IBM® Technical Support Appliance
構成アシスタント・ガイド

バージョン 2.7.0.0

2020 年 8 月

目次

概要 3

プレディスカバリーのネットワークの考慮事項 3
役立つ資料 4

概要 5

スコープ・セットの定義 5
スコープの作成時に考慮すべき事項 7
ディスカバリー資格情報 8
ディスカバリー資格情報のセットアップ時に考慮すべき事柄 9

はじめに 10

TSA の初期セットアップと構成 10
ディスカバリーの準備 10
ディスカバリーのステップ 10

デバイスのディスカバリーの構成 13

オペレーティング・システムおよびホスト 13
IBM Power Systems 14
ハードウェア管理コンソール (HMC) 15
Integrated Virtualization Manager (IVM) 16
仮想 I/O サーバー (VIOS) 区画 16
AIX 16
Linux on Power 18
IBM i 20
UNIX システム 22
Solaris 22
Solaris (Oracle iLOM を使用) 23
Linux 23
HP-UX 24
VMware vCenter Server および VMware ESXi 25
Windows 27
Windows (WINRM を使用) 27
Windows (SMB1 を使用) 29
ATM デバイス 32
管理モジュール 32
Flex System Manager (FSM) デバイス 32

シャーシ管理モジュール (CMM) デバイス 32
拡張管理モジュール (AMM) デバイス 33
HP Proliant ブレード・サーバー (HP OnBoard Administrator を使用) 33
統合管理モジュール (IMM) および統合管理モジュール II (IMM2) デバイス 34
HP Integrity および HP9000 サーバー (iLO を使用) 34
ネットワーク・デバイス 34
BNT スイッチ 35
Brocade 35
Check Point 35
Cisco 36
F5 Big-IP (TMOS) 36
Fortinet (FortiOS) 37
IBM b タイプのストレージ・エリア・ネットワーク (SAN) スイッチ 37
Juniper 37
Palo Alto Networks (PAN-OS) 38
QLogic スイッチ 38
ストレージ・デバイス 38
EMC Corporation のストレージ 39
HP StorageWorks P2000 Modular Smart Array 40
IBM DS3xxx、DS4xxx、または DS5xxx ストレージ 41
IBM DS6xxx / DS8xxx ストレージ 41
IBM FlashSystem、v9000 41
IBM ProtecTIER 42
IBM SVC、V7000/V3700 ストレージ 42
IBM TS3100 テープ・ライブラリー 42
IBM TS3200 テープ・ライブラリー 43
IBM TS3310 テープ・ライブラリー 43
IBM TS3494、TS3953 テープ・ライブラリー 43
IBM TS3500、TS3584 テープ・ライブラリー 43
IBM TS4500 テープ・ライブラリー 44
IBM TS7700 テープ・ライブラリー 45
IBM V7000 Unified ストレージ 45
IBM XIV ストレージ 45
nSeries または NetApp ストレージ 46
ファイアウォールの考慮事項 47
ディスカバリーの問題 51
継続的に対応すべき考慮事項 52

トラブルシューティング 53

AMM Discovery のアクティブ・セッション 53

付録 A: 用語および定義 54

付録 B: その他の項目 55

ユーザー・インターフェースのダウンロード機能 55

付録 C: VMware ESXi の CIM プロバイダー 56

付録 D: WINRM を使用する Windows 60

概要

IBM Technical Support Appliance (TSA) は、IBM サポート契約を最大限に活用するための使いやすいツールです。TSA は、ご使用の IT インフラストラクチャーから重要な情報技術要素やそれらの関係性を検出し、そのデータを分析するために安全に IBM サポートに転送します。IBM サポートはこのデータから、お客様のデータ・センター内のサーバーやネットワーク・コンポーネント間の複雑な関係についての知見を得ることができます。

本資料は、TSA のインストール、計画、および構成に役立つ情報とガイダンスを提供する目的で作成されました。

プレディスカバリーのネットワークの考慮事項

初めてのディスカバリーおよび送信のために TSA を構成する前に、次の事項が対処済みであることを確認してください。本資料の説明は、TSA がインストール済みで、Web インターフェースがアクセス可能であり、TSA が最新レベルに更新されていることを前提としています。そうなっていない場合は、「Technical Support Appliance セットアップ・ガイド」(本資料のこれ以降の箇所では「セットアップ・ガイド」と呼びます) を参照してください。

TSA プレディスカバリーのネットワークの考慮事項	
ネットワーキング	
	TSA から IBM へのファイアウォール・アクセスを開きます。セットアップ・ガイドの**『IBM サポートに接続するための構成要件』**のセクションを参照してください。
	IBM への接続に SSL プロキシーが使用されている場合、それが TSA で構成済みであることを確認してください。セットアップ・ガイドの**『IBM への接続』**のセクションを参照してください。 SSL インスペクションはサポートされていません。プロキシーで SSL インスペクションを使用している場合、この一連の操作では無効にしてください。
	TSA とターゲット・デバイスの間にファイアウォールが存在する場合、必要なポートが開いていることを確認してください。詳しくは、『ファイアウォールの考慮事項』(47 ページ) を参照してください。

役立つ資料

以下のリンクを使用すると、Technical Support Appliance に関する Web サイトにすぐに移動できます。IBM Technical Support Appliance を使用して作業を開始するうえで必要なすべての情報を参照できます。ibm.com からセットアップ・ガイドやセキュリティーに関する資料にアクセスしたり、サンプル・レポートを表示したり、Technical Support Appliance インストール・コードをダウンロードしたりできます。

Technical Support Appliance について詳しくは、https://ibm.biz/TSAdemo を参照してください。

概要

TSA は、導入済みのオペレーティング・システム・コンポーネント、ファームウェア・コンポーネント、物理サーバー、ネットワーク・デバイス、仮想 LAN といった、ご使用の IT インフラストラクチャーに関する情報をディスカバーします。収集する情報の範囲と詳細度を最適化するには、TSA 内でディスカバリー・デバイスを識別するための構成タスクを行う必要があります。

TSA は、お客様のネットワーク環境への影響を可能な限り小さくすることを試みます。そのために、ディスカバリー・プロセスでは反復と、よく計算されたアプローチが採用されています。このアプローチでフル・ディスカバリーにかかる時間は最長で 72 時間です。ディスカバリー・ジョブの状況は、**「要約」**パネルの**「ジョブの要約」**セクションを表示してモニターできます。

ディスカバリー・プロセスの一環で、TSA はまず、資格情報を使用せずに、定義済みのスコープ内でデバイスの検出を試みます。これには、低干渉の IP スキャン、スタックの指紋照合、およびポート・マッピングによる、Nmap を使用したデバイスのディスカバーと分類が含まれます。一般に、このアクティビティーは侵入検知システム (IDS) を作動させるほどのものではありませんが、ローカル設定が厳重である場合は作動させることがあります。

TSA が IT インフラストラクチャーに関する情報を収集するようにするには、TSA に以下の情報を提供します。

- スコープ
- アクセス資格情報

スコープ・セットの定義

スコープ・セットは、個々のスコープを論理的なグループにまとめたものです。スコープは IP アドレスを使用して、環境のディスカバーを開始する場所を TSA に伝えます。スコープ・セットは、1 つ以上のスコープから構成されます。スコープの項目には次の 3 つのタイプがあります。

- サブネット - IP アドレスとサブネット・マスクによって定義されます。サブネットはクラス C サブネットに制限されています。
- IP 範囲 - 開始と終了の間のすべての IP アドレスが含まれます。
- IP アドレス / ホスト - 個々の IP アドレスまたはホスト名。

- ホスト名は、ディスカバリー時ではなく、入力時に解決されます。詳細については、『スコープの作成時に考慮すべき事項』(7 ページ) を参照してください。

必要な場合、あるスコープについて、ホスト、範囲、またはサブネット定義を指定してスコープ除外を定義することができます。その結果に含まれる IP アドレスは、そのスコープの一部とみなされず、スキャンはされません。

TSA では、次の 3 つのタイプのスコープ・セットがサポートされています。

1. **一般スコープ・セット**: 個別の IT ネットワーク・エレメントをディスカバーできます。このスコープ・セットには、IP アドレス、IP アドレスの範囲、またはネットワークあるいはサブネットを使用してこれらのネットワーク・エレメントの場所を特定する 1 つ以上のスコープが含まれます。
2. **HMC 動的スコープ・セット**: 1 つ以上の IBM POWER Systems HMC の IP アドレスおよび関連する資格情報を指定できます。また、HMC が管理するすべての LPAR に関する情報も、LPAR の IP アドレスを識別せずに収集できます。動的スコープ・セットでは、これらの LPAR に正常にアクセスするためにユーザーが提供する資格情報を使用します。
3. **VMware 動的スコープ・セット**: 1 つ以上の VMware vCenter Server または ESXi のインスタンスの IP アドレス、および関連する資格情報を指定できます。また、VMware が管理するすべての仮想マシンに関する情報も、仮想マシンの IP アドレスを識別せずに収集できます。動的スコープ・セットでは、これらの仮想マシンに正常にアクセスするためにユーザーが提供する資格情報を使用します。

HMC および VMware vCenter Server / ESXi の場合、動的スコープ・セットの使用をお勧めします。動的スコープ・セットでは、個別の LPAR/仮想マシンのディスカバリー・スコープを作成および管理する場合と比べ、TSA で行う構成にかける労力が少なくて済みます。また、LPAR または仮想マシンを時間の経過とともに追加したり削除したりする環境では、動的スコープ・セットによって、スコープ・セットを変更することなくこうした状況に対応できます。

TSA でディスカバリー・スコープを定義するための詳細な手順は、セットアップ・ガイドの『**ディスカバリー・スコープの設定**』セクションを参照してください。

スコープの作成時に考慮すべき事項

スコープのセットアップには、標準として定義されている方法はありませんが、時間と労力の節約になるいくつかの考慮事項があります。

- 可能な場合には、動的スコープ・セットを使用して、HMC とその管理対象 LPAR、または VMware vCenter Server / ESXi およびその管理対象仮想マシンのディスカバリーを定義します。動的スコープ・セットを使用すると、LPAR または仮想マシンのスコープを定義する必要はありません。
- 複数のデバイスをディスカバーするには、個々の IP アドレスやホスト名ではなく 、IP 範囲やサブネット・スコープを使用します。そのようにすれば、スコープ定義の数が制限され、管理が容易になります。
- サブネット・スコープ定義を使用する場合、スコープ・セットごとに 1 つのみ含めてください。サブネット・スコープ定義が、クラス C ネットワーク (256 IP アドレス) 以下に解決するようにしてください。
- 「**一般スコープ・セットのインポート**」機能を使用して、指定した名前と入力テキスト・ファイルにある IP アドレスのリストに基づいて新しいスコープ・セットを作成します。詳しい手順については、セットアップ・ガイドの『**ディスカバリー・スコープ**』→『**一般スコープ・セットのインポート**』セクションを参照してください。
- 現時点では TSA は IP アドレスのみを保管します。これは、ホスト名がディスカバリー時ではなく入力時に解決されることを意味します。ベスト・プラクティスとしては、ホスト名ではなく IP アドレスまたは IP 範囲を使用してスコープを定義することをお勧めします。
- スコープ・セットに含まれる IP アドレスの数が多くなるほど、ディスカバリーにかかる時間は長くなります。ディスカバリーにかかる時間を最小限にするには、検出したい要素のみが対象となるようにスコープを設定してください。

一般スコープ・セットを使用する場合、スコープ・セットの解決結果の (範囲またはサブネットのスコープ定義を拡張した後の) IP アドレスの累積数を 400 以下に制限します。単一のスコープ・セットで 400 を超える IP アドレスがスキャン

