedule(スケジュール): Shared Schedule(共有スケジュール)

Select Shared Schedule(共有スケジュールの選択): Monthly(毎月)

New(新規)をクリックします。

7. Create New Shared Schedule(新しい共有スケジュールの作成)ページで、スケジュールの名前および説明を入力します。

Add schedule(スケジュールの追加)→Scheduled Time(スケジュール時刻)を選択して、シャットダウンタスクの開始時刻として 1800 時を選択します。

No repeat(繰り返しなし)をクリックし、Month (week view)(毎月(週表示))を選択して、Repeat Schedule(繰り返しスケジュール)画面で **Week 3**(第 3 週)および **Saturday**(土曜日)を選択します。

Year (week view)(年(週表示))を選択して、6 月以外のすべての月を選択します。

8. Create New Shared Schedule(新しい共有スケジュールの作成)ページで、Advanced(詳細設定)をクリックし、このタスクの開始日および終了日(1 年間)を選択して、OK をクリックします。

9. New Schedule(新規スケジュール)ページで、Add(追加)をクリックして、このタスクのコンピュータまたはコンピュータのグループを選択します。

10. Power Control Device - Shut down(デバイスの電源制御 - シャットダウン)タスクページで、Save changes(変更の保存)をクリックします。

1 年中、6 月を除く、毎月の第 3 土曜日午後 6 時にスケジュールされたシャットダウンタスクが作成されます。

 **メモ:** Power Control Device - Shut down(デバイスの電源制御 - シャットダウン)タスクを一部のシステムですぐに実行するには、Task Status(タスクステータス)ペインで、Quick Run(クイック実行)をクリックして、システムを選択します。

## SNMP の設定タスクの作成

 **メモ:** このタスクは、Windows オペレーティングシステムだけで実行する管理下システムで設定できます。

Configure SNMP(SNMP の設定)タスクを使用して、セキュリティ、トラップおよびエージェントなど、SNMP サービスプロパティを設定できます。

1. **Manage(管理)**→ **Jobs and Tasks(ジョブとタスク)**をクリックして、**Task Management Portal(タスク管理ポータル)**を表示します。
2. **Jobs and Tasks Quick Start(ジョブおよびタスクのクイックスタート)**ウェブパーツで、**Create a new job or task(ジョブまたはタスクの新規作成)**をクリックします。
3. **Create New Task(新規タスクの作成)**ページで、**Dell Tasks(Dell タスク)**→ **Other(その他)**フォルダ下の **Configure SNMP(SNMP の設定)**タスクを選択します。
4. 右ペインの **SNMP Task Settings(SNMP タスク設定)**で、**Add or Modify SNMP Service Properties(SNMP サービスプロパティの追加または変更)**を選択します。
5. **Security(セキュリティ)**をクリックして、コミュニティのセキュリティプロパティを設定します。
6. **SNMP Service Security Properties(SNMP サービスセキュリティプロパティ)**ページで、組織の認定コミュニティ名を追加して、Dell Management Console がホストからの SNMP パケットを許可するかどうかを指定します。

識別に関係なく、ネットワークの任意のホストからの SNMP 要求を受け入れるには、**Accept SNMP packets from any host(任意のホストから SNMP パケットを受け入れる)**をクリックします。

Dell Management Console サーバーからの SNMP パケットの受け入れを制限するには、**Accept SNMP packets from these hosts(これらのホストの SNMP パケットを受け入れる)**をクリックし、**Add(追加)**をクリックして、Dell Management Console サーバーのホスト名または IP アドレスを **Host name, IP, or IPX(ホスト名、IP または IPX)**アドレスボックスに入力します。

7. **SNMP Task Settings(SNMP タスク設定)**セクションで、**Traps(トラップ)**をクリックし、コミュニティ名を指定して、トラップの宛先を設定します。
8. **SNMP Task Settings(SNMP タスク設定)**セクションで、**Agents(エージェント)**をクリックして、エージェントの物理的な位置、およびこのエージェントの担当者を指定します。
9. **OK** をクリックして、SNMP の設定タスクを作成します。

このタスクは、**Dell Tasks(Dell タスク)**下の **Jobs and Tasks(ジョブとタスク)**ポータルページに表示されます。

 **メモ:** このタスクを実行する前に、SNMP サービスを管理下システムで有効にします。

10. タスクをシステムのグループで実行するには、**New Schedule(新規スケジュール)**をクリックします。
11. **Create New Schedule(新規スケジュールの作成)**ページで、**Now(今すぐ)**を選択します。
12. **Selected Devices(選択したデバイス)**セクションで、**Add(追加)**をクリックして、このタスクを実行するデバイスを追加します。

 **メモ:** 変更を有効にするには、管理下システムで SNMP サービスを再起動します。

## 管理下システムで Server Administrator コマンドを実行するためのコマンドラインビルダタスクの作成

コマンドラインビルダタスクは、リモート Server Administrator タスク、IPMI タスクまたはリモートアクセスコントローラタスクなどの事前定義されたタスクです。このタスクでは、1 台の管理下システムまたは管理下システムのセットを対象として、定義されたパラメータまたはコマンドのセットを使用して、実行可能ファイルを実行できます。

コマンドラインビルダタスクを作成して、管理下システムのグループのシステムシャーシ、オペレーティングシステム、ソフトウェアプロファイルおよびハードウェアプロファイル情報など、システム情報の要約を表示するには、次の手順を実行します。

 **メモ:** このデータを取得するには、Server Administrator が Dell 管理コンソールの管理下システムにインストールされている必要があります。

1. **Manage(管理)**→ **Jobs and Tasks(ジョブとタスク)**をクリックして、**Task Management Portal(タスク管理ポータル)**を表示します。
2. **Jobs and Tasks Quick Start(ジョブおよびタスクのクイックスタート)**ウェブパーツで、**Create a new job or task(ジョブまたはタスクの新規作成)**をクリックします。
3. **Create New Task(新規タスクの作成)**ページの **Dell Tasks(Dell タスク)**→ **Other(その他)**フォルダ下で、**Command Line Builder(コマンドラインビルダ)**タスクを選択します。
4. **Command Line Type(コマンドラインタイプ)**から、**Remote Server Administrator(リモート Server Administrator)**を選択して、**omreport** を選択します。

