VMware Carbon Black Cloud Workload ガイド

変更日：2023 年 10 月 26 日

VMware Carbon Black Cloud Workload 1.2

vmware®

最新の技術ドキュメントは、 VMware の Web サイト （https://docs.vmware.com/jp/）

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
〒 108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

目次

VMware Carbon Black Cloud Workload ガイド

VMware Carbon Black Cloud Workload ガイド は、vCenter Server で仮想マシン ワークロードを保護するために VMware Carbon Black Cloud™ Workload Plug-in をインストール、構成、および使用する方法について説明します。

この情報は、Carbon Black Cloud Workload Plug-in をインストール、構成、使用するユーザーを対象としています。

対象ユーザー

この情報は、Windows または Linux システム管理者としての経験があり、仮想マシン テクノロジーおよびデータセンターの運用に詳しい方を対象としています。本書は、VMware ESXi™、VMware vCenter Server®、VMware Tools™、VMware NSX-T Data Center™ など、VMware vSphere® に精通していることを前提としています。

Carbon Black Cloud Workload 概要

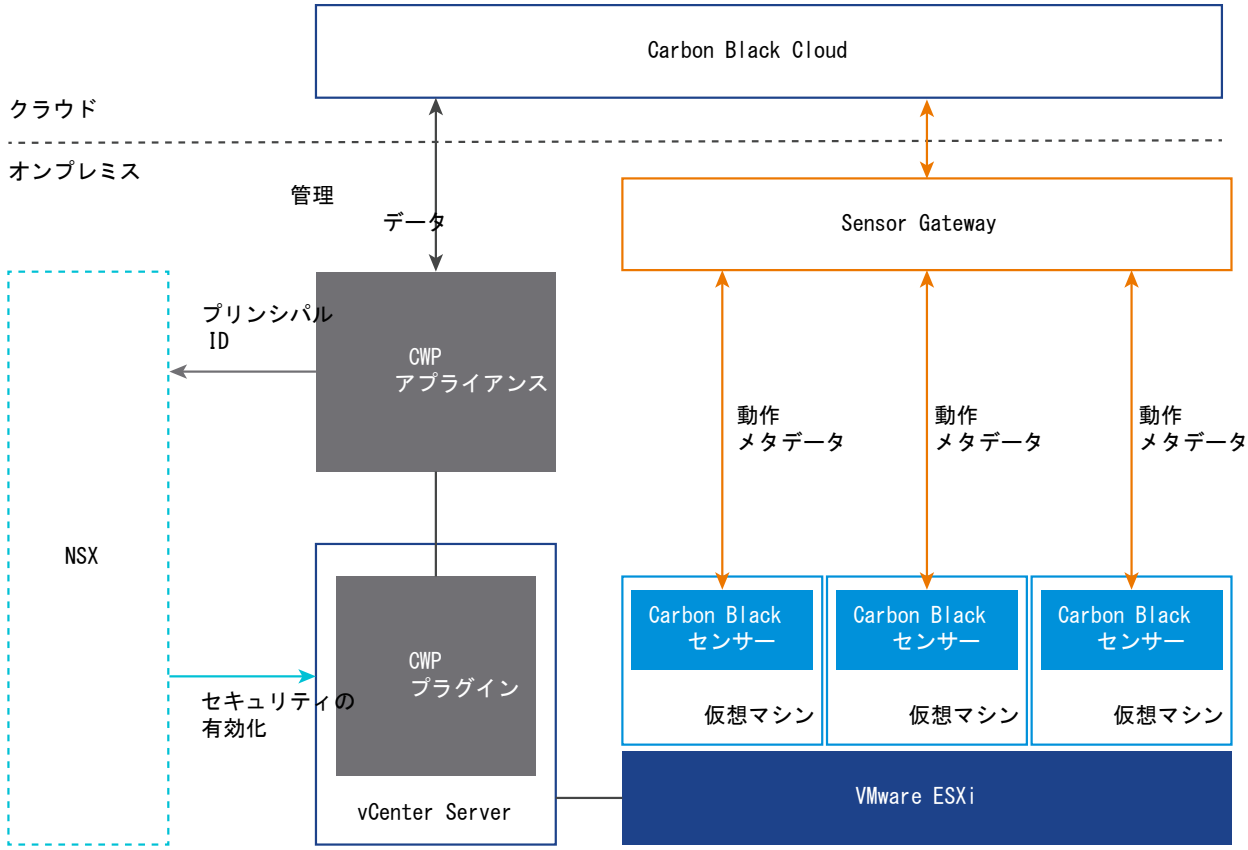
1

VMware Carbon Black Cloud™ Workload は、仮想環境で実行されているワークロードを保護するデータセンター セキュリティ製品です。Carbon Black Cloud Workload は、仮想マシンに保護機能を組み込むことにより、セキュリティを仮想環境に内在させます。vCenter Server で Carbon Black を有効にしたら、Carbon Black Cloud Workload で保護されているインベントリを表示し、Carbon Black Cloud Workload Plug-in によって提供されるインベントリおよびリスク評価ダッシュボードを表示できます。

Carbon Black Cloud コンソールからデータセンターのワークロードを簡単に監視し保護できます。Carbon Black Cloud Workload Plug-in は、データセンターのインベントリを詳細に可視化し、コンポーネントのライフサイクルを徹底管理します。

リリース 1.1 以降では、Carbon Black Cloud Workload と VMware NSX-T Data Center™ の統合によって、Carbon Black Cloud で観察された動作に基づく NSX 修正ポリシーをトリガできます。保護された仮想マシン (VM) で修正をトリガする Carbon Black Cloud アラートでは、NSX-T Distributed Firewall (DFW) ポリシーを使用して修正を実行できます。

Carbon Black Cloud Workload は、互いに相互作用するいくつかの主要なコンポーネントで構成されています。



最初に、登録プロセスを通じて Carbon Black Cloud を vCenter Server に接続する Carbon Black Cloud Workload アプライアンス のオンプレミス OVF または OVA テンプレートを展開する必要があります。登録が完了すると、Carbon Black Cloud Workload アプライアンス は Carbon Black Cloud Workload Plug-in を展開し vCenter Server からインベントリを収集します。収集されたインベントリ データは、プラグインの[インベントリ] タブに表示され、Carbon Black Cloud コンソールにも伝達されます。

ワンクリック インストール プロセスで、アプリケーション ワークロードが実行されている仮想マシン上で Carbon Black を有効にできます。

Carbon Black を正常に有効にしたら、Carbon Black Cloud Workload Plug-in および [仮想マシン] - [監視] タブからインベントリ データとプロセスを表示および監視できます。

Carbon Black Cloud コンソールに移動してセンサー グループを作成し、組織のセキュリティ ニーズに合わせてポリシーを設定できます。Carbon Black Cloud コンソールから潜在的な脅威を特定、調査、および修正できます。Carbon Black Cloud の詳細については、Carbon Black Cloud コンソールの右上にある [ヘルプ] メニューの[ユーザー ガイド]を参照してください。

Carbon Black Cloud Workload アプライアンス

Carbon Black Cloud Workload アプライアンス は、オンプレミス ベースの制御ポイントであり、vCenter Server と Carbon Black Cloud の間のリエゾンとして機能します。アプライアンスは、vCenter Server からワークロード インベントリ データを収集し、そのデータを Carbon Black Cloud と共有します。

アプライアンスは、Carbon Black Cloud と NSX Manager の間の通信チャネルも提供します。これは、NSX のファイアウォール保護機能を備えた Carbon Black Cloud ペアの強力なデータ分析機能です。アプライアンスを使用して、NSX 統合を Carbon Black Cloud 組織に登録します。アプライアンスは、プリンシパル ID を介して NSX に登録されます。証明書ベースの認証が提供されるため、管理者ユーザーの認証情報を維持する必要はありません。ロールの割り当てまたはプリンシパル ID の追加については、「VMware NSX-T Data Center 製品ドキュメント」を参照してください。

Carbon Black Cloud Workload Plug-In

Carbon Black Cloud Workload Plug-in は、ライフサイクル管理を改善し、vCenter Server で直接リアルタイムの可視化を実現します。プラグインは、特定の仮想マシンで実行されるプロセスおよびネットワーク接続を直接可視化します。Carbon Black Cloud Workload Plug-in は、セキュリティ チーム全体の可視化と制御を実現するために、Carbon Black Cloud と連携して動作します。

vCenter Server

vCenter Server は、データセンターからインベントリ データを収集するために使用されます。収集されたインベントリ データは、セキュリティ割り当てに使用されます。Carbon Black Cloud Workload Plug-in は、直接表示するため vCenter Server で使用できます。

Carbon Black Cloud

Carbon Black Cloud は、使いやすい単一のコンソールを使用して、複数のワークロード セキュリティ機能を統合するクラウドネイティブ サービスです。インフラストラクチャや InfoSec などのさまざまなチームが、セキュリティを強化するために単一の信頼できる情報源を共有できます。

次世代のアンチウイルス (NGAV) 検出と動作分析に基づいて、Carbon Black Cloud コンソールにアラートが表示されます。コンソールを使用して、保護された仮想マシンの修正をトリガする Carbon Black Cloud アラートを表示し、特定の NSX-T Distributed Firewall (DFW) ポリシーのタグを修正に適用します。

Carbon Black ランチャ

展開作業を最小限に抑えるため、VMware Tools で軽量な Carbon Black ランチャ を使用できます。データセンターで Carbon Black を有効にすると、ランチャが仮想マシンに Carbon Black センサーをダウンロードしてインストールする場合に、サイレント インストールがトリガされます。

Windows 仮想マシンと Linux 仮想マシンで Carbon Black を有効にできます。

- [Windows 仮想マシン]: Windows 仮想マシンの場合、Carbon Black ランチャ は VMware Tools に含まれています。ワークロードのランチャを受け取るには、VMware Tools をインストールするかバージョン 11.2 以降 にアップグレードする必要があります。
- [Linux 仮想マシン]: Linux 仮想マシンの場合、VMware Tools Operating System Specific Packages (OSPs) で入手できるランチャを手動でインストールする必要があります。http://packages.vmware.com/ のパッケージ リポジトリから、ゲスト オペレーティング システム用の Carbon Black ランチャ をダウンロードしてインストールします。

NSX Manager

NSX Manager アプリケーションは、NSX 環境を管理するための Web ベースのユーザー インターフェイスを提供します。NSX Manager のインストール、管理、およびセキュリティの詳細については、VMware NSX 製品ドキュメントを参照してください。

Carbon Black Sensor Gateway

Carbon Black Sensor Gateway は、vSphere ワークロードに展開されたセンサーと Carbon Black Cloud 間のすべてのインバウンドおよびアウトバウンド通信のブリッジとして機能するオンプレミス コンポーネントです。詳細については、Carbon Black Sensor Gateway のインストールと使用 を参照してください。

vSphere の環境で Carbon Black を有効にするための準備

2

vSphere 環境で Carbon Black を有効にする前に、環境の準備が整っていて、Carbon Black Cloud コンソールにアクセスできることを確認します。

次の VMware Carbon Black Cloud の動作環境要件を参照してください。

- VMware Carbon Black Cloud™ Workloads の動作環境要件
- VMware Carbon Black Cloud™ 脆弱性管理の動作環境要件

次のトピックを参照してください。

- インストーラのダウンロード
- Carbon Black Cloud にアクセスしています

インストーラのダウンロード

Carbon Black Cloud Workload Plug-in のソフトウェアを備えた Carbon Black Cloud Workload アプライアンス はすべて、完全なインストールに使用される単一の Open Virtualization Appliance (OVA) にバンドルされています。インストールするためには、Carbon Black Cloud Workload アプライアンス OVA をダウンロードする必要があります。

VMware [Downloads (ダウンロード)] ページから Carbon Black Cloud Workload アプライアンス OVA をダウンロードできます。

手順

1 VMware Customer Connect ポータルにログインします。

Customer Connect プロファイルの作成については、KB 2007005 を参照してください。Customer Connect でアカウントにユーザーを招待する方法については、KB 2070555 を参照してください。

2 https://customerconnect.vmware.com/downloads の VMware ダウンロード ページにアクセスします。

3 [All Products (すべての製品)] ドロップダウン メニューから [Endpoint & Workload Security (エンドポイントとワークロードのセキュリティ)] を選択します。

4 OVA をローカル データストアまたはローカル Web サーバにダウンロードします。

OVA ファイル名は次の形式 (cwp-va-*<release-number>*-*<build-number>*_OVF10.ova) になります。たとえば、cwp-va-1.0.0.0-17066560_OVF10.ova です。

5 Carbon Black Cloud Workload アプライアンス OVA ファイルのファイル パスをコピーします。

たとえば、ローカル Web サーバに OVA ファイルをダウンロードした場合は、`http://<local-web-server>/cwp-va-1.0.0.0-17066560_OVF10.ova` となります。このパスは、アプライアンスの展開時に指定します。

結果

Carbon Black Cloud Workload アプライアンス OVA ファイルを使用できます。

次のステップ

Carbon Black Cloud Workload アプライアンス を展開して構成します。

Carbon Black Cloud にアクセスしています

Carbon Black Cloud に接続する必要があります。

Carbon Black Cloud サービスに登録する場合、またはサービスに招待された場合は、登録を確認する招待メールが届きます。この E メールには、Carbon Black Cloud コンソール アカウントのアクティブ化とセットアップに使用できるリンクと手順が記載されています。組織にすでに Carbon Black Cloud のインスタンスが確立されている場合は、ご使用の認証情報を使用してコンソールにログインするだけです。

招待メールが届かない、または Carbon Black Cloud サービスに関するサポートが必要な場合は、VMware Carbon Black サポート チーム (https://www.carbonblack.com/support/) にお問い合わせください。vSphere に関連するサポートが必要な場合は、VMware のサポート チーム (https://www.vmware.com/support/contacts.html) にお問い合わせください。

vSphere 環境での Carbon Black の有効化

3

Carbon Black Cloud Workload アプライアンス は、vCenter Server 環境内の任意の ESXi ホストに仮想アプライアンス（OVA ファイルとしてパッケージ化）として展開されます。アプライアンスを展開したら、アプライアンスを vCenter Server に登録する必要があります。次に、Carbon Black Cloud コンソールと vCenter Server に展開されたオンプレミス アプライアンス間の接続を確立するように アプライアンスを構成する必要があります。接続が確立されると、アプライアンスは仮想マシン インベントリ データを Carbon Black Cloud コンソールにインポートします。Windows 仮想マシンと Linux 仮想マシンで Carbon Black を有効にできます。

次のトピックを参照してください。

- ステップ 1: Carbon Black Cloud Workload アプライアンス の展開と構成
- Carbon Black Launcher を使用した仮想マシンの準備
- 手順 2: 仮想マシンで Carbon Black を有効にする

ステップ 1: Carbon Black Cloud Workload アプライアンス の展開と構成

Carbon Black Cloud Workload アプライアンス は vCenter Server とペアリングします。vCenter Server ごとに 1 つの Carbon Black Cloud Workload アプライアンス を展開する必要があります。

最初に Carbon Black Cloud Workload アプライアンス を展開し、アプライアンスを vCenter Server に登録します。アプライアンスを展開したら、API ID とキーを Carbon Black Cloud から生成する必要があります。

ここで Carbon Black Cloud Workload アプライアンス を構成し、Carbon Black Cloud Workload アプライアンス と Carbon Black Cloud の間を接続を確立します。

ステップ 1A: Carbon Black Cloud Workload アプライアンス を vCenter Server に展開する

管理クラスタに Carbon Black Cloud Workload アプライアンス オンプレミスを展開する必要があります。OVA ファイルを取得したら、vSphere Client を使用してアプライアンスを展開できます。

注： アプライアンス インターフェイスのアクセスを許可された管理者のみに制限するには、ネットワーク制御を実装する必要があります。アプライアンス インターフェイスへの無制限のネットワーク アクセスは必要ありません。

前提条件

- システム要件を確認します。
- Carbon Black Cloud Workload アプライアンス OVA ファイルが使用可能であることを確認します。詳細については、インストーラのダウンロード を参照してください。

手順

1. vSphere Client にログインします。
2. Carbon Black Cloud Workload アプライアンス をインストールするホストを右クリックし、[Deploy OVF Template (OVF テンプレートを展開)] をクリックします。
3. [Deploy OVF Template (OVF テンプレートを展開)] ページで、次の値を設定し、[Next (次へ)] をクリックします。

オプション	説明
[OVF テンプレートを選択]	■ [URL]: リモート Web サーバに Carbon Black Cloud Workload アプライアンス [URL] を入力します。サポートされる URL ソースは HTTP および HTTPS です。 例: `http://<local-web-server>/cwp-va-1.0.0.0-17066560_OVF10.ova`. ■ [ローカル ファイル]: [Choose Files (ファイルを選択)] をクリックし、ダウンロードした OVA ファイルを選択します。
[名前とフォルダを選択]	(オプション) OVA ファイルの名前を [Workload Appliance] に変更します。
[コンピューティング リソースを選択]	(オプション) 選択したホストが、Carbon Black Cloud Workload アプライアンス を展開する適切なリソースかどうかを確認します。
[詳細を確認]	詳細を確認します。製品は、[CBC Workload Appliance VA] である必要があります。
[使用許諾契約]	VMware の使用許諾契約を受け入れるには、「[すべての使用許諾契約を受け入れる]」をクリックします。
[ストレージを選択]	展開された OVA のファイルの保存方法を選択します。 展開された OVF または OVA テンプレートを保存するデータストアを選択します。構成ファイルと仮想ディスク ファイルはデータストアに保存されます。仮想マシンまたは vApp および関連付けられているすべての仮想ディスク ファイルを収容するのに十分な大きさのデータストアを選択します。
[ネットワークを選択]	vCenter Server に接続するネットワークを選択します。 [IP アドレスの割り当て設定]: [IP プロトコル]を [IPv4] または [IPv6] として選択します。

オプション	説明
[テンプレートのカスタマイズ]	a [アプリケーション]: ■ *admin* および *root* ユーザー アカウントのパスワードを入力し、パスワードの長さが文字数の要件を満たしていることを確認します。これらのパスワードは、後で vCenter Server に登録する場合に必要です。 パスワードは次の要件を満たしている必要があります。 ■ 8 文字以上 ■ 1 文字以上の小文字 ■ 1 文字以上の数字 ■ 1 文字以上の特殊文字 ■ 20 文字未満 b [ネットワーク プロパティ]: ■ アプライアンスの構成中に DHCP を使用可能にする場合は、設定値を空のままにします。 ■ 固定 IP アドレスを設定する場合: ■ ドメイン名とドメイン検索パス: 仮想マシンのホスト名。たとえば、**`host.example.local`** の場合、ドメイン名フィールドに **`host`** と入力し、ドメイン検索パス フィールドに **`example.local`** と入力します。 ■ ネットワーク管理者に問い合わせて、次の必須の値を追加します: デフォルト ゲートウェイ、ドメイン名サーバ、ネットワーク 1 IP アドレス、ネットワーク 1 ネットマスク。
[設定内容の確認]	詳細を確認し、[Finish (終了)] をクリックします。

OVA のインポートと展開が開始されます。パブリック ネットワークのダウンロード速度によっては、時間がかかる場合があります。

4 展開が完了したら、Carbon Black Cloud Workload アプライアンス の仮想マシン (VM) に移動し、パワーオンします。

デフォルトで、Carbon Black Cloud Workload アプライアンス のタイム ゾーンは UTC であり、変更できません。

5 Carbon Black Cloud Workload アプライアンス の IP アドレスをメモします。

結果

Carbon Black Cloud Workload アプライアンス が展開されます。

次のステップ

アプライアンスを vCenter Server に登録します。

手順 1B: Carbon Black Cloud Workload アプライアンスを vCenter Server に登録するオプション

Carbon Black Cloud Workload アプライアンス を展開したら、アプライアンスを vCenter Server に登録します。オンプレミスの vCenter Server または VMware Cloud on AWS Software-Defined Data Center (SDDC) のいずれかに登録できます。

オンプレミスの vCenter Server にアプライアンスを登録

Carbon Black Cloud Workload アプライアンス を展開したら、新しいアプライアンスをオンプレミスの vCenter Server に登録できます。

前提条件

- Carbon Black Cloud Workload アプライアンス を展開しました。
- Carbon Black Cloud Workload アプライアンス の仮想マシンがパワーオン状態です。
- アプライアンスには、vCenter Server と通信するための HTTPS (443) 接続が必要です。

手順

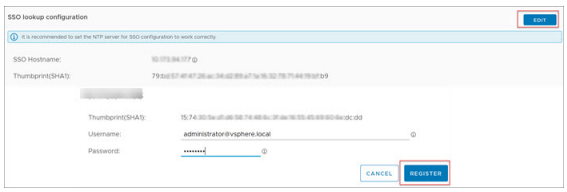
1 ブラウザから、**admin** 認証情報を使用して Carbon Black Cloud Workload アプライアンス (`https://<appliance IP address>`) にログインします。

アプライアンス ダッシュボードがデフォルトのホーム ページとして表示されます。

2 [Appliance (アプライアンス)] - [Registration (登録)] ページに移動します。

3 「[SSO ルックアップ設定]」セクションで、[Edit (編集)] をクリックし、次の値を設定します。

重要: Carbon Black Cloud Workload アプライアンス と vCenter Single Sign-On サーバの時刻を同期する必要があります。SSO サーバの時刻と Carbon Black Cloud Workload アプライアンス の時刻が同期するように NTP サーバを指定する必要があります。詳細については、NTP サーバ設定の構成 を参照してください。



SSO ルックアップ設定	説明
SSO ホスト名	vCenter Single Sign-On (SSO) の IP アドレスまたは FQDN を入力し、[Register (登録)] をクリックします。 SSO サーバと Carbon Black Cloud Workload アプライアンス の時刻を同期する必要があります。 **注:** Carbon Black Cloud Workload アプライアンス は、サービス アカウントを使用して vCenter Server とやり取りします。このサービス アカウントは、セキュリティと管理性を向上するために SSO サーバで作成されます。このサービス アカウントを作成するには、SSO 管理者の認証情報が必要です。SSO 管理者の認証情報は、このセッションにのみ使用され、Carbon Black Cloud では保持されません。
ユーザー名とパスワード	vCenter SSO 管理者のユーザー名とパスワードを入力します。vCenter SSO 管理者グループにメンバーを追加するには、vSphere のドキュメントを参照してください。
VMware Cloud on AWS	デフォルトで、トグルスイッチはオフになっています。設定を変更しないでください。
サムプリント (SHA1)	SSO サーバの SHA1 サムプリントを確認します。

4 「[vCenter Server の詳細]」セクションで [Register (登録)] をクリックし、次の値を設定します。

vCenter Server の詳細	説明
vCenter Server のホスト名	リストから必要な vCenter Server のホスト名を選択します。vCenter Server ごとに 1 つの Carbon Black Cloud Workload アプライアンス をインストールできます。
プラグイン	登録が完了したら、登録された Carbon Black Cloud Workload Plug-in のバージョンが使用可能になります。
サムプリント (SHA256)	vCenter Server の SHA256 サムプリントを確認します。

5 [Register (登録)] をクリックします。

6 変更を反映するには、Carbon Black Cloud Workload アプライアンス からログアウトし、Carbon Black Cloud Workload アプライアンス の登録に使用したのと同じ*管理者*ロールで再度 vCenter Server にログインします。

または、vSphere Client ブラウザを更新します。

結果

アプライアンスを vCenter Server に正常に登録しました。

Carbon Black Cloud Workload Plug-in は、vCenter Server に表示されます。Carbon Black アイコンが、左側のナビゲーション ペインと vSphere Client の [ショートカット] メニューに表示されます。

次のステップ

Carbon Black Cloud コンソールに移動し、API ID とプライベート キーを生成します。

VMware Cloud on AWS SDDC 内の vCenter Server への Carbon Black Cloud Workload アプライアンスの登録

Carbon Black Cloud Workload アプライアンス を展開したら、アプライアンスを VMware Cloud on AWS Software-Defined Data Center (SDDC) で使用可能な vCenter Server に登録できます。

前提条件

- Carbon Black Cloud Workload アプライアンス を展開しました。
- Carbon Black Cloud Workload アプライアンス の仮想マシンがパワーオン状態です。
- SDDC は、VMware Cloud on AWS で展開され構成されます。
- SDDC でファイアウォール ルールを構成します。詳細については、SDDC で必要なファイアウォール ルールを参照してください。
- アプライアンス IP アドレスの NAT ルールを構成します。詳細については、アプライアンス IP アドレスの NAT ルールの作成 を参照してください。

手順

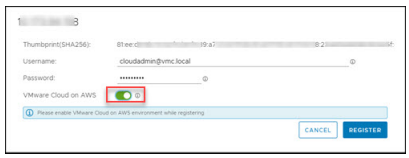
1 ブラウザから、**admin** 認証情報を使用して Carbon Black Cloud Workload アプライアンス (`https://<appliance IP address>`) にログインします。

アプライアンス ダッシュボードがデフォルトのホーム ページとして表示されます。

2 [Appliance (アプライアンス)] - [Registration (登録)] ページに移動します。

3 「[SSO ルックアップ設定]」セクションで、[Edit (編集)] をクリックし、次の値を設定します。

重要: Carbon Black Cloud Workload アプライアンス と vCenter Single Sign-On サーバの時刻を同期する必要があります。SSO サーバの時刻と Carbon Black Cloud Workload アプライアンス の時刻が同期するように NTP サーバを指定する必要があります。詳細については、NTP サーバ設定の構成 を参照してください。

SSO ルックアップ設定	説明
SSO ホスト名	vCenter Single Sign-On (SSO) インスタンスの IP アドレスまたは FQDN を入力し、[Register (登録)] をクリックします。 VMC URL は [SDDCs] - [Settings (設定)]の vmc.vmware.com に記載されています。例: **`vcenter.sddc-x-x-x-x.vmwarevmc.com`***https://* ヘッダーを入力しないでください。 SSO サーバと Carbon Black Cloud Workload アプライアンス の時刻を同期する必要があります。
VMware Cloud on AWS	VMware Cloud on AWS 環境をオンに切り替えます。 
ユーザー名とパスワード	VMware Cloud on AWS の vSphere 管理用のユーザー名とパスワードを入力します。例: **`cloudadmin@vmc.local`**.
サムプリント (SHA1)	SSO サーバの SHA1 サムプリントを確認します。

4 「[vCenter Server の詳細]」セクションで [Register (登録)] をクリックし、次の値を設定します。

vCenter Server の詳細	説明
vCenter Server のホスト名	リストから必要な vCenter Server のホスト名を選択します。vCenter Server ごとに 1 つの Carbon Black Cloud Workload アプライアンス をインストールできます。
プラグイン	登録が完了したら、登録された Carbon Black Cloud Workload Plug-in のバージョンが使用可能になります。
サムプリント (SHA256)	vCenter Server の SHA256 サムプリントを確認します。

5 [Register (登録)] をクリックします。

アプライアンスは、VMware Cloud on AWS SDDC 内の vCenter Server に登録されます。

結果

Carbon Black Cloud Workload アプライアンス からログアウトし、登録時に使用したのと同じ *Cloud Admin* ロールで、SDDC から vCenter Server にログインします。

