HP Universal CMDB

ソフトウェアバージョン: コンテンツ・パック 16.00（CP16）

ディスカバリ / インテグレーション・コンテンツ・ガイド - 全般的な参照情報

ドキュメントリリース日: 2015 年 7 月
ソフトウェアリリース日: 2015 年 7 月

ご注意

保証

HP製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載は、追加保証を提供するものではありません。ここに含まれる技術的、編集上の誤り、または欠如について、HPはいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、HPからの有効な使用許諾が必要です。商用コンピューターソフトウェア、コンピューターソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

商標について

Adobe™ は、Adobe Systems Incorporated (アドビシステムズ社) の登録商標です。

Microsoft ® およびWindows ® は、米国におけるMicrosoft Corporationの登録商標です。

UNIX ® は、The Open Groupの登録商標です。

ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

- ソフトウェアバージョンの番号は、ソフトウェアのバージョンを示します。
- ドキュメントリリース日は、ドキュメントが更新されるたびに変更されます。
- ソフトウェアリリース日は、このバージョンのソフトウェアのリリース期日を表します。

更新状況、およびご使用のドキュメントが最新版かどうかは、次のサイトで確認できます。
https://softwaresupport.hp.com/。

このサイトを利用するには、HP Passportへの登録とサインインが必要です。HP Passport IDを登録するには、HPサポートサイトで登録のボタンをクリックするか、HPパスポートのログインページでアカウント作成のボタンをクリックします。

適切な製品サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HPの営業担当にお問い合わせください。

サポート

次のHPソフトウェアサポートサイトを参照してください。https://softwaresupport.hp.com。

このサイトでは、HPのお客様窓口のほか、HPソフトウェアが提供する製品、サービス、およびサポートに関する詳細情報をご覧いただけます。

HPソフトウェアオンラインではセルフソルブ機能を提供しています。お客様のビジネスを管理するのに必要な対話型の技術サポートツールに、素早く効率的にアクセスできます。HPソフトウェアサポートのWebサイトでは、次のようなことができます。

- 関心のあるナレッジドキュメントの検索
- サポートケースの登録とエンハンスメント要求のトラッキング
- ソフトウェアパッチのダウンロード
- サポート契約の管理
- HPサポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部のサポートを除き、サポートのご利用には、HP Passportユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport IDを登録するには、HPサポートサイトで登録のボタンをクリックするか、HPパスポートのログインページでアカウント作成のボタンをクリックします。

アクセスレベルの詳細については、次のWebサイトをご覧ください。
https://softwaresupport.hp.com/web/softwaresupport/access-levels。

HP ソフトウェア・ソリューションは、HPSW のソリューションと統合に関するポータル Web サイトです。このサイトでは、お客様のビジネスニーズを満たすHP製品ソリューションを検索したり、HP製品間の統合に関する詳細なリストやITILプロセスのリストを閲覧することができます。このサイトのURLはhttp://h20230.www2.hp.com/sc/solutions/index.jsp です。

目次

第1章: 新しいポートの定義方法

次の手順を実行して **portNumberToPortName.xml** ファイルを編集し、新しいポートを定義します。

1. ［**アダプタ管理**］ウィンドウ（［**マネージャ**］ > ［**データ フロー管理**］ > ［**アダプタ管理**］）で、次のように portNumberToPortName.xml ファイルを検索します。［**リソースの検索**］ボタンをクリックし、［**名前**］ボックスに **portNumberToPortName.xml** を入力します。［**次を検索**］をクリックし、［**閉じる**］をクリックします。

   ［**リソース**］表示枠にファイルが選択され、ファイルの内容が内容表示枠に表示されます。

   このファイルの詳細については、「portNumberToPortName.xml ファイル」(32ページ)を参照してください。

2. 次のように、ファイルに行を追加し、パラメータを変更します。

   <portInfo portProtocol="xxx" portNumber="xxx" portName="xxx" discover="0" cpVersion="xx"/>

パラメータ	説明
portProtocol	ディスカバリに使用するネットワーク・プロトコル（udp または tcp）。
portNumber	検出されるポート番号。 この属性は、数値または範囲。範囲はカンマ、ダッシュ、またはその両方で区切られる。例 :"10, 21, 45"、"10-21"、または "10-21, 45, 110"。
portName	表示されるこのポートの名前。
discover	**1** : このポートは検出される必要がある。 **0** : このポートは検出される必要がない。
cpVersion	パッケージ・マネージャを使用して **portNumberToPortName.xml** ファイルを別の UCMDB システムにエクスポートする場合に使用する。他のシステム上の **portNumberToPortName.xml** ファイルにこのアプリケーション用のポートが含まれ、追加の必要がある新しいポートが含まれていない場合、**cpVersion** 属性を使用し、新しいポートの情報を他のシステム上のファイルにコピーする。 **cpVersion** の値は、**portNumberToPortName.xml** ファイルのルートに表示される値よりも大きい必要がある。 たとえば、ルートの **cpVersion** 値が次のように **3** の場合。

パラメータ	説明
	<portList parserClassName="com.hp.ucmdb.discovery.library.communication.downloader.cfgfiles.KnownPortsConfigFile" cpVersion="3"> 新しいポート・エントリには **cpVersion** 値として **4** が含まれる必要がある。 <portInfo portProtocol="udp" portNumber="1" portName="A1" discover="0" cpVersion="4"/> **注:** ルートの **cpVersion** 値がない場合、新しいポート・エントリに任意の負ではない数を追加できる。 このパラメータは、コンテンツ・パックのアップグレード中にも必要となる。詳細については、「cpVersion 属性を使用してコンテンツ更新を確認する方法」(7ページ)を参照してください。

第2章: cpVersion 属性を使用してコンテンツ更新を確認する方法

cpVersion 属性は、portNumberToPortName.xml ファイルに含まれ、ポートが検出されたコンテンツ・パックのリリースを示します。たとえば、次のコードでは LDAP ポート 389 がコンテンツ・パック 11.00 で検出されたと定義されます。

```
<portInfo portProtocol="tcp" portNumber="389" portName="ldap" discover="11" cpVersion="11"/>
```

コンテンツ・パックのアップグレード中に、DFM ではこの属性を使用して、既存の portNumberToPortName.xml ファイル（ユーザ定義のポートを含む場合がある）と新しいファイルをスマート結合します。以前ユーザが追加したエントリは削除されず、以前ユーザが削除したエントリは追加されません。

portNumberToPortName.xml ファイルの詳細については、「portNumberToPortName.xml ファイル」(32ページ)を参照してください。