**Add(追加)**をクリックします。

**system(システム)**を選択して、**Add(追加)**をクリックします。

**summary(サマリ)**を選択して、**Add(追加)**をクリックします。

または、**Command Syntax(コマンド構文)**で、**omreport system summary** と入力します。

 **メモ:** ドロップダウンリストからパラメータを 4 つまで選択できます。この後、パラメータドロップダウンは、動的には入力されなくなります。

5. **Advanced(詳細設定)**をクリックし、ユーザー資格情報を入力して、出力記録用ログファイルのパスを指定し、**OK** をクリックします。

-  **メモ:** 資格情報を指定しない場合、管理下デバイスとの通信にシステムログイン用の資格情報が使用されます。
-  **メモ:** また、タスクは管理下デバイスとの通信に管理ステーションのシステムログイン用の資格情報を使用するため、サポートされている Linux オペレーティングシステムを実行する管理下システムの資格情報を指定しない場合、タスクは失敗し、複数の「Access Denied」(アクセスが拒否されました)メッセージが表示されます。
-  **メモ:** Linux を実行する管理下システムでこのタスクを作成する場合、**Task Options**(タスクオプション)タブを選択し、**SSH port number**(SSH ポート番号)を指定して、**Generate Trusted key for Linux**(Linux の信頼済みキーの設定)を選択します。

コマンドラインビルダタスクが、**Dell Tasks**(Dell タスク)フォルダ下に表示されます。

6. タスクをシステムのグループで実行するには、**New Schedule**(新規スケジュール)をクリックします。
7. **Create New Schedule**(新規スケジュールの作成)ページで、**Now**(今すぐ)を選択します。
8. **New Schedule**(新規スケジュール)ページで、**Add**(追加)をクリックして、このタスクを実行するデバイスを追加します。

## リモートアクセスコントローラコマンドを実行するための管理下システムでのコマンドラインビルダタスクの作成

リモートアクセスコントロールコマンドを実行するコマンドラインビルダタスクを管理下システムに作成するには、次の手順を実行します。

-  **メモ:** これらのコマンドを実行するには、Dell リモートアクセスコントローラが Dell Management Console の管理下システムに存在する必要があります。

1. **Manage**(管理)→ **Jobs and Tasks**(ジョブとタスク)をクリックして、**Task Management Portal**(タスク管理ポータル)を表示します。
2. **Jobs and Tasks Quick Start**(ジョブおよびタスクのクイックスタート)ウェブパーツで、**Create a new job or task**(ジョブまたはタスクの新規作成)をクリックします。
3. **Create New Task**(新規タスクの作成)ページの **Dell Tasks**(Dell タスク)→ **Other**(その他)フォルダ下で、**Command Line Builder**(コマンドラインビルダ)タスクを選択します。
4. **Command Line Type**(コマンドラインタイプ)から、**Dell OpenManage Remote Access Controller**(Dell OpenManage リモートアクセスコントローラ)を選択して、**setniccfg**を選択します。

**Add**(追加)をクリックします。

`-s` を選択し、値 `192.168.0.120 255.255.255.0 192.168.0.1` を入力して、**Add**(追加)をクリックします。

または、**Command Syntax**(コマンド構文)で、`setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1` と入力します。

-  **メモ:** ドロップダウンリストからパラメータを 4 つまで選択できます。この後、パラメータドロップダウンは、動的には入力されなくなります。

5. **Advanced**(詳細設定)をクリックし、ユーザー資格情報を入力して、ログファイルのパスを指定し、**OK** をクリックします。

-  **メモ:** 資格情報を指定しない場合、管理下デバイスとの通信に工場設定時の資格情報が使用されます。

コマンドラインビルダタスクが、**Dell Tasks**(Dell タスク)フォルダ下に表示されます。

6. タスクをシステムのグループで実行するには、**New Schedule**(新規スケジュール)をクリックします。
7. **Create New Schedule**(新規スケジュールの作成)ページで、**Now**(今すぐ)を選択します。
8. **New Schedule**(新規スケジュール)ページで、**Add**(追加)をクリックして、このタスクを実行するデバイスを追加します。

## Dell デバイスの関連付けタスクの作成

**Import Microsoft Active Directory**(Microsoft Active Directory のインポート)または **Import Domain Membership/WINS**(ドメインメンバーシップ/WINS のインポート)タスクを使用、あるいは Altiris Agent をターゲットデバイスにプッシュすることでデバイスを検出する場合、Dell デバイスは分類されません。

Active Directory インポートまたはドメインリソースでのデバイスの検出の詳細については、[Dell Management Console](#) の『オンラインヘルプ』を参照してください。

接続プロファイルを検出された各デバイスに関連付け、これらのデバイスを Dell デバイスとして分類します。

接続プロファイルには、検出およびインベントリモジュールがデバイスのリモートエージェントと通信するために必要なプロトコル設定および資格情報が含まれています。この関連付けがない場合、デバイスの検出およびインベントリが正しく機能しないことがあります。ネットワークポロジまたはプロトコル設定の変更を反映し、新しいデバイスの関連付けを作成するには、Dell デバイスの関連付けタスクを定期的に実行するように設定する必要があります。

このタスクを作成するには、次の手順を実行します。

1. **Manage**(管理)→ **Jobs and Tasks**(ジョブとタスク)をクリックして、**Task Management Portal**(タスク管理ポータル)を表示します。

- Jobs and Tasks Quick Start (ジョブおよびタスクのクイックスタート) ウェブパーツで、Create a new job or task (ジョブまたはタスクの新規作成) をクリックします。
- Create New Task (新規タスクの作成) ページの Dell Tasks (Dell タスク) → Other (その他) フォルダ下で、Associate Dell Devices (Dell デバイスの関連付け) タスクを選択します。
- 右ペインで、デフォルトの接続プロファイルを選択して、Select the target devices you want to associate with the selected connection profile (選択した接続プロファイルと関連付けるターゲットデバイスを選択する) の下で、Import Microsoft Active Directory (Microsoft Active Directory のインポート) または Import Domain Membership/WINS (ドメインメンバーシップ/WINS のインポート) タスクを介して検出されるデバイスを選択します。
- Apply to (適用先) → Resources (リソース) を選択します。
- Select Resources (リソースの選択) ページで、THEN ドロップダウンから Add Rule (ルールの追加) をクリックし、exclude resources not in resource list (リソースリストにないリソースを除外する) を選択して、省略記号 (...) をクリックします。
- Available Resources (使用可能なリソース) のグループから、Group (グループ) の下で、タスクを実行するデバイスを選択して、OK をクリックします。  
選択したデバイスが、Create New Task (新規タスクの作成) ページに表示されます。
- タスクをすぐに実行するようにスケジュールします。

