

バージョン 2.8.0.0

Technical Support Appliance
セットアップ・ガイド



注記

本書および本書で紹介する製品をご使用になる前に、[139 ページの『特記事項』](#)に記載されている情報をお読みください。

本書は、IBM® Technical Support Appliance のバージョン 2、リリース 8、モディフィケーション 0、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典：

Version 2.8.0.0
Technical Support Appliance
Setup Guide

発行：

日本アイ・ビー・エム株式会社

担当：

トランスレーション・サービス・センター

© Copyright International Business Machines Corporation 2011, 2021.

目次

図.....	vii
第 1 章概要.....	1
ユーザー・アカウントとユーザー・グループ.....	1
ディスカバリー・スコープとスコープ・セット.....	1
ディスカバリー資格情報.....	2
ディスカバリー・スケジュール.....	2
送信スケジュール.....	3
第 2 章前提条件.....	5
TSA イメージのダウンロード.....	5
TSA の要件.....	5
Web ブラウザーの要件.....	5
IBM サポートに接続するための構成要件.....	6
ディスカバリー環境における資格情報とソフトウェア要件.....	6
第 3 章 Technical Support Appliance のインストール.....	9
VMware ESXi Web インターフェースを使用したインストール.....	9
Microsoft Hyper-V への TSA のインストール.....	12
tsausr パスワードの作成 (必須).....	19
ネットワーク詳細の構成.....	19
第 4 章 Technical Support Appliance のセットアップ.....	21
Technical Support Appliance へのログイン.....	21
ご使用条件への同意.....	24
セットアップ・ウィザードを使用した初期設定.....	25
IBM への接続の設定.....	26
Technical Support Appliance の登録.....	28
クロックの設定.....	30
送信スケジュールのセットアップ.....	31
Technical Support Appliance の更新.....	32
ネットワーク設定の構成.....	33
基本ネットワーク設定の構成.....	34
拡張ネットワーク設定の構成.....	35
証明書のセットアップ.....	41
SSL サーバー証明書状況の表示.....	42
CSR の生成とダウンロード.....	42
カスタム証明書のインストール (署名者の使用).....	43
カスタム証明書のインストール (代替方式).....	44
デフォルト証明書の復元.....	45
インベントリー・データ・クリーンアップのスケジュール.....	46
第 5 章ディスカバリーと IBM への送信のセットアップ.....	49
ディスカバリー・スコープ.....	49
HMC 動的スコープ.....	49
VMware 動的スコープ.....	58
一般ディスカバリー・スコープ.....	68
スコープ・セットのインポート.....	73
ディスカバリー設定.....	74

接続設定の構成.....	74
ディスカバリー資格情報.....	75
資格情報の表示.....	75
資格情報の詳細の表示.....	76
資格情報の追加.....	76
資格情報の変更.....	79
資格情報の削除.....	80
ディスカバリー・スケジュール.....	80
ディスカバリー・スケジュールの表示.....	81
ディスカバリー・スケジュールの追加.....	81
ディスカバリー・スケジュールの変更.....	83
ディスカバリー・スケジュールの無効化.....	84
ディスカバリー・スケジュールの削除.....	84
ディスカバリーの実行.....	84
スコープでのディスカバリーの実行.....	87
ディスカバリー履歴.....	90
送信スケジュール.....	91
送信スケジュールの表示.....	91
送信スケジュールの変更.....	92
送信スケジュールの無効化.....	93
送信の実行.....	94
データ・スナップショット.....	94
インベントリー要約の表示.....	96
ディスカバリーの問題のデバッグ.....	97
認証状況.....	97
不明なデバイス.....	98

第 6 章 管理タスクのセットアップ..... 99

状況情報.....	99
アクティビティ・ログの表示.....	99
インベントリー・クリーンアップ・アーカイブの表示.....	100
パスワード.....	101
パスワードの変更.....	101
セキュリティ.....	101
セッション・タイムアウト設定の変更.....	102
パスワードの最長使用日数の変更.....	102
バックアップとリストア.....	102
更新.....	105
定期保守の有効化.....	107
ログとトレース.....	108
シャットダウン.....	109
ツール.....	110
ネットワーク・ツール.....	110
データベース・ツール.....	112
資料.....	113

第 7 章 Technical Support Appliance (TSA) について IBM サポートに問い合わせる. 115

IBM サポート・ポータルで Case をオープンする.....	115
IBM コール・センターでのサービス・リクエストの生成.....	115

付録 A Technical Support Appliance の設定..... 117

Technical Support Appliance の登録.....	117
IBM 接続の設定.....	119
クロックの設定.....	121
送信スケジュールのセットアップ.....	123
更新.....	124

付録 B DHCP ネットワーク詳細の構成	127
付録 C ユーザー・アカウントとユーザー・グループ	129
ユーザー・アカウントとユーザー・グループの表示.....	129
ユーザー・アカウントとユーザー・グループの追加.....	129
ユーザー・グループの追加.....	130
ユーザー・アカウントの追加.....	132
ユーザー・アカウントとユーザー・グループの変更.....	134
ユーザー・アカウントの変更.....	134
ユーザー・グループの変更.....	135
ユーザー・アカウントとユーザー・グループの削除.....	136
ユーザー・アカウントの削除.....	136
ユーザー・グループの削除.....	136
ユーザー補助	137
特記事項	139
商標.....	139



1. VM の作成/登録.....	9
2. 作成タイプの選択.....	10
3. OVF および VMDK ファイルの選択.....	10
4. ストレージの選択.....	11
5. デプロイメント・オプション.....	11
6. 設定の選択内容の確認.....	12
7. Hyper-V マネージャー	13
8. 仮想マシン名.....	13
9. 世代の指定.....	14
10. 開始メモリー.....	15
11. ネットワーキングの構成.....	16
12. 仮想ハード・ディスクの接続.....	17
13. 要約.....	18
14. Hyper-V マネージャー	18
15. パスワードの変更.....	19
16. 新規パスワード.....	19
17. ネットワーク構成のセットアップ.....	19
18. ネットワーク構成.....	20
19. ログイン.....	22
20. パスワードの変更.....	22
21. ご使用条件.....	24
22. セットアップ・ウィザード	25
23. IBM への接続.....	26

24. 登録.....	28
25. クロック.....	30
26. 毎週 (日曜日 - 土曜日).....	31
27. 使用可能な更新.....	32
28. 使用可能な更新はありません.....	33
29. セットアップ・ウィザードが完了しました	33
30. ネットワーク.....	34
31. 「ネットワーク (拡張)」 ページへのアクセス.....	36
32. ネットワーク (拡張) - グローバル.....	37
33. ネットワーク (拡張) - ネットワーク・インターフェース.....	38
34. ネットワーク (拡張) - DNS 設定.....	39
35. ネットワーク (拡張) - ネットワーク経路.....	40
36. 新規ネットワーク経路.....	41
37. SSL サーバー証明書状況.....	42
38. 証明書署名要求.....	43
39. カスタム証明書のインストール.....	44
40. カスタム証明書のインストール.....	45
41. アプライアンス証明書をデフォルトに設定.....	45
42. インベントリー・クリーンアップのスケジュール.....	46
43. HMC 動的スコープ.....	49
44. HMC 動的スコープ・セットの表示.....	50
45. HMC 動的スコープ・セットの追加.....	52
46. 例: Linux LPAR のアクセス情報の入力.....	53
47. HMC 動的スコープ・セットのインポート.....	55
48. VMware 動的スコープ	59

49. VMware 動的スコープ・セットの表示.....	60
50. VMware 動的スコープ・セットの追加.....	61
51. Linux 仮想マシンのアクセス情報の入力.....	62
52. Windows 仮想マシンのアクセス情報の入力.....	63
53. VMware 動的スコープ・セットのインポート.....	64
54. ディスカバリー・スコープ・セット.....	69
55. 一般ディスカバリー・スコープ	70
56. スコープ・セットのインポート.....	74
57. 新規ディスカバリー資格情報.....	75
58. ディスカバリー資格情報の詳細.....	76
59. 新規ディスカバリー資格情報.....	77
60. ディスカバリー・スケジュール.....	81
61. ディスカバリー・スケジュールの追加.....	82
62. 毎週 (日曜日 - 土曜日).....	83
63. 特定のスコープでのディスカバリーの実行.....	85
64. HMC 動的スコープ.....	86
65. VMware 動的スコープでのディスカバリーの実行.....	86
66. ディスカバリー・スコープ.....	87
67. 特定のスコープでのディスカバリーの実行.....	88
68. HMC 動的スコープ.....	88
69. 特定のスコープでのディスカバリーの実行.....	89
70. VMware 動的スコープ.....	89
71. VMware 動的スコープでのディスカバリーの実行.....	90
72. ディスカバリー履歴.....	91
73. 送信スケジュールの編集.....	92

74. 毎週 (日曜日 - 土曜日).....	93
75. 今すぐ送信を実行.....	94
76. データ・スナップショット	95
77. データ・スナップショット生成日	95
78. インベントリー要約.....	96
79. インベントリー要約の詳細.....	97
80. 認証状況.....	98
81. アクティビティ・ログ.....	99
82. インベントリー・クリーンアップ・アーカイブ.....	100
83. バックアップとリストア.....	104
84. 更新.....	105
85. 使用可能な更新.....	106
86. 今すぐ更新を実行.....	107
87. ログとトレース.....	108
88. シャットダウン.....	109
89. ネットワーク・ツール.....	111
90. 資料.....	113
91. 登録.....	118
92. IBM 接続.....	120
93. クロック.....	122
94. 送信スケジュールの編集.....	123
95. 毎週 (日曜日 - 土曜日).....	124
96. 更新.....	125
97. 使用可能な更新.....	125
98. 今すぐ更新を実行.....	126

99. ネットワーク構成のセットアップ.....	127
100. ネットワーク構成.....	127
101. DHCP IP アドレス.....	128
102. グループ.....	130
103. ユーザー・グループの追加.....	131
104. ユーザー・アカウントとグループ.....	132
105. ユーザー・アカウントの追加.....	133
106. 管理ユーザー・アカウントの変更.....	135

第1章 概要

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・センター内のアプライアンス、ミドルウェア、サーバー、ネットワーク・コンポーネントの間の複雑な関係についての知見を得ることができます。

TSA には、セットアップおよびシステムとデータへのアクセス 権限をカスタマイズするための Web ベースのユーザー・インターフェース (UI) が含まれます。この UI を使用して、データのディスカバリーと送信のスケジュールを変更することもできます。

ディスカバリー・プロセスの一環で、TSA はまず、ディスカバリー資格情報を使用せずに、定義済みのスコープ内でエンドポイントの検出を試みます。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。

一般スコープ・セットを使用すると、個々の IT ネットワーク要素をディスカバーできます。スコープ・セットには、個々のネットワーク要素の場所を IP アドレスまたはホスト名、IP アドレスの範囲、ネットワークまたはサブネットを使用して示すスコープが 1 つ以上含まれています。

HMC および VMware vCenter Server / ESXi には、動的スコープ・セットを使用することをお勧めします。動的スコープ・セットは、個々の LPAR/仮想マシンに対してディスカバリー・スコープを作成して管理するよりも、TSA の構成作業が少なく済みます。また、LPAR や仮想マシンが時間の経過とともに追加されたり削除されたりする環境でも、動的スコープ・セットを使用すれば、スコープ・セットを変更することなく変化に対応することができます。

ユーザー・アカウントとユーザー・グループ

なんらかの TSA 機能を実行するには、一定の権限レベルが必要となります。認証済みユーザーが適切な権限レベルがない状態で機能を実行しようとするすると、エラーが表示されて機能は実行されません。

組織内では、さまざまな職種に対する役割を作成できます。ある操作を行うための許可が、特定の役割に対して割り当てられます。TSA ユーザーは特定の役割を割り当てられます。この役割を割り当てられることによって、特定のシステム機能を実行するために必要な許可を取得します。このようにして、役割に割り当てられたすべてのユーザーはその役割に関連付けられた権限レベルを持つようになります。また、ユーザーを役割に追加したり、ユーザーをある役割から別の役割に変更したり、ユーザーを役割から削除することは簡単です。

TSA では、関連付けられた権限レベルを持つユーザー・グループを使用して役割が管理されます。ユーザーはユーザー・アカウントで管理されます。ユーザー・アカウントには、1 つまたは複数のユーザー・グループにあるメンバーシップを割り当てることができます。これらのメンバーシップを通して、ユーザーは特定の機能を実行するための権限レベルを取得します。

さらに、ユーザー・グループを選択したスコープ・セットに制限することができます。スコープ・セットは、TSA がディスカバー可能な IT 要素を特定する IP アドレスまたはホスト名、アドレス範囲、サブネットのコレクションです。ユーザー・グループにスコープ・セット制限を指定することは、ユーザー・グループのメンバーのアクセスをさらに制限する 1 つの方法です。例えば、特定ユーザー・グループに関連付けられた権限レベルとスコープ・セット制限を組み合わせることで、Linux® システムの保守の責任を持つユーザーといった、プラットフォーム固有のユーザー・グループを作成することが可能です。

ディスカバリー・スコープとスコープ・セット

ディスカバリー・スコープは、TSA のディスカバー対象とするリソースを識別します。ディスカバリー・スコープはディスカバリー・スコープ・セットにグループ化されます。

ディスカバリー中にアクセスされるリソースを定義する IP アドレスまたはホスト名、IP アドレスの範囲、ネットワークまたはサブネットを使用することで、ディスカバリー・スコープを指定できます。ディスカ

バリー・スコープは最小で単一の IP アドレスまたはホスト名に、最大で IP アドレスの範囲またはネットワークにできます。

スコープ・セットの作成を簡単にするために、ファイルを使用して IP アドレスおよびホスト名が含まれるリストをインポートできます。詳細については、[73 ページの『スコープ・セットのインポート』](#)のセクションを参照してください。

ディスカバリー・スコープに含まれる IP アドレスの数が増えるほど、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・スコープ・セットを有効/無効にしたり、スコープ・セット内のスコープから IP アドレスや IP アドレスの範囲、ネットワークまたはサブネットを除外したりして、ディスカバリーのサイズを変更することができます。

注: パフォーマンスを向上させるために、スコープ・セット内の IP アドレス (IP アドレス、範囲、サブネット、および除外) の累積数を 400 以下に制限してください。

注: ホスト名を使用して定義されたスコープまたはインポートのリストには、スコープが作成または編集されるたびに IP アドレスに解決されるホスト名が含まれます。TSA は、ネットワーク・リソースのディスカバリー時にホスト名を使用しません。

関連タスク

[ユーザー・アカウントとユーザー・グループの追加](#)

ユーザー・アカウントとユーザー・グループを追加して、TSA 機能へのアクセスを制御できます。

ディスカバリー資格情報

ディスカバリー資格情報は、ディスカバリー中にリソースにアクセスするために TSA が使用するユーザー名、パスワードまたは SSH 鍵、Simple Network Management Protocol (SNMP) コミュニティー文字列のコレクションです。

ディスカバリーを行うリソースに対して、ディスカバリー資格情報をセットアップして保守する必要があります。提供するアクセス情報は資格情報のタイプによって異なりますが、通常は少なくとも名前とパスワードまたは SSH 鍵が含まれます。

ディスカバリー資格情報はすべてのスコープ・セットに適用することも、単一のスコープ・セットに制限することもできます。単一のスコープ・セットに適用される資格情報を定義すると、パフォーマンスが向上し、無効なログイン試行を防止することでアカウントがロックされることがなくなります。

リソースにアクセスするとき、TSA は特定スコープに関連付けられた各資格情報を「**ディスカバリー資格情報**」ページにリストされた順に使用します。これはリソースへの TSA アクセスが許可されるまで行われます。例えば、コンピューター・システムにアクセスしているとき、TSA はコンピューター・システムの資格情報リストに指定され、スコープ・セットに関連付けられた最初のユーザー名とパスワードを使用します。特定のコンピューター・システムに対してユーザー名とパスワードが正しくない場合は、TSA は自動的にコンピューター・システムの資格情報リストにある次のユーザー名とパスワードを使用します。

ヒント: 資格情報を保存する前に、**コンピューター・システム**、**コンピューター・システム (Windows)**、**SNMP**、**SNMPV3** などのシステム・タイプに対する有効な資格情報を指定したかどうかをテストできます。このテストにより、資格情報が有効に定義されていることを確認できます。

ヒント:

- AIX® や Windows などの特定の同じタイプのすべてのデバイスに対して、共通パスワードを用いたサービス・アカウントを使用してください。次に、このデバイス・タイプのすべてのインスタンスをディスカバリーするための単一の資格情報を定義できます。
- 有効期限のないパスワードを持つアカウントを使用します。
- 必要な場合、SSH 鍵を使用します。

ディスカバリー・スケジュール

ディスカバリー・データが常に最新かつ正確になるように、ディスカバリーはスケジュールされた日時に実行されます。TSA には、定義されたすべてのスコープ・セットのディスカバリーを実行するデフォルトの「フル・ディスカバリー」スケジュールがあります。このデフォルトのスケジュールは必要に応じて変更できます。また、複数のスケジュールを作成して、各スコープ・セットのディスカバリーを複数の異なる

る日時に分散させることもできます。詳細、履歴、前回実行されたディスカバリーの状態を表示することもできます。

ディスカバリー・スケジュールを変更するときには、名前、スコープ・セット、開始時刻、ディスカバリーの頻度を指定します。ディスカバリー・スケジュールがデフォルトのディスカバリーの場合、開始時刻とディスカバリーの頻度のみを変更するだけで構いません。オンデマンドでディスカバリーを実行することもできます。

ディスカバリーの期間は、リソースの数と複雑さを含む要素の数によって異なり、完了までに最大 72 時間かかる場合があります。

送信スケジュール

IBM が最新かつ正確な情報を確実に保持するために、ディスカバリー・データは安全な状態にパッケージされ、スケジュールされた日時に IBM サポートに送信されます。TSA にはデフォルトの送信スケジュールが設定されていますが、これは必要に応じて変更することができます。オンデマンドで送信を実行することもできます。前回実行された送信の状態を表示することもできます。

送信の経過時間は、ディスカバリー・データの容量に基づいて異なります。

第 2 章 前提条件

TSA をセットアップして使用するには、ディスクバリー環境で要求される資格情報や IBM サポートに接続するための構成要件といった前提条件を満たしていることを確認する必要があります。

TSA イメージのダウンロード

TSA イメージには、Microsoft Hyper-V サーバー用 [TSA-HYPERV-<version>] と VMware サーバー用 [TSA-VMWARE-<version>] があります。

ダウンロード手順については、<https://ibm.biz/TSAdemo> を参照してください。

TSA の要件

TSA をセットアップして使用する前に、以下の前提条件を満たしていることを確認してください。

x86 64 ビットのハードウェア

TSA は x86 64 ビット・システム上にロードする必要があります。

ハイパーバイザー

TSA では VMware ESXi または Microsoft Hyper-V が必要になります。

注：現時点で製造元によってサポートされているバージョンの ESXi または Hyper-V のみを使用してください。

プロセッサ

TSA では最小 2.26 GHz、4 コアのプロセッサが必要です。

CPU

TSA では 4 つの 64 ビット CPU が必要です。

メモリー

TSA では 16 GB メモリーが必要です。

直接アクセス・ストレージ・デバイス (DASD)

TSA では 150 GB の DASD が必要です。

ネットワーク

TSA では 1 ギガビットのイーサネット・アダプターが必要です。

Web ブラウザーの要件

ディスクバリーと送信をセットアップおよびモニターするには、Web ベースのユーザー・インターフェースを使用します。

TSA では以下のインターネット・ブラウザがサポートされます。

- Mozilla Firefox V78.4.0 Extended Support Release (ESR)
- Microsoft Edge V86.0.622.56 for Windows 10
- Google Chrome V86.0.4240.111 (64 ビット)

これらのブラウザは以下のサイトからダウンロードできます。

- [Mozilla Firefox](http://www.mozilla.org/products/firefox/) (http://www.mozilla.org/products/firefox/)
- [Microsoft Edge](https://www.microsoft.com/en-us/edge) (https://www.microsoft.com/en-us/edge)
- [Google Chrome](https://support.google.com/chrome/answer/95346?hl=en) (https://support.google.com/chrome/answer/95346?hl=en)

IBM サポートに接続するための構成要件

TSA は、直接接続で、またはユーザーが用意したプロキシ (IBM との通信を許可するように構成されている必要があります) を介して IBM サポートに接続できます。プロキシを使用している場合は、TLS/SSL インスペクションはサポートされません。プロキシを介したすべての要求は、TLS/SSL によって停止されることなく IBM に直接フローを許可される必要があります。

「ネットワーク接続」の表で説明されるように、IBM サーバーのホスト名と IP アドレスへの接続を、お客様のファイアウォールが許可するようにしておく必要があります。お客様のネットワークが IBM サーバーへのアクセスを許可しない場合、IBM サポートへの TSA トランザクションが失敗します。

DNS 名	IP アドレス	ポート	プロトコル
esupport.ibm.com	129.42.54.189	443	HTTPS (IBM へ)
	129.42.56.189		
	129.42.60.189		

IBM サーバー環境は完全に NIST SP800-131A 準拠であり、TLS 1.2 プロトコル、SHA-256 以上の強度のハッシュ関数、2048 ビット以上の強度の RSA 鍵をサポートしています。

注: SSL インスペクションはサポートされていません。プロキシで SSL インスペクションを使用している場合は、これらのフローに対して無効にしてください。

Blue Coat プロキシの場合は、IBM サーバーに対する「プロトコル検出」を無効にしてください。以下の構成ルールを追加します。

- url.domain=esupport.ibm.com detect_protocol (none)
- url.address=129.42.54.189 detect_protocol (none)
- url.address=129.42.56.189 detect_protocol (none)
- url.address=129.42.60.189 detect_protocol (none)

ディスカバリー環境における資格情報とソフトウェア要件

お客様の環境でエンドポイントまたはリソースのディスカバリーを行うには、TSA がそれらのリソースに対するアクセス権限を持っている必要があります。TSA がリソースにアクセスする際に使用する各リソースにサービス・アカウントを作成することを推奨します。

リソース上にサービス・アカウントを作成したら、そのサービス・アカウントのリソース上に定義された資格情報に一致する資格情報を TSA 上に定義して保持する必要があります。TSA はそれらの資格情報を使用してリソースにアクセスします。資格情報の要件は環境やディスカバー対象リソースのタイプによって異なりますが、通常はユーザー名とパスワードまたは SSH 鍵を含みます。一部のリソースには固有のソフトウェア要件が含まれる場合があります。

資格情報のタイプ	アクセス情報
コンピューター・システム	<p>ユーザー名: デバイスにアクセスするためのユーザー名。</p> <p>パスワード/パスフレーズ: デバイスにアクセスするためのパスワード/パスフレーズ。</p> <p>認証タイプ: デバイスでの認証のタイプ。</p> <ul style="list-style-type: none">• パスワード - 指定されたパスワードを使用します。• PKI - 特定のスコープ・セットに関連付けられた SSH 鍵を使用します。

資格情報のタイプ	アクセス情報
コンピューター・システム (Windows)	<p>ユーザー名: Windows コンピューター・システムにアクセスするためのユーザー名。</p> <p>パスワード: Windows コンピューター・システムにアクセスするためのパスワード。</p>
ネットワーク要素 (SNMP)	<p>コミュニティ文字列: デバイス用のコミュニティ文字列。</p>
ネットワーク要素 (SNMPV3)	<p>ユーザー名: デバイスにアクセスするためのユーザー名。</p> <p>パスワード: デバイスにアクセスするためのパスワード。</p> <p>プライベート・パスワード: SNMP にデータ暗号化が設定されている場合に使用されるパスワード。</p> <p>認証プロトコル: SNMP によって使用される認証プロトコルのタイプ。</p> <ul style="list-style-type: none"> • なし • MD5 • SHA
その他 (Cisco デバイス)	<p>ユーザー名: Cisco デバイスにアクセスするためのユーザー名。</p> <p>パスワード: Cisco Device 用のパスワード。</p> <p>イネーブル・パスワード: Cisco Device 用のイネーブル・パスワード。</p>
その他 (Cisco Works)	<p>ユーザー名: CiscoWorks サーバーにアクセスするためのユーザー名。</p> <p>パスワード: CiscoWorks サーバーにアクセスするためのパスワード。</p>

注：資格情報とソフトウェア要件についての詳細な情報は、「構成アシスタント・ガイド」を参照してください。

第 3 章 Technical Support Appliance のインストール

TSA には事前インストール済みのソフトウェアが含まれます。TSA はパッケージ化され、VMware インストール用にイメージ形式で、または Microsoft Hyper-V インストール用に VHDX イメージ形式で配布されます。VMware の場合、TSA は VMware Web インターフェイス (ESXi 用) を使用してインストールできます。Hyper-V の場合、TSA は Hyper-V マネージャーを使用してインストールできます。このセクションでは、これらの方法を使用して TSA をインストールする手順について説明します。

VMware ESXi Web インターフェイスを使用したインストール

始める前に

TSA でハードウェアを制御するためには、VMware ESXi 6.5 以上がロードされている必要があります。

このタスクについて

以下の手順に従って TSA イメージをインストールします。

手順

1. VMware ESXi Web インターフェイスを使用して、ESXi システムにログインします。
2. 「**Create/Register VM**」をクリックします。仮想マシンの新規作成ウィザードが表示されます。



図 1. VM の作成/登録

3. 「作成タイプの選択」画面で、「**OVF または OVA ファイルから仮想マシンをデプロイ**」オプションを選択して「次へ」をクリックします。

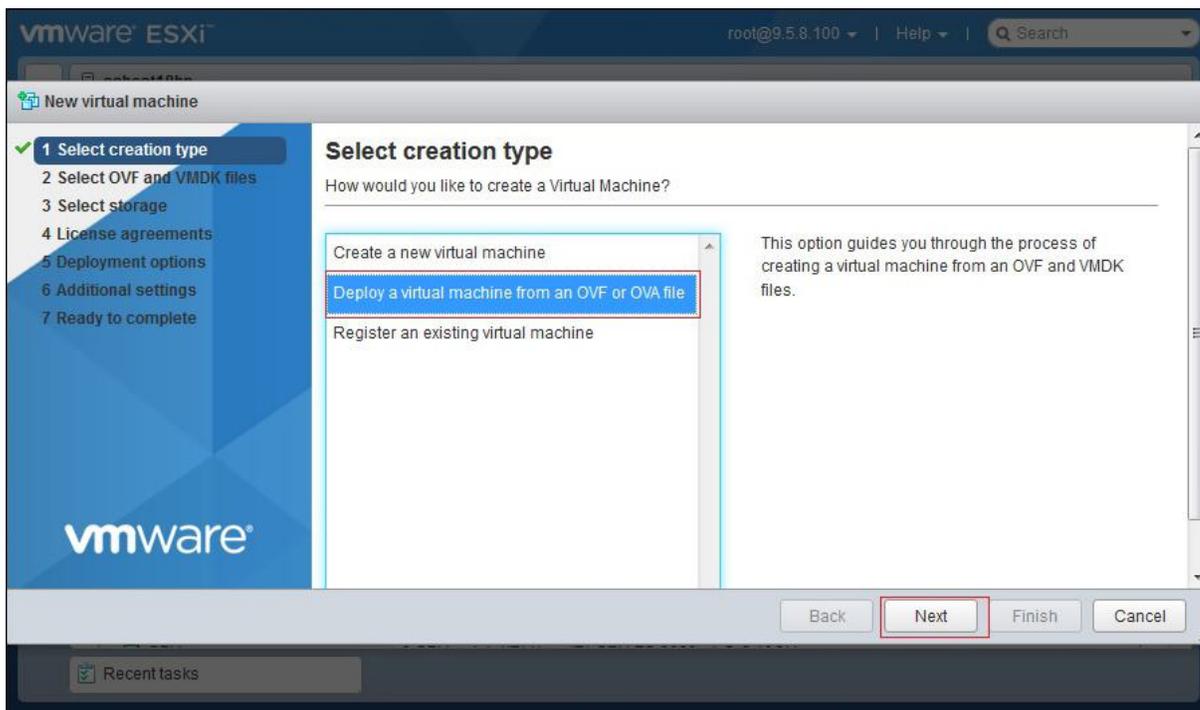


図 2. 作成タイプの選択

4. **OVF** および **VMDK** ファイルの選択画面で、「クリックしてファイルを選択するか、ドラッグ/ドロップします」ボックス内をクリックし、Fix Central からダウンロードしたイメージ・ファイルを選択します。仮想マシンの固有の名前を入力するか、デフォルト値を使用し、「次へ」をクリックします。

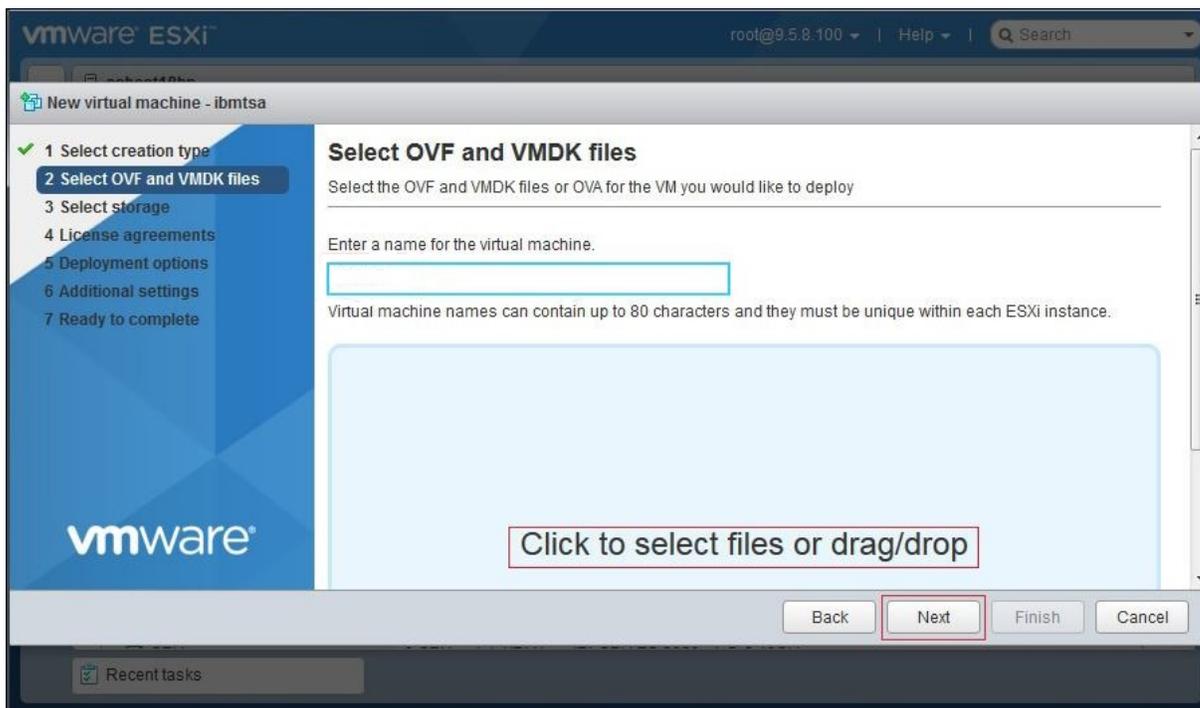


図 3. OVF および VMDK ファイルの選択

5. 「**Select storage**」画面で、構成ファイルとディスク・ファイルを格納するデータ・ストアを、表示されるリストから選択します。次に、「**Next**」をクリックします。

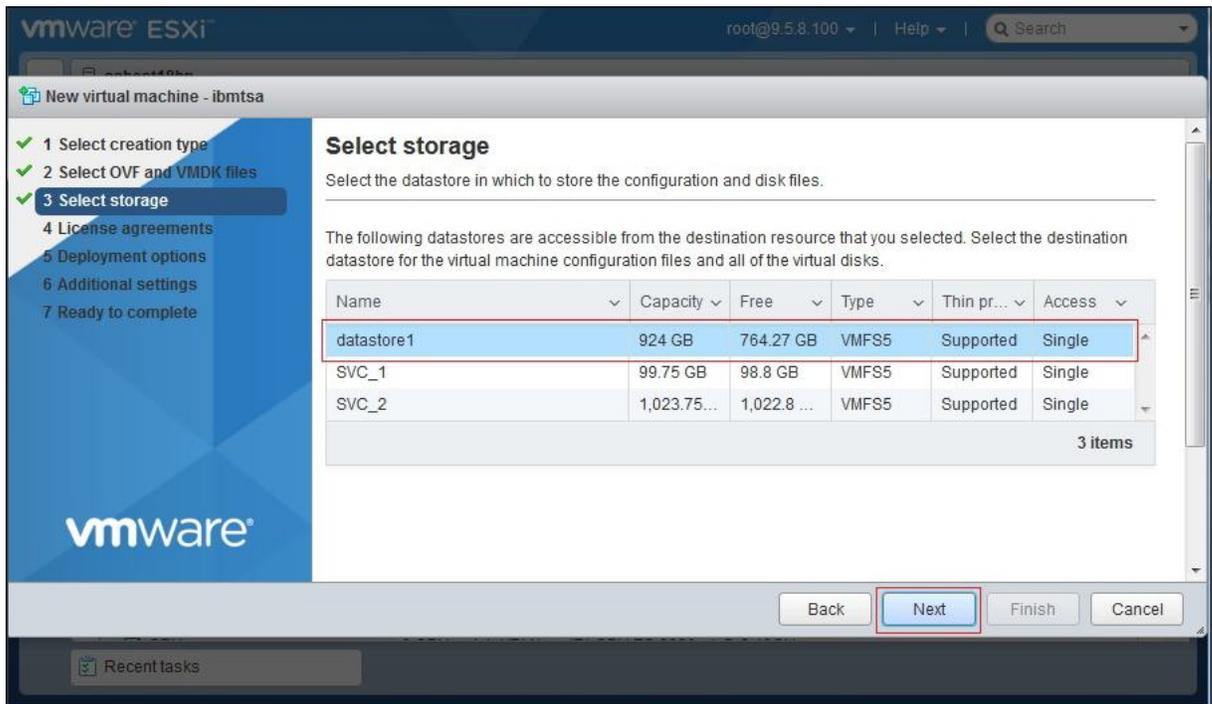


図 4. ストレージの選択

6. 「**Deployment options**」画面で、「**VM Network**」ドロップダウン・リストからネットワーク・マッピングを選択します。

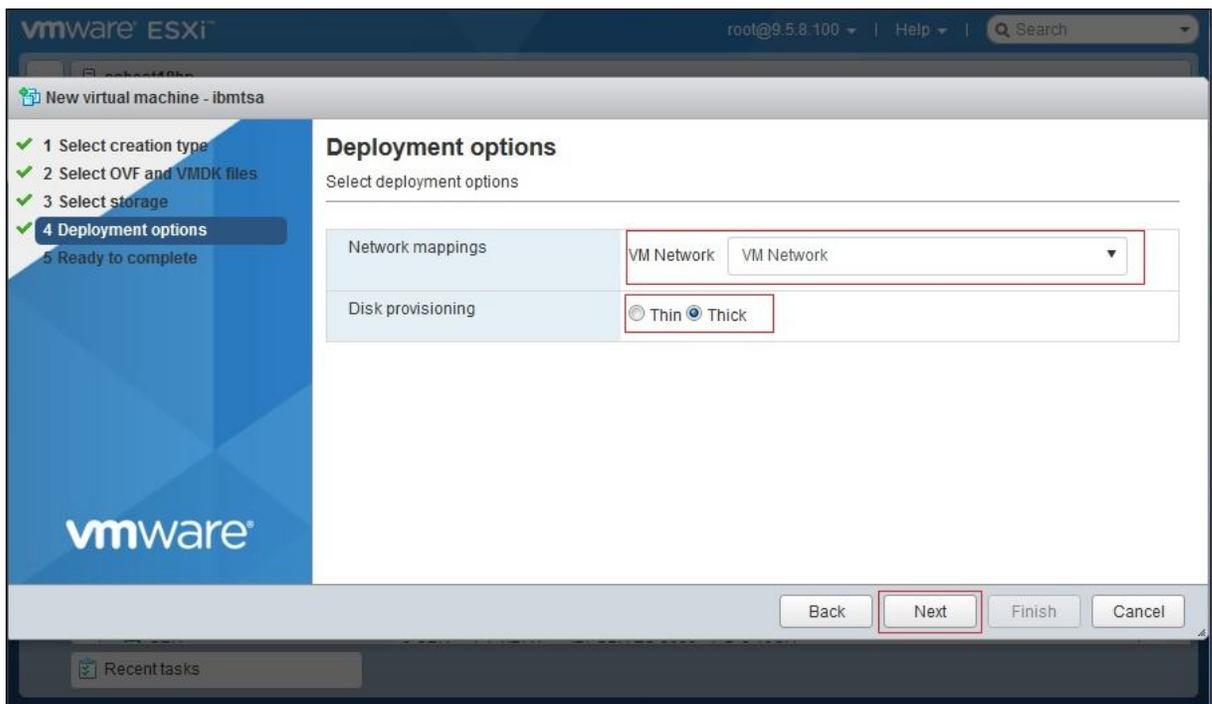


図 5. デプロイメント・オプション

7. ディスクのプロビジョニングに「**Thick**」オプションを選択し、「**次へ**」をクリックします。
8. 「**Ready to complete**」画面で、指定したすべての設定を確認します。何らかの変更が必要な場合は、「**Back**」をクリックし、関連オプションに変更を加えます。問題がなければ、「**Finish**」をクリックします。

重要: 仮想マシンのデプロイ中はブラウザのページを更新しないでください。

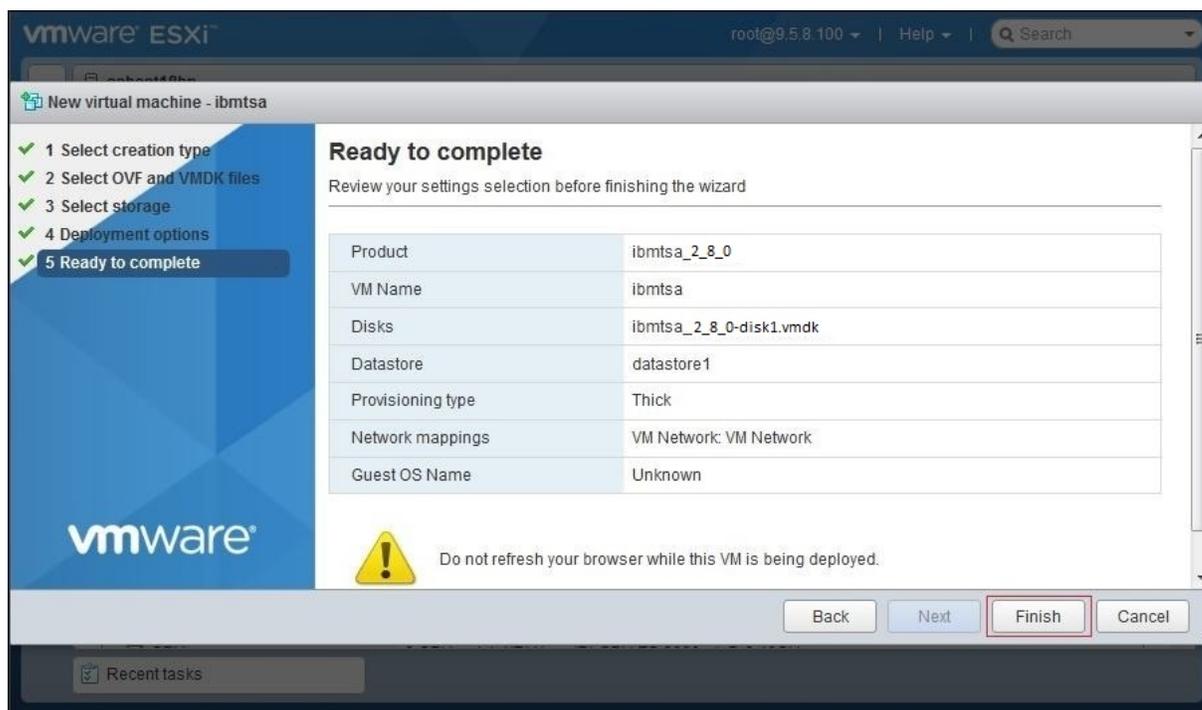


図 6. 設定の選択内容の確認

TSA 仮想マシンがシステムにインストールされます。

9. TSA コンソールで、「**ibmtsa ログイン**」に「**tsausr**」、「パスワード」に「**configTsa**」と入力します。
10. 必須: ログイン・パスワードを変更するために、「19 ページの『**tsausr パスワードの作成 (必須)**』」セクションにリストされているステップを続けて実行します。
11. インストールを完了するために、「19 ページの『**ネットワーク詳細の構成**』」セクションにリストされているステップを続けて実行します。

Microsoft Hyper-V への TSA のインストール

始める前に

TSA を Hyper-V 上にセットアップして使用する前に、以下の前提条件を満たしていることを確認してください。

- Hyper-V Server 2016 または 2019
- Hyper-V マネージャー
- Hyper-V マネージャー経由で仮想ネットワーク・スイッチが作成済み

このタスクについて

以下の手順に従って TSA を Hyper-V 上にインストールします。

手順

TSA 2.5 を Hyper-V 上にインストールするには、以下の手順に従ってください。

1. TSA イメージのダウンロード後、*ibmtsa_2800.zip* ファイルから *ibmtsa_2800.vhdx* ファイルを解凍し、Hyper-V サーバー上のディレクトリにそのファイルを移動します。
2. Hyper-V マネージャーを開始して、クライアント・システムから Hyper-V サーバーに接続します。
3. 「**Browse**」をクリックして、システムに保存されているイメージを選択します。