コンテンツ・パックが正常にデプロイされているか確認するには、次の手順を実行します。

1. 最新のサービス・パック・リリースをインストールします。
2. UCMDB サーバを起動します。
3. すべてのサービスが実行中であることを確認します。詳細については、『HP Universal CMDB 管理ガイド』の HP Universal CMDB サービスの項を参照してください。
4. 最新のコンテンツ・パック・リリースをインストールおよびデプロイします。詳細については、『Content Pack Installation Guide』を参照してください。
5. ［**アダプタ管理**］ウィンドウで、**portNumberToPortName.xml** ファイルにアクセスします。
6. ユーザ定義のポートは削除されておらず、ユーザが削除したポートは追加されていないことを確認します。

第3章: リモート・マシンにコピーされたファイルの削除方法

ディスカバリの実行中、Data Flow Probe により、リモート Windows マシンにファイルがコピーされます。詳細については、「リモート・マシンにコピーされるファイル」(11ページ)を参照してください。

ディスカバリ完了後にコピー先マシンにコピーされたファイルを削除するように DFM を構成するには、次の手順を実行します。

1. **globalSettings.xml** ファイルにアクセスします（［**アダプタ管理**］ > ［**AutoDiscoveryContent**］ > ［**構成ファイル**］）。
2. **removeCopiedFiles** パラメータを見つけます。
   - **true** :ファイルは削除されます。
   - **false** :ファイルは削除されません。
3. ファイルを保存します。

HPCmd の動作を制御するには、次の手順を実行します。

1. **globalSettings.xml** ファイルにある **NtcmdAgentRetention** パラメータを見つけます。
2. 次のいずれかの値を入力します。
   - **0** :（標準設定）サービスを登録解除し、リモートの実行可能ファイルを削除します（**登録解除**: サービスのリストに表示されないようにするために、サービスを停止してリモート・マシンからサービスを削除します）。
   - **1** : サービスを登録解除しますが、実行可能ファイルをファイル・システムに残します。
   - **2** : サービスを実行中のままにし、実行可能ファイルをファイル・システムに残します。

第4章: Windows 2008 および Windows Server 2008 R2 マシンから HPCmd を実行する方法

プローブが Windows 2008 または Windows Server 2008 R2 マシンにインストールされている場合、次の手順を実行して、HPCmd を適切に機能させます。

1. プローブを停止します。
2. **regedit** コマンドを実行し、標準の Windows レジストリ・エディタ・アプリケーションを開きます。
3. レジストリ・エディタで、次のレジストリ・キーに移動します。

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

4. このキーの下に **REG_DWORD** パラメータ **SCMApiConnectionParam** があります。
   a. ない場合は、新しい **REG_DWORD** パラメータ **SCMApiConnectionParam** を追加し、その値を 0x80000000 に設定します。
   b. レジストリにこの値がすでにある場合、この値を 0x80000000 マスクと結合します（ビット単位の論理和を使用）。たとえば、レジストリに値 0x1 があった場合、この値を 0x80000001 に設定します。

   > **注: UAC が有効になっている** Windows 2008 マシンから HPCmd を実行するには、次の手順も追加で実行します。**Windows Server 2008 R2 マシンで、これらの手順を実行しないでください。**

5. hp\UCMDB\DataFlowProbe\bin ディレクトリで **wrapper.exe** ファイルを見つけます。
6. **wrapper.exe** ファイルを右クリックし、［**プロパティ**］を選択します。
7. ［**互換性**］タブで、次を実行します。
   a. ［**互換モード**］を選択します。
   b. ［**Windows XP（Service Pack 2）互換モードでこのプログラムを実行する**］を選択します。

c. ［**管理者としてこのプログラムを実行する**］を選択します。

8. プローブを起動します。

注: HPCmd では、DCOM プロトコルを使用してリモート・マシンに接続します。DCOM プロトコルでは、ポート **135**、**137**、**138** および **139** がオープンになっている必要があります。また、**1024** ~ **65535** の任意のポートが使用されますが、WMI / DCOM / RPC が使用するポート範囲を制限する方法があります。ファイアウォールを使用する場合の DCOM の設定については、http://support.microsoft.com/kb/154596/en-us を参照してください。

第5章: リモート・マシンにコピーされるファイル

ディスカバリの実行中、マシンのコンポーネントのディスカバリを有効にするため、Data Flow Probe はリモート Windows マシンにファイルをコピーします。ファイルは、リモート・マシン上の **%SystemRoot%\system32\drivers\etc** フォルダにコピーされます。

注:

- ［データ フロー管理］では、**HPCmdSvc.exe** を実行し、リモート・マシン上のシェルに接続して取得します。
- リモート Windows マシン上で **Host Connection by Shell**、**Host Resources by Shell**、または **Host Applications by Shell** ジョブにより **wmic** コマンドが起動されると、空の **TempWmicBatchFile.bat** ファイルが作成されます。

以下のファイルがコピーされます。

ファイル	コンテンツ・パックのバージョン	説明
adsutil.vbs	すべて	Microsoft IIS アプリケーションのディスカバリに使用される Visual Basic スクリプト。IIS を検出するため、DFM はこのスクリプトをリモート・マシンにコピーする。 **関連 DFM ジョブ :**IIS Applications by NTCMD or UDA
diskinfo.exe	すべて	**wmic** によりディスク情報が取得できない場合に、ディスク情報の取得を有効にする実行可能ファイル。 DFM は **wmic** クエリを使用して、標準設定のディスク情報を検出する。ただし、**wmic** クエリが実行できない場合、DFM はリモート・マシンに **diskinfo.exe** ファイルをコピーする。**wmic.exe** が PATH システム変数に含まれていない場合、またはこのファイル自体がリモート・マシンに存在しない場合（Windows 2000）に、この障害が発生することがある。 **関連 DFM ジョブ :**Host Resources by Shell

ファイル	コンテンツ・パックのバージョン	説明
Exchange_Server_2007_Discovery.ps1	CP4	MS Exchange 2007 のディスカバリのための PowerShell スクリプト。 DFM は、NTCMD で Microsoft Exchange 2007 を検出するために PowerShell シナリオを使用する。このため、このファイルをリモート・マシンにコピーする必要がある。 **関連 DFM ジョブ：** • Microsoft Exchange Connection by NTCMD or UDA • Microsoft Exchange Topology by NTCMD or UDA