正常に登録されると、vCenter Server に Carbon Black Cloud Workload Plug-in を表示できます。Carbon Black  アイコンが、左側のナビゲーション ペインと vSphere Client の [ショートカット] メニューに表示されます。

次のステップ

Carbon Black Cloud コンソールに移動し、API ID とプライベート キーを生成します。

SDDC で必要なファイアウォール ルール

SDDC を VMware Cloud on AWS で展開し構成したら、安全な通信のためのファイアウォール ルールを構成する必要があります。

1 VMC コンソールにログインします。

2 [Networking & Security (ネットワークとセキュリティ)] タブで、[Gateway Firewall (ゲートウェイ ファイアウォール)] をクリックします。

3 必要なタブに移動し、次のファイアウォール ルールが構成されていることを確認します。

ファイアウォール ルール	送信元	宛先	サービス/適用先
[Management Gateway (管理ゲートウェイ)] タブに移動し、アプライアンスが HTTPS 経由で vCenter Server と通信できる受信ルールを追加します。	任意またはアプライアンスの IP アドレス	vCenter Server	HTTPS
[Management Gateway (管理ゲートウェイ)] タブに移動し、vCenter Server がアプライアンスと通信できる送信ルールを追加します。	vCenter Server	任意またはアプライアンスの IP アドレス	任意
[Compute Gateway (コンピューティング ゲートウェイ)] タブに移動し、アプライアンスと仮想マシンが Carbon Black Cloud と通信できるアップリンク ルールを追加します。	任意	任意	任意

注： 組織のネットワーク設定に基づいて、特定の URL のルールの範囲を狭めることができます。アプライアンスが Carbon Black Cloud と外部接続していることを確認します。

アプライアンス IP アドレスの NAT ルールの作成

Carbon Black Cloud Workload アプライアンス を展開したら、アプライアンスの IP アドレスは、SDDC ネットワーク内からのみアクセス可能なプライベート IP アドレスになります。IP アドレスに安全にアクセスするには、

アプライアンスのパブリックにアクセス可能な IP アドレスを生成し、ネットワーク アドレス変換 (NAT) を使用して、パブリック IP アドレスをアプライアンスのプライベート IP アドレスでマッピングする必要があります。

1 VMC コンソールにログインします。

2 [Networking & Security (ネットワークとセキュリティ)] タブで、[パブリック IP アドレス]をクリックします。

3 パブリック アクセスが可能なアプライアンスの IP アドレスを生成します。パブリック IP アドレスを要求または解放するには、「VMware Cloud on AWS のネットワークとセキュリティ」のドキュメントを参照してください。

4 NAT ルールを作成し、新しいパブリック IP アドレスをアプライアンスのプライベート IP アドレスでマッピングします。

NAT ルール	パブリック IP アドレス	サービス	パブリックおよび内部ポート	内部 IP アドレス	ファイアウォール
NAT ルールに任意の名前を付ける	以前に生成されたパブリック IP アドレスを追加	すべてのトラフィック	任意	Carbon Black Cloud Workload アプライアンス の IP アドレスを追加	内部アドレスと一致

NAT ルールを作成または変更するには、「VMware Cloud on AWS のネットワークとセキュリティ」を参照してください。

手順 1C：API ID と API プライベート キーの生成

Carbon Black Cloud コンソールから API キーを生成し、生成された API キーを使用して、vCenter Server に展開された Carbon Black Cloud コンソールと Carbon Black Cloud Workload アプライアンス の間の接続を確立する必要があります。vCenter Server ごとに 1 台のアプライアンスを構成できます。組織に対して複数のアプライアンスを構成できます。複数のアプライアンスを設定している場合、各アプライアンスに個別の API キーを生成します。

アプライアンスを展開したら、事前定義されたカスタム アクセス レベルを使用して、そのアプライアンスの API キーを生成します。同じカスタム アクセス レベルを使用して、組織に複数のアプライアンスを構成できます。

前提条件

- vCenter Server で Carbon Black Cloud Workload アプライアンス を展開していることを確認します。詳細については、ステップ 1A: Carbon Black Cloud Workload アプライアンス を vCenter Server に展開する を参照してください。
- 組織内のアプライアンスには、`CWP Appliance` カスタム アクセス レベルを使用します。バージョン 1.2 以降では、アプライアンスに事前定義されたカスタム アクセス レベルは、必要なすべての権限を保持します。

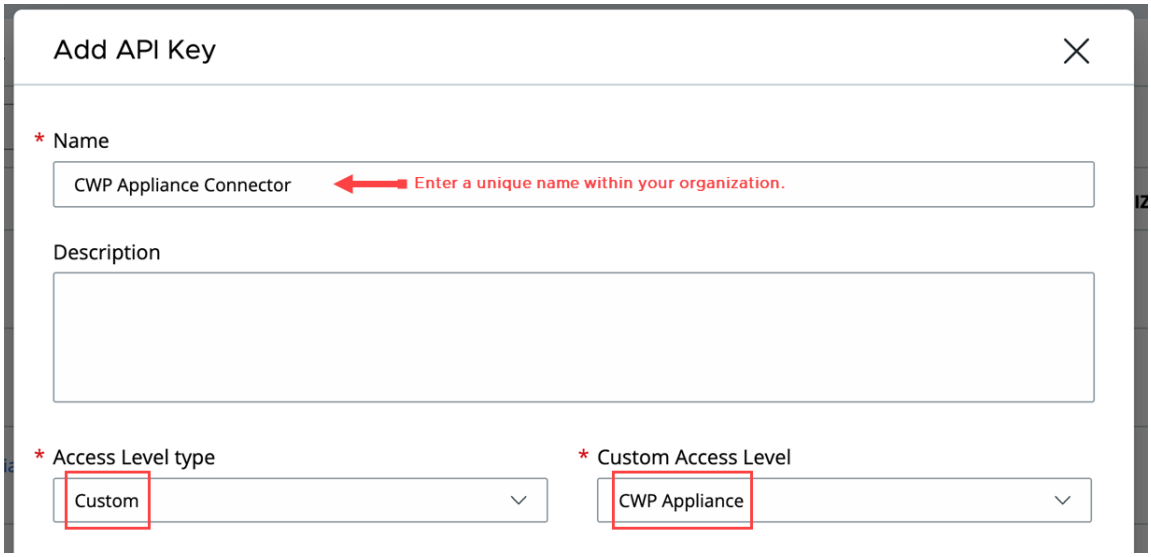
手順

1 Carbon Black Cloud コンソールにログインします。

2 左側のナビゲーション ペインで、[設定] - [API アクセス] 画面に移動します。

3 [API キー] タブを選択し、[API キーを追加] をクリックします。

[API キーを追加] ウィンドウが表示されます。



4 アプライアンス API キーの名前を入力します。名前は Carbon Black Cloud 組織において一意である必要があります。

5 [アクセス レベル タイプ] ドロップダウン メニューから [カスタム] を選択します。

6 [カスタム アクセス レベル] ドロップダウン メニューから、アプライアンスの `CWP Appliance` カスタム アクセス レベルを見つけて選択します。

7 [保存] をクリックします。

Carbon Black Cloud コンソールは、API ID と API プライベート キーを生成します。

8 両方のキーをコピーします。

後でこれらのキーを使用して、アプライアンスと Carbon Black Cloud コンソールの間の接続を確立します。

注： アプライアンスごとに使用できる API ID とプライベート キーは 1 つだけです。アプライアンスに生成された API ID とプライベート キーを使用すると、他のアプライアンスに同じ API ID とプライベート キーを使用できなくなります。

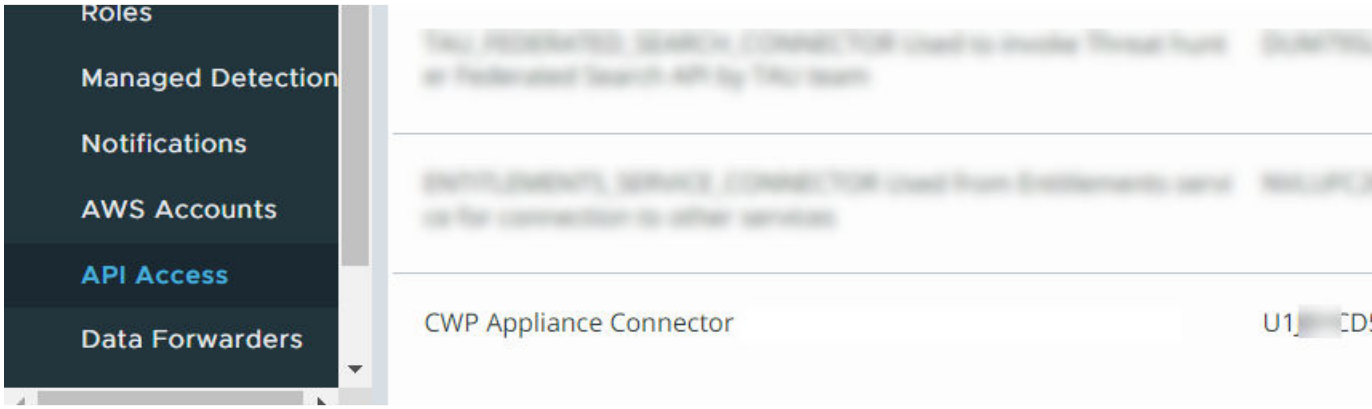
次のステップ

キーを使用して Carbon Black Cloud Workload アプライアンス と Carbon Black Cloud コンソールの間の Carbon Black Cloud Workload アプライアンスを Carbon Black Cloud に接続する します。

後でキーを表示してコピーする場合は、次の手順を実行します。

1 [設定] - [API アクセス] - [API キー] タブに移動します。

2 前に作成したアプライアンス API 名に移動し、編集アイコンの横にある下矢印をクリックします。



3 [API の認証情報] をクリックします。

[API の認証情報] ダイアログ ボックスが表示されます。キーをコピーします。

手順 1D: Carbon Black Cloud Workload アプライアンスを Carbon Black Cloud に登録する

Carbon Black Cloud Workload アプライアンス を vCenter Server に登録し、認証情報を生成したら、アプライアンスを Carbon Black Cloud に登録できます。

Carbon Black Cloud Workload アプライアンスを Carbon Black Cloud に接続する

Carbon Black Cloud コンソールから認証情報を生成したら、Carbon Black Cloud Workload アプライアンスを構成して Carbon Black Cloud との接続を確立します。

前提条件

- Carbon Black Cloud Workload アプライアンス 仮想マシンがパワーオン状態であることを確認します。
- API キー が Carbon Black Cloud コンソールから生成され、コピーされていることを確認します。詳細については、手順 1C：API ID と API プライベート キーの生成 を参照してください。

- アプライアンスには、vCenter Server および Carbon Black Cloud と通信するための HTTPS (443) 接続が必要です。

手順

1 vSphere Client にログインします。

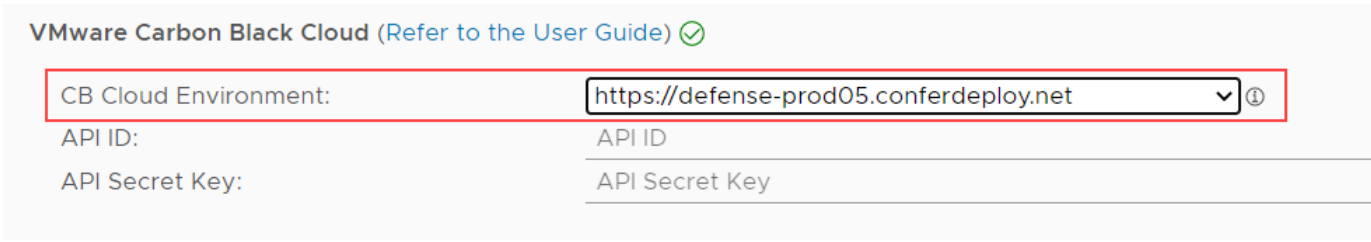
2 Carbon Black Cloud Workload アプライアンス 仮想マシンがパワーオン状態であることを確認するには、仮想マシン コンソールを開き、アプライアンスの IP アドレスを書き留めます。

3 ブラウザから、**admin** 認証情報を使用して Carbon Black Cloud Workload アプライアンス (**https://<appliance IP address>**) にログインします。

4 [アプライアンス] - [登録] 画面に移動します。

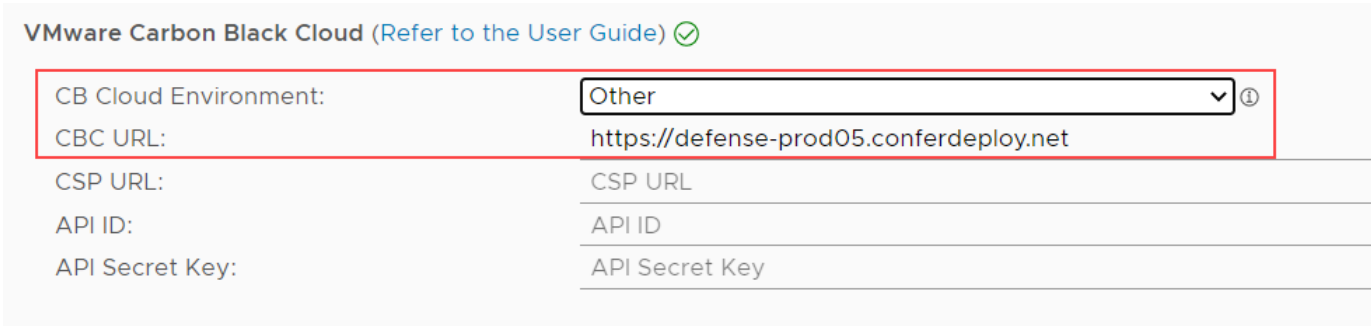
5 Carbon Black Cloud セクションで、[編集] をクリックします。

6 [CB クラウド環境] ドロップダウン メニューから Carbon Black Cloud 環境を選択します。



7 オプション。Carbon Black Cloud 環境が表示されない場合は、[CB クラウド環境] ドロップダウン メニューから [その他] を選択し、[CBC URL] を入力します。

現在、VMware Cloud services は Carbon Black Cloud Workload アプライアンス に統合されています。したがって、[CSP URL] の指定は必須ではありません。



8 次の必須の値を設定します。

a [CB クラウド環境]: ホストされている Carbon Black Cloud の場所に従って Carbon Black Cloud コンソール URL を入力します。

b API ID：Carbon Black Cloud コンソールからコピーした 10 桁の *API ID* を貼付けます。

c API プライベート キー：Carbon Black Cloud コンソールからコピーした *API プライベート キー* を貼付けます。

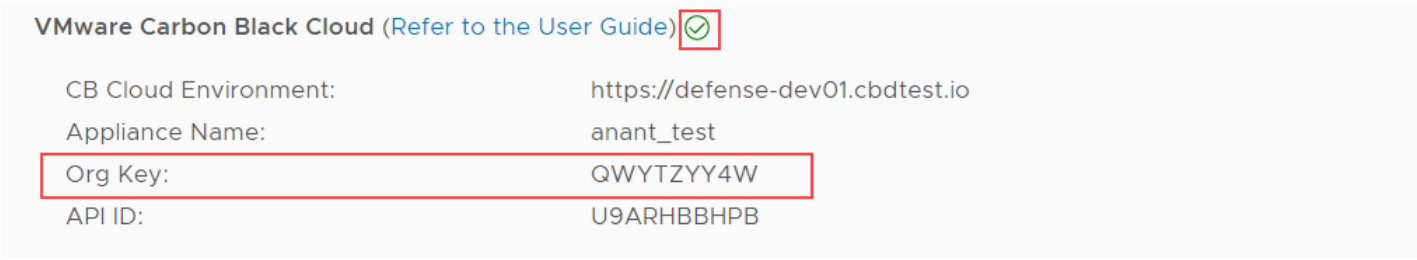
9 [保存] をクリックします。

結果

緑のチェック マークが表示されている場合、vCenter Server、Carbon Black Cloud Workload アプライアンス、および Carbon Black Cloud の間の接続が確立されています。

登録に成功した後:

- 登録済みの Carbon Black Cloud Workload アプライアンス がバージョン 1.2 の場合、組織キーが表示されます。
- 登録済みの Carbon Black Cloud Workload アプライアンス がバージョン 1.1 の場合、組織名が表示されます。
- 登録済みの Carbon Black Cloud Workload アプライアンス がバージョン 1.1 より前の場合、組織キーが表示されます。



次のステップ

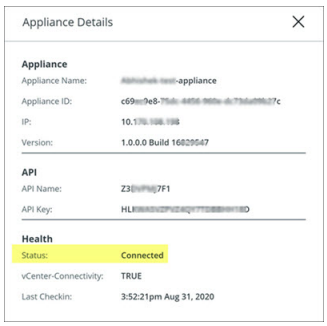
接続が正常に確立されると、データを vCenter Server の Carbon Black Cloud Workload Plug-in に表示できます。左側のナビゲーション ペインで Carbon Black アイコンをクリックすると、[サマリ] タブにアプライアンスの健全性とインベントリのステータスが表示されます。

接続の確認

Carbon Black Cloud Workload アプライアンス と Carbon Black Cloud の間の接続が正常に確立されたかどうかを確認します。

手順

1. Carbon Black Cloud コンソールにログインします。
2. 左側のナビゲーション ペインから、[Settings (設定)] - [API Access (API アクセス)] - [API Keys (API キー)] ページの順にクリックします。
3. アプライアンス API に移動します。アプライアンスの API 名の横にリンクが付いたアプライアンス名が表示されます。
4. リンク付きアプライアンス名をクリックします。アプライアンスの健全性と接続ステータスを表示できます。



5. [Inventory (インベントリ)] - [Workloads (ワークロード)] - [Not Enabled (無効)] ページの順に移動します。仮想マシン (VM) データを表示できます。

6 次の `curl` コマンドを使用して接続を確認することもできます。

```
curl -v telnet://<carbonblack_prod_url>:443
* Rebuilt URL to: <carbonblack_prod_url>:443/
* Trying xx.00.xx.x...
* TCP_NODELAY set
* Connected to carbonblack_prod_url (xx.00.xx.x) port 443 (#0)
```

```
curl -v telnet://<vcsa_on_vc>:443
* Rebuilt URL to: telnet://<vcsa_on_vc>:443/
* Trying xx.0.0.xx...
* TCP_NODELAY set
* Connected to vcsa_on_vc (xx.0.0.xx) port 443 (#0)
```

結果

接続が確立されると、トラブルシューティング ログが VMware と共有されます。

次のステップ

オプトアウトするには、[Troubleshooting (トラブルシューティング)] - [Logs (ログ)] ページに移動し、ログ エクスポート機能をオフに切り替えます。詳細については、アプライアンスのログ を参照してください。

インベントリの表示

アプライアンスがクラウドに正常に接続されると、インベントリを Carbon Black Cloud Workload Plug-in および Carbon Black Cloud コンソールに表示できます。

手順

1 Carbon Black Cloud Workload Plug-in にインベントリを表示します。

   a vCenter Server の Carbon Black Cloud Workload Plug-in に移動します。

   b [Inventory (インベントリ)] - [Not Enabled (無効)] タブに移動します。

   c ワークロードを保護するには、手順 2: 仮想マシンで Carbon Black を有効にする 。

2 インベントリを Carbon Black Cloud コンソールに表示します。

   a 左側のナビゲーション ペインで、[Inventory (インベントリ)] - [Workloads (ワークロード)] - [Not Enabled (無効)] タブに移動します。

   b [Not Enabled (無効)] タブを更新します。

   仮想インベントリは、アプライアンスを接続してから数分以内に表示されます。

手順 1E: Carbon Black Cloud Workload アプライアンスを NSX-T に登録する

Carbon Black Cloud Workload アプライアンス を vCenter Server と Carbon Black Cloud に登録したら、NSX 統合を Carbon Black Cloud 組織に登録できます。

これは、Carbon Black Cloud Workload アプライアンス と NSX Manager アプライアンスの間の信頼を設定するオンボーディング ワークフローです。オンボーディングが完了すると、Carbon Black Cloud Workload アプライアンス は、Carbon Black Cloud が使用する 1 つ以上の事前定義済み分散ファイアウォール (DFW) ポリシー テンプレートを作成し、初期認証および構成プロセスの一部としてインスタンスを作成します。次の NSX DFW ポリシーと関連タグを作成します。

- `CB-NSX-Quarantine` – このポリシーでは、仮想マシンのワークロードがネットワークから隔離されます。これは、NSX 管理者向けの読み取り専用ポリシーです。このポリシーでは、次のネットワーク フローが許可されます。
  - IP アドレスの DHCP と名前解決のための DNS トラフィック。
  - Carbon Black Cloud への接続を維持するためにセンサーが必要とする FQDN のリストへの HTTPS トラフィック。
- `CB-NSX-Isolate` – このポリシーでは、仮想マシンのワークロードがネットワークから完全に隔離されます。これは、NSX 管理者向けの読み取り専用ポリシーです。
- `CB-NSX-Custom` – NSX セキュリティ管理者がカスタマイズ可能。上級ユーザーは、このようなポリシーを使用してカスタム セキュリティ体制を作成できます。

NSX-T 統合の後に、新しく作成した NSX ポリシーを使用して、Carbon Black Cloud コンソール内の仮想マシン ワークロードを修正したり、すでに適用されている NSX ポリシーを特定の仮想マシン ワークロードから削除したりできます。

前提条件

- Carbon Black Cloud Workload アプライアンス 仮想マシンがパワーオン状態であることを確認します。
- SSO 登録が有効であることを確認します。
- Carbon Black Cloud Workload アプライアンス には、vCenter Server と Carbon Black Cloud の両方の有効な登録が必要です。
- Carbon Black Cloud と Carbon Black Cloud Workload アプライアンス の間の通信は HTTPS 経由です。
- NSX と Carbon Black Cloud Workload アプライアンス の間の通信は HTTPS 経由で行われ、NSX プリンシパル ID を使用した証明書ベースの認証が使用されます。ロール割り当てまたはプリンシパル ID の追加については、「VMware NSX-T Data Center 製品ドキュメント」を参照してください。
- サポートされている NSX-T バージョンは 3.1.3 以降です。

手順

1. **admin** 認証情報を使用して Carbon Black Cloud Workload アプライアンス (**https://<appliance IP address>**) にログインします。
2. [Appliance (アプライアンス)] - [Registration (登録)] ページに移動します。
3. [NSX details (NSX の詳細)] セクションで、[NSX hostname (NSX ホスト名)] ドロップダウン メニューから NSX Manager の IP アドレスを選択します。

   [Register (登録)] ボタンがアクティブになります。

4 NSX のオンボーディングをトリガするには、[Register (登録)] をクリックします。

5 NSX 管理者ユーザーとパスワードを入力し、[Register (登録)] をクリックします。

NSX がオンボーディングされると、緑色のチェック マークが正常に登録されたことを示します。プロセスが完了するまでに最大 15 秒かかる場合があります。

6 すべてのオブジェクトが NSX Manager に作成されていることを確認します。

a **admin** 認証情報を使用して NSX Manager にログインします。

b [Inventory (インベントリ)] - [Groups (グループ)] ページに移動し、次のグループが存在するかどうかを確認します。

- CB-NSX-Custom-Group
- CB-NSX-Isolate-Group
- CB-NSX-Quarantine-Group

c [Security (セキュリティ)] - [Distributed Firewalls (分散ファイアウォール)] - [CATEGORY SPECIFIC RULES (カテゴリ固有のルール)] ページに移動して、次のデフォルト ポリシーが存在するかどうかを確認します。

- CB-NSX-Custom
- CB-NSX-Isolate
- CB-NSX-Quarantine

d [Inventory (インベントリ)] - [Context Profiles (コンテキスト プロファイル)] - [Context Profiles (コンテキスト プロファイル)] ページに移動し、CB-NSX-Quarantine-Context-Profile が有効な FQDN で存在するかどうかを確認します。

次のステップ

NSX のオフボーディング プロセスをトリガするには、 を選択してオフボーディングを確認します。

Carbon Black Launcher を使用した仮想マシンの準備

ワンクリックで簡単に展開して、データセンターで Carbon Black を有効にできます。展開作業を最小限に抑えるため、VMware Tools で軽量な Carbon Black ランチャ を使用できます。Carbon Black ランチャ は、Windows および Linux 仮想マシンで使用できる必要があります。

Carbon Black Cloud Workload Plug-in から Carbon Black を有効にすると、ランチャが仮想マシンに Carbon Black センサーをダウンロードしてインストールする場合に、サイレント インストールがトリガされます。インストール プロセスでは、特定のプラットフォームでサポートされている適切なコンポーネントをインストールします。

Carbon Black ランチャ は、次のように Windows 仮想マシンと Linux 仮想マシンで使用できます。

- [Windows 仮想マシン]: Windows 仮想マシンの場合、Carbon Black ランチャ は VMware Tools に含まれています。

ワークロードのランチャを受け取るには、VMware Tools をインストールするか、バージョン 11.2 以降 にアップグレードする必要があります。

- [Linux 仮想マシン] : Linux 仮想マシンの場合、VMware Tools Operating System Specific Packages (OSPs) で入手できるランチャを手動でインストールする必要があります。

  http://packages.vmware.com/ のパッケージ リポジトリから、ゲスト オペレーティング システム用の Carbon Black ランチャ をダウンロードしてインストールします。詳細については、Linux 仮想マシン用 Carbon Black Launcher を参照してください。

ランチャが使用可能になったら、Carbon Black Cloud Workload Plug-in から Carbon Black の有効化を進めることができます。

Carbon Black Windows 仮想マシン用のランチャ

Windows 仮想マシンの場合、Carbon Black ランチャ は VMware Tools に含まれています。ワークロードのランチャを受け取るには、VMware Tools をインストールするか、バージョン 11.2 以降 にアップグレードする必要があります。

詳細については、VMware Tools のドキュメント を参照してください。

重要： 仮想マシンにはインターネット接続が必要です。

ランチャ ログは次の場所にあります。

- ESXi ホスト: VMware Tools をインストールするか、バージョン 11.2 以降 にアップグレードする場合、ログファイルは `/vmfs/volumes/datastore_name/VM_NAME/vmware.log` にあります。
- Windows 仮想マシン: Carbon Black のインストールをトリガする場合、ログは `C:\Windows\Temp\Cbinstall*.log` または `SystemTemp\Cbinstall*.log` で作成されます。
- Windows 仮想マシン: Carbon Black のインストールが完了すると、ログは `C:\Windows\Temp\cb-install*.log` または `SystemTemp\Cb-install*.log` で作成されます。

Linux 仮想マシン用 Carbon Black Launcher

ワークロードが実行されているゲスト Linux 仮想マシン (VM) で Carbon Black を有効にするには、まず、VMware パッケージ リポジトリを使用して Carbon Black ランチャ をインストールする必要があります。Linux 仮想マシン (または仮想マシンにバイナリを提供するために使用されるサーバ) は、*https://packages.vmware.com* サイトにアクセスできる必要があります。

これは、インストールの推奨方法です。Linux ディストリビューションに適用できる場合は手順を実行します。Linux 仮想マシンの *root* 権限が必要です。

前提条件

- Linux 仮想マシン (または仮想マシンにバイナリを提供するために使用されるサーバ) は、https://packages.vmware.com にアクセスできる必要があります。*packages.vmware.com* へのアクセシビリティを確認するには、`ping packages.vmware.com` コマンドを使用します。次に `curl -Is https://packages.vmware.com/cb/cblauncher` コマンドを実行します。curl 要求は、`HTTP/1.1 200 OK` ステータス コードを返します。