 **メモ:** Associate Dell Devices (Dell デバイスの関連付け) は、サーバータスクであるため、Symantec 管理コンソールだけで作成および実行できます。そのため、New Schedule (新規スケジュール) 下の Quick Run (クイック実行) および Target Selection (ターゲット選択) オプションは表示されません。

このタスクの結果を表示するには、次の手順を実行します。

- Manage (管理) → All Resources (すべてのリソース) をクリックします。
- 関連付けられる Dell デバイスが、Organizational Views (組織ビュー) → All Devices (すべてのデバイス) の下に表示されます。

## Dell タスクロールアウトポリシー

大規模な多層 (階層) エンタープライズを管理して、ネットワーク上でデバイスを監視する場合、タスクサーバーを複数のシステムにインストールすることで、Symantec 管理コンソールの負荷を軽減することができます。また、これにより、ジョブおよびタスクのダウンロードのために Altiris Agent が最も近いタスクサーバーにアクセスするため、ネットワークトラフィックを軽減できます。

階層関係の作成および管理の詳細については、『オンラインヘルプ』を参照してください。

多層タスクサーバーアーキテクチャをサポートするため、Dell タスクでは、登録されているすべてのタスクサーバーで Dell タスクロールアウトポリシーを実行する必要があります。

Dell タスクロールアウトポリシーを登録されているすべてのタスクサーバーで実行するには、次の手順を実行します。

- ビルトインコレクションを使用してすべてのタスクサーバーをターゲットとするロールアウトポリシーを手動で有効にします。
- ロールアウトポリシーを有効にしたら、タスクコンポーネントが導入される次のポーリング間隔まで待機します。

## サイトサーバー (タスクサーバー) の Notification Server コンピュータへの登録

- Settings (設定) → Notification Server (Notification Server) → Site Server Settings (サイトサーバー設定) をクリックします。
- 左ペインで、Site Management (サイト管理) リストを展開します。
- タスクサーバーが表示されない場合、New (新規) → Site Server (サイトサーバー) をクリックします。
- Site Server (サイトサーバー) を Available computers (使用可能なコンピュータ) のリストから選択して、OK をクリックします。
- このサーバーに必要なサービスを選択します。

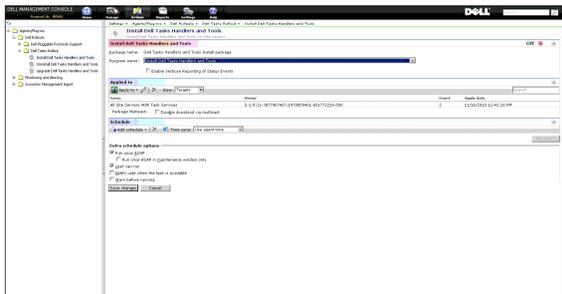
サーバーは、タスクサーバーのサイトサーバーとして正しく設定されます。

Jobs and Tasks (ジョブとタスク) ポータル (Manage (管理) → Jobs and Tasks (ジョブとタスク)) の Task Server (タスクサーバー) ウェブパーツに、Notification Server コンピュータに登録されているすべてのタスクサーバーが表示されます。Notification Server およびタスクサーバーが同じシステム上にある場合、コンピュータカウントに 1 と表示されます。

## Dell タスクロールアウトポリシータスクの作成

- Actions (アクション) → Agents/Plug-ins (エージェント / プラグイン) → Rollout Agents/Plug-ins (ロールアウトエージェント / プラグイン) をクリックします。
- Dell Tasks Rollout (Dell タスクロールアウト) フォルダ下で、Install Dell Tasks Handlers and Tools (Dell タスクハンドラおよびツールのインストール) を選択します。

- 右ペインの Program Name(プログラム名)で、Install Dell Tasks Handlers and Tools(Dell タスクハンドラおよびツールのインストール)を選択します。



- Apply to(適用先)→ Computers(コンピュータ)をクリックします。

**メモ:** ポリシーは、タスクサーバー要件と一致するタスクだけに適用できます。詳細については、『オンラインヘルプ』を参照してください。

- Select Computers(コンピュータの選択)画面で、Add rule(ルールの追加)をクリックします。
- THEN ドロップダウンメニューで、exclude computers in(コンピュータを除外する)を選択し、Computer list(コンピュータリスト)を選択して、(...)をクリックします。
- タスクサーバーとして含めないコンピュータを選択して、OK をクリックします。
- Dell Advanced Tasks Handlers Install(Dell 詳細設定タスクハンドラインストール)ページで、タスクのスケジュールを入力して、Save changes(変更の保存)をクリックします。

**メモ:** 同じ手順を実行して、Dell Configuration Tasks handlers install(Dell 設定タスクハンドラインストール)タスクを作成できます。

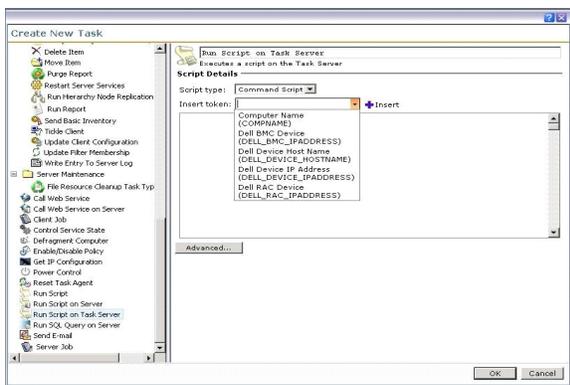
このポリシーは、内部的にタスクを作成して、タスクコンポーネントを導入します。

## タスクトークン

トークンは、特定の状況を例外として、値のないアイテムです。Dell 管理コンソールでは、事前定義されたトークンを使用してコマンドラインタスクを作成できます。これらのトークンは、タスク実行時にターゲットデバイスに対応する実際の値に置き換えられます。