ファイル	コンテンツ・パックのバージョン	説明
GetFileModificationDate.vbs	CP5	ファイルの変更日を取得するための Visual Basic スクリプト（ロケールは無視される）。 もっとも一般的な使用事例は、検出されたアプリケーションの構成ファイルの最終変更日を DFM が取得する必要がある場合。 **関連 DFM ジョブ :** • Apache Tomcat by Shell • File Monitor by Shell • IIS Applications by NTCMD or UDA • JEE Weblogic by Shell • JEE WebSphere by Shell or JMX • JEE WebSphere by Shell • SAP System by Shell • Service Guard Cluster Topology by TTY • Siebel Application Server Configuration • Software Element CF by Shell • Veritas Cluster by Shell • Web Server by Shell
getfilever.vbs	すべて	実行中のソフトウェアのバージョンを特定するのに使用される Visual Basic スクリプト。スクリプトは、Windows マシン上の実行可能ファイルまたは DLL ファイルのバージョンを取得する。 このスクリプトは、リモート・マシン上の特定ソフトウェアのバージョンを取得するために、シェルベースのアプリケーション署名プラグインにより使用される。 **関連 DFM ジョブ :**Host Applications by Shell

ファイル	コンテンツ・パックのバージョン	説明
junction.exe	CP5	この実行可能ファイルは、Sysinternals Suite（http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx）に含まれ、分岐ポイントの作成を有効にする。リモート・マシン上に **linkd.exe** および **mklink.exe** ツールが存在しない場合、DFM はこのファイルを使用する。 DFM が Windows x64 マシン上でディスカバリを実行するとき、DFM は、そのマシン上で実行されている Windows のリダイレクト機能をバイパスする必要がある。DFM は **linkd.exe** または **mklink.exe** ツールのいずれかを使用して **%SystemRoot%\System32** フォルダへのリンクを作成することで、これを実行する。ただし、これらのツールがリモート・マシン上に存在しない場合、DFM はリモート・マシンに **junction.exe** を転送する。その後、DFM は 64 ビット・バージョンのシステム実行可能ファイルを起動できるようになる（仮にこの 64 ビット・バージョンを使用しない場合、DFM は分離された 32 ビットの領域にロックされる）。 この分岐ポイントは、ディスカバリが完了すると自動的に削除される。 **関連 DFM ジョブ：** • Host Resources by Shell • Host Applications by Shell • Microsoft Exchange Connection by NTCMD or UDA • Microsoft Exchange Topology by NTCMD or UDA
meminfo.exe	すべて	メモリ情報の取得を有効にする実行可能ファイル。 DFM は **wmic** クエリを使用して、メモリ情報を検出する。ただし、**wmic** クエリが実行できない場合、DFM はリモート・マシンに **meminfo.exe** ファイルをコピーする。**wmic.exe** が PATH システム変数に含まれていない場合、またはこのファイル自体がリモート・マシンに存在しない場合（Windows 2000）に、この障害が発生することがある。 **関連 DFM ジョブ :**Host Applications by Shell

ファイル	コンテンツ・パックのバージョン	説明
reg_mam.exe	すべて	レジストリのクエリを有効にする Microsoft reg.exe ファイルのコピー。 DFM でネイティブの reg.exe ファイルが検出されない場合、この実行可能ファイルがリモート Windows マシンにコピーされる。このツールが標準では含まれていない、一部の旧バージョンの Windows (Windows 2000など) でこの状況が発生する。 **関連 DFM ジョブ :**Host Applications by Shell

第6章: コンテンツ・パックの構成ファイル

コンテンツ・パックには、コマンドのタイムアウトやユーティリティの利用、アプリケーション署名など共通に使われるパラメータを構成するための構成ファイルが含まれています。

本項の内容

globalSettings.xml ファイル

以下の表で **globalSettings.xml** 構成ファイル（［**データ フロー管理**］ > ［**アダプタ管理**］ > ［**リソース**］ > ［**パッケージ**］ > ［**AutoDiscoveryContent**］ > ［**構成ファイル**］）に含まれるパラメータを説明します。

パラメータ	説明
AdditionalClasspath	別パターン（データベース・パターンなど）の実行を有効にする追加パス。すべてのパスは **$PROBE_INSTALL/root/lib/collectors/** に相対的である必要がある。**probeManager/discoveryResources/** フォルダからの相対パスで指定され、セミコロンで区切られている必要がある。 **例：** **<property name="AdditionalClasspath">db/oracle/.;db/mssqlserver/.</property>** この場合、classpath には次のパスが含まれることになる。 • **$PROBE_INSTALL/root/lib/collectors/probeManager/discoveryResources/db/oracle/** • **$PROBE_INSTALL/root/lib/collectors/probeManager/discoveryResources/db/mssqlserver/**
allowCaliperOnHPUX	HP-UX 上で caliper の実行を許可するかどうかを示す。この設定は **WebSphere_By_Shell** アダプタで使用され、**ps** コマンドが失敗したときに代わりに完全なコマンド・ラインを取得す

パラメータ	説明
	る。 **標準設定 :** false
allowCallhome	コール・ホームを許可するかどうかを示す。 **標準設定 :**true
allowCallhomeInterval	同じホストからの 2 つのコール・ホーム要求で許可される間隔（時間）。 **標準設定 :**24
allowDataCenterCallhome	コール・ホームへのデータ・センター IP アドレスを許可するかどうかを示す。 **標準設定 :**true
allowGettingCredentialSecuredAttribute	Jython スクリプトによる資格情報のセキュリティ保護されたデータの取得を許可（true）するか、禁止（false）するかを示す。この設定が false に設定されている場合、Jython スクリプトは機密性のある資格情報データ（サーバ側に格納されているパスワードなど）を取得できない。 **標準設定 :**true
allowPFilesOnSunOS	Solaris 上で pfiles の実行を許可するかどうかを示す。 **標準設定 :** false **注意:**このパラメータを true に設定すると、一部の Solaris システム上の一部のプロセスで問題が発生する場合がある。
allowPFilesOnHPUX	HP-UX 上で pfiles の実行を許可するかどうかを示す。 **標準設定 :** false **注意:**このパラメータを true に設定すると、一部の HP-UX システム上の一部のプロセスで問題が発生する場合がある。
autoTruncateDbEncoding	CMDB の基盤となるデータベースで使用されるエンコーディングを示す。このプロパティは短縮後に送信する必要がある文字数を計算するために使用される。 **標準設定 :**UTF8