されると、ディスカバリー・プロセス中にパフォーマンス、サーバーまたはネットワークに関する問題が発生する可能性があります。

- TSA では、複数のスコープ・セットで IP アドレスを定義することは不可能ではありません。しかし、これは通常は避けるべきです。そのようにしても、ディスカバリーにかかる時間が長くなるだけで、何か追加の情報を収集できるわけではないからです。
- 次のようにスコープをスコープ・セットにグループ化して、デバイスの論理グループを作成します。
  - 同一のデバイス・タイプを 1 つのスコープ・セットに入れてグループ化します。例えば、IBM FlashSystem ストレージ・サブシステム用のスコープ・セットを作成します。
  - 同じジオグラフィーにあるデバイスをグループ化します。
  - ビジネス・アプリケーションまたはサービスに基づいてデバイスをグループ化します。

ディスカバリー資格情報

いくつかの例外を除き、ディスカバリーを実行するには、ご使用の環境を十分に理解するために必要な詳細情報を取得するために、一定のレベルのアクセス権が必要になります。

普通は、TSA が使用するためのサービス・アカウントをディスカバリー・デバイス上に作成する必要があります。プラットフォーム・タイプごとに必要な具体的なアクセス権限については、以下のセクションを参照してください。これらのサービス・アカウントの管理をシンプルにするには、特定の製品ファミリーのすべてのデバイスで同じユーザー名を使用します。

TSA がデバイスに接続するために使用するサービス・アカウントを保守するタスクは、以下のいずれかの方法を使用してシンプルにできます。

- 有効期限のないパスワードが設定されたサービス・アカウントを作成する
- SSH 鍵の使用がサポートされているデバイス製品ファミリーでは SSH 鍵を使用する

アプライアンスのアクセス資格情報を定義する方法について詳しくは、セットアップ・ガイドの**『ディスカバリー資格情報の設定』**のセクションを参照してください。

ディスカバリー資格情報のセットアップ時に考慮すべき事柄

アプライアンスは、資格情報をアクセス・リストに掲載されている順序で使用しようとします。ディスカバリーのスピードを上げるには、資格情報が環境に最適な順序でリストされていることを確認してください。以下にいくつかの考慮事項を挙げます。

- 必要に応じて、資格情報を特定のスコープ・セットに制限します。これにより、不必要なログインの試行が制限され、ディスカバリーのパフォーマンスが向上します。
- SSH 鍵は以下のデバイスのディスカバリーに使用できます。
  - AIX
  - Cisco
  - Linux
  - HMC
  - IBM i
  - IVM
  - Sun SPARC (Solaris)
  - SVC / V7000
  - VIOS
  - Fortinet
  - HP-UX
  - IBM FlashSystem
  - F5 BIG-IP
  - Check Point

1 つのスコープ・セットにリンク付けできる SSH 鍵資格情報は 1 つのみです。

- TSA 専用の個別のサービス・アカウントを作成して、必要最低限の権限を付与するのがベスト・プラクティスです。

はじめに

このセクションでは、TSA の構成のベスト・プラクティスや推奨事項をいくつか紹介します。

TSA の初期セットアップと構成

セットアップ・ガイドの以下のセクションの説明を参照してください。

- Technical Support Appliance のインストール
- Technical Support Appliance へのログイン
- ご使用条件への同意
- セットアップ・ウィザードによる Technical Support Appliance のセットアップ

ディスカバリーの準備

反復的なプロセスで行うことが推奨されています。最初はネットワークのごく一部をディスカバリーの対象として構成し、回を重ねるごとに対象にするネットワークのセクションを拡大していき、最終的には、必要なネットワークのすべてのセクションがカバーされるようにすることをお勧めします。

ベスト・プラクティスとして、スコープや資格情報に大規模な追加や変更を行った後は、TSA 構成のバックアップを保存してください。詳しくは、「IBM Technical Support Appliance セットアップ・ガイド」の『バックアップとリストア』セクションを参照してください。

ディスカバリーの手順

ディスカバリーの反復ごとに、以下の手順を実行します。

1. ディスカバリーの対象のデバイスを準備します。必要なデバイスと資格情報構成の要件については、『デバイスのディスカバリーの構成』(13 ページ) を参照してください。
2. HMC 動的スコープ・セットの場合、以下の手順を実行します。
   a. 「**HMC 動的スコープ・セット**」ページで HMC の IP アドレスを追加します。
   b. 「**HMC 動的スコープ・セット**」ページで HMC の資格情報を追加します。

c. ディスカバーする LPAR タイプを選択します。各タイプに関して資格情報を指定します。

> 動的スコープ・セットの作成時にディスカバーする LPAR タイプを選択することもできます。また、後ほど反復する際に動的スコープ・セットを編集することにより LPAR タイプを追加することもできます。

d. (オプション)「**HMC 動的スコープ・セット**」ページのテスト機能を使用して、資格情報が正しく定義され、HMC または LPAR との接続を確立するために使用できることを検証します。

3. VMWare 動的スコープ・セットの場合、以下の手順を実行します。

a. VMware vCenter Server の IP アドレスを追加します。

b. VMware vCenter Server で管理していない VMware ESXi ホストの IP アドレスを追加します。

c. 「**VMware 動的スコープ・セット**」ページで、VMware vCenter Server および ESXi のインスタンスの資格情報を追加します。

d. ディスカバーする仮想マシンのタイプを選択します。各タイプに関して資格情報を指定します。

> 動的スコープ・セットの作成時にディスカバーする仮想マシンのタイプを選択することもできます。また、後ほど反復する際に動的スコープ・セットを編集することにより仮想マシンのタイプを追加することもできます。

e. (オプション)「**VMware 動的スコープ・セット**」ページのテスト機能を使用して、資格情報が正しく定義され、VMware vCenter Server および ESXi のインスタンス、さらにはその仮想マシンとの接続を確立するために使用できることを検証します。

4. 一般ディスカバリー・スコープの場合、以下の手順を実行します。

a. 望ましい IP アドレスを、適切なスコープ・セット/スコープに追加します。TSA インスタンスとディスカバリー対象のデバイスの間にファイアウォールがある場合、ディスカバリーを正常に行うためにファイアウォールの適切なポートが開いていることを確認してください。プラットフォーム・タイプごとの、アクセス可能にする必要のあるポートについては、『ファイアウォールの考慮事項』(47 ページ) を参照してください。

b. 必要な資格情報を作成します。「**新規ディスカバリー資格情報**」パネルのテスト機能を使用して、資格情報が適切に定義されていることと、ターゲット・デバイスとの接続を確立するために使用可能かどうかを確認します。

5. この反復に追加された IP アドレスをスキャンするために、フル・ディスカバリーを実行します。
6. 伝送を実行してデータを IBM にアップロードします。

デバイスのディスカバリーの構成

TSA が効率的にディスカバーを行い、コンポーネントに関する有用な情報を収集するためには、資格情報を指定することに加えて、特定のディスカバリー・デバイス構成の前提要件を満たすことが必要になる場合があります。このセクションには、環境内のディスカバリー・デバイスに固有の構成が必要かどうかを判断するための情報を記載します。必要最小限の権限を付与したサービス・アカウントを作成することをお勧めします。ポートとプロトコルについては、『ファイアウォールの考慮事項』セクションも参照してください。

SSH と Telnet の両方のポートが開いているデバイスでは、(セキュリティー上の理由から) TSA はまず SSH を使用して接続を試行します。この SSH 接続が失敗すると、TSA は次に Telnet を使用した接続を試行します。

オペレーティング・システムとホスト

プラットフォーム
IBM Power Systems • ハードウェア管理コンソール (HMC) • Integrated Virtualization Manager (IVM) • 仮想 I/O サーバー (VIOS) 区画 • AIX • Linux on Power
IBM i
UNIX システム • Solaris • Solaris (iLOM を使用) • Linux • HP-UX
VMware vCenter Server および VMware ESXi
Windows

ATM デバイス
管理モジュール • Flex System Manager (FSM) • シャーシ管理モジュール (CMM) • 拡張管理モジュール (AMM) • HP ProLiant ブレード・サーバー (HP OnBoard Administrator を使用) • 統合管理モジュール (IMM および IMM2) • HP Integrity および HP9000 サーバー (iLO を使用)
詳細情報については、上記の各リンクをクリックしてください。

IBM Power Systems

IBM Power systems では、LPAR の構成が HMC または IVM によって管理されるので、HMC 動的スコープ・セットを使用します。HMC 動的スコープ・セットでは、HMC のスコープ定義を作成し、関連する HMC および LPAR の資格情報を指定しますが、管理対象の各 LPAR に対してスコープを作成する必要はありません。HMC がディスカバーされると、TSA はその時点で存在する LPAR を判別し、各 LPAR を自動的にスキャンします。

LPAR の構成が静的である IBM Power Systems では、HMC 動的スコープ・セットに代わる方法として、エンティティーのスコープと資格情報を次の順序で追加して反復します。

1. **HMC または IVM インスタンス**: HMC は、管理対象のすべての Power Systems と、そこに含まれる論理区画に関する概要情報を戻します。IVM は、管理対象の単一のシステムに関する同様の情報を戻します。
2. **VIOS 区画**: これは、これらの区画が所有する物理アダプターやリソースに関する情報を戻します。
3. **個々の区画**: VIOS 以外の区画が物理アダプターを所有する場合もあります。

ハードウェア管理コンソール (HMC)

HMC インスタンスをディスカバーするには、以下の手順を実行します。

環境の準備:

- TSA が HMC を通じて LPAR の管理に関する情報を収集できるようにするには、HMC が RMC ツールを使用して LPAR と通信できる必要があります。HMC および LPAR が、この通信を許容するように構成されていることを確認してください。Linux 向けの RMC ツールについて詳しくは、https://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/yum.html を参照してください。
- データ収集を安全に行うには、HMC でリモート・コマンド実行が有効になっている必要があります。詳しくは、「HMC リモート・コマンドの使用可能および使用不可設定」(https://www.ibm.com/support/knowledgecenter/POWER7/p7ha1/enablinganddisablinghmcremotecommands.htm) を参照してください。

アクセス・リストの資格情報:

- HMC 動的スコープ・セットの場合 - HMC サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- 一般ディスカバリー・スコープ・セットの場合 - コンピューター・システム: HMC サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- HMC ユーザーには、以下の役割が必要です。
  - リソース役割: AllSystemResources
  - タスク役割 (コマンド行タスクについての **hmcoperator** に基づく):
    - ManagedSystem (lshwres、lssyscfg)
    - 論理区画 (lshwres、lssyscfg、viosvrcmd)
    - HMC 構成 (lshmc)
- 必要に応じて、**hmcviewer** 権限を持つユーザー (サービス・アカウント) を使用することもできますが、その場合は、データ収集が部分的になります。

> **hmcviewer** 権限で実行する場合は、VIOS 区画が所有するアダプターに関する情報を取得できません。この情報を取得するには、サービス・アカウントに **hmcoperator** 以上の権限が付与されていることを確認してください。それができない場合は、HMC に加えて VIOS 区画も直接ディスカバーするようにスコープと資格情報を追加してください。

Integrated Virtualization Manager (IVM)

IVM インスタンスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: IVM サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- サービス・アカウントには、表示のみの権限を付与する必要があります。

仮想 I/O サーバー (VIOS) 区画

VIOS インスタンスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- HMC 動的スコープ・セットの場合 - VIOS 区画サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- 一般ディスカバリー・スコープ・セットの場合 - コンピューター・システム: VIOS 区画サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- サービス・アカウントは、管理者アカウント (**padmin**) である必要があります。
- サービス・アカウントのユーザー属性は **rlogin=true** である必要があります。この属性は、SMIT を使用するか、**/etc/security/user** ファイルを編集することで設定できます。
- **/etc/ssh/sshd_config** ファイルのパラメーター **PermitUserEnvironment** は **yes** に設定する必要があります。