Dell Management Console には、次のトークンが事前に定義されています。

- 1 %DELL\_BMC\_IPADDRESS%
- 1 %DELL\_DEVICE\_HOSTNAME%
- 1 %DELL\_RAC\_IPADDRESS%
- 1 %DELL\_DEVICE\_IPADDRESS%



前述のトークンを使用してタスクを作成するには、次の手順を実行します。

- Manage(管理)→ Jobs and Tasks(ジョブとタスク)をクリックして、Task Management Portal(タスク管理ポータル)を表示します。

2. **Jobs and Tasks Quick Start** (ジョブおよびタスクのクイックスタート) ウェブパーツで、**Create a new job or task** (ジョブまたはタスクの新規作成) をクリックします。
3. **Create New Task** (新規タスクの作成) ページで、**Run Script on Task Server** (タスクサーバーでのスクリプトの実行) タスクを選択します。
4. 右ペインで、**Script Type** (スクリプトタイプ) を選択します。
5. コマンドスクリプトテキストを入力して、事前に定義されている Dell トークンを選択します。
6. **Insert** (挿入) をクリックし、トークンをスクリプトテキストに挿入して、**OK** をクリックします。
7. タスクが作成され、左ペインの **Jobs and Tasks** (ジョブとタスク) フォルダの下に表示されます。

## スクリプトまたはコマンドを管理下ストレージシステムで実行するためのタスクトークンを使用したスクリプトの実行タスクの作成

**Run Script on Task Server** (タスクサーバーでのスクリプトの実行) タスクを作成して、Navisecccli コマンドを実行し、管理下ストレージシステムのグループでのパフォーマンスログプロパティの現在の値を取得できます。

 **メモ:** 管理下ストレージシステムが Navisecccli コマンドをサポートしていることを確認してください。Navisecccli コマンドをリモートストレージシステムで実行するように、管理ステーションを設定します。

1. **Manage** (管理) → **Jobs and Tasks** (ジョブとタスク) をクリックします。
2. **Jobs and Tasks Quick Start** (ジョブおよびタスクのクイックスタート) ウェブパーツで、**Create a new job or task** (ジョブまたはタスクの新規作成) をクリックします。
3. **Create New Task** (新規タスクの作成) ページで、**Run Script on Task Server** (タスクサーバーでのスクリプトの実行) タスクを選択します。
4. **Script Type** (スクリプトタイプ) から、**Command Script** (コマンドスクリプト) を選択します。
5. スクリプトテキストで、次のコマンド構文を入力します。
 

```
"C:\NaviCLITool\Navisecccli.exe" -h -AddUserSecurity -password mypass -scope 0 -user Tom analyzer -get -narinterval
```
6. **Insert token** (トークンの挿入) ドロップダウンメニューから、**DELL\_DEVICE\_IPADDRESS** トークンを選択して、**Insert** (挿入) をクリックし、スクリプトテキストの **-h** オプションの後にトークンを挿入して、**OK** をクリックします。
 

次のようなコマンド出力が表示されます。

```
"C:\NaviCLITool\Navisecccli.exe" -h%DELL_DEVICE_IPADDRESS% -AddUserSecurity -password mypass -scope 0 -user Tom analyzer -get -narinterval
```
7. タスクが作成され、左ペインの **Jobs and Tasks** (ジョブとタスク) フォルダの下に表示されます。
8. タスクを管理下ストレージシステムのグループで実行するには、**New Schedule** (新規スケジュール) をクリックします。
9. **Create New Schedule** (新規スケジュールの作成) ページで、**Now** (今すぐ) を選択します。
10. **New Schedule** (新規スケジュール) ページで、**Add** (追加) をクリックして、このタスクを実行する管理下ストレージシステムを追加します。
11. タスクが実行すると、**%DELL\_DEVICE\_IPADDRESS%** トークンが、各ターゲットストレージシステムの実際の IP アドレスに置き換えられます。

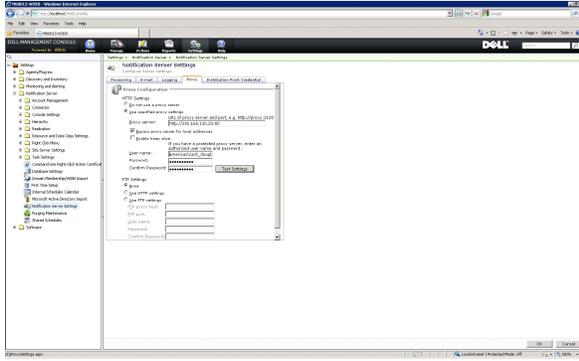
## 保証情報抽出タスクの作成

保証情報抽出タスクは、サーバータスクです。これは、サービスタグの付いた管理下デバイス (特に、Dell PowerEdge システム、Dell PowerConnect スイッチおよび DRAC/CMC) の保証情報を抽出するときに使用できます。このタスクは、Dell サポートウェブサイトから保証情報を取得します。

保証情報抽出タスクを正常に実行できるように、Dell Management Console が Dell サポートウェブサイト に接続できることを確認してください。

プロキシ設定を指定およびテストするには、次の手順を実行します。

1. **Settings** (設定) → **All Settings** (すべての設定) をクリックします。
2. 左ペインで、**Notification Server** → **Notification Server Settings** (Notification Server の設定) をクリックします。
3. 右ペインで、**Proxy** (プロキシ) タブをクリックして、プロキシ設定を行います。



保証情報抽出タスクを作成するには、次の手順を実行します。

1. **Manage (管理)** → **Jobs and Tasks (ジョブとタスク)** をクリックして、**Task Management Portal (タスク管理ポータル)** を表示します。
2. **Jobs and Tasks Quick Start (ジョブおよびタスクのクイックスタート)** ウェブパーツで、**Create a new job or task (ジョブまたはタスクの新規作成)** をクリックします。
3. **Create New Task (新規タスクの作成)** ページの **Dell Utilities (Dell ユーティリティ)** フォルダで、**Warranty Extractor (保証情報抽出)** タスクを選択します。
4. 右ペインで、新しく検出されたデバイスの保証情報を取得する日数を入力します。