パラメータ	説明
autoTruncatePercentage	属性（DDM_AUTOTRUNCATE 修飾子を含む）の値がこのパラメータにより乗算されたサイズ制限を超えると、定義されているサイズの指定部分に短縮される。 **標準設定 :**100 パーセント
clearCommandLineFor Processes	指定されたプロセスのコマンド・ラインをクリアする。 このオプションを使用して、個人的なデータや機密データが CMDB に格納されないようにする。 **標準設定:** srvrmgr.exe、srvrmgr、xCmd.exe、HPcmd.exe、ssonsvr.exe **構文の例外 :**プロセス名には大文字小文字の区別はなし。プロセス名はカンマで区切る必要がある。
consoleCommands	すべての PowerShell 接続にグローバルに使用可能なコマンドのカンマ区切りリスト。 このリストで指定されているコマンドは、CMD インタープリタ（cmd /c "コマンド"）を使用して実行される。
datacentercallhome	管理ゾーンがデータ・センターに設定され、このパラメータが有効である場合、Data Flow Probe は Universal Discovery エージェントからのコール・ホームメッセージを無視する。 **標準設定 :**有効
dbQueryTimeout	すべての SQL クエリのタイムアウト（秒）。クエリ結果の待機時間を示す。 ゼロ（0）より大きな値が設定されている場合のみ、タイムアウトが発生する。 **標準設定 :**100 秒 **注:** 一部の JDBC ドライバでは、この設定はサポートされていない。
ddmagentCiphers	クライアント・マシンとの間で転送されるデータを、UD エージェントが暗号化または復号化するときに使用するアルゴリズム。
ddmagentPrefix	UD エージェントが使用するプレフィックス。
ddmagentProtocol	UD エージェントとの通信にプローブが使用するプロトコル。

パラメータ	説明
ddmagentEnableDownloadResume	再開可能ダウンロードが有効かどうかを指定する。 **true :**再開可能ダウンロード機能は使用可能。 **false :**再開可能ダウンロード機能は使用不可。
ddmagentDefaultBlockLen	UD エージェントとの間でファイルをアップロード / ダウンロードするのに使用される、標準設定のチャンク・サイズ（バイト）。
ddmagentResumableFileSuffix	再開可能転送ファイルの部分に使用されるファイル拡張子。
ddmagentDefaultResumeBlockLen	再開可能ファイル転送の標準設定のチャンク・サイズ（バイト）。
ddmagentEnableUploadResume	再開可能アップロードが有効かどうかを指定する。 **true :**再開可能アップロード機能は使用可能。 **false :**再開可能アップロード機能は使用不可。
defaultSapClients	このパラメータが定義されると、SAP ABAP プロトコルの SAP クライアント番号パラメータを指定する必要はない。その代わり、さまざまなサポート対象クライアントが含まれる、複数の SAP システムに対応する、1 つまたは複数のカンマ区切り資格情報を作成できる。 **例 :** <property name= "defaultSapClients"> 800,500,200,300 </property> **標準設定 :**800
desktopOperatingSystems **serverOperatingSystems**	これら 2 つのパラメータは、ホストのオペレーティング・システムの種類が Desktop であるか Server であるかを決定するのに使用される。ホストのオペレーティング・システム名に、これらリストのいずれかの値が含まれる場合、結果として **host_isdesktop** 属性に値が設定される。それ以外の場合、**host_isdesktop** 属性の値は空欄のまま。
discovereAllListenPorts	アプリケーションの署名の構成に関係する。
discoveredStorageTypes	UCMDB に報告する必要があるストレージ・タイプを記述する。オプションはカンマで区切る。 使用可能なオプションは以下のとおり。

パラメータ	説明
	• FixedDisk • NetworkDisk • CompactDisk • RemovableDisk • FloppyDisk • VirtualMemory • FlashMemory • RamDisk • Ram • No Root Directory • Other • UNKNOWN
enableJeeEnhancedTopology	改善された JEE トポロジのレポートを有効にするかどうかを示す。 **標準設定 :** false
enableNormalizationRuleLabel	正規化ルールの出力値のラベル形式が有効か無効かを指定する。 正規化フィールドに、アンダースコアが含まれる標準設定の形式ではなく、ラベル形式で値を表示する場合、次の手順を実行する。 1. **globalSettings.xml** ファイルに **<property name="enableNormalizationRuleLabel">true</property>** を追加する（存在しない場合）。 2. プローブを再起動する。 **標準設定 :** false
enableSSHSharedHomeDir	このパラメータを **true** にすると、共有ホーム・ディレクトリが設定されたユーザ・アカウントを SSH 経由のインベントリ・ディスカバリで使用できるようになる。たとえば、ホー

パラメータ	説明
	ム・ディレクトリが NFS または Samba を介してマウントされている場合、ユーザが別のコンピュータにログインしても同じディレクトリが使用される。 この機能を正常に動作させるには、（NFS または Samba を介してマウントされるなどの）共有のホーム・ディレクトリが設定されているユーザ・アカウントで実行される Universal Discovery エージェントをインストールすることはできない。すでにインストールされている場合は、アンインストールする。詳細については、『データ・フロー管理ガイド』の「Universal Discovery エージェントを完全にアンインストールする方法」を参照。 この機能を有効にするには、このパラメータ値を **true** に設定する。標準設定値は **false**。 **注意 :**この機能を有効にしてから無効にすると、予期しない動作が発生することがある。 **注:** • この機能を有効にした後は、（NFS または Samba を介してマウントされるなどの）共有のホーム・ディレクトリが設定されたユーザ・アカウントで実行される Universal Discovery エージェントをインストールしないこと。 • UCMDB で、新規作成された空のノード CI が予期せず表示されることがある。削除することも、エイジング・メカニズムにより削除されるのを（通常 40 日後）待つことも可能。 • SSH プロトコルを使用していると、Inventory Discovery by Scanner ジョブで、ソフトウェア使用率情報が報告できない。
IgnoreClassAttributes	ディスカバリ結果の処理の属性を無視する。 **形式:** node.name、node.description Data Flow Probe はノード属性名と説明を検証しない。プローブはこれらの属性を UCMDB に報告しない。 **標準設定:** node.misc_info