AIX

AIX インスタンスをディスカバーするには、以下の手順を実行します。

環境の準備:

- パッケージ bos.perf.tools および openSSH/openSSL がインストール済みであることを確認します。
- サービス・アカウントに対する無効なログイン試行の失敗を無効にします。

アクセス・リストの資格情報:

- HMC 動的スコープ・セットの場合 - AIX 区画サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- 一般ディスカバリー・スコープ・セットの場合 - コンピューター・システム: AIX サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- サービス・アカウントには、root、または sudo 権限を持つアカウントを使用できます。
- サービス・アカウントのユーザー属性は **rlogin=true** である必要があります。この属性は、SMIT を使用するか、**/etc/security/user** ファイルを編集することで設定できます。
- 非 root のサービス・アカウントで AIX の sudo 権限を使用できるようにするには、次のようにします。
  - sudo RPM (sudo-1.6.9p15-2noldap) および ssh ファイル・セット (AIX インスタンスの openssh.base.server、openssh.base.client) をインストールします。
  - TSA がシステムへのアクセスに使用できるターゲット AIX インスタンスに非 root ユーザー ID を作成します。
  - 各 AIX インスタンスの **/etc/sudoers** を変更し、TSA が sudo 権限を使用して指定のコマンドを実行できるようにします。

    # Cmnd 別名の指定

    ```
    Cmnd_Alias TSA_CMDS = /usr/bin/lparstat, /usr/sbin/no,
    /usr/sbin/nfso, /usr/bin/lslicense, /usr/sbin/vmo,
    /usr/sbin/ioo, /usr/sbin/lvmo, /usr/sbin/schedo,
    /usr/bin/sysdumpdev, /usr/sbin/smtctl, /usr/sbin/emgr,
    /usr/bin/sissasraidmgr, /usr/sbin/lswpar,
    /usr/sbin/cpuextintr_ctl, /usr/sbin/lsnim, /usr/sbin/raso,
    /usr/sbin/bosdebug, /usr/sbin/chedition,
    /usr/esa/bin/esacli, /usr/sbin/bootinfo,
    /usr/bin/mpio_get_config, /usr/bin/cat /etc/objrepos/CuData,
    ```

```
/usr/bin/cat /etc/objrepos/CuData.vc, /usr/bin/cat
/var/adm/ras/bootlog, /usr/bin/cat
/etc/lpp/diagnostics/data/diagrpt*.dat, /usr/bin/tapeutil,
/usr/lpp/OV/bin/opcagt, /usr/DynamicLinkManager/bin/dlnkmgr
view, /usr/sbin/powermt version, /usr/sbin/powermt display,
/usr/bin/pcmpath query, /usr/sbin/datapath query
```

ユーザー特権の指定

```
<ユーザー名> ALL = NOPASSWD: TSA_CMDS
```

> <ユーザー名> は、TSA が AIX の情報を収集するために使用する非 root のサービス・アカウントです。この <ユーザー名> は、各 AIX インスタンス上のユーザーです。各 AIX インスタンスの **/etc/sudoers** ファイルを、上記のとおりに更新する必要があります。

または

/etc/sudoers を上記のように変更する代わりに、ユーザー特権を以下のように指定することもできます。

```
<ユーザー名> ALL = NOPASSWD: ALL
```

> <ユーザー名> は、TSA が AIX の情報を収集するために使用する非 root のサービス・アカウントです。このユーザー指定は、このサービス・アカウントですべての AIX コマンドに sudo 権限を使用できるようにします。

Linux on Power

Linux on Power インスタンスをディスカバーするには、以下の手順を実行します。

環境の準備:

- サービス・アカウントに対する無効なログイン試行の失敗を無効にします。

アクセス・リストの資格情報:

- HMC 動的スコープ・セットの場合 - Linux 区画サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- 一般ディスカバリー・スコープ・セットの場合 - コンピューター・システム: Linux サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。

- 非 root のサービス・アカウントで Linux の sudo 権限を使用できるようにするには、次のようにします。
  - TSA がシステムへのアクセスに使用できる実際のターゲット Linux インスタンスに非 root ユーザー ID を作成します。
  - 各 Linux インスタンスの **/etc/sudoers** を変更し、TSA が sudo 権限を使用して指定のコマンドを実行できるようにします。

    # Cmnd 別名の指定

    ```
    Cmnd_Alias TSA_CMDS = /usr/sbin/lsvpd, /sbin/lsvpd,
    /usr/sbin/lscfg, /sbin/lscfg, /usr/sbin/lsmcode,
    /sbin/lsmcode, /usr/sbin/lvmdiskscan, /sbin/lvmdiskscan,
    /usr/sbin/dmidecode, /usr/bin/mtlib, /usr/bin/tapeutil,
    /usr/bin/crontab, /sbin/fdisk, /bin/ls -alR /boot/*,
    /bin/cat /proc/irq/*, /bin/cat /proc/net/vlan/config,
    /bin/cat /proc/ppc64/rtas/*, /bin/cat /proc/sys/kernel/cap-
    bound, /bin/cat /proc/sys/kernel/random/entropy_avail
    ```

    # ユーザー特権の指定

    ```
    <ユーザー名> ALL = NOPASSWD: TSA_CMDS
    ```

    > <ユーザー名> は、TSA が Linux の情報を収集するために使用する非 root のサービス・アカウントです。この <ユーザー名> は、各 Linux インスタンス上のユーザーです。各 Linux インスタンスの **/etc/sudoers** ファイルを、上記のとおりに更新する必要があります。

    または

    /etc/sudoers を上記のように変更する代わりに、ユーザー特権を以下のように指定することもできます。

    ```
    <ユーザー名> ALL = NOPASSWD: ALL
    ```

    > <ユーザー名> は、TSA が Linux の情報を収集するために使用する非 root のサービス・アカウントです。このユーザー指定は、このサービス・アカウントですべての Linux コマンドに sudo 権限を使用できるようにします。

- IBM によるサポート・オファリングの一部として AIX 用の IBM Proweb ポータルを使用している場合、HMC 動的スコープ・セットを使用して TSA を構成することをお勧めします。または、HMC、および Power Systems の

論理区画 (VIOS を含む) をディスカバーするように TSA を構成することもできます。

- HMC 動的スコープ・セットを使用してスキャンすることにより、ProWeb で取り出して分析される各 LPAR の詳細な OS 構成情報を取得できます。

> HMC 環境のスコープと資格情報の追加については、「IBM Technical Support Appliance セットアップ・ガイド」の『**HMC 動的スコープ**』セクションを参照してください。

- Power Systems の各種エンティティーをスキャンしてレポート用に収集するデータのレベル:
  - HMC のみをスキャンすることで、「特定済み」タブ、HMC トポロジー、Power Systems ファームウェア、IBM i の推奨、Linux の推奨、HMC/VIOS/AIX、「契約」タブにあるすべての重要情報、アダプター情報を取得できます。
  - VIOS 区画を直接スキャンすることで、アダプター・ファームウェアおよび接続済みのストレージに関する追加情報を取得できます。
  - LPAR を直接スキャンすることで、OS の詳細、さらには PowerHA、GPFS、PowerSC などの特定のソフトウェアのインスタンスを含む LPAR についての追加情報を取得できます。

IBM i

IBM i インスタンスは、SSH 接続を使用してディスカバーされます。IBM i インスタンスに SSH がインストールおよび構成されていない場合、以下の手順を実行します。

環境の準備:

以下の製品/オプションがインストールされ、IBM i 7.2 用に構成されていることを確認します。

- IBM Portable Utilities for i、5733-SC1
- Qshell、5770-SS1、オプション 30
- Portable App Solutions Environment、5770-SS1、オプション 33
- IBM Developer Kit for Java、5770-JV1

以下の製品/オプションがインストールされ、IBM i 7.3 用に構成されていることを確認します。

- IBM Portable Utilities for i、5733-SC1
- Qshell、5770-SS1、オプション 30
- Portable App Solutions Environment、5770-SS1、オプション 33
- IBM Developer Kit for Java、5770-JV1 オプション 16
- Java SE 8 32 ビット

以下の製品/オプションがインストールされ、IBM i 7.4 用に構成されていることを確認します。

- IBM Portable Utilities for i、5733-SC1
- Qshell、5770-SS1、オプション 30
- Portable App Solutions Environment、5770-SS1、オプション 33
- IBM Developer Kit for Java、5770-JV1 オプション 16
- Java SE 8 32 ビット

SSH デーモンを開始するには、以下のコマンドを実行します。

```
SBMJOB CMD (CALL PGM (QP2SHELL) PARM('/QOpenSys/usr/sbin/sshd'))
```

IBM i で SSHD サービスを開始するには、以下のコマンドを実行します。

```
STRTCPSVR SERVER(*SSHD)
```

IBM i で SSH を構成する方法について詳しくは、次の Redbook の 21 章から 23 章を参照してください: http://www.redbooks.ibm.com/redpapers/pdfs/redp4163.pdf

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントのユーザー・クラスは、***USER** を含め、どのクラスにすることもできますが、PTF 情報を収集する (**DSPPTF** コマンドを使用して行う) には追加のオブジェクト権限が必要です。
- **DSPPTF** には、出荷時から、オブジェクト権限に関する次のような制限があります。

- このコマンドには、出荷時から ***EXCLUDE** 共通権限が付与されています
- **QPGMR**、**QSYSOPR**、**QSRV**、**QSRVBAS** の各ユーザー・プロファイルには、出荷時から、このコマンドを使用するための専用権限が付与されています
- **QSECOFR** ユーザー・プロファイル、またはユーザー・クラス ***SECOFR** を持つユーザー・プロファイルは、いつものとおりこのコマンドを実行できます

- オブジェクト・タイプが ***CMD** の **QSYS/DSPPTF** オブジェクトについては、その権限を編集して他のユーザーがこのコマンドを実行できるようにすることができます。
- TSA に新しいサービス・アカウントを作成する場合は、以下の推奨事項が当てはまります。
  - ユーザー・クラスを ***USER** にしてユーザー・プロファイルを作成する
  - **GRTOBJAUT** コマンドを使用して、このユーザー・プロファイルに **DSPPTF** コマンドの実行 (オブジェクトは、オブジェクト・タイプが ***CMD** の **QSYS/DSPPTF**) を許可する。

UNIX システム

Solaris

Solaris デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

- Solaris システムでは、SUNWscpu (ソース互換性) パッケージがインストールされていることを確認します。
- 一部の Solaris システムでは、シリアル番号を取得するために SNEEP をインストールして構成する必要があります。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。

- サービス・アカウントには、非 root のアカウントを使用できます。

Solaris (Oracle iLOM を使用)

Solaris デバイス (Oracle iLOM を使用) をディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、**オペレーター**特権または**管理者**特権を付与できます。

Linux

Linux インスタンスを IBM Power System 上で実行している場合の手順については IBM Power Systems の『Linux on Power』セクション (18 ページ) を参照してください。

Linux on x86 デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

- pciutils パッケージがインストールされていることを確認します。そこに含まれる `lspci` コマンドを使用して、アダプターや外部ストレージ・デバイスへの接続に関する情報を収集します。

アクセス・リストの資格情報:

- VMware 動的スコープ・セットの場合 - Linux 仮想マシン・サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- 一般ディスカバリー・スコープ・セットの場合 - コンピューター・システム: Linux サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- `/bin/sh` をこのアカウントのシェルとして設定します。
- Linux (x86) の場合、サービス・アカウントには、root または `sudo` 権限を持つアカウントを使用できます。
- 非 root サービス・アカウントを使用してディスカバーを行うには、Linux システム上の **/etc/sudoers** ファイルに以下を追加します。

Cmnd 別名の指定

```
Cmnd_Alias TSA_CMDS = /usr/sbin/dmidecode
```

ユーザー特権の指定

```
<ユーザー名> ALL = NOPASSWD: TSA_CMDS
```

<ユーザー名> は、TSA が Linux の情報を収集するために使用する非 root のサービス・アカウントです。この <ユーザー名> は、各 Linux インスタンス上のユーザーです。各 Linux インスタンスの **/etc/sudoers** ファイルを、上記のとおりに更新する必要があります。

または

/etc/sudoers を上記のように変更する代わりに、ユーザー特権を以下のように指定することもできます。

```
<ユーザー名> ALL = NOPASSWD: ALL
```

<ユーザー名> は、TSA が Linux の情報を収集するために使用する非 root のサービス・アカウントです。このユーザー指定は、このサービス・アカウントですべての Linux コマンドに sudo 権限を使用できるようにします。

HP-UX

HP-UX デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- 非 root のサービス・アカウントで HP-UX の sudo 権限を使用できるようにするには、次のようにします。
  - 各 HP-UX デバイスの **/usr/local/etc/sudoers** を変更し、TSA が sudo 権限を使用して指定のコマンドを実行できるようにします。

    # Cmnd 別名の指定

    ```
    Cmnd_Alias TSA_CMDS
    =/usr/sbin/diskinfo,/opt/hpvm/bin/hpvmstatus
    ```

    # ユーザー特権の指定

```
<ユーザー名> ALL=(ALL) NOPASSWD:TSA_CMDS
```

<ユーザー名> は、TSA が HP-UX の情報を収集するために使用する非 root のサービス・アカウントです。

VMware vCenter Server および VMware ESXi

VMware 環境の場合、VMware 動的スコープ・セットを使用します。VMware 動的スコープ・セットでは、VMware vCenter Server / ESXi 用のスコープ定義を作成し、関連する VMware と仮想マシンの資格情報を提供しますが、管理対象の各仮想マシンに対してスコープを作成する必要はありません。VMware vCenter Server / ESXi がディスカバーされると、TSA はその時点で存在する仮想マシンを判別し、各仮想マシンを自動的にスキャンします。

仮想マシンの構成が静的である VMware 環境では、VMware 動的スコープ・セットに代わる方法として、エンティティーのスコープと資格情報を次の順序で追加して反復します。

1. **vCenter Server インスタンス**: これは、管理対象の ESXi ホストと、そこに含まれる仮想マシンのゲストに関する概要情報を戻します。
2. **ESXi ホスト**: vCenter Server によって管理していない ESXi ホストを追加します。
3. **個々の仮想マシンのゲスト**: これにより、オペレーティング・システムに関するさらに詳細な情報を収集することができます。

VMware 環境用に TSA を構成する場合、以下のアクションをお勧めします。

1. 使用可能な場合には VMware vCenter Server をディスカバーするように TSA を構成します。VMware vCenter Server の自動ディスカバーによって、TSA は、vCenter Server が管理する VMware ESXi ホストすべてに関する情報を収集します。ESXi ホストに関する構成情報は不要です。
2. VMware vCenter Server によって ESXi ホストが管理されていない場合にのみ VMware ESXi ホストをディスカバーするよう TSA を構成します。
3. ESXi ホスト上の仮想マシンごとに VMware ツールをインストールします。VMware ツールがインストールされていない場合、IP アドレスや、インストールされているオペレーティング・システムなどの一部のインベントリー・データにアクセスできません。

4. 各 VMware ESXi ホストで CIM インターフェースがアクティブになるよう構成します。CIM インターフェースにより、TSA は ESXi ホスト内のアダプターに関する詳細情報を収集できます。CIM プロバイダーの詳細については、『付録 C』(56 ページ) を参照してください。

管理対象の ESXi サーバーの情報に加えて vCenter サーバー・インスタンスをディスカバーするには、以下の手順を実行します。

環境の準備:

- ESXi ホスト上の仮想マシンごとに VMware ツールをインストールします。
- 各 VMware ESXi ホストで CIM インターフェースがアクティブになるよう構成します。
- フル・ディスカバリーのためには、CIM ポート (5989) に TSA がアクセスできなければなりません (ファイアウォールなどでブロックされないようにします)。

アクセス・リストの資格情報:

- VMware 動的スコープ・セットの場合 - VMware vCenter Server サービス・アカウントのユーザー名 / パスワード。
- 一般ディスカバリー・スコープ・セットの場合 - コンピューター・システム: VMware vCenter Server サービス・アカウントのユーザー名 / パスワード。
- サービス・アカウントには、**管理者**役割の権限、または少なくとも以下の追加特権を持つカスタムの読み取り専用役割の権限が必要です。
  - グローバル → ライセンス
  - グローバル → 設定
  - ホスト → CIM
  - ホスト → 構成 → 変更設定
  - ホスト → CIM→ CIM 対話

ESXi デバイスを直接ディスカバーするには、以下の手順を実行します。

環境の準備:

- ESXi ホスト上の仮想マシンごとに VMware ツールをインストールします。

- 各 VMware ESXi ホストで CIM インターフェースがアクティブになるよう構成します。

アクセス・リストの資格情報:

- VMware 動的スコープ・セットの場合 - VMware ESXi サービス・アカウントのユーザー名 / パスワード。
- 一般ディスカバリー・スコープ・セットの場合 - コンピューター・システム: VMware ESXi サービス・アカウントのユーザー名 / パスワード。
- サービス・アカウントには、**管理者**役割の権限が必要です。

Windows

TSA は、以下の方法で Windows のインスタンスのディスカバリーをサポートします。

- WINRM
- SMB1

> より安全なインターフェースである WINRM を使用した Windows のディスカバリーが推奨されます。

Windows (WINRM を使用)

WINRM を使用して Windows デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

環境を準備するための最も一般的な方法は、ターゲットの Windows サーバーにインストールされている、認証局によって生成されたサーバー証明書を使用する方法です。証明書は、次の条件を満たしている必要があります。

- 認証局から発行されたルート証明書と中間証明書が、信頼されたルート認証局の証明書の中に含まれている。
- サーバー証明書が個人証明書にインストールされている。
- サーバー証明書が、サーバーの完全修飾ホスト名に対して発行されたものであることを示している。

- サーバー証明書に、このサーバーの秘密鍵が含まれている。

以下のコマンドは、リモート HTTPS 接続用の WINRM を構成します。

winrm quickconfig -transport:https

このコマンドは、以下の操作を行います。

- WINRM がアクティブではない場合に有効にする
- 再起動時に WINRM が自動的に開始するように WINRM サービスを変更する
- WINRM HTTPS リスナーを構成する
- リモート HTTPS 接続を許可するように Windows ファイアウォール規則を変更する

このコマンドは、以下の出力を生成します。**y** を入力して、変更内容を確認します。

```
WinRM サービスはこのマシン上で既に実行中です。
管理のためのこのマシンへのリモート・アクセスを許可するように WinRM がセットアップされていません。
次の変更を行う必要があります。

HTTPS://* に WinRM リスナーを作成して、このマシン上のすべての IP への WS-Man リクエストを受け入れるようにする。
CredSSP 認証に使用するために、サービスに対して CertificateThumbprint 設定を構成する。
ローカル・ユーザーにリモートから管理権限を付与するために
LocalAccountTokenFilterPolicy を構成する。

これらの変更を行いますか [y/n]? y

リモート管理の WinRM が変更されました。

HTTPS://* に WinRM リスナーが作成され、このマシン上のすべての IP への WS-Man リクエストを受け入れるようになりました。
このサービスに必要な設定を構成しました。
ローカル・ユーザーにリモートから管理権限を付与するために
LocalAccountTokenFilterPolicy を構成しました。
```

最後に、HTTPS 経由でのユーザー ID/パスワード認証を許可するために、次のコマンドを実行します。

winrm set winrm/config/service/auth @{Basic="true"}

代替手段として、自己署名証明書を使用することもできます。この構成の手順については、『付録 D: WINRM を使用する Windows』(60 ページ) に示されています。

アクセス・リストの資格情報:

- VMware 動的スコープ・セットの場合: サービス・アカウントのユーザー名 / パスワード。
- 一般ディスカバリー・スコープ・セットの場合: コンピューター・システム (Windows): サービス・アカウントのユーザー名 / パスワード。
- サービス・アカウントは、次のいずれかのグループに含まれている必要があります。
  - 管理者
  - WinRMRemoteWMIUsers__

ユーザーを WinRMRemoteWMIUsers__ グループに追加するには、以下のコマンドを実行します。

```
net localgroup WinRMRemoteWMIUsers__ [user_id] /add
```

Windows (SMB1 を使用)

Windows デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

- Windows Scripting Host (WSH) サービスまたは Windows Management Instrumentation (WMI) サービス、および VBScript が、ターゲット・デバイスで使用可能であることを確認します。
- ポート 445 がファイアウォールや IP セキュリティー・ポリシーでブロックされていないことを確認します。TSA には、TCP/IP を介した Server Message Block (SMBv1) プロトコルが必要なためです。
- セキュリティー・ポリシーを適用するには、**「スタート」→「コントロール パネル」→「管理ツール」**に移動し、ポリシーの保存場所がローカルであるか Active Directory であるかに応じて、次のナビゲーションを選択します。
  - ポリシーがローカルに保存されている場合: **「管理ツール」→「ローカル セキュリティー ポリシー」→「ローカル コンピューターの IP セキュリティー ポリシー」**
  - ポリシーが Active Directory に保存されている場合: **「管理ツール」→「Default Domain Security の設定」→「Active Directory の** IP セキュリ

ティー ポリシー」または「**管理ツール**」→「**Default Domain Controller Security Settings**」→「**Active Directory** の IP セキュリティー ポリシー」

- TSA は、システムの %TEMP% および他のディレクトリーにアクセスするために、隠しリモート管理ディスク共有へのアクセス権限を必要とします。また TSA がリモート・レジストリーにアクセスするには、プロセス間通信共有 (IPC$) へのアクセス権限も必要です。プロセス間通信共有サーバー・サービスが開始されていることを確認してください。このサーバー・サービスを開始するには、「**コントロール パネル**」→「**管理ツール**」→「**サービス**」→「**Server**」にアクセスします。
- Remote Registry サービスがアクティブであることを確認します。これは、TSA が Windows デバイスとのセッションを確立するために必要です。

アクセス・リストの資格情報:

Windows リリース 2012 R2 以降:

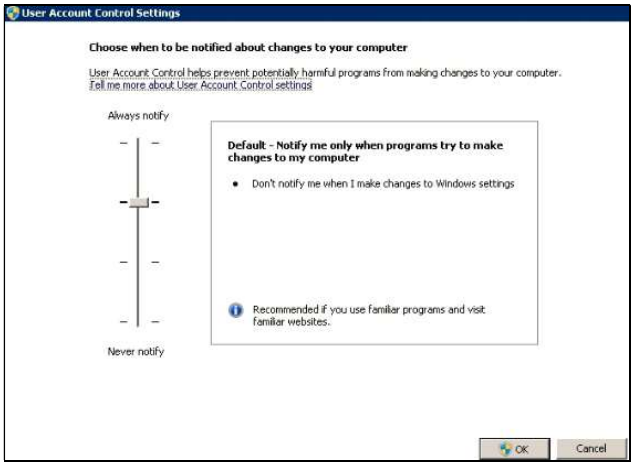
- VMware 動的スコープ・セットの場合 - 基本管理者のアカウント / パスワード。このアカウントは、ユーザー・アカウント制御 (UAC) の設定に関係なく有効です。
- 一般ディスカバリー・スコープ・セットの場合 - コンピューター・システム (Windows): 基本管理者のアカウント / パスワード。このアカウントは、ユーザー・アカウント制御 (UAC) の設定に関係なく有効です。

