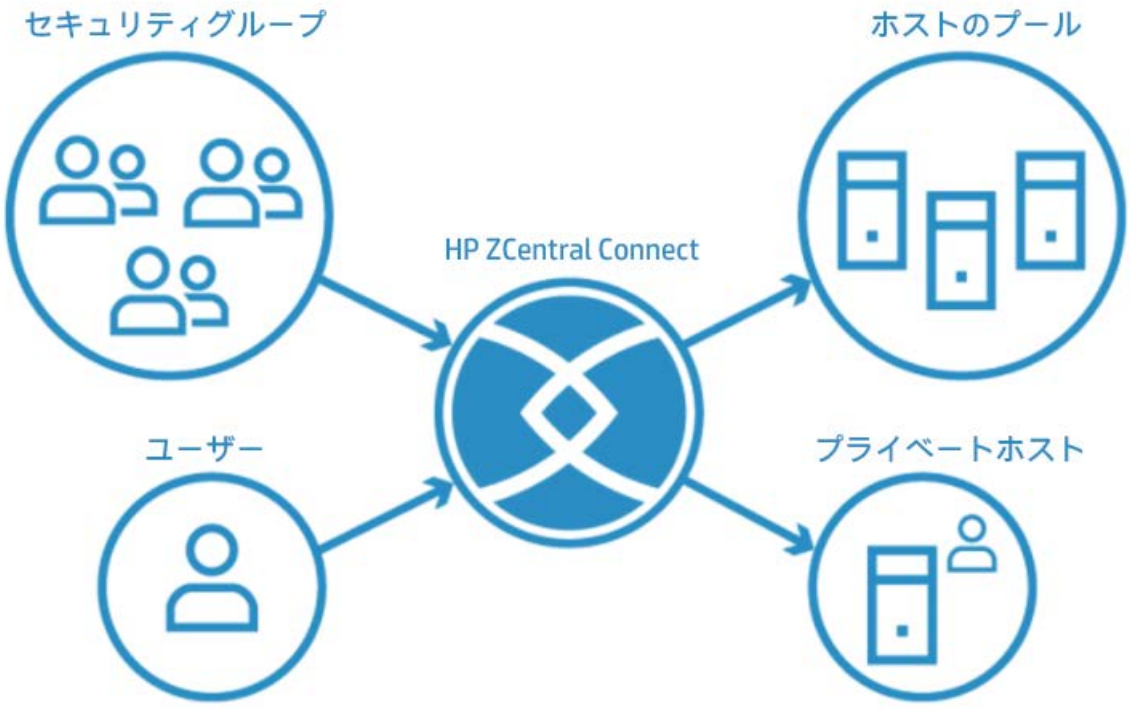
HP ZCentral Connect ユーザーガイド

本書の内容

1. 概要

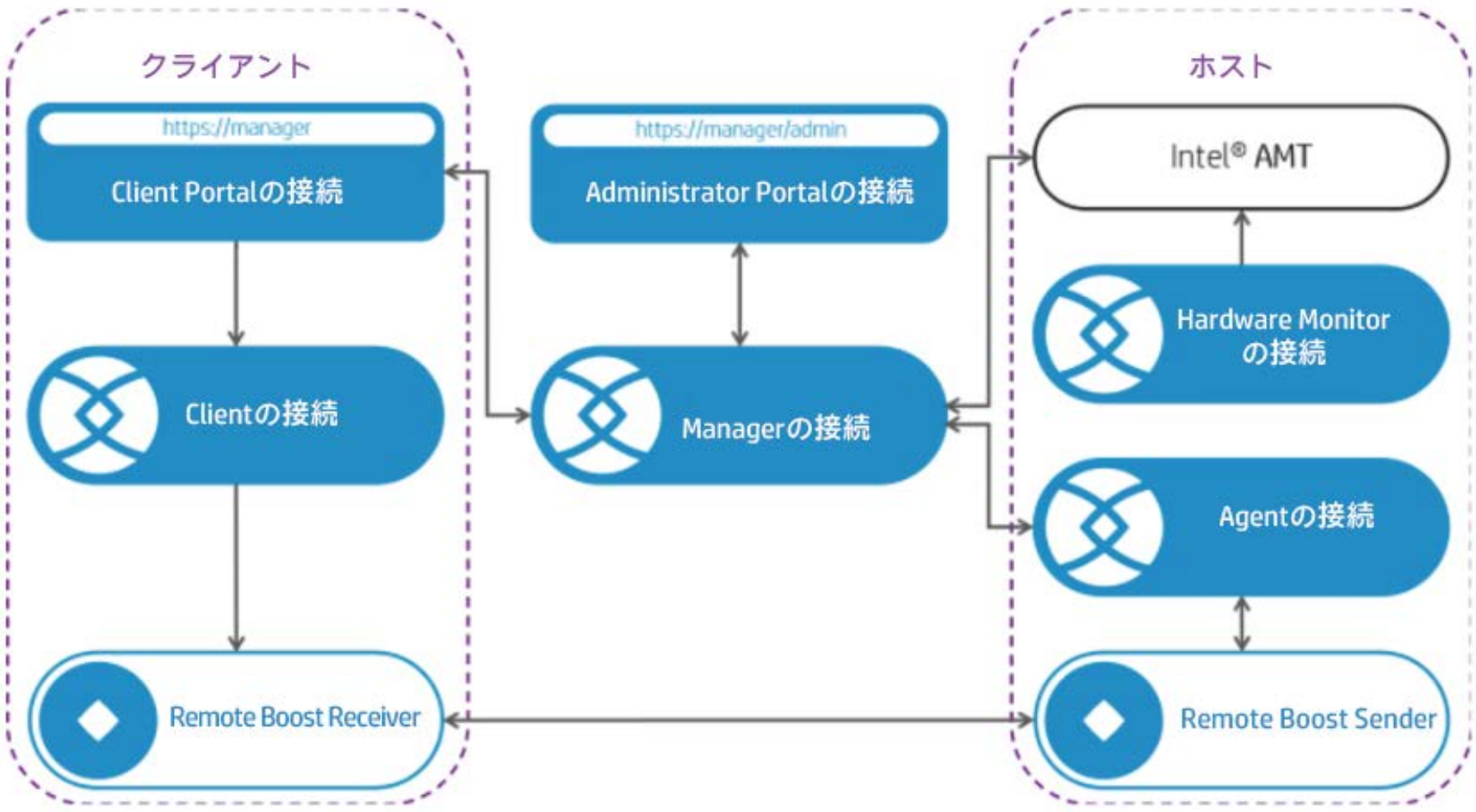
管理/仲介ソリューションである HP ZCentral Connect を使用することで、IT 管理者は多くのユーザーのリモートワークステーションを管理・編成することができます。ZCentral Connect は、HP ZCentral Remote Boost、Intel vPro®プラットフォーム：Intel® Active Management Technology（AMT）などの既存ツールおよび市場標準を活用して、管理者に軽量かつ効果的なリモート管理エクスペリエンスをもたらします。

ZCentral Connect では、「管理者」と「ユーザー」という 2 つの基本的な役割が定義されています。「管理者」は、ワークステーション（ホスト）の接続の仲介、管理、監視のポリシーを構築する責任があります。「ユーザー」は、HP ZCentral Remote Boost を介してリモートで作業するためのリモートワークステーションを求めます。



1.1. コンポーネント

次の図は、ZCentral の主要コンポーネントの概要を示しています。



コンポーネント	説明
HP ZCentral Connect Manager	管理者とユーザー両方の Web エンドポイントをホストする HP ZCentral Connect Manager Windows サービス
HP ZCentral Connect Administrator Portal	管理者向けの Web エンドポイント。例：https://zcentralconnect.local.domain/admin
HP ZCentral Connect Client Portal	ユーザー向けの Web エンドポイント。例：https://zcentralconnect.local.domain/
HP ZCentral Connect Client	エンドユーザーのマシンでローカルに HP ZCentral Remote Boost を起動します
HP ZCentral Remote Boost Receiver	ホストとの Remote Boost 接続を確立します
Intel® AMT	ZCentral がリモートで電源状態を管理し、ワークステーションのシステムイベントを監視できるようにします

コンポーネント	説明
HP ZCentral Connect Agent	ホストの状態を監視し、ステータスの更新を Manager に送信します
HP ZCentral Connect Hardware Monitor	電源装置の状態を監視し、イベントを Intel® AMT に報告します
HP ZCentral Remote Boost Sender	グラフィック、オーディオ、USB データを Remote Boost Receiver に送信します

1.2. 機能

ZCentral Connect の主な機能は次のとおりです。

機能	説明
ホストインベントリ	ZCentral Connect には管理対象ホストのリストが含まれています。この場合ホストは、ユーザーによるリモートデスクトップアクセスを目的としたワークステーションです。
HP ZCentral Remote Boost 接続の仲介	ZCentral Connect は、ユーザー向けの ZCentral Remote Boost Sender を実行している適切なホストを仲介します。仲介ポリシーは、管理者が構成できます。
リモート電源管理	管理者とユーザーは Intel® AMT テクノロジーを活用して、ホストの電源をリモートで管理できます。
ホストモニタリング	ログインしたユーザーと ZCentral Remote Boost Sender サービスのステータスについてホストをアクティブに監視します。ZCentral Connect Agent が必要です。
プール	1 つまたは複数のホストと 1 つまたは複数のグループおよび/またはユーザーとの関連付け。
プライベートホスト	単一のホストと単一のユーザーの関連付け。

1.3. 要件と互換性

1.3.1. ZCentral Connect の導入要件

ZCentral Connect を導入するには、いくつかの要件を満たす必要があります。

- HP ZCentral Connect Manager（サービス）：
  - Microsoft Active Directory Domain Services 2012 R2 以降
  - Windows10（バージョン 1607 以降）、Windows Server 2016、または Windows Server 2019 に加わったドメイン
  - .NET Framework4.7.1 以降
  - 推奨される最小システム要件
    - 4 コア 2GHz CPU（i3、i5、i7、Xeon または vCPU）
    - 4 GB の RAM
    - 240 GB ソリッドステートドライブ（少なくとも 50 GB の空き容量）
    - 1 Gbps ネットワーク接続

- HP ZCentral Connect Client（ユーザー側）：
  - HP RGS Receiver バージョン 7.5、HP ZCentral Remote Boost Receiver 2020 以降
  - Windows/Linux®（RHEL/Suse/ThinPro）/macOS®
    - Edge バージョン 42.17134 以降
    - Chrome バージョン 70.0.3538 以降
    - Firefox バージョン 60.3.0 以降
- HP ZCentral Connect Agent（ホスト側）：
  - HP RGS Sender バージョン 7.5、HP ZCentral Remote Boost Sender 2020 以降
  - Intel® AMT バージョン 9 以降（リモート電源制御に必要）
  - Agent サービス（ログインと HP RGS Sender または HP ZCentral Remote Boost Sender サービスのステータスを監視するために必要）
    - Windows 10
    - Linux®（RHEL7/RHEL8/Ubuntu18.04/Ubuntu20.04）

1.3.2. ZCentral ソリューションの互換性

ZCentral ソリューションには、次の 2 つの主要コンポーネントが含まれます。

- Connect - リモートリソースとその関連付けを管理するために使用されます。
- Remote Boost - ユーザーをリモートマシンにアクティブに接続するために使用されます。

ZCentral ソリューションの全機能を使用するには、すべての ZCentral ソフトウェアコンポーネントの最新バージョンが必要です。ZCentral Connect の各リリースは、前述した Manager、Agent、Client などのすべてのコンポーネントのリリースです。Connect Manager の更新されたバージョンは、古いバージョンの Connect Agent および Client と互換性がありますが、新しい機能のために古いバージョンの機能の一部が制限される場合があります。

ZCentral Connect を Remote Boost と完全に統合し、最新の機能を利用するには、Remote Boost のバージョンも最新である必要があります。Connect は、以前は HP RGS と呼ばれていた古いバージョンの Remote Boost をサポートしていますが、古いバージョンの Remote Boost では機能が制限されます。

最新の Connect 機能の詳細については、このドキュメントの「高度な管理者機能」セクションを参照してください。

注意：エンドユーザーは、ZCentral Connect を介してアクセスされる各ワークステーションオペレーティングシステムおよびソフトウェアアプリケーションが、オペレーティングシステムまたはソフトウェアアプリケーションプロバイダーの条件に従って適切にライセンスが付与されていることを確認する責任があります。

2. はじめに

ZCentral Connect の使用を開始するためのいくつかの前提条件：

1. 以前に ZCentral Connect Beta バージョンをインストールしている場合、続行する前にアンインストールしてください
2. ZCentral Connect Manager を実行でき、Microsoft Active Directory Domain に接続されているマシンを利用できるようにします
3. ZCentral Remote Boost Sender と Intel® AMT でプロビジョニング済みのワークステーション（ホスト）のセットを用意します
4. ユーザーが ZCentral Connect にアクセスできるように、すべてのマシンに ZCentral Remote Boost Receiver をインストールします

ZCentral Connect の使用を開始するための簡単な手順を以下に示します。

1. ZCentral Connect Manager をインストールします
2. ZCentral Connect Administrator Portal にログインします
3. ZCentral Connect で管理するホストを登録またはインポートします
4. 必要に応じて Active Directory からユーザーとセキュリティグループをインポートします
5. プールとプライベートホストを構成します
6. 有効なライセンスファイルがインストールされていることを確認します
7. ZCentral Connect Client Portal のアドレスをユーザーと共有し、ユーザーがホストへのセッションを作成できるようにします

2.1. Intel® AMT との統合

ZCentral Connect Manager を介した電源操作を有効にするには、最初に Intel® AMT と統合し、各ホストをプロビジョニングする必要があります。

注意：セキュリティ上の理由から、ZCentral Connect を Intel® AMT と統合する際には、Kerberos を使用することを強くお勧めします。Manager では、AMT デバイスとの通信に対して TLS（Transport Layer Security）接続のみがサポートされます。Manager と AMT デバイス間の双方向認証を提供する場合は、相互 TLS（mTLS）をお勧めします。

2.1.1. AMT のプロビジョニング

HP ワークステーションのプロビジョニングの概要については、HP が提供するホワイトペーパー『HP のビジネスノートパソコン、デスクトップ、およびワークステーションにおける Intel® AMT のセットアップと構成』を参照してください。AMT のプロビジョニングの詳細については、Intel が提供するドキュメント『Intel® Active Management Technology の実装』を参照してください。

エンタープライズプロビジョニング

追加されたセキュリティ、および TLS、mTLS、Kerberos への簡単なアクセスのメリットを活用するには、エンタープライズプロビジョニングが必要です。エンタープライズプロビジョニングは、手動プロセスが実行不可能な多数の AMT デバイスのプロビジョニングにも役立ちます。

- エンタープライズプロビジョニングには、Intel（R）セットアップおよび構成ソフトウェア（SCS）およびそこに含まれるリモート構成サーバー（RCS）が必要です。
- 環境のセットアップの際には、『SCS ユーザーガイド』をことができます。
- Intel®は、Windows ホストマシンで実行でき、RCS からプロビジョニングを要求できる AMT 構成ユーティリティ（ACU）実行ファイルを提供します。
- Microsoft System Center Configuration Manager（SCCM）用の Intel® SCS アドオンは、一括プロビジョニングに役立ちます。

ZCentral Connect で使用する Windows マシンのグループをプロビジョニングするために実行できるいくつかの手順の例を以下に示します。

1. Active Directory（AD）Integration、Access Control List、TLS、および Mutual Authentication（mTLS）を使用して、プロビジョニングプロファイルを作成します。
2. ACU 実行ファイルを呼び出すスクリプトを作成して、ConfigViaRCSOnly コマンドを指定し、Intel® SCS を使用してデバイスをプロビジョニングし、それをリモート構成サーバー（RCS）と作成したプロファイルで指定します。
3. グループポリシーを使用して、プロビジョニングが必要なマシンにスクリプトと ACU 実行ファイルを配布します。

注意：Linux®では AMT 構成ユーティリティはサポートされていません。Windows OS を起動するか、「ベアメタルのセットアップと構成」（『Intel® SCS ユーザーガイド』を参照）を使用する必要があります。

手動プロビジョニング

システムで実行できる最も基本的なプロビジョニングは、手動プロセスによるものです。このプロビジョニングでサポートされる機能は、エンタープライズプロビジョニングと比較すると制限されています。さらにこのプロセスでは、プロビジョニングが必要な各ホストへの物理的アクセスを必要とします。

ZCentral Connect 用の Intel® AMT を有効にし、構成するために必要な手順を要約したリストを以下に示します。

1. マシンを起動します
2. POST 処理中に F6 または Ctrl + P を押して、MEBx セットアップメニューに入ります（これはワークステーションのモデルによって異なります）
3. [MEBx ログイン]を選択し、デフォルトのパスワード「admin」を入力します
4. 新しいパスワードを入力します。AMT パスワードに関するベストプラクティスについては、HP が提供するホワイトペーパー『HP のビジネスノートパソコン、デスクトップ、およびワークステーションにおける Intel® AMT のセットアップと構成』を参照してください
5. [Intel® AMT の構成]を選択します
6. [パワーコントロール]を選択します
7. [ホストのスリープ状態]で、[Intel® AMT ON]のオプションが、[On in S0, ME Wake in S3, S4-5]に設定されていることを確認します
8. Esc キーを押して前のメニューに戻ります

9. [ネットワークアクセスの有効化]を選択します
10. Y を押してネットワークアクセスを有効化します
11. MEBx セットアップメニューを終了します

Intel® AMT が正しくプロビジョニングされたことを確認するには、http://<hostname>:16992 を参照し、ユーザー名「admin」と新しく作成したパスワードでサインインします。

注意：TLS をセットアップする前のネットワークトラフィックは暗号化されていません。クローズドネットワークで手動プロビジョニングのセットアップと構成を実行することをお勧めします。
次に、Manager が必要とする TLS を AMT デバイスにセットアップする必要があります。これは、MeshCommander を使用して行うことができます。次の手順は、プロセスの例を示しています。

1. MeshCommander を開きます
2. ルート証明書をまだ構成していない場合は、次の手順に従います。
    1. [証明書マネージャー]タブ（左端の証明書アイコン）を開きます
    2. ルート証明書を作成します
    3. 新しいルート証明書を確認し、.cer ファイルを保存します
    4. Manager を実行しているマシンの証明書ストアに.cer ファイルをインポートします
        - Manager サービスを実行しているアカウントはこの証明書を信頼する必要があります
        - これに最適な場所は、LocalMachine の信頼されたルートストアです
        - この単一の信頼されたルート証明書を使用して、今後各ホストの TLS 証明書を発行できます

3. MeshCommander に戻り、[コンピューターの管理]タブ（左端の 2 つのモニターアイコン）を開きます
4. プロビジョニングされたばかりのホストを追加します
5. ホストに接続します
6. [セキュリティ設定]タブを開きます
7. [証明書の追加...]をクリックして、作成したルート証明書を信頼されたルート証明書として追加します
8. [証明書の発行]をクリックし、ルート証明書を使用して TLS サーバー（HTTPS）証明書を発行します
    - 共通名が、Manager でホストを参照するために使用する予定の名前と一致していることを確認してください
9. [リモート TLS セキュリティ]の横にあるリンクをクリックします
10. 新しく発行された証明書とサーバー認証 TLS のみを選択します
11. [OK]をクリックし、TLS を使用してホストに再接続し、接続をテストします

TLS が有効になっている場合、Web インターフェイスには https://<hostname>:16993 経由でアクセスすることができます。

相互 TLS は、MeshCommander を介してセットアップすることもできます。次の手順は、プロセスの例を示しています。

1. MeshCommander を開きます
2. mTLS を使用してホストを構成するのが初めての場合は、次の手順に従います。
    1. [証明書マネージャー]タブ（左端の証明書アイコン）を開きます
    2. TLS のセットアップ時に作成されたルート証明書を使用して、Intel（R）AMT コンソールの新しい Client 証明書を発行します
        - 使用される共通名は後で必要とされ、特定のホストに関連付けられていません
    3. 新しい Client 証明書を確認し、.p12 ファイルを保存します
    4. ZCentral Connect Manager マシン上の LocalMachine の個人証明書ストアに証明書をインポートします
        - 「相互 TLS」セクションの手順に従って、Manager と統合します
3. 構成されているホストに接続します
4. [セキュリティ設定]タブを開きます
5. [リモート TLS セキュリティ]の横にあるリンクをクリックします
6. [セキュリティ]に[相互認証 TLS]のみを選択します
7. 発行された証明書の共通名をリモート CN のリストに追加します
8. [OK]をクリックします
9. Manager を介してホストに接続します

注意：相互 TLS が推奨されますが、必須ではありません。

注意：MeshCommander を介して TLS と mTLS を有効にする場合、ルート証明書をファイルシステムからインポートすることもできます。秘密鍵もインポートする必要があります。

注意：このプロセスはホストごとに個別に実行する必要があり、手動プロビジョニングで Kerberos をセットアップすることはできません。スケーラブルで安全なソリューションには、エンタープライズプロビジョニングを使用してください。

2.1.2. AMT 接続オプション

2.1.2.1. 通信の暗号化

TLS

TLS（Transport Layer Security）は Manager が必要とし、Manager と AMT デバイス間の通信を暗号化するために使用されます。AMT デバイスは、接続を確立するために Manager から信頼される必要があるサーバー証明書を保持します。名前の不一致エラーを回避するために、Manager がホストに使用するホスト名は、証明書の共通名またはサブジェクト代替名と一致する必要があります。

注意：AMT デバイスに対して TLS を有効にするには、Intel® SCS によるエンタープライズプロビジョニングを使用してプロビジョニングするか、MeshCommander などの外部ツールを使用して手動でプロビジョニングした後に有効にする必要があります。

相互 TLS

相互 TLS（mTLS）は、2 番目の証明書検証を含めることで TLS の上に追加できる付加的なセキュリティレイヤーです。HP は mTLS の使用を推奨していますが、必須ではありません。Manager が AMT からのサーバー証明書を信頼する必要があることに加えて、AMT デバイスは、Manager がアクセスできるクライアント証明書を信頼する必要があります。AMT で mTLS に使用されるクライアント証明書は特別で、ユーザー環境でセットアップするための追加手順が必要です（『Intel® SCS ユーザーガイド』の「第 9 章：証明機関の準備」を参照してください）。
Manager サービスを実行しているアカウントは、クライアント証明書の秘密鍵にアクセスできる必要があります。これを行うには、AMT デバイスによって信頼されている証明機関がクライアント証明書を発行する必要があります。この証明書は、現行ユーザーまたはローカルマシン（Manager を実行しているアカウントによって異なります）に対する Manager コンピューターの個人証明書ストアに配置する必要があります。AD アカウントを使用して Manager サービスを実行する場合、証明書は現行ユーザーの個人ストアに存在する必要があります。LOCALSYSTEM またはマネージドサービスアカウント（MSA）を使用して Manager サービスを実行する場合、証明書はローカルマシンの個人ストアに存在する必要があります。さらに、MSA を使用する場合は、秘密鍵へのアクセスを許可する必要があります。これは、次の手順に従って実行できます。

1. ローカルマシン証明書を管理するための MMC スナップインを開きます（certlm.msc を実行します）
2. 発行された AMT クライアント証明書を右クリックします
3. [すべてのタスク] -> [秘密鍵の管理]をクリックします
4. MSA をユーザーのリストに追加し、読み取りアクセス許可を付与します

次に、証明書のサブジェクト名を、Manager 設定ファイルの AMTMutualAuthCertName 設定の値として追加する必要があります。『ユーザーガイド』の「詳細設定」セクションに記載されている手順に従って、設定ファイルを編集します。

注意：AMTMutualAuthCertName 設定に値がある場合、証明書の収集が試行されます。証明書が見つからない場合、すべての AMT 接続が失敗します。証明書は要求されるまで AMT デバイスに送信されないため、証明書にアクセスできる限り、mTLS 以外の接続は影響を受けません。
注意：AMT デバイスに対して mTLS を有効にするには、Intel® SCS によるエンタープライズプロビジョニングを使用してプロビジョニングするか、MeshCommander などの外部ツールを使用して手動でプロビジョニングした後に有効にする必要があります。

2.1.2.2. 認証

AMT で使用する認証方法は、ホストを作成、編集、またはインポートするときに、[AMT 認証/セキュリティ]フィールドで選択できます。TLS は Manager に必要であるため、すべてのオプションにデフォルトで存在します。すべてのオプションは、相互 TLS（mTLS）もサポートしています。

Kerberos

ZCentral Connect は、Kerberos を使用して AMT デバイスで認証できます。Kerberos 認証はより高度なセキュリティを提供し、各ホストの AMT 資格情報を管理する必要はありません。Kerberos 認証を利用するには、Manager を実行しているアカウントに、プロビジョニング中にセットアップされるアクセス許可を付与する必要があります。Intel® SCS を使用してプロビジョニングプロファイルを作成しているときに、Manager を実行しているアカウントに「PT 管理」レルム権限を付与する必要があります（『Intel® SCS ユーザーガイド』の「ACL へのユーザーの追加」セクションを参照してください）。アカウントをプロファイルに直接追加するか、すでにアクセス許可を有しているグループにアカウントを追加することで、アクセス許可を付与できます。プロビジョニングプロセス中、プロビジョニングサーバーはサービスプリンシパル属性を持つ AD にオブジェクトを追加します。Manager で使用されるホスト名は、接続を成功させるためにこれらのサービスプリンシパルのいずれかと一致する必要があります。

注意：アカウントにアクセス許可が付与された後に、Manager サービスを再起動する必要があります。

注意：AMT デバイスに対して Kerberos 認証を有効にするには、Intel® SCS を使用したエンタープライズプロビジョニングによりプロビジョニングする必要があります。

Digest

Manager は、ユーザー名とパスワードを使用して AMT デバイスに接続できます。ユーザー名とパスワードは、AMT に接続する必要があるホストごとに保持する必要があります。AMT に使用されるパスワードは、Manager によって保存されるときに暗号化されます。Digest は手動プロビジョニングによって有効になります。

注意：Digest 認証は最も安全性の低い認証オプションであり、各ホストの資格情報を維持する必要があるため、HP では推奨されていません。AMT デバイスとの通信を行うたびに、ユーザー名とパスワードをネットワーク経由で送信する必要があります。代わりに Kerberos 認証の使用を検討することをお勧めします。

注意：Digest を使用している場合は、AMT ホストごとに異なるパスワードを使用することをお勧めします。これにより、単一のパスワードが漏洩した場合の攻撃領域が減少します。

3. HP ZCentral Connect Manager のインストール

Manager は、ワークステーション、サーバー、仮想マシンなどのさまざまなプラットフォームにインストールできます。

Manager インストーラーでは、次の操作が実行されます。

1. Manager ファイルを%PROGRAMDATA%および%PROGRAM FILES%ディレクトリにコピーします
2. Manager を実行する Windows サービスを作成します
3. 自己署名証明機関によって署名された証明書を作成して、Manager ネットワーク通信を暗号化します
4. Manager マシンでファイアウォールルールを作成して、管理者とユーザーがネットワークから ZCentral Connect ページにアクセスできるようにします
5. 管理者ユーザーのユーザー定義パスワードを作成します
6. Manager Windows サービスを開始します

注意：インストーラーによって作成された証明書の代わりに独自の証明書を使用する必要がある場合は、「独自の証明書の使用」に記載されている手順に従ってください。

開始するには、Manager をインストールするマシンにログインし、インストールウィザードの指示に従ってください。

インストールウィザードを実行中に、管理者パスワードを定義し、Manager のネットワーク接続方法を構成するように求められます。カスタムネットワーク構成が必要な場合は、次の設定を変更してください。

- Web アドレスは、Manager サービスがバインドするネットワークエンドポイントです。これは、インストール時に作成された証明書の共通名として使用されます。Web アドレスは、完全修飾ドメイン名または IP アドレスにすることができます。
- Web サービスポートは、HTTPS 経由で Manager に接続するために使用される TCP ポートです。安全な接続のデフォルトのポートは 443 です。別のポートを選択する場合は、Manager ページにアクセスするときに、URL にそのポート番号を含める必要があります。たとえば、Web アドレス：zcentralconnect およびポート：8443 を選択した場合、ブラウザーで https://zcentralconnect:8443 を使用して接続する必要があります。
- メッセージバスポートは、Agent が HP ZCentral Connect Manager と通信するために使用される TCP ポートです。安全な接続のデフォルトポートは 8883 です。詳細については、『Agent 展開ガイド』を参照してください。

注意：Remote Boost Sender が Manager システムで実行されている場合は、ポート 42966 を使用しないでください。

失敗した場合は、「トラブルシューティング」ページのインストールのトラブルシューティングに従ってください。

3.1.サービスアカウントの選択

ZCentral Connect Manager はサービスとして実行され、次の 3 種類のアカウントのいずれかを使用できます。

- マネージドサービスアカウント（MSA）
- 標準の Active Directory アカウントまたはサービスアカウント
- LocalSystem アカウント

注意：アカウントのタイプを問わず、提供されたユーザー名はローカルコンピューターの管理者でなければなりません。

インストーラーから、アカウントのタイプと必要なパラメーターの入力が求められます。マネージドサービスアカウントを使用するには特別なセットアップと構成が必要ですが、標準のドメインアカウントのように手動によるパスワードの管理や維持は必要ありません。MSA のパスワードは AD によって管理され、定期的に再生成されるため、セキュリティが強化されます。スクリプト MSASetup.ps1 は、Manager で使用する MSA の作成と構成をサポートするために、インストールパッケージ内のスクリプトディレクトリに提供されています。LocalSystem を使用して Manager サービスを展開することはお勧めしません。詳細については、「LocalSystem の使用禁止」セクションを参照してください。

注意：インストール後に Manager サービスを実行するために使用されるアカウントの変更はサポートされていません。アカウントの変更が必要な場合は、Manager の再インストールが必要です。次のセクションでは、Manager で MSA を作成して使用するために必要な手順の概要を説明します。

3.1.1. マネージドサービスアカウントについて

マネージドサービスアカウントは、Manager サービスをホストするための推奨アカウントタイプです。MSA の詳細については、以下を参照してください。

- マネージドサービスアカウントの概要
- MSA のベストプラクティス

3.1.2. Microsoft RSAT ツールのセットアップ

MSASetup.ps1 スクリプトには、Microsoft RSAT が提供する PowerShell モジュールが必要です。これらのツールは通常、サーバーバージョンの Windows にインストールされます。以下で説明されているように、Windows10 では追加のインストールが必要になる場合があります。

- PowerShell ExecutionPolicy

注意：この手順は、オペレーティングシステムの構成によってはオプションとなる場合があります。

3.1.3. KDS ルートキーの存在の確認

ドメインコントローラーがマネージドサービスアカウントを作成する前に、キー配布サービス（KDS）のルートキーが存在している必要があります。詳細については、次をご覧ください：KDS ルートキー

KDS ルートキーの存在を確認するには、PowerShell プロンプトから次のコマンドを実行します。* Get-KdsRootKey *。このコマンドは、ルートキーの詳細を含む出力を生成します。出力が表示されない場合は、上記のリンクの手順に従ってルートキーを作成します。

注意：ルートキーを作成する必要がある場合は、MSA を作成する前に 10 時間待機する必要があります。

3.1.4. PowerShell スクリプトの実行の有効化

MSASetup.ps1 の実行を試みて、ExecutionPolicy エラーを受け取った場合、スクリプトの実行を可能にするためには、現在の実行ポリシーをバイパスしなくてはならない場合があります。次のコマンドを実行して、実行ポリシーをバイパスします。

- PowerShell.exe -ExecutionPolicy Bypass -File .\MSASetup.ps1 [command] [account]
- パラメーターの詳細については、以下を参照してください

注意：この手順は、オペレーティングシステムの構成によってはオプションとなる場合があります。

3.1.5. マネージドサービスアカウントの作成

MSASetup.ps1 スクリプトを使用して MSA を作成します。ZCentral Connect Manager をインストールする予定のマシンからスクリプトを実行します。マシンは Active Directory Domain に参加している必要があります。

- 次のコマンドを実行します：MSASetup.ps1 [command] [account]
- command パラメーターは add または remove のいずれかになります。
- add は、MSA を作成し、ローカルマシンで使用できるように構成します。
- remove は、ローカル MSA 構成を削除し、AD から MSA を削除します。
- アカウントは、MSA のアカウントの名前です。
- 正常に実行されると、アカウントは、マネージドサービスアカウント OU の下にある Active Directory のユーザーおよびコンピューターツール内に表示されます。

たとえば、「hpmangermsa」という名前の MSA を作成するには、次のコマンドを実行します。

- MSASetup.ps1 add hpmanagermsa

3.1.6. Manager のインストール中における MSA の指定

[マネージドサービスアカウント（MSA）を使用する]が選択されている場合、インストールプロセス中に、インストーラーからアカウント情報の入力が求められます。このアカウントは DOMAIN\ACCOUNTNAME 形式で指定する必要があります。アカウントが MSA の場合、アカウント名は末尾のドル記号を使用して指定する必要があります。たとえば、MSA アカウント名が「hpmanagermsa」でドメイン名が「somedomain.com」の場合、次を使用して、インストーラーで MSA を指定します。

- somedomain\hpmanagermsa$

3.2. サイレントインストール

Manager インストーラーはサイレントインストールをサポートします。サイレントインストールには、次のプロパティが使用されます。

- Hostname：Manager に使用するホスト名。
- Port：Manager に使用する Web サービスポート（オプション：デフォルトは 443）。
- MessageBusPort：Manager に使用するメッセージバスポート（オプション：デフォルトは 8883）。
- AdminPassword：Administrator Portal に使用する管理者パスワード。
- Service_Account：DOMAIN\ACCOUNT 形式で Manager サービスを実行するために使用されるアカウント名。MSA を指定するときは、末尾に$を含めます。
- ServiceAccountType：Manager サービスの実行に使用されるアカウントタイプ。LocalSystem または SvcAccount。
- ServiceAccountPassword：Manager の実行に使用されるサービスアカウントのパスワード。MSA の場合は空白のままにします。

デフォルトのポートを使用した信頼できるエンタープライズ環境におけるサイレントインストールの例：

msiexec.exe /i HP_ZCentral_Connect_2020_Manager.msi /qn Hostname=zcentralconnect.domain.local AdminPassword=SuperSecretPassword Service_Account=domain\zcentralconnectmsa$ Service_Account_Type=SvcAccount

ラボ環境でのサイレントインストールの例：

msiexec.exe /i HP_ZCentral_Connect_2020_Manager.msi /qn Hostname=zcentralconnect Port=8443 MessageBusPort=8080 AdminPassword=SuperSecretPassword Service_Account=LocalSystem Service_Account_Type=LocalSystem

注意：ZCentral Connect Administrator のパスワードは常に安全に保管し、書き込まれるスクリプトに保存しないようにしてください。

3.3. HP ZCentral Connect Administrator Portal へのアクセス

ZCentral Connect をインストールすると、Manager がインストールされているマシンにネットワーク接続されている任意のマシンで、サポートされているブラウザーの 1 つから ZCentral Connect Administrator Portal にアクセスできるようになります。

注意：デフォルトのポート 443 とは異なるポートを選択した場合は、必ず URL でネットワークポートを指定してください。

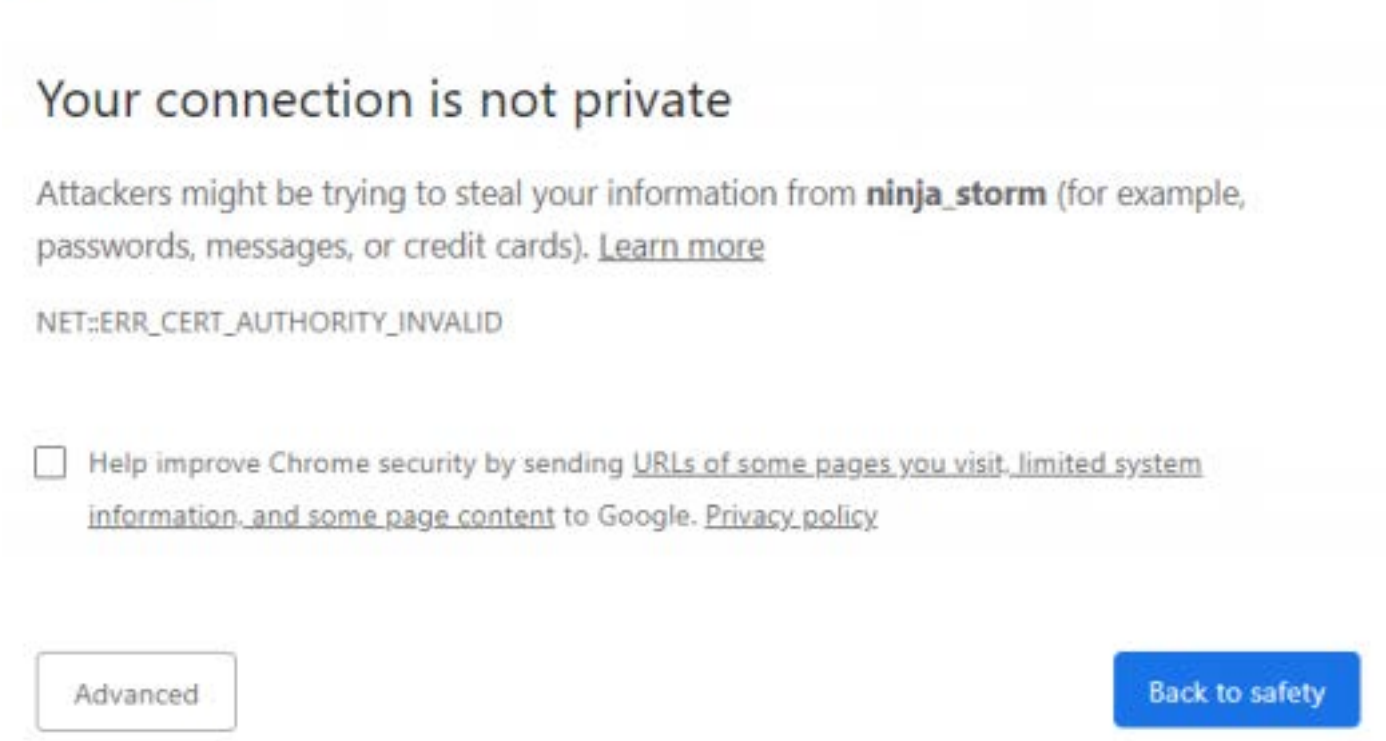
Manager は、インストール時に独自の証明書と自己署名証明機関（CA）を作成するため、CA がクライアントマシンで信頼されるようになるまでは「お使いの接続は、プライベートではありません」といった警告メッセージが表示されます。

注意：「使用環境における自己署名証明機関の承認」セクションのガイドに従って、クライアントマシンで CA を承認することができます。

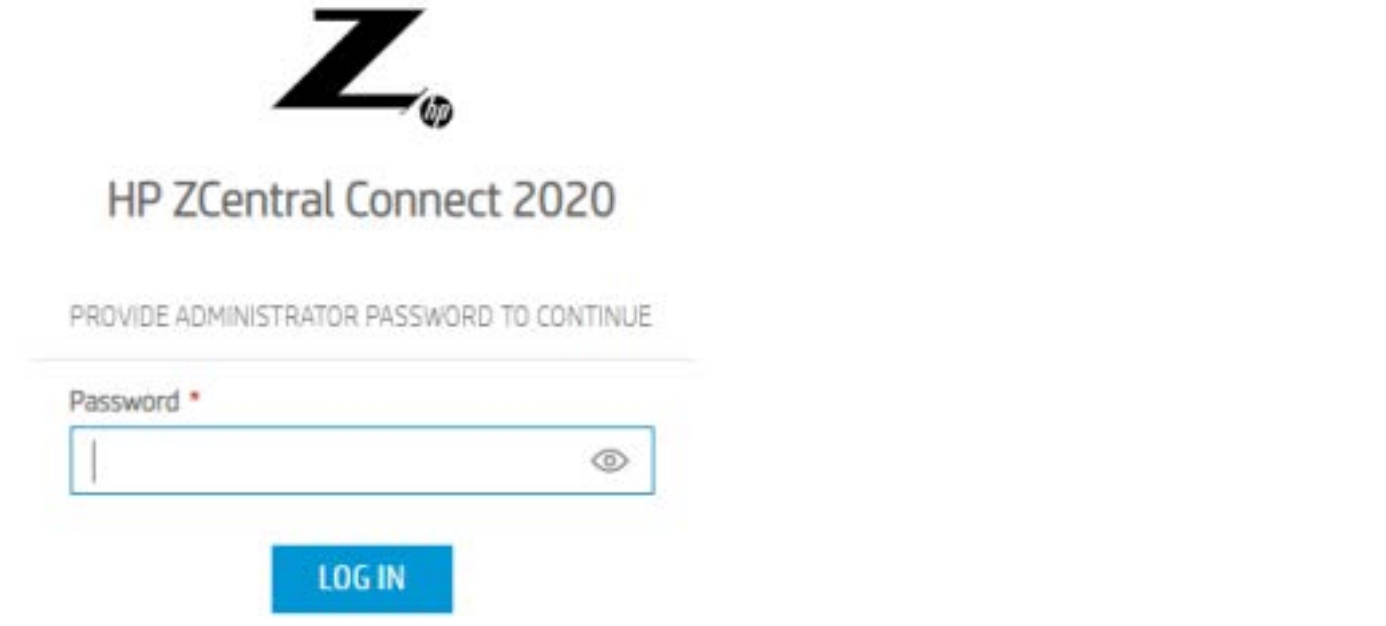
注意：インストール中に作成された証明書の代わりに独自の証明書を使用する必要がある場合は、「独自の証明書の使用」セクションに記載されている手順に従ってください。

注意：インストール中に作成された証明機関をマシンが信頼している場合、このメッセージは表示されません。独自の証明書の構成についてサポートが必要な場合は、このユーザーガイドの「独自の証明書の使用」セクションに記載されている手順に従ってください。マシンが証明機関をどのように信頼するかについて詳細を確認したい場合は、このユーザーガイドの「証明機関の信頼」セクションを参照してください。

続行するには、[詳細]をクリックして、[ホスト名に進む（安全ではない）]オプションを選択します。



初めてログインする場合、ZCentral Connect Manager のインストール時に定義したパスワードを入力します。



ログインすると、[ホスト]ページが表示されます。

3.4. 管理者パスワードの変更

管理者パスワードを変更するには、画面の右上にあるユーザーアイコンを探します。

[パスワードの変更]をクリックします。

現在のパスワードと新しいパスワードを入力します。[パスワードの確認]フィールドで新しいパスワードを確認します。

変更を適用するには、[パスワードの変更]ボタンをクリックします。

3.5. 詳細設定

HP ZCentral Connect には構成可能な設定が一定数ありますが、現時点では、HP ZCentral Connect Portal 経由でそれらの設定にアクセスすることはできません。

管理者は、次の場所にある設定ファイルを変更することで、HP ZCentral Connect の動作をカスタマイズできます：

%PROGRAMDATA%\HP\ZCentralConnectManager\settings.json

注意：変更を有効にするには、ZCentral Connect Manager サービスを再起動する必要があります。

サポートされているフィールドと対応するデフォルトの値は以下のように定義されています。

```
{
/* Hostname where HP ZCentral Connect listens to.*/
"Hostname": "myconnecthostname.domain",

/* ZCentral Connect HTTPS port.*/
"Port": "443",

/* Port where ZCentral Connect listens for Agent connections.*/
"MessageBusPort": "8883",

/* The thumbprint of the certificate used to encrypt HP ZCentral Connect network traffic.*/
"CertificateThumbprint": "",

/* The store of the certificate used to encrypt HP ZCentral Connect network traffic.*/
"CertificateStore": "Root",

/* Defines the number of days before the admin will get notified when the certificate is about to expire.*/  "CertificateExpirationDaysToNotify": "30",

/* Removes the capability to perform power operations from the HP ZCentral Connect Client Portal.*/
"DisablePowerOperationsForUsers": "false",

/* Disables single sign-on authentication option for HP ZCentral Connect Client Portal users.*/
"DisableKerberosAuth": "false",

/* Defines how long the authentication cookie for an admin or user will last.Format: "HH:mm:ss".*/
"CookieExpirationTime": "00:30:00",

/* Expiration time, in days, for an Agent authentication token.*/
"AgentTokenExpirationTimeInDays": "30",

/* Defines the frequency for automatic Agent authentication token renewal process.Format: "Days.HH:mm:ss".Example: 1.00.00:00 will renew every 24 hours;
0.04.00:00 will renew every 4 hours.*/
"AgentTokenRenewPeriod": "1.00:00:00",

/* Defines the number of concurrent connection requests that the Manager Message Bus can handle at a time.This value can be lowered to reduce the Manager resource
utilization.*/
"MessageBusConnectionBacklog": "20",

/* Defines the list of Users that can always connect to a Host when the Pool option Prevent Unmanaged Connections is enabled.List usernames only, FQDN is not
supported.Format: "username1 username2 (...)".*/
"UsersAlwaysAllowedToLogin": "Administrator",

/* Expiration time, in days, for the authentication token used in AMT Alerts subscription.*/
"AmtSubscriptionTokenExpirationTimeInDays ": "365",

/* Defines the frequency for automatic AMT Alerts authentication token renewal process.Format: "Days.HH:mm:ss".Example: 90.00.00:00 will renew every 90 days */
"AmtTokenRenewInterval ": "90.00:00:00",
```

/* Defines the frequency for System Event synchronization.The Manager will reach out to AMT devices to sync subscriptions and System Events.Format: "Days.HH:mm:ss".Example: 1.00.00:00 will renew every 24 hours; 0.04.00:00 will renew every 4 hours.*/

"AmtHardwareEventPolling": "12:00:00"

}

注意：設定ファイルには、内部使用のみを目的とした、変更してはならない、上述以外の他のプロパティが含まれている場合があります。

4. 管理者機能

管理者の役割は、ZCentral Connect を管理および監視することです。

ZCentral Connect Administrator Portal には、https://zcentralconnect.local.domain/admin のように、ZCentral Connect Client Portal アドレスに/admin の接尾辞を追加することで、アクセスすることができます。

ZCentral Connect は HP ワークステーション上で Intel® AMT サポートを活用して、統合されたリモート管理/リモート監視エクスペリエンスを提供します。詳細については、「Intel® AMT との統合」セクションを参照してください。

仲介機能に関して、ホストをユーザーが利用できるようにするために、管理者はプールやプライベートホストを構成する必要があります。プールとプライベートホストを作成するために管理者が実行すべきアクションの簡単なリストを以下に示します。

- プールを作成する
    1. ホストを登録またはインポートします
    2. セキュリティグループおよび/またはユーザーをインポートします
    3. プールを作成し、ホストとセキュリティグループ/ユーザーをプールに割り当てます
- プライベートホストの関連付けを作成する
    1. ホストを登録またはインポートします
    2. ユーザーをインポートします
    3. ホストとユーザーの間にプライベートホストの関連付けを作成します

次に、このガイドでは、管理者が利用できる主な機能のデモンストレーションを示します。

4.1. ホスト

[ホスト]ページは、ZCentral Connect の主要な領域の 1 つです。このページでは以下が提供されます。

- 管理対象ホストのインベントリ
- リモートホストの電源管理
- リモートホストの監視

4.1.1. ホストの登録とインポート

開始するには、Administrator Portal にアクセスし、左側のメニューにある[ホスト]をクリックして[ホスト]ページに移動します。

新しいホストの登録は、次の 2 つの方法で実行できます。

- ホストを追加：IP アドレス、ホスト名、または完全修飾ドメイン名から単一のホストを追加します。
- ホストをインポート：Microsoft Active Directory から 1 つ以上のホストをインポートします。Microsoft Active Directory は、次の方法で検索できます。
    - 名前：Active Directory 内のホストの名前
    - メンバー：グループの一部であるすべてのホストを検索します

注意：「メンバー」の検索では、Active Directory にセキュリティグループの正確な名前を入力する必要があります。

[検索アイコン]をクリックすると、Manager は Active Directory に対してクエリを実行し、検索結果を下の表に表示します。

注意：検索結果はアルファベット順には表示されません。

いずれのシナリオでも、ZCentral Connect のホスト管理方法を構成するオプションが提供されます。各オプションの説明は次のとおりです。

- ホスト名：ホストの有効なネットワーク名（IP アドレス、ホスト名、または完全修飾ドメイン名）。以下の「ホスト名のベストプラクティス」を参照してください。
- Agent でホストステータスを監視する：チェックを入れると、Manager はこのホスト上の Agent からの接続を待機します（ログインの変更と Remote Boost Sender サービスを監視できます）。このオプションでは、ZCentral Connect Agent をインストールする必要があります。詳細については、『Agent 展開ガイド』を参照してください。
- AMT でホストを管理する：チェックを入れると、Manager はこのホストの電源状態をリモートで監視および制御し、サポートされている場合は、システムイベントの受信を試みます。このオプションでは、このホストに対して Intel® AMT をプロビジョニングする必要があります。詳細については、「Intel® AMT との統合」および「システムイベント」セクションを参照してください。
- AMT に対する代替ホスト名、および代替ホスト名または IP アドレスを使用する：通常のホスト名とは異なる FQDN または IP アドレスを介して AMT デバイスにアクセスできる場合、このオプションは、代替ホスト名を使用して AMT デバイスに接続するよう Manager に指示します。詳細については、「Intel® AMT との統合」セクションを参照してください。
- AMT 認証/セキュリティ：Kerberos 認証が選択されている場合、Manager サービスの実行に使用されるアカウントが AMT デバイスでの認証に使用されます。Kerberos 認証では、Manager がサービスアカウントまたは MSA を使用する必要があります。Digest が選択されている場合、Manager はユーザー名とパスワードの認証を使用して AMT デバイスに接続します。この認証方法は、最も安全性の低いオプションであるため、HP では推奨されていません。詳細については、「Intel® AMT との統合」セクションを参照してください。

注意：Digest を使用している場合は、AMT ホストごとに異なるパスワードを使用することをお勧めします。これにより、単一のパスワードが漏洩した場合の攻撃領域が減少します。

- AMT ユーザー名および AMT パスワード：これらは、このホストの AMT デバイス用に構成された Digest 資格情報です。Kerberos が AMT に使用される場合、これらは有効になりません。

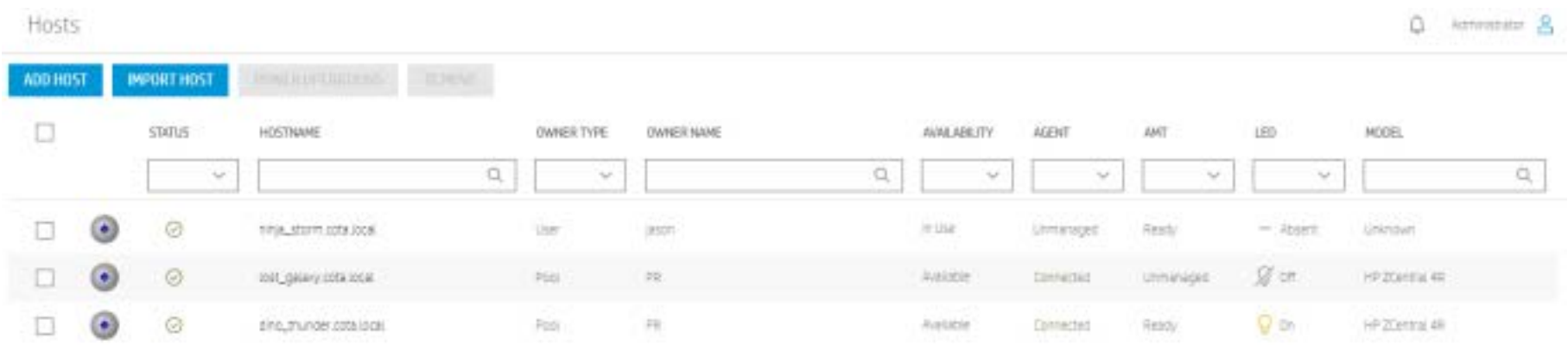
ホストが追加またはインポートされると、[ホスト]ページに表示されます。

注意：ホスト名は、ZCentral Connect によって小文字に変換されます。

注意：現時点で ZCentral Connect では、あるホストがどのセキュリティグループに属しているか、またはあるセキュリティグループにどのホストが属しているかを表示する方法は提供されていません。管理者は、この情報を表示するために、この製品の外部にある Active Directory ツールを使用する必要があります。

ホスト名のベストプラクティス

ZCentral Connect では、ホスト名が一意である必要があります。ただし、ネットワーク上でホストを参照する方法はいくつかあります。例として、ホスト名、FQDN、DNS エイリアス、IP が挙げられます。セキュリティと機能上の理由から、ZCentral Connect は各ホストに対して 1 つの参照のみを保持する必要があります。単一のホストが複数回登録されている場合、複数のユーザーが同時に同じホストに割り当てられる可能性があります。単一のホストに対する複数の参照を回避するには、環境と構成に応じて、単一タイプの参照のみを使用することがベストプラクティスです。FQDN は、ほとんどの Intel® AMT 環境ではデフォルトで必要とされるため、推奨されるパターンです。



4.1.2. ステータス

各ホストのステータスは、Manager が検出できるエラーの影響を受けます。エラーが検出されない場合、特定のホストの[ホスト]ページのステータス列に緑色のチェックマークが表示されます。エラーがある場合、この列には赤い警告アイコンが表示されます。アイコンをクリックすると、ステータスに影響するエラーのリストが表示されます。

ホストステータスに影響を与える可能性のあるエラーがいくつかあります。

ZCentral エラー：

ZCentral エラーは、リモートデスクトップ接続に関連するホストの可用性に影響を与えます。エラーカテゴリは次のとおりです。

- Agent：Agent はメッセージバスに接続されている必要がありますが、接続されていません。このエラーは、Agent の接続ステータスが[切断]である場合、ホストの電源がオフになっている場合、または一部の機能を許可するために Agent の監視が必要であるがホストに対して有効になっていない場合に発生します。
- 管理されていない接続：ユーザーは、同じユーザーによってチェックアウトされていないホストにログインしています。これは、可用性に関係なく、ホストで発生する可能性があります。管理されていない接続に関してホストを監視するには、Agent が接続されている必要があります。プールで[管理されていない接続を防ぐ]オプションを使用すると、ZCentral Connect は、許可されていないユーザーが Remote Boost を使用してホストに接続することを防止できます。この機能の詳細については、以降の「管理されていない接続を防ぐ」セクションを参照してください。
- AMT：AMT 接続ステータスはエラー状態です。各エラーの詳細については、「トラブルシューティング」ページの「AMT エラー」セクションを参照してください。
- Remote Boost Sender：ホスト上で Remote Boost Sender プロセスが実行されていません。Remote Boost Sender プロセスを監視するには、Agent が接続されている必要があります。
- Hardware Monitor：ホスト上で ZCentral Hardware Monitor プロセスが実行されていません。Remote Boost Sender プロセスを監視するには、Agent が接続されている必要があります。

システムエラー：

システムエラーには 2 つのタイプがあり、Intel® AMT によって生成されます。詳細については、以降の「イベント」セクションを確認してください。

- システム起動：ZCentral Connect は、AMT11 以降をサポートするホストからの初期化エラーを検出できます。詳細については、以降の「サポートされているイベント」セクションを確認してください。
- 電源：ZCentral Connect は、HP ZCentral 4R Workstation の電源エラーを検出できます。詳細については、以降の「サポートされているイベント」セクションを確認してください。

注意：Agent 関連のエラーを検出するには、Agent が接続状態または切断状態である必要があります。

注意：ステータスは、ホストのチェックアウトを妨げるものではありません。ただし、ホストのステータスは、プールからユーザーに割り当てられるときの優先度に影響します。ホストで検出されるエラーが多いほど、優先度は低くなります。

4.1.3. 可用性

可用性はホストの仲介状態を定義します。このプロパティの状態は次のとおりです。

- 使用可能：ホストはチェックアウト可能です。
- チェックアウト済み：ホストはユーザーによってチェックアウト済みです。
- 使用中：ホストはチェックアウトしたユーザーによってアクティブに使用されており、ホスト上の Agent は、ユーザーがログインしたことを Manager に通知済みです。この状態は、Agent がホストにインストールされている場合に限り発生します。

注意：[Agent でホストステータスを監視する]がホストに対して無効になっている場合、可能性のある状態は「使用可能」および「チェックアウト済み」です。

プール内におけるホストの優先順位付け

プールからホストをチェックアウトする場合、ユーザーは特定のホストを選択できません。代わりに、ZCentral Connect は、ユーザーがプールから新しいセッションを要求するときに、ユーザーのホストを選択します。

ZCentral Connect は、特定のプール内におけるすべてのホストの使用バランスを均等に保つよう試みます。このために、しばらくチェックアウトされていないホストを優先させます。最近チェックアウトされたホストは、優先順位の一番下に移動されます。

[ステータス]フィールドに表示されるホストエラーも、プール内のホストの優先度に影響します。ホストのエラー数が多いほど、優先度は低くなります。プール内におけるホストの優先順位付けに関する簡単な概要を以下に示します。

- エラーのないホストは、チェックアウトリストの一番上に配置されます。これらの中で、最も長い期間チェックアウトされていないホストが最初に提示されます。
- エラーが 1 つあるホストは、エラーのないホストの次に優先されます。
- エラーが 2 つあるホストは、エラーが 1 つあるホストの次に優先されます（以下同様）。

注意：[Remote Boost 対応ホストのみを提供]の高度な機能を使用する場合、エラーのあるホストをユーザーに提供しないようにプールを構成できます。この機能の詳細については、以降の「Remote Boost 対応ホストのみを提供」セクションを参照してください。

4.1.4. Agent ステータス

[ホスト]ページの[Agent]列は、ホストに関連付けられている Agent のステータスを追跡します。次のような状態があります。

- 管理されていません：[Agent でホストステータスを監視する]オプションがホストに対して有効になっていません。
- 接続済み：Agent がメッセージバスに接続されています。
- 切断：Agent はメッセージバスに接続されている必要がありますが、接続されていません。これは、Agent がインストールされていない、Agent が接続できない、またはホストの電源がオフになっている場合に発生する可能性があります。

注意：Agent の展開プロセスが完了するまで、Agent は切断状態になります。詳細については、『Agent 展開ガイド』を参照してください。

4.1.5. AMT ステータス

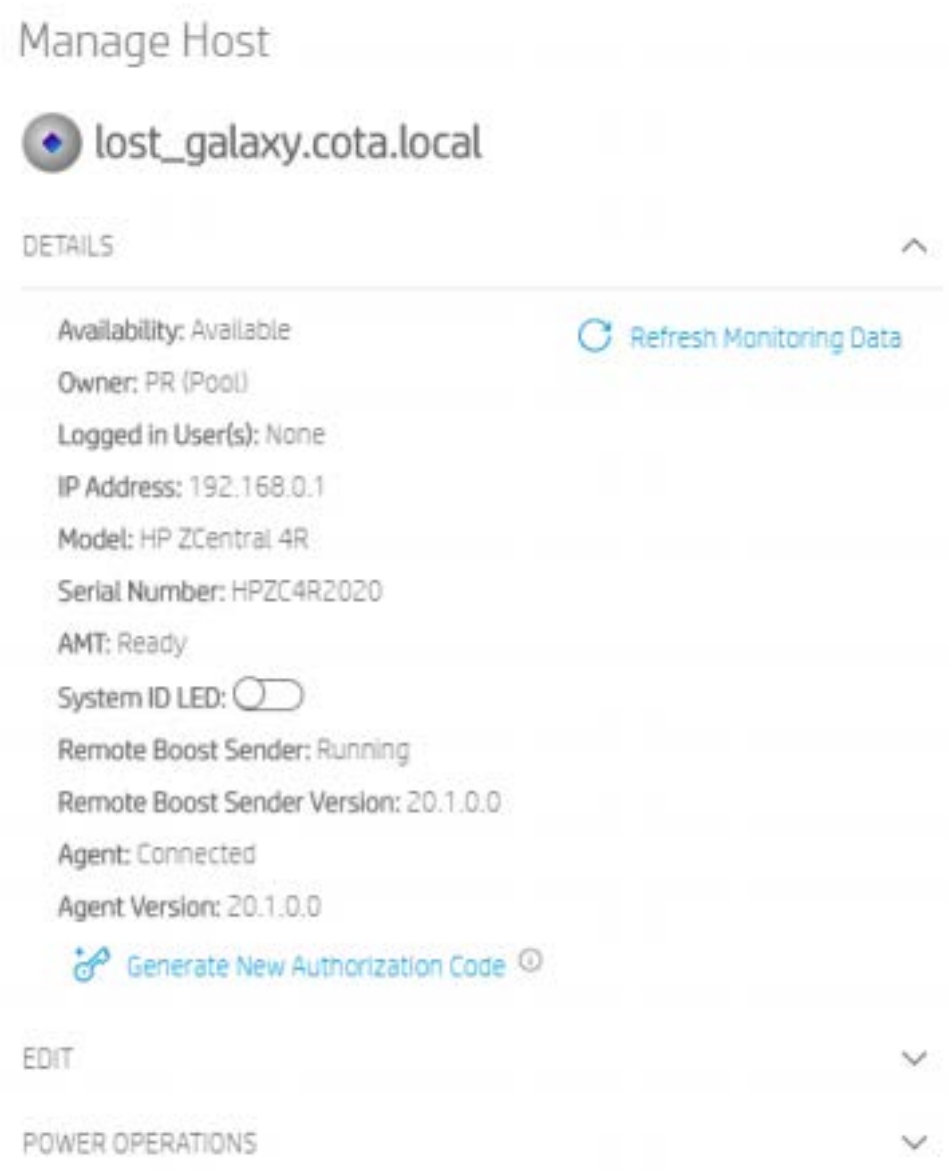
AMT デバイスとの現在の接続ステータスの追跡は、ホストの AMT 属性を使用して実行できます。次のような状態があります。

- 管理されていません：ホストに対して AMT 管理が有効になっていません。これは、ホストの管理パネルから有効にできます。
- 保留中：このホストに対して AMT 管理が有効になっており、Manager は現在の構成を使用して AMT デバイスに接続しようとしています。
- 準備完了：このホストに対して AMT 管理が有効になっており、Manager は AMT を使用してホストに正常に接続できました。
- エラー：このホストに対して AMT 管理が有効になっており、Manager は AMT デバイスへの接続に関する問題に直面しました。エラーの詳細は、そのホストの管理パネルに表示されます。各エラーの詳細については、「トラブルシューティング」ページの「AMT エラー」セクションを参照してください。

AMT ステータスが準備完了である場合、ハードウェアモデル、シリアル番号、IP アドレスなどのホスト情報はホストの管理パネルで確認でき、サポートされている場合、Manager はこのホストのシステムイベントを受信することができます。

4.1.6. ホストの管理

監視データの表示またはホストのリモート管理を行うには、表のホスト名をクリックすると、右側のパネルにホストの詳細が表示されます。

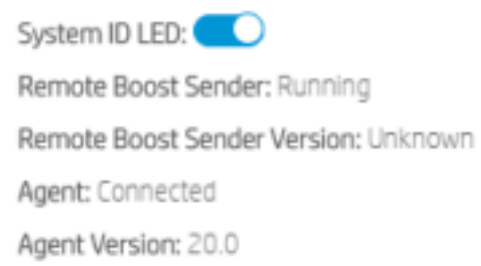


注意：AMT ステータスが管理されていませんである場合、すべての電源操作機能が無効になり、一部のハードウェア情報が使用できなくなります。

システム ID LED

システム ID LED の状態はこのパネルで表示および制御でき、ZCentral Connect Agent バージョン 20.1 以降がインストールおよび接続されており、ホストが HP ZCentral 4R Workstation である場合に限り、利用可能です。

システム ID LED は、ラック内のワークステーションを識別するために使用される光源で、潜在的なメンテナンスや一般的な識別の目的で視覚的な合図を提供します。また、Connect Administrator Portal を介して ZCentral Connect により完全に制御できるため、現在の状態（オンまたはオフ）を視覚化して、変更することができます。いずれかの基準が満たされない場合、システム ID LED の状態はなしとなり、制御機能を利用できません。

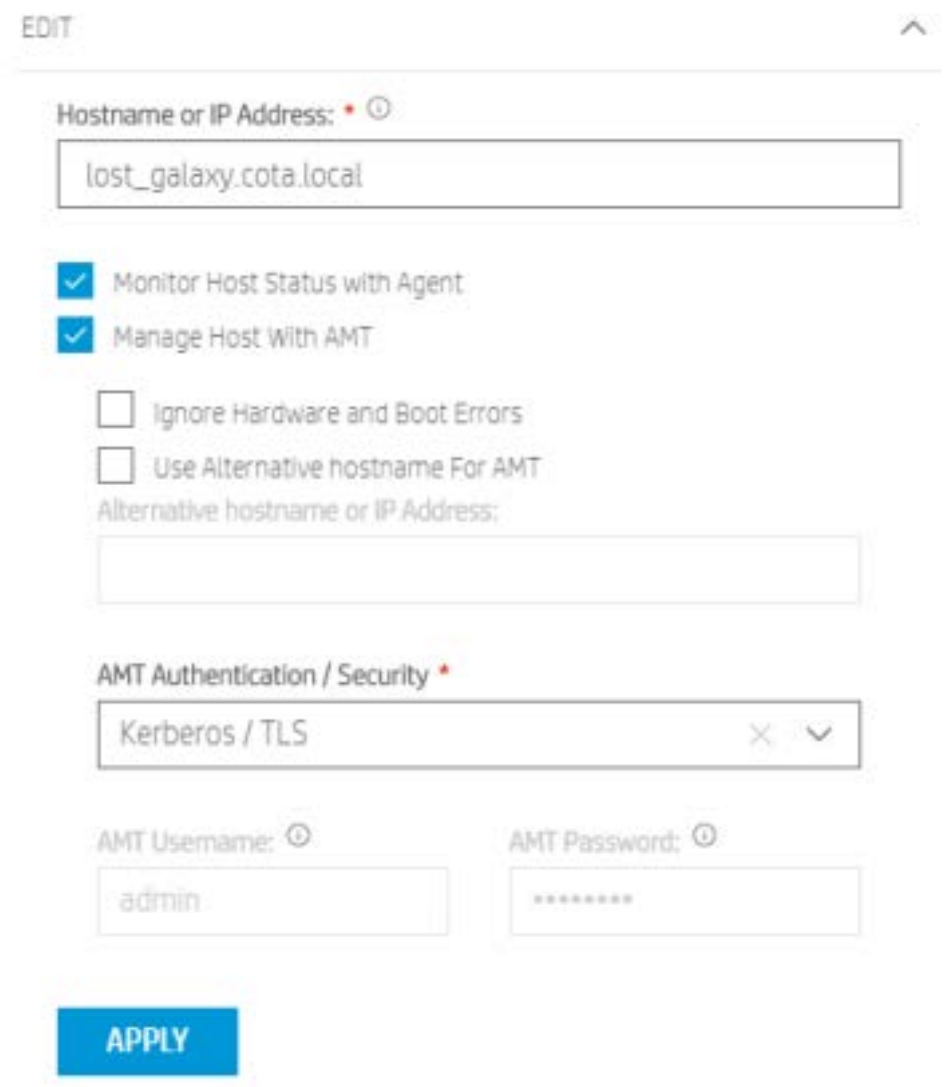


注意：ZCentral Agent のステータスが切断であるが、ホストが以前に HP ZCentral 4R Workstation モデルとして識別されている場合、システム ID LED の状態は不明となり、制御は引き続き表示されますが、Agent が再接続されるまで無効になります。

ホストの編集

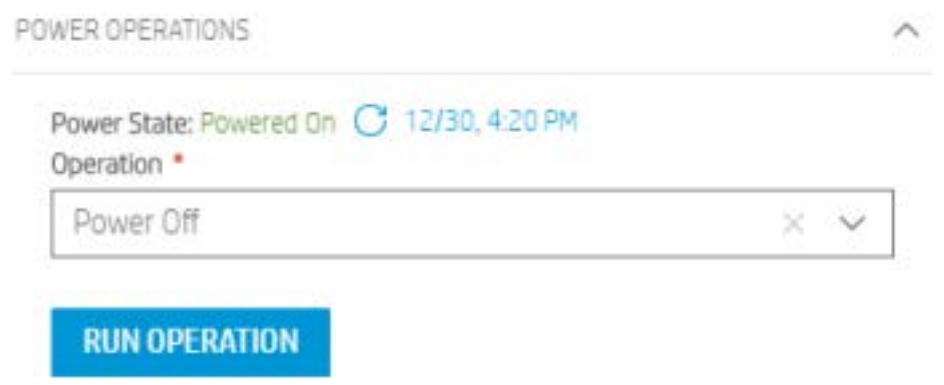
管理パネルで、[編集]ドロップダウンを開くことでホストの情報を編集できます。

ホスト名、AMT、および Agent の設定を変更できます。



電源操作

[電源操作]では、ホストの電源状態を表示し、リモートで管理できます。ホストの電源状態を変更するには、ドロップダウンメニューから操作を選択し、[操作の実行]ボタンをクリックします。電源操作が完了すると、現在の電源状態が更新されます。電源状態は、現在の状態の横にある[更新]をクリックすることで、いつでも更新できます。



利用可能なリモート電源操作は次のとおりです。

- 電源オン
- 電源オフ
- グレースフルシャットダウン
- リセット
- グレースフルリスタート

注意：グレースフルシャットダウンとグレースフルリスタートには、バージョン 9 以降の Intel® AMT が必要です。また、Intel® Management and Security Application Local Management Service をターゲットホストにインストールする必要があります。Intel® Management Engine Firmware を更新する方法については、「トラブルシューティング」ページの「Intel® Management Engine Firmware の更新」セクションを確認してください。ホストの電源をオンにするか、再起動した後に、適切な電源操作が再び利用できるようになるまでに 2〜3 分かかる場合があります。

リモート電源操作が完了すると、メッセージが表示されます。

注意：管理パネルを閉じるために、電源操作が完了するのを待つ必要はありません。

4.1.7. システムイベント

Intel® AMT バージョン 11 以降を搭載したホストの場合、ZCentral Connect Manager は、ホストからイベントを受信するために自身をサブスクライブできます。これらのイベントは、上記の「ステータス」セクションに示されるように、ホストのステータスを追加します。

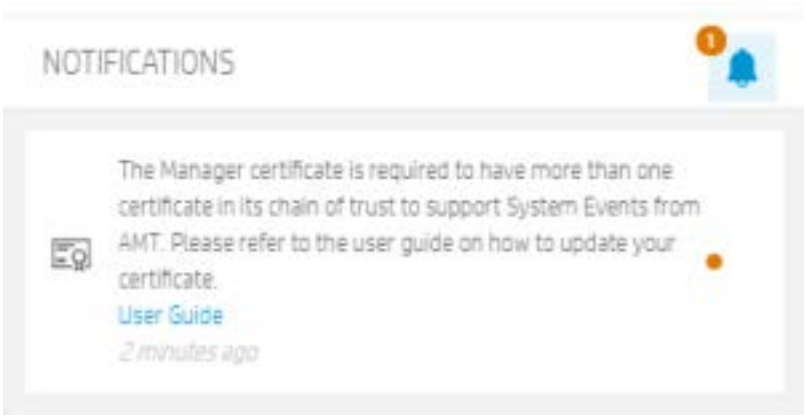
[ホストの管理]パネルでシステムイベントを無効にするには、[ハードウェアとブートエラーを無視する]オプションにチェックを入れるか、AMT によるホストの監視を無効にします。

前提条件

Manager に Intel® AMT からのシステムイベントをサブスクライブさせるには、いくつかの前提条件を満たしている必要があります。

1. システムイベントを使用できるようにするには、ホストに AMT バージョン 11 以降が必要です。
2. ホストは AMT で管理する必要があり、AMT ステータスは準備完了状態である必要があります。
3. ZCentral Connect Manager は、証明機関によって署名された証明書を使用している必要があります。HP ZCentral Connect 20.1 を新規インストールしている場合、この要件はすでに満たされています。バージョン 20.0 からアップグレードする場合は、「トラブルシューティング」ページの「バージョン 20.0 からのアップグレード」セクションを参照してください。
4. ZCentral Connect Manager が使用するホスト名は、完全修飾ドメイン名（FQDN）または IP アドレスである必要があります。証明書は、ZCentral Connect Manager が使用する FQDN または IP アドレスに発行する必要があります。

注意：自己署名証明書が使用されている場合、Administrator Portal には、システムイベントでは証明機関が署名した証明書が必要であることを知らせる通知が表示されます。



Agent にバンドルされている ZCentral Hardware Monitor は必須ではありませんが、システムイベントの全体的なエクスペリエンスを向上させます。Hardware Monitor がインストールされていると、Manager はホストのオペレーティングシステムの実行中にシステムイベントを受信できます。Hardware Monitor が存在しない場合、システムイベントはホストの起動時のみまたは定期的に受信されます。

注意：ZCentral Connect Agent パッケージには、HP Zcentral 4R Workstation に Hardware Monitor を自動的にインストールするインストールスクリプトが付属しています。

サポートされているイベント

AMT バージョン 11 以降のホスト：

システム起動エラー

1. ホスト OS が予期せずにシャットダウンしました。
   オペレーティングシステムに重大な障害がある場合に発生します。Windows システムでは、これは通常、ブルースクリーンエラーとみなされます。このエラーから回復する方法としてホストのリセットがありますが、問題が解決しない場合はさらにメンテナンスが必要になる場合があります。
2. ホストが OS の起動に失敗しました。
   POST 処理中にホストに問題がある場合、またはオペレーティングシステムをタイムリーに起動できなかった場合に発生します。このエラーから回復する方法としてホストのリセットがありますが、問題が解決しない場合はさらにメンテナンスが必要になる場合があります。

HP ZCentral 4R Workstation の場合、次のイベントも利用できます。

電源エラー

1. 冗長モードで設置された 2 つの電源装置：1 つの電源装置がオフラインです。冗長性はありません。
   ワークステーションによって、電源装置の 1 つがオフラインであることが検出されたときに発生します。この場合、電源の冗長性が損なわれます。電源に問題がある可能性があります。
2. 非冗長モードで設置された 2 つの電源装置：1 つの電源装置がオフラインです。
   システムは低電力構成になっています。ワークステーションによって、電源装置の 1 つがオフラインであることが検出されたときに発生します。この場合、電源装置の出力が低下します。電源に問題がある可能性があります。

システムイベントの同期

場合によっては、ZCentral Connect Manager がシステムイベントを見逃したり、通知を受けなかったりする可能性があります。これは、AMT デバイスと Manager 間のネットワークが使用できなくなった場合、またはイベントの発生時に Manager がオフラインである場合に発生する可能性があります。これはよく発生することではありませんが、ZCentral Connect Manager には同期メカニズムがあります。これにより、すべてのイベントが ZCentral Connect Administrator Portal によって確実に報告されます。

システムイベントの同期機能は、システムイベントをサポートするすべてのホストを反復処理し、システムの現在の状態が Manager に報告されることを確認します。デフォルトでは、システムイベントの同期は 12 時間ごとに実行され、設定 AmtHardwareEventPolling を変更することで構成できます。詳細については、「詳細設定」セクションを参照してください。

[ホストの管理]パネルの[監視データの更新]ボタンをクリックすると、特定のホストに対するシステムイベントを手動で同期できます。

サブスクリプションとトークンの更新

AMT デバイスと Manager 間の通信は、暗号化と認証によって保護されています。暗号化は、Manager が使用する TLS 証明書によって実現されます。Manager 証明書の構成の詳細については、このユーザーガイドの「証明書」セクションを参照してください。

認証は、Manager が AMT デバイス内で自身をサブスクライブして AMT アラートを受信するときに発生します。サブスクリプションプロセスは、AMT で管理され、サブスクリプションをサポートするホストが Manager に登録されると自動的に発生します。サブスクリプションは、Manager によって発行された認証トークンを介して AMT デバイスを識別し、このデバイスによって発行されたアラートを信頼できるようにします。
デフォルトでは、サブスクリプショントークンの有効期限は 1 年に設定されています。Manager は、各ホストに対して 90 日ごとにサブスクリプショントークンを更新します。Manager が使用するデフォルトの有効期限と更新期間は、AmtSubscriptionTokenExpirationTimeInDays と AmtTokenRenewInterval の設定をそれぞれ変更することにより、Manager 設定ファイルで構成できます。詳細については、「詳細設定」セクションを参照してください。

AMT デバイスが 365 日を超えて切断されると、サブスクリプショントークンの有効期限が切れ、AMT デバイスはシステムイベントを Manager に送信できなくなります。これが発生した場合は、Manager の[ホスト]ページに移動し、[ホストの管理]パネルで[ホスト]をクリックしてから[監視データの更新]ボタンをクリックして、AMT デバイスのサブスクリプションを更新する必要があります。

その他

システムイベントは、30 秒後に AMT デバイスによって送信されます。つまり、ネットワークトラフィックによっては、ZCentral Connect Manager が新しいイベントを受信するまでに 30 秒以上かかる場合があります。

詳細については、『トラブルシューティング』ガイドの「システムイベント」セクションを参照してください。

4.1.8. ホストの削除

Manager から 1 つまたは複数のホストを削除する場合は、テーブル内のチェックボックスを使用してホストを選択してから、[削除]ボタンをクリックします。
このホストがプールまたはプライベートホストの一部である場合、削除する前に、そのホストをその関連付けから削除する必要があります。
注意：セッションでアクティブに使用されているホストを削除することはできません。そのホストを削除するには、[セッション]タブからそのセッションを終了する必要があります。

4.2. プール

プールは、ホストのグループとセキュリティグループ/ユーザー間の論理的な関連付けです。プールの一部であるすべてのホストは、関連付けられたセキュリティグループのユーザーメンバー、および直接関連付けられたユーザーが利用できます。

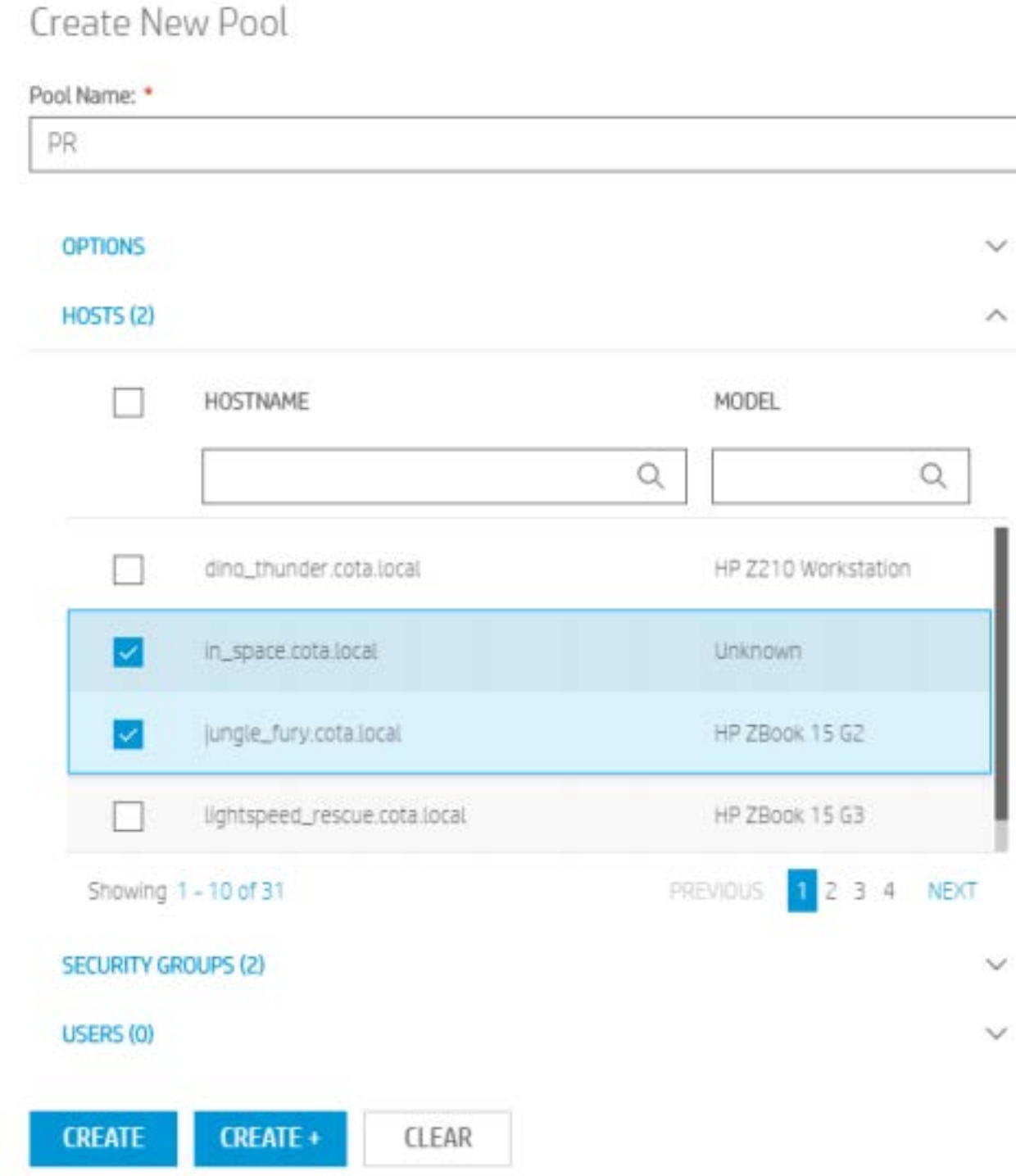
プールは作成、編集、削除することができます。

注意：ホストは、一度に 1 つのプールまたはプライベートホストの一部にしかなれません。

4.2.1. プールの作成

新しいプールを作成するには、左側のパネルの[プール]タブにアクセスして、[新しいプールの作成]をクリックします。

ダイアログでプールに名前を割り当て、プールに含めるホストを選択し、プールに割り当てるセキュリティグループおよび/またはユーザーを選択します。それぞれ数の制限なく選択できます。



[作成]ボタンをクリックすると、プールが作成されます。直接関連付けられているすべてのユーザーと、プールに関連付けられているセキュリティグループのユーザーは、そのプール内のホストとのセッションを作成できます。

注意：Manager は、使用頻度が最も低い優先順位に従って、適格なユーザーにホストを割り当てます。ユーザーが前のセッションから同じホストを受け取ることは保証されていません。

4.3. プライベートホスト

プライベートホストは、単一のホストと単一のユーザー間の論理的な関連付けです。

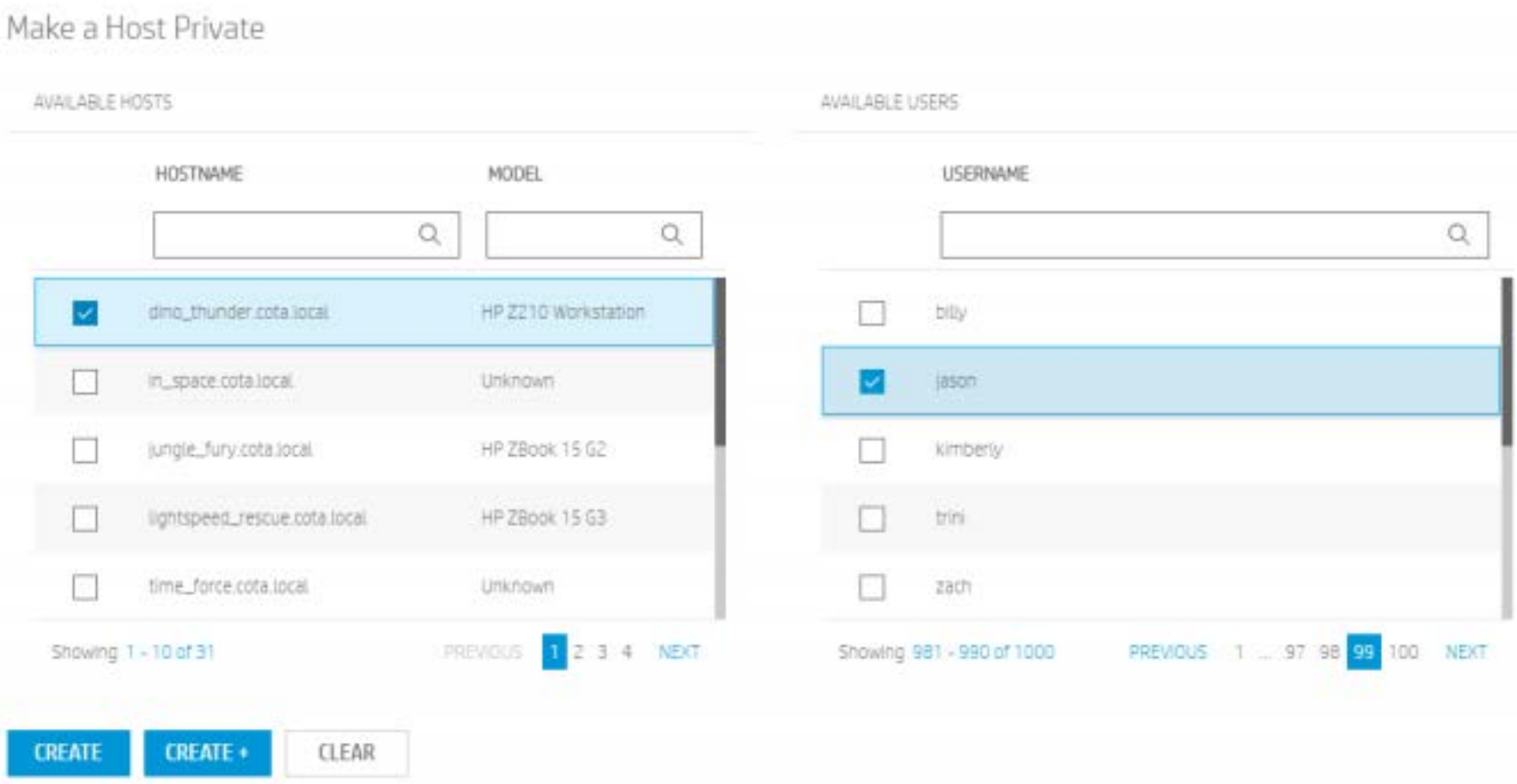
プライベートホストの関連付けは、作成および削除のみが可能です。

4.3.1. プライベートホストの関連付けの作成

新しいプライベートホストの関連付けを作成するには、左側のパネルの[プライベートホスト]タブを開いて[ホストをプライベートにする]をクリックします。

1 つのホストと 1 つのユーザーのみ選択する必要があります。

注意：プールまたは別のプライベートホストの関連付けの一部であるホストは、新しいプライベートホストの関連付けでは使用できません。



[作成]ボタンをクリックすると、ホストはプライベートとみなされます。関連付けられたユーザーのみが、そのホストとのセッションを作成できます。

4.4. セキュリティグループ

Active Directory には、ユーザーアカウントとコンピューターアカウントという 2 つの形式の一般的なセキュリティプリンシパルがあります。これらのアカウントは物理エンティティ（人またはコンピューター）を表します。一部のアプリケーションでは、ユーザーアカウントを専用のサービスアカウントとして使用することもできます。セキュリティグループは、これらのユーザーアカウント、コンピューターアカウント、およびその他のグループを管理可能な単位にまとめるために使用されます。

4.4.1. セキュリティグループのインポート

新しいセキュリティグループをインポートするには、左側のパネルの[セキュリティグループ]タブを開いて[グループのインポート]をクリックします。

新しいウィンドウで、検索ボックスにターゲットのセキュリティグループ名の最初の文字を入力して、「名前」で Microsoft Active Directory を検索します。

[検索アイコン]をクリックすると、Manager は Active Directory に対してクエリを実行し、検索結果を次の表に表示します。

必要な数のセキュリティグループを選択し、[インポート]ボタンをクリックします。

注意：現時点で Manager では、あるホストまたはユーザーがどのセキュリティグループに属しているか、またはあるセキュリティグループにどのユーザーおよびホストが属しているかを表示する方法は提供されていません。管理者は、この情報を表示するために、この製品の外部にある Active Directory ツールを使用する必要があります。

4.5. ユーザー

ユーザーは、ZCentral Connect Client User の論理的な表現です。ユーザーは Active Directory からインポートし、必要に応じて後で Manager から削除できます。

4.5.1. ユーザーのインポート

新しいユーザーをインポートするには、左側のパネルの[ユーザー]タブを開いて[ユーザーのインポート]をクリックします。

新しいウィンドウで、次の方法により Microsoft Active Directory を検索します。

- 名前：Active Directory 内のユーザーの名前
- ユーザー名：Active Directory 内のユーザーのユーザー名
- 電子メール：Active Directory 内のユーザーの電子メール
- メンバー*：グループの一員であるすべてのユーザーを検索します

注意：「メンバー」の検索では、Active Directory にセキュリティグループの正確な名前を入力する必要があります。

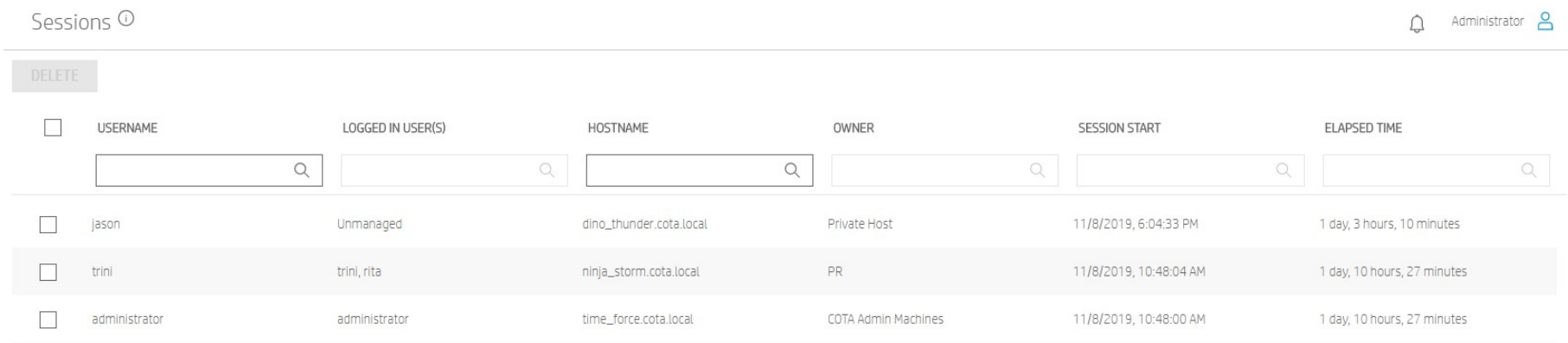
[検索アイコン]をクリックすると、Manager は Active Directory に対してクエリを実行し、検索結果を次の表に表示します。

必要な数のユーザーを選択し、[インポート]ボタンをクリックします。

注意：現時点で ZCentral Connect では、あるユーザーがどのセキュリティグループに属しているか、またはあるセキュリティグループにどのユーザーが属しているかを表示する方法は提供されていません。管理者は、この情報を表示するために、この製品の外部にある Active Directory ツールを使用する必要があります。

4.6. セッション

セッションは、ユーザーとホスト間の Remote Boost 接続の論理的な表現です。既存のセッションは、[セッション]パネルに表示されます。



管理者は、各ユーザーが使用しているホストを監視し、アクティブなセッションを強制的に終了できます。アクティブなセッションを削除すると、ホストは「使用可能」の状態に戻ります。ただし、Remote Boost 接続がすぐに停止することはありません。

4.7. 証明書

Manager は、秘密鍵基盤（PKI）を使用する Transport Layer Security（TLS）との通信を保護します。証明書は、TLS 暗号化接続をセットアップするために使用されます。また証明書は、ZCentral Connect Manager により、接続しているエンティティに認証を提供するためにも使用されます。これには、Manager への登録または接続を試みる ZCentral Connect Agent が含まれます。Agent が Manager から提供された証明書を信頼しない場合、Agent は正常に接続できません。

エンタープライズ証明機関（CA）によって発行された証明書は、ドメインに参加しているホスト上で実行されているすべての Agent によって信頼されます（正しいグループポリシー設定が使用されていることが条件です）。このため、エンタープライズが発行した証明書に対して必要な管理ははるかに少なくなります。エンタープライズ CA によって新しい証明書が Manager に発行されると、ドメイン内のすべての Agent とエンドユーザーブラウザーは、新しい証明書を信頼します。追加手順は不要です。

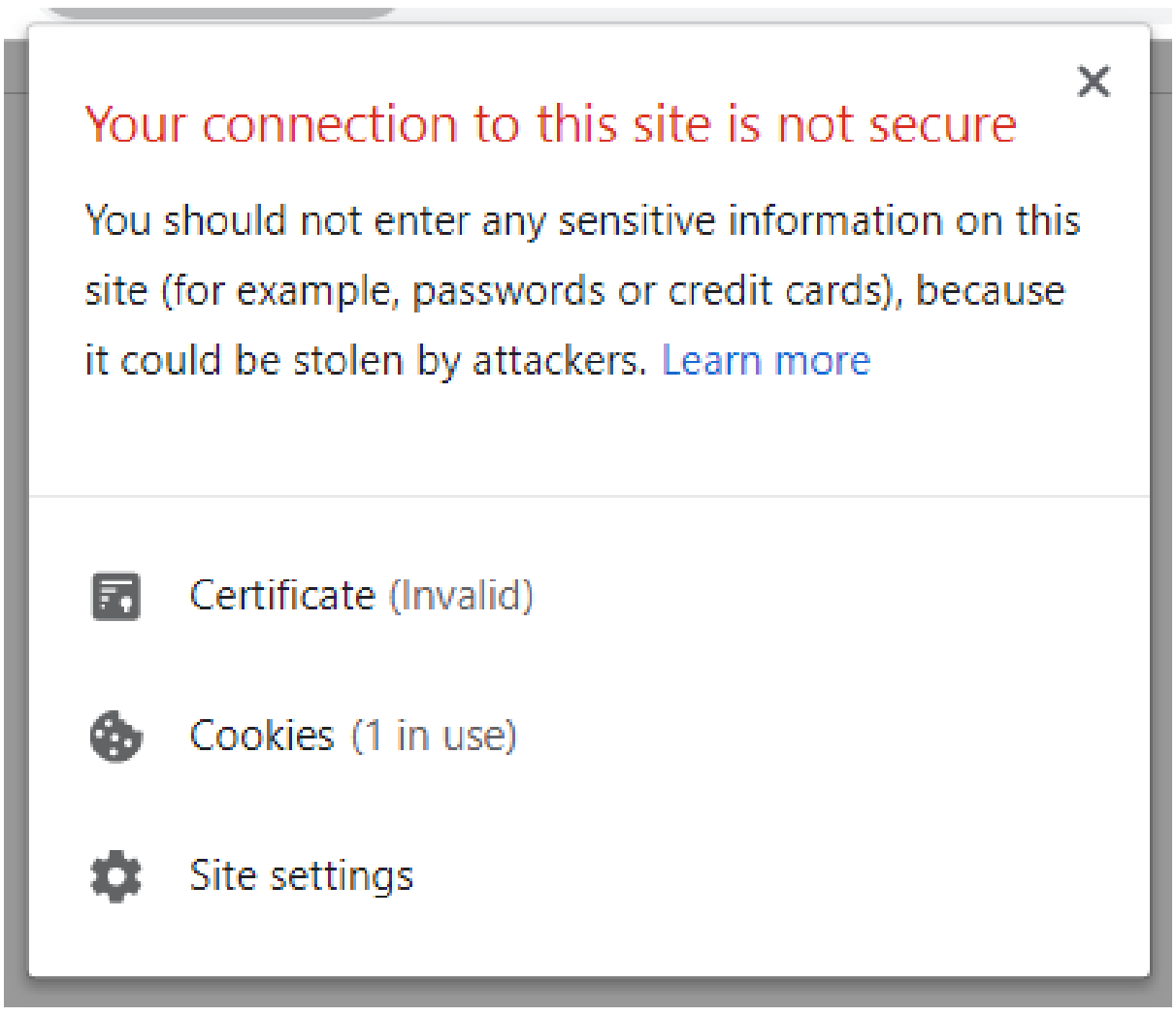
インストール時から暗号化された通信を確保するために、Manager のインストーラーは、最初に起動したときに Manager が使用する自己署名 CA によって署名された証明書を作成します。**証明書の有効期限は、Manager のインストール日から 1 年後です。**これらの証明書は、ドメインでは自動的に信頼されません。インストール中に作成される自己署名 CA は、エンタープライズが発行した証明書と同じレベルの認証を提供するために、ドメイン内のホストによって信頼される必要があります。セキュリティと管理性の理由から、HP ではエンタープライズ発行の証明書を可及的速やかに使用することをお勧めします。詳細については、**「独自の証明書の使用」**セクションを参照してください。インストールによって作成された証明書を使用することが唯一の選択肢であり、有効期限が迫っている場合は、更新の手順に関する**「新しい HP ZCentral Connect Manager 証明書の更新または構成」**セクションを参照してください。

自己署名証明書（または自動的に信頼されない証明書）を使用する場合、Agent インストーラーはユーザーにその証明書を受け入れることを求めます。これが行われると、ホストが信頼していない場合でも、Agent がその証明書を信頼するようになります。**Manager が証明書を変更した場合、Agent は新しい証明書も信頼する必要があります。エンタープライズが発行した証明書を使用する場合、これはドメイン内のホストによって自動的に信頼され、追加の手順は必要ありません。**新しい証明書が別の自己署名証明書またはその他の信頼できない証明書である場合は、追加の管理手順が必要です。詳細については、**「Agent に新しい Manager 証明書を信頼させる」**セクションを参照してください。

- Manager は、システム証明書ストア（デフォルトではローカルマシンの個人ストア）を使用して、証明書を保存し、これにアクセスします。

4.7.1. 使用環境における自己署名証明機関の承認

インストール中に作成された自己署名証明機関を承認することにより、クライアントブラウザーは警告を表示せずに Manager 証明書を信頼します。以下は、例として Google Chrome を使用して作成されました。他のブラウザーは、類似の証明書へのアクセス方法を提供します。



1. URL バーにホスト名または IP アドレスを入力して、HP ZCentral Connect サービスにアクセスします。
2. URL の[セキュリティで保護されていない]領域をクリックして、[証明書]をクリックします。
3. [証明書パス]タブにアクセスし、[HP ZCentral Connect CA]をクリックしてから、[証明書の表示]をクリックします。
4. [詳細]タブにアクセスし、[ファイルへコピー...]をクリックします。
5. 証明書のエクスポートウィザードに従って、HP ZCentral Connect の証明書をファイルに保存します。デフォルトのエクスポート設定を使用します。
6. Chrome の設定にアクセスします。
7. [詳細設定]をクリックします。
8. [プライバシーとセキュリティ]で、[証明書の管理]をクリックします。
9. [信頼されたルート証明機関]タブをクリックします。
10. [インポート]をクリックします。
11. エクスポートした証明書を選択し、ウィザードに従ってインポートを完了します。
12. ページを更新します。

4.7.2. Agent に新しい Manager 証明書を信頼させる

Manager Config App を使用して、Manager が使用する証明書を生成または構成する場合、接続されているすべての Agent は、新しい証明書を信頼するために更新されます。このプロセスについては、「新しい HP ZCentral Connect Manager 証明書の更新または構成」セクションで説明されています。更新または構成プロセス中に Agent を更新できなかった場合、または証明書が手動で変更された場合は、Agent を手動で構成する必要があります。

1. 新しい証明書の拇印を収集します（手順については、「証明書の拇印を見つける」セクションを参照してください）
2. Agent ホストにアクセスします
3. Agent サービスを停止します
4. AgentConfig アプリケーションを実行して、ManagerCertificateThumbprint 設定を新しい証明書の拇印に設定します
    - 例：AgentConfig.exe set --ManagerCertificateThumbprint XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
5. Agent サービスを再起動します

注意：このプロセスは、スクリプトを使用して自動化できます。詳細については、『Agent 展開ガイド』の「スクリプトの例」セクションを参照してください。

4.7.3. 独自の証明書の使用

ZCentral Connect Manager で他の証明書を使用するには、Manager を実行しているアカウントで読み取り可能で、エクスポート可能なキーが必要です。証明書はローカルマシンの個人ストアに配置されます（デフォルト）。Manager が TLS 通信の証明書を使用するには、次の手順を実行する必要があります。

1. Manager が正しくインストールされており、ブラウザーからアクセスできることを確認します。
2. Manager 用に選択したホスト名を使用して証明書を生成します。
    - たとえば、URLhttps://zcentralconnectdemo.domain.local を介して Manager にアクセスできる場合、証明書の生成に使用する必要があるホスト名は、「zcentralconnect.domain.local」 です。
    - エンタープライズ環境では、コンピューター証明書テンプレートを使用できます。
3. 互換性を高めるために、RSA 形式を使用して証明書の秘密鍵を生成してください。
4. エクスポート可能な秘密鍵を含む証明書を LocalMachine の個人証明書ストアに配置します
    - これは、ファイルから証明書をインポートするか、エンタープライズ環境に証明書を登録することで実行できます。
    - 登録を使用する場合、秘密鍵を証明書テンプレートでエクスポートできるように設定できます。それ以外の場合は、リクエストの一部として設定を変更する必要があります。
    - たとえば、certlm.msc を使用して新しい証明書を要求する場合は、次の手順に従います。
        1. [詳細]を展開し、[プロパティ]をクリックします
        2. [秘密鍵]タブに移動し、[鍵オプション]を展開します
        3. [秘密鍵をエクスポート可能にする]の横にあるチェックボックスをオンにします
5. Manager Config App を実行して、その証明書を使用するように Manager を構成します。
    - --configure コマンドを使用して ManagerConfig.exe を実行し、証明書の拇印と Manager の実行に使用されるサービスアカウントを渡します。
    - 例：ManagerConfig.exe certificate --configure --serviceAccount domain\zcentralconnectmsa$ -- certificateThumbprint XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

注意：使用されるストアは、Manager を実行しているサービスアカウントによって秘密鍵がエクスポート可能かつ読み取り可能である限り、変更することができます（詳細については、「詳細設定」セクションを参照してください）。

ファイルからの証明書のインポート

1. 証明書ファイル（.pfx または.p12）をダブルクリックし、[証明書のインストール]をクリックします。
2. ローカルマシンを選択します
3. 必要に応じてパスワードを入力します
4. [このキーをエクスポート可能としてマークする]の横のチェックボックスがオンになっていることを確認します
5. [すべての拡張プロパティを含める]の横のチェックボックスがオンになっていることを確認します

6. 次のウィンドウで、[すべての証明書を次のストアに配置する]を選択し、証明書のインポートのターゲット場所として[個人]を指定します
7. ウィザードを終了します

証明書の拇印を見つける

1. Windows タスクバーの Windows ボタンを右クリックして、[ファイル名を指定して実行]を選択します。
2. 「certlm.msc」と入力します
3. 左側のパネルで、[個人]>[証明書]を展開します
4. 右側のパネルで、[発行先]列と[発行者]列を使用して、インポートしたばかりの証明書を探します。HP ZCentral Connect の展開時に使用されたホスト名と一致する証明書を見つけます
5. 証明書をダブルクリックして、[詳細]タブを開きます。[拇印]の値まで下にスクロールします

手動構成

Manager Config App が、証明書を使用できるように Manager を構成する際に実行するのと同じ手順のほとんどは、必要に応じて次の手順に従って手動で実行できます。

1. Manager サービスを実行しているアカウントに秘密鍵の読み取りアクセス許可を付与します
    1. ローカルマシン証明書を管理するための MMC スナップインを開きます（certlm.msc を実行します）
    2. Manager で TLS 用の証明書を右クリックします（[個人]->[証明書]の下）
    3. [すべてのタスク]->[秘密鍵の管理]をクリックします
    4. サービスアカウントをユーザーのリストに追加し、読み取りアクセス許可を付与します
2. Manager が使用するポートに証明書をバインドします
    - これは、netsh コマンドを使用して実行できます（こちらを参照してください）
3. Manager の settings.json ファイルを更新します
    1. %PROGRAMDATA%\HP\ZCentralConnectManager でファイル settings.json を開き、CertificateThumbprint の値を証明書の拇印に置き換えます

注意：証明書を手動で構成するには、エンタープライズ証明書が使用されていないすべての Agent に対する信頼できる証明書を手動で更新する必要があります。すべての AMT アラートサブスクリプションの更新も、各ホストを手動で更新して実行する必要があります。

4.7.4. 証明機関の信頼

マシンが証明書を信頼する場合、このルート証明書によって発行される証明書も信頼されます。HP ZCentral Connect Manager が使用する証明書が、ZCentral Connect Agent または Client がインストールされているホストが信頼する証明機関によって発行された場合、Manager 証明書も信頼されます。証明機関を使用して組織内で証明書を発行する場合、ルート証明書は組織全体で信頼できます。多くの場合、これは Active Directory 証明機関（AD CA）を使用して実行されます。デフォルトでは、AD CA を使用すると、Windows OS を使用してドメインに参加しているすべてのマシンで、ドメイン CA のルート証明書が自動的に信頼されます。ルート証明書は Windows 証明書ストアに配置されます。

Linux では、AD はルート証明書を Linux のトラストストアに自動的に追加しませんが、グループポリシーを使用して信頼を追加できます。Linux でルート証明書の信頼を追加するには、手動またはスクリプトを使用して次の手順で実行できます。

Ubuntu

1. PEM 形式の.crt 証明書ファイルを/etc/pki/ca-trust/source/anchors/にコピーします
2. sudo update-ca-trust enable を実行します
3. update-ca-trust extract を実行します
4. update-ca-trust を実行します

RHEL

1. PEM 形式の.crt 証明書ファイルを/usr/local/share/ca-certificates/にコピーします
2. sudo update-ca-certificates を実行します

4.8. HP ZCentral Connect Manager Config App（ManagerConfig.exe）

HP ZCentral Connect には、管理者 UI の外部でいくつかの操作を実行するためのツールが付属しています。

このツールは ManagerConfig.exe と呼ばれ、通常、HP ZCentral Connect Manager のインストール先と同じフォルダー内にあります。
%PROGRAMFILES%\HP\ZCentralConnectManager\bin

4.8.1. HP ZCentral Connect 管理者パスワードの復元

管理者パスワードは、HP ZCentral Connect のインストール時に定義されます。管理者パスワードを紛失した場合は、付属の HP ZCentral Connect Config App を使用して復元できます。

1. 管理者コマンドプロンプトを開き、HP ZCentral Connect Manager がインストールされているフォルダーに移動します（通常は %PROGRAMFILES%\HP\ZCentralConnectManager\bin）。

2. コマンドプロンプトで、次のコマンドを入力し、Enter キーを押します。
   ManagerConfig.exe password --recover
3. 新しい管理者パスワードを入力し、Enter キーを押します。
4. 新しい管理者パスワードを確認し、Enter キーを押します。
5. 新しいパスワードを使用して HP ZCentral Connect にログインします。

注意：HP ZCentral Connect Config App を実行するには、コンピューターの管理者権限を必要とします。

注意：入力された新しいパスワードの文字列は、セキュリティ上の理由からコンソールに表示されません。

注意：管理者パスワードの復元後も、既存の管理者セッションは終了しません。パスワードの変更を有効にするには、新しい資格情報を使用して再度ログインする必要があります。

4.8.2. 新しい HP ZCentral Connect Manager 証明書の更新または構成

ZCentral Connect Manager が使用する証明書を更新または変更する場合は、ManagerConfig App を使用する必要があります。更新すると、Manager がすでに使用している証明機関（CA）によって署名された新しい証明書が生成されます。構成は、エンタープライズ CA によって発行された証明書、またはサードパーティベンダーから購入した証明書がすでに存在する場合に使用します。いずれの場合も、Manager サービスが実行されており、Administrator Portal にローカルでアクセスできる必要があります。

Config App は、Manager 証明書の更新と構成の両方に対して実行される証明書更新プロセスを開始します。

このプロセスは、切断された Agent、または古い Agent を確認することから始まり、これらが見つかった場合は警告が発せられます。プロセスが続行される場合、Config App は新しい証明書を Manager に通知し、接続されているすべての Agent に新しい証明書情報を提供するようサーバーに指示します。各 Agent はこの情報を保存して、新しい証明書が使用されると Manager に接続できるようにします。このプロセス中に Agent に接触できなかった場合、ユーザーは続行する前に再度警告を受けます。さらにこのプロセスでは、すべての AMT デバイスから古い証明書をクリーンアップするために、すべての AMT アラートサブスクリプションが削除されます。

証明書の更新プロセスが完了すると、新しい証明書が Manager によって使用されるように構成され、サービスが再開します。

注意：自動証明書更新プロセスでは、Manager と Agent の両方がバージョン 20.1 以降を実行している必要があります。

警告：Manager が使用する証明書を更新すると、すべての Agent とユーザーが新しい証明書または新しい証明機関（CA）を信頼するようになります。新しい証明書または CA がクライアントマシンによって信頼されていない場合、ブラウザーは安全でない接続の警告を表示します。また、すべての AMT デバイスから古い証明書をクリーンアップするために、すべての AMT アラートサブスクリプションが削除されます。サブスクリプションは、デフォルトで 12 時間後に自動的に更新されます（設定 AmtHardwareEventPolling を変更することで構成可能です。詳細については、「詳細設定」セクションを参照してください）。または、Manager の[ホスト]ページに移動し、[ホスト]をクリックしてから、[ホストの管理]パネルの[監視データの更新]ボタンをクリックして、手動で更新することができます。

既存の証明書の更新

注意：ZCentral Connect 20.0 のインストールで以前に作成された証明書を更新する場合は、「トラブルシューティング」ページの「20.0 の自己署名証明書の更新」セクションの手順を参照してください。

更新するには、Manager を実行しているコンピューターの証明書ストアに証明機関（CA）をインポートする必要があり、Manager を実行しているアカウントは CA 秘密鍵にアクセスできる必要があります。Manager のインストール中に作成された証明書を使用する場合、これはデフォルトで実行されます。カスタム証明書が使用されている場合は、「別の証明書の構成」セクションを参照してください。

以下の手順に従って、Config App を使用して Manager 証明書を更新します。

1. 管理者コマンドプロンプトを開き、HP ZCentral Connect Manager がインストールされているフォルダーに移動します（通常は %PROGRAMFILES%\HP\ZCentralConnectManager\bin）。
2. Manager が現在使用している CA によって署名された証明書を更新するには、コマンドプロンプトで次のコマンドを入力し、Enter キーを押します。
   ManagerConfig.exe certificate --renew --serviceAccount <Account used to run the Manager service>
3. 関連する証明書に関する情報がコンソールに表示されます。
4. 証明書の更新プロセスが実行され、コンソールに警告が表示されます。プロンプトが表示されたら、「yes」と入力して手順を続行します。

注意：--quiet をコマンドに追加すると、コンソール上で求められる確認をバイパスできます。

注意：--offline をコマンドに追加すると、自動証明書更新プロセスを回避できます。この使用は、Manager が実行されていないときに限られます。

注意：--serviceAccount は、新しい証明書の秘密鍵への正しいアクセスを許可するために必要です。インストール時に指定したものと同じアカウントを使用します。

別の証明書の構成

独自の証明書の構成についてサポートが必要な場合は、「独自の証明書の使用」セクションに記載されている手順に従ってください。マシンが証明機関をどのように信頼するかについて詳細を確認したい場合は、「証明機関の信頼」セクションを参照してください。

以下の手順に従って、Config App を使用して別の Manager 証明書を構成します。

1. 管理者コマンドプロンプトを開き、HP ZCentral Connect Manager がインストールされているフォルダーに移動します（通常は %PROGRAMFILES%\HP\ZCentralConnectManager\bin）。
2. 別の証明書を使用するように Manager を構成するには、コマンドプロンプトで次のコマンドを入力し、Enter キーを押します。
   ManagerConfig.exe certificate --configure --certificateThumbprint <The thumbprint of the certificate to use> -- serviceAccount <Account used to run the Manager service>
3. 関連する証明書に関する情報がコンソールに表示されます。
4. 証明書の更新プロセスが実行され、コンソールに警告が表示されます。プロンプトが表示されたら、「yes」と入力して手順を続行します。

注意：--quiet をコマンドに追加すると、コンソール上で求められる確認をバイパスできます。

注意：--serviceAccount は、新しい証明書の秘密鍵への正しいアクセスを許可するために必要です。インストール時に指定したものと同じアカウントを使用します。

5. 高度な管理者機能

管理者による手動の介入を少なくしてホストを維持するために役立ついくつかの高度な機能が提供されています。

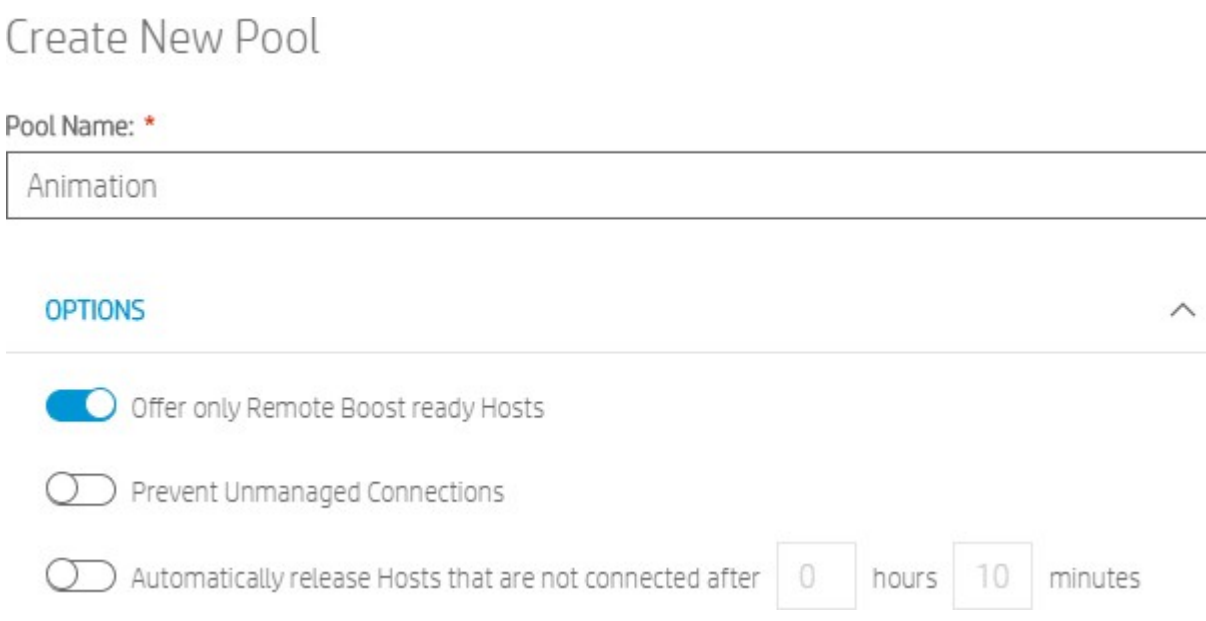
5.1. Remote Boost 対応ホストのみを提供

プールごとに Remote Boost 対応ホストのみを提供することができます。これにより、このプールにアクセスできるユーザーに次の基準を満たすホストのみが提供されるようになります。

- Agent が接続されており、Manager に報告している
- ログインしているユーザーがいない
- Remote Boost Sender サービスが実行されている

この機能を有効にするには、サイドメニューからプールのコンテンツにアクセスし、新しいプールを作成するか、既存のプールを編集します。

プールダイアログの[オプション]で、[Remote Boost 対応ホストのみを提供]のトグルをクリックします。



その他

管理者が既存のプールで[Remote Boost 対応ホストのみを提供]オプションを切り替えた場合、そのプールから作成された既存のセッションは影響を受けません。これは、このプールからすでにセッションに参加しているホストが、上記の基準を満たしていない可能性があることを意味します。これらのホストがリリースされてプールに戻ると、新しいオプションが適用されます。

5.2. 管理されていない接続を防ぐ

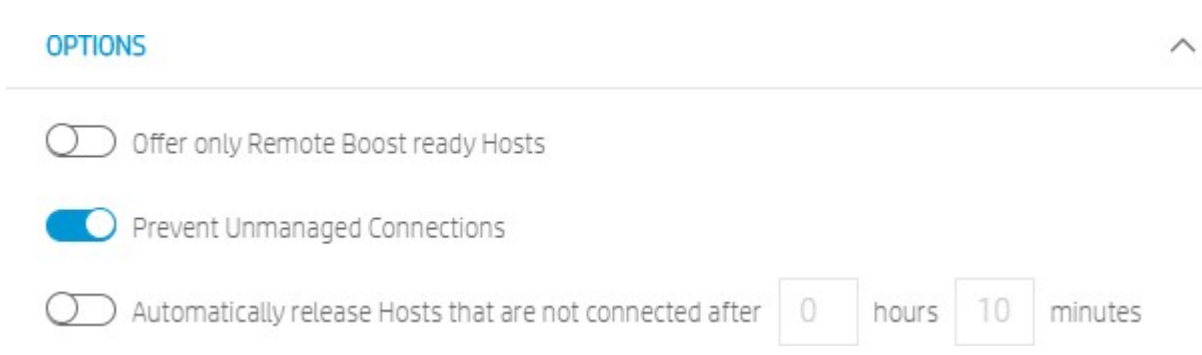
ZCentral Connect は、プールとプライベートホストに対する[管理されていない接続を防ぐ]オプションを有効にすることで、ホストへのユーザーアクセスを制限できます。この機能は、HP ZCentral Remote Boost バージョン 20.1 以降で利用可能なユーザーフィルタリング機能をベースとしています。

このオプションを有効にすると、Manager は、Remote Boost 経由で接続できるユーザー名を決定するようにホストを構成します。

この機能を適切に有効にするには、ホストで次の要件が満たされている必要があります。

- ZCentral Remote Boost Sender バージョン 20.1 以降がインストールされていること。
- ZCentral Connect Agent バージョン 20.1 以降がインストールされていること。

この機能は、既存のプールまたはプライベートホストを作成または編集することで有効にできます。ダイアログの[オプション]で、[管理されていない接続を防ぐ]オプションをオンにします。管理者は、設定ファイルのプロパティ UsersAlwaysAllowedToLogin を使用して、常にホストへの接続を許可されるユーザーのリストを設定することもできます（詳細については、「詳細設定」セクションを参照してください）。この設定は、この機能が有効になっているすべてのプールに適用されます。



注意：[管理されていない接続を防ぐ]が有効になっている状態でホストがプールまたはプライベートホストの関連付けに割り当てられ、ホストを監視している Agent がタイミングを問わず切断されると、Manager はそのホストの Remote Boost 構成を更新できなくなり、許可されたユーザー名リストは Agent が再接続するまで変更されません。

接続を許可されたユーザー

接続を許可されるユーザーは、Manager によって定義されます。Manager は、これらのユーザーのユーザー名が Remote Boost に接続することを許可します。
ZCentral Connect の[管理されていない接続を防ぐ]オプションで使用可能なすべての構成リストを以下に挙げます。

[管理されていない接続を防ぐ]が無効になっているか、または関連付けにまったく割り当てられていない場合にプールまたはプライベートホストの関連付けに割り当てられたホスト

- 誰でも接続を許可されます。

[管理されていない接続を防ぐ]が有効になっており、かつアクティブなセッションがない場合にプールまたはプライベートホストの関連付けに割り当てられたホスト

- Manager 設定の UsersAlwaysAllowedToLogin プロパティに含まれているユーザー名を持つユーザーは接続を許可されます。

注意：他のいかなるユーザーも、ホストとのセッションを作成するまでは、Remote Boost を介してこのホストに接続することはできません。

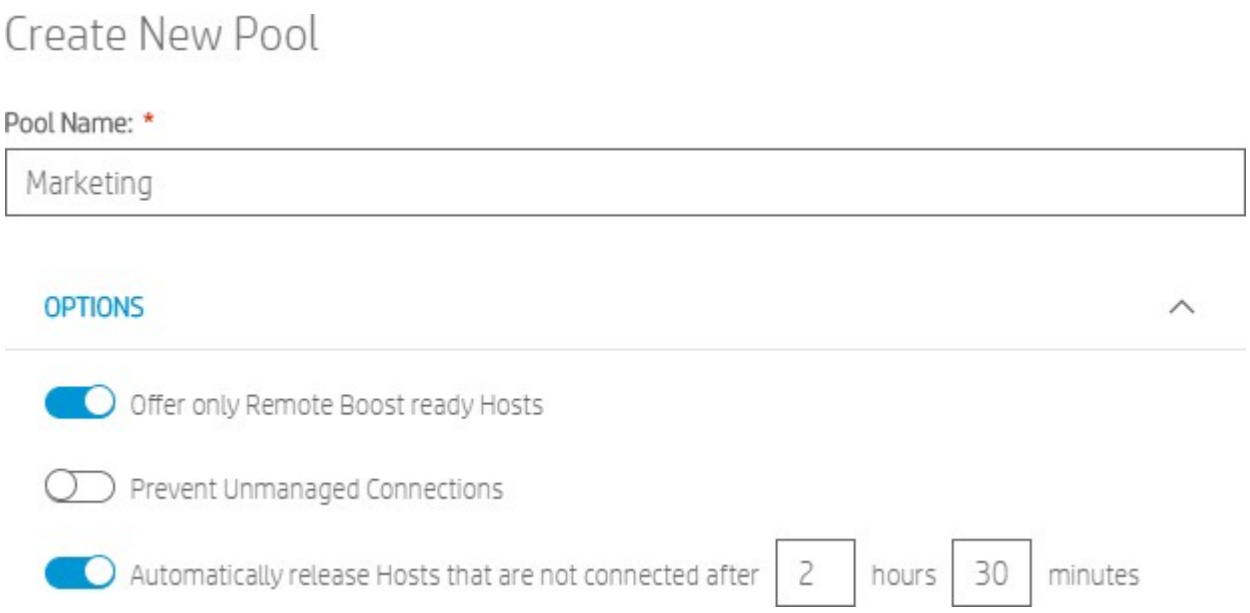
[管理されていない接続を防ぐ]が有効になっており、かつアクティブなセッションがある場合にプールまたはプライベートホストの関連付けに割り当てられたホスト

- Manager 設定の UsersAlwaysAllowedToLogin プロパティに含まれているユーザー名を持つユーザーは接続を許可されます。
- ホストへのアクティブなセッションを持つユーザーは、ユーザー名が承認され、接続を許可されます。

注意：[管理されていない接続を防ぐ]プールオプションを無効にすると、このプール内のホストに接続するためのアクセス許可が全ユーザーに返されます。

5.3. ホストを自動的にリリース

プールごとにタイムアウト期間を設定して、特定の条件下でホストを自動的にリリースすることができます。ホストは、チェックアウトされているが、ログインしたことがないか、一定期間ログアウトしている場合は自動的にリリースできます。
この機能を有効にするには、サイドメニューからプールのコンテンツにアクセスし、新しいプールを作成するか、既存のプールを編集します。
プールダイアログの[オプション]で、[接続されていないホストを自動的にリリース]のトグルをクリックします。



タイムアウト期間はデフォルトで 10 分に設定されていますが、自動リリースオプションがオンになっている場合は、1 分から 99 時間 59 分までの範囲で選択できます。
注意：ユーザーがログインしている場合、Manager はそのホストをプールにリリースバックしません。自動リリースは、ユーザーがセッションを有しているが、ホストでログインしていない場合にのみ有効になります。

その他

管理者が既存のプールの自動リリース構成を変更した場合、新しい自動リリース値は既存のセッションに適用されません。これに対する唯一の例外は、Manager が再起動した場合です。この場合、Manager がオンラインに戻ったときに、更新されたプール構成オプションが既存のすべてのセッションに適用されます。Manager が再起動すると、最初の Agent ステータス更新メッセージが各ホストに送信されるまで、自動リリースタイマーは開始しません。最初の Agent ステータス更新時にログインしていないホストはログインしていないとみなされ、タイマーは「残りの」タイマー値ではなく、完全なタイマー値で再スタートします。自動リリースが有効になっている状態でプールにホストが割り当てられ、ホストを監視している Agent がタイミングを問わず切断されると、Manager はタイマーの実行を停止し、自動リリースのタイムアウトのためホストとのセッションを閉じることはありません。切断された Agent は、ホストの現在の状態について Manager に正確に報告することができません。Agent が Manager に再接続すると、自動リリースタイマーは完全な値で再スタートします。
自動リリースタイマーは、Agent が接続されており、ホストにログインしているユーザーがいないときにのみ実行されます。したがって、自動リリースを有効にするためにプールを構成する場合は、[Remote Boost 対応ホストのみを提供]機能もオンにすることをお勧めします。この補完機能の詳細については、「Remote Boost 対応ホストのみを提供」セクションを参照してください。
通常、Agent トークンを更新しても、自動リリース機能を妨げることはありません。ただし、トークンの更新中に自動リリースタイマーが失効した場合、セッションは閉じられず、Agent の再接続時にタイマーは完全な値で再スタートします。

6. HP ZCentral Connect Agent

HP ZCentral Connect Agent は、ZCentral ソフトウェアのオプションコンポーネントです。これにより ZCentral Connect では、ホストへのログインステータスの変更の監視、および HP ZCentral Remote Boost Sender の実行停止の検出が可能になります。Agent をホストにインストールすると、チェックアウト済みのユーザーが実際にはホストにログインしていることを確認できる、想定外のユーザーがホストにログインすると警告が表示される、Remote Boost Sender の実行が停止すると警告が表示されるといったメリットが得られます。ZCentral Connect Agent は、Windows 10 と Linux®（RHEL 7、RHEL8、Ubuntu 18.04、または Ubuntu 20.04）の両方にインストールできるサービスです。Agent サービスはローカル管理者として実行され、Manager のインストール中に構成されたメッセージバスポートを使用して Manager に接続します。

6.1. ZCentral Connect Agent のインストール

詳細については、『Agent 展開ガイド』を参照してください。

6.2. Agent トークンと更新

ZCentral Connect Agent および Manager 間の通信は、暗号化と認証でセキュリティが確保されます。暗号化のセキュリティは、Manager が使用する TLS 証明書で確保されます。Manager 証明書の構成の詳細については、このユーザーガイドの「証明書」セクションを参照してください。

認証のセキュリティは、Agent の展開プロセス時に確保されます。Agent のインストール担当者は、一意かつ 1 回のみ使用可能な認証コードの入力が必要です。この登録パスワードにより、インストールされた Agent が識別されるため、Manager が Agent を信頼した上で認証トークンを Agent と交換できます。Agent のトークンとは、ファイルシステムの保護フォルダーに Agent が保持する秘密のトークンで、オペレーティングシステムによっては暗号化されています。

認証トークンの有効期限は 30 日ごとに失効します。各 Agent の認証トークンは、1 日 1 回、またはホストとのセッションが終了するたびに、Manager が更新します。Manager が使用するデフォルトの有効期限と更新期間は、Manager 設定ファイルの AgentTokenExpirationTimeInDays と AgentTokenRenewPeriod を変更することにより、それぞれ構成可能です。詳細については、『ユーザーガイド』の「詳細設定」セクション参照してください。

Agent の切断期間が 30 日を上回ると、認証トークンの有効期限が失効し、Agent が Manager に接続してステータスの更新を送信できなくなります。この場合、新しいトークンを受け取るには、Agent を Manager に再登録する必要があります。詳細については、「登録」セクションの手順に従ってください。

注意：トークン更新プロセスは、Manager で 1 日 1 回実行されます。Manager サービスの開始 24 時間後、または Agent が接続するたびに実行するようにスケジュール設定されています。

6.3. ZCentral Connect AgentConfig

AgentConfig は、ZCentral Connect Agent と並行してインストールされるコマンドラインツールで、管理者による Agent のカスタマイズと登録を可能にするツールです。このツールは、Agent のインストール先と同じフォルダー、つまり Windows の場合は%PROGRAMFILES%\HP\ZCentralConnectAgent\bin、Linux®の場合は /opt/hp/zcentralconnectagent に通常は格納されています。

6.3.1. Agent の登録

Agent を登録するには、register パラメーターを指定して AgentConfig ツールを実行する必要があります。例：

AgentConfig.exe register

注意：AgentConfig は、管理者特権のコマンドプロンプト（Windows では Administrator、Linux®では root）で実行する必要があります。

注意：Linux®では、インストール完了後に AgentConfig register を実行するよう、RPM と DEB の各インストーラーから求められます。Windows では、登録はインストールプロセスに組み込まれています。

登録コマンドでは、必要な登録パラメーターの入力が求められます。以前に Agent が登録されていた場合は、AgentConfig により、現在設定されている値が表示されます。登録コマンドでは、次のパラメーターの入力が求められます。

- AgentHostname：ホストのホスト名。Manager に登録済みのホストの名前と一致する必要があります。
- ManagerHostname：HP ZCentral Connect Manager のホスト名。
- ManagerPort：HP ZCentral Connect Manager の HTTPS ポート。
- ManagerMessageBusPort：HP ZCentral Connect Manager のメッセージバスポート。
- AuthorizationCode：Manager の Web インターフェイスから取得した、ホストに対する認証コード。

完了すると、登録プロセスによって設定ファイルが更新され、Agent サービスが再起動します。

6.3.2. 設定の構成

AgentConfig を使用して、ZCentral Connect Agent サービスの構成を更新することもできます。例：

AgentConfig.exe set --ManagerCertificateThumbprint 65D6B7431D8A5F8E52D3BBA3B9D3B5B242A2BC5D

注意：Agent サービスでカスタマイズ可能なすべてのプロパティの一覧については、次のセクションを参照してください。

注意：AgentConfig を使用して設定をカスタマイズしても、Agent サービスは自動的に再起動しません。新しい設定を有効にするには、Agent サービスを手動で再起動する必要があります。

設定構成コマンドを実行すると、AgentConfig ツールにより、Agent 用の内部設定ファイルが更新されます。

ZCentral Connect Agent の設定

ZCentral Connect Agent の設定には、インストールプロセス中に自動で構成される設定が一定数あるほか、必要に応じて後で管理者が変更できる設定もあります。設定ファイルは次のパスにあります：%PROGRAMDATA%\HP\ZCentral ConnectAgent\settings.json（Windows）および/etc/hpzcentralconnectagent/settings.json（Linux®）。

注意：AgentConfig ツールを使用して、次のプロパティを変更/更新できます。

注意：変更を有効にするには、ZCentral Connect Agent サービスを再起動する必要があります。

サポートされているフィールドと対応するデフォルトの値は以下のように定義されています。

```
{
/* The hostname of HP ZCentral Connect Manager.*/
"ManagerHostname": "myconnecthostname.domain",

/* The HTTPS Port of HP ZCentral Connect Manager.*/
"ManagerPort": "443",

/* The Message Bus Port of HP ZCentral Connect Manager.*/
"ManagerMessageBusPort": "8883",

/* The thumbprint of the Manager certificate used to encrypt network traffic.*/
"ManagerCertificateThumbprint": "",

/* The hostname of this Host.It must match how the Host is registered in the Manager.*/
 "AgentHostname": "myhostname.local",

 /* Defines the time in seconds that the Agent will wait before reconnecting with the Manager after a new token is received.*/
"TokenRenewReconnectionWaitTime": "10",

 /* Defines the maximum time in seconds of the Keep Alive used on the Message Bus. Keep Alive is a heartbeat message sent on the Message Bus that keeps the active connection open and reliable.*/
 "MessageBusKeepAlive": "30",

 /* Defines the maximum time in seconds that a message can take to reach its destination.*/
 "MessageBusCommunicationTimeout": "20"

 /* Defines the maximum time in seconds that the Agent waits before trying to reconnect to the Message Bus. */
"MessageBusReconnectionWaitTime": "60"

 /* Defines if must ignore the revocation certificate list.If disabled, Trust Chain for Manager certificate must have an available revocation server.*/
 "IgnoreCertificateRevocationErrors": true
}
```

注意：設定ファイルには、内部使用のみを目的とした、変更してはならない、上述以外の他のプロパティが含まれている場合があります。

6.3.3. AgentConfig の無人実行

自動展開の場合は、ユーザー操作なしに AgentConfig ツールを実行できます。これを可能にするため、AgentConfig は次のコマンドライン引数を備えています。

- --quiet：登録中に引数の入力を求めるコマンドラインが AgentConfig で表示されません。このオプションを設定すると、settings.json ファイルの内容が AgentConfig で再利用されます。
- --accept-eula：コマンドライン表示を省略して EULA を受諾します。
- --authorization-code <authorization_code>：コマンドラインから AgentConfig に、登録用の認証コードが入力されます。

無人登録の例：

ステップ 1：必要なパラメーターを構成する：

```
AgentConfig set --AgentHostname myHost.domain.local --ManagerHostname zconnectionmanager.domain.local --ManagerPort 443 -- ManagerMessageBusPort 8883 --ManagerCertificateThumbprint 65D6B7431D8A5F8E52D3BBA3B9D3B5B242A2BC5D
```

ステップ 2： 無人登録：

```
AgentConfig register --quiet --accept-eula --authorization-code 58433e64-95bb-43c2-b53c-4ccc680c6270
```

無人登録および Agent 展開の自動化の詳細については、『Agent 展開ガイド』の「スクリプトの例」セクションを参照してください。

6.4. ZCentral Connect Agent ログ

ZCentral Connect Agent ログの取得方法の詳細については、「トラブルシューティング」ページの「ZCentral Connect Agent のトラブルシューティング」の章を参照してください。

6.5. Linux®における非 root ユーザーとしての Agent の実行

デフォルトでは、Linux®上の Agent サービスは root ユーザーとして実行されます。システムのセキュリティを高めるため、特権の少ないユーザーでサービスを実行することもできます。その場合は、root ユーザーでログインし、以下の手順に従います。

1. ZCentral Connect Agent サービスを停止します：systemctl stop hpzcentralconnectagent
2. Agent サービスを実行するユーザーアカウントを追加します：useradd -U -M zcentralconnect
3. 新しいユーザーにフォルダーのアクセス許可を割り当てます：chown -R zcentralconnect:zcentralconnect /var/log/hpzcentralconnectagent /etc/hpzcentralconnectagent /opt/hp/zcentralconnectagent
4. Agent サービス機能を設定します：setcap CAP_SYS_NICE,CAP_DAC_OVERRIDE,CAP_NET_ADMIN+ep /opt/hp/zcentralconnectagent/ZCentralConnectAgent
5. 作成したユーザーが Agent サービスを実行するように指定します。
    1. 任意のエディターでファイル/etc/systemd/system/multi-user.target.wants/hpzcentralconnectagent.service を編集します。
    2. [サービス]セクションに、次の行を追加します：User=zcentralconnect
    3. ファイルを保存して閉じます。
6. サービス構成をリロードします：systemctl daemon-reload
7. Agent サービスを開始します：systemctl restart hpzcentralconnectagent

6.6. ZCentral Connect Agent のアンインストール

Windows 上の Agent をアンインストールするには、Win キーを押しながら R キーを押し、「appwiz.cpl」と入力します。これにより、[プログラムの追加と削除]ウィンドウが開きます。HP ZCentral Connect Agent のエントリを検索し、通常のアンインストール手順に従います。

Linux 上では、RedHat の rpm -e と Ubuntu の dpkg -r を使用し、hpzcentralconnectagent という名前のパッケージをアンインストールします。パッケージにより、Agent サービスが停止し、インストールされているバイナリがシステムから削除されます。

注意：Agent をアンインストールしても、対応するホストのエントリは Administrator Portal から削除されません。Agent がまだあるとホストが想定している場合、Portal 上ではホストが切断済み Agent の状態になります。

注意：Agent をアンインストールしても、ログファイルや設定ファイルといった残りのデータは削除されません。

7. HP ZCentral Connect Hardware Monitor

Hardware Monitor は、ZCentral Connect 向けにシステムイベント機能を拡張するオプションサービスです。このサービスをインストールしておくと、オペレーティングシステムが ZCentral 4R システムで稼動しているときに、サービスによる電源イベントの通知が可能です。

注意：ZCentral Connect Hardware Monitor は、4R システムへの ZCentral Connect Agent のインストール中に自動でインストールされます。詳細については、『Hardware Monitor』ガイドを参照してください。

8. HP ZCentral Connect Client Portal の機能

HP ZCentral Connect Client Portal を使用すると、ユーザーが HP ZCentral Connect とのやりとりを行って、ホストへのアクセスを要求できます。詳細については、『HP ZCentral Connect Client Portal ガイド』を参照してください。

8.1. 前提条件

Client Portal へのアクセスにユーザーが使用する各クライアントマシンは、次の要件を満たしている必要があります。

- HP RGS Receiver バージョン 7.5、HP ZCentral Remote Boost Receiver 2020 以降がインストールされていること
- サポートされているオペレーティングシステムのいずれかを使用していること
  - Windows 10（64 ビットのみ）
  - Linux®
    - RHEL 7 または RHEL 8
    - Ubuntu 18.04 または Ubuntu 20.04
    - ThinPro 7 以降
    - 注意：Gnome デスクトップがサポートされています。KDE は現在サポートされていません
  - macOS® 10.12 以降

サポートされているインターネットブラウザーのいずれかを使用します

- Chrome バージョン 70.0.3538 以降
- Firefox バージョン 60.3.0 以降
- Edge バージョン 42.17134 以降
- Safari®およびその他のブラウザーのサポートは制限されています

8.2. HP ZCentral Connect Client Portal へのアクセス

HP ZCentral Connect Client Portal には、次のようなデフォルトのポータルアドレスを使用してアクセスできます：https://zcentralconnect.local.domain/。
注意：ZCentral Connect が 443 以外のポートにインストールされている場合、URL に加えてポート番号の入力が必要な場合があります。選択したポートが 8443 の場合の URL は次のとおりです：https://zcentralconnect.local.domain:8443/。

Manager は、インストール時に独自の証明書と自己署名証明機関（CA）を作成するため、CA がクライアントマシンで信頼されるようになるまでは「お使いの接続は、プライベートではありません」といった警告メッセージが表示されます。

注意：CA は、このユーザーガイドの「使用環境における自己署名証明機関の承認」セクションに記載されている手順に従って承認できます。
注意：インストール中に作成された証明機関をマシンが信頼している場合、このメッセージは表示されません。独自の証明書の構成についてサポートが必要な場合は、このユーザーガイドの「独自の証明書の使用」セクションに記載されている手順に従ってください。マシンが証明機関をどのように信頼するかについて詳細を確認したい場合は、このユーザーガイドの「証明機関の信頼」セクションを参照してください。

[詳細]をクリックし、[ホスト名に進む（安全ではない）]オプションを選択して続行します。

Your connection is not private

Attackers might be trying to steal your information from **ninja_storm** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

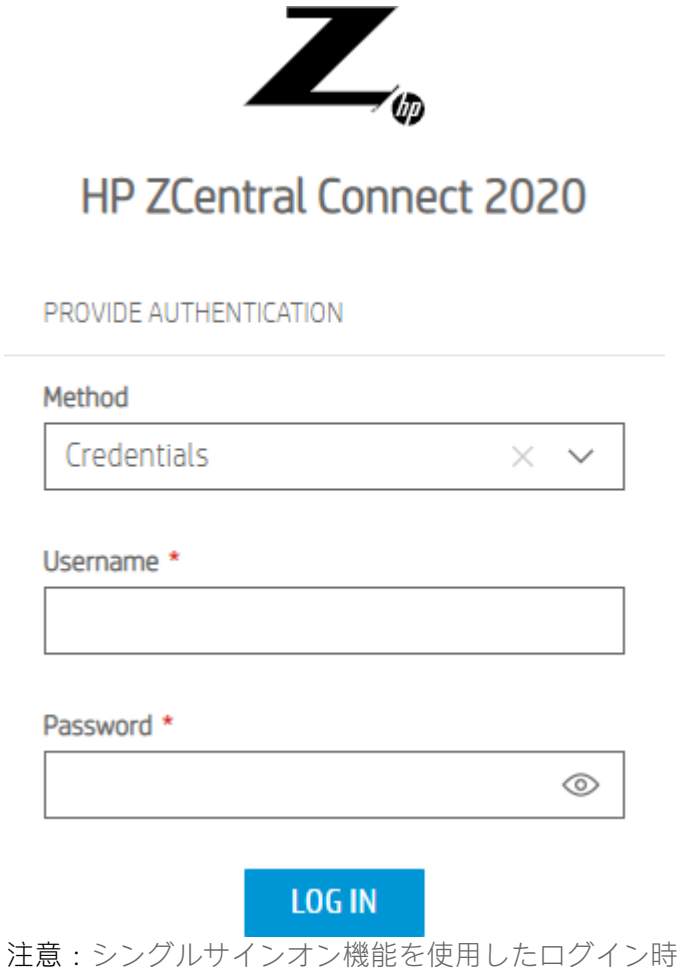
☐ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

Advanced　　Back to safety

8.3. Client の認証

Client Portal では、ユーザーログインに関する 2 種類の認証をサポートしています。

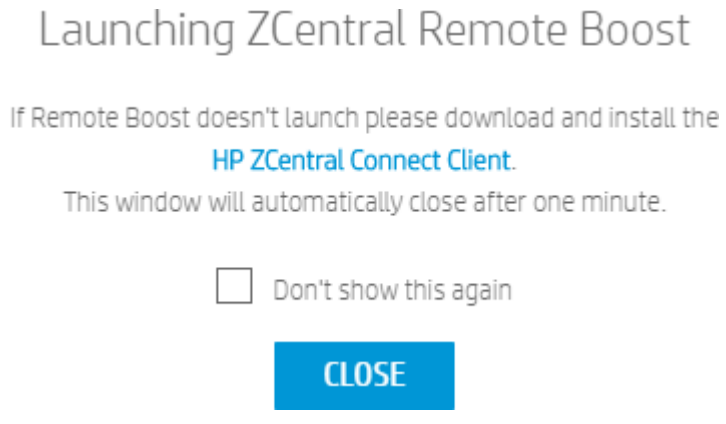
- シングルサインオン：このオプションでは、Kerberos を使用し、Active Directory からローカル OS にログインしているユーザーを活用します。これがデフォルトの認証方法です。
- 資格情報：シングルサインオンが利用できない場合は、Active Directory の資格情報によるログインがユーザーに求められます。



注意：シングルサインオン機能を使用したログイン時に問題が発生する場合は、「トラブルシューティング」ページの「クライアントへのシングルサインオン」セクションをご確認ください。

8.4. HP ZCentral Connect Client

ZCentral Connect Client は、目的のホストを対象とした HP ZCentral Remote Boost Receiver アプリケーションの起動を Client Portal と Administrator Portal の両方で可能にするアプリケーションです。Remote Boost との接続は、[Remote Boost]ボタンをクリックするたびに開始できます。クリックすると、HP ZCentral Connect Client のインストールが必要なことを示すダイアログが表示されます。



[次回から表示しない]オプションを有効にすると、ユーザーが ZCentral Connect のクッキーをブラウザーから削除するまで、このダイアログは表示されません。

8.4.1. HP ZCentral Connect Client のインストール

注意：ZCentral Connect Client をインストールまたは起動する前に、HP ZCentral Remote Boost Receiver または HP Remote Graphics Software Receiver をインストールしておく必要があります。Remote Boost HP ZCentral Remote Boost の Web サイトからダウンロードできます。

Windows

Windows システムの場合は、ダウンロードリンクをクリックして、HP ZCentral Connect Client インストーラーをダウンロードします。インストーラーファイルをダブルクリックし、メッセージを閉じてから、Administrator Portal の[Remote Boost を起動]ボタンまたは Client Portal の[ホストに接続]ボタンをクリックして操作をやり直します。

ZCentral Connect Client をアンインストールするには、Windows の[プログラムの追加と削除]を開いて[HP ZCentral Connect Client]を選択し、アンインストールプロセスに従います。

Linux®

Linux®システムの場合、ダウンロードリンクをクリックすると、Remote Boost URI プロトコルを登録できる.sh ファイルがダウンロードされます。このスクリプトは、サポートされているどの Linux®環境にもインストールできます。

- RHEL 7
- RHEL 8
- Ubuntu 18.04

- Ubuntu 20.04
- ThinPro 7 以降

ZCentral Connect Client をインストールするには、次の手順に従います。

1. install_zcentralconnect_client.sh ファイルに実行権限を付与します
    - chmod +x install_zcentralconnect_client.sh
2. スクリプトを実行します
    - sudo ./install_zcentralconnect_client.sh
3. ブラウザーのメッセージを閉じてから、Administrator Portal の[Remote Boost を起動]ボタンまたは Client Portal の[ホストに接続]ボタンをクリックして操作をやり直します。

HP ThinPro では、ユーザー向けのデフォルトブラウザー構成により、ZCentral Connect の各ページから Remote Boost の起動を可能にする手順が別途必要です。ThinPro で ZCentral Connect Client を有効にする方法の 1 つは、Firefox 用のカスタムランチャーの作成です。

1. ThinPro デスクトップを右クリックします
2. [作成]>[その他]>[カスタム]にアクセスします
3. [カスタムショートカット]を右クリックして、[編集]をクリックします
4. 名前は、次のような意味のある名前に変更できます：HP ZCentral Connect Client
5. 実行するコマンドに続けて「firefox https://<HPZCentralConnectHostname>:<port>/」と入力します。例：Firefox https:// zcentralconnectdemo /
6. [適用]をクリックします
7. このランチャーを使用すると、HP ZCentral Connect Portal に直接アクセスできるうえ、Remote Boost も正常に起動できます。

ZCentral Connect Client をアンインストールするには、-u パラメーターを指定して、同じ install_zcentralconnect_client.sh を実行します。

例：sudo ./install_zcentralconnect_client.sh -u

注意：HP ThinPro で Firefox をアップグレードする場合は、HP ZCentral Connect Client を再インストールすることをお勧めします。

macOS®

macOS®の場合、ダウンロードリンクをクリックすると、Remote Boost URI プロトコルを登録して Remote Boost ランチャーを開く、圧縮ファイルの app.zip がダウンロードされます。このアプリケーションは、macOS® Sierra（10.12）以降でサポートされています。

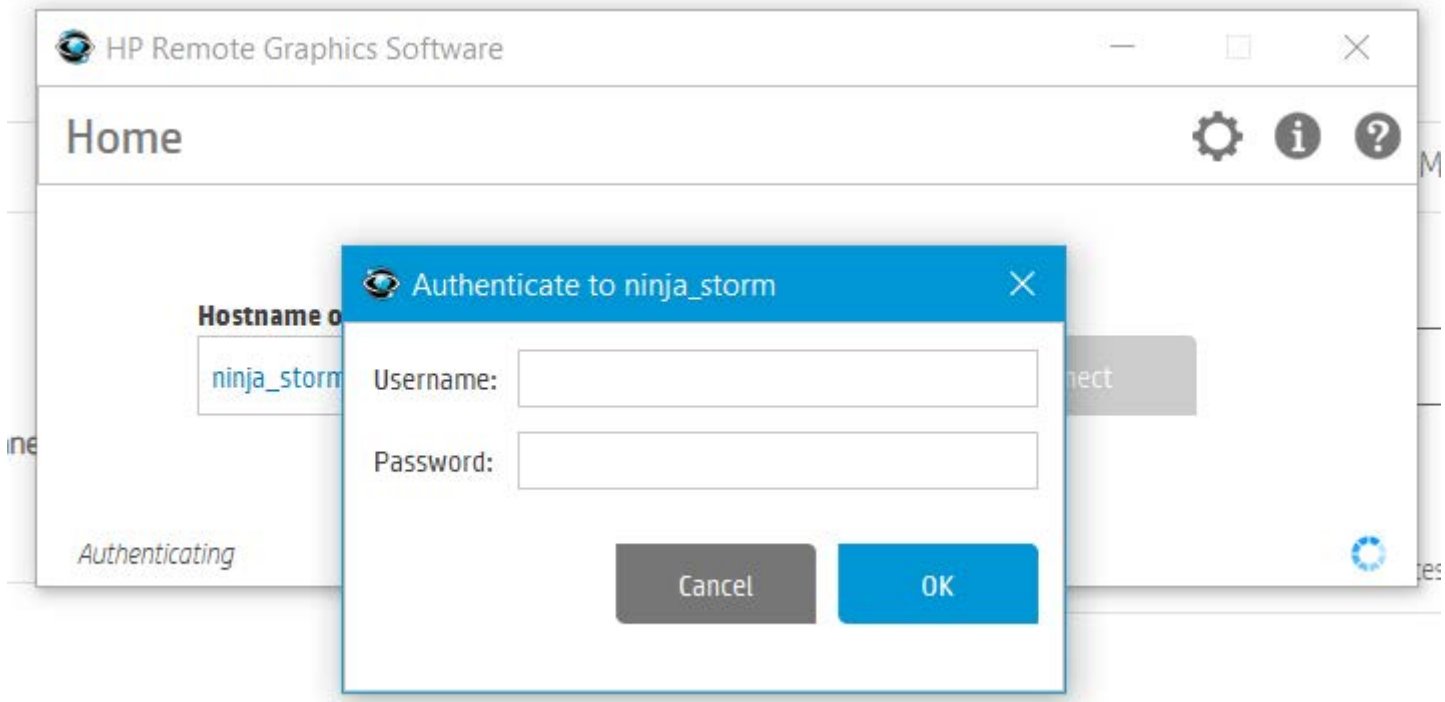
macOS®に ZCentral Connect Client をインストールするには、次の手順に従います。

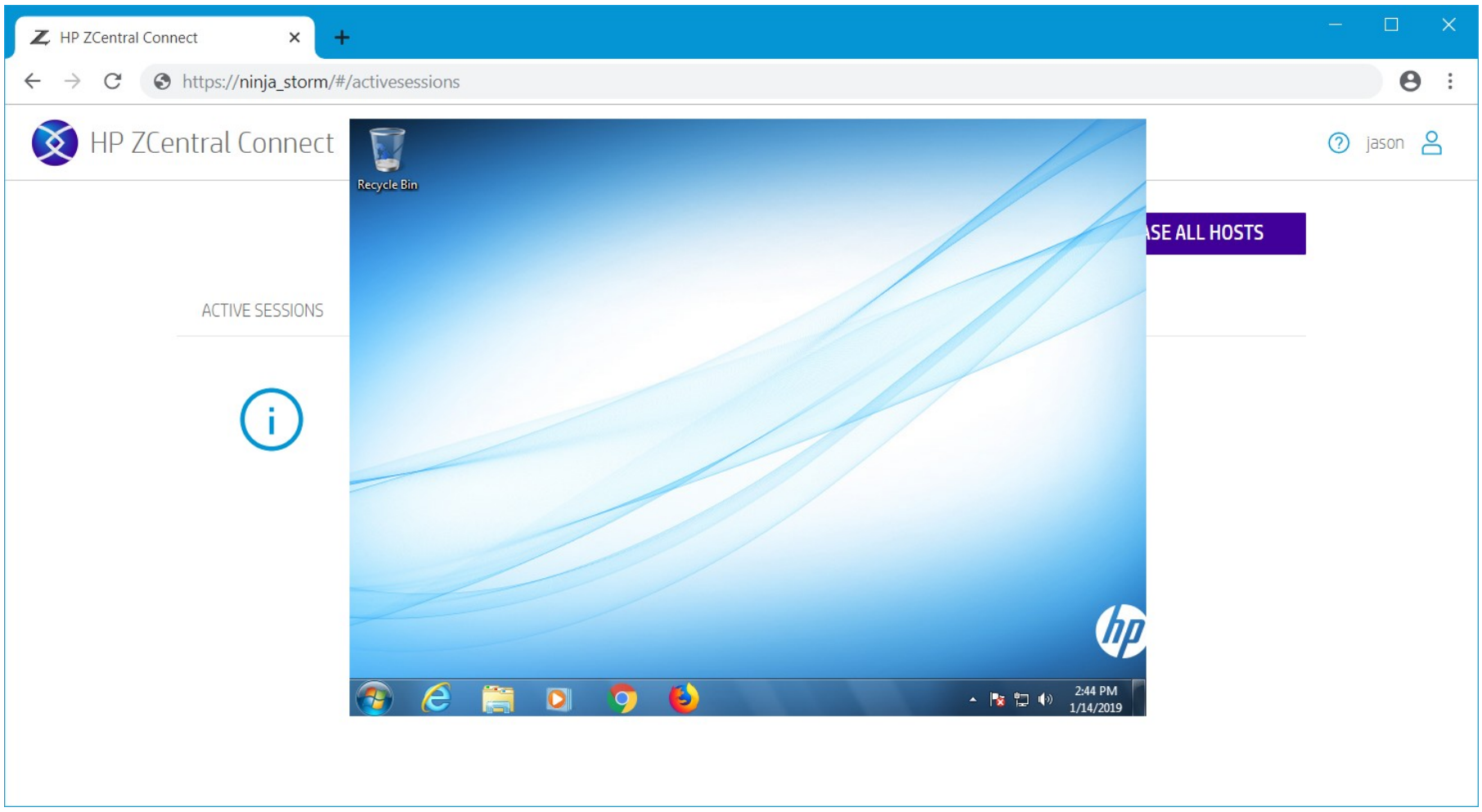
1. HP ZCentral ConnectClient.app.zip を解凍します
2. HP ZCentral Connect Client.app を常駐場所にコピーします。このファイルは、Remote Boost を起動するたびに使用されます
3. Control キーを押してから、HP ZCentral Connect Client.app をクリックします
4. ショートカットメニューから[開く]を選択します
5. [開く]をクリックします

8.4.2. HP ZCentral Connect Client をインストール済みの場合

ZCentral Connect Client をインストールしておくと、Administrator Portal の[Remote Boost を起動]ボタンまたは Client Portal の[ホストに接続]ボタンをクリックして、ZCentral Remote Boost との接続を開始できます。ZCentral Connect Client により、Remote Boost が起動し、割り当てられたホストへのリモート接続が開始します。

注意：ZCentral Connect では、ZCentral Remote Boost との接続に関するセキュリティポリシーは変更されません。シングルサインオンおよびその他の認証機能は、Remote Boost 機能として利用でき、Remote Boost ユーザーガイドを使用して構成できます。





8.4.3. Linux ホストに対する Remote Boost を使用した認証

ドメインに参加している Linux ホストにログインする場合、ログイン先のマシンで構成されているドメインレルムと一致する、完全修飾ドメイン資格情報を使用してログインする必要があります。その例を以下に示します。

DNS に参加しているドメイン名が DOMAIN.NETWORKNAME の場合は、次のようにログインする必要があります。

username@DOMAIN.NETWORKNAME

参加しているドメイン名が domain.networkname の場合は、次のようにログインする必要があります。

username@domain.networkname

また、ユーザーがユーザー名のみを使用して認証できるように、FQDN 資格情報を使用しないようにホストを構成することもできます。このように構成するには、ターミナルウィンドウを開いて root ユーザーでログインし、次の手順に従います。

1. 任意のエディターでファイル/etc/sssd/sssd.conf を編集します
2. 行 use_fully_qualified_names = True を use_fully_qualified_names = False に変更します
3. ファイルを保存して閉じます
4. sssd サービスを再起動します：systemctl restart sssd
5. サービス構成をリロードします：systemctl daemon-reload

これらの変更を完了すると、ユーザーは以下を使用してログインできるようになります。

username

9. ライセンスガイド

ZCentral Connect Manager のライセンスは、Manager ソフトウェアにのみ適用されます。無料ソフトウェアの ZCentral Connect Agent と ZCentral Connect Client は、自由にインストールして使用できます。

ライセンスファイルは、ユーザーがホストとの新規セッションを開始するたびに、Manager ソフトウェアによってチェックされます。ライセンス数が最大になると、新規セッションの開始は拒否されます。この番号は、ライセンスファイル内に「Qty=N」として定義されています。ライセンスで許可されている最大数量は、「詳細」セクションでも確認できます。最大 5 つの接続をサポートする 60 日間の無料トライアルライセンスをダウンロードする方法、またはライセンスの購入と更新については、hp.com/Zcentral をご覧ください。

9.1. 使用ライセンス（LTU）購入時のホスト名および数量の指定

ZCentral Connect Manager のライセンスファイルを取得するときには、Manager をインストールして稼動させるサーバーのホスト名を指定する必要があります。サーバーのホスト名を確認するには、Windows のコマンドプロンプトで「hostname」と入力します。

また、サポートする同時セッション数を表す数量の指定も必要です。通常は、購入した数量をすべて引き換えて使用しますが、数量の一部を引き換えて、複数の ZCentral Connect Manager でのセッションのライセンスに指定することもできます。

ライセンスファイル内の署名には、指定したホスト名と数量が反映されています。ライセンスファイル内のいずれかのフィールドを変更すると、ライセンスキーが無効になります。お使いの Manager サーバーのホスト名を変更する必要がある場合や接続数を増やしたい場合は、管轄の HP リージョナルライセンスセンターにお問い合わせください。

9.2. HP ZCentral Connect Software のライセンスファイルをインストールする方法

1. ライセンスファイルを ZCentral Connect Manager のデータディレクトリにコピーします：%PROGRAMDATA%\HP\ZCentralConnectManager
2. 管理者として、Services.msc アプリを使用して HP ZCentral Connect Manager サービスを再起動します

ライセンスに問題がある場合は、「トラブルシューティング」ページの「ライセンス」セクションをご確認ください。

注意：ZCentral Connect Agent および ZCentral Connect Client には、ライセンスファイルは必要ありません。

注意：ライセンスファイルには拡張子.lic が必ず付きます。

注意：ZCentral Connect のライセンスメカニズムでは、ライセンスファイルは一度に 1 つしかチェックアウトできません。ライセンスのアップグレード後は、最新のライセンスのみをデータディレクトリに保持することをお勧めします。

10. セキュリティに関する推奨事項

ZCentral Connect は、お使いの環境で予防措置をいくつか講じることで、セキュリティを最大限高めることができます。その一部を以下に示します。

10.1. シングルサインオン認証の使用

エンドユーザーのパスワード保護を強化するには、資格情報オプションではなくシングルサインオンオプションを使用した、ZCentral Connect Client Portal 経由のユーザー認証をお勧めします。シングルサインオンでは、Kerberos を使用した認証が行われるため、パスワードを入力して送信する必要はありません。エンドユーザーにシングルサインオンを使用させるには、ZCentral Connect Manager が使用する Active Directory ドメインに、ユーザーのデバイスを参加させておく必要があります。特定のデバイスをドメインに参加させておけない場合は、使用できる認証は資格情報による認証のみに限定されます。

注意：シングルサインオンが正常に機能しない場合は、「トラブルシューティング」ページの「クライアントへのシングルサインオン」セクションをご確認ください。

10.2. ネットワークトランスポートセキュリティ

10.2.1. TLS プロトコル

ZCentral Connect ソフトウェアでは、ソフトウェアが稼動しているオペレーティングシステムで利用可能な最高の TLS プロトコルと最強の暗号化方式がすでに使用されています。お使いの環境に旧型または旧式のオペレーティングシステムが存在する場合、一部のネットワーク接続時のネゴシエーションに、よりレベルの低い TLS 標準と潜在的に脆弱な暗号化方式が使用されることがあります。必須ではありませんが、TLS 1.2 を使用した接続のみを許可するように ZCentral Connect Manager を制限し、一部の脆弱な暗号化方式を無効にする方が望ましいこともあります。

ZCentral Connect Manager では、オペレーティングシステムで決められたネットワークセキュリティ設定が使用されるため、Manager の動作を変更するためには、一部のレジストリ設定を変更する必要があります。レジストリの編集は、正しく行わないとオペレーティングシステムに悪影響を及ぼす可能性があるため注意してください。これらの設定を変更すると、SSL 暗号化の実行をオペレーティングシステムに任せているシステム上のすべてのネットワークアプリケーションに、その影響が及びます。他のプログラムへの影響を最小限に抑えるには、HP ZCentral Connect Manager が常駐するマシン上の主要ソフトウェアを HP ZCentral Connect Manager に限定することをお勧めします。また、変更を加える前に Windows レジストリをバックアップすることも肝要です。レジストリのバックアップと復元を実行する方法については、こちらから Microsoft の操作説明を参照してください。

注意：ZCentral Connect の管理対象ワークステーションに、バージョンが 11.x.77 以下の Intel® AMT が存在する場合は、Manager をホストしているシステムでアウトバウンド接続用の TLS1.1 がサポートされていることを確認してください。TLS1.1 のクライアントサポートや SHA1 ハッシュは、Windows のレジストリ設定で明示的に無効にしないでください。以下の手順は、インバウンド接続用の TLS をサポートするようにサーバーを構成する方法のみを示しているためご注意ください。ファームウェアは常に最新バージョンに更新しておくことをお勧めします。

許可する接続を TLS1.2 に制限するには、こちらの Microsoft の操作説明に従って、TLS1.0 と TLS1.1 を無効、TLS1.2 を有効にしてください。中間キーがまだ存在しない場合は、キーの作成が必要な場合があります。大まかな手順を次に示します。

Manager マシンの場合：

1. スタートメニューをクリックし、Registry Editor アプリを検索して開きます。パスに移動します [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols]
2. [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0]の下に、Server という名前のサブキーを作成し、その中に Enabled という名前の DWORD エントリを作成します。Enabled の値は必ず 0 に設定してください。
3. [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1]で同じ手順を繰り返します。
4. システムを再起動してレジストリの変更を取得します。

この時点では、TLS1.0 と TLS1.1 の提供を無効に変更すれば十分です。必須ではありませんが、次の手順に従って TLS1.2 プロトコルを明示的に有効にすることもできます。

1. [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]の下に、Server という名前のサブキーを作成し、その中に Enabled という名前の DWORD エントリを作成します。Enabled の値は必ず 1 に設定してください。
2. システムを再起動してレジストリの変更を取得します。

10.2.2 脆弱な暗号化方式（トリプル DES および RC4）の無効化

ZCentral Connect Manager では、HTTPS サーバーを起動する暗号化方式はオペレーティングシステムからの提供に任せています。オペレーティングシステムがサポートする暗号化方式が脆弱な場合は、Manager に関する TLS 通信のセキュリティが侵害されることがあります。Windows Server 2016 および Windows Server 2019 の新規インストールに使用する暗号化方式として代替できることがテストで判明した、トリプル DES および RC4 暗号の無効化に関する注意事項は、次のセクションに記載しています。暗号化方式の有効化と無効化の詳細については、Microsoft が提供するガイドを参照してください。

注意：レジストリを変更すると、オペレーティングシステムに悪影響が及ぶことがあります。レジストリのバックアップと復元を実行する方法については、こちらから Microsoft の操作説明を参照してください。お使いの Windows オペレーティングシステムでトリプル DES を無効にするには、次のようにレジストリを変更します。

1. スタートメニューをクリックし、Registry Editor アプリを検索して開きます。パスに移動します [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]
2. [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168]の下に、Enabled という名前の DWORD エントリを作成し、その値を必ず 0 に設定します。

お使いの Windows オペレーティングシステムで RC4 暗号化方式を無効にするには、次のようにレジストリを変更します。

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]
  - "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128]
  - "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128]
  - "Enabled"=dword:00000000

レジストリの変更を取得するには、HP ZCentral Connect Manager サービスを再起動してください。

10.3. LocalSystem の使用禁止

サービスは LocalSystem として実行するのではなく、マネージドサービスアカウントまたは AD アカウントのいずれかを使用して Manager サービスをホストすることをお勧めします。MSA を使用すると、セキュリティが次の 2 点で向上します。

- MSA 用のパスワードがエンドユーザーに公開されることがありません。MSA パスワードは、マシン間のやりとりでのみ取得して使用できます。さらに、MSA 用の堅牢なパスワードの維持と定期的なローテーションは、ドメインコントローラーが行います。
- 操作に必要なアクセス許可のみを MSA に付与できます。これにより、基盤となるサービスの侵害で公開されるシステムが、（LocalSystem としての実行と比較して）MSA アカウントのアクセス許可ごとに限定されます。

10.4. 管理者アカウントのパスワード

要件

管理者アカウントを保護できるように、ZCentral Connect Manager にはパスワードに関する次の要件があります。

- 文字数は 12 文字から 128 文字まで
- 先頭と末尾が空白文字でない
- 周知のパスワードの一覧に含まれていない

これらの要件は、Manager のインストール中に加え、構成ユーティリティおよび UI 内で行われる検証により、確実に順守されます。

推奨事項

要件に加えて、NIST のガイドラインに従うことも肝要です。最新のガイドラインはこちらで確認できます。

10.5. Agent のデータフォルダーの保護

ZCentral Agent のインストーラーでは、データフォルダーが管理者またはルートで保護されるように、データフォルダーのアクセス許可が設定されます。これらのアクセス許可は、管理者以外がアプリケーションのデータファイルにアクセスして読み取りと書き込みを行うことを防ぐために設定されているため、変更しないでください。

Windows では、Agent がセキュリティ対策をさらに講じてホスト情報を保護します。これらの対策が利用できない場合は、「Microsoft の CNG api の利用に問題がありました」など、Agent ログファイルに書き込まれる警告メッセージが表示されます。この警告が表示された場合は、Windows OS が最新であることを確認してください。警告が続く場合は、HP サポートにお問い合わせください。

11. バックアップと復元

次の手順を実行して、ZCentral Connect Manager データのバックアップと復元を行います。

注意：ホスト用の AMT パスワードは、ZCentral Connect Manager を最初に展開した Windows インストールで暗号化されています。別の Windows インストールでバックアップを復元する場合は、すべての AMT パスワードを管理者が再入力する必要があります。詳細については、「トラブルシューティング」ページの[既知の問題と制限]セクションをご確認ください。

11.1.バックアップの作成

1. Windows サービス管理コンソールを使用して HP ZCentral Connect Manager サービスを停止します。
2. フォルダー%PROGRAMDATA%\HP\ZCentralConnectManager にすべてのファイルを保存します。
3. 証明機関（CA）証明書を保存します。
    1. Windows タスクバーの Windows ボタンを右クリックして、[ファイル名を指定して実行]を選択します。
    2. 「certmgr.msc」と入力します。
    3. 左側のパネルで、[信頼されたルート証明機関]>[証明書]を展開します。
    4. 右側のパネルで、分かりやすい名前が HP ZCentral Connect CA の証明書を探してダブルクリックします。
    5. [詳細]タブにアクセスし、[ファイルへコピー]をクリックします。
    6. ウィザードに従い、証明書の秘密鍵をエクスポートするチェックボックスをオンにします。[すべての拡張プロパティをエクスポートする]がオンになっていて、AES256-SHA256 暗号化が選択されていることを確認してください。
    7. ウィザードを終了して、CA 証明書をファイルにエクスポートします。
4. TLS 証明書を保存します。
    1. Windows タスクバーの Windows ボタンを右クリックして、[ファイル名を指定して実行]を選択します。
    2. 「certmgr.msc」と入力します。
    3. 左側のパネルで、[個人]>[証明書]を展開します。
    4. 右側のパネルで、分かりやすい名前が HP ZCentral Connect Manager の証明書を探してダブルクリックします。
    5. [詳細]タブにアクセスし、[ファイルへコピー]をクリックします。
    6. ウィザードに従い、証明書の秘密鍵をエクスポートするチェックボックスをオンにします。[すべての拡張プロパティをエクスポートする]がオンになっていて、AES256-SHA256 暗号化が選択されていることを確認してください。
    7. ウィザードを終了して、証明書をファイルにエクスポートします。
5. Windows サービス管理コンソールを使用して HP ZCentral Connect Manager サービスを再起動します。

11.2. バックアップの復元

注意：Manager の新規インストールにバックアップを復元する場合は、最初に Manager をインストールしてから、次の手順に従って続行してください。

注意：Manager のバージョンが異なる場合は、バックアップに互換性がありません。バックアップと復元は、同じバージョンの Manager でのみ行えます。

1. Windows サービス管理コンソールを使用して HP ZCentral Connect Manager サービスを停止します。
2. 保存されたすべてのファイルをバックアップから%PROGRAMDATA%\HP\ZCentralConnectManager フォルダーに復元します。
3. 証明機関（CA）証明書を復元します。
    1. CA 証明書ファイルをダブルクリックし、[証明書のインストール]をクリックします。
    2. ローカルマシンを選択します。
    3. 次に表示されるウィンドウで、[このキーをエクスポート可能としてマークする]と[すべての拡張プロパティを含める]がオンになっていることを確認します。
    4. 次に表示されるウィンドウで、[すべての証明書を次のストアに配置する]を選択し、証明書のインポート先として[信頼されたルート証明機関]を指定します。
    5. ウィザードを終了します。
4. Manager TLS 証明書を復元します：
    1. 証明書ファイルをダブルクリックし、[証明書のインストール]をクリックします。
    2. ローカルマシンを選択します。
    3. 次に表示されるウィンドウで、[すべての証明書を次のストアに配置する]を選択し、証明書のインポート先として[個人]を指定します。
    4. ウィザードを終了します。
    5. Windows タスクバーの Windows ボタンを右クリックして、[ファイル名を指定して実行]を選択します。
    6. 「certmgr.msc」と入力します。
    7. 左側のパネルで、[個人]>[証明書]を展開します。
    8. 右側のパネルで、[発行先]列と[発行者]列を使用して、インポートしたばかりの証明書を探します。Manager の展開時に使用されたホスト名と一致する証明書を見つけます。
    9. 証明書のプロパティを開き、分かりやすい名を次の名前に設定します：HP ZCentral Connect Manager
    10. 証明書をダブルクリックして、[詳細]タブにアクセスします。拇印の値まで下にスクロールします。

5. Manager 構成ファイルを確認します：

    1. フォルダー%PROGRAMDATA%\HP\ZCentralConnectManager にアクセスします。
    2. ファイル settings.json を開きます。
    3. ホスト名とポートのプロパティが現在のコンピューターの値と一致するかどうかを確認します。必要に応じて値を調整します。
    4. CertificateThumbprint プロパティの値が証明書の拇印と一致するかどうかを確認します。必要に応じて値を調整します。
    5. Manager Config App を実行して、その証明書を使用するように Manager を構成します。

        - Manager の実行に使用する証明書の拇印とサービスアカウントを引き渡す--configure コマンドを使用して、ManagerConfig.exe を実行します。
        - 例：ManagerConfig.exe certificate --configure --serviceAccount domain\zcentralconnectmsa$ -- certificateThumbprint XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

6. Windows サービス管理コンソールを使用して HP ZCentral Connect Manager サービスを再起動します。

12. アンインストール

Manager をアンインストールするには、Win キーを押しながら R キーを押し、「appwiz.cpl」と入力します。これにより、[プログラムの追加と削除]ウィンドウが開きます。HP ZCentral Connect Manager エントリを検索し、通常のアンインストール手順に従います。

注意：Manager をアンインストールしても、クライアントマシンや管理対象ワークステーションには何の影響も及びません。

注意：Manager データはアンインストール中に削除されません。すべての Manager データは、%PROGRAMDATA%\HP\ZCentralConnectManager フォルダーに残ります。

13. 既知の問題と制限

「トラブルシューティング」ページの[既知の問題と制限]セクションをご確認ください。

著作権およびライセンス

商標について

サードパーティーについて

サードパーティーのソースコードとライセンスは、必要に応じて HP ZCentral Connect とともに再配布されます。

ドキュメントバージョン

エディション：20.1.2

部品番号：M46647-002