**メモ:** 初めて保証情報抽出タスクを実行する場合は、すべての管理下デバイスの保証情報が取得されます。2 回目以降の実行では、新しく検出されたデバイス (つまり、最初のタスク実行後に Dell Management Console により検出されたデバイス) の保証情報が取得されます。古い保証情報 (つまり、取得後 60 日経過した保証情報) は更新されません。

**Delete all existing warranty information (すべての既存の保証情報の削除)** を選択するか、**refresh information retrieved n days ago (n 日経過した情報を更新する)** に値を入力して日数を指定した更新を行うことで、すべての保証情報を更新できます。

**メモ:** 保証情報レポートにより、取得された情報が表示されない場合、プロキシ設定が正しく有効にされているかどうかを確認して、その後のすべてのレポートに対して、**Delete all existing warranty information (すべての既存の保証情報の削除)** を選択する必要があります。

5. Dell Management Console が多くのデバイスを管理する場合、保証情報抽出タスクの完了に時間がかかることがあります。タスクが長時間実行される場合、タスクが情報を取得して処理する範囲を、サイズ「n」のサブセットで行うように指定できます (これは、**Update information for 'n' devices at a time (一度に「n」台のデバイスの情報をアップデートする)** フィールドで指定されます)。

**Warranty report (保証情報レポート)** をクリックして、指定した n 台のデバイスで取得した情報を表示できます。

6. **OK** をクリックします。

このタスクは、**System Jobs and Tasks (システムのジョブとタスク)** → **Notification Server** 下の **Jobs and Tasks (ジョブとタスク)** ポータルページに表示されます。

7. タスクをシステムのグループで実行するには、**New Schedule (新規スケジュール)** をクリックします。
8. **Create New Schedule (新規スケジュールの作成)** ページで、**Now (今すぐ)** を選択します。

Dell Management Console により管理されなくなったデバイス、つまり、Dell Management Console のデバイスリストから削除されたデバイスの履歴情報を表示できます。この情報は、保証情報抽出タスクを実行するたびにアップデートされ、**Device Status (デバイスステータス)** 列に表示されます。

## CMC ファームウェアのアップデート

リモートシャーシ管理コントローラ (CMC) または統合仮想コンソールのファームウェアをアップデートするには、CMC ファームウェアのアップデートタスクを使用します。

ファームウェアは、アクティブおよびスタンバイ CMC で同時にアップデートできます。アクティブ/スタンバイ CMC および仮想コンソールが選択された場合、アクティブ/スタンバイ CMC、仮想コンソールの順にアップデートされます。

<b>Active Chassis Management Controller (アクティブシャーシ管理コントローラ)</b>	これを選択して、アクティブシャーシ管理コントローラファームウェアをアップデートします。
<b>Stand-By Chassis Management Controller (スタンバイシャーシ管理コントローラ)</b>	これを選択して、スタンバイシャーシ管理コントローラファームウェアをアップデートします。
<b>CMC Firmware Image File Location (CMC ファームウェアイメージファイルの場所)</b>	アクティブまたはスタンバイシャーシ管理コントローラのアップデートに使用されるファームウェアイメージのパスおよびファイル名を指定します。
<b>Integrated KVM (iKVM) (統合 KVM (iKVM))</b>	これを選択して、iKVM ファームウェアをアップデートします。
<b>iKVM Firmware Image File Location (iKVM ファームウェアイメージファイルの場所)</b>	iKVM のアップデートに使用されるファームウェアイメージのパスおよびファイル名を指定します。
<b>Advanced (詳細設定)</b>	認証証明書を指定して、コマンドロギングを有効にします。 <a href="#">タスクオプション</a> を参照してください。

## タスクオプション

UserID(ユーザー ID)	管理下システムのユーザー ID を入力します。
Password(パスワード)	パスワードを入力します。
KG Key(KG キー)	<p>KG キー値を入力します。</p> <p>KG キーは、ファームウェアとアプリケーションの間で使用する暗号化キーを生成するための公開キーです。KG キー値は、偶数の 16 進文字です。KG キーは、IPMI タスクだけで表示されます。</p> <p><b>KG 値の表示</b></p> <p>現在の KG キー値を確認するには、次のコマンドを実行します(コマンドラインビルダタスクを使用します)。</p> <pre>ipmitool raw 0x18 0x56 &lt;CHAN&gt; 0x00 0x0</pre> <p>このコマンドで、&lt;CHAN&gt; は、個々の LAN チャネル番号です。</p> <p>KG キーなど、タスク出力をファイルに保存します。この KG キーを使用して、他の IPMI CLI タスクを実行します。</p>
Log(ログ)	<p>情報ログを設定して、タスクの実行詳細をログファイルに書き込みます。ログファイルは、ローカルファイルシステム(タスクサーバー)だけで作成できます。</p> <ul style="list-style-type: none"><li>1 <b>Output to file(ファイルに出力)</b> - 情報をファイルに記録します。このオプションは、実行アプリケーションの標準出力をログファイルに書き込みます。このオプションを選択した場合、ログファイルのパス名およびファイル名を入力する必要があります。このオプションはデフォルトで無効に設定されています。 指定したログファイルが存在する場合、このオプションを選択すると、そのログファイルが上書きされます。</li><li>1 <b>Append(追加)</b> - 実行コマンドのログ情報を指定ファイルに追加します。ファイルが存在しない場合、Dell Management Console により新しいファイルが作成されます。</li><li>1 <b>Include Errors(エラーを含める)</b> - Dell Management Console により検出されたすべてのエラーをログファイルに書き込みます。</li></ul>
SSH	<p>SSH ポート番号を設定して、必要な情報を提供します。</p> <p>SSH オプションは、Dell OpenManage Server Administrator タスクだけで使用できます。</p> <ul style="list-style-type: none"><li>1 <b>SSH Port Number(SSH ポート番号)</b> - 管理下 Linux システムで SSH ポート番号を設定します。デフォルト値は 22 です。</li><li>1 <b>Generate Trusted Key(トラステッドキーの生成)</b> - デバイスとの通信用のトラステッドデバイスキーを生成します。このオプションはデフォルトで無効に設定されています。このオプションを有効にすると、Linux システムでのタスクの初回実行時、およびシステムプロパティが変更されたときにタスクが実行されます。</li></ul>