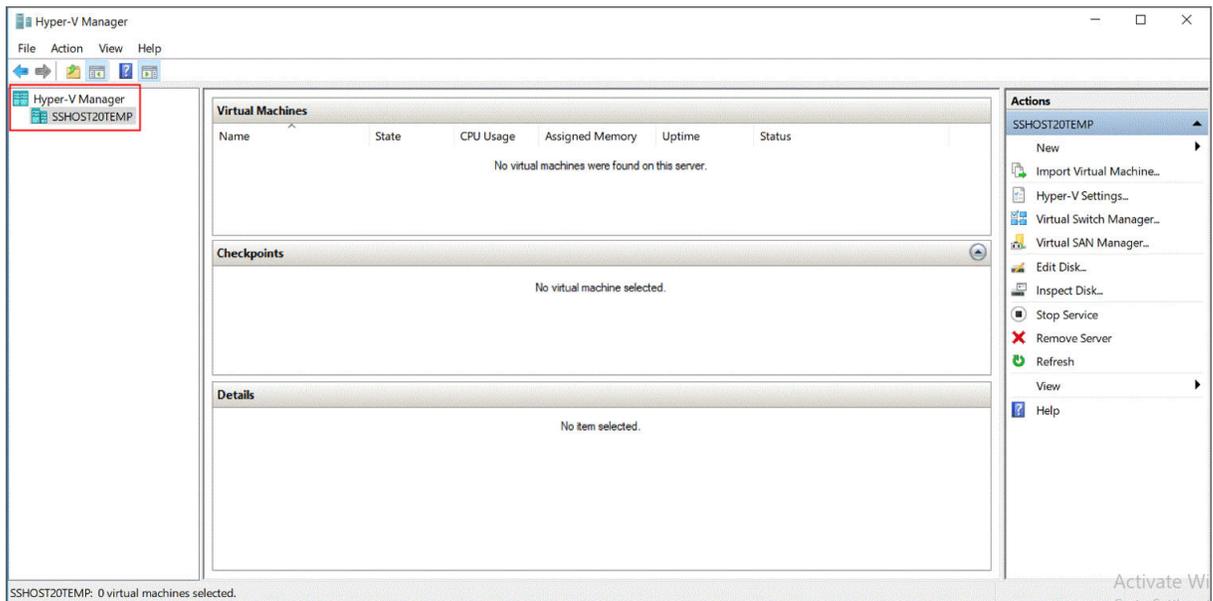


図 7. Hyper-V マネージャー

4. 「**Action**」メニューで、「**New**」 → 「**Virtual Machine**」を選択します。仮想マシンの新規作成ウィザードが表示されます。
5. 新規仮想マシンの名前を「**Name**」に入力し、「**Next**」をクリックします。

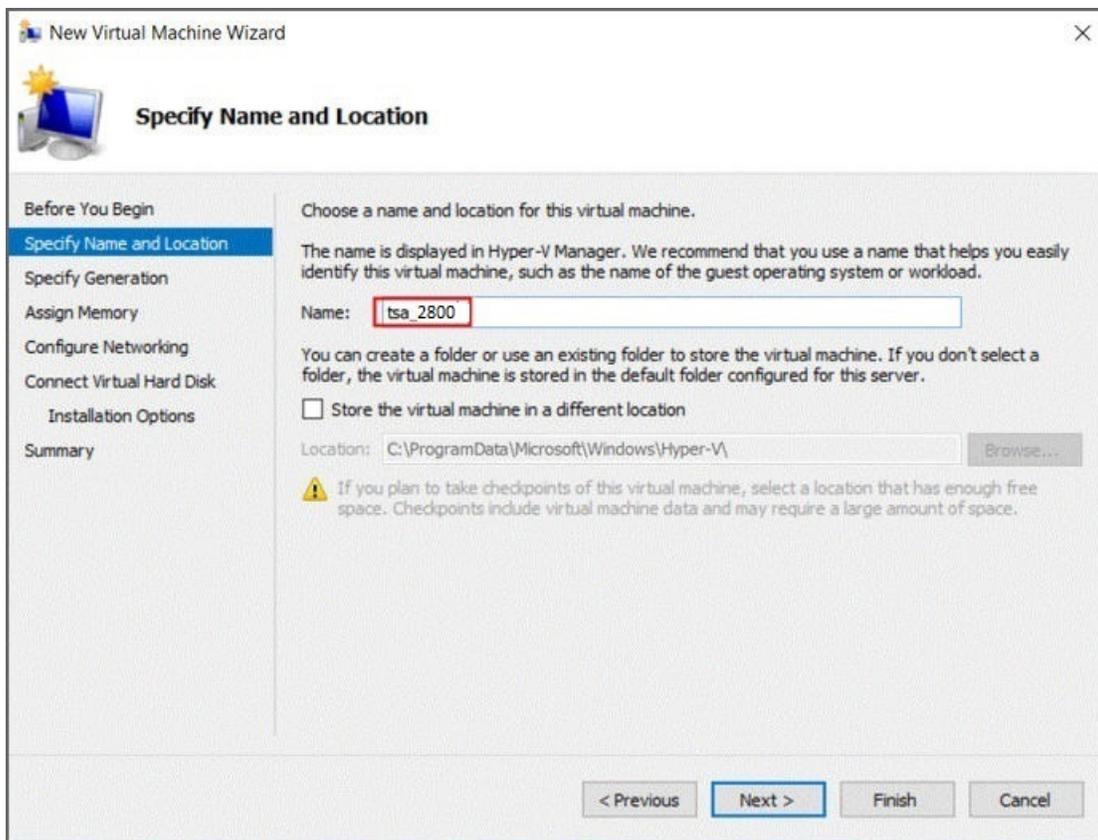


図 8. 仮想マシン名

6. 仮想マシンの世代として「**Generation 1**」を選択して「**Next**」をクリックします。

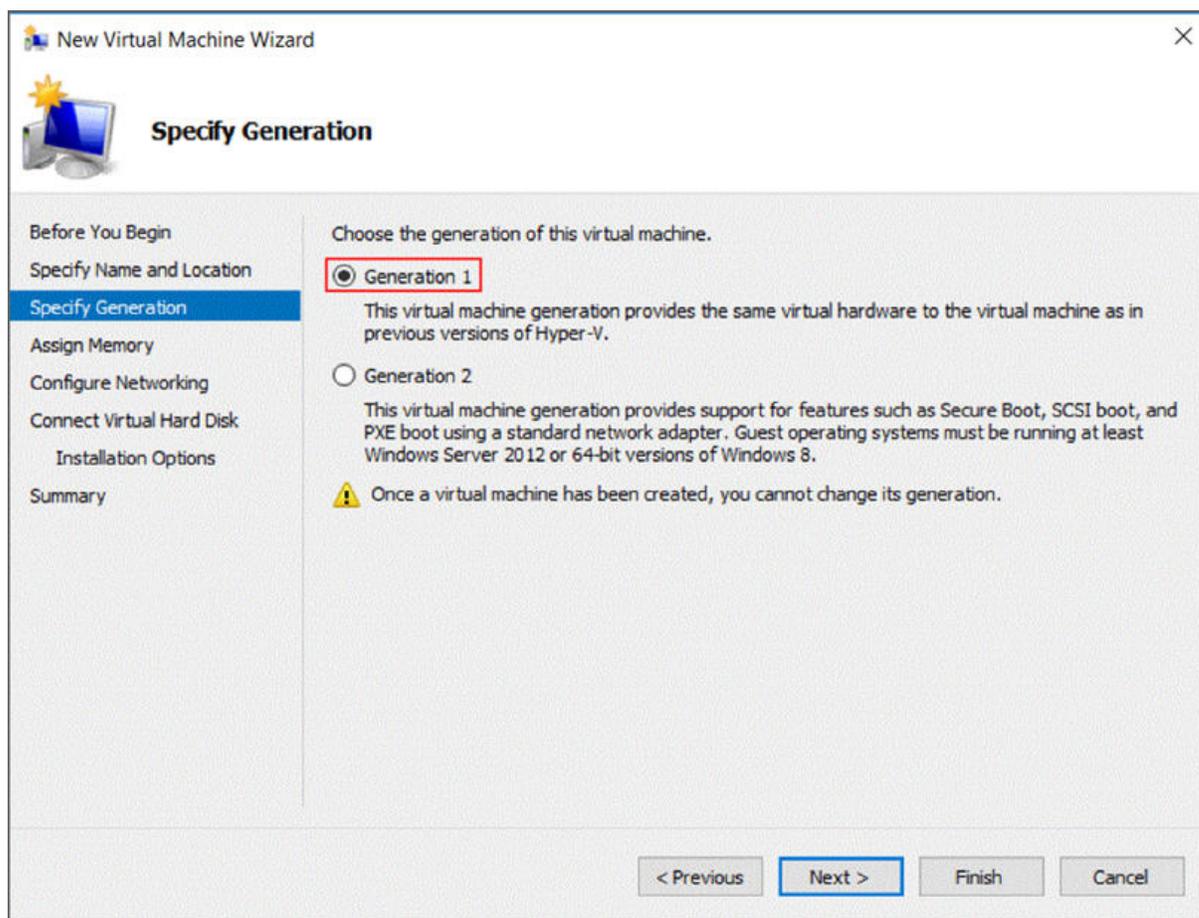


図 9. 世代の指定

7. 「**Startup memory**」を 16384 MB として入力し、「**Next**」をクリックします。

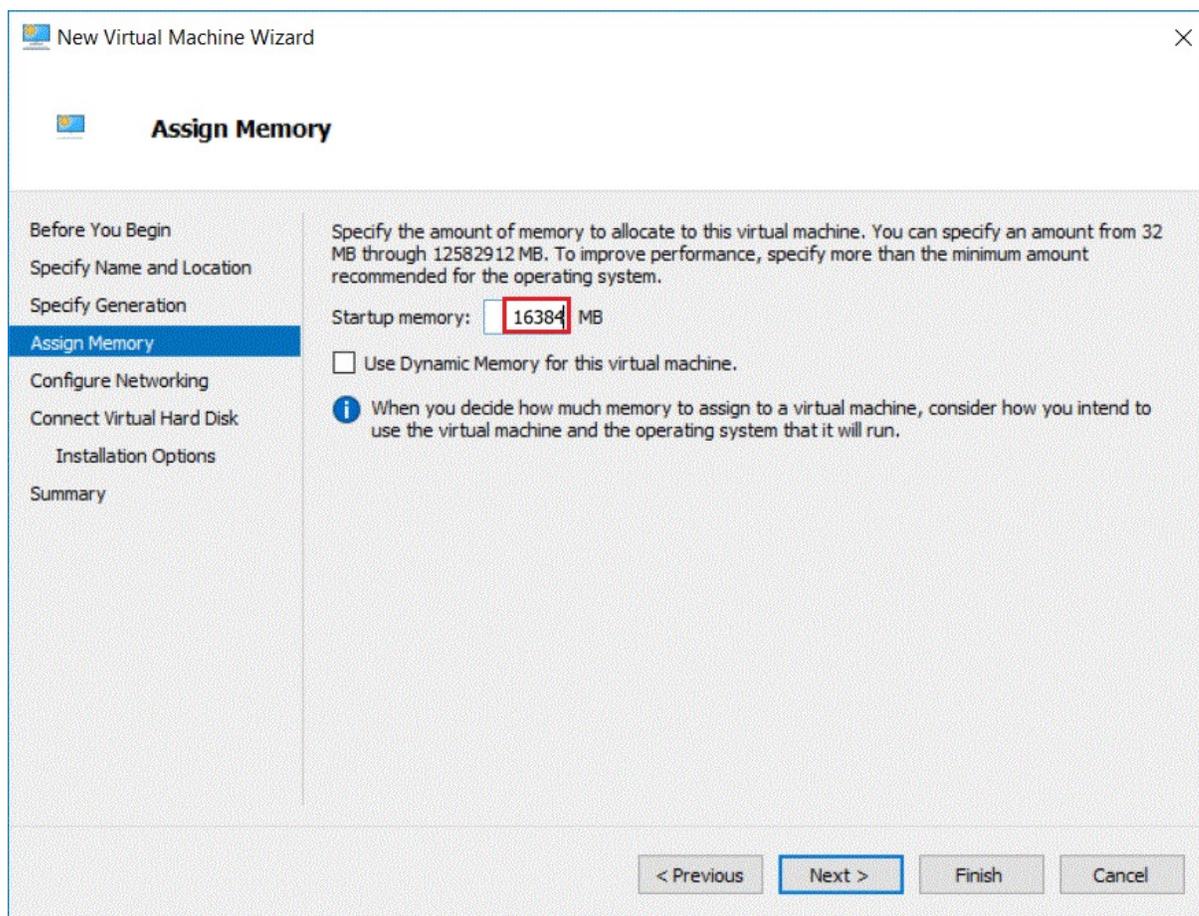


図 10. 開始メモリー

8. 事前構成済みの仮想スイッチを選択して「Next」をクリックします。

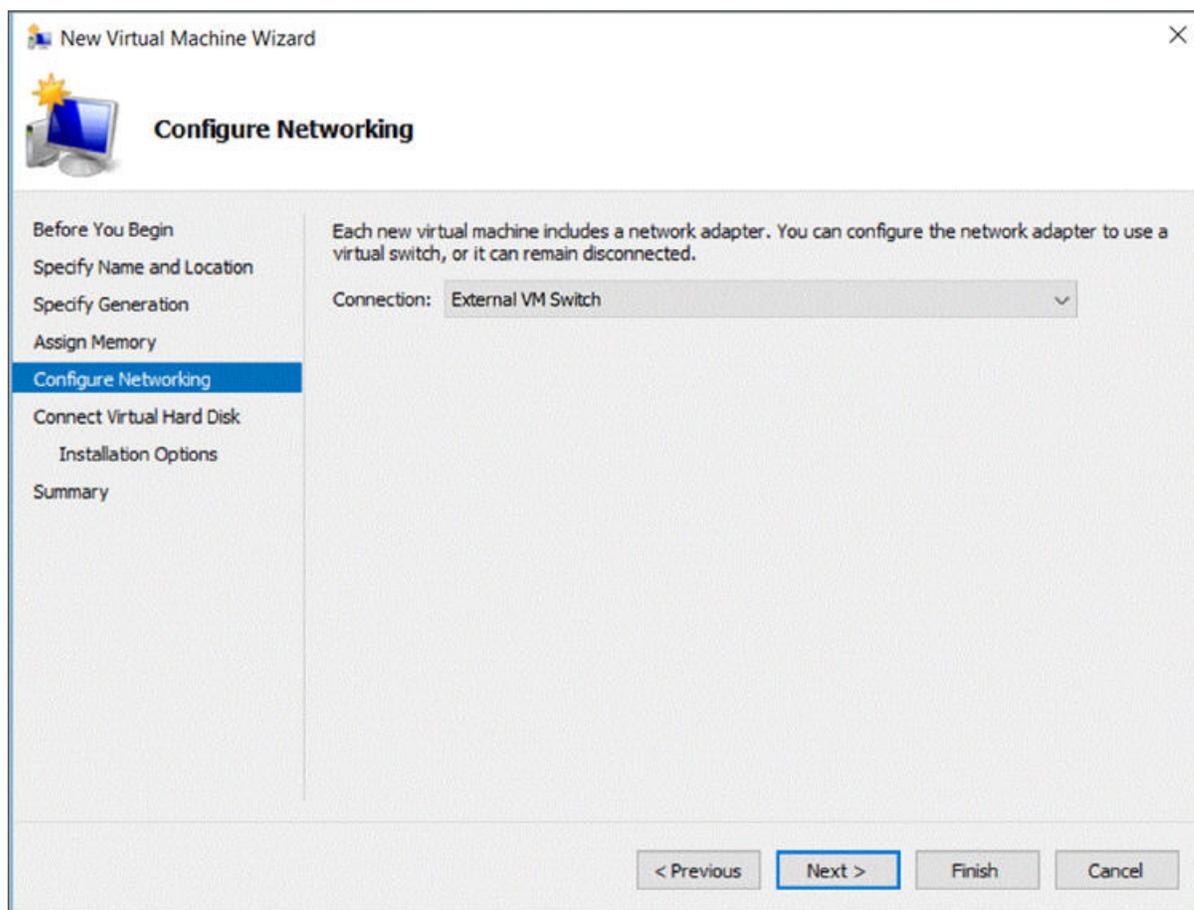
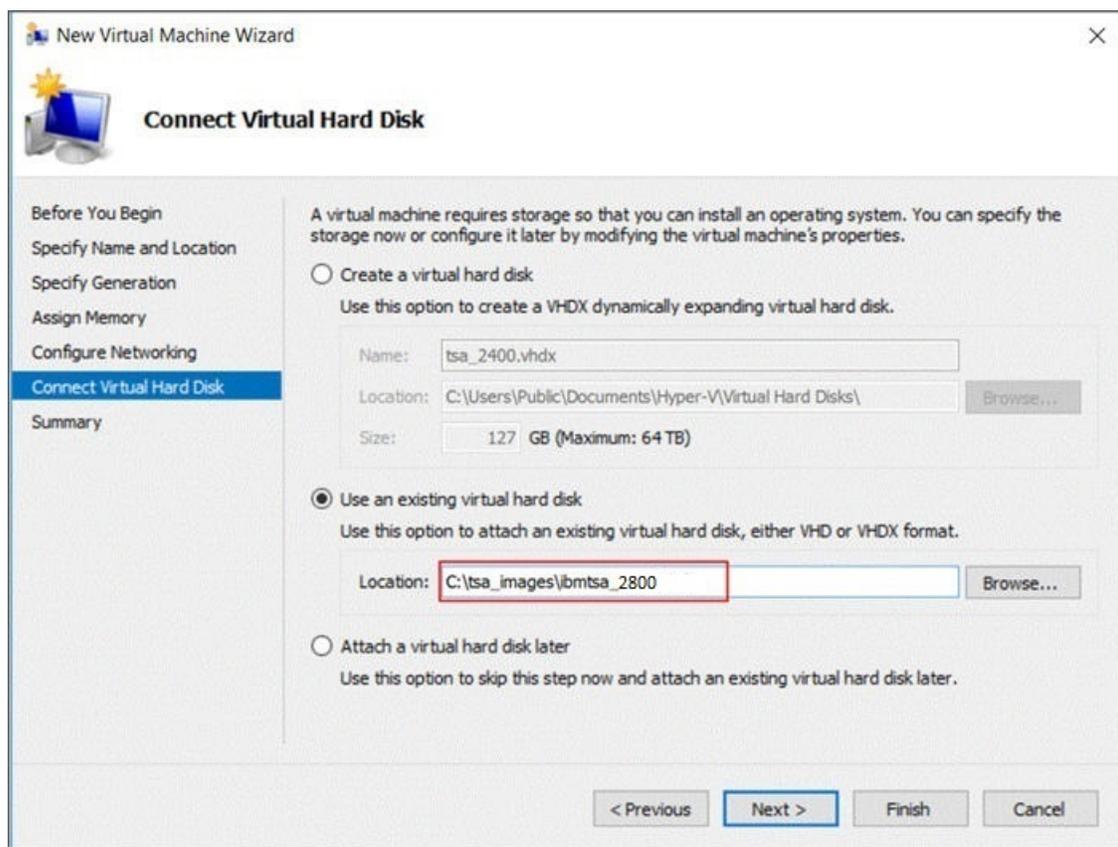


図 11. ネットワーキングの構成

9. 「既存の仮想ハード・ディスクを使用」オプションを選択し、手順 2 で Hyper-V サーバーにコピーした `ibmtsa_2800.vhdx` ファイルを参照し、「次へ」をクリックします。



- 図 12. 仮想ハード・ディスクの接続
10. 「**Summary**」 ページで、設定を確認して「**Finish**」をクリックします。

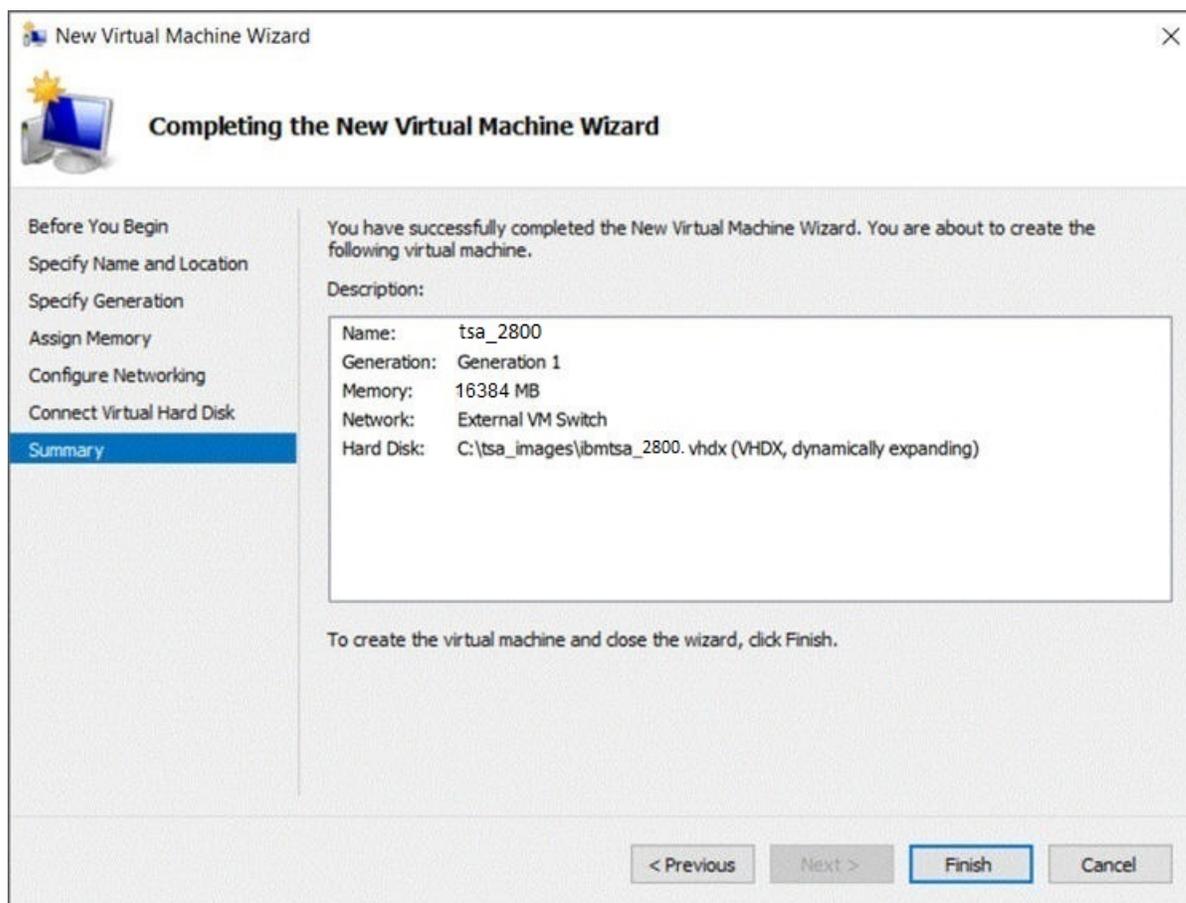


図 13. 要約

- 新規仮想マシンが Hyper-V マネージャーの下に追加されます。仮想マシンを選択し、「**Action**」メニューに移動して「**Start**」をクリックします。

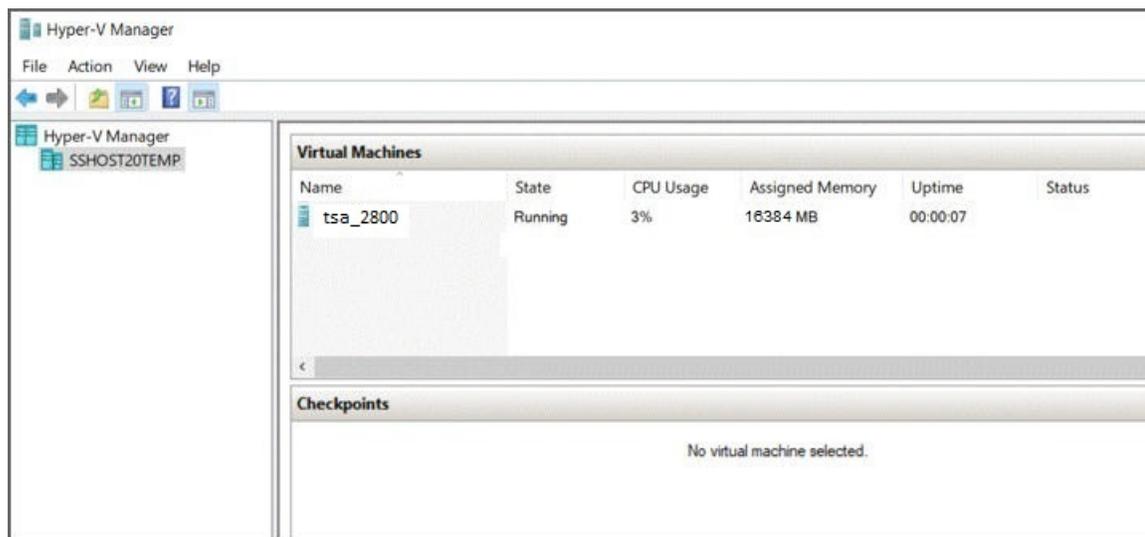


図 14. Hyper-V マネージャー

- 「アクション」メニューで、「接続」を選択してコンソール・セッションを開始します。TSA コンソールで、「ibmtsa ログイン」に「tsausr」、「パスワード」に「configTsa」と入力します。
- 必須: ログイン・パスワードを変更するために、「19 ページの『tsausr パスワードの作成 (必須)』」セクションにリストされているステップを続けて実行します。
- インストールを完了するために、「19 ページの『ネットワーク詳細の構成』」セクションにリストされているステップを続けて実行します。

tsausr パスワードの作成 (必須)

セキュリティ上の理由から、*tsausr* のパスワードを初期値から変更 することをお勧めします。以下の手順に従って *tsausr* パスワードを変更します。

手順

1. 「TSA 構成メニュー」から、オプション「**2) tsausr パスワードの変更**」を選択します。

```
----- TSA Config Menu -----
1) Setup network configuration
2) Change tsausr password
3) Set Appliance certificate to default
4) Exit

Choose an option: 2
```

図 15. パスワードの変更

2. 「**New password**」プロンプトで新規パスワードを入力します。「**Retype new password**」プロンプトで同じパスワードを入力します。新規パスワードは最小 7 文字の長さにする必要があります。

```
Changing password for user tsausr.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Returning to menu in 5 seconds...
```

図 16. 新規パスワード

ネットワーク詳細の構成

手順

1. 「TSA 構成メニュー」からオプション「**1) ネットワーク構成のセットアップ**」を選択します。

```
----- TSA Config Menu -----
1) Setup network configuration
2) Change tsausr password
3) Set Appliance certificate to default
4) Exit

Choose an option: _
```

図 17. ネットワーク構成のセットアップ

2. 以下のネットワーク構成の詳細を入力します。

```

Enter IPTYPE={static|dhcp}:static
Enter Hostname(default=ibmtsa):ibmappliance
Enter IP Address:10.10.10.10
Enter Netmask:255.255.255.255
Enter Gateway Address:10.10.10.1
Enter network domain of system for DNS usage(optional):example.com
Enter DNS 1(optional):10.20.20.20
Enter DNS 2(optional):10.30.30.30
Enter DNS 3(optional):10.40.40.40

Confirm network configuration
IPTYPE:static
HOSTNAME:ibmappliance
IPADDR:10.10.10.10
NETMASK:255.255.255.255
GATEWAY:10.10.10.1
DOMAIN:example.com
DNS1:10.20.20.20
DNS2:10.30.30.30
DNS3:10.40.40.40
[y|n]:_

```

図 18. ネットワーク構成

- a) 「**IPTYPE = {static|dhcp}**」を入力します。「static」または「dhcp」を入力します。「static」の場合はこの手順に従い、それ以外の場合は、[127 ページの『付録 B DHCP ネットワーク詳細の構成』](#)のセクションの dhcp 構成手順に進んでください。

IPTYPE: static

「**ホスト名を入力 (デフォルト =ibmtsa)**」。デフォルト・ホスト名を変更できます。使用するホスト名が固有であることを確認してください。

IP アドレスを入力します。

「**ネットマスクを入力**」および「**ゲートウェイを入力**」。

「**DNS 使用のためのシステムのネットワーク・ドメインを入力 (オプション)**」。

「**DNS 1 を入力 (オプション)**」、「**DNS 2 を入力 (オプション)**」、および「**DNS 3 を入力 (オプション)**」。

指定したネットワーク構成の詳細が、確認のために表示されます。

- b) **[y|n]**を入力して、ネットワーク構成を確認または破棄します。「y」を入力すると、ネットワーク構成が保存されてシステムが自動的に再起動します。

注：構成が正しくない場合は、詳細を変更できます。「n」を入力して現在の設定を無視し、ステップ [20 ページの『2.a』](#) から構成をやり直します。

- c) 新しいネットワーク構成を有効にするために、システムは 15 秒後に再起動します。

- d) ブラウザーからセキュア HTTP を使用して、上で入力したホスト名または IP アドレスを指定して TSA にアクセスします。

例: `https://<hostname | IP address>`

注：初回接続時には、ブラウザーでセキュリティー例外が表示されます。TSA にログインするには、セキュリティー証明書を受け入れて続行する必要があります。

注：ユーザー・インターフェースを介して TSA の基本ネットワーク設定を変更するには、[34 ページの『基本ネットワーク設定の構成』](#)にある手順に従ってください。拡張ネットワーク設定を構成するには、[35 ページの『拡張ネットワーク設定の構成』](#)にある手順に従ってください。

3. [21 ページの『第 4 章 Technical Support Appliance のセットアップ』](#)に記載している手順に従って Technical Support Appliance をセットアップします。

タスクの結果

TSA のセットアップが正常に完了したら、[49 ページの『第 5 章 ディスカバリーと IBM への送信のセットアップ』](#)を参照してください。

第 4 章 Technical Support Appliance のセットアップ

このタスクについて

以下の手順に従って TSA の使用を開始します。まだ行っていない場合は、5 ページの『第 2 章 前提条件』を確認してください。

手順

1. 21 ページの『[Technical Support Appliance へのログイン](#)』
2. 24 ページの『[ご使用条件への同意](#)』
3. 25 ページの『[セットアップ・ウィザードを使用した初期設定](#)』
 - a) 26 ページの『[IBM への接続の設定](#)』
 - b) 28 ページの『[Technical Support Appliance の登録](#)』
 - c) 30 ページの『[クロックの設定](#)』
 - d) 31 ページの『[送信スケジュールのセットアップ](#)』
 - e) 32 ページの『[Technical Support Appliance の更新](#)』
4. 33 ページの『[ネットワーク設定の構成](#)』
5. 41 ページの『[証明書のセットアップ](#)』.
6. オプション: [129 ページの『付録 C ユーザー・アカウントとユーザー・グループ』](#)

次のタスク

TSA のセットアップが完了したら、49 ページの『[第 5 章 ディスカバリーと IBM への送信のセットアップ](#)』でその他のタスクの実行方法についての情報を参照してください。

Technical Support Appliance へのログイン

手順

1. TSA にネットワーク・アクセスできるシステムから、インターネット・ブラウザを開きます。
詳細については、5 ページの『[Web ブラウザーの要件](#)』を参照してください。
2. ブラウザーのアドレス・バーに以下の URL を入力します。

```
https://<hostname or IP address>
```

注: <hostname> ではうまくいかない場合は、TSA に割り当てられている IP アドレスを試してください。

3. プロンプトが出されたら、以下の情報を入力します。

ユーザー ID:

「admin」を入力します。

パスワード:

TSA 管理者パスワードを入力します。

初期パスワードは「passw0rd」です。この初期パスワードは、TSA にログオンしてから変更する必要があります。

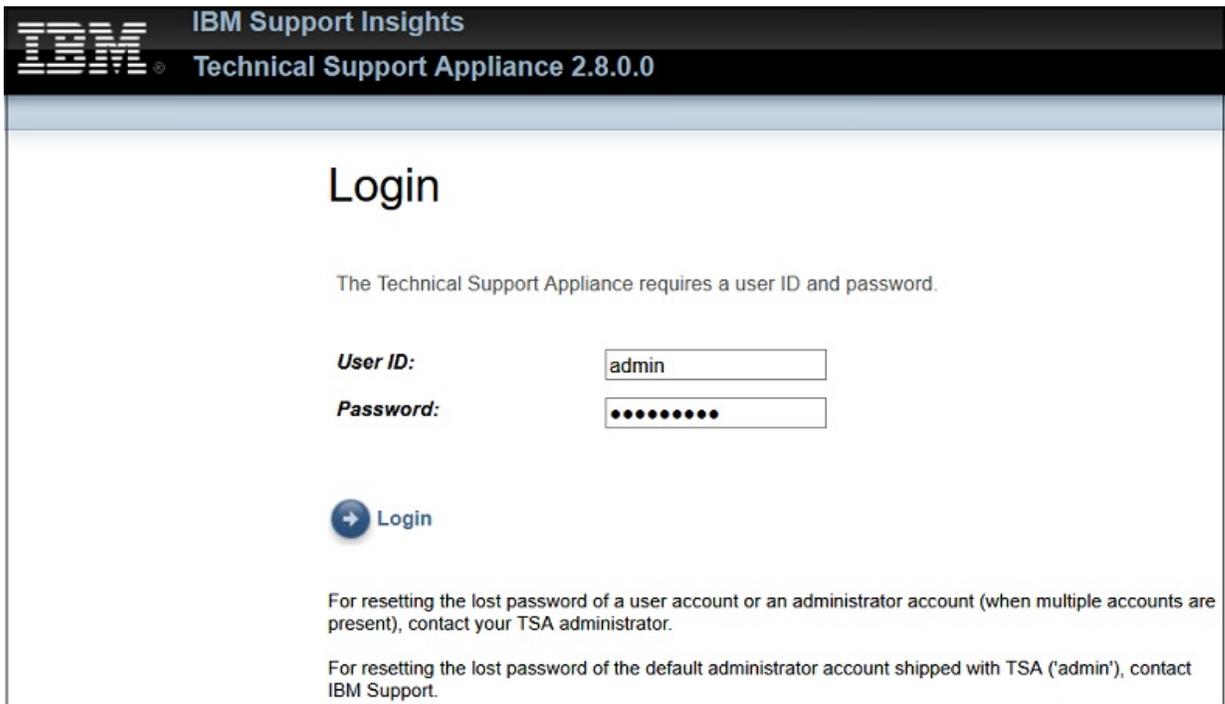


図 19. ログイン

「パスワードの変更」ページが初回ログイン時に表示されます。

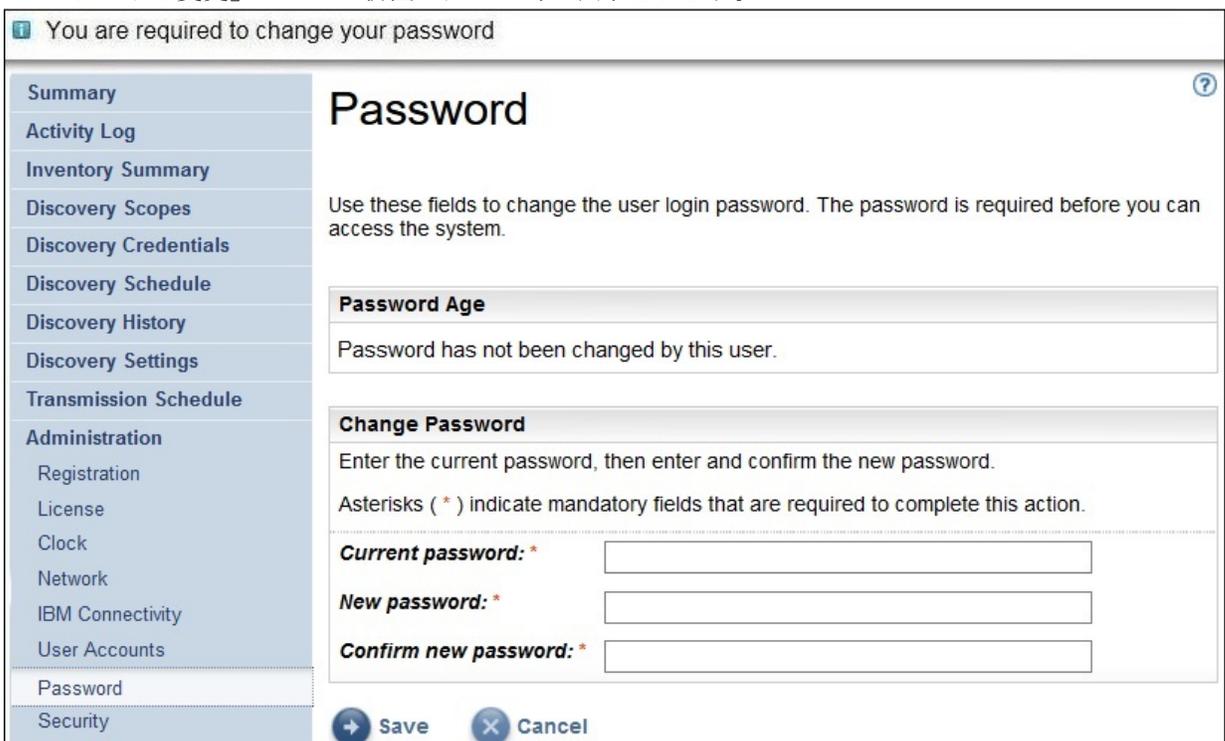


図 20. パスワードの変更

初期パスワードを変更するには、以下の手順に従います。

- a) 新規パスワードを入力します。
 - パスワードは以下のルールに準拠する必要があります。
 - 長さが 8 文字以上である。

- 少なくとも 1 文字の英字と英字以外の文字を含む。
 - ユーザー名を含まない。
 - 直前の 8 つのパスワードのいずれかと同じパスワードを使用しない。
 - 少なくとも 90 日ごとに変更する必要があるが、1 日に 2 回以上変更してはならない。
- b) 「**新規パスワードの確認**」フィールドに新規パスワードを再入力します。
パスワードが保存される前に、入力した 2 つのパスワードが比較されて一致していることが確認されます。
- c) 後で参照するために、新規パスワードを記録しておいてください。
重要: パスワードはリカバリーできないので、パスワードを紛失したり忘れてしまった場合に、TSA にログオンして資格情報を変更することはできません。ユーザー・アカウント、または管理者アカウント (アカウントが複数ある場合) のパスワードを紛失したり忘れてしまったときは、TSA 管理者に連絡してください。(TSA に付属する) デフォルトの管理者アカウントのパスワードを紛失したり忘れてしまった場合は、IBM サポートに連絡してください。
- d) 「**保存**」をクリックします。最初のサインオンでは、「**ご使用条件**」ページが表示されます。

ご使用条件への同意

ご使用条件を読んで同意し、先に進みます。

License Agreement

Read the following license agreements carefully and Accept to proceed further.

IBM Base License Agreement

International License Agreement for Non-Warranted Programs

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE THE PROGRAM: AND

* PROMPTLY RETURN THE UNUSED MEDIA AND DOCUMENTATION TO THE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGRAM WAS DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.

1. Definitions

"Authorized Use" - the specified level at which Licensee is authorized to execute or run the Program. That level may be measured by number of users, millions of service units ("MSUs"), Processor Value Units ("PVUs"), or other level of use specified by IBM.

"IBM" - International Business Machines Corporation or one of its subsidiaries.

"License Information" ("LI") - a document that provides information and any additional terms specific to a Program. The Program's LI is available at www.ibm.com/software/sla. The LI can also be found in the Program's directory, by the use of a system command, or as a booklet included with the Program.

"Program" - the following, including the original and all whole or partial copies: 1)

IBM License and Statement of Work

[View IBM License and Statement of Work](#)

IBM Notices and Information

[View IBM Notices and Information](#)

Terms and Conditions for Separately Licensed Code

[View Terms and Conditions for Separately Licensed Code](#)

[Accept](#)

図 21. ご使用条件

ご使用条件には、以下の項目が含まれます。

- **IBM 基本ご使用条件:** IBM 基本ご使用条件を表示します。
- **IBM ライセンスと作業指示書:** 「**IBM ライセンスと作業指示書**」をクリックすると、IBM ライセンスと作業指示書が表示されます。
注: TSA は GDPR ([EU/2016/679]) に準拠しています。GDPR 準拠情報は、「**IBM ライセンスと作業指示書**」セクションで確認できます。
- **IBM 注意事項およびお知らせ:** 「**IBM 注意事項およびお知らせの表示**」をクリックすると、IBM 注意事項およびお知らせが表示されます。

- **別途使用許諾されるコードのご利用条件:** 「別途使用許諾されるコードのご利用条件の表示」をクリックすると、別途使用許諾されるコードのご利用条件が表示されます。

「同意」をクリックすると、ご使用条件に同意したことになります。ライセンスに同意すると、TSA を構成するための**セットアップ・ウィザード**が表示されます。**セットアップ・ウィザード**を使用して TSA を構成することも、ウィザードを閉じて、要件に従って TSA 設定を構成することもできます。

注: 同意した後にご使用条件を再度表示する場合は、ナビゲーション・ペインで「管理」 > 「ライセンス」をクリックします。

関連概念

25 ページの『[セットアップ・ウィザードを使用した初期設定](#)』

セットアップ・ウィザードを使用して、TSA の初期設定をセットアップできます。

117 ページの『[Technical Support Appliance の設定](#)』

セットアップ・ウィザードで終了したりスキップした設定は、TSA の左側ナビゲーション・メニューで手動で設定することができます。

セットアップ・ウィザードを使用した初期設定

セットアップ・ウィザードを使用して、TSA の初期設定をセットアップできます。

使用条件に同意すると、**セットアップ・ウィザード**が自動的に表示されます。

注: **セットアップ・ウィザード**を手動で開始するには、ナビゲーション・ペインで「ツール」 > 「セットアップ・ウィザード」 > 「セットアップ・ウィザードの開始」をクリックします。



図 22. セットアップ・ウィザード

セットアップ・ウィザードに従って、以下の手順を実行できます。

- 26 ページの『[IBM への接続の設定](#)』
- 28 ページの『[Technical Support Appliance の登録](#)』
- 30 ページの『[クロックの設定](#)』
- 31 ページの『[送信スケジュールのセットアップ](#)』
- 32 ページの『[Technical Support Appliance の更新](#)』

注: **セットアップ・ウィザード**で設定の構成を終了したりスキップしたりした場合は、TSA のナビゲーション・ペインで手動で構成することができます。このような設定の構成方法について詳しくは、[117 ページ](#)の『[付録 A Technical Support Appliance の設定](#)』を参照してください。

IBM への接続の設定

手順

TSA が IBM に接続するために使用する構成を表示、変更、およびテストできます。

IBM Connectivity

Use this page to view, change, and test the configuration that the system uses to connect to IBM.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Access

Select whether the system connects to IBM using a direct connection or thru a SSL proxy connection.

Select: * Allow direct SSL connection

SSL Proxy Settings

Defines SSL proxy to use for Internet access.