パラメータ	説明
ignoreLocalizedVirtualInterfacesPatternList	ホスト・キーの作成処理に関与させてはならない、ローカライズされた Windows 仮想インタフェース説明のパターンをリストする。 **形式 :**文字列のカンマ区切りリスト。空白を追加することはできない。
ignoreVmwareInterfaces	VMware MAC アドレスを無視するかどうかを示す。 • **物理 MAC が存在する場合**（標準設定）。パターンで物理 MAC アドレスが見つからない場合にのみ、VMware MAC アドレスが使用される。 • **常時 :**VMware MAC アドレスは常に無視される。
jdbcDrivers	このパラメータには、専用データベース・サーバに接続するのに使用されるドライバ・クラスを列挙する。サブキーの名前は、資格情報で使用されるものと同じである必要がある（プロトコルの sqlprotocol_dbtype 属性）。 標準設定の JDBC ドライバ以外のドライバが使用されている場合、変更する。 **標準インストールの場合のデフォルト値は以下のとおり。** <property name="jdbcDrivers:> <oracle> oracle.jdbc.OracleDriver </oracle> <oracleSSL> oracle.jdbc.OracleDriver </oracleSSL> <MicrosoftSQLServer> net.sourceforge. jtds.jdbc.Driver </MicrosoftSQLServer> <MicrosoftSQLServer> net.sourceforge.jtds. jdbc.Driver </MicrosoftSQLServerNTLM> <MicrosoftSQLServerNTLMv2> net.sourceforge.jtds.jdbc.Driver </MicrosoftSQLServerNTLMv2> <Sybase> com.sybase.jdbc.SybDriver </Sybase>

パラメータ	説明
	<db2> com.ibm.db2.jcc.DB2Driver </db2> <mysql> com.mysql.jdbc.Driver </mysql> </property>
jdbcPreUrls	このパラメータには、専用データベース・サーバに接続するのに使用される URL テンプレートを列挙する。サブキーの名前は、資格情報で使用されるものと同じである必要がある（プロトコルの sqlprotocol_dbtype 属性）。標準設定の JDBC ドライバ以外のドライバが使用されている場合、変更する。値は使用されるドライバによって異なり、ドライバのマニュアルから取得する必要がある。 **注:** XML 標準に従い、アンパサンド記号（&）はエスケープ処理（&）する必要がある。 **標準インストールの場合のデフォルト値は以下のとおり。** <property name="jdbcPreUrls"> <oracle>jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS= (PROTOCOL=tcp) (HOST=%%ipaddress%%)(PORT=%%protocol_port%%)) (CONNECT_DATA=(%%connect_data%%=%%sqlprotocol_ dbsid%%))) </oracle> <oracleSSL>jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS= (PROTOCOL=tcps) (HOST=%%ipaddress%%)(PORT=%%protocol_port%%)) (CONNECT_DATA=(%%connect_data%%=%%sqlprotocol_ dbsid%%))) </oracleSSL> <MicrosoftSQLServer> jdbc:jtds:sqlserver:// %%ipaddress%%:%%protocol_port%%; instanceName=%%sqlprotocol_dbname%%; loginTimeout=%%protocol_timeout%%; logging=false;ssl=request </MicrosoftSQLServer> <MicrosoftSQLServerNTLM> jdbc:jtds:

パラメータ	説明
	sqlserver://%%ipaddress%%: %%protocol_port%%;instanceName= %%sqlprotocol_dbname%%;domain= %%sqlprotocol_windomain%%; loginTimeout= %%protocol_timeout%%;logging=false </MicrosoftSQLServerNTLM> <MicrosoftSQLServerNTLMv2>jdbc:jtds:sqlserver://%% ipaddress%%:%%protocol_port%%;instanceName=%% sqlprotocol_dbname%%;domain=%% sqlprotocol_windomain%%;loginTimeout=%% protocol_ timeout%%;logging=false;ssl=request;useNTLMv2=true </MicrosoftSQLServerNTLMv2> <Sybase> jdbc:sybase:Tds: %%ipaddress%% :%%protocol_port%%?DatabaseName= %%sqlprotocol_dbname%% </Sybase> <db2> jdbc:db2://%%ipaddress%%: %%protocol_port%%/ %%sqlprotocol_dbname%% </db2> <mysql> jdbc:mysql://%%ipaddress%%: %%protocol_port%%/ %%sqlprotocol_dbname %%</mysql> <parameters> <parameter type="oracle" name="connect_data"> <value>SERVICE_NAME</value> <value>SID</value> </parameter> <fallbackExceptionList> <error type="oracle">.*ORA\-12514.*</error> </fallbackExceptionList> </parameters> </property> 各 <parameter> 要素には name 属性、および 1 つまたは複数

パラメータ	説明
	の <value> タグが設定される。各 <parameter> は、形式 “%%[parameter name]%%” （%%connect_data%% など）を使用して、Oracle URL テンプレートに使用できる。 <parameter> に複数の <value> タグが設定されている場合、解析エンジンはテンプレート文字列内の取り得る値のすべての順列を生成し、クライアントは各順列を使用してデータベース・サーバへの接続を試みる。 接続中にエラーが発生することがあるため、<fallbackExceptionList> 要素には、エラーが発生したときに無視すべきエラーを指定する。エンジンが該当するエラーを無視すると、エンジンは、テンプレート文字列に含まれる値の別の順列を使用して接続を試みる。<fallbackExceptionList> に指定されていないエラーが発生すると、エンジンは別の順列を試みることなくジョブは失敗し、キャッチされたエラー・メッセージが表示される。
loadExternalDTD	XML の検証中、DTD ファイルをダウンロードしないように file_mon_utils を構成するのに使用される。 **標準設定 :** false
maxExecutionRecords	通信ログに格納可能な実行記録の最大数を指定する。このパラメータは、ディスカバリ処理で大量のデータが検出される場合に使用する必要がある。パラメータは、アダプタ・レベルで上書き可能。この場合、パラメータを適切な記録数の上限値が設定されたアダプタに追加する（プローブのマニュアルを参照してください）。 **標準設定 :**-1（制限なし）
maximumConnectionsPerSecond	プローブからほかのマシンに対する新しい接続数の秒あたりの制限を有効にする。 • **0 :**接続数の制限なし。 • **> 0 :**接続の最大数。この制限に達した場合、新しい接続の作成を試みるジョブはすべて、以下の "timeToSleepWhenMaximumConnectionsLimitReached" パラメータで決定された期間だけ待機する。 **標準設定 :**0（制限なし）
maxStoreSentResults	通信ログに格納可能な送信結果の最大数を指定する。