特定の条件を満たせば、基本管理者アカウント以外のアカウントを使用することもできます。アカウントは、ローカルまたはドメインの管理者アカウントである必要があり、ユーザー・アカウント制御 (UAC) の設定が特定の要件を満たしている必要があります。サポートされるアカウントのタイプと UAC 設定の組み合わせを以下の表にまとめます。UAC に関する追加情報については、Microsoft Windows の資料を参照してください。

	ユーザー アカウント制御の設定			
	常に通知する	プログラムがコンピューターに変更を加えようとする場合のみ通知する (デフォルト設定)	プログラムがコンピューターに変更を加えようとする場合のみ通知する (デスクトップを暗転しない)	通知しない
基本管理者	はい	はい	はい	はい
ドメイン管理者グループのユーザー	いいえ	はい	はい	はい
ローカル管理者グループのユーザー	いいえ	はい	はい	はい
非管理者アカウント (ドメインまたはローカル)	いいえ	いいえ	いいえ	いいえ

UAC 設定にアクセスするには、**[スタート]**、**「コントロール パネル」**の順にクリックします。検索ボックスに**「uac」**と入力して、**「ユーザー アカウント制御設定の変更」**をクリックします。

以下が、デフォルトの設定です。



ATM デバイス

特定のモデルの ATM デバイスをディスカバーすることができます。ATM デバイス (そのコンポーネントに関する基本情報を含む) をディスカバーするには、以下の手順を実行します。

環境の準備:

- Wincor Nixdorf モデル - 『Windows (SMB を使用)』の指示に従います。

管理モジュール

IBM Flex Systems の場合、エンティティーのスコープと資格情報を次の順序で追加して反復するのが最善です。

1. **Flex System Manager (FSM):** これは、Flex System Manager と、それらが管理するシャーシおよび関連付けられたコンピュート・ノードに関する概要情報を戻します。

   > FSM がない場合は、CMM と、Flex System 上にある POWER コンピュート・ノードを管理するすべての HMC をスキャンすることをお勧めします。

2. **シャーシ・マネージメント・モジュール (CMM):** FSM によって管理されないシャーシに関しては、各シャーシとそれらに関連付けられたノードに関する概要情報を取得するためにそれぞれの CMM を示します。
3. **コンピュート・ノード:** これは、オペレーティング・システムに関する詳細情報を戻します。

Flex System Manager (FSM) デバイス

FSM デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、**SMAdmin** 権限が必要です。

シャーシ管理モジュール (CMM) デバイス

CMM デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、少なくとも**オペレーター**権限が必要です。

拡張管理モジュール (AMM) デバイス

AMM デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、少なくとも**オペレーター**権限が必要です。

HP ProLiant ブレード・サーバー (HP OnBoard Administrator を使用)

Hewlett Packard (HP) ProLiant Server では、HP OnBoard Administrator (HP OBA) のエンティティーのスコープおよび資格情報を追加するのが最適です。HP OBA は、HP OnBoard Administrator、それが管理するエンクロージャー、およびエンクロージャーに含まれるコンピュート・ノードに関する概要情報を戻します。

HP OnBoard Administrator (OBA) を使用して HP ProLiant ブレード・サーバーをディスカバーするには、以下の手順を実行します。

環境の準備:

- HP OBA はアクティブ・モードになっている必要があります。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、HP Onboard Administrator に対する **OA 管理者**、**OA オペレーター**、または **OA ユーザー**の**権限**が必要です。**OA ユーザー権限**役割が推奨されています。

TSA はアクティブ状態の HP OnBoard Administrators からのみ情報を収集します。スタンバイ状態の HP OnBoard Administrators からは情報は収集されません。

統合管理モジュール (IMM) デバイスおよび 統合管理モジュール II (IMM2) デバイス

IMM デバイスおよび IMM2 デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、いずれでも有効な権限を付与できます。

HP Integrity および HP9000 サーバー (iLO を使用)

iLO は HP Integrity および HP9000 サーバーに含まれる個別のプロセッサー・カードで、サーバーに関する基本的なハードウェア情報を提供します。iLO は、サーバー自体の電源が入っていなくても、サーバーが接続されるとすぐにアクティブになります。

iLO を使用して HP Integrity および HP9000 サーバーに関する要約レベルのインベントリー情報をディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、いずれでも有効な権限レベルを付与できます。**ユーザー**権限が推奨されています。

ネットワーク・デバイス

このセクションには、以下のタイプのネットワーク・デバイスに関する詳細情報を記載します。

プラットフォーム
BNT スイッチ
Brocade スイッチ
Check Point
Cisco スイッチ
F5 Big-IP (TMOS)

Fortinet (FortiOS)
IBM b タイプのストレージ・エリア・ネットワーク (SAN) スイッチ
Juniper スイッチ
Palo Alto Networks (PAN-OS)
QLogic スイッチ
詳細情報については、上記の各リンクをクリックしてください。

BNT スイッチ

BNT スイッチをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、**admin** 権限が必要です。

Brocade

Brocade デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- 仮想ファブリック・モードを無効にする場合: サービス・アカウントには、いずれでも有効な権限を付与できます。**ユーザー**権限が推奨されています。
- 仮想ファブリック・モードを有効にする場合: サービス・アカウントには、Fabric OS に対する **Admin** 権限が必要です。

Check Point

Check Point システムをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- サービス・アカウントには、管理者権限 (**adminRole**) が必要です。
- サービス・アカウントには、CLI コマンドを実行するための SSH アクセスが必要です。

Cisco

Cisco デバイスをディスカバーするには、以下のコンピューター・システム資格情報または SNMP 資格情報を使用できます。

アクセス・リストの資格情報:

- コンピューター・システムまたはその他 (Cisco Device) またはその他 (Cisco Works): サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵。
- サービス・アカウントには、**ネットワーク管理**役割の特権が必要です。
- SNMP: コミュニティー・ストリングを入力 (SNMPv1 および SNMPv2 用)。
- SNMP (SNMPv3):
  - 次の情報を入力します。
    - ユーザー名
    - パスワード
    - プライベート・パスワード (オプション)
  - 認証プロトコルを選択: なし、MD5、SHA

スコープ内のネットワーク・デバイスすべてに対する読み取りアクセス権のある TSA が、単一のコミュニティー文字列を使用できるようにすることが重要です。

F5 Big-IP (TMOS)

TMOS を実行している F5 Big-IP システムをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- サービス・アカウントには、F5 管理者権限が必要です。

- サービス・アカウントには、TMSH CLI コマンドを実行するための SSH アクセスが必要です。

Fortinet (FortiOS)

FortiOS を実行している Fortinet デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

- システム・コンソールが、コマンド出力全体を表示するように構成されていることを確認します。

```
config system console
set output standard
end
```

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- サービス・アカウントには、少なくとも読み取り専用権限が必要です。

IBM b タイプのストレージ・エリア・ネットワーク (SAN) スイッチ

IBM b タイプの SAN デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- 仮想ファブリック・モードを無効にする場合: サービス・アカウントには、いずれでも有効な権限を付与できます。**ユーザー**権限が推奨されています。
- 仮想ファブリック・モードを有効にする場合: サービス・アカウントには、Fabric OS に対する **Admin** 権限が必要です。

Juniper

Juniper デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、管理者権限が必要です。

注: メモリー・サイズ情報のディスカバリーには、デバイスに Junos® バージョン 12.1 以降がインストールされている必要があります。

Palo Alto Networks (PAN-OS)

PAN-OS で実行されている Palo Alto Network システムをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、Superuser または Superuser (読み取り専用) が必要です。
- サービス・アカウントには、REST API アクセス (ポート 443) が必要です。

QLogic スイッチ

QLogic スイッチをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、管理者権限が必要です。

ストレージ・デバイス

このセクションには、以下のタイプのストレージ・デバイスおよびテープ・デバイスに関する詳細情報を記載します。

プラットフォーム
EMC Corporation のストレージ
HP StorageWorks P2000 Modular Smart Array
IBM DS3xxx、DS4xxx、または DS5xxx
IBM DS6xxx または DS8xxx
IBM FlashSystem、v9000
IBM ProtecTier
IBM SVC または V7000/V3700

プラットフォーム
IBM TS3100 テープ・ライブラリー
IBM TS3200 テープ・ライブラリー
IBM TS3310 テープ・ライブラリー
IBM TS3494、TS3953 テープ・ライブラリー
IBM TS3500、TS3584 テープ・ライブラリー
IBM TS4500 テープ・ライブラリー
IBM TS7700 テープ・ライブラリー
IBM V7000 Unified
IBM XIV
nSeries または NetApp
詳細情報については、上記の各リンクをクリックしてください。

EMC Corporation のストレージ

EMC CLARiiON / VNX / VMAX

EMC CLARiiON / VNX / VMAX の各デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

- EMC SMI-S プロバイダー製品のインスタンスが Windows または Linux システムにインストールされていることを確認します。デフォルトでは、TSA は EMC SMI-S の推奨に従って、SLP を使用してプロバイダーの場所をディスカバーします。ネットワーク・セキュリティー・ポリシーによって SLP ネットワーク・トラフィックがブロックされている場合は、SLP を使用しないで EMC SMI-S プロバイダーに直接アクセスするように TSA を構成できます。

- ご使用のネットワーク・セキュリティーが SLP ネットワーク・トラフィックを許容していない場合、**「ディスカバリー設定」→「接続設定」**ページを使用して、EMC SMI-S プロバイダーが照会要求を行うために listen するポートに関する情報を指定します。
- SMI-S プロバイダーが使用している IP アドレスの 1 つ以上がスコープ・セットに定義済みであることを確認します。TSA は、SMI-S プロバイダーに接続して、管理対象の EMC デバイスに関する情報を取得します。個々の EMC デバイスの IP アドレスは、スコープ・セット内に含める必要はありません。TSA は、使用可能な場合は HTTPS を使用して SMI-S プロバイダーに接続を試みます。そうでない場合は、HTTP が使用されます。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、いずれでも有効な役割を付与できます。**モニター**役割が推奨されています。

SMI-S プロバイダーの資格情報のみを TSA に入力する必要があります。EMC デバイスの資格情報を入力する必要はありません。

EMC Data Domain

EMC Data Domain デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、必要最小限の権限を付与できます。

HP StorageWorks P2000 Modular Smart Array

HP Storage システムをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、必要最小限の権限を付与できます。

IBM DS3xxx、DS4xxx または DS5xxx ストレージ

IBM DS3xxx、DS4xxx または DS5xxx の各デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

- ストレージ・マネージャーで、リモート **smcli** コマンドの使用が許容されていることを確認します。

アクセス・リストの資格情報:

- 保護されていないストレージ・デバイスの場合、資格情報は不要です。
- 保護されたストレージ・デバイスの場合、以下の手順を実行します。
  - コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
  - サービス・アカウントには、**admin** 役割または**モニター**役割を設定できます。**モニター**役割が推奨されています。

IBM DS6xxx / DS8xxx ストレージ

IBM DS6xxx / DS8xxx デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

- ストレージ・マネージャーで、リモート **dscli** コマンドの使用が許容されていることを確認します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには**モニター**役割が必要です。

IBM FlashSystem、v9000

IBM FlashSystems をディスカバーするには、以下の手順を実行します。

環境の準備:

- 以前のモデルの場合、システムのディスカバーを正常に行うには、MCP (Management Control Port) がアクティブ状態にある必要があります。
  - システムがアクティブ状態にあるか確認するには、コマンド - `system status` を実行します。

- 2 つの IP アドレスのうちの一方の IP がダウンすると、システムはパッシブ状態になります。もう一方のイーサネット・ポートをアクティブにするには、コマンド - `sync activate` を実行します。
- ディスカバーされるシステムは、管理 IP アドレスまたは構成ノード (あるいはその両方) でなければなりません。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワードまたはユーザー名/SSH 鍵認証。
- サービス・アカウントには、いずれでも有効な役割を付与できます。**モニター**役割が推奨されています。

IBM ProtecTIER

ProtecTIER デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、管理者特権が必要です。

IBM SVC、V7000/V3700 ストレージ

SVC デバイスおよび V7000/V3700 デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: 認証のためのユーザー名/パスワードまたはユーザー名/SSH 鍵。
- サービス・アカウントには、いずれでも有効な役割を付与できます。**モニター**役割が推奨されています。

IBM TS3100 テープ・ライブラリー

TS3100 テープ・ライブラリー・デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、管理者権限が必要です。

IBM TS3200 テープ・ライブラリー

TS3200 テープ・ライブラリー・デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、管理者権限が必要です。

IBM TS3310 テープ・ライブラリー

TS3310 テープ・ライブラリー・デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

- Web サービスは、常にセキュア・モードで構成されます。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、管理者権限が必要です。

IBM TS3494、TS3953 テープ・ライブラリー

TS3494、TS3953 テープ・ライブラリー・デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、必要最小限の権限を付与できます。

IBM TS3500、TS3584 テープ・ライブラリー

以下の前提条件が必要です。

- TS3500 テープ・ライブラリーは、ファームウェア・レベル 8xxx (以上) である必要があります。
- Advanced Library Management System (ALMS) がインストール済みで有効になっている必要があります。

SSL と 非 SSL の両方の接続がサポートされています。

TS35xx テープ・ライブラリー・デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

- TS3500 Web インターフェースは、**「パスワード保護なし」**と**「パスワード保護」**のどちらを使用しても構成できます。
  - **「パスワード保護」**がアクティブな場合、以下の**『アクセス・リストの資格情報』**で説明しているように資格情報を作成します。
  - **「パスワード保護」**が無効な場合、資格情報は必要ありません。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、管理者権限が必要です。

IBM TS4500 テープ・ライブラリー

以下の前提条件が必要です。

- TS4500 テープ・ライブラリーはファームウェア・レベル 1.4.1.2 以降 (最大 1.7.0.0) である必要があります。
- Advanced Library Management System (ALMS) がインストール済みで有効になっている必要があります。

SSL と 非 SSL の両方の接続がサポートされています。

TS4500 テープ・ライブラリー・デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

- TS4500 Web インターフェースは、**「パスワード保護」**付きでのみ構成可能です。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントは、**サービス**役割にマップされる必要があります。

IBM TS7700 テープ・ライブラリー

TS7700 テープ・ライブラリー・デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントに必要なのは、**読み取り専用**権限のみです。

IBM V7000 Unified ストレージ

V7000 Unified デバイスをディスカバーするには、以下の手順を実行します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、いずれでも有効な役割を付与できます。**モニター**役割が推奨されています。

IBM XIV ストレージ

XIV デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

- ストレージ・マネージャーで、リモート **xcli** コマンドの使用が許容されていることを確認します。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには**読み取り専用**ユーザー役割が必要です。
- XIV システムで、アラート生成前の無効なサインオン試行のしきい値が低く設定されている場合もありますので、ご注意ください。大きな資格情報セットを使用している場合は、この制限を超過することで、不必要に問題が報告される可能性があります。XIV デバイスを単一のスコープ・セットにまとめて、それらのサービス・アカウントの資格情報をそのスコープ・セットに制限することを試してみてください。

nSeries または NetApp ストレージ

nSeries または NetApp デバイスをディスカバーするには、以下の手順を実行します。

環境の準備:

- データ収集は、Data ONTAP CLI、RLM CLI および SP CLI で構成されたシステムでサポートされています。ただし、BMC CLI はサポートされていません。
- **telnet.distinct.enable** オプションをオンにしておく必要があります。

アクセス・リストの資格情報:

- コンピューター・システム: サービス・アカウントのユーザー名/パスワード。
- サービス・アカウントには、必要最小限の権限を付与できます。

ファイアウォールの考慮事項

アプライアンスとディスカバリー・デバイスの間にあるファイアウォールは、完全で正常なディスカバリーの実行を妨げることがあります。

ファイアウォールをトラバースする必要があるケースでは、ディスカバー対象のデバイスのタイプによっては、ファイアウォールのポートを開いておく必要がある場合があります。通常は、ポート 22 (SSH) と 161 (SNMP) を開いておく必要があります。これらに加えて、サポート対象のデバイスに応じ、以下の表にある適切なポートを開いておく必要があります。

ディスカバリー・エンドポイント	ポート	インターフェース/プロトコル
多数	161	SNMP
ストレージ・デバイス		
DS6000 / DS8000	1750 (HTTP) または 1751 (HTTPS)	DSCLI
DS3000 / DS4000 / DS5000	2463	SMCLI
XIV	7778	XCLI
nSeries または NetApp	22 / 23	SSH または Telnet
SVC または V7000/V3700	22	SSH
V7000 Unified	22	SSH
IBM TS3500	443 / 80	HTTPS または HTTP
IBM TS4500	443 / 80	HTTPS または HTTP
IBM TS7700	443 / 80	HTTPS または HTTP
IBM TS3100 / TS3200 / TS3310	80	HTTP
IBM TS3494、TS3953	23	Telnet
IBM ProtecTier	22	SSH

ディスカバリー・エンドポイント	ポート	インターフェース/プロトコル
HP Storage	22 / 23	SSH または Telnet
IBM Flash System、v9000	22	SSH
EMC Corporation のストレージ - CLARiion/VNX/VMAX	427 - (デフォルト) SLP ディスカバリーが許可されている場合。SLP ディスカバリーが無効の場合、このポートは使用されません。 EMC SMI-S プロバイダーによって構成されている HTTPS / HTTP ポート; デフォルト値は 5989 / 5988	SLP、HTTPS / HTTP
	EMC SMI-S プロバイダーを使用して EMC ストレージ・デバイスをディスカバーするための SLP ディスカバリー・オプションを有効または無効にできます。	
EMC Corporation のストレージ – EMC Data Domain	22	SSH*
オペレーティング・システムとホスト		
FSM	22 / 23	SSH または Telnet
CMM	22 / 23	SSH または Telnet
AMM	22 / 23	SSH または Telnet
HP ProLiant ブレード・サーバー (HP OnBoard Administrator を使用)	22 / 23	SSH または Telnet
IMM & IMM2	22 / 23	SSH または Telnet
HP Integrity / HP 9000 サーバー用 HP iLO	22 / 23	SSH* または Telnet
ネットワーク・デバイス		

ディスカバリー・エンドポイント	ポート	インターフェース/プロトコル
Brocade	161 / 22 /23	SNMP、SSH、Telnet
IBM b タイプのストレージ・エリア・ネットワーク (SAN) スイッチ	22 /23	SSH、Telnet
Cisco	161 / 22 / 23	SNMP、SSH、Telnet
BNT	22 / 23	SSH または Telnet
Juniper	22 / 23	SSH または Telnet
QLogic	22 / 23	SSH* または Telnet
Fortinet (FortiOS)	22 / 23	SSH または Telnet
Palo Alto Networks (PAN-OS)	443	HTTPS
F5 Big-IP (TMOS)	22 / 23	SSH または Telnet
Check Point	22 / 23	SSH または Telnet
オペレーティング・システム / サーバー・プラットフォーム		
HMC	22	SSH
VIOS	22	SSH
AIX	22	SSH
Linux	22	SSH
Windows	445	SMBv1
VMware vCenter	443	HTTPS
VMware ESXi	443、5989	HTTPS
IVM	22 / 23	SSH または Telnet
IBM i	22	SSH
SUN	22	SSH

ディスカバリー・エンドポイント	ポート	インターフェース/プロトコル
▪ TSA は、SSH のマークが付いたデバイスに関して、SSH v1 のみをサポートします*。		

ディスカバリーの問題

ディスカバリーの問題の多くは、アクセスや権限の問題によるものです。

最も一般的なアクセスの問題は、デバイス上の必要なポートへのアクセスがファイアウォールによってブロックされることによるものです。開いてアクセス可能にしておく必要のあるポートは、デバイス・タイプによって異なります。利用可能なポートを判別するには、『ファイアウォールの考慮事項』セクション (47 ページ) を参照してください。

最も一般的な権限の問題には、以下のものがあります。

- **資格情報が定義されていない**。デバイスの資格情報が TSA で定義されていて、デバイス上に適切なサービス・アカウントが作成されていることを確認します。
- **資格情報のユーザー名またはパスワードが正しくない**。 資格情報の作成または編集時に**テスト**機能を使用して、資格情報が有効であることを確認します。
- **資格情報のパスワードの有効期限が切れている**。
- **資格情報に、デバイスに対する必要な権限が不足している**。ターゲット・デバイスに対する資格情報の要件を確認するには、『デバイス・ディスカバリーの構成』セクション (13 ページ) を参照してください。
- **有効な資格情報タイプを使用していない**。Windows デバイスでは、「コンピューター・システム」資格情報ではなく、「コンピューター・システム (Windows)」資格情報を作成します。

「**認証状況**」ページ (**「ツール」→「認証状況」**) で、サービス・アカウントの資格情報に期限切れのパスワードがないか、または無効になったものがないか確認してください。

継続的に対応すべき考慮事項

ネットワークの適切な部分が TSA で定義され、正常にスキャンされた後は、TSA がディスカバリーと伝送を適切なスケジュールで定期的に実施するようにできます。

次のようなアクティビティーを継続的に実行する必要があります。

- TSA によって生成されたレポートを、IBM 担当員と定期的に確認する。
- TSA ユーザー・インターフェースを使用して定期的にバックアップを実施し、TSA 構成のコピーを保存する。

この操作では、TSA によって収集されたデータは保存されません。構成情報のみが保存されます。

- 「**認証状況**」ページ (「**ツール**」→「**認証状況**」) で、サービス・アカウントの資格情報に期限切れのパスワードがないか、または無効になったものがないかを定期的に確認してください。
- デバイスのサービス・アカウントのパスワードが更新されたら、TSA でもパスワードも更新し、TSA の資格情報の定義がターゲット・デバイスの資格情報と常に同期しているようにする。
- ご使用の環境のセキュリティー・ポリシーが許すなら、サービス・アカウントに有効期限のないパスワードを設定するか、SSH 鍵を使用する。そのようにしておけば、TSA ユーザー・インターフェースとデバイスのパスワードを定期的に更新する必要がなくなります。

トラブルシューティング

AMM のディスカバリーでのアクティブ・セッション

AMM デバイスには、同時にアクティブにできるセッションの数を制限する設定 (最大数は 20) があります。この設定値が、TSA がセッションを作成できるだけの数になっていないと、AMM デバイスをディスカバーすることができません。

AMM デバイスのアクティブ・セッション数の制限を変更するには、以下の手順を実行します。

1. Web ブラウザーに AMM デバイスの IP アドレスを入力して、AMM Web インターフェースにログインします。
2. 「**MM Control**」→「**Login Profiles**」に起動します。
3. TSA がデバイスをディスカバーするために使用するログイン ID をクリックします。
4. 「**Maximum simultaneous active sessions**」の設定値を大きな値に変更します。
5. ページの右下にある「**保存**」をクリックします。

付録 A: 用語および定義

本資料は、読者がインターネット・プロトコル (IP) ネットワークおよびプロトコルに関して十分に理解していることを前提としています。

用語	定義
ディスカバリー・デバイス	TSA によってディスカバー可能な、デプロイ済みの IT インフラストラクチャー・コンポーネントを表します。代表的なデバイスとしては、サーバー、コンピューター・システム (IBM、Dell、HP など)、ストレージ・エレメント、およびネットワーク・エレメント (スイッチ、ブリッジ、ルーターなど) などがあります。

付録 B: その他の項目

ユーザー・インターフェースのダウンロード機能

Web ブラウザーの使用時に、「すべてのログをダウンロード」(**「アクティビティー・ログ」** ページ)、ファイルのダウンロード (**「ディスカバリー履歴」**ページ)、または文書のダウンロード (**「文書」**ページ) が正常に完了しないことがあります。この問題を解決するには、「IBM Technical Support Appliance セットアップ・ガイド」にあるように、サポートされている別の Web ブラウザーを使用してみてください。それができない場合は、ご使用のブラウザーのプロパティーをデフォルト設定に戻してみてください。

付録 C: VMware ESXi の CIM プロバイダー

CIM プロバイダーは、VMware ESXi を実行しているサーバーに関するハードウェアおよびファームウェアの追加情報を収集できる VMware ESXi プラグイン・セットです。TSA および VMware vCenter のどちらも、この追加情報を有効活用できます。

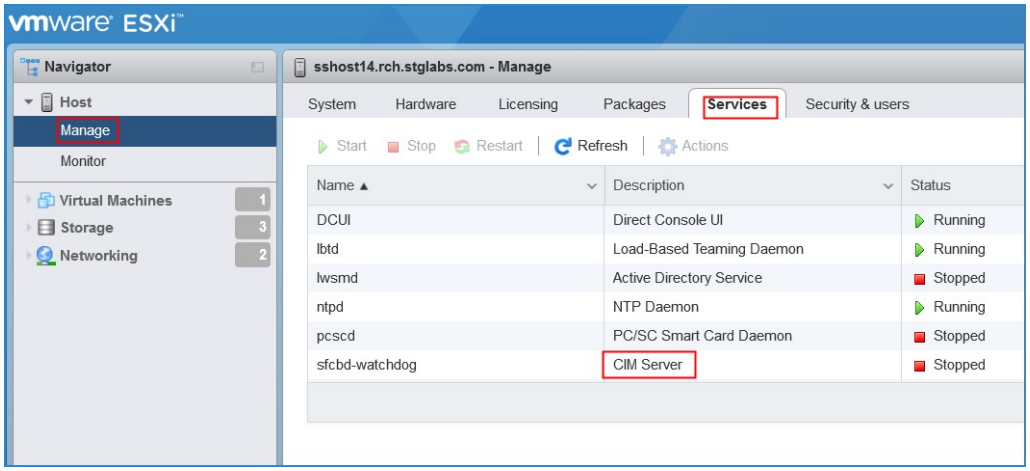
CIM プロバイダー・プラグインは、サーバーおよびコンポーネントの製造元によって開発されています。CIM プロバイダー・プラグインが ESXi に確実に含まれるようにするには、CIM プロバイダー・プラグインが含まれている、カスタマイズされたインストール・イメージを使用してください。CIM プロバイダーがインストールされていない既存の VMware ESXi インスタンスの場合は、サーバーおよびコンポーネントの製造元から必要なプラグインを入手して、ESXi にインストールしてください。VMware は、製造元が提供する各種プラグインのリストを提供しています。

詳細については、
https://www.vmware.com/resources/compatibility/pdf/vi_cim_guide.pdf を参照してください。

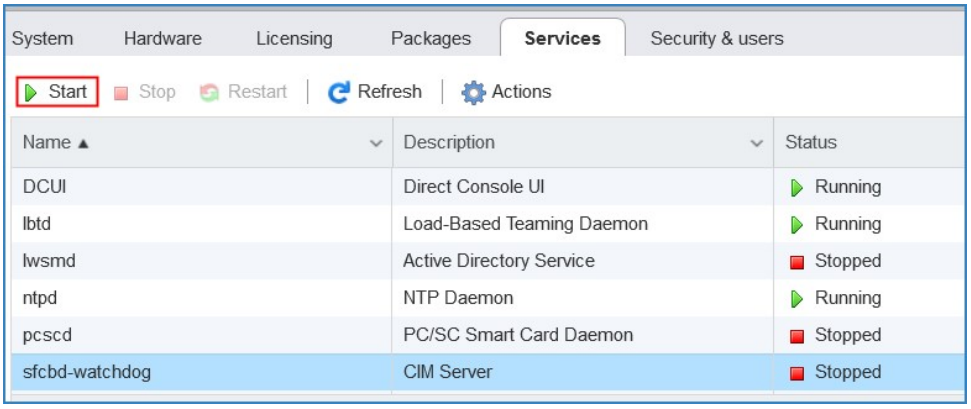
CIM プロバイダーがアクティブであるか確認し、アクティブでない場合に CIM プロバイダーをオンにするために、以下の手順を実行します。

VMware vSphere Web Client の場合

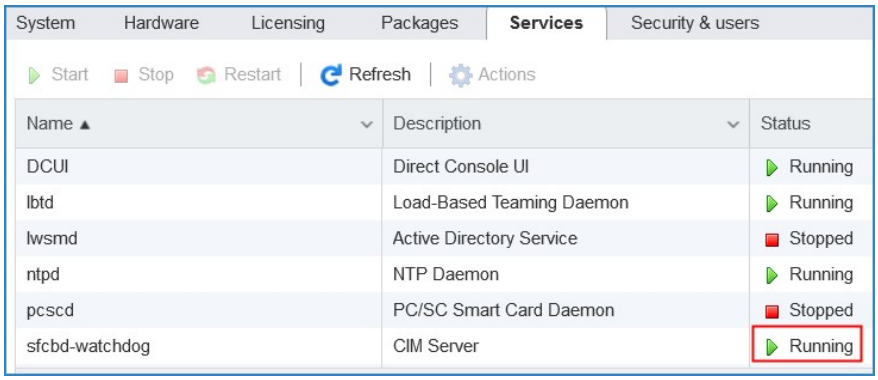
- VMware vSphere Web Client にログインします。
- 左側のナビゲーション・ウィンドウで**「ホスト」→「管理」**をクリックし、右ペインで**「サービス」**タブをクリックします。
- **「CIM サーバー」**を含むサービスのセットが表示されます。



- 「**CIM サーバー**」が「**停止**」状態の場合、それを選択して「**開始**」をクリックします。



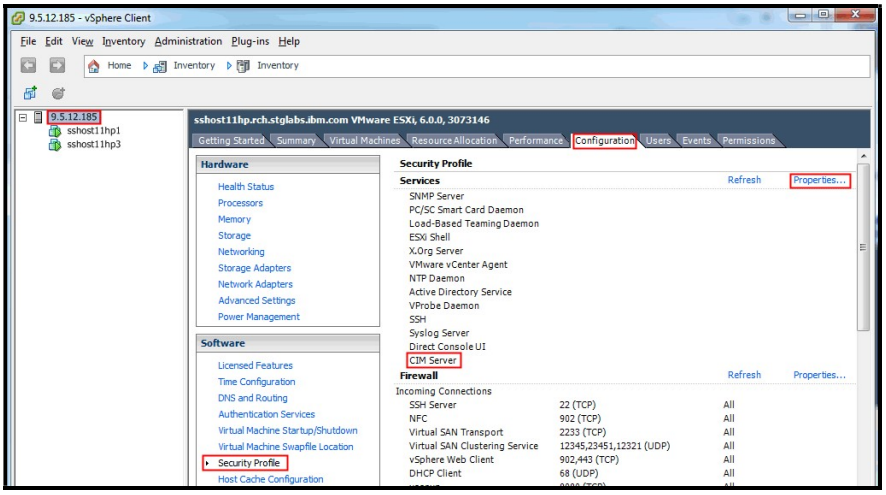
- CIM サーバー・サービスが開始され、状況は「**実行中**」状態になります。



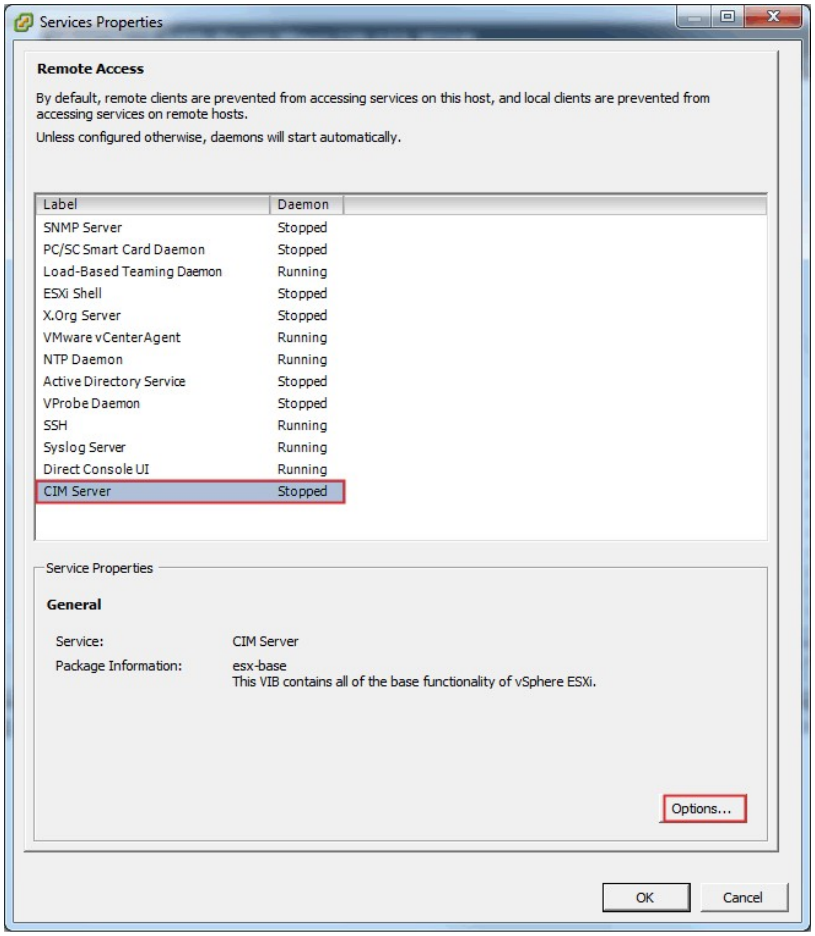
VMware vSphere Client の場合

- VMware vSphere Client を開始します。
- 左側のナビゲーション・ウィンドウで ESXi サーバー IP をクリックし、右ペインで「**構成**」タブをクリックします。

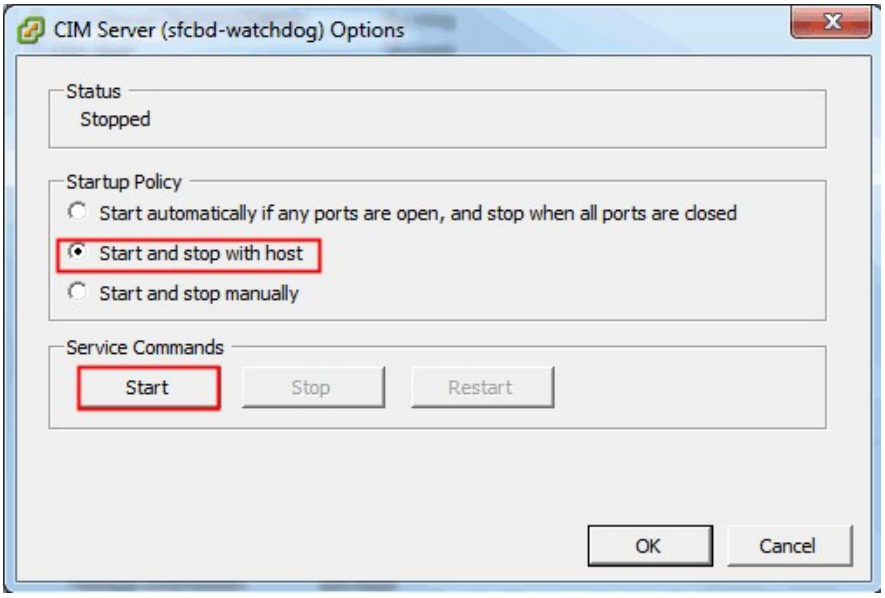
- 右ペインの「**ソフトウェア**」選択メニューから「**セキュリティー・プロファイル**」を選択します。「**CIM サーバー**」を含むサービスのセットが「**サービス**」 セクションに表示されます。



- 「**サービス**」セクションで「**プロパティー...**」項目を選択します。



- 「**CIM サーバー**」が「**停止**」状態の場合、それを選択して「**オプション...**」をクリックします。次のダイアログ・ウィンドウが表示されます。



- 「**開始ポリシー**」(「**ホストで開始と停止**」オプション) を選択し、「**開始**」をクリックして CIM サーバーを起動します。

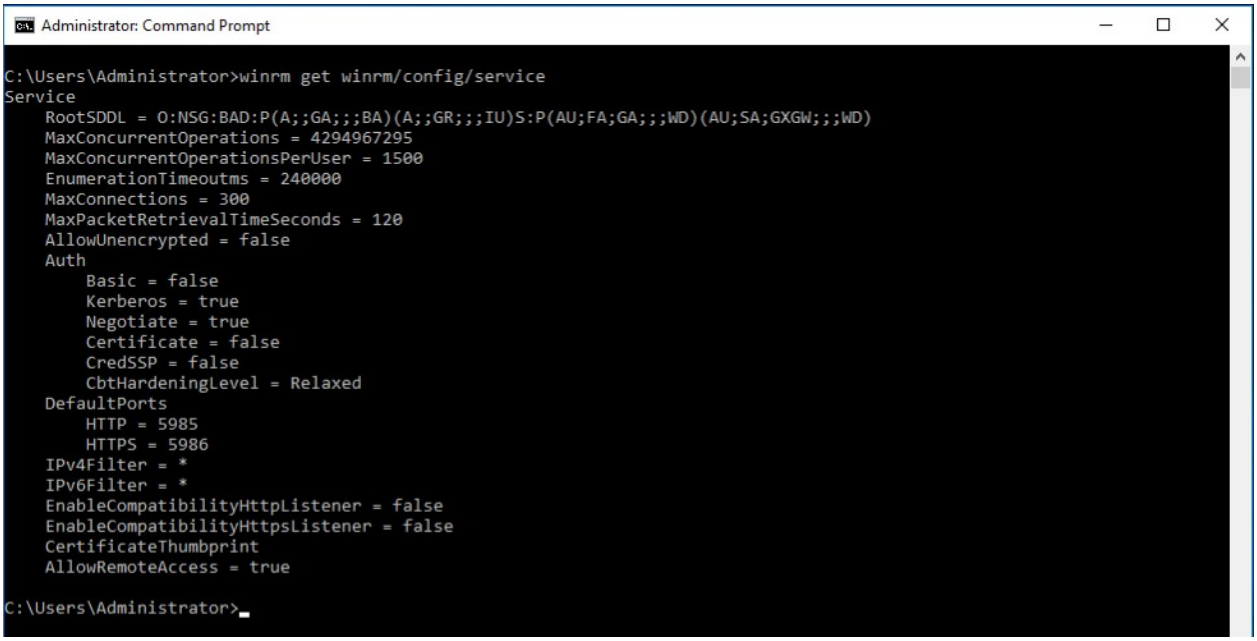
付録 D: WINRM を使用する Windows

Windows 2012 および 2016 Server の場合、WINRM サービスは自動的に開始されます。ただし、リモート管理はデフォルトでは有効になりません。ここでは、WINRM が自己署名証明書を使用するリモート接続を受け入れることができるようにするために必要な操作を簡単にまとめています。次の事柄が含まれます。

- WINRM が、ユーザー ID/パスワードで認証を行う HTTPS 接続を受け入れることができるようにする
- 自己署名証明書を、有効にされた WINRM の HTTPS リスナーと関連付ける
- ポート 5986 (デフォルト WINRM HTTPS ポート) でのインバウンド接続を許可するように Windows ファイアウォールを変更する

以下のコマンドを使用して、HTTPS を介したリモート接続を許可するように、WINRM を設定します。

- 次のコマンドを使用して、WINRM サービスの現在の状態を確認します:



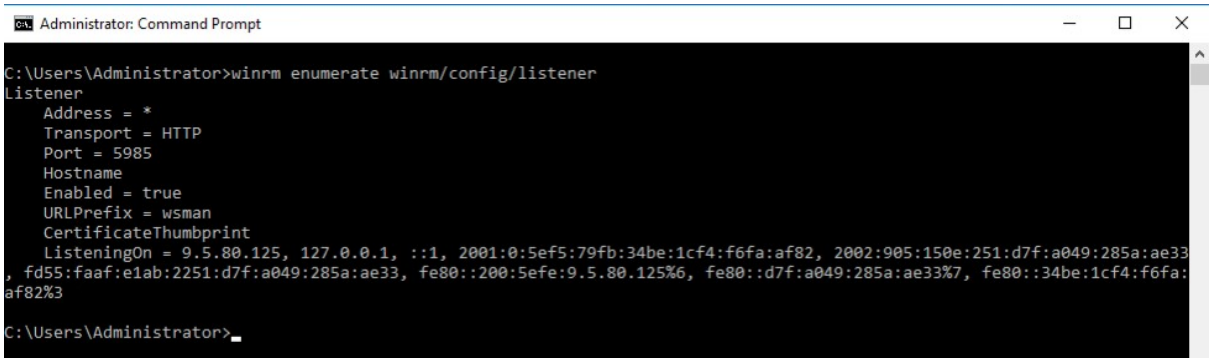
winrm get winrm/config/service

- **AllowUnencrypted** の値は *false* である必要があります。*true* になっている場合は、次のコマンドを使用して *false* に変更します:

  winrm set winrm/config/service @{AllowUnencrypted="false"}
- **Basic** の値は *true* である必要があります。*false* になっている場合は、 次のコマンドを使用して *true* に変更します:

  winrm set winrm/config/service/auth @{Basic="true"}
- 次のコマンドを使用して、WINRM が HTTPS リスナーを持っているか確認します。

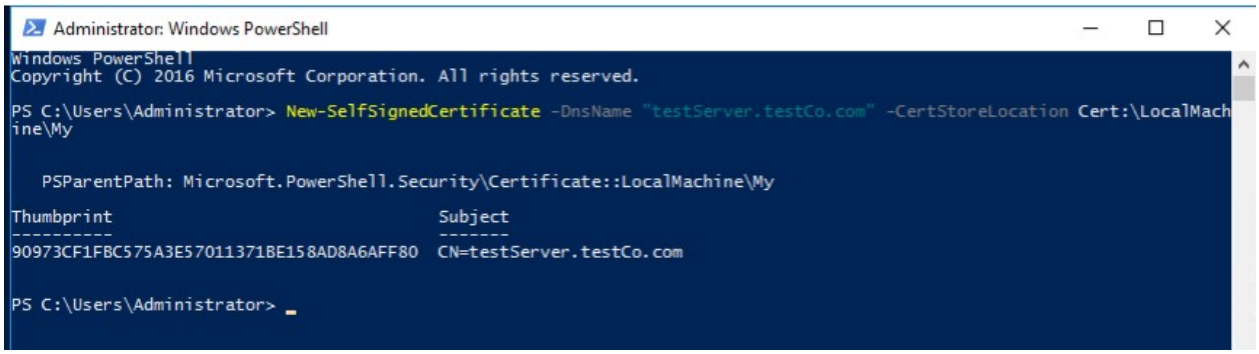
  winrm enumerate winrm/config/listener



- 上記のコマンドの例では、HTTP リスナーしか存在しないので、HTTPS リスナーを構成する必要があります。HTTPS リスナーが構成されていない場合に使用可能にするには、以下の手順に従ってください。
  - 以下のように、PowerShell を使用して自己署名証明書を作成します。

    New-SelfSignedCertificate -DnsName "myHost@myBusiness.com" -CertStoreLocation Cert:\LocalMachine\My

    > 上記の例の DnsName **(myHost@myBusiness.com)** を、Windows サーバーの Windows 完全修飾ドメイン名に置き換えます。
  - 次の手順で使用するので、証明書のサムプリントを保存します。



- 次のコマンドを使用して HTTPS リスナーを作成します:
  winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="myHost@myBusiness.com"; CertificateThumbprint="[COPIED_CERTIFICATE_THUMBPRINT]"}
- 次のコマンドを使用して、HTTPS が構成されたことを確認します:
  winrm enumerate winrm/config/listener
- WINRM への受信リモート接続を許可するように Windows ファイアウォールを変更します。
  - **「コントロール パネル」→「システムとセキュリティ」→「Windows ファイアウォール」** と移動します。
  - **「詳細設定」をクリックします。「セキュリティが強化された Windows ファイアウォール」**ウィンドウが表示されます。
  - **「受信の規則」**をクリックします。
  - **「操作」**メニューを選択し、**「新しい規則」**をクリックします。**「新規の受信の規則ウィザード」**が表示されます。
  - **「ポート」**を選択し、**「次へ」**をクリックします。
  - **「TCP」→「特定のローカル ポート」**を選択し、5986 を指定します。**「次へ」*をクリックします。***
  - **「接続を許可する」**オプションを選択し、**「次へ」**をクリックします。
  - **「ドメイン」、「プライベート」、「パブリック」**のチェック・ボックスが選択されていることを確認し、**「次へ」**をクリックします。
  - 新規規則に名前を指定し (Windows Remote Management (HTTPS-In) など)、**「完了」**をクリックします。

特記事項

IBM Corporation
Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589
Produced in the United States of America
August 2020.

本書は米国 IBM が提供する製品およびサービスについて作成したものです。 本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。

情報は予告なしに変更される場合があります。 日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。

IBM の将来の方向性および指針に関するすべての記述は、予告なく変更または撤回される場合があります。これらは目標および目的を提示するものにすぎません。

IBM、IBM ロゴ、POWER、System I、System p および i5/OS は、世界の多くの国で登録された International Business Machines Corporation の商標です。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

IBM ハードウェア製品は、新部品のみ、または新部品と再製部品の組み合わせにより製造されています。 ただし、いずれの場合であれ、IBM 所定の保証が適用されます。

本装置は FCC 規則の対象となります。購入者への最終納入の前に、該当する FCC 規則に適合する予定です。

IBM 以外の製品に関する情報は、その製品の供給者から入手したものです。

IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM のホーム・ページ、http://www.ibm.com もインターネットでご覧ください。

インターネット上の IBM System p のホーム・ページ (http://www.ibm.com/systems/p) もご覧ください。

インターネット上の IBM System I のホーム・ページ (http://www.ibm.com/systems/i) もご覧ください。

PSW03007-USEN-00