IP address or hostname: * 9.5.80.143
The IP address or host name of the proxy server.

Port: * 80
The port number of the proxy server.

SSL Proxy Authentication

Define the authentication user name and password required by the SSL proxy.

User name: *
The user name that the proxy server requires for authentication.

Password: *
The password associated with the user name that the proxy server requires for authentication.

Confirm password: *

Save & Test Connection Exit Wizard

図 23. IBM への接続

1. 「アクセス」 ペインで、以下のインターネット・アクセス・タイプのいずれかを選択します。

直接 SSL 接続を許可

TSA は、直接接続を使用して IBM に接続します。

SSL プロキシ接続を使用

TSA は、SSL プロキシ接続を使用して IBM に接続します。

認証を行う SSL プロキシ接続を使用

TSA は、認証ありの SSL プロキシ接続を使用して IBM に接続します。

2. 「SSL プロキシ接続を使用」または「認証を行う SSL プロキシ接続を使用」を選択した場合は、プロキシ・サーバーに関する次の情報を指定します。

IP アドレスまたはホスト名

プロキシ・サーバーの IP アドレスまたはホスト名。

注：ホスト名を入力する際に下線 ("_") を含めることはできません。

ポート

プロキシ・サーバーのポート番号。

3. 「認証を行う SSL プロキシ接続を使用」を選択した場合は、プロキシ・サーバーに関する次の情報を指定します。

ユーザー名

プロキシ・サーバーが認証のために使用するユーザー名。

パスワード

プロキシ・サーバーが認証のために使用するユーザー名に関連付けられたパスワード。

パスワードの確認

パスワードを再度入力します。パスワードが保存される前に、入力した2つのパスワードが比較されて一致していることが確認されます。

次のタスク

- 「保存して接続をテスト」をクリックして、指定した接続を保存してテストします。接続に成功すると、「次へ進む」ボタンが表示されます。
- 「次へ進む」をクリックして、「登録」ページに進みます。
または
- 「ウィザードを閉じる」をクリックしてセットアップ・ウィザードを終了し、「要約」ページに進みます。

Technical Support Appliance の登録

システムご担当者の連絡先とシステムの所在地情報を表示および変更できます。

手順

IBM Connectivity
Registration

Clock
Transmission Schedule
Update

Registration

This page allows you to view and change the system service contact and physical location information.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Service Contact

Identifies the person who IBM Support should contact if there is a problem with this system. Contact information (Contact name, Telephone number, Email address, and IBMid) is optional. It will be used to assist IBM in providing your company with the results of the Technical Support Appliance analysis.

Company name: * IBM_TEST
Name of the organization that owns or is responsible for this system.

Contact name:
Name of the person in your organization who is responsible for repairs and maintenance of the system.

Telephone number:
Telephone number where the contact person can be reached. The telephone number should include the area code, exchange numbers, and extension.

Email:
Email address of the contact person.

IBMid:
You can log on to the [IBM Client Insights Portal](#) with your associated IBMid to download your TSA Reports in 1-2 days after each data transmission. Need an IBMid? Go to <https://www.ibm.com/account> to sign up.

System Location

Identifies where this system has been installed. The information should allow someone to quickly find the system when necessary for maintenance or other purposes.

Country or region: * MEXICO
The country or region where the system is located. If your country or region is not listed, select a neighboring country or region.

State or province: * Jalisco
The state or province where the system is located.

Postal code: * 45000
The postal code where the system is located.

City: * GDL
The city or locality where the system is located.

Street address: * Camino
The first line of the system location address.

Telephone number:
The telephone number of the room where the system is located. The telephone number should include the area code, exchange numbers, and extension.

Building, floor, office:
The building, floor, and office where the system is located.

Back Save & Continue Exit Wizard

図 24. 登録

1. サービスの連絡先情報を次のフィールドに指定します。

会社名

TSA を使用する組織の名前。

連絡先名

(オプション) 組織内の TSA 担当者の名前。

電話番号

(オプション) 担当者と連絡が取れる電話番号。電話番号には、市外局番、局番、内線番号を含める必要があります。電話番号に括弧は使用しないでください。

E メール

(オプション) 担当者の E メール・アドレス。

IBMid

(オプション) IBM Client Insights Portal でレポートを表示することを許可する対象者の IBMid。

注：TSA レポートは、それぞれのデータ転送の 1 日か 2 日後に、関連付けられている IBMid で <https://clientinsightsportal.ibm.com/> にログインしてダウンロードできます。IBMid を登録するには <https://www.ibm.com/account> に移動してください。

注：サービス連絡先は、システムに問題がある場合に IBM サポートが連絡を取る必要がある相手を識別します。連絡先情報は、IBM が貴社に Technical Support Appliance の分析の結果を提供するために使用します。

2. TSA のロケーション情報を次のフィールドに指定します。

国または地域

TSA がある国または地域。

都道府県/州

TSA がある都道府県。都道府県が不明な場合は、*Unknown* と入力します。

郵便番号

TSA がある場所の郵便番号。

市区町村

TSA がある市区町村。

番地

TSA がある場所の住所。

電話番号

(オプション) TSA がある部屋の電話番号。電話番号には、市外局番、局番、内線番号を含める必要があります。電話番号に括弧は使用しないでください。

建物、階、オフィス

(オプション) TSA がある建物、階、オフィス。

次のタスク

- 「保存して続行」をクリックして、登録情報を保存し、「クロック」ページに進みます。
 - 「戻る」をクリックして、「IBM 接続」ページに戻ります。
- または
- 「ウィザードを閉じる」をクリックしてセットアップ・ウィザードを終了し、「要約」ページに進みます。

クロックの設定

セットアップ時に、TSA システムの時刻、日付、およびローカル・タイム・ゾーンを設定できます。

手順

IBM Connectivity
Registration
Clock
Transmission Schedule
Update

Clock

Asterisks (*) indicate mandatory fields that are required to complete this action.

Select Time Zone

Define the Greenwich Mean Time (GMT) offset corresponding to the time zone where this system is located and whether the system clock should automatically adjust when Daylight Savings Time (DST) changes.

GMT offset: * +0:00 - Greenwich Mean Time

DST adjustment: * Automatically adjust for daylight saving changes

Select Time Option

Select whether to use a local or public NTP (Network Time Protocol) server to update the system clock automatically or manually configure it.

Select: * Manually configured system clock

Date and Time

Manually set the system date and time.

Date (mm/dd/yyyy): * 03/02/2020
Defines the manually set system date.

Time (hh:mm:ss): * 16:26:16
Defines the manually set system time.

NTP Settings

Defines the IP addresses or hostnames of up to 2 Network Time Protocol servers for system clock synchronization.

NTP server 1: *
Defines the IP address or hostname for NTP server 1.

NTP server 2:
Defines the IP address or hostname for NTP server 2.

Back Save & Continue Skip Exit Wizard

図 25. クロック

1. 「GMT オフセット」ドロップダウン・リストから、ローカル・タイム・ゾーンを選択します。
2. 「DST 調整」ドロップダウン・リストから夏時間 (DST) 調整を選択します。

注: すべてのタイム・ゾーンで DST が使用できるわけではありません。DST を許容していないタイム・ゾーンでこのオプションを選択すると、エラー・メッセージが表示されます。

3. 「時間オプションの選択」ドロップダウン・リストから、システム・クロックを更新する方法を選択します。

オプションとして、システム・クロックを Network Time Protocol (NTP) サーバーと同期して自動的に更新する方法と、システム・クロックを手動で構成する方法があります。

- a) システム・クロックを手動で構成することを選択した場合は、システムの日付と時刻を設定する必要があります。日付と時刻の情報を「日付」フィールドと「時刻」フィールドに入力します。
- b) システム・クロックを Network Time Protocol (NTP) サーバーと同期して自動的にシステム・クロックを更新することにした場合は、NTP サーバーの IP アドレスとホスト名を指定する必要があります。「NTP サーバー」フィールドに、サーバー (2 つまで) の IP アドレスまたはホスト名の情報を入力します。

注: TSA からネットワーク経由で NTP サーバーにアクセスできることを確認してください。

次のタスク

- 「保存して続行」をクリックして、クロック情報を保存し、「送信スケジュール」ページに進みます。
または
 - 「スキップ」をクリックして、「送信スケジュール」ページにスキップします。
- ウィザードの前のステップの設定を変更するには、次のようにします。
- 「戻る」をクリックして、「登録」ページに戻ります。
- ウィザードを終了するには、次のようにします。
- 「ウィザードを閉じる」をクリックしてセットアップ・ウィザードを終了し、「要約」ページに進みます。

送信スケジュールのセットアップ

TSA には、指定された時刻に送信プロセスを実行するための、デフォルトのスケジュールが設定されています。このスケジュールはニーズに合わせて変更できます。

手順

1. 「時刻(時間)」リストおよび「時刻(分)」ドロップダウン・リストを使用して新しい時刻を選択します。
2. 「日選択モード」を選択します。

毎週(日曜日 - 土曜日)

特定の曜日(複数可)に送信をスケジュールする場合は「毎週(日曜日 - 土曜日)」オプションを選択します。

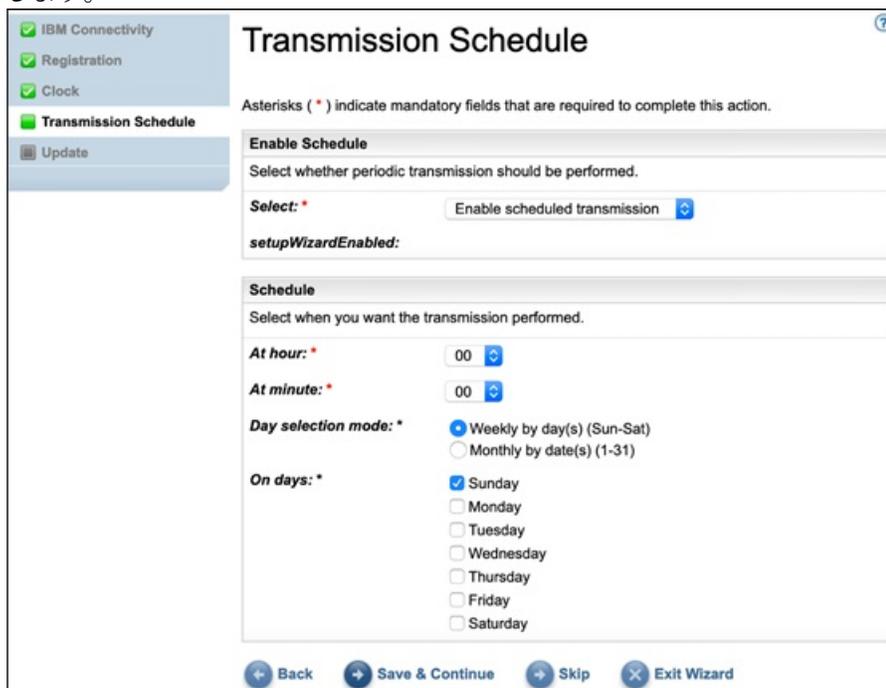


図 26. 毎週(日曜日 - 土曜日)

「曜日」フィールドで該当するチェック・ボックスをチェックして、曜日を1つ以上選択します。

毎月の日(1-31)

毎月特定の日(複数可)に送信をスケジュールする場合は、「毎月の日(1-31)」オプションを選択します。

「曜日」フィールドで該当するチェック・ボックスをチェックして、日付を1つ以上選択します。

注: 特定の月の最終日より後の日を選択すると、その特定の月の最終日にジョブがトリガーされません。

注: 新しく収集されたデータが送信されるまでの待ち時間が長くなるように、必ず、ディスカバリーの開始時刻を送信時刻より前にしてください。

次のタスク

- 「**保存して続行**」をクリックして送信スケジュールを保存し、「**更新**」ページに進みます。
または
- 「**スキップ**」をクリックして、「**更新**」ページにスキップします。
ウィザードの前のステップの設定を変更するには、次のようにします。
- 「**戻る**」をクリックして、「**クロック**」ページに戻ります。
ウィザードを終了するには、次のようにします。
- 「**ウィザードを閉じる**」をクリックして**セットアップ・ウィザード**を終了し、「**要約**」ページに進みます。

Technical Support Appliance の更新

TSA を、使用可能な最新バージョンに更新できます。

更新が使用可能な場合、次の「**更新**」ページが表示されます。

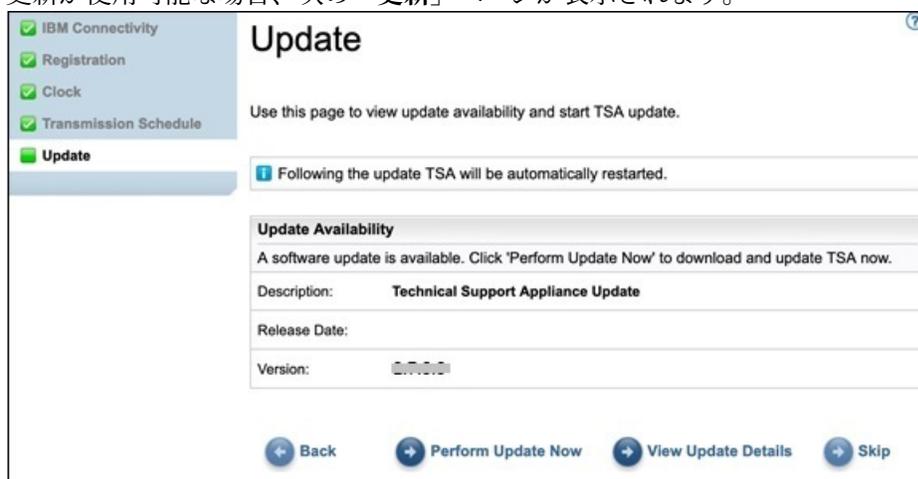


図 27. 使用可能な更新

- 「**今すぐ更新を実行**」をクリックして更新をインストールし、**セットアップ・ウィザード**を実行します。
または
- 「**更新詳細の表示**」をクリックして、更新内容に関する情報を表示します。
ウィザードの前のステップの設定を変更するには、次のようにします。
- 「**戻る**」をクリックして、「**送信スケジュール**」ページに戻ります。
ウィザードを完了するには、次のようにします。
- 「**スキップ**」をクリックして、更新を適用せずに**セットアップ・ウィザード**を完了します。
使用可能な更新がない場合は、次の「**更新**」ページが表示されます。

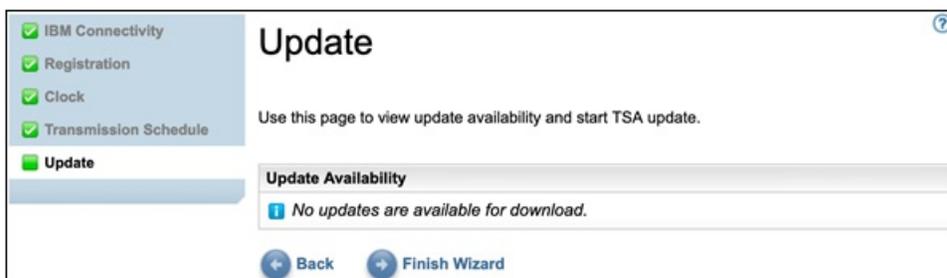


図 28. 使用可能な更新はありません

- 「ウィザードの終了」をクリックしてセットアップ・ウィザードを完了します。「セットアップ・ウィザードが完了しました」ページが表示されます。

または

- 「戻る」をクリックして、「送信スケジュール」ページに戻ります。

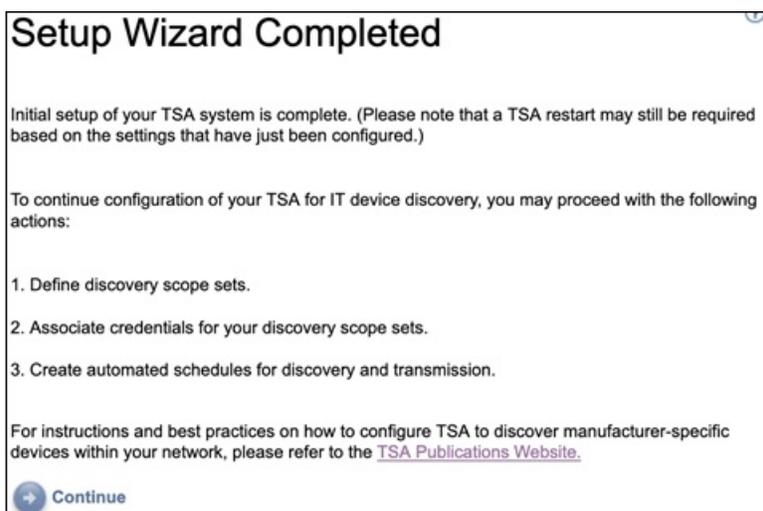


図 29. セットアップ・ウィザードが完了しました

- 「次へ進む」をクリックして、「要約」ページに進みます。

注：「クロック」ページの変更は、有効にするために再起動が必要になるものがあります。例えば、日付や時刻を設定した場合や、手動構成から NTP サーバー構成に変更した場合には、システムの再始動を求めるプロンプトが出されます。

- 「OK」をクリックしてセットアップ・ウィザードを終了し、「要約」ページに戻ります。「要約」ページが表示され、システムが再起動します。

注：セットアップ・ウィザードで設定の構成を終了したりスキップしたりした場合は、TSA のナビゲーション・ペインで手動で構成することができます。このような設定の構成方法について詳しくは、[117 ページ](#)の『付録 A Technical Support Appliance の設定』を参照してください。

ネットワーク設定の構成

TSA をインストールするには、基本的なネットワーク設定の構成が必要です。その基本的な設定が現在ご利用中の IT ネットワークに適したものであれば、このセクションはスキップできます。

始める前に

「ネットワーク」ページでは、以下のいずれかを実行できます。

- 最初の基本的なネットワーク設定を変更する
- 複数のネットワークにアクセスするために TSA を構成する

コンソールから基本ネットワーク設定を構成するには、19 ページの『ネットワーク詳細の構成』セクションの手順に従います。

基本ネットワーク設定の構成

「ネットワーク」ページでは、最初のネットワーク設定を変更できます。

手順

1. ナビゲーション・ペインで、「管理」 > 「ネットワーク」をクリックします。
「ネットワーク」ページが表示されます。

Network

This page allows you to view and change the system network configuration.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Identity

Define the unique name for this system on the network. If you are using a DHCP server for IP configuration, this name will be requested from the DHCP server.

Hostname: *
The network unique identifying name for this system.

Domain name suffix: *
The name assigned as the domain name for this system.

IP Assignment

Select whether the IP address is manually configured or should be obtained dynamically.

Select: *

Static IP Configuration

Defines the static IP configuration for this interface. For those interfaces where DHCP is enabled, the dynamic IP configuration assigned by the DHCP server will override these static settings.

IP address: *
Defines the IP address for this system.

Subnet mask: *
Defines the subnet mask that will be used by this system.

Gateway address: *
Defines the IP address of the system/router that network requests out of the current subnet will get routed to.

Name Services

Specify whether you use a Domain Name System server on your network to translate hostnames into IP addresses.

Select: *

DNS Server Search Order

Defines the IP addresses of up to 3 Domain Name System servers to search for hostname resolution.

DNS server 1: *
Defines the IP address for the DNS server to search 1st.

DNS server 2:
Defines the IP address for the DNS server to search 2nd.

DNS server 3:
Defines the IP address for the DNS server to search 3rd.

図 30. ネットワーク

2. 「ホスト名」フィールドで、ローカル・ネットワーク上のこのシステムの固有名を指定します。
3. 「ドメイン・ネームのサフィックス」フィールドで、ローカル・ネットワーク上のこのシステムのドメイン・ネームとして使用されている名前を指定します。

4. 「IP 割り当て」に「**手動で構成した静的 IP を使用**」を選択します。 DHCP アドレスの割り当てについては、[127 ページの『付録 B DHCP ネットワーク詳細の構成』](#)のセクションを参照してください。
5. 静的 IP アドレスを構成します。
 - a) 「**IP アドレス**」フィールドに、このシステムの IP アドレスを入力します。
 - b) 「**サブネット・マスク**」ドロップダウン・リストで、このシステムで使用するサブネット・マスクを選択します。
 - c) 「**ゲートウェイ・アドレス**」フィールドに、現在のサブネットの外の要求を処理するシステムまたはルーターの IP アドレスを入力します。
6. IP の割り当て方法に応じて「**ネーム・サービス**」を指定します。
 - a) 手動で構成した静的 IP の場合は、「**DNS を使用し、下記のサーバー・アドレスを使用**」オプションを選択します。
 - b) DHCP で IP アドレスを割り当てた場合は、「**DNS を使用するが、DHCP 経由でサーバー・アドレスを取得**」オプションを選択します。
7. ホスト名を解決するとき使用するドメイン・ネーム・システム (DNS) サーバーの IP アドレスを最大 3 つ入力します。

TSA は、表示されている順序でサーバーを検索します。
8. 「**保存**」をクリックしてネットワーク設定を保存します。

システムの再起動を求めるプロンプトが出されます。



注意: ネットワーク設定を変更するときは、注意してください。 ネットワーク構成を間違えると、TSA UI に到達できなくなる可能性があります。 そうなった場合は、TSA コンソールを使用してネットワーク構成を修復する必要があります。

- VMware の場合は、VMware ESXi Web インターフェースまたは VMware vSphere Client を使用します
- Microsoft Hyper-V の場合は、Hyper-V Manager を使用します

9. 設定を保存せずに「**ネットワーク**」ページを終了するには、「**キャンセル**」をクリックします。

拡張ネットワーク設定の構成

複数のネットワークにアクセスするように TSA を構成する場合は、「**ネットワーク (拡張)**」ページを使用してこれらのネットワーク設定を指定します。

拡張ネットワーク設定を構成するには、以下の手順に従います。

1. ナビゲーション・ペインで、「**管理**」 > 「**ネットワーク**」をクリックします。
2. 下部ナビゲーション・ペインで、「**関連リンク**」で、「**拡張ネットワーク**」をクリックします。

Network

This page allows you to view and change the system network configuration.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Identity

Define the unique name for this system on the network. If you are using a DHCP server for IP configuration, this name will be requested from the DHCP server.

Hostname: *
The network unique identifying name for this system.

Domain name suffix: *
The name assigned as the domain name for this system.

IP Assignment

Select whether the IP address is manually configured or should be obtained dynamically.

Select: *

Static IP Configuration

Defines the static IP configuration for this interface. For those interfaces where DHCP is enabled, the dynamic IP configuration assigned by the DHCP server will override these static settings.

IP address: *
Defines the IP address for this system.

Subnet mask: *
Defines the subnet mask that will be used by this system.

Gateway address: *
Defines the IP address of the system/router that network requests out of the current subnet will get routed to.

Name Services

Specify whether you use a Domain Name System server on your network to translate hostnames into IP addresses.

Select: *

DNS Server Search Order

Defines the IP addresses of up to 3 Domain Name System servers to search for hostname resolution.

DNS server 1: *
Defines the IP address for the DNS server to search 1st.

DNS server 2:
Defines the IP address for the DNS server to search 2nd.

DNS server 3:
Defines the IP address for the DNS server to search 3rd.

Related links

- [Advanced network](#)

図 31. 「ネットワーク (拡張)」 ページへのアクセス

「ネットワーク (拡張)」 ページが表示されます。

「ネットワーク (拡張)」 ページは、次の個別のページに分割されています。

- グローバル
- ネットワーク・インターフェース
- DNS 設定
- ネットワーク経路

これらの個々のページにアクセスするには、表示するページのタブをクリックします。

重要: ページを離れる前に「保存」をクリックして、そのページのフィールドに加えた変更を保存する必要があります。変更を有効にするためにシステムを再起動するよう促すプロンプトが出されます。

グローバル

このページを使用して、グローバル・ネットワーク設定を表示および変更します。

Network (advanced) ?

Asterisks (*) indicate mandatory fields that are required to complete this action.

Global Network Interfaces DNS Settings Network Routes

Use this page to view and change global system network settings.

Identity

Define the unique name for this system on the network. If you are using a DHCP server for IP configuration, this name will be requested from the DHCP server.

Hostname: *
The network unique identifying name for this system.

Domain name suffix: *
The name assigned as the domain name for this system.

Save

図 32. ネットワーク (拡張) - グローバル

ID

ネットワーク上のこのシステムの ID を定義します。

1. 「ホスト名」フィールドで、このシステムの固有名を指定します。
2. 「ドメイン・ネームのサフィックス」フィールドで、このシステムのドメイン・ネームとして使用する名前を指定します。

ネットワーク・インターフェース

TSA は、eth0 および eth1 という 2 つのネットワーク・インターフェース・コントローラー (NIC) を持つように構成されています。このページを使用して、選択したネットワーク・インターフェースの現在の設定を表示したり変更したりします。

1. eth0 ネットワーク・インターフェースを選択するには、「**eth0**」をクリックします。
2. eth1 ネットワーク・インターフェースを選択するには、「**eth1**」をクリックします。

Network (advanced) ?

Asterisks (*) indicate mandatory fields that are required to complete this action.

Global **Network Interfaces** DNS Settings Network Routes

eth0 eth1

Use this page to view and change the current settings for the selected network interface.

IP Assignment

Select whether the IP address is manually configured or should be obtained dynamically.

Select: *

Static IP Configuration

Defines the static IP configuration for this interface. For those interfaces where DHCP is enabled, the dynamic IP configuration assigned by the DHCP server will override these static settings.

IP address: *
Defines the IP address for this system.

Subnet mask: *
Defines the subnet mask that will be used by this system.

Default Gateway Route

Select whether this interface provides the route to the default gateway.

Select: *

Default Gateway

Defines the IP address of the system/router that network requests will get routed to when no specific route exists.

Gateway address: *
IP address of the default gateway system.

図 33. ネットワーク (拡張) - ネットワーク・インターフェース

IP 割り当て

このシステムに IP アドレスを割り当てる方法を選択します。オプションとして、DHCP サーバーから IP アドレスを動的に取得する方法と、手動で構成した静的 IP アドレスを使用する方法があります。手動で構成した静的 IP アドレスを使用することを選択した場合、このページでシステム IP アドレスを構成する必要があります。

静的 IP 構成

静的 IP アドレスを手動で構成することを選択した場合は、このネットワーク・インターフェースの IP 情報を次のように指定します。

1. 「IP アドレス」フィールドに、このシステムの IP アドレスを指定します。
2. 「サブネット・マスク」ドロップダウン・リストで、このシステムで使用するサブネット・マスクを選択します。

デフォルト・ゲートウェイ経路

このネットワーク・インターフェースが、デフォルト・ゲートウェイへの経路を提供するかどうかを指定します。

デフォルト・ゲートウェイ

「ゲートウェイ・アドレス」フィールドに、このシステムのデフォルト・ゲートウェイの IP アドレスを指定します。

DNS 設定

このページを使用して、DNS 設定を表示および変更します。

Network (advanced) ?

Asterisks (*) indicate mandatory fields that are required to complete this action.

Global Network Interfaces **DNS Settings** Network Routes

Use this page to view or change the Domain Name Services (DNS) settings.

Name Services

Specify whether you use a Domain Name System server on your network to translate hostnames into IP addresses.

Select: * Use DNS, using server addresses below ▼

DHCP Interface

Select the network interface that is associated with DHCP server you wish to use.

Select interface: * eth0 ▼

DNS Server Search Order

Defines the IP addresses of up to 3 Domain Name System servers to search for hostname resolution.

DNS server 1: * 1.10.1.10
Defines the IP address for the DNS server to search 1st.

DNS server 2: 11.11.11.11
Defines the IP address for the DNS server to search 2nd.

DNS server 3:
Defines the IP address for the DNS server to search 3rd.

Domain Suffix Search Order

Defines up to 3 domain suffixes to search for hostname resolution.

Domain suffix 1: abc.def.com
Defines the domain suffix to search 1st.

Domain suffix 2:
Defines the domain suffix to search 2nd.

Domain suffix 3:
Defines the domain suffix to search 3rd.

Save

図 34. ネットワーク (拡張) - DNS 設定

ネーム・サービス

ホスト名を IP アドレスに変換するためのネットワーク上のドメイン・ネーム・システム (DNS) を指定します。次のオプションから選択できます。

- DNS を使用するが、DHCP サーバーからサーバー・アドレスを取得する。

このオプションを選択する場合は、使用する DHCP サーバーに関連付けられているネットワーク・インターフェースを選択する必要があります。

- DNS を使用し、指定するサーバー・アドレスを使用する。

このオプションを選択する場合は、このページで DNS サーバーを少なくとも 1 つ指定する必要があります。

DHCP インターフェース

使用する DHCP サーバーに関連付けられているネットワーク・インターフェースを選択します。

DNS サーバーの検索順序

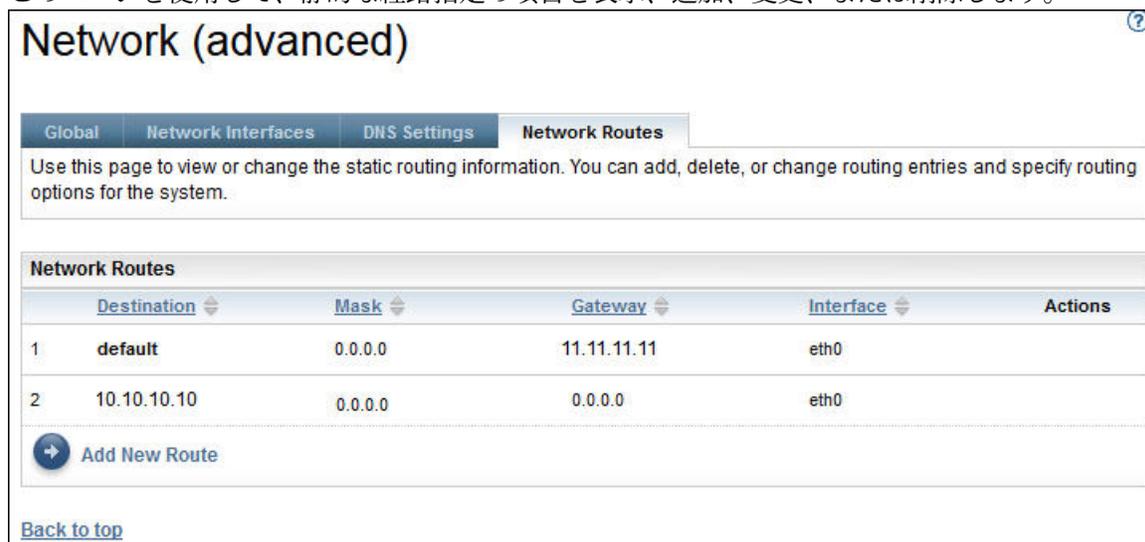
DNS を使用し、指定するサーバー・アドレスを使用することにした場合、ホスト名を解決するときに使用するドメイン・ネーム・システム (DNS) サーバーの IP アドレスを最大 3 つ入力します。TSA は、表示されている順序でサーバーを検索します。

ドメイン・サフィックスの検索順序

DNS を使用し、指定するサーバー・アドレスを使用することにした場合、ホスト名を解決するときに使用するドメイン・ネームのサフィックスを最大 3 つ入力します。TSA は、これらのドメイン・ネームのサフィックスを表示順に検索します。

ネットワーク経路

このページを使用して、静的な経路指定の項目を表示、追加、変更、または削除します。



The screenshot shows the 'Network (advanced)' configuration page. The 'Network Routes' tab is selected. Below the tab is a descriptive text: 'Use this page to view or change the static routing information. You can add, delete, or change routing entries and specify routing options for the system.' Below this is a table with the following data:

	Destination	Mask	Gateway	Interface	Actions
1	default	0.0.0.0	11.11.11.11	eth0	
2	10.10.10.10	0.0.0.0	0.0.0.0	eth0	

Below the table is a button labeled 'Add New Route' and a link labeled 'Back to top'.

図 35. ネットワーク (拡張) - ネットワーク経路

ネットワーク経路ごとに以下の情報が表示されます。

宛先

TCP/IP 宛先ネットワーク・ホストまたはサブネット・アドレスを指定します。

マスク

経路を追加する際にネットワーク・マスクとして使用するサブネット・マスクを指定します。これは、IP アドレスのホスト部分のサブネット・アドレスです。ネットワーク・インターフェースはさまざまなサブネット・マスクを使用できるので、サブネット・マスクを選択することで経路を追加できます (可変サブネット経路)。経路を追加するときは、32 ビットのドット付き 10 進表記でサブネット・マスクを選択する必要があります。

ゲートウェイ

IP パケットを経路指定するための TCP/IP ゲートウェイ・アドレスを指定します。

インターフェース

メニューからアダプターを選択します。テーブル項目に関連付けられているネットワーク・アダプターの名前を選択してください。

アクション

「削除」(🗑️)アイコンをクリックして経路を削除します。

注: この図に示されている 2 つの経路は、変更も削除もできません。

「新規経路の追加」をクリックして、新規静的ネットワーク経路を定義します。「ネットワーク経路」ページが表示されます。

ネットワーク経路の追加

静的ネットワーク経路を追加できます。

手順

ネットワーク経路を追加するには、以下の手順に従います。

1. 「ネットワーク (拡張)」 - 「ネットワーク経路」ページで、「新規経路の追加」をクリックします。「ネットワーク経路」ページが表示されます。

Network Route ⓘ

Use this page to view or change the static routing information. You can add, delete, or change routing entries and specify routing options for the system.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Details

The following describes the static routing entry.

Destination:*	12.20.13.14	IP destination network host or subnet address.
Gateway:*	98.76.54.32	IP gateway address for routing the IP packets.
Subnet mask:*	192.0.0.0	The subnet mask for the host portion of the IP address.
Interface:*	eth0	Associated network interface for this route.

➔ Save ✕ Cancel

図 36. 新規ネットワーク経路

2. 「宛先」フィールドに、TCP/IP 宛先ネットワーク・ホストまたはサブネットの IP アドレスを入力します。
3. 「ゲートウェイ」フィールドに、情報を経路指定するための TCP/IP ゲートウェイ・アドレスを入力します。アドレスは、32 ビットのドット 10 進表記で指定する必要があります。例: xxx.xxx.xxx.xxx。
4. 「サブネット・マスク」ドロップダウン・リストで、この経路のネットワーク・マスクとして使用するサブネット・マスクを選択します。
5. 「インターフェース」ドロップダウン・リストから、この経路と関連付けるネットワーク・アダプターを選択します。
6. 「保存」をクリックして、このネットワーク経路を保存します。

証明書のセットアップ

「証明書」ページでは、証明書の署名情報を表示したり、証明書を生成してインストールしたり、証明書をインポートしたりできます。これらは、ユーザー・インターフェースがアクセスを受けるときに、TSA が Web サーバーに提示するサーバー証明書です。

セットアップを容易にするために、TSA のデフォルト構成では、汎用の自己署名 SSL サーバー証明書が実装されます。安全性の強化のために、初期デプロイメントと構成手順が完了した後で、デフォルトの証明

書を別のものに置き換えることをお勧めします。TSA では、この TSA に固有の自己署名 SSL サーバー証明書を作成してインストールすることも、任意の認証局の署名が付いたカスタム証明書を作成してインストールすることも、カスタム SSL サーバー証明書が含まれている独自の Java 鍵ストア・ファイルをアップロードすることもできます。

カスタム証明書は次のいずれかの方法でインストールできます。

- 43 ページの『カスタム証明書のインストール (署名者の使用)』
- 44 ページの『カスタム証明書のインストール (代替方式)』

SSL サーバー証明書状況の表示

TSA を構成すると、Technical Support Appliance と一緒に提供されているデフォルトの TSA 証明書がインストールされます。

手順

1. ナビゲーション・ペインで、「管理」 > 「証明書」をクリックします。
「証明書」ページが表示されます。

SSL Server Certificate Status	
Default SSL Server certificate is installed.	
Issued by:	CN=www.ibm.com, OU=Technical Support Appliance, O=IBM, L=Armonk, ST=New York, C=US
Issued to:	CN=www.ibm.com, OU=Technical Support Appliance, O=IBM, L=Armonk, ST=New York, C=US
Serial number:	4be3287b
Signature algorithm:	SHA256withRSA
Issued on:	Wednesday Apr 19 11:05:05 BST 2017
Expires on:	Thursday Apr 07 11:05:05 BST 2067
Generate and install a new Self-Signed Certificate	

図 37. SSL サーバー証明書状況

「SSL サーバー証明書状況」セクションには、TSA にインストールされている SSL サーバー証明書に関する情報が表示されます。証明書情報には、*Issued by*、*Issued to*、*Issued on*、*Expires on*、*Serial number*、および *Signature algorithm* が含まれます。

2. この TSA に固有の自己署名証明書をインストールするには、「新規自己署名証明書の生成とインストール」をクリックします。自己署名証明書を生成してインストールするとアプライアンスが自動的に再起動することを示す警告メッセージが表示されます。

注：「新規自己署名証明書の生成とインストール」ボタンが表示されるのは、デフォルトの証明書が TSA にインストールされている場合のみです。

CSR の生成とダウンロード

認証局によって認証された SSL 証明書を申請するには、以下の情報を指定して証明書署名要求 (CSR) ファイルを生成し、そのファイルをダウンロードする必要があります。

手順

1. ナビゲーション・ペインで、「管理」 > 「証明書」をクリックします。
「証明書」ページが表示されます。

Certificate Authority Signing Request

Enter the following information for the Certificate Signing Request(CSR) to be created:

Common Name: *

Organization Unit: *

Organization: *

City: *

State: *

Country: * The country or region where the system is located. If your country or region is not listed, select a neighboring country or region.

Number of days until expiration: *

[Generate and download Certificate Signing Request\(CSR\) file](#)

図 38. 証明書署名要求

2. TSA の完全修飾ホスト名 (FQDN) を「**共通名**」フィールドに入力します。最小文字数制限は 1 で、最大文字数制限は 64 です。
3. 組織内の部門を区別する組織名を「**組織単位**」に指定します。
4. 法人、合資会社、大学、政府機関の名称を「**組織**」に指定します。
5. 「**市区町村**」フィールドに、TSA が稼働している市区町村名または地区名を指定します。
6. 「**都道府県**」フィールドに、TSA が稼働している都道府県名を指定します。都道府県が不明な場合、または都道府県がない国の場合は、*Unknown* と入力します。
7. 「**国**」ドロップダウンで、TSA が稼働している国名を選択します。
8. 証明書が作成された時点から数えた、証明書が有効である日数を**有効期限までの日数**に指定します。
9. 指定された情報を含む CSR ファイルを作成してダウンロードするには、「**証明書署名要求 (CSR) ファイルの生成とダウンロード**」をクリックします。

注: TSA に付属しているデフォルトの証明書を復元するには、[45 ページの『デフォルト証明書の復元』](#)のセクションを参照してください。

カスタム証明書のインストール (署名者の使用)

カスタム証明書をインストールするには、この機能を使用します。認証局によって生成されたサーバー証明書、認証局のルート証明書、および認証局の中間証明書が必要です。

始める前に

証明書ファイル (ルート、中間、およびサーバー証明書) が以下のいずれかの形式であることを確認してください。

- *.crt*
- *.der*
- *.pem*

手順

TSA に証明書をアップロードしてインストールするには、以下の手順を実行します。

1. ナビゲーション・ペインで、「**管理**」 > 「**証明書**」をクリックします。
「**証明書**」ページが表示されます。

Upload and install custom certificate using signers (a certificate chain)

Use this action to import multiple signers (a certificate chain) certificates and install a custom SSL server certificate from file.

To install a custom SSL certificate, import required multi-signers from file, then click "Upload ..."