パラメータ	説明
	通信ログに非常に多くの結果が格納されるような場合にこのパラメータを変更する。 この値が 0 より大きい場合、削除された結果および更新された結果について、対応する個数の結果がログに格納される。このため、結果のセットには **maxStoreSentResults** の値の 2 倍の個数が格納される。 **標準設定 :**-1（制限なし）
maxPingIPv6CountPerRange	Ping スイープの範囲ごとの最大 IPv6 数を指定する。 **標準設定 :**1000000
multipleDB2Instances	複数の DB2 インスタンスが同じサーバにインストールされているかどうかを示す。 **標準設定:** true
multipleUpdateIgnoreTypes	UCMDB によって使用される。列挙 CI タイプに**バルク更新**警告が生成されなくなる。
notRecordedMethods	通信ログに記録されないメソッドのリストを指定する。 メソッドが通信ログに記録されないようにするには、通信ログからメソッドの名前をコピーし、ここで追加する。 **例 :** <property name="notRecordedMethods"> <method>getLastCommandOutputBytes</method> </property>
NtcmdAgentRetention	NTCMD エージェントのリテンション・モード。接続を閉じるときの、リモート NTCMD サービスとその実行可能ファイルの処理方法を指定する。 • **0**（標準設定）**:** サービスを登録解除し、リモートの実行可能ファイルを削除する。 • **1 :**サービスを登録解除しますが、実行可能ファイルをファイル・システムに残す。 • **2 :**サービスを実行中のままにし、実行可能ファイルを残す。
NtcmdSessionUseProcessBuilder	このパラメータは **NtcmdSessionAgent** に使用し、常に **true** で

パラメータ	説明
	ある必要がある。このパラメータで、新規プロセスの作成方法を指定する。 • **true :**新規プロセスは ProcessBuilder により作成される（Java 5.0 からの新 API）。 • **false :**新規プロセスは Runtime.exec により作成される（Java 1.4.2 からの旧 API）。後方互換性の問題がある場合にのみ、false に設定する。
objectSendAmountThreshold	検出されたオブジェクト数がこのしきい値を超過すると、オブジェクトはサーバにただちに送信される。jython スクリプトに sendObject(s) API を使用する必要がある。 **標準設定 :**2000 オブジェクト
objectSendTimeThreshold	前回のオブジェクト・レポートから指定された時間（秒）が経過すると、オブジェクトはサーバにただちに送信される。jython スクリプトに 0sendObject(s) API を使用する必要がある。 **標準設定** :300 秒
pingClientTypeIp	（**Inventory Discovery by Scanner** ジョブ専用）クライアント IP アドレスの ping を許可するかどうかを示す。 **標準設定 :** false
pingHostName	（**Inventory Discovery by Scanner** ジョブ専用）ホスト名の ping を許可するかどうかを示す。 **標準設定 :** false
portExpirationTime	プローブのデータベースでの TCP / UDP ポート・エントリの有効期限（秒）。 **標準設定 :**60 秒
powershellConnectionIdleTimeout	powershellconnector.exe プロセスの最大アイドル時間（ミリ秒）を定義する。 コマンドが実行されるたびに、タイマーの状態はリセットされる。 **標準設定 :**3600000 ミリ秒（1 時間）
processExpirationTime	プローブのデータベースでのプロセス・エントリの有効期限（秒）。

パラメータ	説明
	標準設定 :60 秒
protocolConnectionOrder	**Host Connection by Shell** ジョブのプロトコル接続順序。 **標準設定:** ssh、telnet、ntadmin
remoteProcessTimeout	起動後、リモート・プロセスは定義された時間（ミリ秒）以内にプローブに接続する必要がある。接続できない場合、**リモート プロセスに接続できませんでした**というエラーが発生する。 **標準設定 :**300000 ミリ秒（5 分）
removeCopiedFiles	場合によっては、クライアント・マシンのスクリプトとサードパーティ製ユーティリティが DFM によってコピーされる。**removeCopiedFiles** パラメータで、ディスカバリの完了後にこれらのファイルを削除する必要がある（true）か、ない（false）かを定義する。
reportPhysicalSerialNumbers	スキャン・ファイルの **hwsmbiosPhysicalAttributeSerialNumber** から物理シリアル番号を報告するかどうかを示す。 **標準設定 :** false
ResultProcessIsLenient	**true** に設定すると、ディスカバリ結果の処理はゆるやかになる（非推奨）: • 報告される文字列属性に大きすぎる値が設定されている場合、CMDB クラス・モデル定義に応じて、文字列は自動的に切り詰められる。 • OSH 属性が無効な場合（タイプ / 存在しない属性 / ID 属性が存在しない）、バルク全体ではなく無効な OSH のみが削除される（標準設定はバルク全体が削除される）。 **標準設定 :** false
setBiosUuidToMicrosoftStandart	Windows オペレーティング・システムの BIOS UUID 値を、本来の BIOS 値ではなく Microsoft スタイル（一部のバイト・オーダーが逆）で報告するかどうかを示す。Host Connection ジョブに影響する。 • **false**（標準設定）**:**本来の BIOS 格納値に変換する • **true :**Microsoft 標準に変換する。

パラメータ	説明
	注: このパラメータを **true** に設定すると、VMware ジョブまたはその他の統合により検出された BIOS UUID 値との競合が発生する場合がある。
shellGlobalBandwidthLimit	ディスカバリ・ノードとの間でファイルをアップロード、およびダウンロードするための最大バンド幅（キロビット / 秒）。 **注:** 値が設定されていないか、0 が設定されている場合、使用可能なバンド幅すべてが使用される。
shellGlobalCommandTimeout	すべてのシェル・クライアント・コマンドのグローバル・タイムアウト（ミリ秒）。コマンドの結果の待機時間を示す。 **標準設定 :**15000 ミリ秒
siebelCommandTimeout	Siebel コマンドの結果の待機時間。 **標準設定 :**3 分（180000 ミリ秒）
snmpGlobalRequestTimeout	SNMP を使用した要求がタイムアウトする時間（ミリ秒）。 **標準設定 :**3,000 ミリ秒 **注:** この値はすべての SNMP 要求に対するグローバル値である。特定クエリ（クエリが標準設定のタイムアウトよりも長い時間を要する）の SNMP 要求のタイムアウトを上書きする場合、次のように SNMP クライアントの executeQuery メソッドに 2 番目のパラメータとしてタイムアウト値を入力する。**snmpClient.executeQuery (SNMP_QUERY_STRING, QUERY_TIMEOUT_IN_MILLISECONDS)**
snmpTestQueries	SNMP エージェントのための標準設定の SNMP テスト・クエリを定義する。特定デバイス用に上書きできる。 **標準設定 :** <property name="snmpTestQueries"> <query> 1.3.6.1.2.1.1.1,1.3.6.1.2.1.1.2, string</query>