- Linux 仮想マシンに次の依存関係をインストールする必要があります。
  - *libglib-2.0*
  - *libgthread*
  - *gnupg2*
- Linux 仮想マシン用 Carbon Black ランチャ 1.3 以降を使用し、カスタム構成の場合にアップロードできるオプションのセンサー構成ファイルと一緒に、Carbon Black センサー キット バージョン 2.13 以降をインストールします。Carbon Black ランチャ 1.3 では、Linux センサー キット バージョン 2.13 以降でのカスタム構成のサポートが導入されています。
- Linux 仮想マシン用 Carbon Black ランチャ 1.1 以降を使用してバージョン 2.11.2 以降の Carbon Black センサー キットをインストールします。Carbon Black ランチャ 1.1 では、センサー キット 2.11.2 以降に含まれるすべてのファイルに対して完全なデジタル署名検証が適用されます。
  - Carbon Black センサー バージョン 2.11.2 以降では、tar-ball は完全な署名検証で有効になっています。Carbon Black ランチャ 1.1 以降を使用して 2.11.2 より前のバージョンの Carbon Black センサー キットをダウンロードしてインストールする場合、センサー キットで署名検証機能が有効にならず、署名の検証に失敗するためセンサーのインストールを完了できません。
  - Carbon Black ランチャ 1.0 以前を使用して Carbon Black センサー キット 2.11.2 以降をインストールすると、Launcher は完全な検証なしでセンサーをインストールします。

手順

1 [Ubuntu システムの場合]:

a 次のコマンドを使用して、VMware パッケージ パブリック キーを取得してインポートします。

```
curl -L https://packages.vmware.com/cb/cblauncher/key/VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-KEY.pub --output VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-KEY.pub
```

```
apt-key add VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-KEY.pub
```

b `/etc/apt/sources.list.d` の下に *cblauncher.list* という名前のファイルを作成します。

c 次のコンテンツで `/etc/apt/sources.list.d/cblauncher.list` を作成または編集します。

```
deb [arch=amd64] https://packages.vmware.com/cb/cblauncher/latest/ubuntu xenial main
```

d 次のコマンドを使用してパッケージをインストールします。

```
apt-get update
apt-get install cblauncher
```

2 [RHEL/CentOS/Oracle/Amazon Linux システムの場合]:

a 次のコマンドを使用して、VMware パッケージ パブリック キーを取得してインポートします。

```
wget https://packages.vmware.com/cb/cblauncher/key/VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-KEY.pub

rpm --import VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-KEY.pub
```

b `/etc/yum.repos.d` の下に *cblauncher.repo* という名前のファイルを作成します。

c 次のコンテンツで `/etc/yum.repos.d/cblauncher.repo` ファイルを編集します。

```
[repo-cblauncher]
name=cblauncher repo
baseurl=https://packages.vmware.com/cb/cblauncher/latest/
enabled=1
gpgcheck=1
```

d 次のコマンドを使用して Carbon Black ランチャ パッケージをインストールします。

```
yum install cblauncher
```

3 [SLES システムの場合]:

a 次のコマンドを使用して、VMware パッケージ パブリック キーを取得してインポートします。

```
wget https://packages.vmware.com/cb/cblauncher/key/VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-KEY.pub

rpm --import VMWARE-CBLAUNCHER-PACKAGING-GPG-RSA-KEY.pub
```

b 次のリポジトリを追加します。

```
zypper ar "https://packages.vmware.com/cb/cblauncher/latest/" cblauncher
```

c 次のコマンドを使用して Carbon Black ランチャ パッケージをインストールします。

```
zypper install cblauncher
```

4 Carbon Black ランチャ がインストールされているかどうかを確認するには、Linux ディストリビューションに基づく root 権限で次のコマンドを実行します。

- CentOS/RHEL/Oracle 6.x の場合は、次のコマンドを使用します。

```
service cblauncher status
```

- SUSE/Ubuntu/Amazon などの他のすべてのディストリビューションでは、次のコマンドを使用します。

```
systemctl status cblauncher
```

ステータスは実行中である必要があります。

結果

Launcher をインストールしたら、Carbon Black Cloud Workload Plug-in の Windows 仮想マシンと同様に、Linux 仮想マシンで Carbon Black を有効にすることができます。

Linux 仮想マシンに Launcher をインストールする代替方法

ワークロードが実行されている Linux 仮想マシン (VM) で Carbon Black ランチャ を有効にするには、最初に Launcher をインストールする必要があります。このインストール方法は、代替方法です。リポジトリを構成しない場合は、この代替方法を使用できます。

Linux ディストリビューションに該当する手順を実行します。

1 Linux 仮想マシンに移動します。

2 パッケージをダウンロードし、適切な Linux ディストリビューションのコマンドを実行します。

注： 実際のビルド番号は変更される場合があります。ビルド番号を使用可能な正しい番号に置き換える必要があります。たとえば、cblauncher-1.0.0-*16928845*.x86_64 の 16928845 を使用可能なビルド番号に置き換えます。

表 3-1. インストールに使用する Linux パッケージとコマンド

Linux ディストリビューション	パッケージをダウンロードするためのリンク	インストールに使用するコマンド
[Ubuntu]	1 `https://packages.vmware.com/cb/cblauncher` に移動します。 2 特定のバージョンを選択するか、[最新]のバージョンをクリックします。 3 [ubuntu /] をクリックし、`cblauncher_[version]-[build-number]_amd64.deb` パッケージに移動します。	■ `dpkg -i cblauncher_[version]-[build number]_amd64.deb` 例: `dpkg -i cblauncher_1.0.0-16928845_amd64.deb`
[RHEL/SUSE/CentOS/Oracle/ Amazon Linux]	1 `https://packages.vmware.com/cb/cblauncher` に移動します。 2 特定のバージョンを選択するか、[最新]のバージョンをクリックします。 3 `cblauncher-[version]-[build-number].x86_64.rpm` パッケージを見つけます。	■ `rpm -Uvh cblauncher-[version]-[build number].x86_64.rpm` 例: `rpm -Uvh cblauncher-1.0.0-16928845.x86_64.rpm`

3 Carbon Black ランチャ デーモンを起動するには、Linux ディストリビューションに基づく root 権限で次のコマンドを実行します。

- CentOS/RHEL/Oracle 6.x の場合は、次のコマンドを使用します。

```
service cblauncher start
```

- SUSE/Ubuntu/Amazon などの他のすべてのディストリビューションでは、次のコマンドを使用します。

```
systemctl start cblauncher
```

4 Carbon Black ランチャ デーモンを停止するには、Linux ディストリビューションに基づく root 権限で次のコマンドを実行します。

- CentOS/RHEL/Oracle 6.x の場合は、次のコマンドを使用します。

```
service cblauncher stop
```

- SUSE/Ubuntu/Amazon などの他のすべてのディストリビューションでは、次のコマンドを使用します。

```
systemctl stop cblauncher
```

5 Carbon Black ランチャ ステータスを確認するには、Linux ディストリビューションに基づく root 権限で次のコマンドを実行します。

- CentOS/RHEL/Oracle 6.x の場合は、次のコマンドを使用します。

```
service cblauncher status
```

- SUSE/Ubuntu/Amazon などの他のすべてのディストリビューションでは、次のコマンドを使用します。

```
systemctl status cblauncher
```

ステータスは実行中である必要があります。

Launcher をインストールした後、Carbon Black Cloud Workload Plug-in の Windows 仮想マシンと同様に、Linux 仮想マシンで Carbon Black を有効にすることができます。

Sectigo 証明書のインストール

センサーを Windows Server 2008 R2 および Windows 7 にインストールすると、Sectigo 署名証明書がオペレーティング システムのトラスト ストアに追加されていない場合、シグネチャ情報を検証に失敗する可能性があります。

Sectigo 署名証明書をダウンロードしてインストールするには、次の手順を実行します。

手順

1 Sectigo 中間証明書画面に移動し、 ルート証明書セクションを見つけます。

2 AAA 証明書サービスの [ダウンロード] リンクをクリックします。

3 SHA-2 Root: USERTrust RSA 認証局の [ダウンロード] リンクをクリックします。

4 証明書をインストールするには、`.crt` ファイルをダブルクリックし、デフォルトのオプションを受け入れます。

注： プロンプトが表示されたら、保存場所の下の [ローカル マシン] と [現在のユーザー] の両方のオプションの証明書をインストールする必要があります。

次のステップ

Windows Server 2008 R2 および Windows 7 のマシンで Carbon Black を有効にできるようになりました。

手順 2: 仮想マシンで Carbon Black を有効にする

アプリケーション ワークロードが実行されている仮想マシン (VM) で、Carbon Black を有効にする必要があります。

前提条件

- Carbon Black Cloud Workload アプライアンス を展開して構成しました。
- Carbon Black を有効にするオペレーティング システムを確認します。詳細については、2 章 vSphere の環境で Carbon Black を有効にするための準備 を参照してください。
- Windows 2008 R2 や Windows 7 などの古いオペレーティング システムがある場合は、Carbon Black センサー MSI に署名するために Sectigo 証明書を使用していません。**信頼されたルート証明機関** の証明書ストアに Sectigo 証明書がインストールされていることを確認します。詳細については、Sectigo 証明書のインストール を参照してください。
- Carbon Black ランチャ を使用できます。

手順

1 管理者の認証情報を使用して vSphere Client にログインします。

2 左側のナビゲーション ペインで、[Carbon Black] をクリックします。

3 [インベントリ] - [無効] タブに移動します。

4 [Status (ステータス)] 列で仮想マシンの適格性を確認します。対象の仮想マシンでのみ Carbon Black を有効にできます。

ステータス	説明
対象	仮想マシンで VMware Tools と Carbon Black ランチャ の正しいバージョンが使用できます。先に進み、仮想マシンで Carbon Black を有効にできます。
対象外	いくつかの理由により、お使いの仮想マシンが Carbon Black を有効にできない場合があります。たとえば、 ■ 仮想マシンはパワーオフされています。 ■ VMware Tools または Carbon Black ランチャ の必要なバージョンは使用できません。 ■ 仮想マシンの *isolation.tools.setinfo.disable* パラメータが *true* に設定されている場合。 仮想マシンを適格にするには、不適格基準に基づいて次のいずれかのアクションを実行できます。 ■ 仮想マシンをパワーオンにします。 ■ Windows 仮想マシンの場合: VMware Tools の 11.2 以降 をインストールします。すでにインストール済みの場合は、同バージョン以降にアップグレードします。 ■ Linux 仮想マシンの場合: Launcher を手動でインストールします。詳細については、Linux 仮想マシン用 Carbon Black Launcher を参照してください。 ■ *isolation.tools.setinfo.disable* パラメータを *false* に設定します。詳細については、vSphere のドキュメントを参照してください。
サポート対象外	Carbon Black Cloud Workload はオペレーティング システム (OS) または OS バージョンに対応していません。サポートされている OS とバージョンにアップグレードします。詳細については、2 章 vSphere の環境で Carbon Black を有効にするための準備 を参照してください。

5 Carbon Black を有効にする 1 つ以上の適格な仮想マシンを選択して、[有効化] をクリックします。

オプション	説明
使用可能な最新バージョンで Carbon Black を有効にするには、以下を実行します。	次の手順に進みます。使用可能な最新のセンサー バージョンで Carbon Black を有効にします。
特定のバージョンで Carbon Black を有効にするには、以下を実行します。	1 [詳細] をクリックします。各オペレーティング システム (OS) の使用可能なバージョンのリストが表示されます。 2 サポートされているセンサー バージョンのみがリストされています。ドロップダウン メニューから必要なバージョンを選択します。 3 (オプション) *構成*ファイルを使用して Carbon Black Cloud 設定を事前に構成できます。構成ファイルは *.ini* ファイル形式でアップロードできます。[ファイルのアップロード] をクリックします。*構成*ファイルを参照して選択します。 サンプル構成ファイルとパラメータの詳細を表示するには、 構成ファイルの詳細を参照してください。

6 確認ダイアログ ボックスが表示されます。[OK] をクリックします。

結果

Carbon Black が有効です。

■ [仮想マシン] - [概要] - [Carbon Black] ウィジェットの順に移動します。インストールされているバージョンを表示できます。

- [Carbon Black] - [インベントリ] - [有効] タブの順に移動します。仮想マシンのステータスが*アクティブ*であることを確認できます。

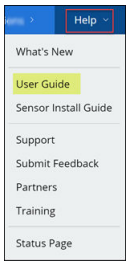
次のステップ

ワークロードが実行されている仮想マシンで Carbon Black を有効にしたら、Carbon Black Cloud Workload Plug-in の vSphere Client を使用してデータセンターのインベントリを監視できます。vCenter Server の直接的な可視性を使用して、ライフサイクル管理を実行できます。

vSphere Client の Carbon Black[概要] 画面には、Carbon Black が有効になっている仮想マシンの概要が表示されます。

Carbon Black Cloud コンソールに移動してセンサー グループを作成し、組織のセキュリティ ニーズに合わせてポリシーを設定できます。Carbon Black Cloud コンソールから潜在的な脅威を特定、調査、および修正できます。

Carbon Black Cloud の詳細については、Carbon Black Cloud コンソールの右上にある [ヘルプ] メニューの [ユーザー ガイド] を参照してください。



構成ファイルの詳細

特定のセンサー バージョンで Carbon Black を有効にする場合は、*構成*ファイルをアップロードできます。*構成*ファイルを使用して Carbon Black Cloud の設定を事前に行うことができます。デフォルトで、仮想マシンには Carbon Black Cloud の *Standard* ポリシーが割り当てられます。組織の要件に基づいて、*構成*ファイルで代替ポリシーを定義できます。

サンプル構成ファイル

```
[customer]
EncodedCompanyCode = 7X2KTWJQHO@RUO@R5I1LNO3@E319A
CompanyCode = NBEA3DLZ
BackendServer = prod01.xyz.io
```

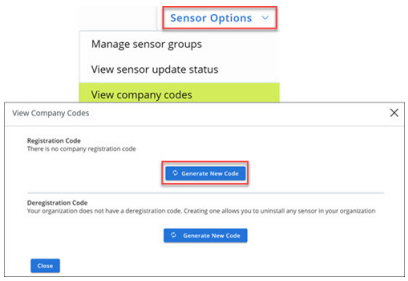
必須の構成ファイル パラメータ

EncodedCompanyCode、*CompanyCode*、および *BackendServer* は、構成ファイルに必要な必須パラメータです。次のように、必須パラメータの値を取得できます。

[EncodedCompanyCode] および [CompanyCode]: 会社の登録コードを取得するには、

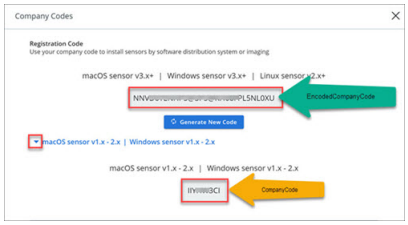
1 Carbon Black Cloud コンソールにログインし、左側のナビゲーション ペインで [Workloads (ワークロード)] をクリックします。

2 [Sensor Options (センサー オプション)] をクリックし、[View company codes (会社コードを表示)] をクリックします。



3 [登録コード]の下の [Generate New Code (新しいコードを生成)] ボタンをクリックします。

4 生成されたコードをメモします。長い文字列コードは、[EncodedCompanyCode] です。コードをコピーしてプレーン テキスト エディタに貼り付けます。



5 セクションを拡張し、短い文字列コードを表示します。短い文字列コードは、[CompanyCode] です。コードをコピーしてプレーン テキスト エディタに貼り付けます。

6 両方のコードを構成ファイルに貼り付けます。

[BackendServer]: リージョンに基づいて、Carbon Black Cloud のデバイス サービス URL を入力します。例: **`https://devices.confer.net`** 各リージョンのデバイス サービス URL の完全なリストを表示するには、「Carbon Black Cloud: API へのアクセスに使用される URL」を参照してください。

追加の構成ファイル パラメータ

「仮想マシン ワークロードへのセンサーのインストール」に記載のとおり、構成ファイルにパラメータを追加できます。

Carbon Black Cloud Workload Plug-in の使用

4

アプライアンスを展開し構成したら、vCenter Server で Carbon Black Cloud Workload Plug-in を表示できます。

Carbon Black Cloud Workload Plug-in を表示するには:

- 管理者の認証情報を使用して vSphere Client にログインします。
- Carbon Black  アイコンが、左側のナビゲーション ペインまたは vSphere Client の [ショートカット] メニューに表示されます。

Carbon Black Cloud Workload Plug-in ダッシュボードまたは [Summary (概要)] タブには、さまざまなウィジェットが表示され、健全性とインベントリ ステータスの概要をすばやく確認できます。また、アセットに影響を与える脆弱性や製品の重大な脆弱性も表示できます。

- [Inventory (インベントリ)] - [Not Enabled (無効)] タブに移動して、データセンター インベントリの Carbon Black を有効にします。
- [Inventory (インベントリ)] - [Enabled (有効)] タブを使用して、Carbon Black によって保護されているインベントリのリストを表示し、データセンター インベントリの選択に対して Carbon Black を更新または無効にします。

  Carbon Black Cloud Workload Plug-in は、[Inventory (インベントリ)] - [Enabled (有効)] - [Deployment Type (展開タイプ)]列で、保護されたインベントリを検出しワークロードと VDI に分類します。
- [Vulnerabilities (脆弱性)] タブに移動して、アセットに影響する脆弱性を表示します。

個々の仮想マシンの [Summary (概要)] または [Configure (構成)] タブに移動して、Carbon Black を有効化または更新できます。個々の仮想マシンの [Monitor (監視)] タブに移動して、仮想マシン固有の OS またはアプリケーション レベルの脆弱性を表示できます。

次のトピックを参照してください。

- センサーのステータスおよび詳細
- ホスト ユーザー ワールドの自動インストール
- ホスト ユーザー ワールドの手動インストール
- 脆弱性管理

センサーのステータスおよび詳細

Carbon Black Cloud Workload Plug-in [Inventory (インベントリ)] - [Enabled (有効)] タブの [Status (ステータス)] 列は、センサーのインストールまたはアクティブな状態、およびセンサーで実行された管理者アクションを示します。

表 4-1.

センサーのステータス	説明
アクティブ	センサーは適切に Carbon Black Cloud と通信しています。
非アクティブ	センサーは過去 30 日間 Carbon Black Cloud と通信していません。
登録済み	センサーは登録されています。
登録解除済み	センサーは登録解除またはアンインストールされています。センサーは Carbon Black Cloud コンソールから削除されるまで、*登録解除済み*ステータスの [Inventory (インベントリ)] - [Not Enabled (無効)] タブにあります。 **注：** 仮想マシンが削除されたり、別の vCenter Server に移動したりすると、センサーが削除されます。削除されたセンサーは、Carbon Black Cloud コンソールに*登録解除済み*として表示されます。3 日以上非アクティブで、vCenter Server から *削除*アクションを受け取ったワークロード センサーは、自動的に [登録解除]されます。
エラー	センサーがエラーをレポートしています。
更新可能	センサーは最新の使用可能なセンサー バージョンに更新できます。
バイパス	センサーは、Carbon Black Cloud 管理者によって*バイパス* モードになります。アセットに関するポリシーの適用はすべて無効になり、センサーはクラウドにデータを送信しません。 センサーの更新中に、センサーが一時的に*バイパス* モードになる場合があります。
隔離	センサーは Carbon Black Cloud 管理者によって隔離モードにされ、潜在的に悪意のあるアクティビティの拡散を緩和するためにネットワークから隔離されます。

ホスト ユーザー ワールドの自動インストール

Carbon Black Cloud ホスト モジュールは、ホスト ユーザー ワールド プロセスとして ESXi 上で実行され、仮想マシンに一意の ID 情報を提供します。vCenter Server でホストごとにホスト ユーザー ワールドを手動でインストールする時間を節約し、アプライアンスと通信するように設定するために、新しく導入された自動インストールおよび構成フローを使用できます。

ホスト ユーザー ワールドをクラスタ内の単一ホストまたは複数のホストにインストールします。

前提条件

- ESXi 6.7 以降のホスト
- vCenter Server 6.7 以降
- Carbon Black Cloud Workload アプライアンス 1.1 以降
- ホストをパワーオンし、vCenter Server に接続する必要があります。

手順

1 管理者の認証情報を使用して vSphere Client にログインします。

2 インベントリ ツリーからホストを選択し、[Configure (構成)] タブをクリックします。

3 [Carbon Black] - [Security (セキュリティ)] ページに移動し、[Enable Host Module (ホスト モジュールを有効にする)] をクリックします。

このアクションには最大 5 分かかります。

インストールが完了すると、ステータスが「インストール可能」から「最新」に変わります。ホスト ユーザー ワールド バージョンとその一般的なステータスが接続中と表示されます。

4 ホスト ユーザー ワールドを最新バージョンにアップグレードするには、[Upgrade Host Module (ホスト モジュールのアップグレード)] をクリックします。

アップグレードが完了すると、ステータスが「インストール可能」から「最新」に変わります。

5 オプション。クラスタ内のすべてのホストに Carbon Black Cloud ホスト モジュールをインストールするには:

a インベントリ ツリーからクラスタを選択し、[Configure (構成)] タブをクリックします。

b [Carbon Black] - [Security (セキュリティ)] ページに移動し、[Enable Host Module (ホスト モジュールを有効にする)] をクリックします。

c [VMware Carbon Black Cloud] ポップアップで [Confirm (確認)] を選択します。

次のステップ

VDI クローンの自動識別と登録を有効にするには、vCenter Server 環境で Linux または Windows 仮想マシンに Carbon Black Cloud センサーをインストールします。詳細については、『VMware Carbon Black Cloud センサーのインストール ガイド』を参照してください。

ホスト ユーザー ワールドの手動インストール

ホスト ユーザー ワールド モジュールは、vSphere Lifecycle Manager サービスを使用してクラスタ内の個々のホストまたはすべてのホストをまとめて修正することで、ESXi ホストにインストールできます。このサービスを使用すると、vSphere Lifecycle Manager の単一イメージを、環境内の ESXi ホストのライフサイクルをインストールおよび管理する代替方法として使用できます。

ホスト ユーザー ワールド モジュールをインストールするには、まず [Settings (設定)] タブでサードパーティのダウンロード元を追加する必要があります。ダウンロード元は、ソフトウェアのダウンロードに使用するオンライン デポです。

次に、vSphere Lifecycle Manager デポとダウンロード元の間の同期を開始して、ローカルの vSphere Lifecycle Manager デポをすぐに更新します。その結果、ダウンロードする必要がある VMware Carbon Black コンポーネント (ESX 用) は、[Image Depot (イメージ デポ)] タブに表示されます。vSphere Lifecycle Manager がオンライン デポと同期する場合、更新メタデータのみがダウンロードされます。ステージングまたは修正中に実際のペイロードがダウンロードします。

最後に、デポでホストされている ESXi イメージに対して ESXi ホストのコンプライアンス ステータスを確認し、そのイメージに対して [Updates (更新)] タブでホストを修正します。

vSphere Client の vSphere Lifecycle Manager ユーザー インターフェイスの詳細については、「ホストとクラスタのライフサイクルの管理」を参照してください。

前提条件

- ホストは ESXi 7.0 以降を実行している必要があります。
- ホストをパワーオン状態して、vCenter Server に接続する必要があります。
- vSphere Lifecycle Manager イメージを使用するために必要な権限を所有します。詳細については、vSphere 7.0 → ESXi および vCenter Server ドキュメントに含まれる「ホストとクラスタのライフサイクルの管理」を参照してください。

手順

1. 管理者の認証情報を使用して vSphere Client にログインします。
2. [Menu (メニュー)] - [Lifecycle Manager]を選択します。
3. [Settings (設定)] タブで、[Administration (管理)] - [Patch Setup (パッチ セットアップ)]を選択します。

   vSphere Lifecycle Manager のデフォルトのダウンロ-ド元はインターネットです。
4. サードパーティ製コンポーネント (ESX 用の Carbon Black コンポーネントなど) をダウンロードするには、[New (新規)] をクリックして、ダウンロード元の URL アドレスを入力します。

オプション	説明
https://prod.cwp.carbonblack.io/cbhost/*us*/online-depot/index.xml	米国地域のデポ URL。
https://prod.cwp.carbonblack.io/cbhost/*au*/online-depot/index.xml	アフリカ連合地域のデポ URL。
https://prod.cwp.carbonblack.io/cbhost/*ap*/online-depot/index.xml	アジア太平洋地域のデポ URL。
https://prod.cwp.carbonblack.io/cbhost/*eu*/online-depot/index.xml	ヨーロッパ地域のデポ URL。

   説明はオプションです。
5. 変更を維持するには、[Save (保存)] をクリックします。

   ソース URL は、ダウンロード元のリストの一番下に表示されます。

6 ローカルの vSphere Lifecycle Manager デポをすぐに更新するには、[Actions (アクション)] ドロップダウン メニューから [Sync Updates (更新の同期)] を選択します。

vSphere Lifecycle Manager は、使用するように構成したオンライン デポからソフトウェアをダウンロードします。Carbon Black コンポーネントは [Image Depot (イメージ デポ)] - [Components (コンポーネント)]テーブルで使用できます。

7 クラスタ内のホストを単一のイメージで管理できるようにするには、イメージをセットアップする必要があります。

a [vSphere Client] ドロップダウン [メニュー]、[Hosts and Clusters (ホストとクラスタ)] をクリックし、イメージで管理するクラスタを選択します。

b [Updates (更新)] タブで、[Hosts (ホスト)] - [Image (イメージ)] を選択し、[Setup Image (セットアップ イメージ)] ボタンをクリックします。

[Convert to an Image (イメージに変換)] ページが表示されます。

c 手順 1 でイメージを定義するには、関連するドロップダウン メニューから ESXi バージョンを選択し、[Add Components (コンポーネントの追加)] をクリックして、 VMware Carbon Black コンポーネントを選択します。

Carbon Black コンポーネントは、[その他のコンポーネント]の表に表示されます。

d [Validate (認証)] を選択し、イメージが有効と表示されたら、[Save (保存)] をクリックします。

e 手順 2 で定義したイメージを使用してホストのコンプライアンスを確認するには、ホストを選択し、[Check Compliance (コンプライアンスの確認)] をクリックします。

f クラスタ内のすべてのホストが新しく定義したイメージに準拠している場合は、[Finish Image Setup (イメージのセットアップを終了)] をクリックし、アクションを確認します。

[イメージ] カードと[イメージ コンプライアンス] カードには、イメージ セットアップの概要が表示されます。

8 クラスタ内のすべてのホストを修正します。

a [イメージ コンプライアンス] カードで、[Remediate All (すべて修正)] ボタンをクリックします。

[Review Remediation Impact (修正の影響の確認)] 画面が表示されます。

b エンドユーザー使用許諾契約書の条項に同意し、[Start Remediation (修正の開始)] をクリックします。

修正プロセスが正常に完了すると、[イメージ コンプライアンス] カードが通知します。修正では、ホストに VIB のみがインストールされ、ホスト ユーザー ワールド モジュールは構成されません。