Root certificate file: * No file chosen

Intermediate certificate file: No file chosen

Intermediate certificate file: No file chosen

Intermediate certificate file: No file chosen

TSA certificate file: * No file chosen

図 39. カスタム証明書のインストール

2. 「ルート証明書ファイル」フィールドに、TSA にインストールするルート証明書ファイルの場所を指定します。
3. 「中間証明書ファイル」フィールドに、TSA にインストールする中間証明書ファイルの場所を指定します。

注: 複数の署名者がインポートされている場合は、複数 (最大で 3 個) の中間証明書ファイルが存在することが考えられます。

4. 「TSA 証明書ファイル」フィールドに、TSA にインストールする TSA サーバー証明書ファイルの場所を指定します。
5. 一連の証明書を使用して、指定したすべてのファイル (ルート証明書ファイル、中間証明書ファイル、TSA 証明書ファイル) をアップロードしてカスタム証明書をインストールするには、「証明書チェーンを使用したカスタム証明書のアップロードとインストール」をクリックします。

注: TSA に付属しているデフォルトの証明書を復元するには、[45 ページの『デフォルト証明書の復元』](#)のセクションを参照してください。

カスタム証明書のインストール (代替方式)

カスタム証明書をインストールするには、この機能を使用します。この機能を使用すると、作成済みの完全な Java 鍵ストア・ファイルをデプロイできます。

始める前に

カスタム証明書をデプロイする場合には、「証明書」ページの「認証局署名要求」と「署名者 (証明書チェーン) を使用したカスタム証明書のアップロードとインストール」の機能を使用することをお勧めします。ただし、完全な Java 鍵ストア・ファイル (鍵、カスタム証明書、関連する CA 証明書を含む) を既に個別に構築している場合は、この機能を使用して鍵ストア・ファイルをデプロイできます。鍵ストア・ファイルの場所とこのファイルのパスワードを指定する必要があります。

注: 鍵ストア・ファイルを作成するときに、鍵エントリー・パスワードと鍵ストア・パスワードを同じにしてください。

手順

1. ナビゲーション・ペインで、「管理」 > 「証明書」をクリックします。
「証明書」ページが表示されます。

図 40. カスタム証明書のインストール

2. カスタム・サーバー証明書をインストールするには、以下の手順に従います。
 - a) 「証明書パスワード」フィールドに証明書のパスワードを入力します。
 - b) 「パスワードの確認」フィールドにパスワードを再入力します。
パスワードが保存される前に、入力した2つのパスワードが比較されて一致していることが確認されます。
 - c) 「カスタム証明書ファイル」フィールドに、カスタム証明書が含まれる Java 鍵ストア・ファイルの場所を指定します。
 - d) 指定した Java 鍵ストア・ファイルをアップロードしてカスタム証明書をインストールするには、「**完全な JKS ファイルのアップロードとインストール**」をクリックします。Java 鍵ストア・ファイルには、カスタム証明書と、関連するすべての認証局のルート証明書および中間証明書が含まれている必要があります。アプライアンスが再起動して、新規証明書の使用がアクティブ化されます。

注：TSA に付属しているデフォルトの証明書を復元するには、[45 ページの『デフォルト証明書の復元』](#)のセクションを参照してください。

タスクの結果

新規証明書がインストールされると、TSA は自動的に再始動します。再始動が完了すると、ご使用のブラウザに、新規証明書を信頼するかどうかを確認するセキュリティ・プロンプトが表示されることがあります。

デフォルト証明書の復元

TSA に付属しているデフォルトの証明書を復元するには、TSA コンソールを使用して、「**アプライアンス証明書をデフォルトに設定**」オプションを選択します。

手順

1. TSA コンソールを起動します。
2. 「**TSA 構成メニュー**」から、オプション「**3) アプライアンス証明書をデフォルトに設定**」を選択します。

図 41. アプライアンス証明書をデフォルトに設定

3. アプライアンス証明書をデフォルト証明書に設定していることを確認 [y/n]: y を入力して、TSA 証明書をデフォルト証明書に設定することを確認します。

タスクの結果

デフォルト証明書がインストールされると、TSA は 5 秒後に自動的に再起動します。再起動が完了すると、ご使用のブラウザーに、デフォルト証明書を信頼するかどうかを確認するセキュリティー・プロンプトが表示されることがあります。

インベントリー・データ・クリーンアップのスケジュール

リソースで収集されたすべてのインベントリー・データに対して、それらがディスカバーされたときから、クリーンアップ・タスクをスケジュールまたは手動で実行できます。

このタスクについて



重要: ほとんどのインストール済み環境では、週 1 回クリーンアップ・タスクを実行することをお勧めします。

インベントリー・クリーンアップ・タスクの現在のスケジュールを表示するには、「インベントリー要約」> 「インベントリー・クリーンアップのスケジュール」を選択します。

Schedule	
Next run:	8/9/15 12:00 AM CDT
Runs at:	12:00 AM on Sunday
Dormant age	60 days

History			
Status	Instance	State	Comments
✓	Inventory cleanup	Complete	<ul style="list-style-type: none">Last status: OKLast run: 3/4/16 12:18 AM CSTLast completed: 3/4/16 12:28 AM CSTLast duration: 10 mins, 5 secsInitiator: admin
✓	Inventory cleanup	Complete	<ul style="list-style-type: none">Last status: OKLast run: 6/19/15 4:27 PM CDTLast completed: 6/19/15 4:35 PM CDTLast duration: 8 mins, 19 secsInitiator: admin
✓	Inventory cleanup	Complete	<ul style="list-style-type: none">Last status: OKLast run: 6/13/15 6:06 PM CDTLast completed: 6/13/15 6:11 PM CDTLast duration: 4 mins, 58 secsInitiator: System

図 42. インベントリー・クリーンアップのスケジュール

インベントリー・クリーンアップを手動で実行するには「**今すぐインベントリー・クリーンアップを実行**」をクリックします。

現在のインベントリー・クリーンアップのスケジュールの編集、有効化、または無効化を行うには、以下の手順に従ってください。

手順

1. 「**インベントリー・クリーンアップのスケジュール**」 ページで、「**スケジュールの編集**」をクリックします。
2. 「**インベントリー設定**」 ページで、「**定期インベントリー・クリーンアップを有効にする**」を選択してインベントリー・クリーンアップ・タスクを有効にするか、「**定期インベントリー・クリーンアップを無効にする**」を選択してインベントリー・クリーンアップ・タスクを無効にします。
3. インベントリー・クリーンアップ・タスクを有効にするように選択した場合は、以下の手順を実行します。
 - a) 「**時刻(時間)**」と「**時刻(分)**」のドロップダウン・リストを選択して、新しい時刻を選択します。
 - b) 「**日選択モード**」を選択します。特定の曜日(複数可)にインベントリー・クリーンアップをスケジュールする場合は「**毎週(日曜日 - 土曜日)**」オプションを選択します。毎月特定の日(複数可)にインベントリー・クリーンアップをスケジュールする場合は「**毎月の日(1-31)**」オプションを選択します。
 - c) 「**曜日**」フィールドで該当するチェック・ボックスをチェックすることで、週または月の別の日または追加の日を選択します。

注: 特定の月の最終日より後の日を選択すると、その特定の月の最終日にジョブがトリガーされません。
4. 「**休止期間**」リストから、インベントリー・データを保持する期間を選択します。
5. 「**保存**」をクリックします。

第 5 章 ディスカバリーと IBM への送信のセットアップ

TSA のセットアップが完了すると、様々な管理機能を使用して、ディスカバリー、送信、ジョブを管理できるようになります。

ディスカバリー・スコープ

ディスカバリー・スコープは、IT 要素のディスカバリーに使用する IP アドレスまたはホスト名、IP アドレスの範囲、ネットワークを指定するものです。ディスカバリー・スコープはディスカバリー・スコープ・セットにグループ化されます。

TSA では、次に示す複数のタイプのディスカバリー・スコープを利用できます。

- HMC 動的スコープ・セット - HMC および HMC で管理されているすべてのパーティションをディスカバリーできます。
- VMware 動的スコープ・セット - VMware vCenter または ESXi ホスト、および ESXi ホスト上のすべての仮想マシンをディスカバリーできます。
- 一般ディスカバリー・スコープ - 動的スコープ・セットではディスカバリーできないすべてのリソースをディスカバリーできます。IP アドレスや IP アドレスの範囲、またはネットワークを手動で入力するか、IP アドレスおよびホスト名のリストをファイルから TSA にインポートすることができます。

HMC 動的スコープ

HMC 動的スコープを定義すると、HMC、および HMC で管理されている IBM Power Systems、さらには、それらのシステム上の VIOS、AIX、および Linux の LPAR から詳細なインベントリを収集できます。

このタスクについて

TSA は、定義された HMC からインベントリ情報を取得するだけでなく、それらの HMC で管理されている LPAR を動的に照会します。そのため、スコープ定義をいくつも作成して保守する必要がありません。HMC に対してスコープを定義し、それらの HMC をディスカバリーするときに自動的にスキャンしたい LPAR のタイプ (AIX、VIOS、Linux) を選択してください。この方法には、LPAR が変更されても TSA を再構成する必要がないという利点があります。

HMC Dynamic Scopes	
Name	Actions
hmc_dynamic_1	

[+ Add New HMC Dynamic Scope](#)

[Back to top](#)

図 43. HMC 動的スコープ

HMC 動的スコープの表示

既存の HMC 動的スコープを表示できます。

このタスクについて

既存の HMC 動的スコープを表示するには、ナビゲーション・ペインで「ディスカバリー・スコープ」 > 「HMC 動的スコープ」をクリックします。「HMC 動的スコープ」ページが表示されます。「HMC 動的スコープ」ペインには、HMC 動的スコープのリストが含まれています。

特定の動的スコープ・セットに関連付けられたスコープと資格情報を表示するには、「名前」列でそのスコープ・セット名をクリックします。「HMC 動的スコープ・セット」ページが表示されます。

HMC Dynamic Scope Set

General
Name: tester

HMC

Type	Value	Description	Actions
Address	9.3.106.58	9.3.106.58	

+ Add HMC
+ Import HMC list

HMC Credentials

Name	Type	User Name	Actions
testing	Password	hscroot	

+ Add HMC Credentials

AIX Credentials

Name	Type	User Name	Actions
AIX1	Password	AIXuser	

+ Add AIX Credentials

Linux Credentials

Name	Type	User Name	Actions
LinuxCred	Password	LinuxCredential	

+ Add Linux Credentials

VIOS Credentials

Name	Type	User Name	Actions
VIOSCred	Password	VIOSUser	

+ Add VIOS Credentials

図 44. HMC 動的スコープ・セットの表示

「HMC」ペインには、その動的スコープ・セットでディスカバーされる HMC の IP アドレスのリストが表示されます。HMC がホスト名を使用して定義された場合には、その値が HMC リストの「説明」列に表示されます。「AIX 資格情報」などのさまざまな資格情報ペインには、スコープ・セットに構成された資格情報がリストされます。

HMC 動的スコープの追加

HMC 動的スコープ・セットを追加するには、単一の HMC の IP アドレスまたはホスト名と、その HMC にアクセスするための単一の資格情報を指定します。オプションで、AIX、Linux、および VIOS の資格情報を指定すると、HMC で管理されている IBM Power Systems の LPAR のディスカバリーが可能になります。

HMC 動的スコープ・セットが作成された後に、それを編集することで追加の HMC IP アドレスまたはホスト名を定義できます。また、HMC 動的スコープ・セットの編集により、HMC にアクセスするための複数の資格情報と、LPAR にアクセスするための複数の資格情報もサポートできます。

このタスクについて

スコープ・セットを追加するには、以下の手順に従ってください。

手順

1. ナビゲーション・ペインで、「**ディスカバリー・スコープ**」 > 「**HMC 動的スコープ**」をクリックします。
「**HMC 動的スコープ**」ページが表示されます。
2. 新しい HMC 動的スコープ・セットを定義するには、「**新規 HMC 動的スコープの追加**」をクリックします。
「**HMC 動的スコープ・セット**」ページが表示されます。

図 45. HMC 動的スコープ・セットの追加

3. 「スコープ・セットの説明」ページの「スコープ・セット名」フィールドに、固有の名前を入力します。
4. 「HMC のホスト名または IP アドレスの入力」ページに、HMC の IP アドレスまたはホスト名を入力します。

5. 「HMC のアクセス情報の入力」 ペインで、以下の詳細情報を入力します。
 - a) 「資格情報名」を入力します。
 - b) 「認証タイプ」を選択します。
 - ・ パスワード - 指定されたパスワードを使用します。
 - ・ **PKI** - 特定のスコープ・セットに関連付けられた SSH 鍵を使用します。
 - c) 「ユーザー名」に、HMC での認証に使用するユーザー名を入力します。
 - d) 「認証タイプ」が「パスワード」である場合は、「パスワード」と「パスワードの確認」に入力します。
 - e) 「認証タイプ」が「**PKI**」で SSH 鍵が暗号化されている場合は、「パスフレーズ」と「パスフレーズの確認」に入力します。SSH 鍵が暗号化されていない場合は、この 2 つのフィールドは空のままにしてください。
 - f) 「認証タイプ」が「**PKI**」である場合は、「ファイルの選択」をクリックし、秘密鍵を TSA にアップロードします。公開鍵は、外的な手段で HMC にデプロイする必要があります。
 - g) オプション: 「資格情報のテスト」をクリックして、ターゲット HMC の資格情報をテストします。
6. 「LPAR」 ペインで、動的ディスカバリーに含める LPAR のタイプ (AIX、Linux、VIOS) を選択します。
7. いずれかの LPAR タイプ (AIX、Linux、VIOS) を選択する場合、それぞれのアクセス情報を入力します。

図 46. 例: Linux LPAR のアクセス情報の入力

- a) 「資格情報名」を入力します。
- b) 「認証タイプ」を選択します。
 - ・ パスワード - 指定されたパスワードを使用します。
 - ・ **PKI** - 特定のスコープ・セットに関連付けられた SSH 鍵を使用します。
- c) 個別の LPAR の認証に使用する「ユーザー名」を入力します。
- d) 「認証タイプ」が「パスワード」である場合は、「パスワード」と「パスワードの確認」に入力します。
- e) 「認証タイプ」が「**PKI**」で SSH 鍵が暗号化されている場合は、「パスフレーズ」と「パスフレーズの確認」に入力します。SSH 鍵が暗号化されていない場合は、この 2 つのフィールドは空のままにしてください。

- f) 「**認証タイプ**」が「**PKI**」である場合は、「**ファイルの選択**」をクリックし、秘密鍵を TSA にアップロードします。公開鍵は、外的な手段で各 LPAR にデプロイする必要があります。
 - g) オプション: この HMC が管理する LPAR の **IP アドレス**を入力し、「**資格情報のテスト**」をクリックして資格情報をテストします。
8. 「**保存**」をクリックして HMC 動的スコープ・セットを保存します。

HMC 動的スコープの変更 - HMC の IP アドレス

既存の HMC 動的スコープ・セットに関連付けられた HMC の IP アドレスのリストを変更できます。

このタスクについて

HMC の IP アドレスのリストを変更するには、以下の手順に従ってください。

手順

1. ナビゲーション・ペインで、「**ディスカバリー・スコープ**」 > 「**HMC 動的スコープ**」をクリックします。
「**HMC 動的スコープ**」ページが表示されます。
2. スコープ・セットを編集するには、「**編集**」(✎)アイコンをクリックします。
「**HMC 動的スコープ・セット**」ページが表示されます。
 - HMC の IP アドレスまたはホスト名をスコープ・セットに追加するには、以下の手順に従ってください。
 - a. 「**HMC**」ペインで、「**HMC の追加**」をクリックします。「**HMC 動的スコープ**」ページが表示されます。
 - b. HMC の IP アドレスまたはホスト名を「**IP アドレス**」フィールドに入力します。
 - c. 「**保存**」をクリックして HMC を追加します。
 - スコープ・セットの既存の HMC の IP アドレスを編集するには、以下の手順に従ってください。
 - a. 「**HMC**」ペインで、「**編集**」(✎)アイコンをクリックします。「**HMC 動的スコープ**」ページが表示されます。
 - b. 「**アドレスまたはホストの説明**」ペインで、HMC の IP アドレスまたはホスト名で「**IP アドレス**」フィールドを変更します。
 - c. 「**保存**」をクリックして HMC を変更します。
 - スコープ・セットの既存の HMC の IP アドレスを削除するには、以下の手順に従ってください。
 - a. 「**HMC**」ペインで、「**削除**」(🗑️)アイコンをクリックします。
 - b. ダイアログ・ボックスで、「**OK**」をクリックして、削除することを確認します。

注: HMC 動的スコープ・セットには HMC の IP アドレスが必ず 1 つ以上定義されていなければなりません。すべての HMC の IP アドレスを削除することはできません。

HMC 動的スコープ・セットのインポート

IP アドレスおよびホスト名のリストを、既存の HMC 動的スコープ・セットにインポートすることができます。

このタスクについて

入力ファイルからの IP アドレスまたはホスト名のリストを、既存の HMC 動的スコープ・セットにインポートすることができます。スコープ・セットをインポートするときには、TSA が以下の検証を行います。

- ファイルの各行を検証し、それぞれが有効な IP アドレスまたはホスト名かどうかをチェックします。
- IP アドレスまたはホスト名を検証する際、末尾や先行ブランクのスペースは無視します。
- 重複した IP アドレスまたはホスト名は無視します。

- 既存の HMC IP アドレスと同じ IP アドレスまたはホスト名を持つエントリーは無視します。

手順

IP アドレスをインポートするには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「HMC 動的スコープ」をクリックします。
「HMC 動的スコープ」ページが表示されます。
2. リスト内の既存のスコープをクリックします。「HMC 動的スコープ・セット」ページが表示されます。
3. HMC ペインで、「HMC リストのインポート」をクリックします。「HMC 動的スコープ・セットのインポート」ページが表示されます。
4. 「ファイルの選択」をクリックして、テキスト・ファイルを選択します。

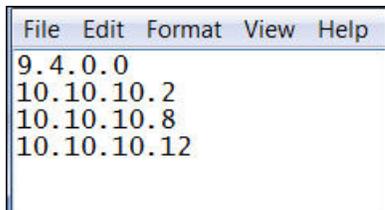


図 47. HMC 動的スコープ・セットのインポート

注: テキスト・ファイルは 1 列のフォーマットにする必要があります。IP アドレスまたはホスト名を 1 行に 1 つずつ入力し、他のデータは含めないでください。

5. 「ファイルのインポート」をクリックして、IP アドレスまたはホスト名をインポートします。
6. 選択したリストをインポートするかどうかを尋ねるダイアログ・ボックスで、「OK」をクリックします。インポートが正常に完了すると、「スコープ "[n]" の IP アドレス/ホスト名のセットを正常にインポートしました」という状況メッセージが表示されます。

注: スコープ・セット・ファイルが原因で HMC 動的スコープ・セットが 400 を超える IP アドレスを持つことになった場合、「このスコープ・セットには、400 個を超える IP アドレスが含まれています。潜在的なパフォーマンスの問題を防止するために、スコープ・セット内の IP アドレスの累積数は、このしきい値以下に抑えてください。」という内容の警告メッセージが表示されます。

7. IP アドレスおよびホスト名をインポートした後、ユーザー・インターフェースの「HMC ディスカバリー・スコープ」ページで HMC 動的スコープ・セットを編集できます。

HMC 動的スコープの変更 - 資格情報

既存の HMC 動的スコープ・セットに関連付けられている資格情報のリストを変更できます。

このタスクについて

HMC 動的スコープ・セットには HMC の資格情報が必ず 1 つ以上定義されていなければなりません。すべての HMC の資格情報を削除することはできません。AIX、Linux、または VIOS の資格情報がない場合、TSA は、その LPAR タイプに関する詳細情報を収集しません。

手順

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「HMC 動的スコープ」をクリックします。
「HMC 動的スコープ」ページが表示されます。
2. スコープ・セットを編集するには、「編集」 (🍌) アイコンをクリックします。
「HMC 動的スコープ・セット」ページが表示されます。
 - HMC、AIX、Linux、または VIOS の資格情報を追加するには、以下の手順に従ってください。

- a. 該当する「資格情報」ペインで、「資格情報の追加」をクリックします。例えば、HMCの資格情報を追加するには、「HMC 資格情報」ペインで、「HMC 資格情報の追加」をクリックします。「新規 HMC ディスカバリー資格情報」ページが表示されます。
 - b. 「資格情報名」を入力します。
 - c. 「認証タイプ」を選択します。
 - パスワード - 指定されたパスワードを使用します。
 - PKI - 特定のスコープ・セットに関連付けられた SSH 鍵を使用します。
 - d. 「ユーザー名」に、HMC または個々の LPAR での認証に使用するユーザー名を入力します。
 - e. 「認証タイプ」が「パスワード」である場合は、「パスワード」と「パスワードの確認」に入力します。
 - f. 「認証タイプ」が「PKI」で SSH 鍵が暗号化されている場合は、「パスフレーズ」と「パスフレーズの確認」に入力します。SSH 鍵が暗号化されていない場合は、この2つのフィールドは空のままにしてください。
 - g. 「認証タイプ」が「PKI」である場合は、「ファイルの選択」をクリックし、秘密鍵を TSA にアップロードします。公開鍵は、外的な手段で HMC または LPAR にデプロイする必要があります。
 - h. オプション: HMC または LPAR の IP アドレスまたはホスト名を「IP アドレス」フィールドに入力し、「資格情報のテスト」をクリックして資格情報をテストします。
 - i. 「保存」をクリックして HMC 動的スコープ・セットの資格情報を保存します。
- HMC、AIX、Linux、または VIOS の資格情報を編集するには、以下の手順に従ってください。
 - a. 該当する「資格情報」ペインで、変更する資格情報の「編集」()アイコンをクリックします。例えば、HMC の資格情報を編集するには、「HMC 資格情報」ペインで、変更する資格情報の「編集」()アイコンをクリックします。「HMC ディスカバリー資格情報の編集」ページが表示されます。
 - b. 「アクセス情報の入力」ペインで、以下の詳細情報を入力できます。
 - 1) 「ユーザー名」に、HMC または個々の LPAR での認証に使用するユーザー名を入力します。
 - 2) 「認証タイプ」を選択します。
 - パスワード - 指定されたパスワードを使用します。
 - PKI - 特定のスコープ・セットに関連付けられた SSH 鍵を使用します。
 - 3) 「認証タイプ」が「パスワード」である場合は、「パスワード」と「パスワードの確認」に入力します。
 - 4) 「認証タイプ」が「PKI」で SSH 鍵が暗号化されている場合は、「パスフレーズ」と「パスフレーズの確認」に入力します。SSH 鍵が暗号化されていない場合は、この2つのフィールドは空のままにしてください。
 - 5) 「認証タイプ」が「PKI」である場合は、「ファイルの選択」をクリックし、秘密鍵を TSA にアップロードします。公開鍵は、外的な手段で HMC または LPAR ごとにデプロイする必要があります。
 - c. オプション: HMC または LPAR の IP アドレスまたはホスト名を「IP アドレス」フィールドに入力し、「資格情報のテスト」をクリックして資格情報をテストします。
 - d. 「保存」をクリックして資格情報を更新します。
 - HMC、AIX、Linux、または VIOS の資格情報を削除するには、以下の手順に従ってください。
 - a. 該当する「資格情報」ペインで、それぞれの資格情報の「削除」()アイコンをクリックします。例えば、HMC の資格情報を削除するには、「HMC 資格情報」ペインで、削除する資格情報の「削除」()アイコンをクリックします。確認メッセージが表示されます。
 - b. 「OK」をクリックして資格情報を削除します。
 - HMC、AIX、Linux、または VIOS の資格情報の順序を変更するには、以下の手順に従ってください。

- a. HMC、AIX、Linux、または VIOS の資格情報が複数存在する場合は、HMC または LPAR の資格情報の順序を変更できます。資格情報が 1 つしかない場合は、資格情報ペインの「アクション」列に上矢印/下矢印は表示されません。
- b. 該当する「資格情報」ペインで「上へ」() 矢印アイコンまたは「下へ」() 矢印アイコンをクリックして、資格情報を再配列します。

動的スコープ・セットの有効化または無効化

HMC 動的スコープ・セットを有効または無効にすることができます。

このタスクについて

無効にしたスコープ・セットは、スケジュールされたディスカバリー時にスキップされます。

注: 手動ディスカバリーは、スコープ・セットの状態にかかわらず常に実行できます。

動的スコープ・セットの無効化

手順

HMC 動的スコープ・セットを無効にするには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「HMC 動的スコープ」をクリックします。
「HMC 動的スコープ」ページが表示されます。
2. 無効にするスコープ・セットの横にある「無効化」() アイコンをクリックします。

動的スコープ・セットの有効化

手順

HMC 動的スコープ・セットを有効にするには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「HMC 動的スコープ」をクリックします。
「HMC 動的スコープ」ページが表示されます。
2. 有効にするスコープ・セットの横にある「有効化」() アイコンをクリックします。

HMC のディスカバリー

HMC 動的スコープ・セット内の単一の HMC のディスカバリーを手動で開始できます。ディスカバリーでは、HMC およびその HMC に関連する LPAR に関する情報が収集されます。

手順

HMC のディスカバリーを手動で開始するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「HMC 動的スコープ」をクリックします。
「HMC 動的スコープ」ページが表示されます。
2. 必要な HMC 動的スコープ・セットの「編集」() アイコンをクリックします。「HMC 動的スコープ・セット」ページが表示されます。
3. ディスカバリーする HMC IP アドレスの横にある「実行」() アイコンをクリックします。

動的スコープ・セットのディスカバリー

HMC 動的スコープ・セットのディスカバリーを手動で開始できます。ディスカバリーでは、スコープ・セットに定義されたすべての HMC およびそれらの HMC に関連する LPAR に関する情報が収集されます。

手順

HMC 動的スコープ・セットのディスカバリーを手動で開始するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「HMC 動的スコープ」をクリックします。
「HMC 動的スコープ」ページが表示されます。
2. ディスカバリーするスコープ・セットの横にある「実行」() アイコンをクリックします。

HMC 動的スコープの削除

既存の HMC 動的スコープ・セットを削除できます。

手順

HMC 動的スコープ・セットを削除するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「HMC 動的スコープ」をクリックします。
「HMC 動的スコープ」ページが表示されます。
2. 削除するスコープ・セットの横にある「削除」() アイコンをクリックします。
3. 「OK」をクリックして HMC 動的スコープ・セットの削除を確認します。

注：HMC 動的スコープ・セットを削除することを確認すると、AIX、Linux、または VIOS の LPAR に関連付けられているアクセス情報も削除されます。

VMware 動的スコープ

VMware 動的スコープを定義すると、VMware vCenter Server および ESXi のインスタンスから詳細なインベントリーを収集できます。また、その VMware vCenter Server または ESXi のインスタンスで管理されている x86 サーバーについての情報と、それらのシステム上の Linux と Windows の仮想マシンについての情報も VMware 動的スコープで収集できます。

TSA は、定義されている VMware vCenter Server および ESXi のインスタンスからインベントリー情報を取得します。また、TSA は、それらの VMware インスタンスで管理されている仮想マシンを動的に照会するので、スコープ定義をいくつも作成して保守する必要がありません。VMware インスタンスに対してスコープを定義し、それらの VMware インスタンスをディスカバリーするときに自動的にスキャンしたい仮想マシンのタイプ (Linux および Windows) を選択してください。この方法には、仮想マシンが変更されても TSA を再構成する必要がないという利点があります。

VMware vCenter Server のディスカバリーは、管理されているすべての VMware ESXi インスタンスを検出するので、VMware ESXi インスタンスを直接ディスカバリーする必要がありません。VMware vCenter Server で管理されていない VMware ESXi インスタンスがある場合は、その VMware ESXi を VMware 動的スコープに定義して、TSA で直接ディスカバリーすることができます。

VMware Dynamic Scopes

Users can define VMware Dynamic Scopes to collect detailed inventory from VMware vCenter Server and VMware ESXi. In addition to retrieving inventory information from the defined VMware vCenter Server or ESXi, TSA also queries managed virtual machines dynamically, without requiring users to create and maintain multiple scope definitions.

Name	Actions
dyvCenter_Scope	
dyVMWare_Scope	
dyVM_Scope	

[+ Add VMware Dynamic Scope](#)

[Back to top](#)

図 48. VMware 動的スコープ

VMware 動的スコープ、スコープ・セット、資格情報の表示

既存の VMware 動的スコープとスコープ・セットを表示できます。

このタスクについて

既存の VMware 動的スコープ・セットを表示するには、ナビゲーション・ペインで「ディスカバリー・スコープ」 > 「**VMware 動的スコープ**」をクリックします。「**VMware 動的スコープ**」ページが表示されます。「**VMware 動的スコープ**」ペインには、VMware 動的スコープのリストが含まれています。

特定の動的スコープ・セットに関連付けられたスコープと資格情報を表示するには、「名前」列でそのスコープ・セット名をクリックします。「**VMware 動的スコープ・セット**」ページが表示されます。

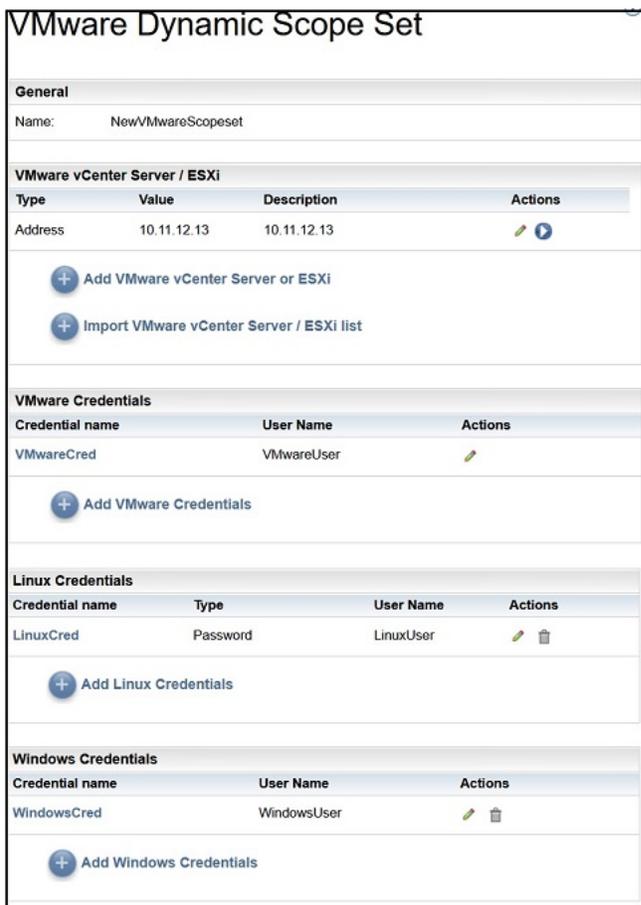


図 49. VMware 動的スコープ・セットの表示

「**VMware vCenter Server / ESXi**」 ペインには、その動的スコープ・セットでディスカバーされる VMware vCenter Server インスタンスと ESXi インスタンスの IP アドレスのリストが表示されます。VMware vCenter Server または ESXi のインスタンスがホスト名を使用して定義された場合には、その値が、VMware vCenter Server / ESXi リストの「説明」列に表示されます。「**Linux 資格情報**」などのさまざまな資格情報 ペインには、スコープ・セットに構成された資格情報がリストされます。

VMware 動的スコープの追加

VMware 動的スコープ・セットを追加するには、単一の VMware vCenter Server インスタンスまたは ESXi インスタンスの IP アドレスまたはホスト名と、その VMware インスタンスにアクセスするための単一の資格情報を指定します。オプションで、Linux および Windows の資格情報を指定すると、VMware インスタンスで管理されている x86 サーバーの仮想マシンのディスカバリーが可能になります。VMware 動的スコープ・セットが作成された後に、それを編集することにより、追加の VMware vCenter Server または ESXi の IP アドレスまたはホスト名を定義できます。また、VMware 動的スコープ・セットの編集により、VMware インスタンスにアクセスするための複数の資格情報と、仮想マシンにアクセスするための複数の資格情報もサポートできます。

このタスクについて

VMware 動的スコープ・セットを追加するには、以下の手順に従ってください。

手順

1. ナビゲーション・ペインで、「**ディスカバリー・スコープ**」 > 「**VMware 動的スコープ**」をクリックします。
「**VMware 動的スコープ**」 ページが表示されます。

2. 新しい VMware 動的スコープ・セットを定義するには、「**VMware 動的スコープの追加**」をクリックします。

「**VMware 動的スコープ・セット**」ページが表示されます。

Summary
Activity Log
Inventory Summary
Discovery Scopes
General Discovery Scopes
Import General Scope Set
HMC Dynamic Scopes
VMware Dynamic Scopes
Discovery Credentials
Discovery Schedule
Discovery History
Discovery Settings
Transmission Schedule
Administration
Tools
Documentation
IBM Support Insights Portal

VMware Dynamic Scope Set

Asterisks (*) indicate mandatory fields that are required to complete this action.

Describe Scope Set

Enter a name for the VMware scope set.

Scope set name: *

Enter Host Name or IP Address of VMware vCenter Server or ESXi

IP address: *

Enter Access Information for VMware

Enter Computer System specific access information.

Credential name: *

User Name: *

Password: *

Confirm password: *

Test Credential

Virtual Machines

Select which types of virtual machines to include in the dynamic discovery.

Select virtual machine types: Linux Windows

Enter Access Information for Linux virtual machines

Enter Computer System specific access information.

Credential name: *

Authentication type: * Password PKI

User Name: *

Password: *

Confirm password: *

Test access credentials for Linux virtual machines

Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the VMware Dynamic Scope Set definition.

IP address: *

Test Credential

Enter Access Information for Windows virtual machines

Enter Computer System specific access information.

Credential name: *

User Name: *

Password: *

Confirm password: *

Test access credentials for Windows virtual machines

Specify the IP address against which you want to test the access credentials. This IP address information is not mandatory to save the VMware Dynamic Scope Set definition.

IP address: *

Test Credential

Save Cancel

図 50. VMware 動的スコープ・セットの追加

3. 「スコープ・セットの説明」ペインの「スコープ・セット名」フィールドに、固有の名前を入力します。
4. 「**VMware vCenter Server または ESXi のホスト名または IP アドレスの入力**」ペインで、VMware vCenter Server インスタンスまたは ESXi インスタンスの IP アドレスまたはホスト名を入力します。
5. 「**VMware のアクセス情報の入力**」ペインで、以下の詳細情報を入力します。
 - a) 「資格情報名」を入力します。

- b) 「**ユーザー名**」に、VMware vCenter Server インスタンスまたは ESXi インスタンスでの認証に使用するユーザー名を入力します。
 - c) 「**パスワード**」と「**パスワードの確認**」に入力します。
 - d) オプション: 「**資格情報のテスト**」をクリックして、ターゲットの VMware vCenter Server インスタンスまたは ESXi インスタンスの資格情報をテストします。
6. 「**仮想マシン**」ペインで、動的ディスカバリーに含める仮想マシン (Linux、Windows) を選択します。
 7. Linux 仮想マシンを選択した場合は、対応するアクセス情報を入力します。

図 51. Linux 仮想マシンのアクセス情報の入力

- a) 「**資格情報名**」を入力します。
 - b) 「**認証タイプ**」を選択します。
 - **パスワード** - 指定されたパスワードを使用します。
 - **PKI** - 特定のスコープ・セットに関連付けられた SSH 鍵を使用します。
 - c) 「**ユーザー名**」に、対応する仮想マシンでの認証に使用するユーザー名を入力します。
 - d) 「**認証タイプ**」が「**パスワード**」である場合は、「**パスワード**」と「**パスワードの確認**」に入力します。
 - e) 「**認証タイプ**」が「**PKI**」で SSH 鍵が暗号化されている場合は、「**パスフレーズ**」と「**パスフレーズの確認**」に入力します。SSH 鍵が暗号化されていなければ、この 2 つのフィールドは空のままにしてください。
 - f) 「**認証タイプ**」が「**PKI**」である場合は、「**ファイルの選択**」をクリックし、秘密鍵を TSA にアップロードします。公開鍵は、外的な手段で各仮想マシンにデプロイする必要があります。
 - g) オプション: 「**IP アドレス**」フィールドに Linux 仮想マシンの IP アドレスまたはホスト名を入力し、「**資格情報のテスト**」をクリックして資格情報をテストします。
8. Windows 仮想マシンを選択した場合は、対応するアクセス情報を入力します。

図 52. Windows 仮想マシンのアクセス情報の入力

- a) 「資格情報名」を入力します。
 - b) 「ユーザー名」に、対応する仮想マシンでの認証に使用するユーザー名を入力します。
 - c) 「パスワード」と「パスワードの確認」を入力します。
 - d) オプション: 「IP アドレス」フィールドに Windows 仮想マシンの IP アドレスまたはホスト名を入力し、「資格情報のテスト」をクリックして資格情報をテストします。
9. 「保存」をクリックして VMware 動的スコープ・セットを保存します。

VMware 動的スコープの変更 - VMware vCenter Server または ESXi の IP アドレス

既存の VMware 動的スコープ・セットに関連付けられている VMware vCenter Server または ESXi の IP アドレスまたはホスト名のリストを変更できます。

このタスクについて

VMware vCenter Server または ESXi の IP アドレスまたはホスト名のリストを変更するには、次の手順を実行します。

手順

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「VMware 動的スコープ」をクリックします。
「VMware 動的スコープ」ページが表示されます。
2. スコープ・セットを編集するには、「編集」 (✎) アイコンをクリックします。
「VMware 動的スコープ・セット」ページが表示されます。
 - VMware vCenter Server または ESXi の IP アドレスまたはホスト名をスコープ・セットに追加するには、以下の手順を実行します。
 - a. 「VMware vCenter Server / ESXi」ペインで、「VMware vCenter Server または ESXi の追加」をクリックします。「VMware 動的スコープ」ページが表示されます。
 - b. 「アドレスまたはホストの説明」ペインの「IP アドレス」フィールドに、VMware vCenter Server または ESXi の IP アドレスあるいはホスト名を入力します。
 - c. 「保存」をクリックして、VMware vCenter Server または ESXi のインスタンスを追加します。
 - スコープ・セットの既存の VMware vCenter Server または ESXi の IP アドレスを編集するには、以下の手順を実行します。

- a. 「VMware vCenter Server/ESXi」 ペインで、「編集」 (✎) アイコンをクリックします。「VMware 動的スコープ」 ページが表示されます。
 - b. 「アドレスまたはホストの説明」 ペインの「IP アドレス」 フィールドで、VMware vCenter Server または ESXi のインスタンスの IP アドレスあるいはホスト名を変更します。
 - c. 「保存」 をクリックします。
- スコープ・セットの既存の VMware vCenter Server または ESXi の IP アドレスを削除するには、以下の手順を実行します。
 - a. 「VMware vCenter Server/ESXi」 ペインで、「削除」 (🗑) アイコンをクリックします。
 - b. ダイアログ・ボックスで、「OK」 をクリックして、削除することを確認します。

注：VMware 動的スコープ・セットには VMware vCenter Server または ESXi の IP アドレスが必ず 1 つ以上定義されていなければなりません。すべての VMware の IP アドレスを削除することはできません。

VMware 動的スコープ・セットのインポート

IP アドレスおよびホスト名のリストを、既存の VMware 動的スコープ・セットにインポートすることができます。

このタスクについて

入力ファイルからの IP アドレスまたはホスト名のリストを、既存の VMware 動的スコープ・セットにインポートすることができます。スコープ・セットをインポートするときには、TSA が以下の検証を行います。

- ファイルの各行を検証し、それぞれが有効な IP アドレスまたはホスト名かどうかをチェックします。
- IP アドレスまたはホスト名を検証する際、末尾や先行ブランクのスペースは無視します。
- 重複した IP アドレスまたはホスト名は無視します。
- 既存の VMware vCenter Server または ESXi のアドレスと同じ IP アドレスまたはホスト名を持つエントリーは無視します。

手順

IP アドレスをインポートするには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「VMware 動的スコープ」 をクリックします。
「VMware 動的スコープ」 ページが表示されます。
2. リスト内の既存のスコープをクリックします。「VMware 動的スコープ・セット」 ページが表示されます。
3. 「VMware vCenter Server / ESXi」 ペインで、「VMware vCenter Server / ESXi リストのインポート」 をクリックします。「VMware 動的スコープ・セットのインポート」 ページが表示されます。
4. 「ファイルの選択」 をクリックして、テキスト・ファイルを選択します。

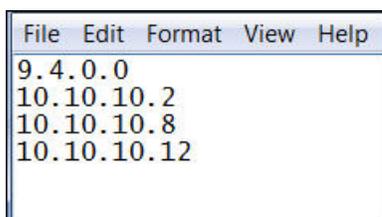


図 53. VMware 動的スコープ・セットのインポート

注：テキスト・ファイルは 1 列のフォーマットにする必要があります。IP アドレスまたはホスト名を 1 行に 1 つずつ入力し、他のデータは含めないでください。

5. 「ファイルのインポート」 をクリックして、IP アドレスまたはホスト名をインポートします。

6. 選択したリストをインポートするかどうかを尋ねるダイアログ・ボックスで、「OK」をクリックします。インポートが正常に完了すると、「**スコープ "[n]" の IP アドレス/ホスト名のセットを正常にインポートしました**」という状況メッセージが表示されます。

注: スコープ・セット・ファイルが原因で VMware 動的スコープ・セットが 400 を超える IP アドレスを持つことになった場合、「このスコープ・セットには、400 個を超える IP アドレスが含まれていません。潜在的なパフォーマンスの問題を防止するために、スコープ・セット内の IP アドレスの累積数は、このしきい値以下に抑えてください。」という内容の警告メッセージが表示されます。

7. IP アドレスおよびホスト名をインポートした後、ユーザー・インターフェースの「**VMware ディスカバリー・スコープ**」ページで VMware 動的スコープ・セットを編集できます。

VMware 動的スコープの変更 - 資格情報

既存の VMware 動的スコープ・セットに関連付けられている資格情報のリストを変更できます。

このタスクについて

VMware 動的スコープ・セットには VMware の資格情報が必ず 1 つ以上定義されていなければなりません。すべての VMware の資格情報を削除することはできません。Linux または Windows の資格情報がない場合、TSA は、その仮想マシン・タイプに関する詳細情報を収集しません。

手順

1. ナビゲーション・ペインで、「**ディスカバリー・スコープ**」 > 「**VMware 動的スコープ**」をクリックします。
「**VMware 動的スコープ**」ページが表示されます。
2. スコープ・セットを編集するには、「**編集**」  アイコンをクリックします。
「**VMware 動的スコープ・セット**」ページが表示されます。
 - VMware または Windows の資格情報を追加するには、以下の手順を実行します。
 - a. 該当する「**資格情報**」ペインで、「**資格情報の追加**」をクリックします。例えば、VMware の資格情報を追加する場合には、「**VMware 資格情報**」ペインで「**VMware 資格情報の追加**」をクリックします。「**新規 VMware ディスカバリー資格情報**」ページが表示されます。
 - b. 「**資格情報名**」を入力します。
 - c. 「**ユーザー名**」に、VMware vCenter Server インスタンスまたは ESXi インスタンス、あるいは Windows 仮想マシンでの認証に使用するユーザー名を入力します。
 - d. 「**パスワード**」と「**パスワードの確認**」を入力します。
 - e. **オプション:** 「**IP アドレス**」フィールドに VMware vCenter Server または ESXi のインスタンス、あるいは Windows 仮想マシンの IP アドレスまたはホスト名を入力し、「**資格情報のテスト**」をクリックして資格情報をテストします。
 - f. 「**保存**」をクリックして資格情報を保存します。
 - Linux の資格情報を追加するには、以下の手順に従ってください。
 - a. 「**Linux 資格情報**」ペインで、「**Linux 資格情報の追加**」をクリックします。「**新規 VMware ディスカバリー資格情報**」ページが表示されます。
 - b. 「**資格情報名**」を入力します。
 - c. 「**認証タイプ**」を選択します。
 - **パスワード** - 指定されたパスワードを使用します。
 - **PKI** - 特定のスコープ・セットに関連付けられた SSH 鍵を使用します。
 - d. 「**ユーザー名**」に、Linux 仮想マシンでの認証に使用するユーザー名を入力します。
 - e. 「**認証タイプ**」が「**パスワード**」である場合は、「**パスワード**」と「**パスワードの確認**」に入力します。