パラメータ	説明
	</property>
ssh-log-level	SSH ログ・レベル。 **レベル :**1-7。7 がもっとも詳細な検出レベル。
tcpExpirationTime	プローブのデータベースでの TCP 接続エントリの有効期限（時間）。 **標準設定 :**24 時間
timeToSleepWhenMaximumConnectionsLimitReached	新しい接続を作成できるようになるまでジョブが待機する必要がある時間（ミリ秒）を決定する（上記 "maximumConnectionsPerSecond"を参照）。 **標準設定 :**1000 ミリ秒（1 秒） **注: maximumConnectionsPerSecond = 0** の場合、このプロパティは無視される。
tnsnamesFilePaths	**tnsnames.ora** ファイルを検索するパス（**tnsnames.ora** 自体を含む（カンマ区切り）） **例 :** <property name= "tnsnamesFilePaths"> c:\temp\tnsnames.ora </property>
useIntermediateFileForWmic	wmic コマンドによるデータ転送に中間一時ファイルを使用するかどうか。 **標準設定 :** false
useJinteropOnWindows	このプロパティは、Windows マシンで使用される。 • **true :**プローブは WMI 検出に JInterop を使用する。 • **false**（標準設定）**:** プローブは WMIdll ネイティブ・コードを使用する。
useNtcmdModifiedMarkers	• **true :**プローブは、NTCMD エージェントのインフラストラクチャにカウンタ付きマーカーを使用する。 • **false**（標準設定）**:**プローブは、古い NTCMD の動作を採用する（カウンタ付きマーカーは使用しない）。

パラメータ	説明
useWinexeOnLinux	この設定は、非 Windows マシンで使用される。 • **true :**プローブは、NTCMD Windows ディスカバリにローカルの winexe 実行可能ファイルを使用する。 • **false**（標準設定）**:** プローブは Windows リモート・プロキシを使用する。

portNumberToPortName.xml ファイル

portNumberToPortName.xml ファイルは、DFM により辞書として使用され、ポート番号を意味のあるポート名にマップすることにより、IpServiceEndpoint CI を作成します。ポートが検出されると、プローブはポート番号を抽出し、このポート番号に対応するポート名があるか **portNumberToPortName.xml** ファイルを検索し、この名前が設定された IpServiceEndpoint CI を作成します。このファイルにポート名が存在しない場合、ポート番号がポート名として使用されます。

同じポート番号に対して、IP 範囲ごとに別の名前を指定できます。この場合、同じポートでも含まれる IP 範囲に応じて異なるポート名が設定されます。

> **注: portNumber** 属性には、数値または範囲を指定できます。範囲はカンマ、ダッシュ、またはその両方で区切られる。例 :"10, 21, 45"、"10-21"、または "10-21, 45, 110"。数値の任意の位置にワイルドカードとして x を使用できます。たとえば、 “5xx00” には、ポート 50000、50100、50200、…51000、51100、51200、…59900 が含まれます。

検出対象とする新規ポートの追加の詳細については、「新しいポートの定義方法」(5ページ)を参照してください。

第7章: 追加のプロトコル情報

本項の内容

拡張されたシェル・インタフェース

UCMDB 10.00 では、シェル・インタフェースが拡張され、Windows マシンとの間でファイルをアップロード、またはダウンロードする場合の制約がなくなりました。これにより、さらに多くの機能が NTCMD と SSH プロトコル、および UD エージェントに適用されるようになりました。

Windows マシンとの間でファイルをアップロード、またはダウンロードするとき、**setBandwidthLimit** パラメータを使用して、ネットワークのバンド幅の消費量を制限できます。

このパラメータは **globalSettings.xml** で設定できます。

プロパティは **shellGlobalBandwidthLimit** です。ファイルのダウンロードおよびアップロードをサポートするシェル・オブジェクトで、ダウンロードまたはアップロード操作で消費されるバンド幅量の上限を設定します（キロビット / 秒）。この値は正の整数である必要があります。標準設定は、上限なしを意味する 0 です。例 :

```
<property name="shellGlobalBandwidthLimit">0</property>
```

速度は、アダプタ・レベルまたはジョブ・レベルで上書きできます（UD エージェントのインストール時、更新時など）。

公開鍵 / 秘密鍵ペアに基づく SSH 接続の作成方法

公開鍵 / 秘密鍵のペアに基づき Secure Shell（SSH）接続を作成するには、次の手順を実行します。

1. （プローブ・マシン上の）Mindterm コンソールを開き、コマンド・ラインから次のコマンドを実行します。

   C:\hp\UCMDB\DataFlowProbe\bin\jre\bin\java.exe -jar
   C:\hp\UCMDB\DataFlowProbe\content\lib\Mindterm.jar

2. Mindterm コンソールで、［**File**］ > ［**Create Keypair**］に移動して、次の値を割り当てます。

   - **Key type/format:** DSA または RSA を選択します
   - **Key length:**
     - **Key type/format = DSA の場合 :** 1024 を選択します
     - **Key type/format = RSA の場合 :** 次のいずれかを選択します。768、1024、1536、2048、4096、8192、16384、または 32768
   - **Identity file:** 名前を割り当てます（標準設定の名前は **identity**）
   - **Password:** パスワードなしの場合は、何も入力しません

   注意: ［**OpenSSH .pub format**］オプションを選択する必要があります。

3. ［**Generate**］をクリックして、マウスを動かして公開鍵 / 秘密鍵を生成します。

4. ペアが生成されたら、**C:\Users\ < ユーザ名 > \AppData\Roaming\MindTerm** に移動します。このディレクトリには、生成された公開鍵 / 秘密鍵のペアが格納されます。公開鍵は、拡張子 **.pub** を伴います。

5. 次のように、接続先とするリモートの Linux / Unix マシンに **.pub** ファイルの内容をコピーします。

   a. Linux / Unix リモート・マシンに接続して、**~/.ssh/authorized_keys** ファイルを探します（ファイルが存在しない場合は作成します）。

   b. ファイルを開いて、次のように編集します。

      vi ~/.ssh/authorized_keys

   c. **authorized_keys** ファイルに **.pub** ファイルの内容を追加します。

   d. **.pub** ファイルの内容の最後に、 < ユーザ名 > @ < プローブ IP > を追加します。たとえ

ば、**.pub** ファイルの内容が次であるとします。

ssh-dss AAAAB3N.....<snippet>.....r2LnQrqhncpJyL1s0id76j6wA==

また、プローブの IP が 16.59.56.255 で、接続に使用するユーザ名が **root** である場合、**~/.ssh/authorized_keys** ファイルの内容に次の記述を追加します。

ssh-dss AAAAB3N.....<snippet>.....r2LnQrqhncpJyL1s0id76j6wA== root@16.59.56.255

e. **~/.ssh/authorized_keys** ファイルを保存して、閉じます。

6. UCMDB を開き、［**データ フロー管理**］ > ［**Data Flow Probe 設定**］ > ［**資格情報**］ > ［**SSH プロトコル**］に移動します。

7. 次のパラメータが設定された新しい SSH プロトコルを追加します。

   - **認証方法 :** publickey
   - **ユーザ名 :** root
   - **キー・ファイル・パス :** C:\\Users\\ < ユーザ名 > \\AppData\\Roaming\\MindTerm\\ < ID ファイル > （ < ID ファイル > は、手順 2 で入力した名前です）。
   - **パスワード :** 公開鍵 / 秘密鍵のペアの作成時にパスワードを入力した場合、ここにも同じパスワードを入力する必要があります。