9 [Configure (構成)] タブで、[Configuration (構成)] - [Security (セキュリティ)] を選択します。

ホストが `Needs install` 状態で表示されます。

10 [Enable Host Module (ホスト モジュールの有効化)] ボタンをクリックします。

操作が正常に完了すると、ホストが `Latest sensor installed` 状態で表示されます。

11 オプション。クラスタからホストを選択し、[Configure (構成)] - [Security (セキュリティ)] ページに移動して、Carbon Black Cloud の概要を表示します。

次のステップ

管理対象クラスタを選択して、[Updates (更新)] - [Hosts (ホスト)] - [Image (イメージ)] ページに移動し、再度[コンプライアンスを確認]します。

イメージは、クラスタ内のすべてのホストに引き続き準拠します。（他のコンポーネントによる）イメージの変更は、ホストからホスト ユーザー ワールド モジュールを削除しません。これは、コンポーネントがすでにイメージに含まれているためです。

脆弱性管理

vCenter Server 管理者は、セキュリティ状況を把握し、パッチ適用と修正のためのメンテナンス ウィンドウをスケジュール設定するため、環境の既知の脆弱性を可視化します。脆弱性評価によって、環境内のリスクをプロアクティブに最小化することができます。これで、既知の脆弱性を Carbon Black Cloud Workload Plug-in から監視できるようになりました。プラグインの [サマリ] タブまたは [脆弱性] タブから脆弱性を検出し、チームと連携してパッチ適用または更新のためのメンテナンス ウィンドウをスケジュール設定できます。脆弱性評価機能を表示するには、データセンターで Carbon Black を有効にする必要があります。Carbon Black を有効にしたら、通常、数分以内に脆弱性データを表示できます。

Carbon Black は、以下に関連する脆弱性を調べます。

- 仮想マシンのオペレーティング システム (OS)。
  - [Windows OS]：Windows 仮想マシンの OS レベルの脆弱性を表示します。システムは OS の詳細と各仮想マシンに適用されたセキュリティ パッチを探します。脆弱性に関連するセキュリティ パッチが適用されていない場合、仮想マシンには脆弱というフラグが付けられます。
  - [Linux OS]：Linux 仮想マシンの OS レベルの脆弱性を表示します。システムは、インストールされているすべてのパッケージのリストで OS の詳細を探します。システムは、仮想マシンにインストールされている脆弱なパッケージを判別し、それらのパッケージに対する CVE を報告します。
- 仮想マシンにインストールされているアプリケーション。
  - [Windows アプリケーション]：Windows 仮想マシンのアプリケーションレベルの脆弱性を表示します。
  - [Linux アプリケーション]：Linux 仮想マシンのアプリケーションレベルの脆弱性を表示します。

[脆弱性] タブ

- 左側のナビゲーション ペインで、Carbon Black  アイコンを使用してして列をフィルタリングできます。
- Carbon Black Cloud Workload Plug-in ダッシュボードで、[脆弱性] タブをクリックします。

重要度のクリティカルはデフォルトのフィルタです。[脆弱性] タブで利用可能なすべての脆弱性のリストに移動するには、[すべて] をクリックします。脆弱性の合計は、すべての監視対象アセットと製品（OS、アプリ、バージョン）にわたるすべての脆弱性の数です。

脆弱性データの表示方法に応じて、[アセット ビュー] タブまたは [脆弱性 ビュー] タブのいずれかを表示できます。[アセット ビュー] タブを使用して、既知の脆弱性があるアセットを表示します。[脆弱性ビュー] タブを使用して、すべてのアセットのすべての脆弱性のリストを表示します。

各仮想マシンに複数の脆弱性がある場合があり、各脆弱性に異なるリスク スコアがある場合があります。リスク スコアに基づいて、脆弱性は重要度のレベル（クリティカル、重要、中、低）でフィルタリングされます。リスク スコアが高いほど、重要度が高くなります。最も高いリスク スコアはクリティカルな脆弱性と見なされます。詳細については、リスク評価を参照してください。

ページのすべてのデータを CSV ファイルにエクスポートするには、[エクスポート] をクリックします。

注： エクスポート機能は、vCenter Server の既知の問題であるため、vCenter Server 6.7 および 7.0 でブロックされます。この問題は、7.0 U1 以降のバージョンで修正されています。

[アセット ビュー] タブでは、Windows および Linux システムに基づいてデータがフィルタリングされます。リスク スコアと共通脆弱性評価システム (CVSS) の詳細を表示するには、[脆弱性の数] の数字をクリックします。詳細を表示する行を展開します。外部の National Vulnerability Database の Web サイトで CVE の詳細を表示するには、National Vulnerability Database リンクをクリックします。影響を受ける仮想マシンのアセット名をクリックして、[仮想マシン > モニタ > Carbon Black > 脆弱性] タブの順に移動します。

[脆弱性] タブでは、Windows および Linux システムの OS レベルの脆弱性とアプリケーションレベルの脆弱性に基づいてデータがフィルタリングされます。

各仮想マシンの脆弱性データは、24 時間ごとに自動的に更新されます。更新された脆弱性データをすぐに表示したい場合は、[再評価] をクリックします。

注： インベントリに新たに追加された仮想マシンの脆弱性データは、通常、数分以内に収集されますが、特定の状況では、最大 24 時間かかる場合があります。

リスク評価

リスク スコアはデータセンターの特定の脆弱性のリスクを正確に表す測定基準です。これは、CVSS 情報を独自の脅威データおよび *Kenna Security* の高度なモデリングと組み合わせることによって実現されます。

リスクの測定

Carbon Black Cloud パートナーは *Kenna Security* と提携し、業界最大の脆弱性、エクスプロイト、およびイベント脅威データのデータベースを活用しています。このデータは、リスクの 3 つの主要な基準にまとめられます。

- [アクティブなインターネット侵害]: ほぼリアルタイムの搾取の存在
- [悪用可能なマルウェア]: 武器化されたエクスプロイト キットでのエクスプロイト モジュールの可用性
- [簡単に悪用可能]: 記録されたエクスプロイトの可用性

共通脆弱性評価システム (CVSS) には、いくつかのメトリックが定義されています。攻撃方法自体に関するメトリックはほとんどありませんが、他のメトリックは、アプリケーションが影響を評価する方法（成功したエクスプロイトの直接的な結果）に依存します。CVSS の詳細については、共通脆弱性評価システムをご覧ください。

リスク スコア

すべての脆弱性に 0.0（リスクなし）～ 10.0（最大リスク）のリスク スコアが割り当てられます。リスク スコアの範囲と重要度は次のように定義されています。

スコアの範囲	重要度
0.0 ～ 3.9	低
4.0 ～ 6.9	中
7.0 ～ 8.9	重要
9.0 ～ 10.0	クリティカル

リスクの計算方法の詳細については、「Kenna Security 脆弱性リスク スコアの理解」を参照してください。

OS レベルの脆弱性の対処

OS レベルのすべての脆弱性は、Carbon Black Cloud Workload Plug-in の [脆弱性] タブで確認できます。[Windows OS] タブには、Windows オペレーティング システムを持つ仮想マシンの脆弱性が一覧表示されます。[Linux OS] タブには、Linux オペレーティング システムを持つ仮想マシンの脆弱性が一覧表示されます。

特定の仮想マシンの OS レベルの脆弱性を表示できます。

1 [仮想マシン] - [モニタ] - [Carbon Black] - [脆弱性] タブの順に移動します。

2 [OS] タブをクリックします。

特定の仮想マシンに関連するすべての OS レベルの脆弱性が一覧表示されます。フィルタ アイコンを使用して列をフィルタリングできます。外部の National Vulnerability Database (https://nvd.nist.gov/外（) の Web サイトを表示することもできます。

Windows OS の脆弱性を解決するには、*CVE-ID* を参照して、提案される KB パッチを適用します。

Linux OS の場合、脆弱性はパッケージ レベルで関連付けられます。[バージョン] と [修正方法] 列には、リストされている脆弱性が修正されたバージョンとビルド番号が表示されます。

Linux OS の脆弱性を解決するには、リストされているバージョンとビルド番号にアップグレードします。

アプリケーション レベルの脆弱性の対処

アプリケーション レベルのすべての脆弱性は、Carbon Black Cloud Workload Plug-in の [脆弱性] タブで確認できます。[Windows アプリケーション] タブには、Windows オペレーティング システムを持つ仮想マシンのアプリケーション レベルの脆弱性が一覧表示されます。[Linux アプリケーション] タブには、Linux オペレーティング システムを持つ仮想マシンのアプリケーション レベルの脆弱性が一覧表示されます。仮想マシンの [仮想マシン] - [モニタ] - [Carbon Black] - [脆弱性] タブには、特定の仮想マシンのアプリケーション レベルの脆弱性が一覧表示されます。

特定の仮想マシンのアプリケーション レベルの脆弱性を表示できます。

1 [仮想マシン] - [モニタ] - [Carbon Black] - [脆弱性] タブの順に移動します。

2 [アプリケーション] タブをクリックします。

仮想マシンでアクティブに実行されているアプリケーションの脆弱性が表示されます。フィルタ アイコンを使用してして列をフィルタリングできます。

クイック リファレンスとして、ベンダーと製品の情報が提供されています。[バージョン] と [修正方法] 列には、リストされている脆弱性が修正されたバージョンとビルド番号が表示されます。脆弱性を解決するには、記載されているバージョンとビルド番号にアップグレードする必要があります。*CVE-ID* を参照して、外部の National Vulnerability Database (https://nvd.nist.gov/) の Web サイトを表示することもできます。

製品に脆弱性を修正するために利用可能な更新がない場合、または Carbon Black に特定の解決策を示すのに十分な情報がない場合は、[修正方法] 列が空になることがあります。

Carbon Black Cloud Workload アプライアンスの使用

5

アプライアンス ダッシュボードを使用して、Carbon Black Cloud Workload アプライアンス 全体のステータスを表示できます。vCenter Server の登録、Carbon Black Cloud への接続、NTP サーバの設定、およびネットワーク設定の表示を行うこともできます。

注： アプライアンス インターフェイスのアクセスを許可された管理者のみに制限するには、ネットワーク制御を実装する必要があります。アプライアンス インターフェイスへの無制限のネットワーク アクセスは必要ありません。

admin 認証情報を使用して Carbon Black Cloud Workload アプライアンス GUI (**https://<appliance IP address>**) にログインできます。アプライアンス ダッシュボードがデフォルトのホーム ページとして表示されます。ダッシュボードには、アプライアンスの全体的な健全性ステータスが表示されます。デフォルトで、アプライアンスのセッション タイムアウトは 5 分です。

次のトピックを参照してください。

- アプライアンス ユーザーの管理
- NTP サーバ設定の構成
- ネットワーク設定の表示と更新
- アプライアンスのプロキシ設定
- アプライアンスの健全性ステータス
- アプライアンス パスワードの維持
- アプライアンスを再起動
- Carbon Black Cloud Workload アプライアンスの再展開
- アプライアンスのログ

アプライアンス ユーザーの管理

アプライアンス管理者は、Carbon Black Cloud Workload アプライアンスのユーザーを管理できます。新しいシステム ユーザーを追加するか、別のグループに割り当てるか、削除します。新しいユーザー アカウントのパスワードを設定したり、アプライアンス内の既存のユーザーのパスワードを更新したりすることもできます。

前提条件

ユーザーが、root と admin 権限を持っている wheel グループに属していることを確認します。

手順

1 *root* 認証情報を使用してアプライアンスにログインします。

2 指定したホーム ディレクトリとユーザーが属するグループを使用して新しいユーザーを作成するには、`useradd -m -G <group-name> <user-name>` コマンドを使用します。

たとえば、`useradd -m -G group1,group2 user1` コマンドを実行します。

例のコマンドは、2 つのグループ (group1 と group2) に含まれる新しいユーザー (user1) を作成します。

3 新しく作成したユーザーの新しいパスワードを設定し、`passwd <user-name>` コマンドを使用します。

たとえば、`passwd user1` コマンドを実行します。

例のコマンドは、user1 の新しいパスワードを作成します。

注： また、`passwd` コマンドを使用して、そのユーザーのパスワードを変更することもできます。

NTP サーバ設定の構成

SSO サーバの時刻と Carbon Black Cloud Workload アプライアンス の時刻を同期するように NTP サーバを構成する必要があります。

前提条件

Carbon Black Cloud Workload アプライアンス を展開しました。

手順

1 ブラウザから、**admin** 認証情報を使用して vCenter Server (**https://<vCenter IP/Domain address>**) にログインします。Carbon Black Cloud Workload アプライアンス はこちらにあります。

2 vCenter Server を使用して時刻同期設定を構成するには、[アプライアンス] - [全般] タブに移動します。

3 [時刻設定] セクションで [編集] をクリックし、次の詳細を追加します。

注： アプライアンスと vCenter Server の時間差により、クロック スキュー エラーが発生します。ナレッジベースの記事の説明に従って、アプライアンスと ESXi ホスト間の NTP 同期を設定します。

時間設定	説明
NTP サーバ	時刻の同期には、NTP (Network Time Protocol) サーバが使用されます。vCenter Server 構成の設定に使用するサーバと同じ NTP サーバを入力します。例えば、**pool.ntp.org** と入力します。複数の NTP サーバを入力する場合は、カンマ区切りのリスト (,) を使用し、その後のエントリの間にスペースを入れます。
フォールバック NTP サーバ	代替 NTP サーバの詳細を入力します。
日付と時刻	日付と時刻が vCenter Server と同期されているかどうかを確認します。

4 [保存] をクリックします。

結果

NTP サーバ設定が構成されます。

ネットワーク設定の表示と更新

[ネットワーク] 画面を使用して、アプライアンス仮想マシンのネットワーク設定を表示します。アプライアンスの IP アドレス、ネットワーク ゲートウェイ、および DNS 関連の詳細に関する詳細を表示できます。ネットワーク設定を更新するには、仮想アプライアンス管理インターフェイス (VAMI) を使用します。アプライアンスのユーザー インターフェイス (UI) からネットワーク設定を変更することはできません。

手順

1 *root* 認証情報を使用してアプライアンスにログインします。

2 仮想アプライアンス管理インターフェイス (VAMI) CLI コマンド `/opt/vmware/share/vami` を実行します。

`/opt/vmware/share/vami/vami_set_network --help` コマンドを使用して、ネットワーク設定で使用可能なオプションのリストを確認します。

3 目的のネットワーク構成パラメータを更新します。

たとえば、

```
vami_set_network <interface> (DHCPV4|DHCPV6|AUTOV6|DHCPV4+DHCPV6|DHCPV4+AUTOV6|
DHCPV4+NONEV6)
vami_set_network <interface> (STATICV4|STATICV4+DHCPV6|STATICV4+AUTOV6|STATICV4+NONEV6)
<ipv4_addr> <netmask> <gatewayv4>
vami_set_network <interface> (STATICV6|DHCPV4+STATICV6) <ipv6_addr> <prefix> (<gatewayv6>|
default)
vami_set_network <interface> STATICV4+STATICV6 <ipv4_addr> <netmask> <gatewayv4>
<ipv6_addr> <prefix> (<gatewayv6>|default)
```

4 アプライアンス仮想マシンを再起動します。

5 **管理者**認証情報を使用してアプライアンスにログインします。

6 [構成] - [ネットワーク] > [ネットワークの詳細] タブで更新されたネットワーク設定を確認します。

結果

NTP サーバ設定が更新されます。

アプライアンスのプロキシ設定

プロキシ サーバを構成することで、Carbon Black Cloud との安全な接続を確立できます。Carbon Black Cloud Workload アプライアンス から Carbon Black Cloud へのすべての送信ネットワーク トラフィックは構成済みのプロキシ サーバを通過します。[HTTP]、[HTTPS]、[SOCKS4] または [SOCKS5] タイプのプロキシ サーバを構成します。

Carbon Black Cloud Workload アプライアンス でプロキシ サーバを設定したら、そのプロキシ サーバから Carbon Black Cloud URL にアクセスできるかどうかを確認できます。

前提条件

- Carbon Black Cloud Workload アプライアンス を Carbon Black Cloud、および vCenter Server に登録します。
- アプライアンスのプロキシ サポートは、バージョン 1.1 以降で利用できます。

手順

1 ブラウザから、**admin** 認証情報を使用して vCenter Server (**https://<vCenter IP/Domain address>**) にログインします。Carbon Black Cloud Workload アプライアンス はこちらにあります。

2 プロキシを設定するには、[Appliance (アプライアンス)] - [Network (ネットワーク)] ページに移動します。

3 [Proxy (プロキシ)] タブを選択し、[Edit (編集)] をクリックします。

   a 必要なプロキシ タイプとして、[HTTP]、[HTTPS]、[SOCKS4]、[SOCKS5] を選択します。

   b プロキシ サーバのホスト名を HTTP または HTTPS スキームなしで入力します。

   `http://` または `https://` ヘッダーを入力しないでください。

   c プロキシ サーバがリッスンするポートを入力します。

   選択したプロキシ タイプの正しいポート値を使用します。ポート番号とプロキシ タイプの組み合わせが正しくないと、Carbon Black Cloud Workload アプライアンスはプロキシを介して Carbon Black Cloud に接続できません。

   d 必要に応じて、プロキシのユーザー名とパスワードを入力します。

4 [Save (保存)] をクリックします。

   プロキシ サーバを設定します。設定が完了すると、その設定はすぐに有効になります。

   プロキシ サーバにアクセスできない場合、設定を保存するとエラー メッセージが表示されます。

5 アプライアンス仮想マシンが設定されたプロキシ サーバを介して Carbon Black Cloud に接続しているかどうかを確認するには、[Verify (確認)] をクリックします。

   [Carbon Black Cloud への接続を確認] ウィンドウが表示されます。

6 アプライアンスの接続先となる Carbon Black Cloud 環境を選択し、[Test (テスト)] をクリックします。

   接続のステータスに関する通知が表示されます。アプライアンスをクラウドに接続できない場合は、プロキシ設定を更新します。

結果

接続ステータスは、[Dashboard (ダッシュボード)] - [Health (健全性)] および [Appliance (アプライアン)] - [Registration (登録)] - [VMware Carbon Black Cloud] パネルで更新されます。

アプライアンスの健全性ステータス

Carbon Black Cloud Workload Plug-in で、Carbon Black Cloud Workload アプライアンス の全体的な健全性ステータスを表示できます。アプライアンス ワーカー、vSphere ワーカー、ゲートウェイ、およびアクセス コントロール サービスはアプライアンス サービスです。また、Carbon Black Cloud Workload Plug-in で各アプライアンス サービスの接続ステータスを表示することもできます。Carbon Black Cloud Workload アプライアンス ダッシュボードでサービスに関する健全性ステータスを表示することもできます。

アプライアンスには、次のいずれかの健全性ステータスが表示されます。

- [接続済み] : アプライアンスが接続されています。
- [切断] : アプライアンスが切断されています。ステータスが切断の場合は、アプライアンス仮想マシンがパワーオン状態であることを確認します。アプライアンスの [登録] タブに移動し、構成を確認します。詳細については、Carbon Black Cloud Workload アプライアンスを Carbon Black Cloud に接続する を参照してください。

  注： vCenter Server の再起動中に、Carbon Black Cloud Workload アプライアンス に vCenter Server が未登録として表示される場合があります。アプライアンスとの接続を確認する前に、vCenter Server が正常に起動して実行されるまで待機する必要があります。

- [不健全] : アプライアンスは接続されていますが、サービスの 1 つが停止しています。個々のアプライアンス サービスの状態は [接続済み] または [切断] です。アプライアンスのステータスが [不健全] の場合は、個々のサービス ステータスを検索します。切断されたアプライアンス サービスの場合は、次のようにサービスを再起動できます。

  a *admin* 認証情報を使用して Carbon Black Cloud Workload アプライアンス に SSH 接続します。

  b `sudo su` コマンドを使用して、*root* ユーザーに切り替えます。

  c 再起動するサービスに適切なコマンドを使用します。

  ```
  systemctl restart cwp-appliance-worker
  ```

  ```
  systemctl restart cwp-access-control-service
  ```

  ```
  systemctl restart cwp-vsphere-worker
  ```

  ```
  systemctl restart cwp-appliance-gateway.service
  ```

  d 再度アプライアンス サービスのステータスを確認します。

  e アプライアンス サービスのいずれかが停止したままの場合は、https://www.carbonblack.com/support/ の VMware Carbon Black サポート チームに連絡するか、https://www.vmware.com/support/contacts.html の VMware サポート チームに連絡してください。

ログ ファイルは、サポート チームが、お客様がサポート チケットを発行した問題のトラブルシューティングを行うのに役立ちます。詳細については、アプライアンスのログ を参照してください。

アプライアンス パスワードの維持

アプライアンスのパスワードは一定期間有効です。維持するには、リセットするか、有効期限を延長します。

アプライアンスのパスワードは、アプライアンスを初めて展開してから 90 日後に期限が切れます。パスワードの有効期限が切れる時に、アプライアンスのユーザー インターフェイスに通知が表示されます。このメッセージは、パスワードの有効期限の 15 日前に表示され、「**パスワードの有効期限が X 日後に切れます**」のようなメッセージが表示されます。Carbon Black Cloud Workload Plug-in には、アプライアンスのパスワードの有効期限に関する通知も表示され、「**アプライアンスのパスワードの有効期限が X 日後に切れます**」というメッセージが表示されます。期限が切れる前にパスワードをリセットする必要があります。また、パスワードの期限を手動で延長したり、永続的に無効にしたりすることもできます。

デフォルトで、アプライアンスのタイム ゾーンは UTC です。

Carbon Black Cloud Workload アプライアンス コンソール ユーザー インターフェイス に root パスワードの有効期限通知が表示されます。アプライアンスの root パスワードの有効期限通知は、vSphere Client ユーザー インターフェイスの一部である Carbon Black Cloud Workload Plug-in でも確認できます。

アプライアンス パスワードのリセット

admin 権限を持つ Carbon Black Cloud Workload アプライアンス からロックアウトされている場合は、パスワードをリセットできます。

手順

1. ブラウザから、**admin** 認証情報を使用して vCenter Server (**https://<vCenter IP/Domain address>**) にログインします。Carbon Black Cloud Workload アプライアンス はこちらにあります。
2. [ホストとクラスタ] で、Carbon Black Cloud Workload アプライアンス を選択します。
3. vCenter Server で、 [サマリ] タブをクリックし、[Web コンソールの起動] をクリックします。

   必要に応じてポップアップ ウィンドウを許可します。
4. [Web コンソール] ウィンドウで、root 認証情報を使用してログインします。
5. `pam_tally2 -u admin` コマンドを使用して、*admin* アカウントがロックされているかどうかを確認します。
6. *admin* アカウントがロックされている場合は、次のコマンドを使用してロックを解除します。

   ```
   pam_tally2 -r -u admin
   ```
7. *admin* ユーザー パスワードを変更するには、次の手順を実行します。
   a. *admin* 認証情報を使用して Carbon Black Cloud Workload アプライアンス に SSH 接続します。

      たとえば、`SSH admin@<Appliance_IP_Address>` です。
   b. `passwd admin` コマンドを使用します。

c 現在のパスワードと希望するパスワードを入力し、後で参照できるようにメモしておきます。

注： 最近の 5 つのパスワードは使用しないでください。パスワードは 8 文字以上にする必要があります。数字、小文字、大文字、特殊文字をそれぞれ 1 つ以上含む、基本的な複雑さに適合するパスワードを入力します。

d admin パスワードを再入力します。

Carbon Black Cloud Workload アプライアンス *admin* ユーザー パスワードが変更されます。

8 期限切れのパスワードをリセットするには、次の手順を実行します。アプライアンスのパスワードは、90 日後に自動的に期限切れになります。

a *admin* 認証情報を使用して Carbon Black Cloud Workload アプライアンス に SSH 接続します。

b パスワードの入力を求められたら、希望する admin パスワードを入力し、後で参照できるように書き留めます。

注： 最近の 5 つのパスワードは使用しないでください。パスワードは 8 文字以上にする必要があります。数字、小文字、大文字、特殊文字をそれぞれ 1 つ以上含む、基本的な複雑さに適合するパスワードを入力します。

c admin パスワードを再入力します。

パスワードが正常に変更されました。

d パスワードが正常に変更されたことを確認するために、再度 Carbon Black Cloud Workload アプライアンス に SSH 接続します。

e 次に、*admin* ユーザー名と変更されたパスワードを使用して Carbon Black Cloud Workload アプライアンス ユーザー インターフェイスにログインします。

9 *root* パスワードをリセットするには、次の手順を実行します。

注： デフォルトでは、セキュリティ上の理由から、*root* ユーザーの SSH アクセスは Carbon Black Cloud Workload アプライアンス で無効になっています。

a *admin* 認証情報を使用して Carbon Black Cloud Workload アプライアンス に SSH 接続します。

b 次のコマンドを使用してパスワードをリセットします。

```
sudo su
passwd root
```

c 現在のパスワードと希望するパスワードを入力し、後で参照できるようにメモしておきます。

Carbon Black Cloud Workload アプライアンス *root* ユーザー パスワードが変更されました。

アプライアンスのパスワード有効期限の延長

パスワードの有効期限は、Carbon Black Cloud Workload アプライアンス に必要な日数まで手動で延長できます。必要に応じて、パスワードの有効期限を永続的に無効にすることもできます。

手順

1 パスワードの有効期限を手動で延長するには

   a *admin* 認証情報を使用して Carbon Black Cloud Workload アプライアンス に SSH 接続します。

   b 次のコマンドを実行し、パスワードの有効期限を、*root* と *admin* の両方のユーザーに必要な日数まで延長します。次の例は、180 日を示しています。180 を必要な日数に置き換えることができます。

   ```
   sudo chage -I -1 -m 0 -M 180 -E -1 admin
   sudo chage -I -1 -m 0 -M <number of days> -E -1 admin
   sudo chage -I -1 -m 0 -M 180 -E -1 root
   sudo chage -I -1 -m 0 -M <number of days> -E -1 root
   ```

   パスワードの有効期限が 180 日にリセットされます。

2 パスワードの有効期限を永続的に無効にするには、以下を実行します。

   a *admin* 認証情報を使用してアプライアンスに SSH 接続します。

   b 次のコマンドを実行し、*root* と *admin* の両方のユーザーに対してパスワードの有効期限を永続的に無効にします。

   ```
   sudo chage -I -1 -m 0 -M 99999 -E -1 admin
   sudo chage -I -1 -m 0 -M 99999 -E -1 root
   ```

   パスワードの有効期限が永続的に無効になります。

管理者パスワードの有効期限を無効にする

デフォルトで Carbon Black Cloud Workload アプライアンスの管理者パスワードは 90 日後に期限が切れます。ただし、アプライアンスの初期インストールおよび構成後にパスワードの有効期限を無効にすることができます。

管理者パスワードの有効期限が切れると、ログインしてコンポーネントを管理できなくなります。また、実行するために管理者パスワードを必要とするタスクまたは API 呼び出しが失敗します。このような状況を事前に解決するには、パスワードの有効期限を無効にして、パスワードの有効期限が切れないようにします。

手順

1 ブラウザから、**admin** 認証情報を使用して vCenter Server (**https://<vCenter IP/Domain address>**) にログインします。Carbon Black Cloud Workload アプライアンス はこちらにあります。