- f. 「**認証タイプ**」が「**PKI**」で SSH 鍵が暗号化されている場合は、「**パズフレーズ**」と「**パズフレーズの確認**」に入力します。SSH 鍵が暗号化されていない場合は、この2つのフィールドは空のままにしてください。
 - g. 「**認証タイプ**」が「**PKI**」である場合は、「**ファイルの選択**」をクリックし、秘密鍵を TSA にアップロードします。公開鍵は、外的な手段で仮想マシンにデプロイする必要があります。
 - h. **オプション:** 「**IP アドレス**」フィールドに Linux 仮想マシンの IP アドレスまたはホスト名を入力し、「**資格情報のテスト**」をクリックして資格情報をテストします。
 - i. 「**保存**」をクリックして Linux の資格情報を保存します。
- VMware または Windows の資格情報を編集するには、以下の手順を実行します。
 - a. 該当する「**資格情報**」ペインで、変更する資格情報の「**編集**」(✎)アイコンをクリックします。例えば、VMware の資格情報を編集するには、変更する資格情報の「**VMware 資格情報**」ペインにある「**編集**」(✎)アイコンをクリックします。「**VMware ディスカバリー資格情報の編集**」ページが表示されます。
 - b. 「**アクセス情報の入力**」ペインで、以下の詳細情報を入力できます。
 - 1) 「**ユーザー名**」に、VMware vCenter Server インスタンスまたは ESXi インスタンス、あるいは Windows 仮想マシンに接続する際の認証に使用するユーザー名を入力します。
 - 2) 「**パスワード**」と「**パスワードの確認**」を入力します。
 - c. **オプション:** 「**IP アドレス**」フィールドに VMware vCenter Server または ESXi のインスタンス、あるいは Windows 仮想マシンの IP アドレスまたはホスト名を入力し、「**資格情報のテスト**」をクリックして資格情報をテストします。
 - d. 「**保存**」をクリックして、資格情報を更新します。
 - Linux の資格情報を編集するには、以下の手順を実行します。
 - a. 「**Linux 資格情報**」ペインで、変更する資格情報の「**編集**」(✎)アイコンをクリックします。「**VMware ディスカバリー資格情報の編集**」ページが表示されます。
 - b. 「**アクセス情報の入力**」ペインで、以下の詳細情報を入力できます。
 - 1) 「**認証タイプ**」を選択します。
 - **パスワード** - 指定されたパスワードを使用します。
 - **PKI** - 特定のスコープ・セットに関連付けられた SSH 鍵を使用します。
 - 2) 「**ユーザー名**」に、Linux 仮想マシンでの認証に使用するユーザー名を入力します。
 - 3) 「**認証タイプ**」が「**パスワード**」である場合は、「**パスワード**」と「**パスワードの確認**」に入力します。
 - 4) 「**認証タイプ**」が「**PKI**」で SSH 鍵が暗号化されている場合は、「**パズフレーズ**」と「**パズフレーズの確認**」に入力します。SSH 鍵が暗号化されていない場合は、この2つのフィールドは空のままにしてください。
 - 5) 「**認証タイプ**」が「**PKI**」である場合は、「**ファイルの選択**」をクリックし、秘密鍵を TSA にアップロードします。公開鍵は、外的な手段で仮想マシンにデプロイする必要があります。
 - 6) **オプション:** 「**IP アドレス**」フィールドに Linux 仮想マシンの IP アドレスまたはホスト名を入力し、「**資格情報のテスト**」をクリックして資格情報をテストします。
 - c. 「**保存**」をクリックして、資格情報を更新します。
 - VMware、Linux、Windows の資格情報を削除するには、以下の手順を実行します。
 - a. 該当する「**資格情報**」ペインで、それぞれの資格情報の「**削除**」(🗑️)アイコンをクリックします。例えば、VMware の資格情報を削除するには、削除する資格情報の「**VMware 資格情報**」ペインにある「**削除**」(🗑️)アイコンをクリックします。確認メッセージが表示されます。
 - b. 「**OK**」をクリックして、資格情報を削除します。
 - VMware、Linux、Windows の資格情報の順序を変更するには、以下の手順を実行します。

- a. VMware、Linux、または Windows の資格情報が複数存在する場合は、VMware または仮想マシンの資格情報の順序を変更できます。資格情報が 1 つしかない場合は、資格情報ペインの「アクション」列に上矢印/下矢印は表示されません。
- b. 該当する「資格情報」ペインで「上へ」() 矢印アイコンまたは「下へ」() 矢印アイコンをクリックして、資格情報を再配列します。

動的スコープ・セットの有効化または無効化

VMware 動的スコープ・セットを有効または無効にすることができます。

このタスクについて

無効にしたスコープ・セットは、スケジュールされたディスカバリー時にスキップされます。

注: 手動ディスカバリーは、スコープ・セットの状態にかかわらず常に実行できます。

動的スコープ・セットの無効化

手順

VMware 動的スコープ・セットを無効にするには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「VMware 動的スコープ」をクリックします。
「VMware 動的スコープ」ページが表示されます。
2. 無効にするスコープ・セットの横にある「有効化」() アイコンをクリックします。

動的スコープ・セットの有効化

手順

VMware 動的スコープ・セットを有効にするには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「VMware 動的スコープ」をクリックします。
「VMware 動的スコープ」ページが表示されます。
2. 有効にするスコープ・セットの横にある「有効化」() アイコンをクリックします。

VMware vCenter または ESXi のディスカバリー

VMware 動的スコープ・セット内の単一の VMware vCenter Server または ESXi のディスカバリーを手動で開始することができます。ディスカバリーでは、VMware インスタンスおよびそのインスタンスに関連する仮想マシンに関する情報が収集されます。

手順

VMware vCenter Server または ESXi のディスカバリーを手動で開始するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「VMware 動的スコープ」をクリックします。
「VMware 動的スコープ」ページが表示されます。
2. 必要な VMware 動的スコープ・セットの「編集」() アイコンをクリックします。「VMware 動的スコープ・セット」ページが表示されます。
3. ディスカバリーする VMware vCenter Server または ESXi の IP アドレスの横にある「実行」() アイコンをクリックします。

動的スコープ・セットのディスカバリー

VMware 動的スコープ・セットのディスカバリーを手動で開始できます。ディスカバリーでは、スコープ・セットに定義されたすべての vCenter Server インスタンスまたは ESXi インスタンスおよびそれらのインスタンスに関連する仮想マシンに関する情報が収集されます。

手順

VMware 動的スコープ・セットのディスカバリーを手動で開始するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「VMware 動的スコープ」をクリックします。
「VMware 動的スコープ」ページが表示されます。
2. ディスカバリーするスコープ・セットの横にある「実行」(▶) アイコンをクリックします。

VMware 動的スコープの削除

既存の VMware 動的スコープ・セットを削除できます。

手順

VMware 動的スコープ・セットを削除するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「VMware 動的スコープ」をクリックします。
「VMware 動的スコープ」ページが表示されます。
2. 削除するスコープ・セットの横にある「削除」(✖) アイコンをクリックします。
3. 「OK」をクリックして VMware 動的スコープ・セットを削除することを確認します。

注: VMware 動的スコープ・セットを削除することを確認すると、Linux 仮想マシンまたは Windows 仮想マシンに関連付けられているアクセス情報も削除されます。

一般ディスカバリー・スコープ

ディスカバリー・プロセスは、インフラストラクチャー内の IT 要素を検索します。ディスカバリー・スコープは、ディスカバリー・プロセスでディスカバリーする単一の IP アドレス、範囲、またはサブネットを定義します。複数のディスカバリー・スコープをグループにして、ユーザーが名前を付けたスコープ・セットにします。

ディスカバリー・スコープとスコープ・セットの表示

既存のディスカバリー・スコープとスコープ・セットを表示できます。

このタスクについて

既存のディスカバリー・スコープ・セットを表示するには、ナビゲーション・ペインで「ディスカバリー・スコープ」 > 「一般ディスカバリー・スコープ」をクリックします。「一般ディスカバリー・スコープ」ページが表示されます。「一般ディスカバリー・スコープ」ペインには、スコープ・セットのリストが含まれています。

スコープ・セットに含まれるスコープを表示するには、該当スコープ・セットをクリックします。「ディスカバリー・スコープ・セット」ページが表示されます。

- 「一般」ペインに、スコープ・セットの名前が表示されます。
- 「IP アドレス数」ペインに、スコープ・セット内の IP アドレスの総数が表示されます。
- 「スコープ」ペインに、スコープ・セット内のスコープの詳細が表示されます。

ディスカバリー・スコープの追加

スコープ・セットを追加してそのセットに新しいスコープを追加したり、既存のスコープ・セットにスコープを追加したり、他のスコープ・セットにスコープを移動したりできます。スコープを追加するには、有効な IP アドレスまたはホスト名、IP アドレスの範囲、ネットワーク、またはサブネットを指定します。

このタスクについて

ヒント: ディスカバリー・スコープとスコープ・セットのセットアップに際して、いくつかの実際的な考慮事項があります。

- ディスカバリー・スコープに含まれる IP アドレスの数が増えるほど、ディスカバリーにかかる時間は長くなります。スコープ・セットを有効/無効にすることにより、またはスコープ・セット内のスコープから IP アドレス、IP アドレスの範囲、ネットワーク、またはサブネットを除外することにより、ディスカバリー・サイズを変更できます。

ディスカバリーにかかる時間を最小限にするには、ディスカバリーする要素のみが対象となるようにディスカバリー・スコープを設定し、ディスカバリーする必要がないスコープ・セットを無効にしたり、ディスカバリーする必要がない IP アドレス、IP アドレスの範囲、ネットワーク、またはサブネットを除外したりします。

注: パフォーマンスを向上させるために、1つのスコープ・セットの IP アドレスの総数は 400 個以下に制限してください。スコープ・セットのインポートについては、[73 ページの『スコープ・セットのインポート』](#)のセクションを参照してください。

- すべての要素が同等であるわけではありません。例えば、多数のインターフェースを持つルーターは、すべてを検出するまでに単一のホストよりも時間がかかる可能性があります。
- デバイス・ディスカバリーに PKI 認証を使用している場合、1つのスコープ・セットに関連付けることができる SSH 鍵は 1 つだけです。

ディスカバリー・スコープをセットアップするためのベスト・プラクティスについて詳しくは、「TSA 構成アシスタント・ガイド」を参照してください。

スコープ・セットとスコープを追加するには、以下の手順に従ってください。

手順

- ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「一般ディスカバリー・スコープ」をクリックします。
「一般ディスカバリー・スコープ」ページが表示されます。
- 新しいディスカバリー・スコープ・セットを定義するには、「新規スコープ・セットの追加」をクリックします。
「ディスカバリー・スコープ・セット」ページが表示されます。

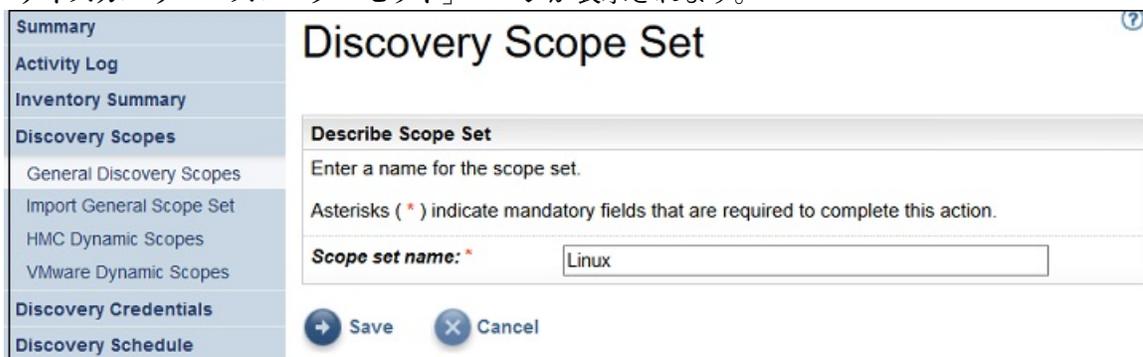


図 54. ディスカバリー・スコープ・セット

- 「スコープ・セット名」フィールドに固有のスコープ・セット名を入力します。
- 「保存」をクリックします。
新しいスコープ・セットが作成され、「一般ディスカバリー・スコープ」ページが表示されます。

Scope set "Linux" created

Discovery Scopes

Asterisks (*) indicate mandatory fields that are required to complete this action.

Select Discovery Option

Select what you want to discover. You can discover a resource for a single IP address or host name, range of IP addresses or subnet.

Discovery Option: *

Describe Address or Host

For discovering a single IP.

IP address: *

Specify the IP address or host name of the system.

図 55. 一般ディスカバリー・スコープ

3. 「ディスカバリー・オプションの選択」 ペインで以下のいずれかのオプションを指定します。

- 単一の IP アドレスまたはホスト

「アドレスまたはホストの説明」に IP アドレスまたはホスト名を入力します。

- IP アドレスの範囲

「アドレス範囲の説明」の所定のフィールドに、開始 IP アドレスと終了 IP アドレス、およびオプションで説明を入力します。

- ネットワークまたはサブネット

「ネットワークまたはサブネットの説明」の所定のフィールドに、IP アドレス、マスク、およびオプションで説明を入力します。

4. ディスカバリーの対象から除外したい IP アドレス、IP アドレスの範囲、またはサブネットがある場合は、「除外の追加」をクリックして以下の手順に従います。

- 「ホスト」、「範囲」、「サブネット」を選択します。
- ディスカバリーの対象から除外する IP アドレス、IP アドレスの範囲、サブネットを指定します。
- オプション: ディスカバリーの対象から除外する IP アドレス、IP アドレスの範囲、またはサブネットの説明を指定します。

注: 除外は、IP アドレスの範囲またはサブネットを定義したスコープにのみ適用されます。

注: IP アドレス、IP アドレスの範囲、サブネット、説明は、スコープ・セット内のスコープや除外で再利用することはできません。

- 除外を追加するには、「除外の追加」をクリックして、前述の手順に従って追加の除外を定義します。

5. 「保存」をクリックしてスコープと除外を保存します。新規スコープがリストに入った「ディスカバリー・スコープ・セット」ページが表示されます。

6. このスコープ・セットにスコープを追加するには、「新規スコープの追加」をクリックし、前述の手順に従ってスコープをさらに定義します。

注: パフォーマンスを向上させるために、1つのスコープ・セットの IP アドレスの総数は 400 個以下に制限してください。

既存のスコープ・セットへのディスカバリー・スコープの追加

既存のスコープ・セットにスコープを追加することができます。

手順

あるスコープを既存のスコープ・セットに追加するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「一般ディスカバリー・スコープ」をクリックします。
「一般ディスカバリー・スコープ」ページが表示されます。
2. 「一般ディスカバリー・スコープ」ペインで、スコープを追加するスコープ・セットをクリックします。
「ディスカバリー・スコープ・セット」ページが表示されます。
3. 「新規スコープの追加」をクリックします。
「一般ディスカバリー・スコープ」ページが表示されます。
4. 「ディスカバリー・オプションの選択」ペインで、次のいずれかのオプションを選択します。
 - 単一の IP アドレスまたはホスト
「アドレスまたはホストの説明」に IP アドレスまたはホスト名を入力します。
 - IP アドレスの範囲
「アドレス範囲の説明」の所定のフィールドに、開始 IP アドレスと終了 IP アドレス、およびオプションで説明を入力します。
 - ネットワークまたはサブネット
「ネットワークまたはサブネットの説明」の所定のフィールドに、IP アドレス、マスク、およびオプションで説明を入力します。
5. ディスカバリーの対象から除外したい IP アドレス、IP アドレスの範囲、またはサブネットがある場合は、「除外の追加」をクリックして以下の手順に従います。
 - a) 「ホスト」、「範囲」、「サブネット」を選択します。
 - b) ディスカバリーの対象から除外する IP アドレス、IP アドレスの範囲、サブネットを指定します。
 - c) オプション: ディスカバリーの対象から除外する IP アドレス、IP アドレスの範囲、またはサブネットの説明を指定します。
注: 除外は、IP アドレスの範囲またはサブネットを定義したスコープにのみ適用されます。
注: IP アドレス、IP アドレスの範囲、サブネット、説明は、スコープ・セット内のスコープや除外で再利用することはできません。
 - d) 除外を追加するには、「除外の追加」をクリックして、前述の手順に従って追加の除外を定義します。
6. 「保存」をクリックしてスコープと除外を保存します。
新規スコープがリストに入った「ディスカバリー・スコープ・セット」ページが表示されます。

ディスカバリー・スコープ・セットの変更

スコープ・セットの設定を変更することにより、既存のディスカバリー・スコープ・セットを変更できます。

このタスクについて

既存のディスカバリー・スコープ・セットを変更するには、以下の手順に従ってください。

手順

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「一般ディスカバリー・スコープ」をクリックします。
「一般ディスカバリー・スコープ」ページが表示されます。

2. スコープ・セットを編集するには、スコープ・セットの横にある「編集」()をクリックします。
- 「ディスカバリー・スコープ・セット」ページが表示されます。スコープの変更、スコープの追加、別のスコープ・セットへのスコープの移動、スコープの削除を行うことによって、スコープ・セットを編集できます。
- スコープを追加するには、以下の手順に従ってください。
 - a. 「新規スコープの追加」をクリックします。
 - b. 「ディスカバリー・オプションの選択」ペインで、次のいずれかのオプションを選択します。
 - 単一の IP アドレス/ホスト
「アドレスまたはホストの説明」に IP アドレスまたはホスト名を入力します。
 - IP アドレスの範囲
「アドレス範囲の説明」の所定のフィールドに、開始 IP アドレスと終了 IP アドレス、およびオプションで説明を入力します。
 - ネットワークまたはサブネット
「ネットワークまたはサブネットの説明」の所定のフィールドに、IP アドレス、マスク、およびオプションで説明を入力します。

注: 「説明」に固有の名前を指定します。他のスコープに既に存在する説明をこのスコープ・セットに指定すると、TSA はその新規スコープの作成を許可しません。「説明」フィールドを空白のままにすると、TSA が IP アドレス範囲/サブネット・マスクを使用して自動的に説明を作成します。
 - c. ディスカバリーの対象から除外したい IP アドレスまたはサブネットがある場合は、「除外の追加」をクリックして以下の手順に従います。
 - 1) 「ホスト」、「範囲」、「サブネット」を選択します。
 - 2) ディスカバリーの対象から除外する IP アドレス、IP アドレスの範囲、サブネットを指定します。
 - 3) 除外を追加するには、「除外の追加」をクリックして、前述の手順に従って追加の除外を定義します。
 - d. 「保存」をクリックしてスコープと除外を保存します。新規スコープがリストに入った「ディスカバリー・スコープ・セット」ページが表示されます。
- あるスコープを別のスコープ・セットに移動するには、以下の手順に従ってください。
 - a. 「スコープの移動」をクリックします。
 - b. 「セット間でスコープを移動」ページで、「スコープ」リストから移動するスコープを選択します。
 - c. 「宛先スコープ・セット」リストから、スコープの移動先のスコープ・セットを選択します。
 - d. 「移動」をクリックします。
 - スコープを編集するには、以下の手順に従ってください。
 - a. 特定のスコープの「編集」()アイコンをクリックします。
 - b. 「ディスカバリー・オプション」、「IP アドレス」、「除外」などを変更できます。
 - c. 「保存」をクリックしてスコープと除外を保存します。新規スコープがリストに入った「ディスカバリー・スコープ・セット」ページが表示されます。
 - スコープを削除するには、以下の手順に従ってください。
 - a. 削除するスコープの横にある「削除」()アイコンをクリックします。
 - b. 「OK」をクリックしてディスカバリー・スコープの削除を確認します。

ディスカバリー・スコープの削除

スコープ・セット内の既存のディスカバリー・スコープを削除するか、スコープ・セット全体を削除することができます。

このタスクについて

手順

ディスカバリー・スコープを削除するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「一般ディスカバリー・スコープ」をクリックします。
「一般ディスカバリー・スコープ」ページが表示されます。
2. 削除するディスカバリー・スコープが含まれるスコープ・セットを編集するために、スコープ・セットの横にある「編集」(✎)アイコンをクリックします。
「ディスカバリー・スコープ・セット」ページが表示されます。
3. 削除するスコープの横にある「削除」(🗑️)アイコンをクリックします。
4. 「OK」をクリックしてディスカバリー・スコープの削除を確認します。

ディスカバリー・スコープ・セットの削除

既存のディスカバリー・スコープ・セットを削除できます。

手順

注: スコープ・セットを削除する前に、そのスコープ・セットに関連付けられたすべての資格情報を削除する必要があります。

ディスカバリー・スコープ・セットを削除するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「一般ディスカバリー・スコープ」をクリックします。
「一般ディスカバリー・スコープ」ページが表示されます。
2. 削除するスコープ・セットの横にある「削除」(🗑️)アイコンをクリックします。
3. 「OK」をクリックしてディスカバリー・スコープ・セットの削除を確認します。

スコープ・セットのインポート

IP アドレスまたはホスト名のリストをインポートして、新しいスコープ・セットを定義することができます。

このタスクについて

指定した名前と、入力ファイル内の IP アドレスまたはホスト名のリストに基づいて、新規スコープ・セットが作成されます。スコープ・セットをインポートするときには、TSA が以下の検証を行います。

- スコープ・セット名が既に存在するかどうかをチェックします。
- ファイルの各行を検証し、それぞれが有効な IP アドレス/ホスト名かどうかをチェックします。
- IP アドレスまたはホスト名を検証する際、末尾や先行ブランクのスペースは無視します。
- 重複した IP アドレスまたはホスト名は無視します。

手順

IP アドレスまたはホスト名をインポートするには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「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」をクリックします。
「一般スコープ・セットのインポート」ページが表示されます。

2. 「新規スコープ・セット名」を入力します。

注: 既存のスコープ・セットで使用されていない固有の名前を入力してください。既存のスコープ・セット名を入力すると、「スコープ・セット名は既に存在します」というエラー・メッセージが表示されます。

3. 「ファイルの選択」をクリックして、テキスト・ファイルを選択します。

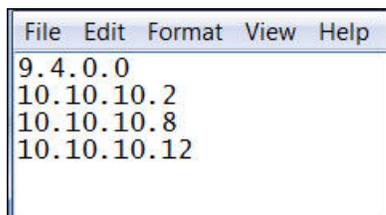


図 56. スコープ・セットのインポート

注: テキスト・ファイルは 1 列のフォーマットにする必要があります。IP アドレスまたはホスト名を 1 行に 1 つずつ入力し、他のデータは含めないでください。

4. 「スコープ・セット・ファイルのインポート」をクリックして、スコープ・セットをインポートします。インポートが正常に完了すると、「スコープ・セットを正常にインポートしました」という状況メッセージが表示されます。

注: スコープ・セット・ファイルの IP アドレスの数が 400 個を超えていると、「スコープ・セットのインポートは成功しましたが、スコープ要素の数が推奨ガイドラインを超えています。パフォーマンスを改善するために、この数を 400 個に制限してください。」という警告メッセージを受け取ります。

5. スコープ・セットをインポートした後、ユーザー・インターフェースの「一般ディスカバリー・スコープ」セクションでスコープ・セットを編集し、「ディスカバリー資格情報」セクションで資格情報を関連付けることができます。

ディスカバリー設定

「ディスカバリー設定」ページを使用して、拡張ディスカバリー設定を調整します。

接続設定の構成

「接続設定」ページを使用して、SLP ディスカバリーを構成し、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します。

このタスクについて

デフォルトでは、ディスカバリー・ジョブは、SLP 照会を実行して EMC SMI-S プロバイダーの IP アドレスやポートを判別することで、EMC SMI-S プロバイダーを見つけようとします。ご使用のネットワーク上で SLP を使用できない場合 (例えば、SLP メッセージをブロックするセキュリティー・ポリシーが存在するなど) でも、SLP ディスカバリーを無効にして EMC SMI-S プロバイダーが照会要求を listen するポートを構成することで、EMC ストレージ・デバイスのディスカバリーを行うことができます。

手順

1. 「有効」または「無効」オプションを選択して、SLP ディスカバリーを有効または無効にします。

注: デフォルトでは、SLP ディスカバリーが有効です。

2. SLP ディスカバリーを無効にする場合、EMC SMI-S プロバイダーの接続ポートを 1 つ以上設定する必要があります。

- a) **EMC SMI-S HTTPS ポート:** EMC SMI-S プロバイダーが照会要求を listen するデフォルトの HTTPS ポートは 5989 です。複数のポートを指定する場合は、コンマで区切ります。EMC SMI-S は、これらのポートで接続要求 (TSA からのものなど) を listen します。接続を開始するためには、TSA がそのポートを認識している必要があります。

- b) **EMC SMI-S HTTP ポート:** EMC SMI-S プロバイダーが照会要求を listen するデフォルトの HTTP ポートは 5988 です。TSA はまず HTTPS 接続 (構成されている場合) を試行し、失敗すると、定義されている HTTP ポートを介して接続を試行します。HTTP 接続をしないようにする場合は、HTTP ポートを定義しないでください。複数の HTTP ポートを指定する場合は、コマンドで区切ります。EMC SMI-S は、これらのポートで接続要求 (TSA からのものなど) を listen します。接続を開始するためには、TSA がそのポートを認識している必要があります。
3. 「保存」をクリックして接続設定を保存します。「ディスカバリー接続設定が正常に保存されました。」というメッセージを受け取ります。

ディスカバリー資格情報

ディスカバリー資格情報は、「**一般ディスカバリー・スコープ**」で構成されたリソースにアクセスするために、TSA がディスカバリー時に使用するユーザー名、パスワードまたは SSH 鍵、Simple Network Management Protocol (SNMP) コミュニティーの文字列です。

資格情報の表示

ディスカバリー・プロセスでは、リソースにアクセスするための資格情報 (ユーザー ID やパスワードなど) が必要となります。

このタスクについて

重要: 指定するアクセス情報は、ディスカバリーのターゲット・リソースのアクセス情報と一致している必要があります。ターゲット・リソースでパスワードなどのアクセス情報を変更する場合は、関連付けられている Technical Support Appliance のアクセス情報も必ず変更してください。

ナビゲーション・ペインの「**ディスカバリー資格情報**」をクリックすると、既存の資格情報を表示できます。「**ディスカバリー資格情報**」ページが表示されます。

Discovery Credentials

The discovery process requires credentials in order to collect inventory from IT elements in your infrastructure. Credentials are a collection of user names, passwords, and Simple Network Management Protocol (SNMP) community strings used by TSA to access discovery targets in your infrastructure.

For Linux, Unix or AIX based systems, the username and password are case sensitive. For Microsoft Windows based systems, only the password is case-sensitive and the username must be a fully qualified username that includes the domain name of the system or the domain name of the Active Directory domain.

Credentials						
Name	Type	Authentication Type	User Name	Password Changed Date	Scope Set Restriction	Actions
Paloalto_Cred	Computer System	Password	admin	5/20/19	PaloAlto_Scope	
EMCSilon_Cred	Computer System	Password	root	1/13/20	EMCSilon_Scope	
SVC_Cred	Computer System	PKI	tsaadmin	3/26/20	SVC_Scope	
XIV_Cred	Computer System	Password	sstation	8/20/19	XIV_Scope	
V7000Unified_Cred	Computer System	Password	tsa	7/29/20	V7000Unified_Scope	
IFS_Cred	Computer System	Password	superuser	1/13/20	IFS_Scope	

図 57. 新規ディスカバリー資格情報

資格情報の詳細の表示

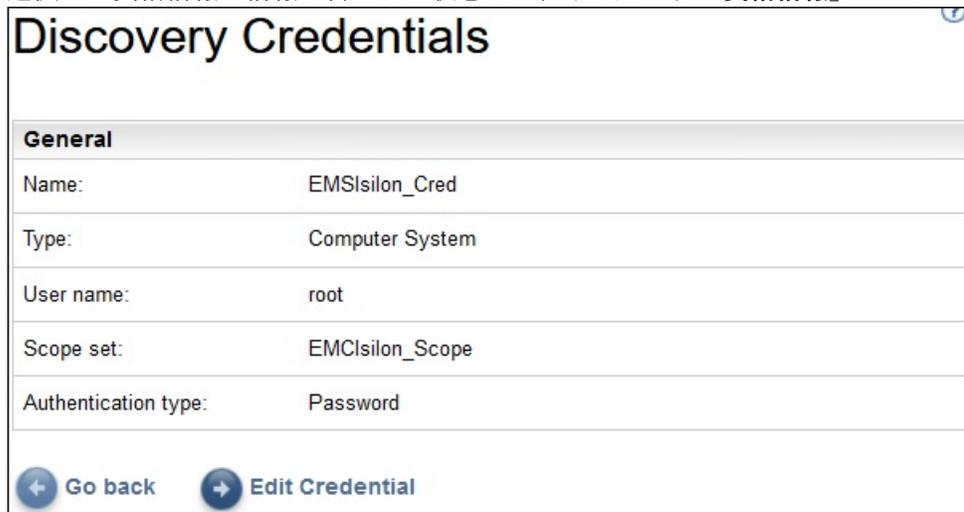
特定のディスカバリー資格情報についての詳細情報を表示できます。

このタスクについて

資格情報の詳細を表示するには、以下の手順に従ってください。

手順

1. ナビゲーション・ペインで、「**ディスカバリー資格情報**」をクリックします。
既存のすべての資格情報がリストされた状態で「**ディスカバリー資格情報**」ページが表示されます。
2. 特定の資格情報の詳細を表示するには、資格情報の名前をクリックします。
選択した資格情報の情報が含まれた状態で「**ディスカバリー資格情報**」ページが表示されます。



The screenshot shows a web interface titled "Discovery Credentials". Below the title is a table with the following information:

General	
Name:	EMSIslon_Cred
Type:	Computer System
User name:	root
Scope set:	EMCIsilon_Scope
Authentication type:	Password

At the bottom of the table, there are two buttons: "Go back" and "Edit Credential".

図 58. ディスカバリー資格情報の詳細

関連タスク

資格情報の変更

資格情報を追加することで、ディスカバリー・プロセスのアクセス制御を提供できます。

資格情報の追加

資格情報を追加することで、ディスカバリー・プロセスにアクセス制御が提供されます。

このタスクについて

資格情報を追加するには、以下の手順に従ってください。

手順

1. ナビゲーション・ペインで、「**ディスカバリー資格情報**」をクリックします。
「**ディスカバリー資格情報**」ページが表示されます。
2. 資格情報を作成するには、「**新規資格情報の追加**」をクリックします。
「**新規ディスカバリー資格情報**」ページが表示されます。

The screenshot shows the 'New Discovery Credentials' configuration page. The left sidebar contains a navigation menu with 'Discovery Credentials' highlighted. The main content area includes the following sections:

- Name:** A text input field for the credential name.
- Select Credential:** A dropdown menu for 'Credential Type' with 'Computer System' selected.
- Enter Access Information:** Radio buttons for 'Authentication type' (Password selected, Public Key Infrastructure (PKI) unselected). Below are text input fields for 'User name', 'Password', and 'Confirm password'.
- Select Scope Set Restriction:** Radio buttons for 'Select' (Limit access information to specified scope selected, Use access information across all scopes unselected).
- Restrict To Selected Scope Set:** A dropdown menu for 'Scope set name' with 'AIX_Scope' selected.
- Test Access Credentials:** A text input field for 'Hostname or IP address' and a 'Test' button.

At the bottom, there are 'Save' and 'Cancel' buttons.

図 59. 新規ディスカバリー資格情報

- 「名前」フィールドに、資格情報の識別名を入力します。
- 「資格情報タイプ」ドロップダウン・リストで、作成する資格情報のタイプを選択します。
- 「アクセス情報の入力」ペインで、選択した資格情報タイプの情報を指定します。

必要な情報は、資格情報タイプによって異なります。それぞれの資格情報タイプに必要なアクセス情報については、[6 ページの『ディスカバリー環境における資格情報とソフトウェア要件』](#)を参照してください。

重要: 指定するアクセス情報は、ディスカバリーのターゲット・リソースのアクセス情報と一致している必要があります。ターゲット・リソースに関するアクセス情報を変更する場合は、関連付けられている TSA のアクセス情報も必ず変更してください。詳しくは、「IBM Technical Support Appliance 構成アシスタント・ガイド」を参照してください。

ヒント: 「ディスカバリー資格情報」ページには、パスワードの最終変更時刻が表示されます。ターゲット・リソースでパスワードを定期的に変更している場合、TSA でもパスワードを変更してターゲット・リソースの新しいパスワードと一致させてあるかどうかを、この情報を使用して確認することができます。ディスカバリー資格情報の表示について詳しくは、[75 ページの『資格情報の表示』](#)を参照してください。

- 「スコープ・セット制限の選択」ペインを使用して、資格情報を単一のスコープ・セットに制限するか、すべてのスコープ・セットに適用するかを指定します。「資格情報タイプ」が「コンピューター・システム」で、「認証タイプ」が「PKI」の場合には、このペインは表示されません。PKI の資格情報は、必ず、単一のスコープ・セットを範囲とする必要があります。

ヒント: 特定のスコープ・セットに制限してディスカバリー資格情報を作成すると、ディスカバリーされたリソースに対して試行される資格情報の数が減ってパフォーマンスが向上する場合があります。

e) 「**選択したスコープ・セットに制限**」 ペインは、資格情報を単一のスコープ・セットに制限する場合に使用します。このペインは、次の2つの状況で表示されます。

- 「**スコープ・セット制限の選択**」 ペインで 「**指定したスコープにアクセス情報を制限**」 を選択した。
- 「**資格情報タイプ**」 が 「**コンピューター・システム**」 で、 「**認証タイプ**」 が 「**PKI**」 である。

この資格情報は、選択したスコープ・セットをディスカバーするときにだけ使用されます。異なるスコープ・セットをディスカバーするときには、その資格情報は使用されません。このようにして、アカウントからロックアウトされる結果になる可能性がある無効なログイン試行を防止します。

f) ご使用の資格情報タイプが 「**コンピューター・システム**」、 「**コンピューター・システム (Windows)**」、 「**SNMP**」、 または 「**SNMPV3**」 の場合、資格情報が正しいかどうかを検証できます。**コンピューター・システム** 資格情報タイプのテスト機能は、以下のデバイスをサポートします。

- SSH または Telnet ベースの認証を使用するデバイス
- XIV[®]
- DS6000™ & DS8000[®]
- VMware ESXi
- VMware vCenter Server
- EMC CLARiiON / VNX / EMC SMI-S 経由の VMAX
- IBM TS3100 / TS3200
- IBM TS3310
- IBM TS3500
- IBM TS4300
- IBM TS4500
- IBM TS7700
- IBM DS3000、DS4000、および DS5000 (パスワードが保護されている場合)
- Windows
- Palo Alto Networks (PAN-OS)

資格情報をテストするには、資格情報をテストする対象のデバイスの IP アドレスまたはホスト名を入力し、「**テスト**」 をクリックします。

注：

- ホスト名を入力する際に下線 ("_") を含めることはできません。
- Linux、AIX、IBM i、または HP-UX オペレーティング・システムを実行しているシステムでディスカバリーの実行または資格情報のテストを行う場合は、SSH を有効にします。

g) 「**保存**」 をクリックします。

新規資格情報が 「**ディスカバリー資格情報**」 ページに表示されます。

注：ディスカバリー資格情報を作成または変更するときは、TSA 構成をバックアップすることがベスト・プラクティスです。

3. リソースにアクセスするために TSA が資格情報を使用する順序を変更するには、資格情報の横にある 「**上矢印**」 アイコン  か 「**下矢印**」 アイコン  のいずれかをクリックして、資格情報をリスト内で上下に移動します。

この順序がどのように使用されるのかについては、2 ページの 『[ディスカバリー資格情報](#)』 を参照してください。

「**ディスカバリー資格情報**」 ページ・リストが、新しい順序で再表示されます。

資格情報の変更

資格情報を追加することで、ディスカバリー・プロセスのアクセス制御を提供できます。

このタスクについて

資格情報を変更するには、以下の手順に従ってください。

手順

- ナビゲーション・ペインで、「**ディスカバリー資格情報**」をクリックします。
既存のすべての資格情報がリストされた状態で「**ディスカバリー資格情報**」ページが表示されます。
- 資格情報の横にある「**編集**」(✎) アイコンをクリックすることで、資格情報を編集します。
「**ディスカバリー資格情報の編集**」ページが表示されます。
 - 「**アクセス情報の変更**」ペインで、この資格情報のアクセス情報を変更できます。
重要: 指定するアクセス情報は、ディスカバリーのターゲット・リソースのアクセス情報と一致している必要があります。ターゲット・リソースに関するアクセス情報を変更する場合は、関連付けられている TSA のアクセス情報も必ず変更してください。詳しくは、「[IBM Technical Support Appliance 構成アシスタント・ガイド](#)」を参照してください。
ヒント: 「**ディスカバリー資格情報**」ページには、パスワードの最終変更時刻が表示されます。ターゲット・リソースでパスワードを定期的に変更している場合、TSA でもパスワードを変更してターゲット・リソースの新しいパスワードと一致させてあるかどうかを、この情報を使用して確認することができます。ディスカバリー資格情報の表示について詳しくは、[75 ページの『資格情報の表示』](#)を参照してください。
 - 「**スコープ・セット制限の選択**」ペインを使用して、資格情報を単一のスコープ・セットに制限するか、すべてのスコープ・セットに適用するかを指定します。「**資格情報タイプ**」が「**コンピューター・システム**」で、「**認証タイプ**」が「**PKI**」の場合には、このペインは表示されません。PKI の資格情報は、必ず、単一のスコープ・セットを範囲とする必要があります。
ヒント: 特定のスコープ・セットに制限してディスカバリー資格情報を作成すると、ディスカバリーの対象リソースに対して試行される資格情報の数が減ってパフォーマンスが向上する場合があります。
 - 「**選択したスコープ・セットに制限**」ペインは、資格情報を単一のスコープ・セットに制限する場合に使用します。このペインは、次の 2 つの状況で表示されます。
 - 「**スコープ・セット制限の選択**」ペインで「**指定したスコープにアクセス情報を制限**」を選択した。
 - 「**資格情報タイプ**」が「**コンピューター・システム**」で、「**認証タイプ**」が「**PKI**」である。この資格情報は、選択したスコープ・セットをディスカバーするときだけに使用されます。この資格情報は、他のスコープ・セットに対しては使用されません。これにより、アカウントからロックアウトされる原因となる可能性がある無効なログイン試行が防止されます。
 - ご使用の資格情報タイプが「**コンピューター・システム**」、「**コンピューター・システム (Windows)**」、「**SNMP**」、または「**SNMPV3**」の場合、資格情報が正しいかどうかを検証できます。これらの資格情報をテストするには、資格情報をテストするターゲットの IP アドレスまたはホスト名を入力し、「**テスト**」をクリックします。
注: ホスト名を入力する際に下線 ("_") を含めることはできません。
 - 「**保存**」をクリックします。
変更された資格情報が「**ディスカバリー資格情報**」ページに表示されます。
- リソースにアクセスするために TSA が資格情報を使用する優先順位を変更するには、資格情報の横にある上矢印(↑) アイコンか下矢印(↓) アイコンのいずれかをクリックして、リスト内で上下に移動します。この順序がどのように使用されるのかについては、[2 ページの『ディスカバリー資格情報』](#)を参照してください。
「**ディスカバリー資格情報**」ページ・リストが、新しい順序で再表示されます。

関連概念

ディスカバリー資格情報

ディスカバリー資格情報は、ディスカバリー中にリソースにアクセスするために TSA が使用するユーザー名、パスワードまたは SSH 鍵、Simple Network Management Protocol (SNMP) コミュニティー文字列のコレクションです。

ディスカバリー環境における資格情報とソフトウェア要件

お客様の環境でエンドポイントまたはリソースのディスカバリーを行うには、TSA がそれらのリソースに対するアクセス権限を持っている必要があります。TSA がリソースにアクセスする際に使用する各リソースにサービス・アカウントを作成することを推奨します。

資格情報の削除

リソースにアクセスするときに TSA が使用する資格情報を削除できます。

このタスクについて

資格情報を削除するには、以下の手順に従ってください。

手順

1. ナビゲーション・ペインで、「**ディスカバリー資格情報**」をクリックします。
「**ディスカバリー資格情報**」ページが表示されます。
2. 削除する資格情報の横にある「**削除**」() アイコンをクリックします。
3. 「**OK**」をクリックして資格情報の削除を確認します。

ディスカバリー・スケジュール

ディスカバリー・データが常に最新かつ正確になるように、ディスカバリーをスケジュールできます。ディスカバリー・スケジュールや前回実行されたディスカバリーの詳細を表示したり、ディスカバリー・スケジュールを変更したり、スケジュールされているディスカバリーを無効にしたりできます。ディスカバリーは、いつでも選択したときに実行することもできます。

始める前に

デフォルトでは、TSA は、フル・ディスカバリー・スケジュールを使用して、HMC 動的スコープ、VMware 動的スコープ、および一般ディスカバリー・スコープに定義されているすべての IT 要素をディスカバリーします。TSA は、ディスカバリー・プロセスの間、影響を最小限にするために各 IT 要素の検出を自動的に分散させます。

代わりに、ユーザー定義のスケジュールを複数作成することもできます。これにより、ネットワークや IT 要素への影響が最小限になる (理想的である) 複数の異なる日時に、細かく設定した複数のディスカバリー・スコープのディスカバリーを分散させることができます。この場合は、ユーザー定義のスケジュールを優先してフル・ディスカバリー・スケジュールを無効にする必要があります。

スケジュールされたディスカバリーの開始時に、アプライアンスはプレディスカバリー・メンテナンス・ジョブを実行します。この間は、インベントリー要約、ディスカバリー・スコープ、ディスカバリー・スケジュール、資格情報などのいくつかの機能が使用不可となります。プレディスカバリー・メンテナンス・ジョブ中には、「**要約**」画面上の「**Discovery Manager**」の状況が警告記号 () に設定されます。さらに、一部の機能が一時的に使用できなくなっていることを示す、次のような警告メッセージが TSA 画面上に表示されます。「**プレディスカバリー・メンテナンスの一部として、Discovery Manager が一時的にオフラインになります。この時間内 (通常は最大 10 分) は、ディスカバリーまたはインベントリーに関連した一部の UI 機能が情報がまったくあるいは一部のみしか表示されない可能性があります。**」

プレディスカバリー・メンテナンスが正常に実行された後、(10 分以内に) 「**要約**」ページ内の「**Discovery Manager**」の状況は「**OK**」() 状態に変わってフル・ディスカバリー・アクティビティが再開されます。

ディスカバリー・スケジュールの表示

ディスカバリー・スケジュールに関する要約情報を表示できます。

このタスクについて

ディスカバリー・スケジュールを表示するには、以下の手順に従ってください。

手順

ナビゲーション・ペインで、「ディスカバリー・スケジュール」をクリックします。

「ディスカバリー・スケジュール」ページが表示されます。

「スケジュール」ペインには、スケジュールごとに、そのスケジュールの名前、スケジュールされている次の実行、実行スケジュール、およびアクション (編集 (✎)、削除 (🗑)、有効化/無効化 (🟢/🟡)、実行 (▶)) が表示されます。

スケジュールに割り当てられているスコープ・セットすべてを表示するには、「展開」 (▶) アイコンをクリックします。フル・ディスカバリー・スケジュールの場合、デフォルトでこのアイコンは、TSA 内で定義されていてそのスケジュールに割り当てられているすべてのスコープ・セットをリストします。

Name	Next run:	Runs at	Actions
▶ Full Discovery	12/15/20 2:15 AM GMT	02:15 AM on Tuesday	✎ 🟢 ▶

Status	Schedule Name	Instance	State	Comments
🟢	Full Discovery	12/8/20 2:15 AM GMT	Complete	<ul style="list-style-type: none">Last status: OKLast run: 12/8/20 2:15 AM GMTLast completed: 12/8/20 2:37 AM GMTLast duration: 22 minutes, 58 secondsInitiator: System

図 60. ディスカバリー・スケジュール

注: TSA をフレッシュ・インストール、マイグレーション、または最新バージョンにアップグレードした場合、その新しい TSA には、デフォルトの日付 (火曜日の午前 2 時 15 分) を使用して作成された「フル・ディスカバリー」というディスカバリー・スケジュールがあります。「フル・ディスカバリー」スケジュールは編集したり無効にしたりできますが、削除することはできません。事前定義されたディスカバリー・スケジュール (有効/無効) がある場合は、マイグレーション後に同じ値が復元されます。

「履歴」ペインには、現在実行中のジョブや以前にディスカバリーされたジョブの状況やスケジュール名などの詳細が表示されます。

ディスカバリー・スケジュールの追加

指定した時刻にディスカバリー・プロセスを実行するためのスケジュールを新しく追加することができます。新しいスケジュールによって、スケジュールした日時に IT 要素のサブセットを TSA でディスカバリーすることができます。

手順

1. ナビゲーション・ペインで、「ディスカバリー・スケジュール」をクリックします。

「ディスカバリー・スケジュール」ページが表示されます。

2. 「ディスカバリー・スケジュールの追加」をクリックします。「ディスカバリー・スケジュールの追加」ページが表示されます。

Add Discovery Schedule

Asterisks (*) indicate mandatory fields that are required to complete this action.