AES256-CBC および AES256-CTR 暗号化アルゴリズムのサポートを有効にする方法

AES256-CBC および AES256-CTR 暗号化アルゴリズムのサポートを有効にするには、次の手順を実行します。

1. UCMDB サーバと Data Flow Probe サービスを停止します。

2. http://www.oracle.com/technetwork/java/embedded/embedded-se/downloads/jce-7-download-432124.html から **UnlimitedJCEPolicyJDK7.zip** ファイルをダウンロードします。

3. ZIP パッケージを展開します。

4. **local_policy.jar** と **US_export_policy.jar** ファイルを **< DataFlowProbe インストール・フォルダ**

> \bin\jre\lib\security ディレクトリにコピーし、古いファイルを置換します。

5. UCMDB サーバと Data Flow Probe サービスを起動します。

第8章: サポート対象の Unix シェル

UCMDB では、次の Unix シェルの使用がサポートされます。

- bash
- csh
- ksh
- tcsh

第9章: トラブルシューティングおよび制限事項

本項では、Universal Discovery を使用したディスカバリの実行に関連する一般的なトラブルシューティングと制限事項について説明します。

- **問題** :UAC が有効になった Windows Vista / 2008-R2 マシンに接続できない

  理由 : Windows Vista 以降、Microsoft は UAC （User Account Control）技術を導入することで、セキュリティ・メカニズムを変更しています。この変更により、ローカルの管理者アカウントを使用する場合、HPCmd でリモートの Windows Vista / 2008-R2 マシンとの接続に問題が発生します。

  解決策 :次の手順を実行して、UAC が有効になったリモートの Windows Vista / 2008-R2 マシンとの HPCmd での接続を有効にします。

  a. HPCmd 接続の確認

     i. プローブ・マシンにログオンします。

     ii. hp\UCMDB\DataFlowProbe\tools ディレクトリで **HPCmd.bat** ファイルを見つけます。

     iii. 同じディレクトリで、**cmd.com** を開きます。

     iv. コマンド・プロンプトで次のコマンドを呼び出します。

     ```
     HPCmd.bat \\<問題のあるマシンの名前または IP> /USER:<ドメイン>\<ユーザ名>
     /PWD:<パスワード>
     ```

  b. HPCmd 接続が成功しない場合、共有フォルダ admin$ にアクセス可能か確認します。

     プローブ・マシンからリモート・マシン上の共有フォルダ **admin$** にアクセスできるか確認します。

     i. プローブ・マシンにログオンします。

     ii. ［**スタート**］ > ［**ファイル名を指定して実行**］を選択して、\\<リモート・マシン名>\admin$ アドレス を入力します。

     iii. **admin$** にアクセスできない場合、次を実行します。

- リモート・マシンにログオンします。
- ［**スタート**］ > ［**ファイル名を指定して実行**］を選択して、regedit を入力します。
- 次のレジストリ・サブキーを見つけます。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
LanmanServer\Parameters
```

- ［**Parameters**］をクリックします。
- **AutoShareServer** レジストリ・エントリが存在しない場合、［**編集**］メニューで［**新規**］ > ［**DWORD (32 ビット) 値**］を選択します。**AutoShareServer** を入力し、［**OK**］をクリックします。
- ［**AutoShareServer**］を選択します。［**編集**］メニューで［**修正**］を選択し、［**値のデータ**］ボックスに 1 を入力します。
- レジストリ・エディタを終了し、コンピュータを再起動します。
- ［**スタート**］ > ［**ファイル名を指定して実行**］を選択して、net start srvnet を入力します。

iv. **admin$** へのアクセスが成功したら、「HPCmd 接続の確認」(38ページ) で説明されているように、HPCmd 接続の確認を再度試行します。

c. 依然として確認に失敗する場合、UAC が有効になった Windows Vista / 2008-R2 マシンに接続します。

i. Windows Vista / 2008-R2 マシンでは、リモートで接続してもローカル管理者にすべての権限はありません。

この問題を解決するには、次のオプションのいずれかを使用します。

- ドメイン管理者資格情報を使用して接続します。
- 次のように、リモート・マシンのレジストリを修正して、ローカル管理者がすべての権限を持てるようにします。

キー	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system

値	LocalAccountTokenFilterPolicy を 1 に設定します。 この値がない場合は、新規に DWORD 値を作成し、1 に設定します。

ii. マシンを再起動します。

- **問題 :** リモートの Linux / UNIX / Mac OS X マシンと通信をすると、ファイル転送が機能せず、スキャナベースのインベントリ・ディスカバリや Universal Discovery エージェントのデプロイなどの操作が失敗します。

  解決策 :

  a. SSH エージェントが SCP / SFTP プロトコルでファイル転送できるように設定されているか確認します。

  b. SSH プロトコルで使用されるユーザのログオン・プロセスに、ログオン・プロセス時に手動のユーザ入力が必要なバナーがないか確認します。

ドキュメントのフィードバックを送信

本ドキュメントについてのご意見、ご感想については、電子メールでドキュメント制作チームまでご連絡ください。このシステムで電子メールクライアントが設定されていれば、このリンクをクリックすることで、以下の情報が件名に記入された電子メールウィンドウが開きます。

『ディスカバリ / インテグレーション・コンテンツ・ガイド - 全般的な参照情報』 (Universal CMDB コンテンツ・パック 16.00（CP16）) に関するフィードバック

本文にご意見、ご感想を記入の上、[送信] をクリックしてください。

電子メールクライアントが利用できない場合は、上記の情報をコピーしてWebメールクライアントの新規メッセージに貼り付け、cms-doc@hp.com 宛にお送りください。

お客様からのご意見、ご感想をお待ちしています。