2 [アプリケーション] - [全般] - [パスワード設定] タブの順に移動します。

   デフォルトで、管理者パスワードの有効期限オプションは有効になっています。

3 管理者パスワードの有効期限を無効にするには、関連するトグル スイッチをクリックします。

   トグル スイッチの状態が非アクティブに切り替わります。

結果

パスワードの更新は要求されません。

アプライアンスを再起動

問題がある場合は、次のいずれかの方法で Carbon Black Cloud Workload アプライアンス を再起動できます。

- vCenter Server で Carbon Black Cloud Workload アプライアンス を右クリックし、[Power (電源)] > [Restart Guest OS (ゲスト OS を再起動)] の順にクリックします。

-OR-

- Carbon Black Cloud Workload アプライアンス に SSH 接続し、`sudo reboot` コマンドを実行します。

Carbon Black Cloud Workload アプライアンスの再展開

Carbon Black Cloud Workload アプライアンス が到達不能で応答しない場合、アプライアンスを再展開できます。同じアプライアンスを再展開するには、同じ SSO と vCenter Server に登録する必要があります。Carbon Black Cloud コンソールからアプライアンスの API ID とキーを再生成し、新しい API ID とキーを使用してアプライアンスと Carbon Black Cloud の間の接続を確立する必要があります。

アプライアンスに接続できないか、アプライアンスが応答しません。パスワードを複数回リセットしてもアプライアンスにログインできません。アプライアンスの問題を解決するために、アプライアンスを再展開することにしました。

手順

1. vCenter Server から古い Carbon Black Cloud Workload アプライアンス を削除します。詳細については、vCenter Server からのアプライアンスの削除 を参照してください。
2. ステップ 1A: Carbon Black Cloud Workload アプライアンス を vCenter Server に展開するの説明に従って、Carbon Black Cloud Workload アプライアンス を展開します。

   注： アプライアンスのユーザー インターフェイスにアクセスできない場合は、Web ブラウザの SSL 証明書キャッシュをクリアしてから、アプライアンスにログインします。
3. オンプレミスの vCenter Server にアプライアンスを登録の説明に従って、アプライアンスを同じ SSO および vCenter Server に登録します。
4. API ID とキーを生成します。詳細については、手順 1C：API ID と API プライベート キーの生成を参照してください。

   重要： アプライアンス名は Carbon Black Cloud 組織に固有である必要があります。元のアプライアンス名や、すでに登録されているアプライアンスの API ID と API プライベート キーは使用できません。
5. API ID と API プライベート キーを使用してアプライアンスを登録します。詳細については、Carbon Black Cloud Workload アプライアンスを Carbon Black Cloud に接続する を参照してください。

アプライアンスのログ

アプライアンスのログ バンドルでは、VMware サポート チームおよびエンジニアリング チームが発生した問題のトラブルシューティングを行うために必要な診断情報が収集されます。サポート チームは、詳細な分析とトラブルシューティングを行うため、クラウドからアプライアンスのログ バンドルを収集できます。アプライアンスから各サービスのログ レベルを設定できます。VMware サポート チームは問題のトラブルシューティング中に、アプライアン

スのログ レベルを変更するように、またはログをエクスポートするように求めることができます。VMware サポート チームは、ログを *prod.cwp.carbonblack.io* ドメインにアップロードします。

ログのエクスポート オプションとログ レベル オプションを構成できます。ログ レベルは、*Root* や *com.vmware.cwp* などの組み込みパッケージ ファイルで構成できます。デフォルトで、*Root* には[警告]が、*com.vmware.cwp* には[情報]がログ レベルとして割り当てられています。

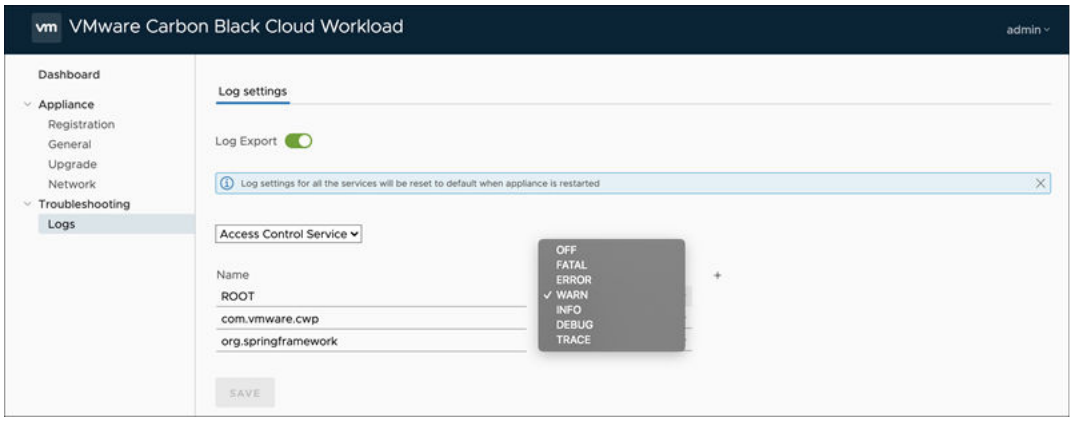
前提条件

- TCP ポート 443 を使用して、*prod.cwp.carbonblack.io* ドメインのファイアウォールを開く必要があります。
- VMware サポート チームは、アプライアンスのログ レベルを変更し、トラブルシューティング用にログをエクスポートできます。トラブルシューティングの目的でログを VMware と共有しない場合は、[ログのエクスポート]を[オフ]に切り替えます。

手順

1 ブラウザから、**admin** 認証情報を使用して vCenter Server (**https://<vCenter IP/Domain address>**) にログインします。Carbon Black Cloud Workload アプライアンス はこちらにあります。

2 [Troubleshooting (トラブルシューティング)] - [Logs (ログ)] ページに移動します。



3 [ログのエクスポート]: デフォルトで、[ログのエクスポート] トグルスイッチは[オン]になっています。ログのエクスポートを[オフ]に切り替えます。

ログは、2 か月ごとの保持スケジュールで削除されます。

4 リストから必要なサービスを選択します。ログ レベルの設定を変更するには、次のようにリストから必要なログ レベルを選択します。

ログ レベル	説明
[オフ]	ログはオフ状態です。このオプションを使用して、特定のサービスのログをオフにします。
[エラー]	アプリケーションを引き続き実行できる可能性のあるエラー イベントのみを記録します。
[警告]	有害な可能性のある状況を記録します。

ログ レベル	説明
[情報]	アプリケーションの進行状況を大まかに強調する情報メッセージを記録します。
[デバッグ]	アプリケーションのデバッグに最も役立つ詳細な情報イベントを記録します。
[トレース]	デバッグ レベルよりも詳細な情報イベントを記録します。

5 変更内容を保存するには、[Save (保存)] をクリックします。

結果

ログのエクスポートとログ レベルの設定が変更されます。

vSphere 環境での Carbon Black の更新

6

更新されたセンサー バージョンが Carbon Black Cloud Workload Plug-in から使用可能な場合は、Carbon Black センサーを更新できます。アプライアンスのアップグレード頻度をスケジュール設定することで、アプライアンスとプラグインを一緒にアップグレードできます。

次のトピックを参照してください。

- 仮想マシンの Carbon Black の更新
- Carbon Black Cloud Workload アプライアンスをアップグレード

仮想マシンの Carbon Black の更新

ワークロードが実行されている仮想マシン (VM) で、Carbon Black センサーをすぐに更新できます。

有効になっているすべての仮想マシンで Carbon Black を更新します。

手順

1 管理者の認証情報を使用して vSphere Client にログインします。

2 左側のナビゲーション ペインで、[Carbon Black] をクリックします。

3 [インベントリ] - [有効] タブに移動します。

4 Carbon Black を更新する 1 つ以上の仮想マシンを選択して、[更新] をクリックします。

確認ダイアログ ボックスが表示されます。

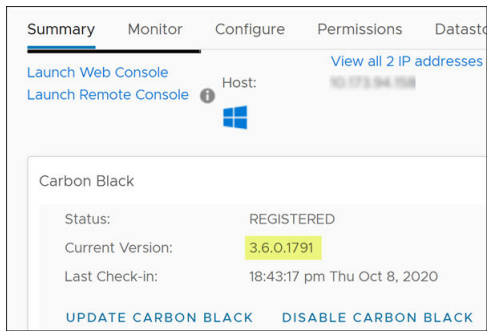
5 [OK] をクリックします。

結果

Carbon Black を使用可能な最新のセンサー バージョンに更新します。

個々の仮想マシンの Carbon Black を更新することもできます。更新する仮想マシン（Windows または Linux）に移動し、[サマリ] タブで Carbon Black パネルまでスクロールします。また、[構成] - [Carbon Black] - [セキュリティ] タブを使用することもできます。

センサーのバージョンは、Carbon Black パネルで確認できます。



Carbon Black Cloud Workload アプライアンスをアップグレード

インスタント アプライアンスのアップグレードまたはスケジュール設定されたアップグレードを実行できます。

アップグレード頻度をスケジュール設定することで Carbon Black Cloud Workload アプライアンス を自動的にアップグレードします。新しいアップグレード バンドルが使用可能になると、選択した日時に基づいてアプライアンスがアップグレードされます。

スケジューラをバイパスするには、[Upgrade Now (今すぐアップグレード)] ボタンを使用します。これは、環境内の重大な問題に対応する必要がある場合に必要になることがあります。

前提条件

TCP ポート 443 を使用して、*prod.cwp.carbonblack.io* ドメインのファイアウォールを開く必要があります。

手順

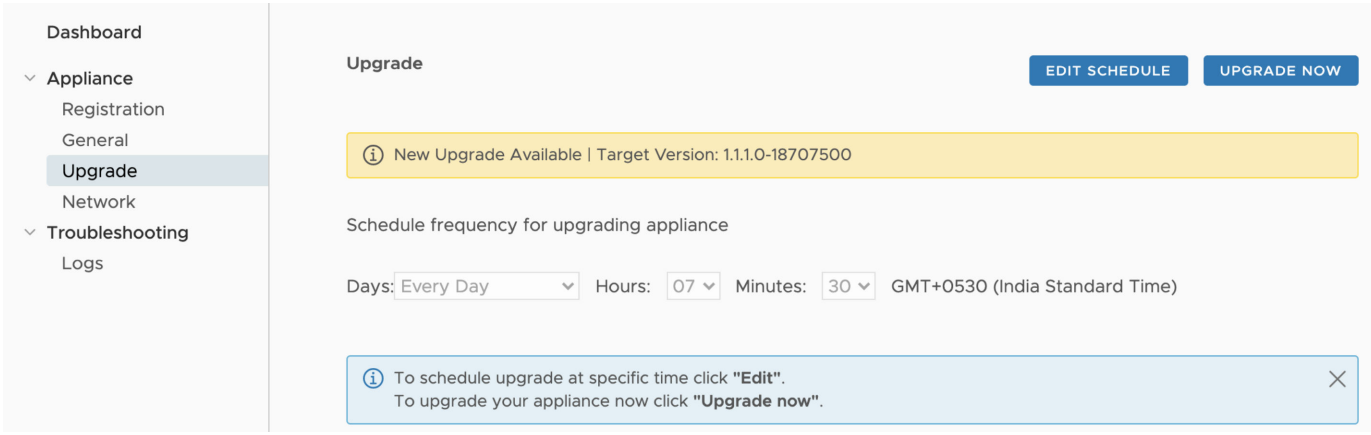
1 ブラウザから、**admin** 認証情報を使用して vCenter Server (**https://<vCenter IP/Domain address>**) にログインします。Carbon Black Cloud Workload アプライアンス はこちらにあります。

2 [Appliance (アプライアンス)] - [Upgrade (アップグレード)] ページに移動します。

3 [Edit (編集)] をクリックして、アップグレードに必要な日、時間、および分を選択します。

4 [Save (保存)] をクリックして、アプライアンスのアップグレードをスケジュール設定します。

アップグレードの日時を、ローカル タイム ゾーンで設定します。アプライアンスは、ローカル時間を UTC 時間に変換します。アップグレードは、アプライアンスの UTC タイム ゾーンで行われます。

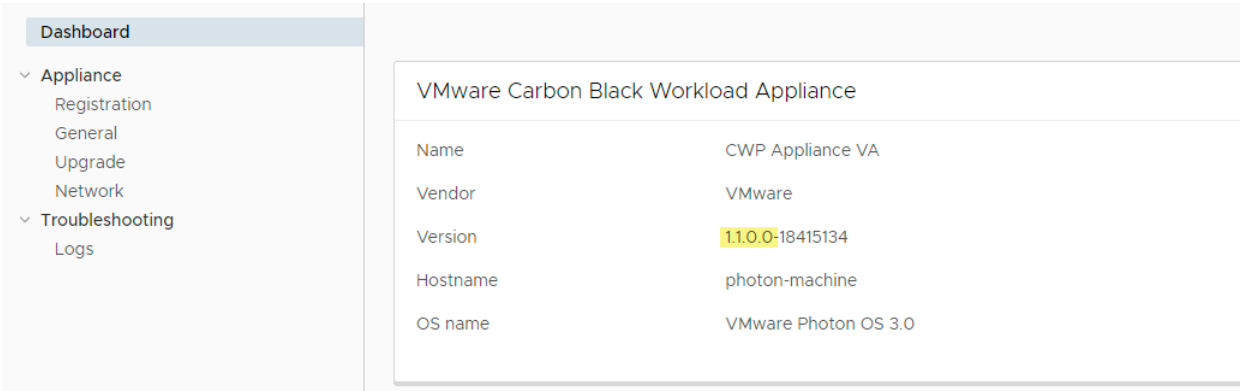


5 オプション。[Upgrade Now (今すぐアップグレード)] ボタンをクリックして、Carbon Black Cloud Workload アプライアンス をすぐにアップグレードします。

[Upgrade Now (今すぐアップグレード)] ボタンは、アップグレードが利用可能な場合にのみ表示されます。

結果

アプライアンスのアップグレード後に Carbon Black Cloud Workload Plug-in もアップグレードされます。アプライアンス ダッシュボードに、新しいバージョンとビルド番号を表示できます。



アプライアンスを 1.0.2 にアップグレード

アプライアンスのバージョン 1.0.2 への自動アップグレードが機能していません。ZIP 解凍エラーが原因で、ダウンロードしたアップグレード バンドルの抽出に失敗します。このトピックで説明する手順に使って、アプライアンスを 1.0.2 バージョンにアップグレードする必要があります。

1 アプライアンスのアップグレード ステータスを確認します。

a ブラウザから、**admin** 認証情報を使用して Carbon Black Cloud Workload アプライアンス (**https://<appliance IP address>**) にログインします。

b [Appliance (アプライアンス)] - [Upgrade (アップグレード)] ページに移動します。

c 自動アップグレードは、設定した日時に開始されます。自動アップグレードに失敗した場合は、アップグレードに失敗エラーが表示されます。

2 アップグレードの失敗理由を確認します。

a *admin* 認証情報を使用してアプライアンス CLI に SSH 接続します。例: `ssh admin@<appliance IP address>`。

b 次のコマンドを実行します。

```
cat /var/log/cwp/apw_upgrade_status.json
```

c 出力のステータス フィールドの値を確認します。サンプル出力は次のとおりです。

```
{"status":"EXTRACTING_WRAPPER_BUNDLE_FAILED","reboot_pending":null,"message":"Zip
entry breaches extract location, entry resolved path: /var/vmware/bundle/bundles/
staging/wrapper-1.0.2.0-xxxxxxxx/cwp-appliance-bundle- 1.0.2.0-xxxxxxxx.zip, extract
location/opt/vmware/cwp/etc/bundles/staging/wrapper- 1.0.2.0-
xxxxxxxx","source_version":null,"target_version":"1.0.2.0-xxxxxxxx"}
```

- ステータスが *EXTRACTING_WRAPPER_BUNDLE_FAILED* の場合、ZIP 解凍エラーが原因でアップグレード バンドルのダウンロードに失敗します。このエラーは、すべての 1.0.1 アプライアンスで発生します。アップグレードの次の手順に進みます。
- ステータスが *TIMEDOUT_WAIT_FOR_TERMINAL_STATUS* の場合、アプライアンスの *root* および *admin* のパスワードが期限切れになります。アップグレードを進めるには、まずパスワードをリセットする必要があります。アプライアンスのパスワードは 90 日後に期限が切れます。アプライアンス パスワードのリセット トピックの説明どおりにパスワードを変更し、次の手順に進みます。

3 シェル (.sh) スクリプト ファイルを次のようにダウンロードして実行します。

a 次のリンクをクリックします。スクリプト ファイルがダウンロードされます。ファイルをローカル マシンに展開します。

https://community.carbonblack.com/gbouw27325/attachments/gbouw27325/cloud_workload_documents/7/1/update-config.zip」を参照してください。

-OR-

次のコードを `update-config` シェル スクリプト ファイルとしてコピーします。

```
CONFIG_FILE="/opt/vmware/cwp/appliance-worker/config/application.yml"

if grep -q "upgrade.staging.location" "${CONFIG_FILE}"
then
    # Already exists, nothing to do
    echo "Settings already up-to-date. Nothing to do!"
else
    # Add config and restart service
    echo "Updating config..."
    sed "-i.$(date +%s)" '1i upgrade.staging.location: /var/vmware/bundle/bundles/
staging' "${CONFIG_FILE}"
```

```
    echo "Restarting appliance worker service..."
    systemctl restart cwp-appliance-worker.service
    sleep 10

    echo "Settings updated successfully!"
fi
```

b 次のコマンドを使用して、スクリプト ファイルをアプライアンス仮想マシンにコピーします。

Linux:

```
scp <Location_Of_update-config.sh_File> admin@<Appliance_VM_IP>:
admin@<Appliance_VM_IP>'s password:
```

Windows:

```
pscp -scp -P 22 <Location_Of_update-config.sh_File> admin@<Appliance_VM_IP>:
admin@<Appliance_VM_IP>'s password:
```

c *admin* 認証情報を使用してアプライアンス仮想マシンに SSH 接続し、*root* ユーザーに切り替えます。

```
ssh admin@<Appliance_VM_IP>
Warning: Permanently added '<Appliance_VM_IP>' (RSA) to the list of known hosts.
admin@<Appliance_VM_IP>'s password:
admin@<Appliance_VM_IP> [ ~ ]$ su -
Password:
root@<Appliance_VM_IP> [ ~ ]#
```

d 次のコマンドを使用してファイルの権限を変更し、ファイルを実行可能にします。

```
# chmod +x /home/admin/update-config.sh
```

e 次のコマンドを使用してスクリプトを実行します。

```
# ./update-config.sh
```

f サンプル出力は次のように表示されます。

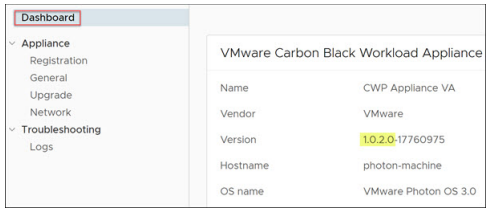
```
Updating config...
Restarting appliance worker service...
Settings updated successfully!
```

4 アプライアンスのアップグレードをスケジュール設定します。アップグレードの詳細については、Carbon Black Cloud Workload アプライアンスをアップグレード を参照してください。

アップグレードがスケジュールどおりにトリガされると、アプライアンス ユーザー インターフェイスのアップグレード ページで結果を監視します。アップグレード プロセスは通常、10 ～ 15 分以内に完了します。

5 アップグレードを確認するには、次の手順を実行します。

- アプライアンス ダッシュボードに移動します。更新されたバージョンとビルド番号を表示できます。



- [Upgrade (アップグレード)] ページに移動します。アップグレード関連のエラー メッセージがないことを確認します。

vSphere 環境からの Carbon Black の無効化

7

Carbon Black Cloud コンソールから、または手動で Carbon Black センサーを無効にできます。無効なセンサーは、[登録解除済み] として表示されます。

不要になったアプライアンスをアンインストールできます。

次のトピックを参照してください。

- Carbon Black センサーの手動アンインストール
- vCenter Server からのアプライアンスの削除

Carbon Black センサーの手動アンインストール

Carbon Black センサーを手動で登録解除できます。センサーは、Carbon Black Cloud コンソールから削除されるまで、*登録解除済み* として Carbon Black Cloud Workload Plug-in に保持されます。

Windows 仮想マシンでのセンサーの手動アンインストール

Windows 仮想マシンのセンサーを手動でアンインストールするには、ナレッジベースの記事に記載されている手順に従ってください。

Linux 仮想マシンでのセンサーの手動アンインストール

Linux 仮想マシンのセンサーを手動でアンインストールするには、ナレッジベースの記事に記載されている手順に従ってください。

Carbon Black Cloud コンソールからのセンサーのアンインストール

Carbon Black Cloud コンソールからセンサーをアンインストールする方法、および登録解除されたセンサーを削除する方法については、Carbon Black Cloud センサーのインストール ガイドを参照してください。

vCenter Server からのアプライアンスの削除

以前に展開した Carbon Black Cloud Workload アプライアンス 仮想マシン (VM) を vCenter Server から削除できます。

前提条件

Carbon Black Cloud Workload アプライアンス 仮想マシンが展開されています。

手順

1 ブラウザから、**admin** 認証情報を使用して vCenter Server (**https://<vCenter IP/Domain address>**) にログインします。Carbon Black Cloud Workload アプライアンス はこちらにあります。

2 [アプライアンス] - [登録]タブに移動します。

3 SSO ルックアップ構成セクションで、[編集] をクリックし、[登録解除] をクリックします。

4 vCenter Server の詳細セクションで、[登録解除] をクリックします。

確認ダイアログ ボックスが表示されます。

5 登録解除するには、[OK] をクリックします。

6 管理者の認証情報を使用して vSphere Client にログインします。

7 Carbon Black Cloud Workload アプライアンス 仮想マシンをパワーオフします。

8 データストアから Carbon Black Cloud Workload アプライアンス 仮想マシンを削除するには、アプライアンス仮想マシンを右クリックします。

9 [ディスクから削除] を選択し、[OK] をクリックします。詳細については、vSphere のドキュメントを参照してください。

アプライアンスは vCenter Server から削除されます。Carbon Black Cloud Workload Plug-in もアンインストールされます。確認するには、ログアウトして vCenter Server にログインします。

10 Carbon Black Cloud コンソールには、アプライアンスの健全性ステータスが [切断] として表示されます。アプライアンスのステータスは、Carbon Black Cloud コンソールで次のように確認できます。

a Carbon Black Cloud コンソールにログインします。

b 左側のナビゲーション ペインから、[設定] - [API アクセス] - [API キー] 画面の順にクリックします。

c アプライアンス API に移動します。アプライアンスの API 名の横にリンクが付いたアプライアンス名が表示されます。

d リンク付きアプライアンス名をクリックします。アプライアンスの健全性ステータスが [切断] として表示されていることを確認できます。

結果

Carbon Black Cloud Workload アプライアンス 仮想マシンは完全に削除されます。

仮想マシンのクローンと Carbon Black Cloud Workload

8

Carbon Black Cloud Workload が有効になっている仮想マシンのクローンを手動で作成すると、一貫性のない動作が発生することがあります。親仮想マシンとクローン仮想マシンは、[有効] タブと [無効] タブの両方に表示されることがあります。Carbon Black Cloud コンソールでも同様の動作が発生することがあります。この問題は、Carbon Black センサーが同じ ID を使用してバックエンドに対する両方の仮想マシンを識別するため発生します。この問題を解決するには、手動で手順を実行し、クローン作成された仮想マシンを Carbon Black Cloud に再登録する必要があります。

Windows 仮想マシン

既存のクローンの問題を次のように修正します。

1 クローン仮想マシンにログインします。たとえば、*WIN10_X64_VDI* です。

2 次のように `repcli reregister` コマンドを実行します。

```
repcli reregister now
```

クローン仮想マシンが再登録され、問題が修正されます。

ゴールド イメージから作成されるクローンが正しく再登録されるように、ゴールド イメージの問題を修正する必要があります。次のように問題を修正します。

1 Carbon Black センサーがインストールされている親仮想マシンにログインします。たとえば、*WIN10_X64_GOLDEN* です。

2 RepCLI ユーティリティにアクセスします。

3 バックグラウンド スキャンを完了し、`RepCLI Status` コマンドを使用してポリシーが更新されていることを確認します。

```
C:\Program Files\Confer> repcli status
```

4 クローン仮想マシンの再登録をスケジュール設定します。次の `repcli reregister` コマンドを使用します。*MASTER* を親仮想マシンのコンピュータ名に変更します。

```
if /i %computername% == MASTER (echo Skipping reregistration) ELSE ("C:\Program
Files\Confer\RepCLI.exe" reregister now) > C:\Temp\CB_reregister.txt
```

例:

```
if /i %computername% == WIN10_X64_GOLDEN (echo Skipping reregistration) ELSE ("C:\Program Files\Confer\RepCLI.exe" reregister now)
```

5 ゴールド イメージからクローンを今すぐ作成します。

クローン仮想マシンに次回ログインすると、スケジュール設定されたコマンドが実行され、クローン作成された仮想マシンが登録されます。

6 クローン仮想マシンにログインします。たとえば、*WIN10_X64_VDI* です。クローン仮想マシンは個別のデバイスとして登録され、新しいデバイス ID が割り当てられます。

詳細については、ナレッジベース (KB) を参照してください。詳細については、『Carbon Black Cloud センサー インストール ガイド』の「*VDI 環境へのセンサーのインストール*」を参照してください。

Linux 仮想マシン

クローン Linux 仮想マシンを Carbon Black Cloud バックエンドに登録する手順を実行します。

1 クローン仮想マシンにログインします。たとえば、*LIN_CENTOS_VDI* です。

2 次のコマンドを使用して *cbagentd* を停止します。Linux ディストリビューションに基づいて root 権限を使用してコマンドを実行します。

- CentOS/RHEL/Oracle 6 の場合は、次のコマンドを使用します。

```
$ sudo service cbagentd stop
```

- その他のすべてのディストリビューションでは、次のコマンドを使用します。

```
$ sudo systemctl stop cbagentd
```

3 次のコマンドを使用して、クローン仮想マシンを登録します。

```
$ sudo /opt/carbonblack/psc/bin/cbagentd -R
```

クローン仮想マシンは個別のデバイスとして登録され、新しいデバイス ID と登録 ID が割り当てられます。

4 次のコマンドを使用して *cbagentd* を開始します。Linux ディストリビューションに基づいて root 権限を使用してコマンドを実行します。

- CentOS/RHEL/Oracle 6 の場合は、次のコマンドを使用します。

```
$ sudo service cbagentd start
```

- その他のすべてのディストリビューションでは、次のコマンドを使用します。

```
$ sudo systemctl start cbagentd
```

VMware Carbon Black Sensor Gateway ユーザー ガイド

9

『Carbon BlackSensor Gateway ユーザー ガイド』では、VMware Carbon Black® Sensor Gateway™ をインストール、構成、および使用してクラウド接続を保護する方法について説明します。

重要： このコンテンツのスタンドアローン PDF バージョンについては、「VMware Carbon Black Cloud Workload ガイド PDF」を参照してください

オンプレミス コンポーネントの Sensor Gateway は、ワークロードに展開された Carbon Black センサーと Carbon Black Cloud の間のすべてのインバウンドおよびアウトバウンド通信のブリッジとして機能します。

対象ユーザー

このガイドは、Windows または Linux システム管理者としての経験があり、仮想マシン テクノロジーおよびデータセンターの運用に詳しい方を対象としています。また、本書では、VMware ESXi™、VMware vCenter Server®、VMware Tools™ などの VMware vSphere® について理解していることを前提としています。

次のトピックを参照してください。

- Sensor Gateway 概要
- Carbon Black Sensor Gateway のインストールと使用
- Sensor Gateway アプライアンスのアップグレード
- Sensor Gateway のトラブルシューティング
- Linux への Sensor Gateway のインストール

Sensor Gateway 概要

アセットにインストールされているセンサーと Carbon Black Cloud との間の通信を制御できます。センサーは、クラウドに直接接続することも、Sensor Gateway を介して接続することもできます。

次の場合は、Sensor Gateway の使用を検討してください。

- 厳しく管理された環境を運用し、ワークロードの安全性を確保し、インターネット トラフィックに直接さらされないようにする場合。
- 追加のプロキシ サーバの所有、管理、および予算作成の負担を軽減する場合。
- 企業ポリシーまたはコンプライアンス要件により、Carbon Black Cloud とのセンサー通信が不可能なネットワーク環境がある場合。

Sensor Gateway には、Carbon Black Cloud に登録されている場合にのみ通信を可能にする登録メカニズムがあります。API キー メカニズムを使用して、不正な Sensor Gateway サーバがクラウドとの通信を開始できないことを確認します。

このリリースで、Carbon Black Cloud は OVA としての Sensor Gateway 展開をサポートします。OVA を展開する場合は、vSphere Client または ESXi Web Client のいずれかを使用できます。詳細については、アプライアンスとして Sensor Gateway をインストール を参照してください。

Carbon Black Cloud コンソールは、最大接続数やリソース容量に達した場合や、Sensor Gateway が停止している場合など、Sensor Gateway サーバ障害の状態に関する通知をトリガします。

Carbon Black Sensor Gateway のインストールと使用

このセクションでは、Sensor Gateway をインストール、構成、および使用する方法について説明します。

Sensor Gateway インストールの準備

Sensor Gateway をインストールする前に環境を準備します。

環境の設定

Sensor Gateway アプライアンスのインストールを正常に実行するには、インストーラを実行する前に必要なタスクと事前チェックを実行する必要があります。

- SSL 署名付き証明書をプロビジョニングします。次のいずれかを選択します。
  - 認証局 (CA) 署名付き証明書この証明書が優先されます。詳細については、Sensor Gateway 証明書 を参照してください。
  - 自己署名付き証明書。この証明書は、各センサー ワークロードのトラスト ストアにこれらの証明書をプッシュする必要があります。詳細については、Sensor Gateway 証明書 を参照してください。

  注： 使用している証明書のプライベート キーが必要です。
- CA 署名付き証明書、または Online Certificate Status Protocol (OCSP) レスポンダを持つ内部証明書がある場合は、証明書チェーン全体をプロビジョニングする必要がある場合があります。Sensor Gateway は、証明書とそのチェーンを使用して OCSP 応答を取得し、すべての要求とホチキス留めします。これにより、センサーが OCSP レスポンダに直接アクセスできなくなります。

  証明書チェーンの構成を提供する任意のオンライン サービスを使用して、証明書チェーン ファイルを生成します。詳細については、証明書チェーン ファイルの作成 を参照してください。
- 各 Sensor Gateway サーバの固定 IP アドレスを取得します。
- DNS エントリを予約します。例：`sensorgateway.company.com`

  環境に Sensor Gateway をインストールするには、その DNS をサーバに以前に割り当てた IP アドレスにマッピングします。

  FQDN を使用して Sensor Gateway を構成する場合は、IP アドレスへの DNS マッピングを使用します。

  注： IP アドレスのみを使用し、IP アドレスを CN と同じにして証明書を作成できます。

- Sensor Gateway のプロキシ機能を使用していて、Sensor Gateway と Carbon Black Cloud の間にプロキシ サーバがある場合は、プロキシを介して Carbon Black Cloud URL にアクセスできることを確認する必要があります。
- センサーのダウンロードがローカル サーバから更新されるように、シグネチャの更新についてローカル ミラー サーバを設定しポリシーを設定します。「シグネチャ ミラーの手順」を参照してください。更新サーバのミラーを設定する場合は、プロキシ経由でアクセス可能であることを確認します。

Sensor Gateway API キーのプロビジョニング

Carbon Black Cloud コンソールから API キーを生成し、生成された API キーを使用して、vCenter Server に展開された Carbon Black Cloud コンソールと Sensor Gateway の間の接続を確立する必要があります。複数の Sensor Gateway を構成している場合、各インスタンスに個別の API キーを生成します。

事前定義されたカスタム アクセス レベルを使用して、Sensor Gateway の API キーを生成します。同じカスタム アクセス レベルを使用して、組織に複数の Sensor Gateway インスタンスを構成できます。

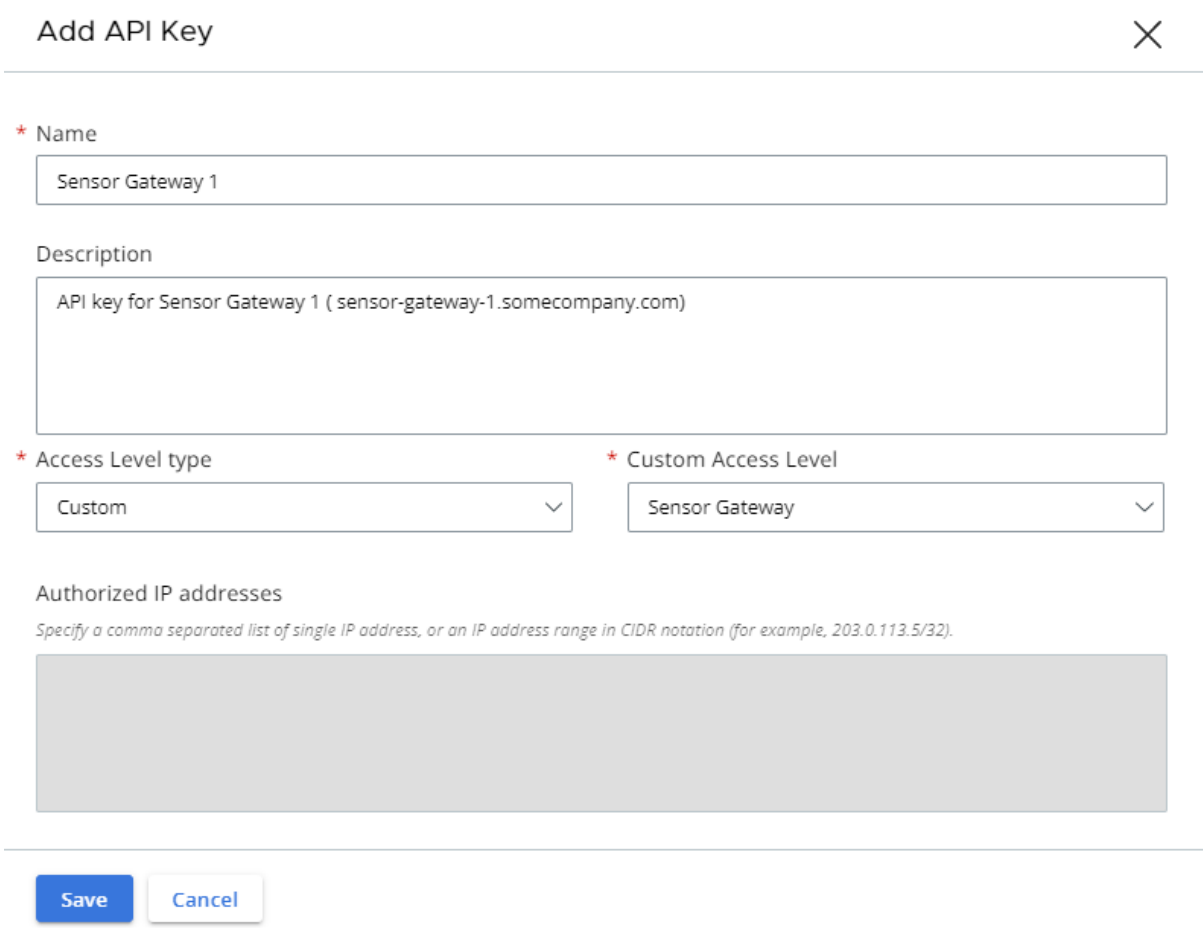
手順

1. Carbon Black Cloud コンソールにログインします。
2. [設定] - [API アクセス] - [API キー] 画面に移動します。
3. [API キーを追加] をクリックします。

   [API キーを追加] ウィンドウが表示されます。
4. Sensor Gateway API キーの名前を入力します。

   名前は組織において一意である必要があります。
5. [アクセス レベル タイプ] ドロップダウン メニューから [カスタム] を選択します。

6 [カスタム アクセス レベル] ドロップダウン メニューから [Sensor Gateway] を選択します。



7 API キーを生成するには、[保存] をクリックします。

Carbon Black Cloud コンソールは、API ID と API プライベート キーを生成します。

8 認証情報をコピーします。

後でこれらのキーを使用して、Sensor Gateway と Carbon Black Cloud の間の接続を確立します。

注： Sensor Gateway ごとに使用できる API ID とプライベート キーのセットは 1 つだけです。Sensor Gateway に生成された認証情報を使用すると、他のインスタンスに同じ API ID とプライベート キーを使用できなくなります。

9 API キーを後で表示してコピーするか、新しい API プライベート キーを生成するには、次の手順を実行します。

a [設定] - [API アクセス] - [API キー] 画面に移動します。

b 前に作成した Sensor Gateway API 名に移動し、[アクション] 列の下矢印をクリックします。

c [API 認証情報] を選択します。

[API 認証情報] ダイアログ ボックスが表示されます。API ID と API プライベート キーをコピーできます。

Carbon Black Cloud のアクセス

次の環境固有の URL への接続を許可するように、ファイアウォールで保護されたネットワークを構成する必要があります。

ファイアウォールをさらに構成し、追加の URL へのアクセス権を付与するには、「ファイアウォールの構成 」を参照してください。

Carbon Black Cloud API URL

環境	AWS リージョン	Carbon Black Cloud URL	デバイスサービス URL
Prod05	US-East-1	https://defense-prod05.conferdeploy.net	https://dev-prod05.conferdeploy.net
Prod06	EU-Central-1	https://defense-eu.conferdeploy.net	https://dev-prod06.conferdeploy.net
ProdNRT	AP-Northeast-1	https://defense-prodnrt.conferdeploy.net	https://dev-prodnrt.conferdeploy.net
ProdSYD	AP-Southeast-2	https://defense-prodsyd.conferdeploy.net	https://dev-prodsyd.conferdeploy.net
UK PoP	EU-West-2	https://ew2.carbonblackcloud.vmware.com	https://ew2-device.carbonblackcloud.vmware.com

Sensor Gateway 関連 URL

環境	Carbon Black Cloud URL	AWS URL	IP アドレス	プロトコル/ポート
Prod05	https://defense-prod05.conferdeploy.net	psc-cwp-prod-applianceservice-content-us.s3.us-east-1.amazonaws.com	動的	TCP/443
Prod06	https://defense-eu.conferdeploy.net	psc-cwp-prod-applianceservice-content-eu.s3.us-east-1.amazonaws.com	動的	TCP/443
ProdNRT	https://defense-prodnrt.conferdeploy.net	psc-cwp-prod-applianceservice-content-au.s3.us-east-1.amazonaws.com	動的	TCP/443

環境	Carbon Black Cloud URL	AWS URL	IP アドレス	プロトコル/ポート
ProdSYD	https://defense-prodsyd.conferdeploy.net	psc-cwp-prod-applianceservice-content-ap.s3.us-east-1.amazonaws.com	動的	TCP/443
UK PoP	https://ew2.carbonblackcloud.vmware.com	prd1ew2-applianceservice-infra-content.s3.eu-west-2.amazonaws.com	動的	TCP/443

Sensor Gateway 証明書

Carbon Black センサー は、証明書を介して Sensor Gateway と通信します。Sensor Gateway は、CA 署名付き証明書と自己署名付き証明書の両方で実行できます。Carbon Black では、信頼された証明書を各マシンに個別にインストールする代わりに、必要なすべての証明書をすべての Sensor Gateway サーバに一度にインストールできるように、CA 署名付き証明書を使用することをお勧めします。

CA 書名付き証明書

認証局 (CA) が証明書を発行すると、証明書には完全修飾ドメイン名 (FQDN) が関連付けられ、CA を信頼するすべてのブラウザまたはデバイスがこの証明書と通信できます。

たとえば、sensorgateway.company.com という CA 署名付き証明書がある場合、ブラウザで開いたとき、または Carbon Black センサー が Sensor Gateway と通信しようとしたとき、マシンの完全修飾ドメイン名（FQDN）が証明書に一致していれば、証明書の検証エラーは発生しません。

CA 証明書を生成するプロセスでは、IP アドレスを割り当てることができます。ブラウザまたは Carbon Black センサー が、https://sensorgateway.company.com または IP アドレス（サブジェクトの代替名または共通名で使用可能）で Sensor Gateway と通信すると、ブラウザもセンサーもエラーを生成しません。

サブジェクトの代替名 (SAN) の IP アドレスと共通名 (CN) の FQDN を含む証明書があり、一部のセンサーが FQDN を使用して Sensor Gateway にアクセスし、他のセンサーが IP アドレスを介してアクセスする場合、Sensor Gateway エントリ ポイントを IP アドレスに登録する必要があります。これにより、Carbon Black Cloud がセンサーに URL を送信すると、URL は Sensor Gateway を指し示すように変更されます。

自己署名付き証明書

CA 署名付き証明書と同様に、自己署名付き証明書でも、証明書の生成時に提供される CN は、マシンの FQDN または IP アドレスと一致する必要があります。自己署名付き証明書を生成するときに、CN の入力を求められたら IP アドレスまたは FQDN を指定できます。たとえば、自己署名付き証明書の CN に IP アドレス 192.168.10.100 を使用する場合は、この同じ IP アドレスを持つ Sensor Gateway マシンにこの証明書をインストールする必要があります。そのように、センサーが Sensor Gateway にアクセスすると、証明書は有効になります。

証明書チェーン ファイルの作成

Carbon Black は、証明書チェーン ファイルを使用して適切な OCSP ステープリングを実行します。

任意のオンライン証明書チェーン コンポーザを使用して Certificate Chain Composer を生成できます。例：KeyCDN Tools。次の手順は、Certificate Chain Composer を使用して証明書チェーンを作成する例です。

手順

1 任意のエディタで証明書 `sgw_certificate.pem` を編集し、`-----BEGIN CERTIFICATE-----` と `-----END CERTIFICATE-----` と一緒にすべてのコンテンツをコピーします。

証明書にすでにチェーンがある場合は、最初に発生した `-----BEGIN CERTIFICATE-----` と `-----END CERTIFICATE-----` のみをコピーします。

2 Certificate Chain Composer サイトのテキスト ボックスにコンテンツを貼り付け、[作成] をクリックします。

このツールは、独自の証明書と証明書の署名に使用されるすべての証明書のチェーン全体を生成します。画面の下半分に証明書チェーンが表示されます。

3 コンテンツ全体をコピーし、任意のエディタに貼り付けます。

注： `-----BEGIN CERTIFICATE-----` から `-----END CERTIFICATE-----` の証明書内のセクションに対応するセクションを削除します。

4 `sgw_chain.pem` ファイルとして保存します。

5 Sensor Gateway をホストしているサーバの `/data/certs` ディレクトリに `sgw_chain.pem` ファイルをコピーします。

6 Sensor Gateway で OCSP Stapling が正しく動作するようにするには、次のコマンドを実行します。

a `openssl x509 -noout -ocsp_uri -in sgw_certificate.pem`

証明書の OCSP レスポンダ URL を出力します。

b `openssl ocsp -issuer sgw_chain.pem -cert sgw_certificate.pem -verify_other sgw_chain.pem -CAfile sgw_chain.pem -no_nonce -url <前のコマンドの OCSP レスポンダ URL>`

OCSP レスポンダからの応答を出力します。たとえば、

```
sgw_certificate.pem: good
This Update: Jul 18 15:35:01 2023 GMT
Next Update: Jul 25 15:35:00 2023 GMT
```

応答がない場合は、ネットワーク接続/ファイアウォール構成を確認して、OCSP 応答が OCSP レスポンダから受信されていることを確認できます。

アプライアンスとして Sensor Gateway をインストール

Sensor Gateway を vSphere Client から Windows 仮想マシンにインストールするか、Web Client インターフェイスを使用して ESXi ホストに直接インストールします。OVA ファイルまたは OVF ファイルのインストールを選択できます。

次の手順に従って、Sensor Gateway ホストに ESXi アプライアンスを直接展開するには、ESXi Web Client インターフェイス (`https://ESXi_host_IP_address_or_hostname`) にログインし、[仮想マシン] を右クリックして [仮想マシンの作成/登録] を選択します。[OVF または OVA ファイルから仮想マシンを展開] を選択すると、手順 4 以降を参照してインストール ウィザードを進めることができます。

前提条件

- API アクセス認証情報が使用可能であることを確認します。詳細については、Sensor Gateway API キーのプロビジョニング を参照してください。
- 環境が必要なネットワーク設定で構成されていることを確認します。詳細については、「ファイアウォールの構成」を参照してください。
- 仮想マシンでのファイアウォール設定でポート 443 の `projects.registry.vmware.com` がブロックされていないことを確認します。

手順

1 vSphere Client を使用して、vCenter Server にログインします。

a Web ブラウザを開き、vCenter Server インスタンスの URL を入力します (**`https://vcenter_server_ip_address_or_fqdn`**)。

b 潜在的なセキュリティ リスクに関する警告メッセージが表示された場合は、Web サイトへの移動の続行を選択します。

ブラウザ	アクション
Microsoft Edge	1 [詳細] をクリックします。 2 表示されたメッセージの下の [Web ページへ移動] をクリックします。
Mozilla Firefox	1 [[Advanced (詳細)]] をクリックします。 2 表示されたメッセージの下の [リスクを受け入れて続行] をクリックします。
Google Chrome	1 [[Advanced (詳細)]] をクリックします。 2 表示されたメッセージの下の [*vcenter_server_ip_address_or_fqdn* に進む] をクリックします。

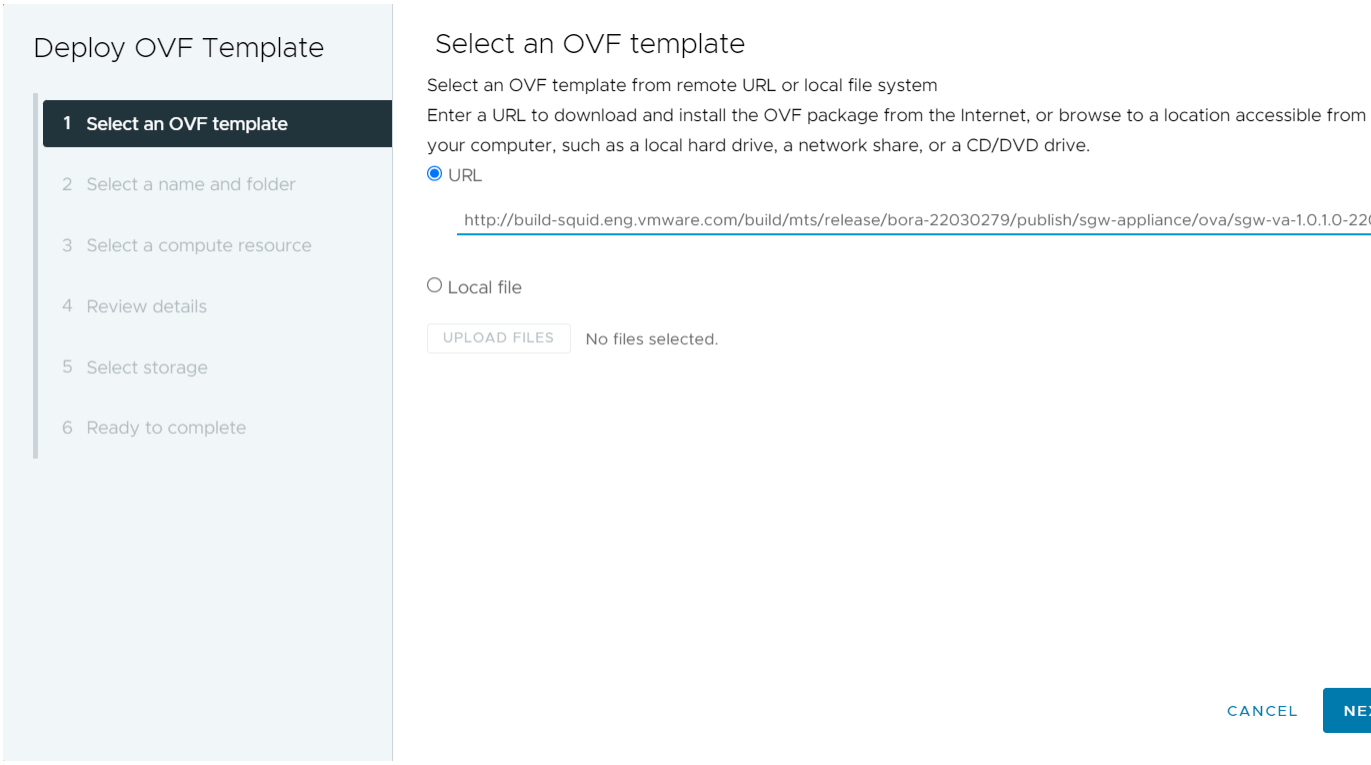
c vSphere のトップ ページで、[vSphere Client (HTML5) の起動] を選択します。

d vCenter Server に対する権限があるユーザーの認証情報を入力し、[ログイン] をクリックします。

vSphere Client が、指定されたユーザーが権限を持つすべての vCenter Server システムに接続されて、vSphere インベントリを表示および管理できるようになります。

2 Sensor Gateway アプライアンス インストーラ `sgw-va-1.2.0.0-22635557_OVF10.ova` を取得するには、[Customer Connect のダウンロード] 画面に移動し、 CBC-CWP-SensorGateway-OVA-122 の下の [今すぐダウンロード] をクリックします。

3 データセンター内のクラスタに移動し、ESXi ホストを右クリックして、[OVF テンプレートの展開] 選択します。



[OVF テンプレートの展開] ウィザードが表示されます。

4 次のいずれかのオプションでテンプレートを選択し、[次へ] をクリックします。

- コピーした OVA リンク アドレスを使用するには、[URL] を選択しアドレスを貼り付けます。
- ローカルに保存された OVA ファイルを使用するには、[ローカル ファイル] を選択し OVA をアップロードします。OVF ファイルをアップロードする場合は、OVF に関連するすべての VMDK ファイルもアップロードする必要があります。

5 一意の名前識別子を入力し、展開された Sensor Gateway 仮想マシンの場所を選択します。

6 次のページで、展開された Sensor Gateway に使用するコンピューティング リソースを選択し、[次へ] をクリックします。

アプライアンスが選択したリソースと互換性があることを確認します。

7 仮想アプライアンスの詳細を確認し、[次へ] をクリックします。

8 エンドユーザー使用許諾契約書を読んで同意し、[次へ] をクリックします。

9 仮想ディスクのフォーマットとストレージ場所を選択します。

仮想ディスクのフォーマット	メリット	デメリット
シン プロビジョニング	■ 最速のプロビジョニング ■ ディスク容量を仮想マシンにオーバーコミットできるようにします	■ メタデータ割り当てのオーバーヘッドと初期書き込み操作中の追加のオーバーヘッドにより、パフォーマンスが最も低下します ■ ストレージのオーバーコミットメントにより、リソースが実際に使用されている場合、アプリケーションの中断やダウンタイムが発生する可能性があります ■ クラスタリング機能をサポートしていません
シック プロビジョニング (Lazy Zeroed)	■ シック プロビジョニング (Eager Zeroed) よりも高速なプロビジョニング ■ シン プロビジョニングよりも優れたパフォーマンス	■ シン プロビジョニングよりもプロビジョニングが少し遅い ■ シック プロビジョニング (Eager Zero) よりもパフォーマンスが低下します ■ クラスタリング機能をサポートしていません
シック プロビジョニング (Eager Zeroed)	■ 最高のパフォーマンス ■ 割り当てられたディスク容量をゼロで上書きすると、セキュリティ リスクが軽減されます ■ Microsoft Cluster Server (MSCS) や VMware Fault Tolerance などのクラスタリング機能をサポートします	プロビジョニングの最長時間

10 ソース ネットワーク毎にターゲット ネットワークを選択し、[次へ] をクリックします。

デフォルトのままにしておくことができます。

11 Sensor Gateway 仮想マシンの展開設定を構成します。

オプション	アクション	例
`Initial root password`	root ユーザー アカウントのパスワードを入力します。	
`Initial admin password`	管理者ユーザー アカウントのパスワードを入力します。	
`CBC URL`	サービスがホストされている環境を表す CBC URL を入力します。Carbon Black Cloud は複数のリージョンでホストされており、URL が異なる場合があります。Carbon Black Cloud 環境のリストについては、Carbon Black Cloud のアクセス を参照してください。	`https://defense-prod05.conferdeploy.net` **注：** 値が `https://` で始まることを確認します
`API ID`	Sensor Gateway と Carbon Black Cloud 間の認証済み通信を許	`9Z5QY2ZDAN`

オプション	アクション	例
`API Secret Key`	可するには、Carbon Black Cloud API ID と API プライベート キーを入力します。Carbon Black Cloud コンソールを使用して、ペアで生成します。不一致がある場合、Carbon Black Cloud は Sensor Gateway からの通信を拒否します。 **注：** 機密データの使用により、vSphere Client は確認を求めるプロンプトを 2 回表示し、ユーザー インターフェイスの値を非表示にします。	`8UE3SHE470T2LZLJZJ2M98TY` **重要：** Sensor Gateway インスタンスごとに新しい API ID と API プライベート キーを生成する必要があります。
`Sensor Gateway Entry Point (https://<sensor-gateway-node-fqdn>)`	センサーが Sensor Gateway にどのように対処するかを定義するには、Sensor Gateway エントリ ポイントを入力します。エントリ ポイントは次と一致する必要があります。 ■ CA 署名付き証明書または自己署名証明書を使用する場合、値は証明書に指定された共通名 (CN) と同じである必要があります。 ■ マシンの IP アドレスまたは FQDN は、証明書の CN と同じである必要があります。	`https://sensorgateway.company.com` この例では、証明書の CN が `sensorgateway.company.com` であると仮定しています。 **注：** Sensor Gateway のサービスは SSL を使用してホストされるため、値が `https://` で始まることを確認します。
`Sensor Gateway Certificate`	Sensor Gateway 証明書ファイルの BEGIN 行と END 行を含むコンテンツを貼り付けます。これにより、Carbon Black センサー が Sensor Gateway と通信できるようになります。	
`Sensor Gateway Certificate Private Key`	Sensor Gateway 証明書プライベート キー ファイルの BEGIN 行と END 行を含むコンテンツを [パスワード] フィールドに貼り付けます。 **注：** 機密データの使用により、vSphere Client は確認を求めるプロンプトを 2 回表示し、ユーザー インターフェイスの値を非表示にします。	
`Sensor Gateway Certificate Chain`	Sensor Gateway 証明書チェーン ファイルの BEGIN 行と END 行を含むコンテンツを貼り付けます。	

オプション	アクション	例
Sensor Gateway Certificate Passphrase	証明書の生成時に作成したパスワードと同じパスワードを使用して、プライベート キーを保護します。Sensor Gateway はこのパスワードを使用して、Carbon Black センサー との通信を暗号化します。 **注：** 機密データの使用により、vSphere Client は確認を求めるプロンプトを 2 回表示し、ユーザー インターフェイスの値を非表示にします。	
Proxy Type	Sensor Gateway がプロキシを介して通信できるようにするには、プロキシ タイプを選択します。 ■ デフォルトでは、なし ■ HTTP または HTTPS それぞれに次のオプションのいずれかを入力します。 ■ プロキシ ホスト: プロキシ ホストの FQDN または IP アドレスを指定します ■ プロキシ ポート: プロキシ サーバが要求を受信するポートを指定します プロキシ タイプとして HTTPS を選択する場合は、HTTPS プロキシ証明書を含める必要があります。	
Proxy Host	プロキシ ホストの FQDN または IP アドレスを入力します。	
Proxy Port	デフォルトで、Sensor Gateway のサービスはポート 443 の SSL でホストされます。このポートが、Sensor Gateway をインストールする仮想マシンで使用されている場合は、別のポートを入力できます。	
HTTPS Proxy Certificate	プロキシ タイプとして HTTPS を選択した場合は、HTTPS プロキシ証明書ファイルの内容全体を貼り付けます。 HTTPS プロキシ証明書の更新を回避するために、Carbon Black では証明書の発行者を含めることをおすすめします。	
Default Gateway	オプション。この仮想マシンのデフォルト ゲートウェイを設定します。	入力はオプションですが、Sensor Gateway に静的 DNS と静的 IP アドレスを割り当てるには、これらのフィールドに入力する必要があります。空白のままにすると、Sensor Gateway は DHCP サーバから IP アドレスを取得します。
Domain Name	オプション。仮想マシンのドメイン名を入力します。	

オプション	アクション	例
Domain Search Path	オプション。この仮想マシンのドメイン名を入力します。	
Domain Name Servers	オプション。ドメイン名にマッピングされているこの仮想マシンの IP アドレスを入力します。	
Network 1 IP Address	オプション。ネットワーク インターフェイスの IP アドレスを設定します。	
Network 1 Netmask	オプション。ネットワーク インターフェイスのネットマスクまたはプリフィックスを設定します。	

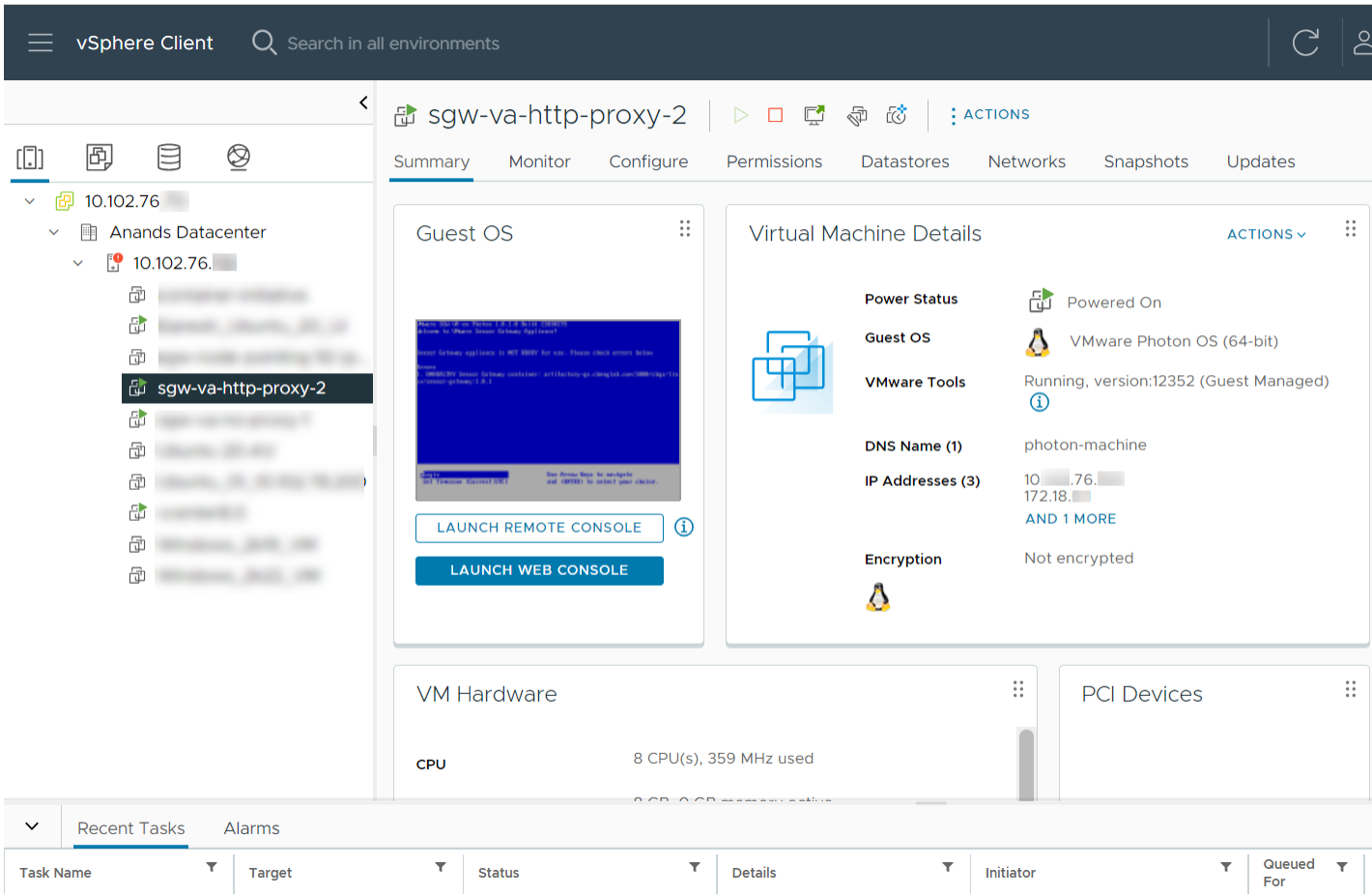
12 構成のセットアップを確認して [終了] をクリックします。

結果

展開の進行状況は、[最近のタスク] タブを使用するか、または [モニタ] - [タスク] 画面に移動して監視できます。展開が完了するまでにいくらか時間がかかります。

次のステップ

Sensor Gateway 仮想マシンをインポートして展開したら、パワーオンできます。操作が完了するまでにいくらか時間がかかります。



アプライアンスの起動後に、Sensor Gateway 仮想マシンを正常に構成した場合、[設定] - [API アクセス] - [Sensor Gateway] タブで Carbon Black Cloud コンソールに登録されていることを確認できます。

アプライアンスのデプロイが失敗で終了する場合は、SGW コンフィギュレータ ツールを使用して設定を再入力し、アプライアンスを再起動します。詳細については、Sensor Gateway アプライアンスの再構成 を参照してください。

Sensor Gateway アプライアンスの再構成

Sensor Gateway OVA のインストール時に設定した初期構成を更新するには、Sensor Gateway (SGW) Configurator ツールを使用します。

システム管理者は、ツールを使用して以前に指定したアプライアンス設定を更新し、Sensor Gateway を再起動して新しい構成を適用します。Carbon Black では、Sensor Gateway の展開が失敗した場合に Configurator ツールを使用することをお勧めします。

SGW Configurator ツールには、依存関係を持つ設定があります。このようなフィールドを変更する場合は、その依存フィールドも更新する必要があります。次の表に、Configurator を使用して更新できるフィールドと、その依存関係がある場合のフィールドを一覧表示します。

Sensor Gateway 設定	依存する Sensor Gateway の設定	メモ
CBC URL	API ID、API Secret Key	Carbon Black Cloud URL を変更する場合は、Sensor Gateway がすでに Carbon Black Cloud に登録され、既存の CBC URL と生成された API ID がある場合にのみ、API ID と API プライベート キーを更新します。
API ID	API Secret Key	別の環境から API プライベート キーを生成した場合は、Carbon Black Cloud URL を更新してその環境を提示します。
API Secret Key	なし	-
Entry Point URL	API ID、API Secret Key、および証明書	Sensor Gateway エントリ ポイントを変更する場合は、証明書の内容全体を再入力します。
Proxy Type	なし	-
Proxy Host	Proxy Certificate プロキシ タイプが HTTPS に設定されている場合。	-
Proxy Port	なし	-

手順

1 Sensor Gateway アプライアンスに admin ユーザーとしてログインします。

2 Configurator コマンドを実行します。

```
$ configure-sgw
```

SGW Configurator ターミナル ユーザー インターフェイスが表示されます。キーボードの矢印または角括弧内の文字を使用して、Configurator オプション間を移動できます。

3 [全般設定] または [TLS 設定] のいずれかの設定を更新します。

たとえば、Carbon Black Cloud への接続を更新する必要がある場合は、関連するフィールドに新しい Carbon Black Cloud URL を入力します。

無効な値を入力すると、有効な入力を促すエラー メッセージが表示されます。有効な URL を入力すると、成功メッセージが表示されます。

4 メイン メニューに戻るには、[戻る] を選択します。

5 オプション。手順 3 を繰り返して、必要な値を更新します。

6 変更内容を保持するには、[保存して終了] を選択します。

7 更新された値を確認し、変更を確認します。

結果

SGW Configurator ツールは、更新された構成で Sensor Gateway サービスを再起動します。

次のステップ

ログ ファイルにアクセスし、すべての構成変更のサマリを表示するには、 コマンドを実行します。

```
$ vim /opt/vmware/sgw/data/logs/configure-sgw.log
```

注： ログ ファイルは、プライベート キーなどの機密データを非表示にします。

Sensor Gateway アプライアンス証明書の更新

証明書の有効期限が間もなく切れる場合、または証明書が侵害された場合に Sensor Gateway OVA の TLS 証明書を更新し、Carbon Black Cloud からセンサーが完全に切断されないようにすることができます。

前提条件

新しい証明書にアクセスしてダウンロードするために、すべてのセンサーが Sensor Gateway アプライアンスに接続されていることを確認します。新しい証明書をアップロードすると、Carbon Black Cloud は各センサーに個別に送信します。

重要： シャットダウンされた仮想マシンは、新しい証明書を受け取らない場合があります。新しい証明書が Sensor Gateway で置き換えられると、センサーは Carbon Black Cloud に接続できません。そのため、新しい証明書を受信して接続の問題を回避するには、Sensor Gateway を介して接続されているすべてのセンサーがアクティブな状態であることを確認します。

手順

1 新しい証明書を取得します。

新しい証明書には、現在の証明書と同じ共通名 (CN) が必要です。

2 [設定] - [API アクセス] - [Sensor Gateways] タブに移動し、証明書を更新する必要がある Sensor Gateway OVA をダブルクリックします。

3 [Sensor Gateway の詳細] セクションで、[オプション] ドロップダウン メニューを選択し、[証明書の更新] をクリックします。

4 [ファイルのアップロード] をクリックし、新しく取得した証明書を選択してアップロードし、[閉じる] をクリックします。

この Sensor Gateway に接続されているセンサーの数に応じて、プロセスが完了するまでに最大 80 分かかります。Carbon Black Cloud は、この Sensor Gateway を介してクラウドに接続されているすべてのセンサーに新しくアップロードされた証明書を送信します。次に、各センサーがクラウドにステータスを送り返し、新しい証明書を正常に受け入れたかどうかを確認します。Carbon Black Cloud コンソールには、センサーが受信したエラーのみ表示されます。

5 Sensor Gateway センサーに接続されることで報告されたエラーを表示するには、[インベントリ] - [仮想マシン ワークロード] - [有効] タブに移動します。

a [Sensor Gateway] フィルタ ファセットから Sensor Gateway を選択します。

b [ステータス] フィルタ ファセットから [エラー] を選択します。

c エラーを報告するセンサーの詳細を表示するには、関連する行をダブルクリックします。

d 新しい証明書を再度アップロードすることで、既存のエラーを修正できます。

エラーが引き続き発生する場合は、Carbon Black Cloud サポートにお問い合わせください。

重要： Carbon Black Cloud コンソールでこの Sensor Gateway に接続されたセンサーからエラーが報告されていない場合にのみ、Sensor Gateway での証明書の更新を続行します。

6 OVA としてデプロイされた Sensor Gateway の TLS 証明書を置き換えます。

a Sensor Gateway アプライアンスに admin ユーザーとしてログインします。

b Configurator コマンドを実行します。

```
$ configure-sgw
```

SGW Configurator ターミナル ユーザー インターフェイスが表示されます。

c [TLS 設定] - [Sensor Gateway] - [Sensor Gateway 証明書] を選択します。

d プロンプトが表示されたら、**BEGIN CERTIFICATE** と **END CERTIFICATE** の行を含む新しい証明書の内容を貼り付け、**Ctrl+D** を 2 回押します。

構成ツールは、バックグラウンドでコンテンツを検証します。新しい証明書が無効な場合は、エラーが表示されます。

e 変更内容を保持するには、[保存して終了] を選択します。

SGW Configurator ツールは、更新された構成で Sensor Gateway サービスを再起動します。

結果

Sensor Gateway が Carbon Black Cloud に再登録されるまでに最大 5 分かかります。

HTTPS プロキシ証明書の更新

Sensor Gateway アプライアンスのインストール中にプロキシ タイプを HTTPS として指定した場合は、HTTPS プロキシ証明書も含まれています。この手順に従って、プロキシ証明書の有効期限が間もなく切れる場合、または証明書が侵害された場合に更新します。

SGW Configurator ツールを使用してプロキシ証明書を更新します。ツールの使用方法の詳細については、Sensor Gateway アプライアンスの再構成を参照してください。

前提条件

次のいずれかを指定できることを確認します。

- 推奨 HTTPS プロキシ証明書の発行者。認証局を指定する場合、有効期限が間もなく切れるときに Sensor Gateway プロキシ証明書を更新する必要はありません。
- プロキシ サーバの証明書チェーン。証明書チェーンを使用する場合は、Sensor Gateway プロキシ証明書を更新する必要があります。

手順

1 新しい HTTPS プロキシ証明書を取得します。

2 Sensor Gateway アプライアンスに admin ユーザーとしてログインします。

3 Configurator コマンドを実行します。

```
$ configure-sgw
```

SGW Configurator ターミナル ユーザー インターフェイスが表示されます。キーボードの矢印または角括弧内の文字を使用して、Configurator オプション間を移動できます。

4 [TLS 設定] - [プロキシ] - [プロキシ証明書] を選択します。

5 **BEGIN CERTIFICATE** と **END CERTIFICATE** の行を含む新しいプロキシ証明書の全内容を貼り付け、**Ctrl+D** を押します。

誤った内容を入力すると、「`ERROR: 無効な値を入力しました。有効な X509 証明書を入力してください`」などのエラーが表示されます。

6 変更内容を保持するには、[保存して終了] を選択します。

7 更新された値を確認し、変更を確認します。

結果

SGW Configurator ツールは、更新された構成で Sensor Gateway サービスを再起動します。

Carbon Black Cloud センサーのインストール

Sensor Gateway をインストールして Carbon Black Cloud に登録すると、新しい Carbon Black センサー インストールを実行できます。

センサーをインストールするための環境の設定

Carbon Black センサー をインストールする前に、次の環境設定を検討してください。

- Sensor Gateway インスタンスの特定

  Carbon Black Cloud コンソールを使用して、Sensor Gateway インスタンスを見つけることができます。

- 会社コードの生成

  センサーのインストール前に会社コードを生成する必要があります。Carbon Black Cloud コンソールを使用して会社コードを取得できます。

Sensor Gateway インスタンスの特定

Carbon Black Cloud コンソールを使用して、Sensor Gateway インスタンスを見つけることができます。

手順

1 アカウントの認証情報を使用して、Carbon Black Cloud コンソールにログインします。

2 左側のナビゲーション バーで、[設定] - [API アクセス] - [Sensor Gateways] の順に選択します。

3 IP アドレスまたは API ID に対応する Sensor Gateway の名前を見つけます。

4 この名前は、会社コードの生成時に必要に応じて書き留めます。

会社コードの生成

センサーのインストール前に会社コードを生成する必要があります。Carbon Black Cloud コンソールを使用して会社コードを取得できます。

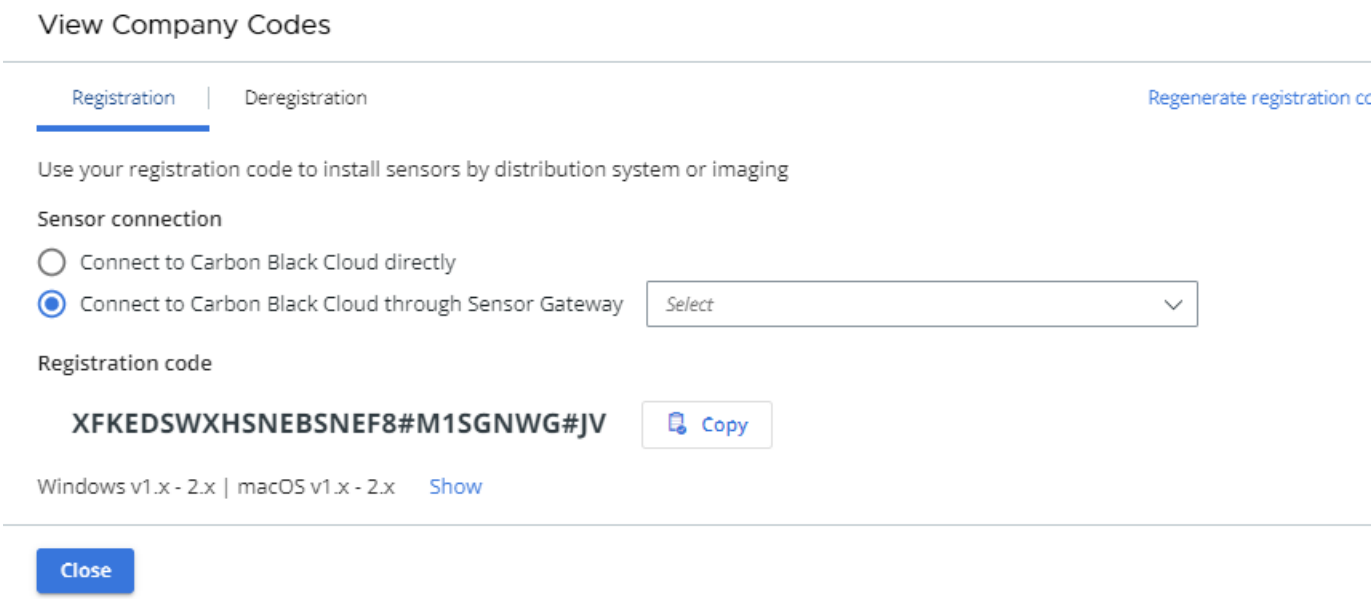
手順

1 左側のナビゲーション バーで、[インベントリ] - [仮想マシン ワークロード] を選択します。

2 [センサー オプション] ドロップダウン メニューから [会社コードの表示] を選択します。

3 [Sensor Gateway を介して Carbon Black Cloud に接続] オプションをクリックします。

Sensor Gateway ドロップダウン メニューが使用可能になります。



4 センサーのインストールに使用する Sensor Gateway エントリ ポイント URL を選択します。

ドロップダウン メニューには、接続されている Sensor Gateway の URL のみが表示されます。

5 登録コードをコピーします。

これは、センサーのインストール時に使用する会社コードです。

Linux 用 Carbon Black Cloud センサーのインストール

Linux 仮想マシン ワークロードの Carbon Black センサー が Sensor Gateway を介して Carbon Black Cloud と通信できるようにするには、センサーをインストールして Sensor Gateway と連携するように構成する必要があります。

前提条件

- 最新の Linux 用 Carbon Black センサー バージョン (2.15 以降) にアクセスできることを確認します。

- Carbon Black Cloud コンソールを使用して仮想マシン ワークロードにセンサーをインストールする方法については、『VMware Carbon Black Cloud センサーのインストール ガイド』を参照してください。コンソール ユーザー インターフェイスを使用してセンサーをインストールする場合は、`/var/opt/carbonblack/psc/cfg.ini` ファイルに `UseSystemCerts=true` プロパティを含めます。詳細については、「エンドポイントへの Linux センサーのインストール」を参照してください。
- 会社コードが使用可能であることを確認します。詳細については、会社コードの生成 を参照してください。

手順

1 Carbon Black センサー for Linux の最新バージョンをダウンロードします。

2 Sensor Gateway が CA 署名付き証明書ですでに構成されている場合は省略します。Sensor Gateway で自己署名付き証明書を使用するには、トラスト ストアに証明書チェーンを追加する必要があります。

   a Sensor Gateway との通信に使用する証明書 `sgw_certificate.pem` ファイルを、Linux 仮想マシン ワークロードの既知の場所にコピーします。

   b 仮想マシン ワークロードの CA 署名付き証明書 `ca-certificates.crt` ファイルに自己署名付き証明書 `sgw_certificate.pem` の内容を追加します。

   ```
   cat sgw_certificate.pem >> CERTFILE_PATH
   ```

   CERTFILE_PATH は、ほとんどの Linux システムで `/etc/ssl/certs/ca-certificates.crt` を示しています。ただし、信頼できる CA 証明書ファイルを選択するには、ディストリビューションのドキュメントで確認する必要があります。

3 次のコマンドを実行して、センサーのインストール ファイルを取得します。

```
wget <location of the sensor installation file>
```

4 センサーのインストール ファイルを解凍します。

```
tar -xvf <tgz installation file>
```

5 以前に生成した会社コードを使用して、センサーのインストールを完了します。

```
./install.sh "<company_code>" --sensor-gateway-cert CERTFILE_PATH
```

CERTFILE_PATH は、ほとんどの Linux システムで `/etc/ssl/certs/ca-certificates.crt` を示しています。ただし、信頼できる CA 証明書ファイルを選択するには、ディストリビューションのドキュメントで確認することをお勧めします。

結果

センサーが正常にインストールされると、Carbon Black Cloud コンソールで実行中の Sensor Gateway が表示されます。

次のステップ

必要に応じて、次のコマンドを実行して、Linux ワークロードからセンサーをアンインストールできます。

```
dpkg --purge cb-psc-sensor
```

Windows 用 Carbon Black センサーのインストール

Sensor Gateway が起動して実行されたら、センサーの新規インストールを実行する必要があります。Windows 仮想マシン ワークロードに Carbon Black センサー をインストールし、Sensor Gateway を介して Carbon Black Cloud と通信するように構成します。

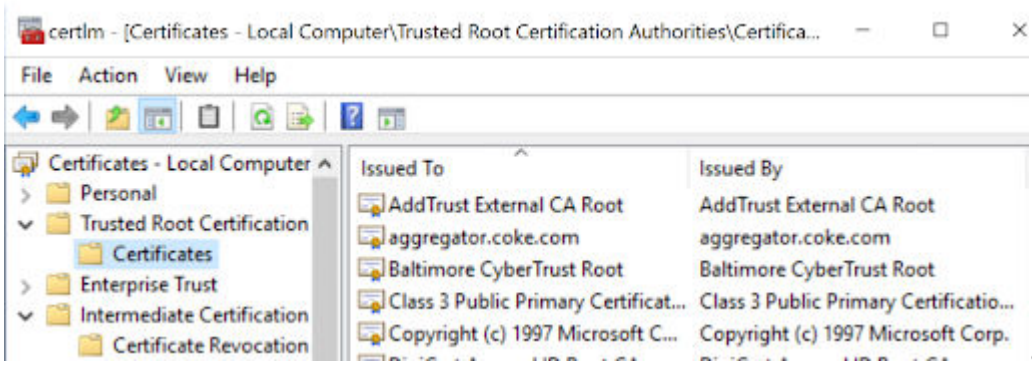
前提条件

- 最新の Windows 用 Carbon Black センサー バージョン (3.8.0.684 以降) にアクセスできることを確認します。
- Carbon Black Cloud コンソールを使用して仮想マシン ワークロードにセンサーをインストールする方法については、『VMware Carbon Black Cloud センサーのインストール ガイド』を参照してください。
- 会社コードが使用可能であることを確認します。詳細については、会社コードの生成 を参照してください。
- プロキシで構成された Sensor Gateway 環境に Carbon Black センサー をインストールすると、センサーのインストールが完了した後に、ローカル スキャナ設定 `UpdateServers` が なし に設定されている場合があります。デフォルトで、センサーは、多数のセンサーが展開されている場合に、ランダムなタイムアウト（最大 2 時間）を使用してシグネチャ パックをダウンロードします。シグネチャのダウンロードでランダムな遅延を回避するには、センサーのインストール中に `DELAY_SIG_DOWNLOAD` コマンド ライン パラメータを **0** に設定します。Windows センサーでサポートされているコマンドの詳細については、『VMware Carbon Black Cloud センサーのインストール ガイド』を参照してください。

手順

1 Sensor Gateway が CA 署名付き証明書を使用する場合は、この手順を省略します。Windows 仮想マシン ワークロードの信頼されたルート証明書フォルダに自己署名付き証明書を追加します。

センサーは、この証明書を使用して、Sensor Gateway



と通信します。

2 センサー インストーラをダウンロードします。

3 Carbon Black Cloud コンソールまたは既存のスクリプトを使用してセンサーをインストールします。

4 以前に生成した会社コードを使用して、センサーのインストールを完了します。

センサーが正常にインストールされると、Carbon Black Cloud コンソールで実行中の Sensor Gateway が表示されます。

Carbon Black Cloud への接続の管理

Carbon Black Cloud コンソールを使用して、センサーと Carbon Black Cloud の間の接続を管理します。ワークロードは、直接または Sensor Gateway を介して Carbon Black Cloud と通信できます。

前提条件

Windows 3.9 以降の Carbon Black センサー がインストールされていることを確認する

手順

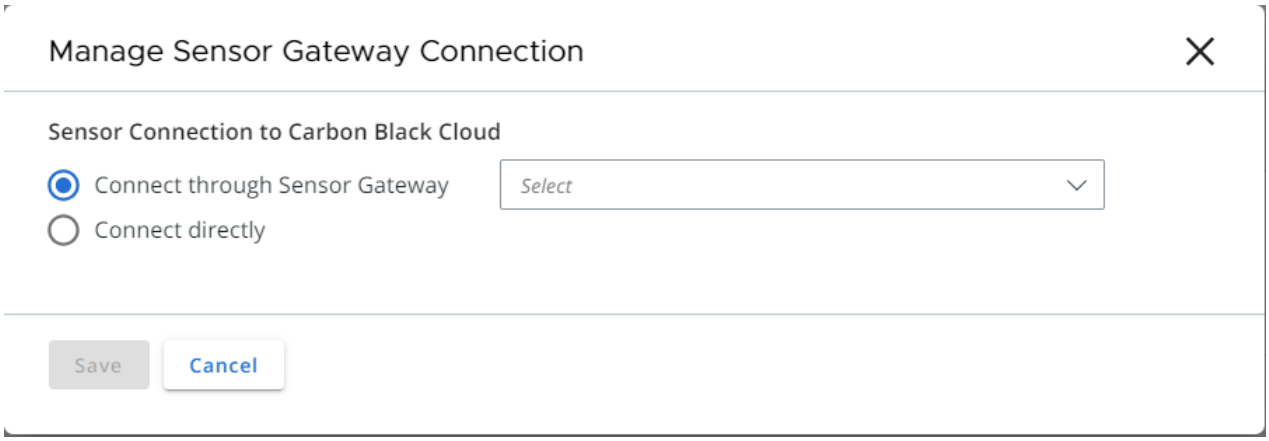
1 Carbon Black Cloud コンソールにログインします。

2 左側のナビゲーション ペインで、[インベントリ] - [仮想マシン ワークロード] または [インベントリ] - [エンドポイント] の順にクリックし、[有効] タブを選択します。

3 [ステータス] 列を見つけて、アクションを実行する 1 つ以上の仮想マシン ワークロードまたはエンドポイントのチェック ボックスを選択します。

[アクション実行] ドロップダウン メニューが表示されます。

4 [Sensor Gateway 接続の管理] を選択します。



[Sensor Gateway 接続の管理] ウィンドウが表示されます。

5 次のいずれかの手順を実行します。

- Sensor Gateway を割り当てるには、[Sensor Gateway を介して接続] ドロップダウン メニューをクリックし、エントリ ポイントを選択します。

  この接続がサポートされているセンサーの数を超えている場合、Sensor Gateway を選択するとすぐに通知されます。

  [有効] タブでアセットの一括選択を実行し、アセットの合計数が 1 ページ サイズを超えると、この設定をすべてのアセットに適用するためのチェック ボックスが表示されます。

- Sensor Gateway に問題がある場合、センサーが Carbon Black Cloud と直接通信するには、[直接接続] を選択します。

6 センサーと Carbon Black Cloud の間の接続タイプを変更するには、[適用] をクリックします。

結果

コンソールに変更が反映されるまでに最大 10 分かかります。

Sensor Gateway 通知

1 台以上の Sensor Gateway サーバをインストールして実行を開始した後、Carbon Black Cloud コンソールを使用して、Sensor Gateway の障害通知をサブスクライブできます。

サブスクライブすると、次の場合に製品内通知と E メールによる通知を受け取ります。

- 組織内の 1 つ以上の Sensor Gateway インスタンスが過去 5 分以内に応答せず、現在 Carbon Black Cloud から切断されている場合。
- 組織内の 1 つ以上の Sensor Gateway インスタンスが、構成されたセンサーの数を超える場合。

> **注：** 各 Sensor Gateway は最大 1 万台の Carbon Black Cloud センサーをサポートします。

Sensor Gateway 通知のサブスクライブ

次の手順を使用して、登録済みの Sensor Gateway インスタンスの状態に関する製品内通知と E メール通知を受信します。

手順

1 [設定] - [通知] 画面で、[統合] タブを選択します。

2 [通知の追加] をクリックします。

3 通知の名前を入力し、[コンポーネント タイプ] ドロップダウン メニューから Sensor Gateway を選択します。

4 通知を受けるタイミングを、Sensor Gateway が切断されたとき、Carbon Black センサーの最大数 10,000 を超えたとき、Sensor Gateway の証明書の有効期限が間もなく切れるとき、またはそのすべてから選択します。

5 関連するドロップダウン メニューから E メールで通知を受信するすべてのユーザーを追加します。

これらのユーザーは、[設定] - [ユーザー] 画面で定義します。

6 オプション。環境内でまだ解決されていないすべてのゲートウェイのサマリを含む通知を 1 日の終わりに受信するには、[1 日の終わりに 1 件のリマインダ メールを送信] オプションをクリックします。

すでに接続がリストアされた Sensor Gateway インスタンスは除外されます。

7 通知サブスクリプションのセットアップを完了するには、[保存] をクリックします。

Sensor Gateway アプライアンスのアップグレード

Carbon Black Cloud コンソールを使用して、Sensor Gateway アプライアンスを使用可能な最新バージョンにアップグレードします。

注：

- アップグレードの進行中は、Sensor Gateway アプライアンスをパワーオフしないでください。そうしないと、Sensor Gateway の再インストールが必要になる場合があります。
- アップグレードしようとしている Sensor Gateway に接続されているセンサーは、アップグレード中に Carbon Black Cloud への接続を失う可能性があります。
- Carbon Black Cloud は、システム エラーが発生した場合、または以前のバージョンの Sensor Gateway に戻す場合に、フォールバック メカニズムを提供します。

手順

1 Carbon Black Cloud コンソールにログインします。

2 [設定] - [API アクセス] - [Sensor Gateways] タブに移動します。

3 アップグレードする Sensor Gateway をダブルクリックします。

[Sensor Gateway の詳細] ペインには、Sensor Gateway の現在のバージョンと新しく使用可能なバージョンが括弧内に表示されます。

4 [オプション] ドロップダウン メニューをクリックし、[バージョンのアップグレード] を選択します。

[Sensor Gateway のアップグレード] ウィンドウが表示されます。

5 アップグレードを確認するには、[アップグレード] を選択します。

結果

Sensor Gateway は正常にアップグレードされ、センサーはクラウドへの接続を再開します。

次のステップ

[設定] - [監査ログ] ページ移動して、アップグレードのステータスを表示できます。たとえば、起動時や成功した場合などです。

Sensor Gateway のトラブルシューティング

トラブルシューティングのトピックを使用して、Sensor Gateway のインストール、使用、アップグレードが期待どおりに動作しない場合の解決策を見つけます。

Sensor Gateway アプライアンスにアクセスできません

問題

Carbon Black Sensor Gateway アプライアンスとの通信の問題が発生する可能性があります。

原因

仮想マシンがパワーオフ状態です。

解決方法

仮想マシンをパワーオンし、仮想マシンが健全な状態になるのを待ちます。再起動を数回行っても動作状態が健全でない場合は、Sensor Gateway アプライアンスの新しいインストールを開始します。アプライアンスとして Sensor Gateway をインストールを参照してください。

Sensor Gateway アプライアンスをインストールするプロセスで、Sensor Gateway エントリ ポイント URL を指定していることを確認します。エントリ ポイント URL は、Sensor Gateway 証明書の生成時に指定した共通名 (CN) と一致する必要があります。詳細については、Sensor Gateway 証明書 を参照してください。

Linux への Sensor Gateway のインストール

次の手順に従って Linux サーバを設定し、構成済みの Linux マシンに Sensor Gateway をインストールします。

重要： Carbon Black では、Sensor Gateway アプライアンスを使用してシステムを設定することをお勧めします。詳細については、アプライアンスとして Sensor Gateway をインストールを参照してください。Sensor Gateway for Linux および関連する HA 機能は間もなく廃止される予定です。

Sensor Gateway をインストールするための環境の設定

Sensor Gateway のインストール用に各 Linux サーバを設定するには、次の手順を実行します。

前提条件

- SSL 署名付き証明書をプロビジョニングします。次のいずれかを選択します。
  - 認証局 (CA) 署名付き証明書この証明書が優先されます。詳細については、Sensor Gateway 証明書 を参照してください。
  - 自己署名付き証明書。この証明書は、各センサー ワークロードのトラスト ストアにこれらの証明書をプッシュする必要があります。詳細については、Sensor Gateway 証明書 を参照してください。

  注： 使用している証明書のプライベート キーが必要です。
- CA 署名付き証明書、または Online Certificate Status Protocol (OCSP) レスポンダを持つ内部証明書がある場合は、証明書チェーン全体をプロビジョニングする必要がある場合があります。Sensor Gateway は、証明書とそのチェーンを使用して OCSP 応答を取得し、すべての要求とホチキス留めします。これにより、センサーが OCSP レスポンダに直接アクセスできなくなります。

  証明書チェーンの構成を提供する任意のオンライン サービスを使用して、証明書チェーン ファイルを生成します。詳細については、証明書チェーン ファイルの作成 を参照してください。
- 各 Sensor Gateway サーバの固定 IP アドレスを取得します。
- DNS エントリを予約します。例：`sensorgateway.company.com`

  環境に Sensor Gateway をインストールするには、その DNS をサーバに以前に割り当てた IP アドレスにマッピングします。

FQDN を使用して Sensor Gateway を構成する場合は、IP アドレスへの DNS マッピングを使用します。

注： IP アドレスのみを使用し、IP アドレスを CN と同じにして証明書を作成できます。

- センサーが Sensor Gateway にアクセスできることを確認します。
- Sensor Gateway がインターネットに接続されていることを確認します。Sensor Gateway には、Carbon Black Cloud への接続が必要です。ただし、デジタル証明書の有効性に関する Online Certificate Status Protocol (OCSP) 応答を取得するには、CA プロバイダにアクセスする必要がある場合があります。
- プロキシの後ろで Sensor Gateway を実行するには、プロキシを使用するように Docker クライアントを構成します。詳細については、「プロキシ サーバを使用するように Docker クライアントを構成する」を参照してください。
- Sensor Gateway のプロキシ機能を使用していて、Sensor Gateway と Carbon Black Cloud の間にプロキシ サーバがある場合は、プロキシを介して Carbon Black Cloud URL にアクセスできることを確認する必要があります。更新サーバのミラーを設定する場合は、プロキシ経由でもアクセス可能であることを確認します。
- 環境が必要なネットワーク設定で構成されていることを確認します。詳細については、「ファイアウォールの構成」を参照してください。
- ファイアウォールの設定でポート 443 の `projects.registry.vmware.com` がブロックされていないことを確認します。

手順

1 サーバに root としてログインし、OpenSSL がインストールされていることを確認します。

まだインストールしていない場合は、システム パッケージ マネージャを使用して OpenSSL をインストールします。

2 証明書を準備します。

a SSL 証明書ファイルに `sgw_certificate.pem` という名前を付けます。

b SSL 証明書のプライベート キー ファイルに `sgw_key.pem` という名前を付けます。

c （自己署名付き証明書を使用している場合は、この手順を省略します。）SSL 証明書チェーン ファイルに `sgw_chain.pem` という名前を付けます。

d （自己署名付き証明書を使用している場合は、この手順を省略します。）証明書が有効かどうかを確認するには、次のコマンドを実行します。

```
openssl verify -CAfile sgw_chain.pem sgw_certificate.pem
```

証明書が有効な場合は、次の応答が得られます：`sgw_certificate.pem: OK`

e ルート レベルで /data フォルダを作成し、サーバに次のサブフォルダを作成します。

- /data/certs - 証明書、キー、およびオプションで証明書チェーン ファイルを保存します。
- /data/logs - 実行時に生成されたログを保存します。

f 証明書、プライベート キー、チェーン ファイルを /data/certs ディレクトリにコピーします。

注： 自己署名付き証明書を使用している場合は、チェーン ファイルは必要ありません。

3 スクリプトをダウンロードします。これは各サーバに Sensor Gateway を個別にインストールして設定します。

```
wget https://prod.cwp.carbonblack.io/sgw/installer/linux/1.2.0/sensor_gw_install.zip
```

4 Sensor Gateway インストール zip ファイルをダウンロードした場所で解凍します。シェル スクリプト sensor_gw_install.sh を見つけます。

5 デフォルトでは、シェル スクリプトは実行可能ではありません。次のコマンドを実行して、スクリプトを実行可能にします。

```
chmod +x sensor_gw_install.sh
```

6 Sensor Gateway 登録 API キーを取得します。

詳細については、Sensor Gateway API キーのプロビジョニング を参照してください。

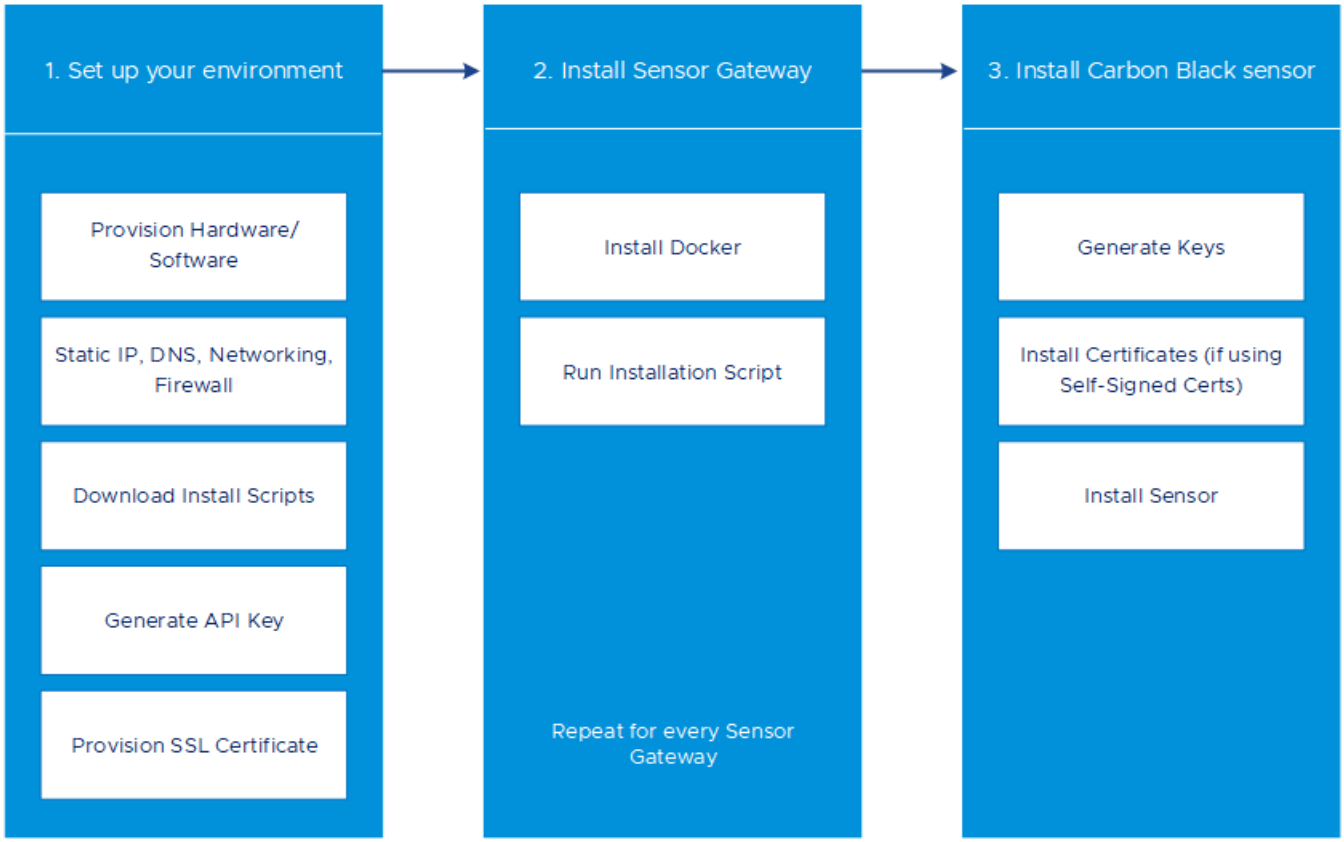
次のステップ

Sensor Gateway をインストールします。

Linux サーバへの Sensor Gateway のインストール

Sensor Gateway を Linux マシンでコンテナ イメージとしてホストします。そのため、Linux サーバにはコンテナ実行機能が必要です。このタイプのインストールでは、複数の Sensor Gateway サーバをインストールする場合は、Sensor Gateway サーバごとに次の手順を繰り返す必要があります。

次の高レベルなインストール ワークフローは、センサーが Sensor Gateway を介して Carbon Black Cloud と通信できるように、システムにさまざまなコンポーネントをインストールして構成する手順を示しています。



前提条件

- Sensor Gateway でポート 443 が開いていることを確認します。
- プロキシの後ろで Sensor Gateway を実行するには、プロキシを使用するように Docker クライアントを構成します。詳細については、「プロキシ サーバを使用するように Docker クライアントを構成する」を参照してください。

手順

1 Docker をインストールします。

Linux ディストリビューションでサポートされている Sensor Gateway に Docker エンジンをインストールする方法については、「CentOS への Docker エンジンのインストール」、「RHEL への Docker エンジンのインストール」、または「Ubuntu への Docker エンジンのインストール」を参照してください。

2 インストール スクリプトがまだ実行可能でない場合は実行可能にします。

```
chmod +x sensor_gw_install.sh
```

3 インストール スクリプトを実行します。

```
./sensor_gw_install.sh
```

4 プロンプトが表示されたら、次を入力します。

オプション	説明	例
API ID	Carbon Black Cloud コンソールで生成された API ID と API シークレット キーにより、Sensor Gateway と Carbon Black Cloud の間の認証通信が可能になります。 API ID と API シークレット キーの両方がペアで生成されます。不一致があるため、Carbon Black Cloud は Sensor Gateway からの通信を拒否します。 **注：** Sensor Gateway ごとに新しい API ID と API シークレット キーを生成する必要があります。	9Z5QY2ZDAN
API シークレット キー		8UE3SHE475T2LZLJNJ2M98TK
Carbon Black Cloud URL	この URL は、サービスがホストされている環境を示します。Carbon Black Cloud は複数のリージョンでホストされており、URL が異なる場合があります。Carbon Black Cloud 環境のリストについては、 Carbon Black Cloud のアクセス を参照してください。	`https://defense-prod05.conferdeploy.net` **注：** 値が `https://` で始まることを確認します
Sensor Gateway エントリ ポイント URL (https://<sensor-gateway-node-fqdn>)	エントリ ポイントは、センサーが通常、Sensor Gateway をどのように対処するかを意味します。 これは次と一致する必要があります。 ■ CA 署名付き証明書または自己署名証明書を使用する場合、この値は証明書に指定された CN と同じである必要があります。 ■ マシンの IP アドレスまたは FQDN は、証明書の CN と同じである必要があります。	`https://sensorgateway.company.com` この例では、証明書の CN が `sensorgateway.company.com` であると仮定しています。 **注：** Sensor Gateway サービスは SSL を使用してホストされるため、値が `https://` で始まることを確認します。
プロキシ タイプ	■ なし: これはデフォルトのオプションです。 ■ HTTPS または HTTP: それぞれについて、次のいずれかのオプションを選択します。 ■ プロキシ ホスト: プロキシ ホストの FQDN または IP アドレスを指定します。 ■ プロキシ ポート: プロキシ サーバが要求を受信するポートを指定します。	HTTP
[オプション:] ボリューム マウント ディレクトリ	Sensor Gateway は、固定ディレクトリを使用して証明書を検索し、ログを保存します。 値を指定しない場合、デフォルトの場所は `/data` ディレクトリです。証明書またはログを別のディレクトリに保存することを選択した場合は、ここで絶対パスを指定できます。 別のフォルダを選択する場合は、このパスの下に証明書とログ フォルダを作成してください。同時に、次のパラメータに進む前に、証明書、プライベート キー、および証明書チェーン（オプション）が証明書フォルダに保存されていることを確認する必要があります。 インストール スクリプトは root 権限で実行されるため、デフォルトでは、これらのディレクトリはすべて所有者およびグループとして root 権限を持ちます。	`/data`

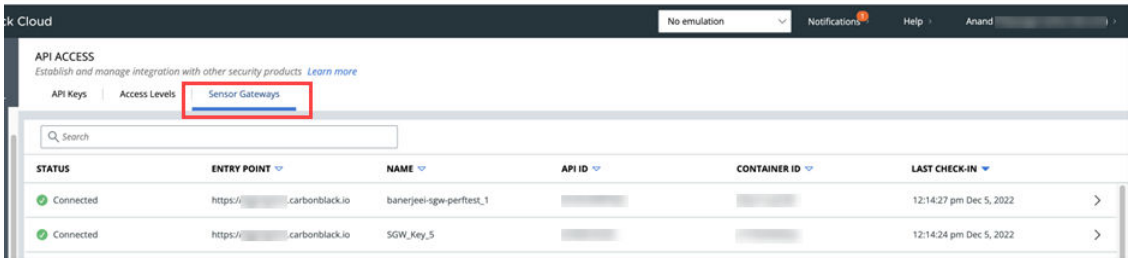
オプション	説明	例
[オプション:]センサー ゲートウェイが実行されているポート	デフォルトで、Sensor Gateway サービスはポート 443 の SSL でホストされます。このポートが、Sensor Gateway をインストールするマシンで何らかの理由で使用されている場合は、別のポートを使用できます。	デフォルトでは、Sensor Gateway はポート 443 で実行されます。
[オプション:] 証明書プライベート キーのパスフレーズ	推奨として、証明書の生成時にプライベート キーを保護するためのパスワードを入力します。Sensor Gateway のインストール中にプロンプトが表示されたら、同じパスワードを入力します。 Sensor Gateway は、同じパスワードを使用して証明書を使用し、センサーとそれ自体の間の通信を暗号化します。	`sgw_key.pem` がパスワードで保護されている場合は、パスワードを入力します。

Sensor Gateway サービスが起動し、Carbon Black Cloud に登録されます。登録が完了するまでに数分かかります。

結果

登録が正常に完了すると、Carbon Black Cloud コンソールの [設定] - [API アクセス] - [Sensor Gateways] 画面に Sensor Gateway が接続済みとして表示されます。

Sensor Gateway 名は API キーから来ています。



次のステップ

Sensor Gateway は信頼性が高く、高い可用性を備えています。複数の Sensor Gateway サーバを展開し、許容可能な遅延でトラフィックを処理するように HA モード（手動）で構成できます。接続またはリソースのしきい値が原因で Sensor Gateway サーバで障害が発生した場合は、別の Sensor Gateway インスタンスにログインして接続の管理を引き継ぐことができます。

Sensor Gateway 証明書の更新

証明書の有効期限が間もなく切れる場合、または証明書が侵害された場合に Linux Sensor Gateway で SSL 証明書を更新し、Carbon Black Cloud からセンサーが完全に切断されないようにすることができます。

前提条件

新しい証明書にアクセスしてダウンロードするために、すべてのセンサーが Sensor Gateway に接続されていることを確認します。新しい証明書をアップロードすると、Carbon Black Cloud は各センサーに個別に送信します。

重要: シャットダウンされた仮想マシンは、新しい証明書を受け取らない場合があります。新しい証明書が Sensor Gateway で置き換えられると、センサーは Carbon Black Cloud に接続できません。そのため、新しい証明書を受信して接続の問題を回避するには、Sensor Gateway を介して接続されているすべてのセンサーがアクティブな状態であることを確認します。

手順

1 新しい証明書を取得します。

新しい証明書には、現在の証明書と同じ共通名 (CN) が必要です。

2 [設定] - [API アクセス] - [Sensor Gateways] タブに移動し、証明書を更新する必要がある Sensor Gateway をダブルクリックします。

3 [Sensor Gateway の詳細] セクションで、[オプション] ドロップダウン メニューを選択し、[証明書の更新] をクリックします。

4 [ファイルのアップロード] をクリックし、新しく取得した証明書を選択してアップロードし、[閉じる] をクリックします。

この Sensor Gateway に接続されているセンサーの数に応じて、プロセスが完了するまでに最大 80 分かかります。Carbon Black Cloud は、この Sensor Gateway を介してクラウドに接続されているすべてのセンサーに新しくアップロードされた証明書を送信します。次に、各センサーがクラウドにステータスを送り返し、新しい証明書を正常に受け入れたかどうかを確認します。Carbon Black Cloud コンソールには、センサーが受信したエラーのみ表示されます。

5 Sensor Gateway センサーに接続されることで報告されたエラーを表示するには、[インベントリ] - [仮想マシン ワークロード] - [有効] タブに移動します。

a [Sensor Gateway] フィルタ ファセットから Sensor Gateway を選択します。

b [ステータス] フィルタ ファセットから [エラー] を選択します。

c エラーを報告するセンサーの詳細を表示するには、関連する行をダブルクリックします。

d 新しい証明書を再度アップロードすることで、既存のエラーを修正できます。

エラーが引き続き発生する場合は、Carbon Black Cloud サポートにお問い合わせください。

重要： Carbon Black Cloud コンソールでこの Sensor Gateway に接続されたセンサーからエラーが報告されていない場合にのみ、Sensor Gateway での証明書の更新を続行します。

---

6 Sensor Gateway の SSL 証明書を置き換えます。

a 新しい証明書の名前を `sgw_certificate.pem` に変更し、プライベート キーを `sgw_key.pem` に変更します。

b 新しい証明書のパブリック キーとプライベート キーを、Sensor Gateway デバイスの `/data/certs` フォルダにコピーします。

c 最初にコンテナ ID `sudo docker ps -a` を取得してからコマンド `sudo docker restart <contained id>` を実行して、Sensor Gateway を再起動します。

結果

Sensor Gateway が Carbon Black Cloud に再登録されるまでに最大 5 分かかります。

Linux Sensor Gateway のアップグレード

専用のアップグレード スクリプトを実行して、Sensor Gateway をアップグレードします。

注： Sensor Gateway のアップグレードでは、プロキシのサポートは有効になりません。プロキシを使用して Sensor Gateway 環境を構成するには、Sensor Gateway を再インストールする必要があります。

前提条件

- 最初の Sensor Gateway インストールから次の情報を入手できることを確認します。
  - Sensor Gateway エントリ ポイント。以前と同じ名前を使用します。使用しない場合は、既存のセンサーが動作を停止する可能性があります。
  - API ID
  - API キー
- Sensor Gateway では、次の Carbon Black センサー バージョンがサポートされています。
  - Carbon Black センサー for Windows 3.8.0.684 以降
  - Carbon Black センサー for Linux 2.13.2.997598 以降
- Sensor Gateway の古いバージョンが実行されており、Carbon Black Cloud とのアクティブな接続があることを確認します。

手順

1 Linux サーバの `sensor-gateway-x.x.x.zip` ファイルをダウンロードして解凍します。

2 現在の Sensor Gateway を特定して停止します。

   a root 認証情報を使用して Linux サーバにログインします。

   b Sensor Gateway の実行中のインスタンスを取得するには、次のコマンドを実行します。

   ```
   docker ps
   ```

   最初の列に `Container ID` が表示されます。

   c 実行中の Sensor Gateway を停止するには、次のコマンドを実行します。

   ```
   docker stop <the Container ID>
   ```

   d すべてのコンテナのリストを取得するため、`Status` 列で終了した Sensor Gateway インスタンスを確認するには、次のコマンドを実行します。

   ```
   docker ps -a
   ```

e Sensor Gateway インスタンスを削除します。

```
docker rm <the Container ID>
```

f すべてのコンテナのリストを取得し、[実行中] または [停止] ステータスの Sensor Gateway がないことを確認します。

```
docker ps -a
```

コマンドの実行結果が表示されない場合は、前のコマンドが正常に実行されなかった可能性があることを示します。次の手順に進まず、Carbon Black サポートにお問い合わせください。

3 Sensor Gateway ファイルの最新バージョンを解凍したディレクトリへの `cd`。

4 Sensor Gateway をインストールします。

```
./sensor_gw_install.sh
```

初回の Sensor Gateway インストール時と同じデータの入力を求めるプロンプトが表示されます。詳細については、Linux サーバへの Sensor Gateway のインストール を参照してください。

結果

Sensor Gateway が正常にアップグレードされました。