Discovery Schedule

Enter the name for this schedule and select the Scope Sets to create a periodic discovery.

Schedule Name: *

Scope Sets:

Show only unassigned Scope Sets

Show all Scope Sets

Select Scope Sets: *

HMC Dynamic Scope Set

Schedule

Select when you want the discovery performed.

At hour: *

At minute: *

Day selection mode: *

Weekly by day(s) (Sun-Sat)

Monthly by date(s) (1-31)

On days: *

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

図 61. ディスカバリー・スケジュールの追加

3. 「スケジュール名」フィールドに、スケジュールの識別名を入力します。
4. **スコープ・セット**
 - a) 「未割り当てのスコープ・セットのみを表示」オプションを選択して、ユーザー定義の他のディスカバリー・スケジュールに割り当てられていないスコープ・セットのみを表示します。
 - b) 「すべてのスコープ・セットを表示」オプションを選択して、すべてのスコープ・セットを表示します。
5. 「スコープ・セットの選択」リストから、対象のスコープ・セットを選択します。
「すべて選択」/「すべて選択解除」を使用してすべてのスコープ・セットを選択したり選択解除したりできます。
6. 「時刻(時間)」リストおよび「時刻(分)」リストを使用して新しい時刻を選択します。
7. 「日選択モード」を選択します。

毎週(日曜日 - 土曜日)
特定の曜日(複数可)にディスカバリーをスケジュールする場合は「毎週(日曜日 - 土曜日)」オプションを選択します。

Schedule

Select when you want the discovery performed.

At hour: *

At minute: *

Day selection mode: *

Weekly by day(s) (Sun-Sat)

Monthly by date(s) (1-31)

On days: *

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

図 62. 毎週 (日曜日 - 土曜日)

「曜日」フィールドで該当するチェック・ボックスをチェックすることで、週の1つ以上の曜日を選択します。

毎月の日 (1-31)

毎月特定の日 (複数可) にディスカバリーをスケジュールする場合は、「毎月の日 (1-31)」オプションを選択します。

「曜日」フィールドで該当するチェック・ボックスをチェックすることで、月の1つ以上の日を選択します。

注: 特定の月の最終日より後の日を選択すると、その特定の月の最終日にジョブがトリガーされません。

8. 「保存」をクリックします。

「ディスカバリー・スケジュール」ページが、新規スケジュールを含んだ状態で再表示されます。

ディスカバリー・スケジュールの変更

TSA には、指定された時刻にディスカバリー・プロセスを実行するための、デフォルトのスケジュールが設定されています。必要に応じて、デフォルトのスケジュールを変更することも、カスタムのスケジュールを使用することもできます。

手順

1. ナビゲーション・ペインで、「ディスカバリー・スケジュール」をクリックします。

「ディスカバリー・スケジュール」ページが表示されます。

2. 「スケジュールの編集」 (✎) アイコンをクリックします。

「ディスカバリー・スケジュールの編集」ページが表示されます。

- a) 「ディスカバリー・スケジュール」ペインで、必要に応じて「スケジュール名」、「スコープ・セット」、および「スコープ・セットの選択」を編集します。

注: デフォルトのフル・ディスカバリーについては、これらのフィールドは編集できません。

- b) 「スケジュール」ペインで、必要に応じて「時刻 (時間)」、「時刻 (分)」、「日選択モード」、および「曜日」を編集します。

3. 「保存」をクリックします。

「ディスカバリー・スケジュール」ページが、変更されたスケジュールが表示された状態で再表示されます。

ディスカバリー・スケジュールの無効化

スケジュール済みディスカバリーを無効にできます。

始める前に

注：ユーザー定義のディスカバリー・スケジュールを構成した場合は、同じ IT 要素が重複してディスカバリーされないように、「フル・ディスカバリー」スケジュールを無効にすることをお勧めします。

手順

スケジュール済みディスカバリーを無効にするには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スケジュール」をクリックします。
「ディスカバリー・スケジュール」ページが表示されます。
2. 該当するスケジュールの「有効化」または「無効化」( または  アイコンをクリックして、ディスカバリー・スケジュールを無効/有効にします。

ディスカバリー・スケジュールの削除

スケジュール済みディスカバリーを削除できます。

手順

スケジュール済みディスカバリーを削除するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スケジュール」をクリックします。
「ディスカバリー・スケジュール」ページが表示されます。
2. 削除するそれぞれのスケジュールの「削除」() アイコンをクリックします。
注：「フル・ディスカバリー」スケジュールは削除できませんが、必要に応じて無効にすることはできます。
選択したディスカバリー・スケジュールの削除を確認するためのメッセージが表示されます。
3. 「OK」をクリックしてスケジュールを削除します。

ディスカバリーの実行

スケジュールされている次のディスカバリーを待たずに、オンデマンドでディスカバリーを実行できます。定義されているすべてのディスカバリー・スコープ、特定のディスカバリー・スケジュール、または特定のディスカバリー・スコープまたはそのセットで、ディスカバリーを実行できます。

手順

すべての定義済みスコープでディスカバリーを実行するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スケジュール」をクリックします。「ディスカバリー・スケジュール」ページが表示されます。
2. 「今すぐフル・ディスカバリーを実行」をクリックします。「履歴」セクションが更新され、ディスカバリーが実行中であることが示されます。
注：TSA は、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。その結果、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。「要約」ページの「ジョブの要約」セクションで、ディスカバリー・プロセスをモニターできます。
3. 特定のスコープに対してディスカバリーを実行するには、そのスコープの「実行」() をクリックします。
4. 「要約」ページ (ナビゲーション・ペインで「要約」をクリックします) をチェックします。「ジョブの要約」ペインにディスカバリーが表示されます。「要約」ページは、TSA の現在の状態を表示するために

定期的に最新表示されます。「**ジョブの要約**」ペインにジョブがリストされなくなったら、「**アクティビティ・ログ**」をチェックします(ナビゲーション・ペインで「**アクティビティ・ログ**」をクリックします)。ディスカバリーは正常に完了します。

一般スコープ・セットでのディスカバリーの実行

手順

特定スコープ・セットでディスカバリーを実行するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「**ディスカバリー・スコープ**」 > 「**一般ディスカバリー・スコープ**」をクリックします。

「**一般ディスカバリー・スコープ**」ページが表示されます。このページには、この TSA に対して定義されているすべてのスコープ・セットのリストが表示されます。



図 63. 特定のスコープでのディスカバリーの実行

2. 特定のスコープ・セットに対してディスカバリーを実行するには、そのスコープ・セットの「**実行**」() アイコンをクリックします。
3. 「**要約**」ページ(ナビゲーション・ペインで「**要約**」をクリックします)をチェックします。「**ジョブの要約**」ペインにディスカバリーが表示されます。「**要約**」ページは、TSA の現在の状態を表示するために定期的に最新表示されます。「**ジョブの要約**」ペインにジョブがリストされなくなったら、「**アクティビティ・ログ**」をチェックします(ナビゲーション・ペインで「**アクティビティ・ログ**」をクリックします)。ディスカバリーは正常に完了します。

HMC 動的スコープ・セットでのディスカバリーの実行

手順

特定スコープ・セットでディスカバリーを実行するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「**ディスカバリー・スコープ**」 > 「**HMC 動的スコープ**」をクリックします。

「HMC 動的スコープ」ページが表示されます。このページには、この TSA に対して定義されているすべてのスコープ・セットのリストが表示されます。

図 64. HMC 動的スコープ

2. 特定のスコープ・セットに対してディスカバリーを実行するには、そのスコープ・セットの「実行」(▶) アイコンをクリックします。
3. 「要約」ページ (ナビゲーション・ペインで「要約」をクリックします) をチェックします。「ジョブの要約」ペインにディスカバリーが表示されます。「要約」ページは、TSA の現在の状態を表示するために定期的に最新表示されます。「ジョブの要約」ペインにジョブがリストされなくなったら、「アクティビティ・ログ」をチェックします (ナビゲーション・ペインで「アクティビティ・ログ」をクリックします)。ディスカバリーは正常に完了します。

VMware スコープ・セットでのディスカバリーの実行

手順

特定スコープ・セットでディスカバリーを実行するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「VMware 動的スコープ・セット」をクリックします。

「VMware 動的スコープ」ページが表示されます。このページには、この TSA に対して定義されているすべてのスコープ・セットのリストが表示されます。

図 65. VMware 動的スコープでのディスカバリーの実行

2. 特定のスコープ・セットに対してディスカバリーを実行するには、そのスコープ・セットの「実行」(▶) をクリックします。

3. 「要約」 ページ (ナビゲーション・ペインで「要約」をクリックします) をチェックします。「ジョブの要約」 ペインにディスカバリーが表示されます。「要約」 ページは、TSA の現在の状態を表示するために定期的に最新表示されます。「ジョブの要約」 ペインにジョブがリストされなくなったら、「アクティビティ・ログ」 をチェックします (ナビゲーション・ペインで「アクティビティ・ログ」 をクリックします)。ディスカバリーは正常に完了します。

スコープでのディスカバリーの実行

スケジュールされている次のディスカバリーを待たずに、オンデマンドでディスカバリーを実行できます。定義されているすべてのディスカバリー・スコープ、特定のディスカバリー・スケジュール、または特定のディスカバリー・スコープまたはそのセットで、ディスカバリーを実行できます。

一般スコープでのディスカバリーの実行

手順

1. ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「一般ディスカバリー・スコープ」 をクリックします。「一般ディスカバリー・スコープ」 ページが表示されます。

General Discovery Scopes

The discovery process searches for IT elements within your infrastructure. A Discovery Scope defines a single IP address or range that is discovered during the discovery process. Scopes are grouped into user named Scope Sets.

Name	Actions
ESXi67_Scope	
ESXi_Scope	
IFS900_Scope	
PT_Scope	
TS7760_Scope	
pFlexCMM_Scope	
vCenter67_Scope	

[+ Add New Scope Set](#)

図 66. ディスカバリー・スコープ

2. ディスカバリー対象のスコープを含むスコープ・セットをクリックします。「ディスカバリー・スコープ・セット」 ページが表示されます。このページには、該当のスコープ・セットに対して定義したすべてのスコープが表示されます。



図 67. 特定のスコープでのディスカバリーの実行

- 特定のスコープに対してディスカバリーを実行するには、そのスコープの「実行」(▶) アイコンをクリックします。
- 「要約」ページ(ナビゲーション・ペインで「要約」をクリックします)をチェックします。「ジョブの要約」ペインにディスカバリーが表示されます。「要約」ページは、TSA の現在の状態を表示するために定期的に最新表示されます。「ジョブの要約」ペインにジョブがリストされなくなったら、「アクティビティ・ログ」をチェックします(ナビゲーション・ペインで「アクティビティ・ログ」をクリックします)。ディスカバリーは正常に完了します。

HMC 動的スコープでのディスカバリーの実行

手順

- ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「HMC 動的スコープ」をクリックします。「HMC 動的スコープ」ページが表示されます。

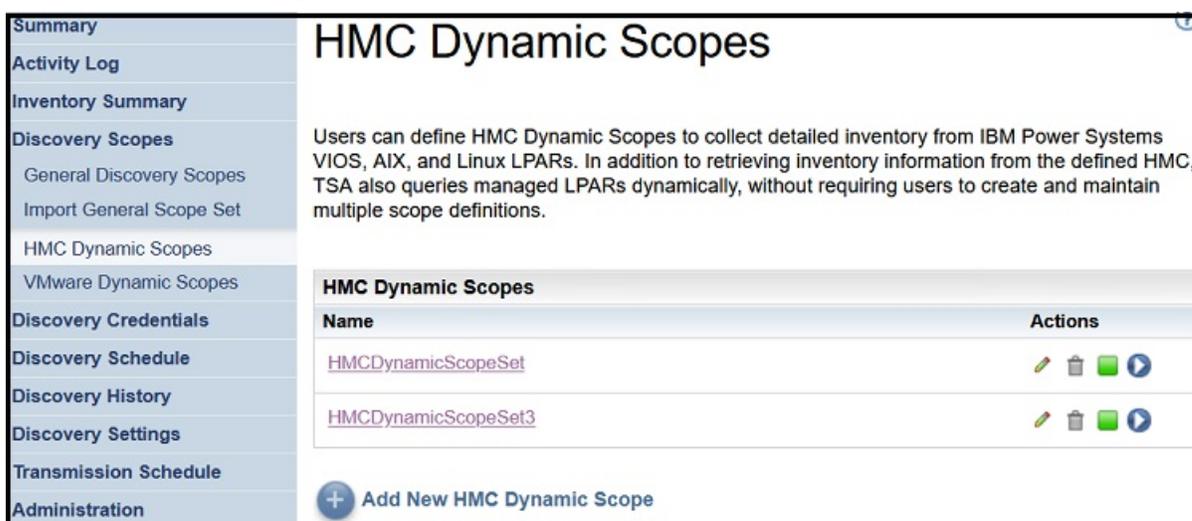


図 68. HMC 動的スコープ

- ディスカバー対象のスコープを含むスコープ・セットをクリックします。「HMC 動的スコープ・セット」ページが表示されます。このページには、該当のスコープ・セットに対して定義したすべてのスコープが表示されます。

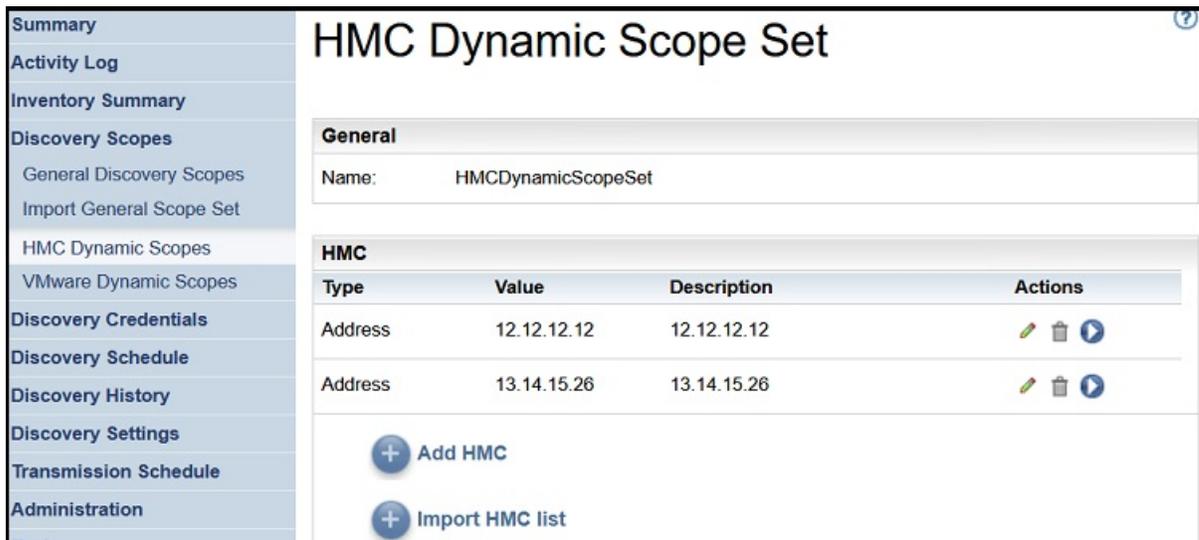


図 69. 特定のスコープでのディスカバリーの実行

- 特定のスコープに対してディスカバリーを実行するには、そのスコープの「実行」(▶)をクリックします。
- 「要約」ページ (ナビゲーション・ペインで「要約」をクリックします) をチェックします。「ジョブの要約」ペインにディスカバリーが表示されます。「要約」ページは、TSA の現在の状態を表示するために定期的に最新表示されます。「ジョブの要約」ペインにジョブがリストされなくなったら、「アクティビティ・ログ」をチェックします (ナビゲーション・ペインで「アクティビティ・ログ」をクリックします)。ディスカバリーは正常に完了します。

VMware 動的スコープでのディスカバリーの実行

手順

- ナビゲーション・ペインで、「ディスカバリー・スコープ」 > 「VMware 動的スコープ」をクリックします。「VMware 動的スコープ」ページが表示されます。

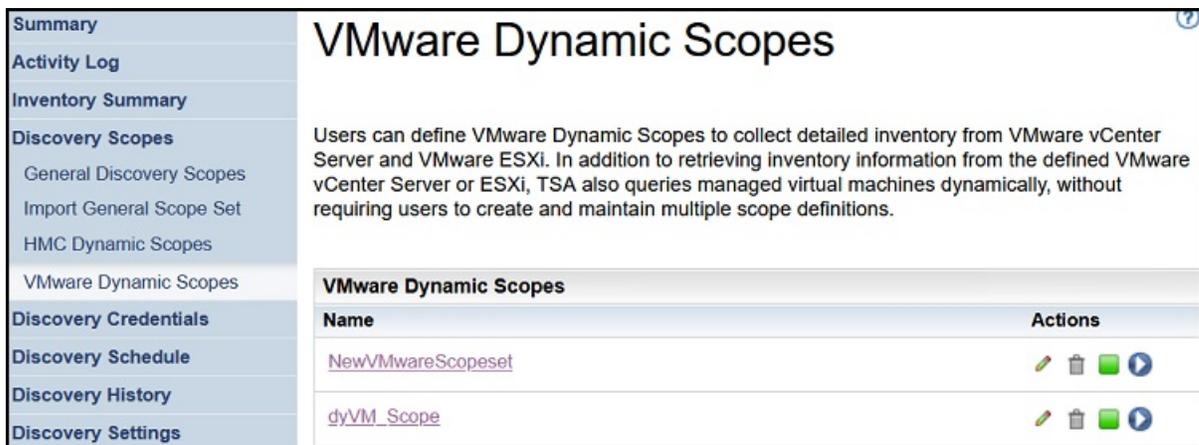


図 70. VMware 動的スコープ

- ディスカバー対象のスコープを含むスコープ・セットをクリックします。「VMware 動的スコープ・セット」ページが表示されます。このページには、該当のスコープ・セットに対して定義したすべてのスコープが表示されます。

図 71. VMware 動的スコープでのディスカバリーの実行

- 特定のスコープに対してディスカバリーを実行するには、そのスコープの「実行」(▶) アイコンをクリックします。
- 「要約」ページ (ナビゲーション・ペインで「要約」をクリックします) をチェックします。「ジョブの要約」ペインにディスカバリーが表示されます。「要約」ページは、TSA の現在の状態を表示するために定期的に最新表示されます。「ジョブの要約」ペインにジョブがリストされなくなったら、「アクティビティ・ログ」をチェックします (ナビゲーション・ペインで「アクティビティ・ログ」をクリックします)。ディスカバリーは正常に完了します。

ディスカバリー履歴

ディスカバリーの完了後にその詳細を見たり、ディスカバリーの 診断ログ・ファイルをダウンロードしたりできます。

手順

ディスカバリー履歴を表示したり診断ログ・ファイルをダウンロードするには、以下の手順に従ってください。

- ナビゲーション・ペインで、「ディスカバリー履歴」をクリックします。
「ディスカバリー履歴」ページが表示されます。ディスカバリー・エントリーのリストが表示されます。エントリーごとに、ディスカバリーの状況、名前、開始時刻、終了時刻が表示されます。

Discovery History

This page allows you to review the details of a discovery after it has completed.

History Entries				
Status	Name	Start Time	End Time	Actions
Complete	IFS 820 (L3)	6/16/15 3:10 AM BST	6/16/15 3:22 AM BST	
Complete	IFS 820 (L1)	6/16/15 3:08 AM BST	6/16/15 3:09 AM BST	
Complete	Full Discovery (L3) : 2 of 3 (IFS 820)	6/16/15 2:37 AM BST	6/16/15 2:49 AM BST	
Complete	Full Discovery (L1) : 2 of 3 (IFS 820)	6/16/15 2:34 AM BST	6/16/15 2:36 AM BST	
Complete	Full Discovery (L3) : 1 of 3 (IFS 840)	6/16/15 2:27 AM BST	6/16/15 2:34 AM BST	

図 72. ディスカバリー履歴

- 「履歴エントリー」リスト内のエントリーに関する詳細情報を表示するには、その履歴エントリーの名前をクリックします。
「エントリー情報」ペインに、選択したディスカバリーに関する情報が表示されます。
- ディスカバリーの診断ログ・ファイルをダウンロードするには、そのディスカバリーの「ダウンロード」() アイコンをクリックします。
- ディスカバリーの診断ログ・ファイルを削除するには、そのディスカバリーの「削除」() アイコンをクリックします。

送信スケジュール

ディスカバリー・データが定期的に IBM サポートに送信されるように、データの送信をスケジュールできます。送信スケジュールや前回実行された送信の詳細を表示したり、送信スケジュールを変更したり、スケジュールされている送信を無効にしたりできます。また、いつでも選択したときにデータを IBM に送信できます。

送信スケジュールの表示

送信スケジュールに関する要約情報を表示できます。

このタスクについて

送信スケジュールを表示するには、以下の手順に従ってください。

手順

ナビゲーション・ペインで、「送信スケジュール」をクリックします。

「送信スケジュール」ページが表示されます。

「スケジュール」ペインには、スケジュールされている次の実行とその日時が表示されます。「履歴」ペインには、現在実行されている送信ジョブと、過去の送信ジョブの状況と追加の詳細情報が表示されます。

送信スケジュールの変更

TSA には、指定された時刻に送信プロセスを実行するための、デフォルトのスケジュールが設定されています。このスケジュールはニーズに合わせて変更できます。

手順

1. ナビゲーション・ペインで、「送信スケジュール」をクリックします。

「送信スケジュール」ページが表示されます。

「スケジュール」ペインには、スケジュールされている次の実行とその日時が表示されます。「履歴」ペインには、現在実行されている送信ジョブと、過去の送信ジョブの状況と追加の詳細情報が表示されます。

2. 「スケジュールの編集」をクリックします。

「送信スケジュール」ページが表示されます。

Summary
Activity Log
Inventory Summary
Discovery Scopes
Discovery Credentials
Discovery Schedule
Discovery History
Discovery Settings
Transmission Schedule
Administration
Tools
Documentation
IBM Support Insights Portal

Transmission Schedule

Asterisks (*) indicate mandatory fields that are required to complete this action.

Enable Schedule

Select whether periodic transmission should be performed.

Select: * Enable scheduled transmission ▼

Schedule

Select when you want the transmission performed.

At hour: * 00 ▼

At minute: * 00 ▼

Day selection mode: *

Weekly by day(s) (Sun-Sat)

Monthly by date(s) (1-31)

On days: *

01 02 03 04 05 06 07
 08 09 10 11 12 13 14
 15 16 17 18 19 20 21
 22 23 24 25 26 27 28
 29 30 31

If days are picked beyond the last day of any given month, the job will be triggered the last day of such month instead.

Save Cancel

図 73. 送信スケジュールの編集

- a) 「時刻(時間)」リストおよび「時刻(分)」ドロップダウン・リストを使用して新しい時刻を選択します。
- b) 「日選択モード」を選択します。

毎週(日曜日 - 土曜日)

特定の曜日(複数可)に送信をスケジュールする場合は「毎週(日曜日 - 土曜日)」オプションを選択します。

Schedule	
Select when you want the transmission performed.	
At hour: *	00 ▼
At minute: *	00 ▼
Day selection mode: *	<input checked="" type="radio"/> Weekly by day(s) (Sun-Sat) <input type="radio"/> Monthly by date(s) (1-31)
On days: *	<input checked="" type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday

図 74. 毎週 (日曜日 - 土曜日)

「曜日」フィールドで該当するチェック・ボックスをチェックすることで、週の1つ以上の曜日を選択します。

毎月の日 (1-31)

毎月特定の日 (複数可) に送信をスケジュールする場合は、「毎月の日 (1-31)」オプションを選択します。

「曜日」フィールドで該当するチェック・ボックスをチェックすることで、月の1つ以上の日を選択します。

注: 特定の月の最終日より後の日を選択すると、その特定の月の最終日にジョブがトリガーされます。

3. 「保存」をクリックします。

「送信スケジュール」ページが、新規スケジュールを含んだ状態で再表示されます。

送信スケジュールの無効化

スケジュール済みデータ送信を無効にできます。

手順

スケジュール済み送信を無効にするには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「送信スケジュール」をクリックします。

「送信スケジュール」ページが表示されます。

2. 「スケジュールの編集」をクリックします。

「送信スケジュール」ページが表示されます。

3. 「スケジュールの有効化」ペインで、「定期送信を無効にする」を選択します。

4. 「保存」をクリックします。

「ディスカバリー・スケジュール」ページが表示され、「スケジュール」ペインに、スケジュールされたディスカバリーが無効になっていることが表示されます。「定期送信を有効にする」をクリックして、スケジュールされた送信を有効にすることができます。

送信の実行

スケジュールされている次の送信を待たずに、オンデマンドで送信を実行できます。

手順

1. ナビゲーション・ペインで、「送信スケジュール」をクリックします。
「送信スケジュール」ページが表示されます。

The screenshot shows the 'Transmission Schedule' page. On the left is a navigation sidebar with items like Summary, Activity Log, Inventory Summary, Discovery Scopes, Discovery Credentials, Discovery Schedule, Discovery History, Discovery Settings, Transmission Schedule (highlighted), Administration, Tools, Documentation, and IBM Support Insights Portal. The main content area has the title 'Transmission Schedule' and a note: 'Previously collected data will be transmitted to IBM at the specified time.' Below this is a 'Schedule' section with a table:

Schedule	
Next run:	12/13/19 9:35 AM GMT
Runs at:	09:35 AM on month day(s): 13, 14, 15

Below the schedule is a 'History' section with a table:

Status	Instance	State	Comments
✓	11/19/19 10:09 PM GMT	Complete	<ul style="list-style-type: none">• Last status: OK• Last run: 11/19/19 10:09 PM GMT• Last completed: 11/19/19 10:50 PM GMT• Last duration: 40 mins,57 secs• Initiator: admin
✓	11/19/19 9:13 PM GMT	Complete	<ul style="list-style-type: none">• Last status: OK• Last run: 11/19/19 9:13 PM GMT• Last completed: 11/19/19 9:44 PM GMT• Last duration: 31 mins,12 secs• Initiator: admin
✓	11/10/19 10:54 PM GMT	Complete	<ul style="list-style-type: none">• Last status: OK• Last run: 11/10/19 10:54 PM GMT• Last completed: 11/10/19 11:26 PM GMT• Last duration: 32 mins,17 secs• Initiator: admin

At the bottom of the main content area are two buttons: 'Edit Schedule' and 'Run Transmission Now'.

図 75. 今すぐ送信を実行

2. 「今すぐ送信を実行」をクリックします。
「履歴」ペインが更新され、送信が実行中であることが示されます。
3. 「要約」ページ (ナビゲーション・ペインで「要約」をクリックします) をチェックします。「ジョブの要約」ペインに送信が表示されます。「要約」ページは、TSA の現在の状態を表示するために定期的に最新表示されます。「ジョブの要約」ペインにジョブがリストされなくなったら、「アクティビティ・ログ」をチェックします (ナビゲーション・ペインで「アクティビティ・ログ」をクリックします)。送信は正常に完了します。

データ・スナップショット

TSA によって収集された未加工、未フォーマットのデータのローカル・コピーを生成して保存できます (データは IBM に送信されません)。また、IBM に最後に送信されたデータも表示できます。

1. ナビゲーション・ペインで、「管理」 > 「データ・スナップショット」をクリックします。「データ・スナップショット」ページが表示されます。



図 76. データ・スナップショット

注: 「前回のデータ・スナップショットをダウンロード」 ボタンは、完了した送信またはデータ・スナップショットがある場合のみ有効になります。

2. 「今すぐデータ・スナップショットを生成」 をクリックして、TSA によって最後に検出されたデータを収集して新しいデータ・スナップショットを生成します。「データ・スナップショットが進行中です。これには最大 2 時間かかる場合があります。 アクティビティ・ログまたは「要約」 ページで状況を確認してください」というメッセージが表示されます。「要約」 ページを表示するには、ナビゲーション・メニューの「要約」 をクリックします。「ジョブの要約」 ペインに、データ・スナップショットの収集状況が、収集が完了するまで表示されます。データ・スナップショット要求の完了状況を確認するには、ナビゲーション・メニューの「アクティビティ・ログ」 をクリックします。
3. 送信サービスまたはデータ・スナップショット・サービスが完了すると、「データ・スナップショット生成日」 が表示されます。



図 77. データ・スナップショット生成日

4. 「前回のデータ・スナップショットをダウンロード」 をクリックして、最新のデータ・スナップショットをダウンロードします。結果のファイル (*collection.tar.xz*) の場所を指定します。データの量によっては、ダウンロード操作に時間がかかる場合があります。*.tar.xz* アーカイブの内容を解凍するには、*tar* ユーティリティ (Linux の場合) または *7-Zip* ユーティリティ (Linux と Windows の両方で使用可能) を使用します。

注:

- 送信ジョブまたは収集ジョブが進行中の場合は、「収集ジョブが現在実行中です。前回のデータ・スナップショットは <<timestamp>> に生成されました。この収集をダウンロードしますか?」 というメッセージが表示されます。
 - 「OK」 をクリックしてダウンロードを続行します。
 - ダウンロードをキャンセルして現在実行中の収集ジョブが完了するのを待つには、「キャンセル」 をクリックします。

- 送信ジョブも収集ジョブも進行中でない場合は、「前回のデータ・スナップショットは <<timestamp>> に生成されました。この収集をダウンロードしますか?」というメッセージが表示されます。「OK」をクリックしてダウンロードを続行します。

インベントリー要約の表示

「インベントリー要約」ページを使用して、コンピューター・システム、オペレーティング・システム、ストレージ・サブシステムなどのディスカバーされた IT 要素の要約を表示します。

「インベントリー要約」ページを表示するには、ナビゲーション・ペインで「インベントリー要約」をクリックします。

Inventory Summary ?

A general summary of IT elements that have been discovered. Some IT elements may not be represented on this summary. For a complete report with detailed information and analysis refer to the Technical Support Appliance reports from your IBM representative.

Inventory Summary	
Hypervisors	No elements discovered
Computer Systems	No elements discovered
Operating Systems	AIX (1)
	Linux (1)
Network Elements	No elements discovered
Storage	IBM SVC, V7000/V3700, V7000 Unified Storage (1)
Unknown IPs	No elements discovered
Last generated: 3/27/18 4:34 AM BST	
Download Inventory Summary	

図 78. インベントリー要約

「インベントリー要約」ページには、IT 要素の 6 つの異なるグループが表示されます。

- **ハイパーバイザー:** HMC、IBM Flex System Manager、VMware、VIOS などのハイパーバイザーが含まれます。
- **コンピューター・システム:** 物理的なコンピューター・システムを含む。
- **オペレーティング・システム:** ベアメタル上または仮想化環境で実行される AIX、Linux などのオペレーティング・システムが含まれます。
- **ネットワーク要素:** スイッチとルーターを含む。
- **ストレージ:** IBM XIV、IBM FlashSystem、EMC、および HP ストレージ・デバイスなどのストレージ・サブシステムが含まれます。加えて、以下のテープ・デバイスも含まれます。
- **不明な IP:** 次のような理由で分類されていない可能性のあるデバイス:

- Summary
- Activity Log
- Inventory Summary
- Discovery Scopes
- Discovery Credentials
- Discovery Schedule
- Discovery History
- Discovery Settings
- Transmission Schedule
- Administration
- Tools
- Network Tools
- Unknown Devices
- Authentication Status
- DB Tools
- Setup Wizard
- Documentation
- IBM Support Insights Portal

Authentication Status

This page provides a summary of the IT elements, defined in scope sets, that have been identified to potentially have issues with credentials. Either no credentials are defined for the associated scope set, credentials are defined for the scope set but none are successful, or a credential that was successful in the past was not successful on the latest discovery attempt. This information should help to determine where new credentials should be created, or where existing credentials should be updated with the correct password.

Note:
Once the problem preventing an element from being identified is resolved, it will no longer display on this list.

IP Address	Last Attempted	Last Successful
9.155.120.226	2/12/20 6:28:14 AM GMT	
9.182.192.107	3/10/20 4:14:43 AM GMT	
9.5.12.187	2/26/20 4:12:57 AM GMT	
9.5.12.201	2/26/20 4:12:57 AM GMT	
9.5.54.240	2/26/20 4:12:57 AM GMT	
9.5.95.56	2/26/20 4:12:57 AM GMT	

1 - 6 of 6 entries Entries per page: 20 | 50 | 100

Device Information

Address:
9.155.120.226

Last Attempted:
2/12/20 6:28:14 AM GMT

Last Successful:

Ports open:
[22, 23, 80, 427, 443, 445, 1750, 1751, 2463, 5986, 5988, 5989, 7778]

Last successful credential used:

Credentials associated with scope:
TS7760_Cred

Scopes including this IP address:
TS7760_Scope

図 80. 認証状況

状況には、資格情報の問題を報告したすべてのデバイス IP が表示されます。問題は、次のような理由が原因である可能性があります。

- 関連付けられたスコープ・セットに対して資格情報が定義されていない。
- スコープ・セットに対して資格情報が定義されているが、認証に成功していない。
- 以前は認証に成功していた資格情報が、直近のディスカバリーの試行で成功しなかった。

各 IP アドレスのリンクをクリックすると、そのデバイスの情報 (前回の試行日時、前回の成功日時、開かれたポート、最後に使用して成功した資格情報、資格情報の最終変更日付、スコープに関連付けられた資格情報、およびこの IP アドレスが含まれているスコープ) が表示されます。この情報は、新しい資格情報を作成する場所、または正しいパスワードで既存の資格情報を更新する必要がある場所を判別するうえで役立ちます。

注: デバイスの資格情報の問題が解決されれば、それに対応するデバイス IP は、リストに表示されなくなります。

不明なデバイス

TSA でディスカバーされたものの、完全に識別できないデバイスに関する情報を表示できます。

これらの不明なデバイスを表示するには、ナビゲーション・ペインで「ツール」 > 「不明なデバイス」をクリックします。「不明なデバイス」ページが表示されます。

「不明な IP」リストの項目をクリックすると、そのデバイスに関する追加の情報が表示されます。

第6章 管理タスクのセットアップ

状況情報

TSA は要約情報、ログ、レポートを提供するので、ジョブとディスカバーされたインベントリーに関する情報や製品情報を即時に見つけることができます。

ナビゲーション・ペインで「要約」をクリックすると、ジョブ、インベントリー、製品情報に関するあらましの要約情報を表示できます。「要約」ページは頻繁にリフレッシュされ、最新の要約情報が表示されます。「要約」ページには、以下の情報が含まれます。

- システム状況

「システム状況」ペインには、現在実行されているサービスとタスクの状況が表示されます。サービスに関するページを表示するには、「システム状況」ペインでサービスの名前をクリックします。

- ジョブの要約

「ジョブの要約」ペインには、現在のジョブの要約が表示されます。

- インベントリー要約

「インベントリー要約」ペインには、ディスカバーされたインベントリーのリストが表示されます。

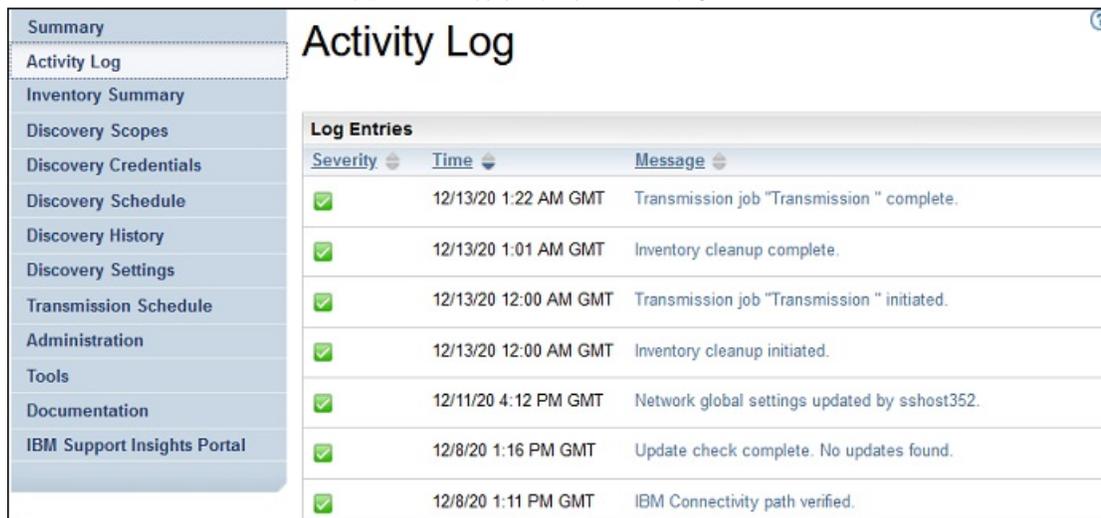
- 製品情報

「製品情報」ペインには、TSA のホスト名と ID が表示されます。

アクティビティ・ログの表示

アクティビティ・ログには、ディスカバー・プロセスおよび送信プロセスに関するログ・メッセージが表示されます。アクティビティ・ログのエントリーをクリックすると詳細が表示されます。

ナビゲーション・ペインの「アクティビティ・ログ」をクリックすると、アクティビティ・ログを表示できます。ログ・エントリーのリストが表示されます。各エントリーには、メッセージ、重大度、およびアクティビティが発生した時間が表示されます。



Activity Log		
Log Entries		
Severity	Time	Message
✓	12/13/20 1:22 AM GMT	Transmission job "Transmission " complete.
✓	12/13/20 1:01 AM GMT	Inventory cleanup complete.
✓	12/13/20 12:00 AM GMT	Transmission job "Transmission " initiated.
✓	12/13/20 12:00 AM GMT	Inventory cleanup initiated.
✓	12/11/20 4:12 PM GMT	Network global settings updated by sshost352.
✓	12/8/20 1:16 PM GMT	Update check complete. No updates found.
✓	12/8/20 1:11 PM GMT	IBM Connectivity path verified.

図 81. アクティビティ・ログ

注：複数のディスカバーがそれぞれのスコープ・セットで実行されるため、フル・ディスカバーでは複数のログ・エントリーが存在する可能性があります。

アクティビティ・ログ・エントリーの詳細を表示するには、エントリーのメッセージをクリックします。

ログ・ファイルをコンピューターに保存するには、「すべてのログをダウンロード」をクリックします。

ログを消去するには、「ログのクリア」をクリックします。

インベントリー・クリーンアップ・アーカイブの表示

「インベントリー・クリーンアップのスケジュール」で指定した休止期間に従ってクリーンアップされたインベントリーを表示できます

このタスクについて

削除したインベントリーを表示するには、以下の手順に従ってください。

手順

1. 「インベントリー・クリーンアップのスケジュール」ページで、「クリーンアップ・アーカイブの表示」をクリックします。「インベントリー・クリーンアップ・アーカイブ」ページが表示されます。

Inventory Cleanup Archive

This page allows you to view and download a list of inventory elements that have not been detected by the discovery job for a time longer than the defined dormant age and have been purged from inventory. These elements will be archived for one year after the date they were purged.