[目次に戻る](#)

[目次に戻る](#)

Dell Management Console バージョン 2.0.2 ユーザーズガイド

---

## メモおよび注意

 **メモ:** コンピュータを使いやすいするための重要な情報を説明しています。

 **注意:** 手順に従わないと、ハードウェアの損傷やデータの損失につながる可能性があることを示しています。

---

本書の内容は予告なく変更されることがあります。  
© 2011 すべての著作権は Dell Inc. にあります。

Dell Inc. の書面による許可のない複製は、いかなる形態においても厳重に禁じられています。

本書に使用されている商標: Dell、DELL、ロゴ、PowerEdge™、PowerVault™、PowerConnect™、OpenManage™ および EqualLogic™ は Dell Inc. の商標です。Microsoft®、Windows®、Microsoft .NET Framework 3.5、Microsoft Internet Explorer® および Windows Server® は米国およびその他の国々における Microsoft Corporation の商標または登録商標です。Altiris®、Symantec™ および Notification Server™ は米国およびその他の国々における Symantec Inc. の商標または登録商標です。Brocade、Itrrepid、および McData は Brocade Communications Systems, Inc. の商標です。

商標または製品の権利を主張する事業体を表すためにその他の商標および社名が使用されていることがあります。それらの商標や会社名は、一切 Dell Inc. に帰属するものではありません。

2011 - 06

---

[目次に戻る](#)

[目次に戻る](#)

## Dell Management Console のユーザーインターフェイス

Dell Management Console バージョン 2.0.2 ユーザーズガイド

- [コンソールモード](#)
- [Home\(ホーム\)メニュー - 基本コンソール用の Dell Management Console ポータルページ](#)
- [Home\(ホーム\)メニュー - 標準コンソール用の Dell Management Console ポータルページ](#)
- [コンソールモードの切り替え](#)
- [アプリケーションの起動](#)
- [設定ページ](#)

この章では、Dell Management Console のユーザーインターフェイス(UI)について説明します。

Symantec Notification Server の基礎となるフレームワークにより、豊富な制御を備えたダイナミックなユーザーインターフェイスが提供されます。

Dell Management Console は、C:\Program Files\Dell\Sysmgmt\dmc にあります。起動アイコンは、Start(スタート)ボタン→Program(プログラム)→Dell OpenManage Applications(Dell OpenManage アプリケーション)→Dell Management Console→Dell Management Console から使用できます。

 **メモ:** セキュアソケットレイヤー(SSL)が Dell Management Console で有効にされている場合、デスクトップのショートカットを編集して、Start(スタート)メニューが新しい SSL ロケーションにポイントするように指定します。たとえば、https://localhost/Dell/CustomConsole です。

Dell Management Console は、メニュー方式で、次の 6 つのメニューで構成されます。

- 1 Home(ホーム)
- 1 Manage(管理)
- 1 Actions(操作)
- 1 Reports(レポート)
- 1 Settings(設定)
- 1 Help(ヘルプ)

---

## コンソールモード

Dell Management Console は、次の 2 つのコンソールモードを提供しユーザー

インターフェイスエクスペリエンスを向上させます。

- 1 基本コンソール - 基本機能へのアクセスを提供します。
- 1 標準コンソール - すべての機能へのアクセスを提供します。

デフォルトでは、標準コンソールが設定されます。要件や提供されるアクセシビリティ権限に基づいて、これらのコンソールモードを切り替えることができます。標準コンソールは、以前のリリースの Dell Management Console で使用できた機能を提供します。

サブメニューは、コンソールに基づいて各メニュー下にまとめられます。

次に、**基本コンソール**の Dell Management Console サブメニューの例を示します。

Home(ホーム)メニューには、Dell Management Console ポータルサブメニューが含まれています。Dell Client Manager のようなプラグインおよびそれらのサブメニューをインストールすると、個々のポータルをこのメニュー下で使用できるようになります。次のサブメニューオプションを使用できます。

- 1 Configuration(設定) - これを選択して資格情報や接続プロファイルなどの初期設定オプションにアクセスします。
- 1 Standard Console(標準コンソール) - これを選択して Dell Management Console を標準コンソールモードで開きます。
- 1 Dell Management Console Portal(Dell Management Console ポータル) - これを選択して Dell Management Console ポータルモードを開きます。コンソールモードによっては、使用可能なさまざまなオプションにアクセスできます。[Home\(ホーム\)メニュー - 基本コンソール用の Dell Management Console ポータルページ](#)または [Home\(ホーム\)メニュー - 標準コンソール用の Dell Management Console ポータルページ](#)を参照してください。
- 1 Discovery and Inventory(検出とインベントリ) - これを選択して次のオプションを表示します。
  - Credentials Management(資格情報管理) - Credentials Management(資格情報管理)機能は、標準コンソールモードと同じです。Credentials Management(資格情報管理)を使用すると、初期設定で、プロトコル資格情報を作成できます。
  - Agentless Inventory(エージェントレスインベントリ) - このインベントリ機能は、標準コンソールモードと同じです。このオプションを使用してインベントリタスクを作成できます。
  - Network Discovery(ネットワーク検出) - ネットワーク検出機能は、標準コンソールモードと同じです。このオプションを使用して検出タスクを作成できます。
- 1 Events and Alerts(イベントとアラート) - これを選択してイベントコンソールを表示します。
- 1 All Devices(すべてのデバイス) - All Devices(すべてのデバイス)ページを表示します。
- 1 Help(ヘルプ) - メニューは、オンラインヘルプへのアクセスおよびその他のマニュアルのリンクを提供します。このメニューから、すべての機能の情報を探ることができます。

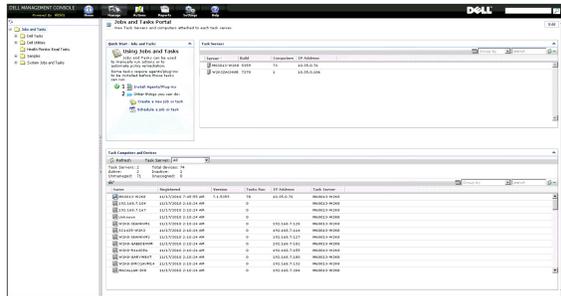
次に、**標準コンソール**の Dell Management Console サブメニューの例を示します。

- 1 Home(ホーム)メニューには、Dell Management Console ポータルサブメニューが含まれています。プラグインをインストールすると、対応するポータルをこのメニュー下で使用できるよう

になります。

- 1 **Manage(管理)**メニューには、コンピュータ、ユーザー、リソースからタスクおよびイベントまで、管理できるすべてのコンポーネントが含まれています。
- 1 **Actions(アクション)**メニューには、エージェントの検出、インベントリ作成、監視および導入など、ネットワークデバイスで実行できるアクションが含まれています。
- 1 **Reports(レポート)**メニューには、Dell Management Console で使用できるすべてのレポートが含まれています。
- 1 **Settings(設定)**メニューは、セキュリティ、Symantec Notification Server およびすべての Dell Management Console を設定するためのサブメニューが含まれています。
- 1 **Help(ヘルプ)**メニューは、オンラインヘルプへのアクセスおよびその他のマニュアルのリンクを提供します。このメニューから、すべての機能の情報を探ることができます。

サブメニューを選択すると、左側のツリー構造を介してナビゲートできるページが表示されます。右側は、データをグラフィックで表現する、さまざまなウェブパーツで構成されます。たとえば、Jobs and Tasks(ジョブとタスク)ポータルページでは、左ペインにツリー構造が表示されます。右ペインには、Quick Start - Jobs and Tasks(クイックスタート - ジョブおよびタスク)、Task Servers(タスクサーバー)および Task Computer and Devices(タスクコンピュータおよびデバイス)ウェブパーツが表示されます。



## Home(ホーム)メニュー - 基本コンソール用の Dell Management Console ポータルページ

Dell Management Console には、ネットワーク上の Dell デバイスを管理および監視するために固有のダッシュボードおよびタスクへのクイックアクセスを提供するポータルページがあります。このページには、Home(ホーム)→Dell Management Console Portal(Dell Management Console ポータル)からアクセスできます。

ポータルページには、デバイス状況、タスクのステータス、アラートなどのウェブパーツが含まれています。ウェブパーツの詳細については、『Dell Management Console ユーザーズガイド』を参照してください。

Dell Management Console を基本コンソールモードで開始するには、Dell Enterprise Management Quick Start(Dell Enterprise Management クイックスタート)ウェブパーツを選択します。このウェブパーツで使用できるさまざまなタブにより、Dell Management Console の基本設定の実行が可能になります。

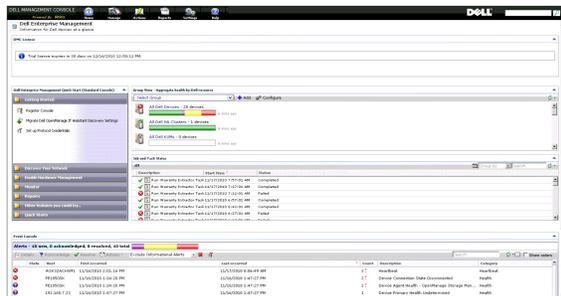
Dell Enterprise Management Quick Start(Dell Enterprise Management クイックスタート)ウェブパーツから、次を実行できます。

- 1 デルテクニカルセンター URL および Dell Management Console FAQ にオンラインでアクセスします。
- 1 既存の資格情報を編集するか、新しい資格情報を追加します。
- 1 Dell PowerEdge サーバーを検出して、デバイスのインベントリを作成します。
- 1 事前に選択されたデバイスの状況ステータスに関する電子メールアラートを、特定のユーザーに送信するように、Dell Management Console を設定できます。

## Home(ホーム)メニュー - 標準コンソール用の Dell Management Console ポータルページ

Dell Management Console には、ネットワーク上の Dell デバイスを管理および監視するために固有のダッシュボードおよびタスクへのクイックアクセスを提供するポータルページがあります。このページには、Home(ホーム)→Dell Management Console Portal(Dell Management Console ポータル)からアクセスできます。

ポータルページには、デバイス状況、タスクのステータス、アラートなどのウェブパーツが含まれています。



Dell Management Console を開始するには、Dell Enterprise Management Quick Start(Dell Enterprise Management クイックスタート)ウェブパーツを選択します。このウェブパーツで使用できるさまざまなタブにより、Dell Management Console の設定が可能になります。

Dell Enterprise Management Quick Start(Dell Enterprise Management クイックスタート)ウェブパーツから、次を実行できます。

- 1 検出範囲を Dell OpenManage IT Assistant から移行。
- 1 ネットワーク上のデバイスを検出して、監視。
- 1 検出されたデバイスのインベントリを作成して、アップデートを適用。
- 1 Dell 固有のレポートを使用、または新しいレポートを作成。

---

## コンソールモードの切り替え

基本コンソールおよび標準コンソールモードを切り替えることができます。Dell Management Console では、デフォルトモードは、標準コンソールに設定されています。基本コンソールおよび標準コンソールへのアクセスはユーザーベースです。特定のモードを選択して、再びログインすると、以前選択されていたモードが使用可能になります。

- 1 標準コンソールモードから基本コンソールモードに切り替えるには、Dell Management Console ポータルページから、Home(ホーム)→ Basic Console(基本コンソール)を選択します。基本コンソールモードの Dell Management Console ポータルページが表示されます。
- 1 基本コンソールモードから標準コンソールモードに切り替えるには、Dell Management Console ポータルページから、Home(ホーム)→ Standard Console(標準コンソール)を選択します。標準コンソールモードの Dell Management Console ポータルページが表示されます。

## Dell Management Consoleポータルページの変更

ポータルページからウェブパーツを追加または削除できます。

- 1 Dell Management Console Portal(Dell Management Console ポータル)ページの右上隅からEdit(編集)を選択します。

 **メモ:** Edit(編集)ボタンがこのページに表示されるのは、Dell Management Console を Dell Web サイト([dell.com/openmanage/register](http://dell.com/openmanage/register))に登録している場合だけです。

- 2 select web part(ウェブパーツの選択)で、ポータルページに表示するウェブパーツを選択して、Add(追加)をクリックします。  
選択したウェブパーツが、ポータルページに追加されます。ポータルページのウェブパーツを目的の位置にドラッグアンドドロップできます。
- 3 Apply(適用)をクリックします。

---

## アプリケーションの起動

Dell Management Console から他のアプリケーションを起動できます。検出されたデバイスのタイプに応じて、Dell Management Console は、デバイスのシステム管理アプリケーションのための統合起動ポイントを提供します。

デバイスのアプリケーションを起動するには、次のオプションから選択します。

- 1 Manage(管理)メニュー
- 1 Resource Manager(リソースマネージャ)
- 1 Settings(設定)メニュー
  - o Dell OpenManage Network Manager
  - o Dell OpenManage RAC コンソール

### 管理メニュー

- 1 Dell Management Console から、Manage(管理)→ All Devices(すべてのデバイス)を選択します。
- 2 All Devices(すべてのデバイス)ページで、たとえば、サーバーなどのデバイスを開き、右クリックして、Management Applications(管理アプリケーション)を選択します。

Dell OpenManage Server Administrator、SOL プロキシ および Telnet などのシステム管理アプリケーションオプションが表示されます。

これらのアプリケーションを起動して、適切なアクションを実行できます。

デバイスで使用できるオプションは、接続プロファイルによって異なります。たとえば、SNMP プロトコルを使用するデバイスを検出した場合、次のオプションを使用できます。

- 1 Dell Open Manage Server Administrator
- 1 Dell Remote Access Controller(DRAC)が存在するシステムの RAC コンソール
- 1 DRAC が存在するシステムの RAC Telnet



1. Dell Management Console から、**Settings**(設定)→ **Console**(コンソール)→ **Right-click Actions**(右クリックアクション)を選択します。
2. **Management Applications**(管理アプリケーション)ページの左ペインで、たとえば、**Dell OpenManage Network Manager** などのアプリケーションをクリックします。

Dell OpenManage Network Manager ページが表示されます。

 **メモ:** このアプリケーションは、インフラストラクチャデバイスの右クリックオプションであるため、**Resource Type**(リソースタイプ)では **Dell Infrastructure Device**(Dell インフラストラクチャデバイス)として表示されます。

ネットワークデバイスのリソースタイプについては、[表 5-1](#) で説明されています。

**表 5-1. Dell デバイスのリソースタイプ**

Dell デバイス	リソースタイプ
Dell PowerEdge システム	Dell Computer (Dell コンピュータ)
プリンタ	Dell Printer (Dell プリンタ)
Dell EMC	Dell Network Storage Device (Dell ネットワークストレージデバイス)
テープ	Dell Network Backup Device (Dell ネットワークバックアップデバイス)
Dell PowerConnect/KVM/ ファイバーチャネルスイッチ	Dell Infrastructure Device (Dell インフラストラクチャデバイス)
Dell Remote Access Controller	Dell OOB (out-of-band) Management Device (Dell OOB (帯域外) 管理コンソール)
Dell PowerVault MD アレイ	Dell Network Storage Device (Dell ネットワークストレージデバイス)
Dell EqualLogic グループ	

 **メモ:** デバイスのリソースタイプは変更しないことをお勧めします。

3. このアプリケーションはコマンドラインタイプで、このアプリケーションのデフォルトロケーションは、**Command Line**(コマンドライン)に表示されます。

 **メモ:** このアプリケーションをデフォルト以外のロケーションにインストールした場合、**Command Line**(コマンドライン)に表示されるロケーションを編集するようにしてください。

## 設定メニュー: Dell OpenManage RAC コンソール

1. Dell Management Console から、**Settings**(設定)→ **Console**(コンソール)→ **Right-click Actions**(右クリックアクション)を選択します。
2. **Management Applications**(管理アプリケーション)ページの左ペインで、たとえば、**RAC コンソール**などのアプリケーションをクリックします。

Dell OpenManage RAC コンソールページが表示されます。

3. このアプリケーションは、Dell 帯域外(OOB)デバイスの右クリックオプションであるため、**Resource Type**(リソースタイプ)には **Dell OOB Management Device**(Dell OOB 管理デバイス)が表示されます。

 **メモ:** デバイスのリソースタイプは変更しないことを強くお勧めします。

4. このアプリケーションは URL タイプで、このアプリケーションのデフォルトロケーションは、**Base URL**(ベース URL)に表示されます。

 **メモ:** URL がデフォルトと異なる場合、または SSL を有効にしている場合、アプリケーション起動が正しく機能するように URL を編集するようにしてください。

## 設定ページ

Configuration(設定)ページは、サーバーキー設定タスク、および次の追加ヘルプリソースを介して、詳細な手順を示す統合ガイドです。これには次が含まれます。

- 1 クライアントおよび Dell Management Console サーバーの両方の SNMP 設定
- 1 検出の設定および実行
- 1 インベントリの実行
- 1 監視の設定
- 1 パッチ管理の設定
- 1 Dell テックセンターおよび Dell Management Console FAQへのリンク

## 設定の管理

設定タスクを使用するには、次の手順を実行します。

1. Dell Management Console で、**Home**(ホーム)→ **Configuration** (設定)を選択します。

**Configuration**(設定) ページが表示されます。**Configuration**(設定)では、**Discovery and Inventory**(検出とインベントリ)、**Monitor Configuration**(監視設定)、**SNMP Alerts**(SNMP アラート)および **Patch Configuration**(パッチ設定)領域を設定できます。

2. **Configuration** (設定)で、これらの設定可能領域から選択して、**Apply**(適用)をクリックします。

- 1 **Discovery and Inventory**(**検出とインベントリ**): 検出およびインベントリに関連するタスクを設定および開始します。
- 1 **Monitor Configuration**(**監視設定**): 監視設定を設定および適用します。
- 1 **SNMP Alerts**(**SNMP アラート**): クライアントの SNMP を設定する方法を示します。
- 1 **Patch Configuration**(**パッチ設定**): Altiris Agent または Lifecycle Controller ベースパッチングのパッチ管理を設定します。

3. 設定する領域のタブをクリックして、手順に従い完了します。

4. 手順を実行して設定を完了します。

---

[目次に戻る](#)