Archived Inventory Entries	
Display Name: c642a-m2b10.pok.stglabs.ibm.com	Last Seen: 2015-10-10 09:38 CDT
Name: c642a-m2b10	Cleaned Up: 2015-11-11 11:19 CST
Subtype: LinuxUnitaryComputerSystem	Manufacturer: IBM
Scope: ?	Model: 8853AC1
Context IP: 9.57.20.84	Serial Number: KQHYLFC
Display Name: c642a-m2b9.pok.stglabs.ibm.com	Last Seen: 2015-10-10 09:38 CDT
Name: c642a-m2b9	Cleaned Up: 2015-11-11 11:19 CST
Subtype: LinuxUnitaryComputerSystem	Manufacturer: IBM
Scope: ?	Model: 7870AC1
Context IP: 9.57.20.83	Serial Number: KQXXDTH

[Back to top](#)

Options

Order by: Cleaned Up

Reverse order Compact view

Download

図 82. インベントリー・クリーンアップ・アーカイブ

2. 「インベントリー・クリーンアップ・アーカイブ」ページで、クリーンアップ・プロセスの一部としてインベントリーから消去されている要素を表示できます。

注:

- このアーカイブ内でインベントリー情報を参照できる期間は1年間のみです。1年後、アーカイブ情報は消去されます。
 - 定義済みのすべてのターゲットが1年以内に活発にディスカバーされている場合、アーカイブは空になります(つまり、クリーンアップされているオブジェクトはありません)。
3. インベントリーの詳細を再配列するには、「オプション」ペインを使用します。
 - a) インベントリーの詳細の表示の順序を設定するには、「オプション」ペインから「順序」プロパティを選択し、「適用」をクリックします。
 - b) 選択したプロパティの逆順で詳細を表示するには、「逆順」オプションを選択します。
 - c) インベントリーの要約を表示するには、「コンパクト・ビュー」オプションを選択します。
 4. インベントリーの詳細をダウンロードするには、「テキスト・ファイルとして」または「CSVファイルとして」をクリックします。インベントリーの詳細のデータをローカルで処理する場合や、そのデータを長期間(1年より長く)コンピューター上に保持する場合は、インベントリーの詳細を保存します。このアーカイブ内に保存されるデータは、1年間のみ維持され、その後消去されます。

パスワード

TSA ユーザー・アカウントを保護するためのパスワードを使用します。

パスワードの変更

TSA ユーザー・パスワードを変更します。

手順

1. ナビゲーション・ペインで、「管理」 > 「パスワード」をクリックします。
「パスワード」ページが表示されます。
2. 「現在のパスワード」フィールドに現在のパスワードを入力します。
3. 「新規パスワード」フィールドに新規パスワードを入力します。
パスワードは以下のルールに準拠する必要があります。
 - 長さが8文字以上である。
 - 少なくとも1文字の英字と英字以外の文字を含む。
 - ユーザー名を含まない。
 - 直前の8つのパスワードのいずれかと同じパスワードを使用しない。
 - 少なくとも90日ごとに変更する必要があるが、1日に2回以上変更してはならない。
4. 「パスワードの確認」フィールドに新規パスワードを再入力します。
パスワードが保存される前に、入力した2つのパスワードが比較されて一致していることが確認されます。
5. 「保存」をクリックします。

次のタスク

重要: パスワードはリカバリーできないので、パスワードを紛失したり忘れてしまった場合は、TSA にログインして資格情報を変更することはできません。ユーザー・アカウント、または管理者アカウント (アカウントが複数ある場合) のパスワードを紛失したり忘れてしまったときは、TSA 管理者に連絡してください。(TSA に付属する) デフォルトの管理者アカウントのパスワードを紛失したり忘れてしまった場合は、IBM サポートに連絡してください。詳細については、[21 ページの『Technical Support Appliance へのログイン』](#)のセクションを参照してください。

セキュリティ

TSA のセキュリティ機能やユーティリティーにアクセスしたり変更を加えたりできます。

「セキュリティ」ページには、使用可能なセキュリティ・ユーティリティーがリストされます。このページで、セッション・タイムアウトの設定を変更したり、すべてのユーザー・アカウントのパスワードの最大使用日数を変更したりできます。

セッション・タイムアウト設定の変更

セキュリティのために、操作が行われない期間が一定期間続くと、ユーザーは TSA からログアウトされます。TSA からのユーザーの自動ログアウトを防止したり、ユーザーがログアウトされるまでの時間を変更したりすることができます。

セッション・タイムアウトの無効化

セッション・タイムアウトを無効にすると、操作が行われない期間が一定期間続いてもユーザーは TSA から自動的にログアウトされません。

手順

1. 「セッション・タイムアウトを無効にする」チェック・ボックスをチェックします。
2. 「セッション・タイムアウト設定の変更」をクリックします。

セッション・タイムアウト値の変更

デフォルトでは、操作が行われない状態が 20 分間続くと、ユーザーはログアウトされます。セッション・タイムアウト値を変更すると、ユーザーがログアウトされるまでの時間を伸ばすことができます。

手順

1. 「セッション・タイムアウトを無効にする」チェック・ボックスをクリアします。
2. 「セッション・タイムアウト」フィールドで、ユーザーが TSA からログアウトされるまでの時間を秒単位で入力します。

注: このセッション・タイムアウトの値を 20 分未満にすることはできません。

3. 「セッション・タイムアウト設定の変更」をクリックします。

パスワードの最長使用日数の変更

セキュリティ対策として、すべてのユーザーは、指定された日数の経過後に TSA ログイン・パスワードの変更を強制されます。デフォルトでは、パスワードの最長日数は 90 日ですが、30 日または 60 日に変更することもできます。

手順

1. ナビゲーション・ペインで、「管理」 > 「セキュリティ」をクリックします。「セキュリティ」ページが表示されます。
2. 「セキュリティ」ページで、スクロールダウンして「パスワードの最長使用日数」ペインを表示します。
3. 「パスワードの最長使用日数」ペインで、「最長日数」ドロップダウン・リストから日数 (30 日、60 日、または 90 日) を選択します。
4. 「パスワードの最長使用日数の変更」をクリックして変更します。確認メッセージ - 「パスワードの最長使用日数が更新されました。」が表示されます。

バックアップとリストア

TSA 構成のバックアップとリストアを行えます。

重要: 定期的にバックアップを実行することを強くお勧めします。また、スコープ・セットや資格情報を変更した後もバックアップを実行する必要があります。

バックアップ日付

最後にバックアップが実行された日時が表示されます。

構成の要約

このオプションを使用して、保存する前に現在の TSA 構成の要約を表示します。

TSA 構成の要約を表示するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「管理」 > 「バックアップとリストア」をクリックします。「バックアップとリストア」ページが表示されます。
2. 「要約の表示」をクリックすると、現在の TSA 構成の要約が表示されます。表示される情報は、バックアップを実行した場合に TSA が保存する構成を示しています。

注: このオプションはポップアップ・ウィンドウを介して表示されます。ご使用の Web ブラウザーでポップアップ・ウィンドウがブロックされる場合、ブラウザーで TSA からのポップアップを表示することを許可する必要がある場合があります。

「要約」ページの「バックアップ」セクションに、バックアップ状況に関連する情報に加え、次のメッセージが表示されます。

- OK (✓) アイコン。前回バックアップが実施されたのが 60 日以内である場合に表示されます。
- 警告 (⚠) アイコン。バックアップが実施されていない期間が 60 日を超え、90 日は超えていない場合に表示されます。
- エラー (✗) アイコン。バックアップが実施されていない期間が 90 日を超えている場合に表示されます。

バックアップ

TSA 構成のコピーを保存する場合にこのオプションを使用します。

TSA 構成をバックアップするには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「管理」 > 「バックアップとリストア」をクリックします。「バックアップとリストア」ページが表示されます。

Summary

Activity Log

Inventory Summary

Discovery Scopes

Discovery Credentials

Discovery Schedule

Discovery History

Discovery Settings

Transmission Schedule

Administration

Registration

License

Clock

Network

IBM Connectivity

User Accounts

Password

Security

Certificates

Backup and Restore

Update

Logging and Trace

Scheduled Maintenance

Data Snapshot

Shutdown

Tools

Documentation

IBM Support Insights Portal

Backup and Restore

This page allows you to backup and restore the system configuration.

Asterisks (*) indicate mandatory fields that are required to complete this action.

Backup Date

Backup has not been performed.

Configuration Summary

Use this action to view the current configuration summary before backing it up.

[View Summary](#)

Backup

Use this action to download a copy of the current configuration to the system on which this Web interface is running. You must enter a password to protect the configuration file.

Password: *

Specify a password to protect the configuration file.

Confirm Password: *

[Backup](#)

Restore

Use this action to restore a saved configuration from file.

Select configuration file to restore and enter the password used when the backup file was created, then click 'Restore'.

File: * No file selected.

Password: *

Specify the password that was used to protect the configuration file.

[Restore](#)

図 83. バックアップとリストア

2. 構成ファイルを保護するためのパスワードを「バックアップ」ペインに入力します。
3. 「パスワードの確認」フィールドにパスワードを再入力します。パスワードが保存される前に、入力した2つのパスワードが比較されて一致していることが確認されます。
注：パスワードは、リストアの際に必要なになるので、安全に保管しておく必要があります。
4. 「バックアップ」をクリックして、バックアップ構成圧縮ファイルをシステムに保存します。
注：生成されるバックアップ構成ファイルは暗号化され、TSA で開くことができます。
注：管理パスワードを最近変更した場合は、パスワードを変更した後のバックアップを作成しておき、リストアはその最新のバックアップ・ファイルを使用して実施してください。

リストア

以前に保存した構成のコピーをリストアする場合にこのオプションを使用します。

TSA 構成をリストアするには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「管理」 > 「バックアップとリストア」をクリックします。「バックアップとリストア」ページが表示されます。
2. 「ファイルの選択」をクリックし、リストアする構成ファイルを見つけて選択します。
3. 構成ファイルをバックアップするために使用されるパスワードを指定します。

4. 「リストア」をクリックします。

リストア・ジョブが、「要約」ページの「ジョブの要約」ペインに表示されます。リストアが完了すると、システムの再始動を求めるプロンプトが出されます。

注：バックアップからリストアすると、既存の構成が削除されます。スコープ定義および資格情報を含めたすべての構成が、バックアップ・ファイルのものに置き換えられます。

注：バックアップ操作またはリストア操作を行うときは、「要約」ページで Discovery Manager のステータスが OK (✓) の状態になっていることを確認してください。Discovery Manager が実行されていない場合、次のメッセージを受け取ります - 「Discovery Manager が実行されていません。「要約」画面で Discovery Manager のステータスに緑色のチェック・マークのアイコンが表示されていることを確認してから、アクティビティーを再開してください（通常は 10 分以内）。」 10 分経過しても Discovery Manager が実行中にならない場合は、IBM Support にお問い合わせください。

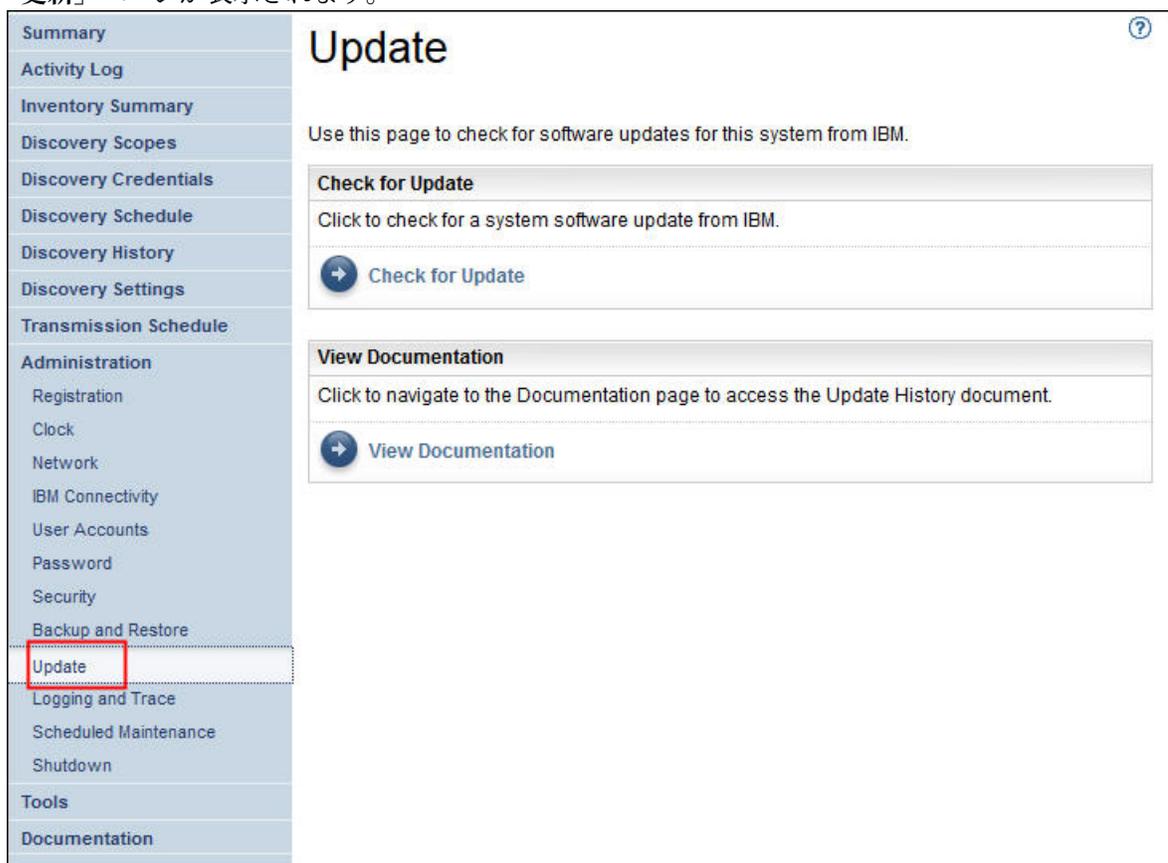
更新

TSA の更新の確認とダウンロードを行えます。

手順

1. ナビゲーション・ペインで、「管理」 > 「更新」をクリックします。

「更新」ページが表示されます。



The screenshot shows the 'Update' page in the Discovery Manager interface. On the left is a navigation sidebar with the following items: Summary, Activity Log, Inventory Summary, Discovery Scopes, Discovery Credentials, Discovery Schedule, Discovery History, Discovery Settings, Transmission Schedule, Administration (Registration, Clock, Network, IBM Connectivity, User Accounts, Password, Security), Backup and Restore, Update (highlighted with a red box), Logging and Trace, Scheduled Maintenance, Shutdown, Tools, and Documentation. The main content area is titled 'Update' and contains the following text and buttons:

- Use this page to check for software updates for this system from IBM.
- Check for Update**
- Click to check for a system software update from IBM.
- [Check for Update](#)
- View Documentation**
- Click to navigate to the Documentation page to access the Update History document.
- [View Documentation](#)

図 84. 更新

2. 「更新の確認」をクリックします。

「使用可能な更新」ページに、使用可能なすべての更新が表示されます。

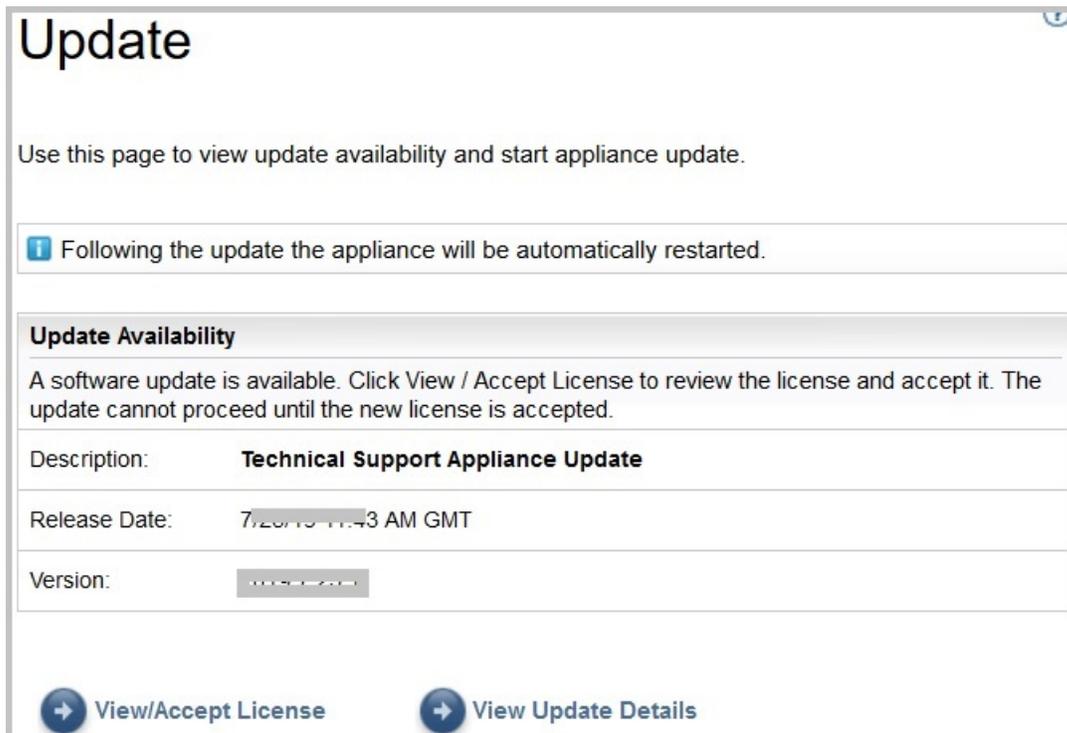


図 85. 使用可能な更新

- 一部の TSA の新規リリースでは、更新に進む前に新しいご使用条件の受諾が必要になります。新規ライセンスがある場合は、「**ライセンスの表示と受諾**」をクリックしてください。「**ご使用条件**」ページが表示されます。
- 「**ご使用条件**」ページ上の「**受諾**」ボタンをクリックすることで、ご使用条件を受諾します。「**今すぐ更新を実行**」ボタンが付いた状態で「**更新**」ページが再表示されます。ご使用条件を受諾する必要がない場合は、「**ライセンスの表示と受諾**」ボタンは表示されません。「**今すぐ更新を実行**」をクリックして続行します。

注：

- ライセンスを受諾すると、「**ライセンスの表示と受諾**」ボタンは表示されなくなります。
- ナビゲーション・ペインで、「**管理**」 > 「**ライセンス**」をクリックして同意済みの最新のご使用条件を表示します。

- 更新をインストールするには、「**今すぐ更新を実行**」をクリックします。

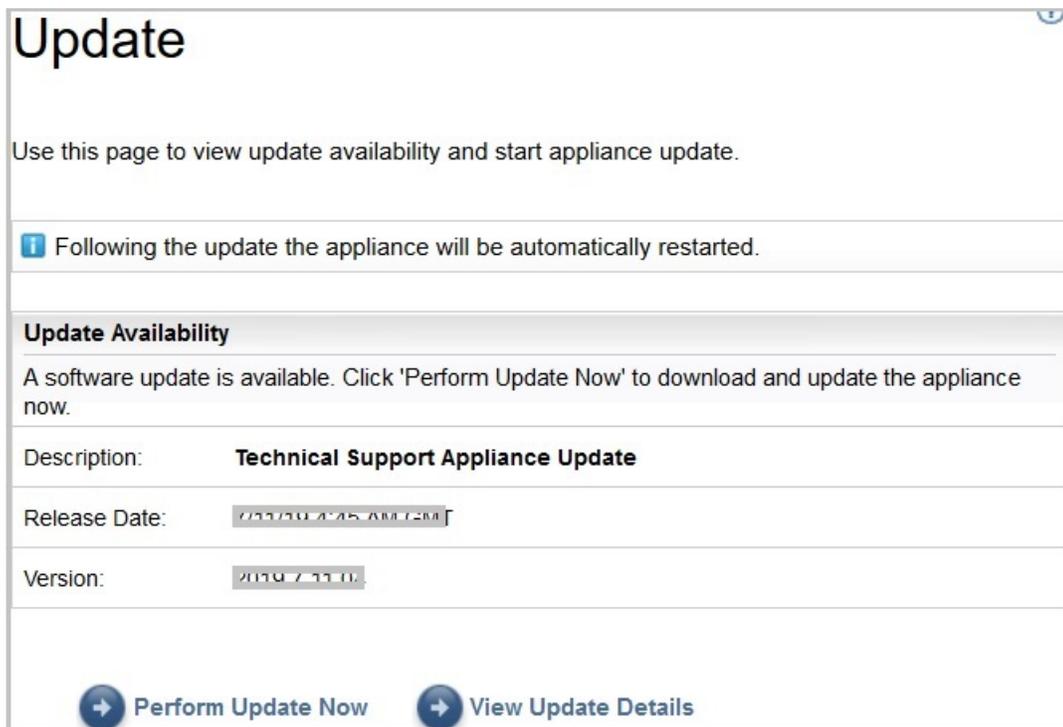


図 86. 今すぐ更新を実行

更新が完了すると、TSA が自動的に再起動します。

- d) 更新のコンテンツについての情報を表示するには、「更新詳細の表示」をクリックします。

定期保守の有効化

TSA を最適なパフォーマンスで実行し続けるために、定期保守機能を有効にすることをお勧めします。

このタスクについて

定期保守ジョブにより、TSA の最適なパフォーマンスが保証されます。この機能は、いつでも有効または無効にすることができます。定期保守を有効にする場合は、保守を自動的に実行する日時を設定できます。定期保守の状況は、「要約」ページの「システム状況」セクションに表示されます。

保守ジョブをスケジュールすると、保守の後でシステムが自動的に再起動します。このシステムの再起動については 1 時間前にユーザーに通知されます。例えば、「定期保守のため、59 分後にシステム再起動ジョブがキューに入れられます。」のような通知を受け取ります。

重要: アプライアンス 保守は、ディスカバリーや送信、またはインベントリー・クリーンアップなどの他のジョブのスケジュールから 30 分以内にはスケジュールしないでください。他の定期ジョブから 30 分以内に保守をスケジュールすると、TSA はそれらのジョブを実行できません。

手順

保守スケジュールを編集するには、以下の手順を実行します。

1. ナビゲーション・ペインで、「定期保守」をクリックします。

「定期保守」ページには、スケジュールされている次の実行とその日時についてのスケジュールが表示されます。「履歴」セクションには、現在実行中の保守ジョブや以前の保守ジョブの状況と詳細が表示されます。

2. 「定期保守」ページで、「スケジュールの編集」をクリックします。

- a) 「スケジュールの有効化」ペインで、定期保守を有効にするか無効にするかを選択します。

- b) 定期保守タスクを有効にすることを選択した場合は、「時刻(時間)」と「時刻(分)」のドロップダウン・リストを選択して、新しい時刻を選択します。
- c) 「日選択モード」を選択します。特定の曜日に保守をスケジュールする場合は「毎週(日曜日 - 土曜日)」オプションを選択します。毎月特定の日に保守をスケジュールする場合は「毎月の日(1-31)」オプションを選択します。
- d) 週または月の別の日または追加の日を選択するには、「曜日」フィールドで該当するチェック・ボックスを選択します。

注: 特定の月の最終日より後の日を選択すると、その特定の月の最終日にジョブがトリガーされません。

3. 「保存」をクリックします。

「定期保守」ページが、新規スケジュールを含んだ状態で再表示されます。

ログとトレース

TSA 診断トレース設定を表示したり変更したりすることができます。また、Discovery Manager トレース・レベルの設定も変更できます。これらの設定を変更するとパフォーマンスに影響を及ぼす可能性があるため、変更は IBM サポートからの指示がある場合にのみ行ってください。

1. ナビゲーション・ペインで、「管理」 > 「ログとトレース」をクリックします。「ログとトレース」ページが表示されます。「TSA トレース・レベル」ペインには、現在のトレース設定(エラー、警告、情報、デバッグ、またはトレース)が表示されます。

The screenshot shows the 'Logging and Trace' configuration page. The left sidebar contains a navigation menu with 'Logging and Trace' highlighted. The main content area has the following structure:

- Summary** (header)
- Activity Log** (header)
- Inventory Summary** (header)
- Discovery Scopes** (header)
- Discovery Credentials** (header)
- Discovery Schedule** (header)
- Discovery History** (header)
- Discovery Settings** (header)
- Transmission Schedule** (header)
- Administration** (header)
 - Registration
 - License
 - Clock
 - Network
 - IBM Connectivity
 - User Accounts
 - Password
 - Security
 - Certificates
 - Backup and Restore
 - Update
 - Logging and Trace** (highlighted)
 - Scheduled Maintenance
 - Data Snapshot
 - Shutdown
- Tools** (header)
- Documentation** (header)
- IBM Support Insights Portal** (header)

The main content area is titled 'Logging and Trace' and includes a help icon. Below the title is a description: 'Use this page to view and modify the TSA diagnostic trace settings and discovery manager trace settings.'

The 'TSA Trace Level' section contains the instruction 'Select the desired trace level.' and five radio buttons: Error, Warning, Information, **Debug** (selected), and Trace.

The 'Discovery Manager Trace Level' section contains the instruction 'Select the desired trace level for discovery manager. Default trace level change apply to discovery related modules only. Improper modification to these properties can seriously impact TSA. Modifications should only be made under the direction of IBM Service.' It includes a checkbox 'Trace level change applies to all modules of discovery manager' (unchecked) and five radio buttons: Fatal, Error, Warning, Information, **Debug** (selected), and Trace.

At the bottom of the page are 'Save' and 'Cancel' buttons.

図 87. ログとトレース

2. 必要な場合は、「TSA トレース・レベル」ペインで、トレース設定の横にあるラジオ・ボタンをクリックしてトレース設定を変更できます。
3. 「保存」をクリックします。

注: デフォルトでは、「TSA トレース・レベル」ペインとその「Discovery Manager トレース・レベル」ペインのトレース・レベルは、「デバッグ」レベルに設定されています。

「Discovery Manager トレース・レベル」の設定を表示したり変更したりするには、次の手順を実行します。

重要: このセクションへの変更は、IBM サービスから指示された場合にのみ行ってください。

1. ナビゲーション・ペインで、「管理」 > 「ログとトレース」をクリックします。「ログとトレース」ページが表示され、現在のトレース設定が示されます。
2. トレース・レベルを Discovery Manager のすべてのモジュールに適用する場合は、「トレース・レベルの変更は Discovery Manager のすべてのモジュールに適用されます」をチェックしてください。
3. 対象のトレース設定の横にあるラジオ・ボタンを選択します。
4. 「保存」をクリックします。

シャットダウン

TSA 操作の一時停止や再開、または TSA のシャットダウンと再始動または電源オフを行うことができます。

シャットダウンには数分かかることがあります。

Summary	Shutdown
Activity Log	
Inventory Summary	
Discovery Scopes	This page provides options for powering off, restarting, suspending or resuming the system.
Discovery Credentials	
Discovery Schedule	Suspend Operations
Discovery History	This action will temporarily stop the system until manually resumed. Scheduled discovery and transmission operations will cease and your infrastructure will not be reported on until the system is restarted or manually invoked. Click "Suspend" if you want to continue and suspend the system.
Discovery Settings	<input type="button" value="Suspend"/>
Transmission Schedule	
Administration	Resume Operations
Registration	This action will resume suspended discovery and transmission operations. Your infrastructure collected data will again be reported on by the system. Click "Resume" if you want to continue and resume the system.
License	<input type="button" value="Resume"/>
Clock	
Network	Shutdown and Restart
IBM Connectivity	This action will shutdown followed by a restart of the system. All existing network connections will be temporarily lost as a result. You will need to open a new browser and re-login to get back in to the user interface. Click "Restart" if you want to continue and restart the system.
User Accounts	<input type="button" value="Restart"/>
Password	
Security	Shutdown and Power Off
Certificates	This action will shutdown and power off the system. All discovery and transmission operations will cease and your infrastructure will not be reported on until the system is restarted. Click "Shutdown" if you want to continue and stop the system.
Backup and Restore	<input type="button" value="Shutdown"/>
Update	
Logging and Trace	
Scheduled Maintenance	
Data Snapshot	
Shutdown	
Tools	
Documentation	
IBM Support Insights Portal	

図 88. シャットダウン

作業の一時停止

このアクションにより、TSA が一時的に停止します。ディスカバリーと送信の作業はすべて停止し、作業が再開されるまで情報は IBM に報告されません。

TSA 操作を一時停止するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「管理」 > 「シャットダウン」をクリックします。「シャットダウン」ページが表示されます。
 2. 「一時停止」をクリックします。
- 注：「要約」ページで TSA の状況を確認できます。TSA が中断状態の場合、「システム状況」ペインに TSA が中断状態であることを示されます。

作業の再開

このアクションにより、一時的に停止していた TSA が再開します。すべてのディスカバリーと送信の作業が再開され、スケジュールどおりに情報が IBM に報告されます。

TSA 操作を再開するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「管理」 > 「シャットダウン」をクリックします。「シャットダウン」ページが表示されます。
2. 「再開」をクリックします。

シャットダウンと再起動

このアクションにより、TSA がシャットダウンされて再起動されます。既存のすべてのネットワーク接続が一時的に切断されます。新規ブラウザを開いて再度ログインする必要があります。

TSA をシャットダウンして再起動するには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「管理」 > 「シャットダウン」をクリックします。「シャットダウン」ページが表示されます。
2. 「再起動」をクリックします。

シャットダウンとパワーオフ

このアクションにより、TSA がシャットダウンおよびパワーオフされます。ディスカバリーと送信の作業はすべて終了し、TSA が再始動されるまでインフラストラクチャーは報告されません。

TSA をシャットダウンしてパワーオフするには、以下の手順に従ってください。

1. ナビゲーション・ペインで、「管理」 > 「シャットダウン」をクリックします。「シャットダウン」ページが表示されます。
2. 「シャットダウン」をクリックします。

注：アプライアンスのシャットダウン後は、VMware ESXi Web インターフェース、または Hyper-V マネージャーを使用して TSA の電源をオンにする必要があります。

ツール

TSA では、TSA 環境のセットアップを支援するツールが提供されます。

ナビゲーション・ペインで「ツール」をクリックすることにより、これらのツールにアクセスできます。

ネットワーク・ツール

「ネットワーク・ツール」ページを使用して、TSA で使用されるネットワーク・プロトコルに関する診断ツールと情報を入力します。

これらの診断ツールにアクセスするには、ナビゲーション・ペインで「ツール」 > 「ネットワーク・ツール」をクリックします。「ネットワーク・ツール」ページが表示されます。

「ネットワーク・ツール」ページがタブごとのページに分割されます。タブをクリックすると、そのタブに対応するページが表示されます。

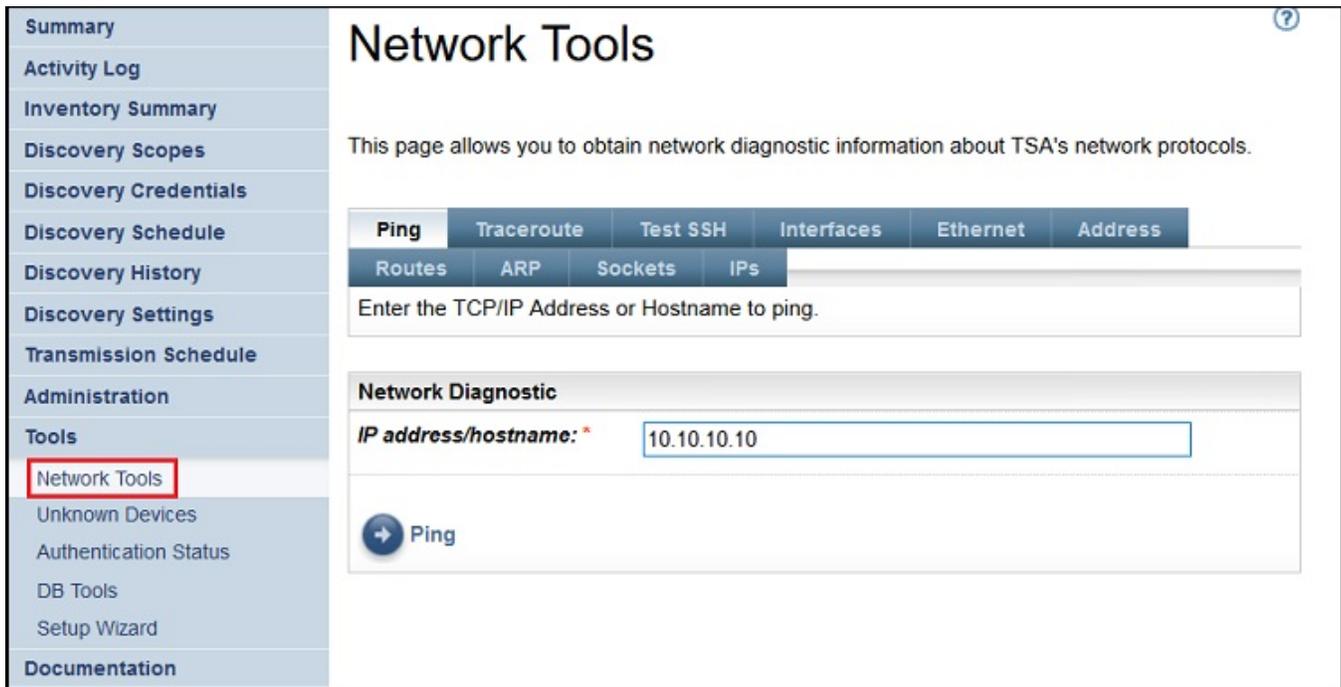


図 89. ネットワーク・ツール

Ping

このページを使用して、リモート・ホストにエコー要求を送信し、ホストがアクセス可能かどうか確認したり、ホスト名または IP アドレスに関する情報を受信したりします。

Traceroute

このページを使用して、パケットが辿るリモート・ホストへのパスを表示します。

SSH のテスト

このページを使用して、ホストに対して定義されているディスカバリー資格情報を使用して SSH でリモート・ホストにアクセスできるかどうかをテストします。

インターフェース

このページを使用して、現在構成されているネットワーク・インターフェースの統計を表示します。

イーサネット

このページを使用して、現在構成されているイーサネット・カードの設定を表示します。

アドレス

このページを使用して、現在構成されているネットワーク・インターフェースの IP アドレスを表示します。

経路

このページを使用して、カーネル IP 経路指定テーブルと、対応するネットワーク・インターフェースを表示します。

ARP

このページを使用して、アドレス解決プロトコル (ARP) 接続の内容を表示します。

ソケット

このページを使用して、TCP/IP ソケットに関する情報を表示します。

IP

このページを使用して、IP パケットのフィルター・ルールに関する情報を表示します。

注: ホスト名を入力する際に下線 ("_") を含めることはできません。

データベース・ツール

「データベース・ツール」ページを使用して、データ保守操作を実行することができます。これらの機能は、IBM サポートからの指示がない限り使用しないことをお勧めします。

データベース上で以下の操作を実行できます。

インベントリー・データベースの再作成

インベントリー・データベースを再作成すると、すべてのインベントリー・データが失われます。さらに、「資格情報の保持」チェック・ボックスがクリアされている場合や、Discovery Manager が使用不可になっている場合、資格情報も失われます。

データベースを再作成するには、以下の手順を実行します。

1. ナビゲーション・ペインで、「ツール」 > 「DB ツール」をクリックします。
2. 「インベントリー・データベースの再作成」セクションの「資格情報とスコープの保存」チェック・ボックスを選択して、すべてのディスカバリー資格情報が保持されるようにします。「資格情報とスコープの保存」オプションを選択しないと、資格情報とスコープは失われるので、すべての資格情報とスコープすべてをもう一度セットアップしなければなりません。ディスカバリー資格情報については詳しくは、75 ページの『[ディスカバリー資格情報](#)』を参照してください。

注：資格情報とスコープを保持できるのは、Discovery Manager が実行中 (緑色のステータス) の場合に限りです。

3. 「インベントリー・データベースの再作成」をクリックします。次の警告メッセージが表示されます - このアクションを実行すると Discovery Manager が一時的に終了します。インベントリー・データベースを再作成してもよろしいですか？
4. 「OK」をクリックしてインベントリー・データベースを再作成します。「データベースの再作成が開始されました」というメッセージが表示されます。データベースの再作成には約 6 時間かかる可能性があります。再作成中は「要約」ページに「dbinit 開始中」というメッセージが表示されます。6 時間後に「アクティビティー・ログ」でステータスが「インベントリー・データベースの再作成は正常に終了しました」になっていることを確認できます。

注：インベントリー・データベースを再作成するときは、Discovery Manager が一時的に終了し、インベントリー・クリーンアップ・アーカイブがクリアされます。

RUNSTATS の実行

RUNSTATS コマンドするには、以下の手順を実行します。

1. ナビゲーション・ペインで、「ツール」 > 「DB ツール」をクリックします。
2. 「RUNSTATS の実行」をクリックします。次の警告メッセージが表示されます - インベントリー・データベース・テーブルに対して RUNSTATS を実行しますか？
3. 「OK」をクリックします。「RUNSTATS が開始されました」というメッセージが表示されます。約 30 分後に、アクティビティー・ログを確認できるようになります。ジョブが完了すると、「インベントリー・データベースに対する RUNSTATS が正常に完了しました」というメッセージが表示されます。

REORG の実行

REORG コマンドするには、以下の手順を実行します。

1. ナビゲーション・ペインで、「ツール」 > 「DB ツール」をクリックします。
2. 「REORG の実行」をクリックします。次の確認メッセージが表示されます - インベントリー・データベース・テーブルに対して REORG を実行しますか？
3. 「OK」をクリックします。「REORG が開始されました」というメッセージがアクティビティー・ログに追加されます。約 30 分後に、アクティビティー・ログを確認できるようになります。ジョブが完了すると、「インベントリー・データベースに対する REORG が正常に完了しました」というメッセージがアクティビティー・ログに追加されます。

資料

IBM Technical Support Appliance の利用を開始する際には、「資料」ページを参照してください。TSA の Web サイト (<https://ibm.biz/TSAdemo>) で、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・レポートを参照したり、TSA のインストール・コードをダウンロードしたりできます。

手順

資料を参照して Technical Support Appliance の詳細を知るには、以下の手順に従ってください。

1. 左ナビゲーション・メニューで「資料」をクリックします。

Summary	<h2>IBM Technical Support Appliance (TSA)</h2> <p>The IBM Technical Support Appliance (TSA) is an easy-to-use tool that enables you to get more value from your IBM Support contracts.</p> <p>The link below will open a new web browser tab directly to the Technical Support Appliance information website on ibm.com. Here you will find everything you need to get started with the IBM Technical Support Appliance. You can access setup guides and security documentation, view sample reports, and download the virtual appliance installation code from IBM Fix Central.</p> <p>Of special note, the Configuration Guide is a helpful index of best practices, tips, and shortcuts to configure TSA to efficiently retrieve IT device information from various hardware manufacturers.</p> <p>Learn more about the Technical Support Appliance: https://ibm.biz/TSAdemo</p> <p> Technical Support Appliance Documentation</p>
Activity Log	
Inventory Summary	
Discovery Scopes	
Discovery Credentials	
Discovery Schedule	
Discovery History	
Discovery Settings	
Transmission Schedule	
Administration	
Tools	
Documentation	
IBM Support Insights Portal	

図 90. 資料

2. Technical Support Appliance の詳細を知るには、<https://ibm.biz/TSAdemo> リンクをクリックします。
3. 「TSA のインストール」ページに、TSA のイメージ、セットアップ・ガイド、構成ガイド、関連するチュートリアルへのリンクがあります。

第 7 章 Technical Support Appliance (TSA) について IBM サポートに問い合わせる

IBM サポートは、お使いのタイム・ゾーンの月曜日から金曜日の営業時間にご利用可能です。

このタスクについて

IBM サポートに問い合わせるには、次の 2 つの方法があります。

1. [IBM サポート・ポータルで Case をオープンする](#)
2. [IBM コール・センターでサービス・リクエストを生成する](#)

IBM サポート・ポータルで Case をオープンする

手順

1. <https://www.ibm.com/mysupport/s/> にログオンします。

注: IBM サポート・ポータルにアクセスするには、まずアカウントを作成する必要があります。

2. ポータル右上の「**Case をオープン**」をクリックします。「**Case をオープン**」ページが表示されます。
3. 「**サポートのタイプ (Type of support)**」を選択します。
4. 「**タイトル (Title)**」、「**製品の製造メーカー (Product manufacturer)**」、「**製品 (Product)**」に入力します。

注: Technical Support Appliance チームにリクエストを直接送信するには、「**製品 (Product)**」フィールドに「Technical Support Appliance」と入力してください。

5. 「**重大度 (Severity)**」を選択します。
6. 「**説明 (Description)**」に入力し、優先言語を選択します。
7. その言語を話せる担当員がいなければ英語でコミュニケーションしてもよいという場合は、「**はい (Yes)**」を選択します。
8. 「**Case の送信 (Submit case)**」をクリックします。

IBM コール・センターでのサービス・リクエストの生成

手順

1. <https://www.ibm.com/planetwide> の発信する国に該当する電話番号にダイヤルします。
2. 言語を選択します。
3. 1 (IBM 製品) を選択します。
4. 2 (ソフトウェア・サポート) を選択します。
5. 製品 ID 5621IZX01 または製品名 *Technical Support Appliance* を使用します。
6. 以下を入力するように求められます。

- 会社の番号/地域
- お客様名/会社名
- 住所/都道府県/市区町村/郵便番号
- 建物/フロア
- TSA が設置されている場所の電話番号
- 連絡先の名前/E メール/電話番号
- 問題記述

- 重大度レベル

付録 A Technical Support Appliance の設定

セットアップ・ウィザードで終了したりスキップした設定は、TSA の左側ナビゲーション・メニューで手動で設定することができます。

Technical Support Appliance の登録

TSA の登録では、分析のために情報を IBM に報告したときに TSA の識別に必要な情報が収集されます。

このタスクについて

登録するには、以下の手順に従います。

手順

1. ナビゲーション・ペインで、「管理」 > 「登録」をクリックします。
「登録」ページが表示されます。

Summary	<h2 style="margin: 0;">Registration</h2> <p>This page allows you to view and change the system service contact and physical location information.</p> <p>Asterisks (*) indicate mandatory fields that are required to complete this action.</p> <div style="border: 1px solid #ccc; padding: 5px;"> <h3 style="margin: 0;">Service Contact</h3> <p>Identifies the person who IBM Support should contact if there is a problem with this system. Contact information (Contact name, Telephone number, Email address, and IBMid) is optional. It will be used to assist IBM in providing your company with the results of the Technical Support Appliance analysis.</p> <p>Company name: * <input type="text" value="IBM_TEST_OK_TO_CLOSE"/> Name of the organization that owns or is responsible for this system.</p> <p>Contact name: <input type="text" value="James"/> Name of the person in your organization who is responsible for repairs and maintenance of the system.</p> <p>Telephone number: <input type="text" value="9345632418"/> Telephone number where the contact person can be reached. The telephone number should include the area code, exchange numbers, and extension.</p> <p>Email: <input type="text" value="james@in.ibm.com"/> Email address of the contact person.</p> <p>IBMid: <input type="text"/></p> <p>You can log on to the IBM Client Insights Portal with your associated IBMid to download your TSA Reports in 1-2 days after each data transmission. Need an IBMid? Go to https://www.ibm.com/account to sign up.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <h3 style="margin: 0;">System Location</h3> <p>Identifies where this system has been installed. The information should allow someone to quickly find the system when necessary for maintenance or other purposes.</p> <p>Country or region: * <input type="text" value="INDIA"/> The country or region where the system is located. If your country or region is not listed, select a neighboring country or region.</p> <p>State or province: * <input type="text" value="TS"/> The state or province where the system is located.</p> <p>Postal code: * <input type="text" value="502032"/> The postal code where the system is located.</p> <p>City: * <input type="text" value="Hyderabad"/> The city or locality where the system is located.</p> <p>Street address: * <input type="text" value="BHEL"/> The first line of the system location address.</p> <p>Telephone number: <input type="text" value="9989122783"/> The telephone number of the room where the system is located. The telephone number should include the area code, exchange numbers, and extension.</p> <p>Building, floor, office: <input type="text" value="3546"/> The building, floor, and office where the system is located.</p> </div> <p style="text-align: center;"> <input type="button" value="Save"/> <input type="button" value="Cancel"/> </p>
Activity Log	
Inventory Summary	
Discovery Scopes	
Discovery Credentials	
Discovery Schedule	
Discovery History	
Discovery Settings	
Transmission Schedule	
Administration	
Registration	
License	
Clock	
Network	
IBM Connectivity	
User Accounts	
Password	
Security	
Certificates	
Backup and Restore	
Update	
Logging and Trace	
Scheduled Maintenance	
Data Snapshot	
Shutdown	
Tools	
Documentation	
IBM Support Insights Portal	

図 91. 登録

- サービスの連絡先情報を次のフィールドに指定します。

会社名

TSA を使用する組織の名前。

連絡先名

(オプション) 組織内の TSA 担当者の名前。

電話番号

(オプション) 担当者と連絡が取れる電話番号。電話番号には、市外局番、局番、内線番号を含める必要があります。電話番号に括弧は使用しないでください。

Eメール

(オプション) 担当者の Eメール・アドレス。

IBMid

(オプション) IBM Client Insights Portal でレポートを表示することを許可する対象者の IBMid。

注: TSA レポートは、それぞれのデータ転送の 1 日か 2 日後に、関連付けられている IBMid で <https://clientinsightsportal.ibm.com/> にログインしてダウンロードできます。IBMid を登録するには <https://www.ibm.com/account> に移動してください。

注: サービス連絡先は、システムに問題がある場合に IBM サポートが連絡を取る必要がある相手を識別します。連絡先情報は、IBM が貴社に Technical Support Appliance の分析の結果を提供するために使用します。

3. TSA のロケーション情報を次のフィールドに指定します。

国または地域

TSA がある国または地域。

都道府県/州

TSA がある都道府県。都道府県が不明な場合は、*Unknown* と入力します。

郵便番号

TSA がある場所の郵便番号。

市区町村

TSA がある市区町村。

番地

TSA がある場所の住所。

電話番号

(オプション) TSA がある部屋の電話番号。電話番号には、市外局番、局番、内線番号を含める必要があります。電話番号に括弧は使用しないでください。

建物、階、オフィス

(オプション) TSA がある建物、階、オフィス。

4. 「保存」をクリックして、登録情報を保存します。

IBM 接続の設定

IBM に接続するときに使用するインターネットの接続情報を指定します。

始める前に

6 ページの表 1 の説明にあるとおり、ご使用のファイアウォールで、IBM サーバーのホスト名と IP アドレスへの接続を許可しておく必要があります。お客様のネットワークが IBM サーバーへのアクセスを許可しない場合、IBM サポートへの TSA トランザクションが失敗します。

手順

1. ナビゲーション・ペインで、「管理」 > 「IBM 接続」をクリックします。

図 92. IBM 接続

2. 「アクセス」 ペインで、以下のインターネット・アクセス・タイプのいずれかを選択します。

直接 SSL 接続を許可

TSA は、直接接続を使用して IBM に接続します。

SSL プロキシ接続を使用

TSA は、SSL プロキシ接続を使用して IBM に接続します。

認証を行う SSL プロキシ接続を使用

TSA は、認証ありの SSL プロキシ接続を使用して IBM に接続します。

3. 「SSL プロキシ接続を使用」または「認証を行う SSL プロキシ接続を使用」を選択した場合は、プロキシ・サーバーに関する次の情報を指定します。

IP アドレスまたはホスト名

プロキシ・サーバーの IP アドレスまたはホスト名。

注：ホスト名を入力する際に下線 ("_") を含めることはできません。

ポート

プロキシ・サーバーのポート番号。

4. 「認証を行う SSL プロキシ接続を使用」を選択した場合は、プロキシ・サーバーに関する次の情報を指定します。

ユーザー名

プロキシ・サーバーが認証のために使用するユーザー名。

パスワード

プロキシ・サーバーが認証のために使用するユーザー名に関連付けられたパスワード。

パスワードの確認

パスワードを再度入力します。パスワードが保存される前に、入力した 2 つのパスワードが比較されて一致していることが確認されます。

5. 「保存」をクリックして IBM 接続情報を保存します。
6. 「接続のテスト」をクリックして、指定した接続をテストします。

重要:

- 接続をテストする前に、接続設定を保存します。
- IBM への有効な接続が必要です。接続がないと、TSA 機能は作動しません。

関連概念

IBM サポートに接続するための構成要件

TSA は、直接接続で、またはユーザーが用意したプロキシ (IBM との通信を許可するように構成されている必要があります) を介して IBM サポートに接続できます。プロキシを使用している場合は、TLS/SSL インспекションはサポートされません。プロキシを介したすべての要求は、TLS/SSL によって停止されることなく IBM に直接フローを許可される必要があります。

クロックの設定

セットアップ時には、TSA のシステム時刻、日付、およびローカル・タイム・ゾーンを設定する必要があります。

手順

1. ナビゲーション・ペインで、「管理」 > 「クロック」をクリックします。
「クロック」ページが表示されます。

図 93. クロック

2. 「GMT オフセット」ドロップダウン・リストから、ローカル・タイム・ゾーンを選択します。
3. 「DST 調整」ドロップダウン・リストから夏時間 (DST) 調整を選択します。

注: すべてのタイム・ゾーンで DST が使用できるわけではありません。DST を許容していないタイム・ゾーンでこのオプションを選択すると、エラー・メッセージが表示されます。

4. 「時間オプションの選択」ドロップダウン・リストから、システム・クロックを更新する方法を選択します。

オプションとして、システム・クロックを Network Time Protocol (NTP) サーバーと同期して自動的に更新する方法と、システム・クロックを手動で構成する方法があります。

- a) システム・クロックを手動で構成することを選択した場合は、システムの日付と時刻を設定する必要があります。日付と時刻の情報を「日付」フィールドと「時刻」フィールドに入力します。
- b) システム・クロックを Network Time Protocol (NTP) サーバーと同期して自動的にシステム・クロックを更新することにした場合は、NTP サーバーの IP アドレスとホスト名を指定する必要があります。「NTP サーバー」フィールドに、サーバー (2 つまで) の IP アドレスまたはホスト名の情報を入力します。

注: TSA からネットワーク経由で NTP サーバーにアクセスできることを確認してください。

5. 「保存」をクリックしてクロック情報を保存します。

タスクの結果

注: 変更内容によっては、変更内容を有効にするために再始動が必要になることがあります。例えば、日付や時刻を設定した場合や、手動構成から NTP サーバー構成に変更した場合には、システムの再始動を求めるプロンプトが出されます。

送信スケジュールのセットアップ

TSA には、指定された時刻に送信プロセスを実行するための、デフォルトのスケジュールが設定されています。このスケジュールはニーズに合わせて変更できます。

手順

1. ナビゲーション・ペインで、「送信スケジュール」をクリックします。

「送信スケジュール」ページが表示されます。

「スケジュール」ペインには、スケジュールされている次の実行とその日時が表示されます。「履歴」ペインには、現在実行されている送信ジョブと、過去の送信ジョブの状況と追加の詳細情報が表示されます。

2. 「スケジュールの編集」をクリックします。

「送信スケジュール」ページが表示されます。

Summary
Activity Log
Inventory Summary
Discovery Scopes
Discovery Credentials
Discovery Schedule
Discovery History
Discovery Settings
Transmission Schedule
Administration
Tools
Documentation
IBM Support Insights Portal

Transmission Schedule

Asterisks (*) indicate mandatory fields that are required to complete this action.

Enable Schedule
Select whether periodic transmission should be performed.

Select: * Enable scheduled transmission ▼

Schedule
Select when you want the transmission performed.

At hour: * 00 ▼

At minute: * 00 ▼

Day selection mode: *
 Weekly by day(s) (Sun-Sat)
 Monthly by date(s) (1-31)

On days: *
 01 02 03 04 05 06 07
 08 09 10 11 12 13 14
 15 16 17 18 19 20 21
 22 23 24 25 26 27 28
 29 30 31

If days are picked beyond the last day of any given month, the job will be triggered the last day of such month instead.

Save Cancel

図 94. 送信スケジュールの編集

- a) 「時刻(時間)」リストおよび「時刻(分)」ドロップダウン・リストを使用して新しい時刻を選択します。
- b) 「日選択モード」を選択します。

毎週(日曜日 - 土曜日)

特定の曜日(複数可)に送信をスケジュールする場合は「毎週(日曜日 - 土曜日)」オプションを選択します。

Schedule	
Select when you want the transmission performed.	
At hour: *	00 ▼
At minute: *	00 ▼
Day selection mode: *	<input checked="" type="radio"/> Weekly by day(s) (Sun-Sat) <input type="radio"/> Monthly by date(s) (1-31)
On days: *	<input checked="" type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday

図 95. 毎週 (日曜日 - 土曜日)

「曜日」フィールドで該当するチェック・ボックスをチェックすることで、週の1つ以上の曜日を選択します。

毎月の日 (1-31)

毎月特定の日 (複数可) に送信をスケジュールする場合は、「毎月の日 (1-31)」オプションを選択します。

「曜日」フィールドで該当するチェック・ボックスをチェックすることで、月の1つ以上の日を選択します。

注: 特定の月の最終日より後の日を選択すると、その特定の月の最終日にジョブがトリガーされます。

3. 「保存」をクリックします。

「送信スケジュール」ページが、新規スケジュールを含んだ状態で再表示されます。

更新

TSA の更新の確認とダウンロードを行えます。

手順

1. ナビゲーション・ペインで、「管理」 > 「更新」をクリックします。
「更新」ページが表示されます。

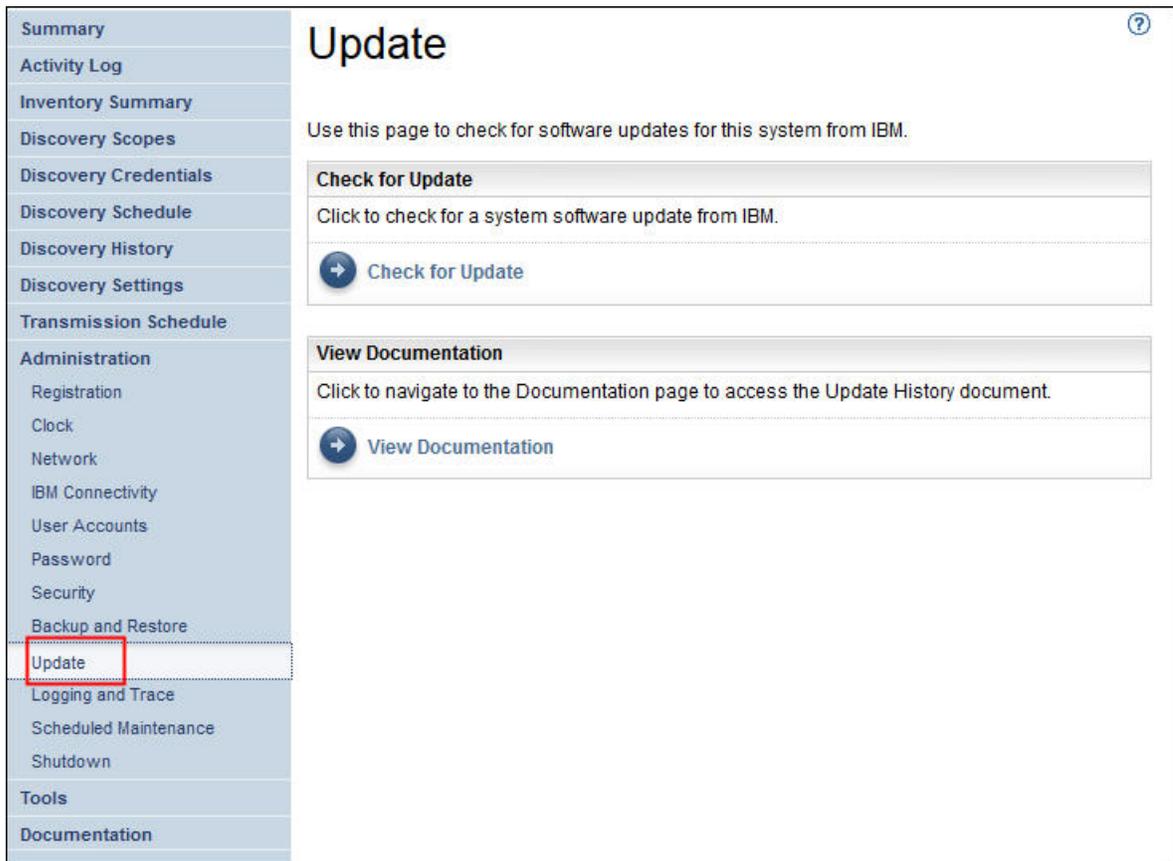


図 96. 更新

2. 「更新の確認」をクリックします。

「使用可能な更新」ページに、使用可能なすべての更新が表示されます。

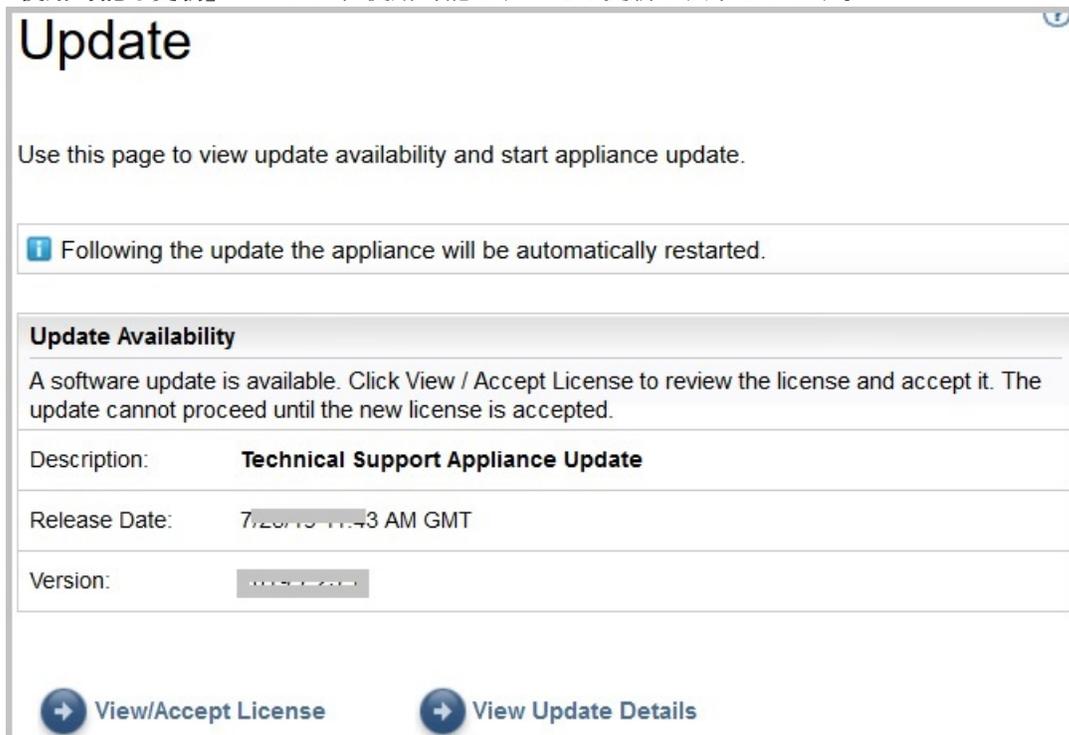


図 97. 使用可能な更新

- a) 一部の TSA の新規リリースでは、更新に進む前に新しいご使用条件の受諾が必要になります。新規ライセンスがある場合は、「**ライセンスの表示と受諾**」をクリックしてください。「**ご使用条件**」ページが表示されます。
- b) 「**ご使用条件**」 ページ上の「**受諾**」ボタンをクリックすることで、ご使用条件を受諾します。「**今すぐ更新を実行**」ボタンが付いた状態で「**更新**」ページが再表示されます。ご使用条件を受諾する必要がない場合は、「**ライセンスの表示と受諾**」ボタンは表示されません。「**今すぐ更新を実行**」をクリックして続行します。

注：

- ライセンスを受諾すると、「**ライセンスの表示と受諾**」ボタンは表示されなくなります。
 - ナビゲーション・ペインで、「**管理**」 > 「**ライセンス**」をクリックして同意済みの最新のご使用条件を表示します。
- c) 更新をインストールするには、「**今すぐ更新を実行**」をクリックします。

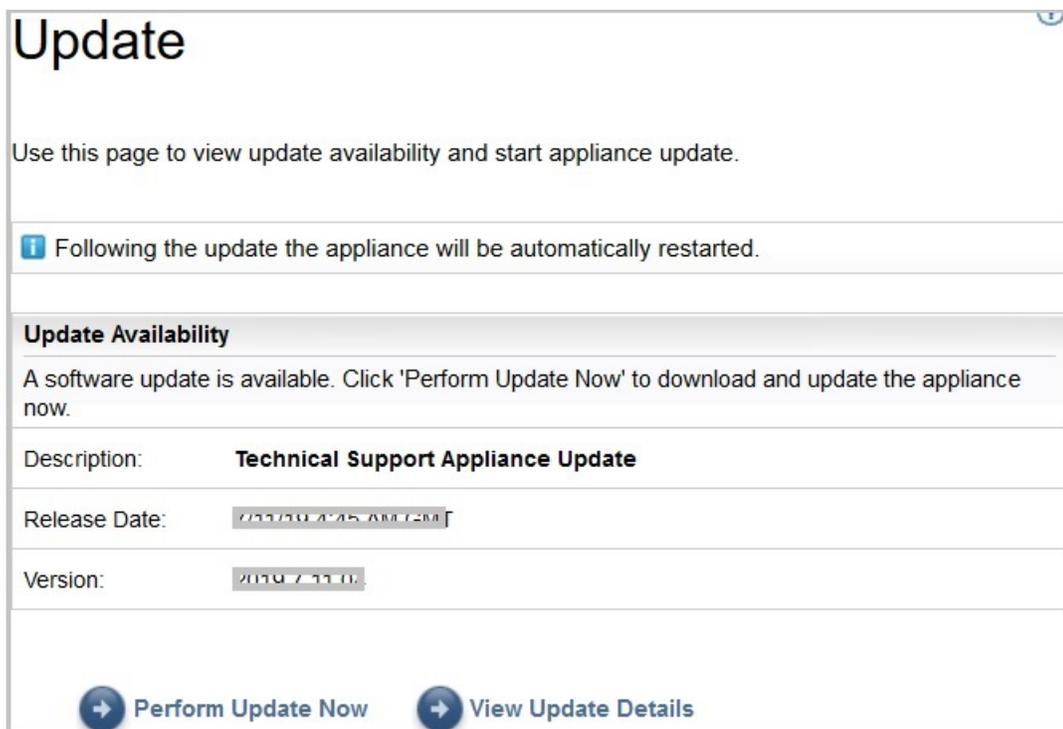


図 98. 今すぐ更新を実行

更新が完了すると、TSA が自動的に再起動します。

- d) 更新のコンテンツについての情報を表示するには、「**更新詳細の表示**」をクリックします。

付録 B DHCP ネットワーク詳細の構成

DHCP ネットワークの詳細を構成するには、以下の手順に従ってください。

手順

1. 「TSA 構成メニュー」からオプション「1) ネットワーク構成のセットアップ」を選択します。

```
----- TSA Config Menu -----
1) Setup network configuration
2) Change tsaur password
3) Set Appliance certificate to default
4) Exit

Choose an option:
```

図 99. ネットワーク構成のセットアップ

2. 以下のネットワーク構成の詳細を入力します。

```
Enter IPTYPE={static|dhcp}:dhcp
Enter Hostname(default=ibmtsa):ibmappliance
Enter network domain of system for DNS usage(optional):example.com
Enter DNS 1(optional):10.20.20.20
Enter DNS 2(optional):10.30.30.30
Enter DNS 3(optional):10.40.40.40

Confirm network configuration
IPTYPE:dhcp
HOSTNAME:ibmappliance
DOMAIN:example.com
DNS1:10.20.20.20
DNS2:10.30.30.30
DNS3:10.40.40.40
[y|n]:
```

図 100. ネットワーク構成

- a) 「**IPTYPE = {static|dhcp}**」を入力します。「dhcp」を入力します。

IPTYPE: dhcp

「**ホスト名を入力 (デフォルト =ibmtsa)**」。デフォルト・ホスト名を変更できます。使用するホスト名が固有であることを確認してください。

「**DNS 使用のためのシステムのネットワーク・ドメインを入力 (オプション)**」。

「**DNS 1 を入力 (オプション)**」、「**DNS 2 を入力 (オプション)**」、および「**DNS 3 を入力 (オプション)**」。

指定したネットワーク構成の詳細が、確認のために表示されます。

- b) **[y|n]**を入力して、ネットワーク構成を確認または破棄します。「y」を入力すると、ネットワーク構成が保存されてシステムが自動的に再起動します。

注：構成が正しくない場合は、詳細を変更できます。「n」を入力して現在の設定を無視し、ステップ 127 ページの『2.a』から構成をやり直します。

- c) 新しいネットワーク構成を有効にするために、システムは 15 秒後にリブートします。

- d) システムがリブートしたら、仮想化マネージャーにログインし、「全般情報」タブにある「IP アドレス」をメモします。

The screenshot shows the VMware vSphere interface for a virtual machine named 'ibmtsa_2.7.0.0'. The 'Networking' section is expanded, and the 'IP addresses' field is highlighted with a red box, showing the IP address '10.10.10.10'. Other sections like 'General Information', 'Hardware Configuration', and 'Resource Consumption' are also visible.

Section	Item	Value
Networking	Host name	sshhost1@ptsia
	IP addresses	10.10.10.10
	VMware Tools	Installed: Yes, Version: 10240, Running: Yes
	Storage	1 disk
Hardware Configuration	CPU	4 vCPUs
	Memory	16 GB
	Hard disk 1	150 GB
	Network adapter 1	VM Network (Connected)
Resource Consumption	Consumed host CPU	42 MHz
	Consumed host memory	3.69 GB
	Active guest memory	6.24 GB
	Storage	Provisioned: 150 GB, Uncommitted: 147.39 GB, Not-shared: 169.99 GB, Used: 169.99 GB

図 101. DHCP IP アドレス

- e) 前の手順で入手した URL をブラウザに指定して TSA にアクセスします。
例: <https://newhost1.new.abclabs.example.com>

注: 初回接続時には、ブラウザでセキュリティー例外が表示されます。TSA にログオンするには、セキュリティー証明書を受け入れて続行する必要があります。

付録 C ユーザー・アカウントとユーザー・グループ

ユーザー・アカウントとユーザー・グループを使用して、TSA 機能に対するアクセス権限を付与できます。

始める前に

TSA は **admin** というユーザー・アカウント名でインストールされています。このアカウントには、すべての TSA 機能を実行する権限があります。次の理由でユーザー・アカウントを追加したい場合があります。

- 別のユーザーが **admin** ユーザーの予備ユーザーとして作業できるようにする。
- 一部のユーザーに TSA の一部の機能を使用させる。

このタスクについて

なんらかの TSA 機能を実行するには、一定の権限レベルが必要となります。認証済みユーザーが適切な権限レベルがない状態で機能を実行しようとする、エラーが表示されて機能は実行されません。

TSA では、権限レベルはユーザー・グループに関連付けられています。ユーザーには、1 つ以上のユーザー・グループのメンバーシップが割り当てられます。これらのグループ・メンバーシップを通して、ユーザーは特定の機能を実行するための権限レベルを取得します。

TSA には、**Administrator** ユーザー・グループと **admin** ユーザー・アカウントが用意されています。**Administrator** ユーザー・グループには、すべてのシステム 機能に対する無制限のアクセス権限があります。**admin** ユーザー・アカウントは、**Administrator** ユーザー・グループに割り当てられます。

ユーザー・アカウントとユーザー・グループの表示

既存のユーザー・アカウントとユーザー・グループを表示できます。

手順

1. ナビゲーション・ペインで、「管理」 > 「ユーザー・アカウント」をクリックします。
「ユーザー・アカウントとグループ」ページが表示されます。
2. 既存のユーザー・アカウントを表示するには、「アカウント」タブをクリックします。
「ユーザー・アカウント」テーブルにユーザー・アカウントが表示されます。

ヒント: 特定のユーザー・アカウントの詳細を表示するには、ユーザー・アカウントの名前をクリックします。右側の「一般」ペインに、選択したユーザー・アカウントに関連付けられているユーザー名、フルネーム、および説明が表示されます。右側の「グループ」ペインをクリックすると、このユーザー・アカウントが属するユーザー・グループが表示されます。

3. 既存のユーザー・グループを表示するには、「グループ」タブをクリックします。
「ユーザー・グループ」テーブルにユーザー・グループが表示されます。

ヒント: 特定のユーザー・グループの詳細を表示するには、ユーザー・グループの名前をクリックします。右側の「一般」ペインに、そのユーザー・グループに関連付けられている名前と権限レベルが表示されます。右側の「スコープ制限」ペインをクリックすると、選択されたユーザー・グループがディスカバーできるスコープ・セットが表示されます。「メンバー」ペインをクリックすると、このユーザー・グループに関連付けられたユーザー・アカウントが表示されます。

ユーザー・アカウントとユーザー・グループの追加

ユーザー・アカウントとユーザー・グループを追加して、TSA 機能へのアクセスを制御できます。

関連概念

[ディスカバリー・スコープとスコープ・セット](#)

ディスカバリー・スコープは、TSA のディスカバー対象とするリソースを識別します。ディスカバリー・スコープはディスカバリー・スコープ・セットにグループ化されます。

ユーザー・グループの追加

ユーザー・グループを追加して、TSA 機能へのアクセスを制御できます。

このタスクについて

ユーザー・グループを追加するには、以下の手順に従ってください。

手順

1. ナビゲーション・ペインで、「管理」 > 「ユーザー・アカウント」をクリックします。
「ユーザー・アカウントとグループ」ページが表示されます。
2. 「グループ」タブをクリックします。

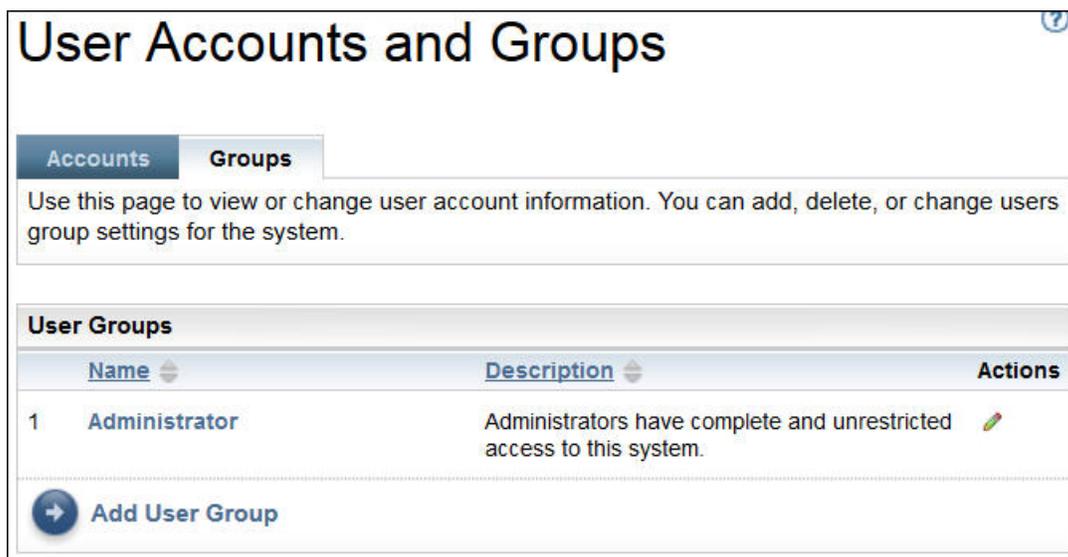


図 102. グループ

3. 「ユーザー・グループの追加」をクリックします。
「ユーザー・グループ」ページが表示されます。

User Group

Use this page to view, add or change user group information.

Asterisks (*) indicate mandatory fields that are required to complete this action.

General

The following describes user group basic information.

Group name: *
Uniquely identifies the group.

Description:
Describes the group.

Member Authority Level

All members of this group will have the following authority level.

Select: *

Restrict To Selected Scope Sets

Identifies the scope sets this group is restricted to.

Scope set name:

- AIX_Scope
- AIX_Scope_TADDM
- AMM_Scope
- Test
- Test_IPRange_ScopeSet
- Tester1
- WindowsScopeSet
- XIV_Scope

図 103. ユーザー・グループの追加

4. 「グループ名」フィールドに、このユーザー・グループに固有の名前を入力します。
5. オプション: 「説明」フィールドに、このユーザー・グループの説明を入力します。
6. このユーザー・グループのメンバーに付与する権限レベルを選択します。

TSA は、次のグループ権限レベルを定義します。

- 管理者 – 制限なし
- ディスカバリー – ディスカバリー機能のみ
- 訪問者 – 読み取り権限のみ

7. このユーザー・グループに「ディスカバリー」権限レベルを指定した場合は、このユーザー・グループに制限されるスコープ・セットを少なくとも 1 つ選択する必要があります。

スコープ・セットの詳細については、[1 ページの『ディスカバリー・スコープとスコープ・セット』](#)を参照してください。

8. 「保存」をクリックしてユーザー・グループを保存します。

新規ユーザー・グループがリストに入った「ユーザー・アカウントとグループ」ページが表示されます。

ユーザー・アカウントの追加

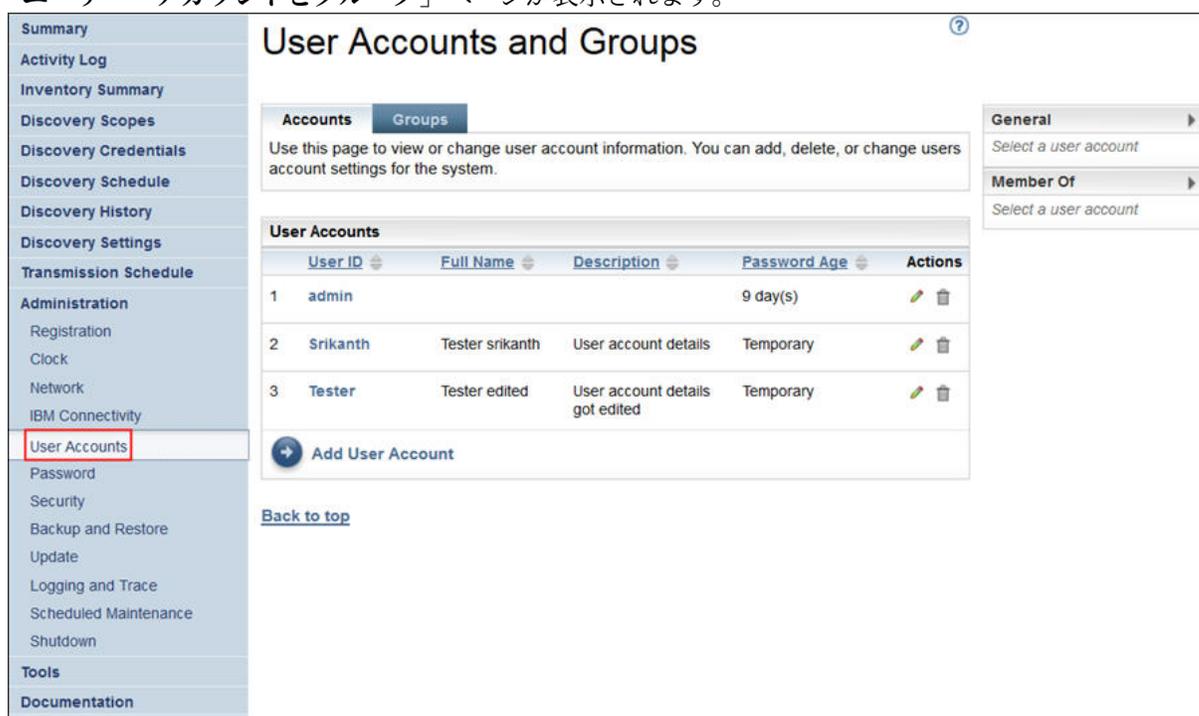
ユーザー・アカウントを追加して、TSA 機能へのアクセスを制御できます。

このタスクについて

ユーザー・アカウントを追加するには、以下の手順に従ってください。

手順

1. ナビゲーション・ペインで、「管理」 > 「ユーザー・アカウント」をクリックします。
「ユーザー・アカウントとグループ」ページが表示されます。



The screenshot shows the 'User Accounts and Groups' page. On the left is a navigation sidebar with 'User Accounts' selected. The main area has tabs for 'Accounts' and 'Groups'. Below the tabs is a table of user accounts:

User ID	Full Name	Description	Password Age	Actions
1	admin		9 day(s)	[Edit] [Delete]
2	Srikanth	Tester srikanth	Temporary	[Edit] [Delete]
3	Tester	Tester edited	Temporary	[Edit] [Delete]

Below the table is an 'Add User Account' button and a 'Back to top' link. On the right, there are dropdown menus for 'General' and 'Member Of', both currently showing 'Select a user account'.

図 104. ユーザー・アカウントとグループ

2. 新規ユーザー・アカウントを定義するには、「ユーザー・アカウントの追加」をクリックします。
「ユーザー・アカウント」ページが表示されます。

User Account ?

Use this page to view, add or change user account information.

Asterisks (*) indicate mandatory fields that are required to complete this action.

General

The following describes user account basic information.

User name: *
Uniquely identifies the user.

Full name:
Identifies the users full name.

Description:
Describes the user.

Enter Password

Enter a new password and then type it again in the confirm field to confirm.

New password: *

Confirm new password: *

Disable Account: Account is disabled

Member Of

The groups this user is a member of.

Select user groups: * VisitorGroup-ForTest
 Administrator

図 105. ユーザー・アカウントの追加

3. 「**ユーザー名**」フィールドに、このユーザー・アカウントの名前を入力します。
4. オプション: 「**氏名**」フィールドに、このアカウントのユーザーの氏名を入力します。
5. オプション: 「**説明**」フィールドに、このユーザー・アカウントの説明を入力します。
6. 「**新規パスワード**」フィールドに、このユーザー・アカウントのパスワードを入力します。

パスワードは以下のルールに準拠する必要があります。

- 長さが 8 文字以上である。
- 少なくとも 1 文字の英字と英字以外の文字を含む。
- ユーザー名を含まない。
- 直前の 8 つのパスワードのいずれかと同じパスワードを使用しない。
- 30 日ごと (デフォルト)、または「[102 ページの『パスワードの最長使用日数の変更』](#)」セクションで指定した日数ごとに少なくとも 1 回変更する必要があるが、1 日に 2 回以上変更してはならない。

7. 「**パスワードの確認**」フィールドに、このユーザー・アカウントのパスワードを再度入力します。
パスワードが保存される前に、入力した 2 つのパスワードが比較されて一致していることが確認されます。

注: パスワードは、このユーザー・アカウントに初めてログインするときに変更する必要があります。

8. このユーザー・アカウントを無効にする場合は、「**アカウントが無効**」チェック・ボックスを選択します。

アカウントを無効にすると、アカウントを削除することなく、アカウントの使用を防止できます。

注: 管理者アカウントを無効にすることや、管理者アカウントのグループを変更することはできません。

9. このユーザー・アカウントのユーザー・グループを選択します。少なくとも1つのユーザー・グループを選択する必要があります。そのユーザーには、選択するグループに対して定義されている権限レベルが付与されます。
10. 「保存」をクリックしてユーザー・アカウントを保存します。
新規ユーザー・アカウントがリストに入った「ユーザー・アカウントとグループ」ページが表示されます。

ユーザー・アカウントとユーザー・グループの変更

既存のユーザー・アカウントとユーザー・グループを変更できます。

ユーザー・アカウントの変更

既存のユーザー・アカウントを変更できます。

このタスクについて

ユーザー・アカウントを変更するには、以下の手順に従ってください。

手順

1. ナビゲーション・ペインで、「管理」 > 「ユーザー・アカウント」をクリックします。
「ユーザー・アカウントとグループ」ページが表示されます。
2. 「アカウント」タブをクリックし、続いてユーザー・アカウントの横にある「編集」(✎)アイコンをクリックします。
「ユーザー・アカウント」ページが表示されます。
3. 「一般」ペインで、このユーザー・アカウントの基本情報を変更できます。
4. 「パスワードの入力」ペインで、パスワードとパスワード管理情報を変更できます。このユーザー・アカウントを無効にすることもできます。

パスワードは以下のルールに準拠する必要があります。

- 長さが8文字以上である。
- 少なくとも1文字の英字と英字以外の文字を含む。
- ユーザー名を含まない。
- 直前の8つのパスワードのいずれかと同じパスワードを使用しない。
- 少なくとも90日ごとに変更する必要があるが、1日に2回以上変更してはならない。

注: パスワードは、このユーザー・アカウントに初めてログインするときに変更する必要があります。

5. このユーザー・アカウントを無効にする場合は、「**アカウントが無効**」を選択します。
アカウントを無効にすると、アカウントを削除することなく、アカウントの使用を防止できます。ユーザー・アカウントの削除については、[136 ページ](#)の『ユーザー・アカウントとユーザー・グループの削除』を参照してください。

注: 管理者アカウントを無効にすることや、管理者アカウントのグループを変更することはできません。

User Account

Asterisks (*) indicate mandatory fields that are required to complete this action.

General

The following describes user account basic information.

User name: *
Uniquely identifies the user.

Full name:
Identifies the user's full name.

Description:
Describes the user.

Enter Password

Enter a new password and then type it again in the confirm field to confirm.

New password:

Confirm new password:

Disable Account: Account is disabled

Member Of

The groups this user is a member of.

Select user groups: * Administrator

図 106. 管理ユーザー・アカウントの変更

6. 「グループ」 ペインで、このユーザー・アカウントが属するユーザー・グループを変更できます。ユーザー・アカウントは、少なくとも1つのユーザー・グループのメンバーでなければなりません。
7. 「保存」 をクリックして変更内容を保存します。
変更された情報が「ユーザー・アカウントとグループ」 ページに表示されます。

ユーザー・グループの変更

既存のユーザー・グループを変更できます。

始める前に

注: 「管理者」 グループは変更できません。

このタスクについて

ユーザー・グループを変更するには、以下の手順に従ってください。

手順

1. ナビゲーション・ペインで、「管理」 > 「ユーザー・アカウント」 をクリックします。
「ユーザー・アカウントとグループ」 ページが表示されます。
2. 「グループ」 タブをクリックし、続いてユーザー・グループの横にある「編集」 (✎) アイコンをクリックします。
「ユーザー・グループ」 ページが表示されます。
3. 「一般」 ペインで、このユーザー・グループの基本情報を変更できます。
4. 「メンバーの権限レベル」 ペインで、このユーザー・グループが持つ権限を「管理者」、「ディスカバリー」、「読み取り」のいずれかに変更できます。

5. 「メンバーの権限レベル」で「ディスカバリー」権限レベルを指定した場合は、このユーザー・グループがディスカバリーする権限を持つスコープ・セットを「選択したスコープ・セットに制限」ペインで変更できます。
6. 「保存」をクリックして変更内容を保存します。
変更された情報が「ユーザー・アカウントとグループ」ページに表示されます。

ユーザー・アカウントとユーザー・グループの削除

既存のユーザー・アカウントとユーザー・グループを削除できます。

ユーザー・アカウントの削除

既存のユーザー・アカウントを削除できます。

このタスクについて

注: 管理者ユーザー・アカウントは削除できません。

ユーザー・アカウントを削除するには、以下の手順に従ってください。

手順

1. ナビゲーション・ペインで、「管理」 > 「ユーザー・アカウント」をクリックします。
「ユーザー・アカウントとグループ」ページが表示されます。
2. 「アカウント」タブをクリックし、削除するユーザー・アカウントの横にある「削除」(🗑️)アイコンをクリックします。
3. 「OK」をクリックしてユーザー・アカウントの削除を確認します。

ユーザー・グループの削除

既存のユーザー・グループを削除できます。

このタスクについて

注: 管理者ユーザー・グループは削除できません。

ユーザー・グループを削除するには、以下の手順に従ってください。

手順

1. 「管理」 > 「ユーザー・アカウント」をクリックします。
「ユーザー・アカウントとグループ」ページが表示されます。
2. 「グループ」タブをクリックし、削除するユーザー・グループの横にある「削除」(🗑️)アイコンをクリックします。
3. 「OK」をクリックしてユーザー・グループの削除を確認します。

注: ユーザー・グループを削除できるのは、そのユーザー・グループにユーザーが割り当てられていない場合のみです。

ユーザー補助

Technical Support Appliance は、サポートされるブラウザのユーザー補助機能の妨げになることはありません。ユーザー補助機能の包括的なリストについては、ご使用のサポートされるブラウザのユーザー補助サポート・ページにアクセスしてください。サポートされるブラウザのリストについては、[5 ページ](#)の『[Web ブラウザーの要件](#)』を参照してください。

本製品の資料は Adobe Portable Document Format (PDF) 形式で提供されており、アクセシビリティの標準に準拠しています。PDF ファイルの使用に問題があり、Web ベース形式の資料を依頼する場合は、依頼の E メールを以下のアドレスに送信してください。

icfeedback@us.ibm.com

または、以下の住所に依頼のメールを送付することもできます。

International Business Machines Corporation
Information Development
3605 Hwy 52 North
Rochester, MN, U.S.A 55901

依頼の際には、説明の件名に資料のタイトル「IBM Technical Support Appliance Setup Guide」を必ず含めてください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

特記事項

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。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。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒 103-8510

東京都中央区日本橋箱崎町 19 番 21 号

日本アイ・ビー・エム株式会社

法務・知的財産

知的財産権ライセンス 渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確認できません。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をお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合が

あります。現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtml をご覧ください。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

Microsoft、Windows、Hyper-V および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Java™ およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

VMware、VMware ロゴ、VMware Cloud Foundation、VMware Cloud Foundation Service、VMware vCenter Server、VMware vSphere は、米国およびその他の国における VMware, Inc. またはその子会社の商標または登録商標です。



部品番号:

(1P) P/N: