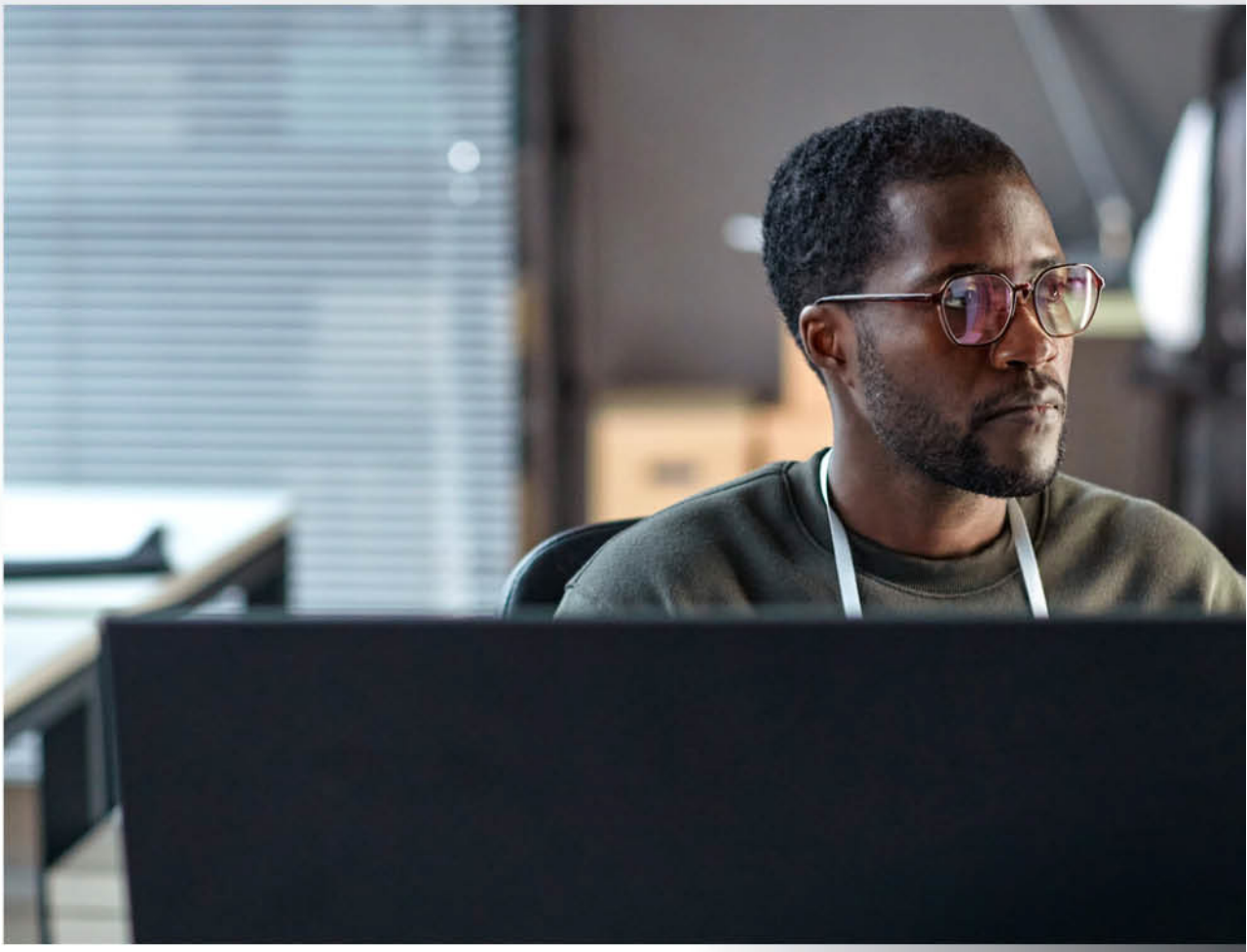
Technisches Whitepaper



HPE Compute Ops Management – Sicherheitsleitfaden

Inhaltsverzeichnis

Kurzübersicht

Hewlett Packard Enterprise revolutioniert das Computing-Management mit einem modernen Ansatz für mehr Einfachheit, Agilität und Leistung. Dieser Ansatz umfasst den Einsatz von Cloud-nativen Architekturen und automatisiertem Firmware-Management in der gesamten Serverflotte.

HPE Compute Ops Management ist eine sichere und skalierbare Cloud-basierte Anwendung, die einen einheitlichen Computing-Betrieb vom Edge bis zur Cloud ermöglicht. Sie optimiert das Infrastrukturmanagement in seinem gesamten Lebenszyklus – von vereinfachtem Statusmanagement bis hin zu automatisiertem Firmware-Management in der gesamten Serverflotte. HPE Compute Ops Management wird über die HPE GreenLake Cloud abgerufen und durch eine Cloud-native Architektur unterstützt, die aus dem komplexen Computing-Betrieb ein benutzerfreundliches Gesamterlebnis vom Edge bis zur Cloud macht.

Dieses Dokument bietet Ihnen eine umfassende Übersicht darüber, wie HPE Compute Ops Management sämtliche Aspekte der Benutzer- und Datensicherheit rigoros durchsetzt. So nutzt es beispielsweise eine rollenbasierte Zugriffskontrolle für Benutzer sowie von HPE CA ausgestellte Zertifikate zur Überprüfung der Authentizität. Dieses Dokument verschafft Ihnen ein gründliches Verständnis der robusten Sicherheitsfunktionen von HPE Compute Ops Management.

HPE Compute Ops Management wurde mit einem Sicherheitsfokus entwickelt und zielt auf drei wesentliche Anforderungen ab:

– Vertrauenswürdiges HPE Compute Ops Management in der Cloud, mit im Server integrierten HPE iLO Managementprozessor. Beide Angebote verfügen über von HPE CA ausgestellte Zertifikate, die zur gegenseitigen Überprüfung der Authentizität verwendet werden.

– Datenverschlüsselung in der Cloud

  - Alle Kundendaten in HPE Compute Ops Management werden bei Inaktivität mithilfe von AES-256 und während der Übertragung mithilfe von TLS 1.2 oder 1.3 verschlüsselt.

– Mandantenfähige Isolierung für mehr Sicherheit

  - Die Daten jedes Kunden von HPE Compute Ops Management sind von denen anderer Mandantenunternehmen logisch isoliert, wodurch Datenschutz und Datenzugriffsschutz sichergestellt wird.

Wichtig: Der in den Server integrierte HPE iLO Managementprozessor kommuniziert mit HPE Compute Ops Management. Das Server-Betriebssystem oder vom Kunden installierte Anwendungen kommunizieren nicht mit HPE Compute Ops Management und tauschen keine Daten damit aus.

Darüber hinaus bietet HPE branchenführende Servicefunktionen, die Sicherheitsunterstützung der Enterprise-Klasse für die Einrichtung sicherer Daten und kontrollierter Zugriffe bereitstellen.

Zielgruppe

Die Zielgruppe dieses Dokuments sind Kunden mit HPE Compute Ops Management. Zu den Kundenrollen gehören Mitarbeitende der Unternehmenssicherheit und des Risikomanagements sowie Serveradministratoren, die mit HPE Compute Ops Management arbeiten werden.

Sie sollten mit Computerkonzepten im Zusammenhang mit Management, Netzwerken, Sicherheit und HPE Servern sowie den infrastrukturellen Bedürfnissen und Anforderungen Ihres Unternehmens vertraut sein.

Tabelle 1. Terminologie

Begriff	Erläuterung
COM	Compute Ops Management
CVE	Common Vulnerabilities and Exposures ist eine Liste von Aufzeichnungen über Schwachstellen bei der Cybersicherheit. Auf der Website cve.mitre.org werden die Umgehungslösungen oder Behebungen für alle entdeckten CVEs verfolgt und aufgezeichnet.
DDoS	Ein Distributed-Denial-of-Service-Angriff ist ein böswilliger Versuch, die Netzwerkkommunikation mit einem Cloud-Service zu unterbrechen.

Tabelle 1. Terminologie (Fortsetzung)

Begriff	Erläuterung
HPE iLO	HPE Integrated Lights-Out. HPE iLO Servermanagementsoftware, mit der Sie HPE Server sicher und nahtlos von überall auf der Welt konfigurieren, überwachen und aktualisieren können. In diesem Dokument bezieht sich der Begriff „HPE iLO" auf HPE iLO 5.
HTTPS	Hyper Text Transfer Protocol Secure bietet sichere Kommunikation für den Datenaustausch über Computernetzwerke. Der HTTPS-Datenverkehr wird über TLS verschlüsselt und bietet Unterstützung für die Authentifizierung über asymmetrischen Schlüsselaustausch.
mTLS	Mutual TLS bietet eine kryptografische Methode für den Aufbau und den Schutz eines sicheren Kommunikationstunnels über Computernetzwerke. In diesem Tunnel authentifiziert der Server den Client und der Client den Server.
RBAC	Bei der rollenbasierten Zugriffskontrolle (Role-Based Access Control) wird einem bestimmten Benutzer eine eindeutige Berechtigung zugewiesen, die es ihm ermöglicht, für eine bestimmte Komponente erlaubte Aktionen durchzuführen. Diese Funktion bietet gerade genug Berechtigungen, um das Zero Trust-Sicherheitsmodell zu unterstützen.
SaaS	Software-as-a-Service ist das Lizenzierungs- und Bereitstellungsmodell für Software auf Abonnementbasis. Es wird zentral gehostet.
SAML	Security Assertion Markup Language bietet ein Protokoll zur Integration von SSO durch den Kunden.
SSO	Single Sign-On ist ein Authentifizierungsmechanismus, der es Benutzern ermöglicht, sich mit einer einzigen ID und einem einzigen Passwort bei mehreren unabhängigen Systemen anzumelden. SSO ordnet mehrere Benutzer innerhalb eines Unternehmens ein, sodass eine einzige Authentifizierung für verteilte Anwendungen verwendet werden kann.
TLS	Das Transport Layer Security-Protokoll bietet kryptografische Methoden, um geschützte und sichere Kommunikationstunnel über Computernetzwerke (Internet) aufzubauen, sodass der Client den Server erkennt.

Übersicht

HPE Compute Ops Management ist eine sichere, skalierbare Cloud-basierte Managementplattform, die auf einer Microservice-Architektur basiert. Sie erleichtert das Onboarding, die Inventarisierung, die Zustands- und Leistungskontrolle sowie das Firmware-Management von HPE Servern wie in Abbildung 1 dargestellt. HPE Compute Ops Management wird kontinuierlich verbessert und um neue Funktionen erweitert.

Hinweis: HPE Compute Ops Management übernimmt das von HPE GreenLake durchgesetzte Cloud-Sicherheits-Framework.

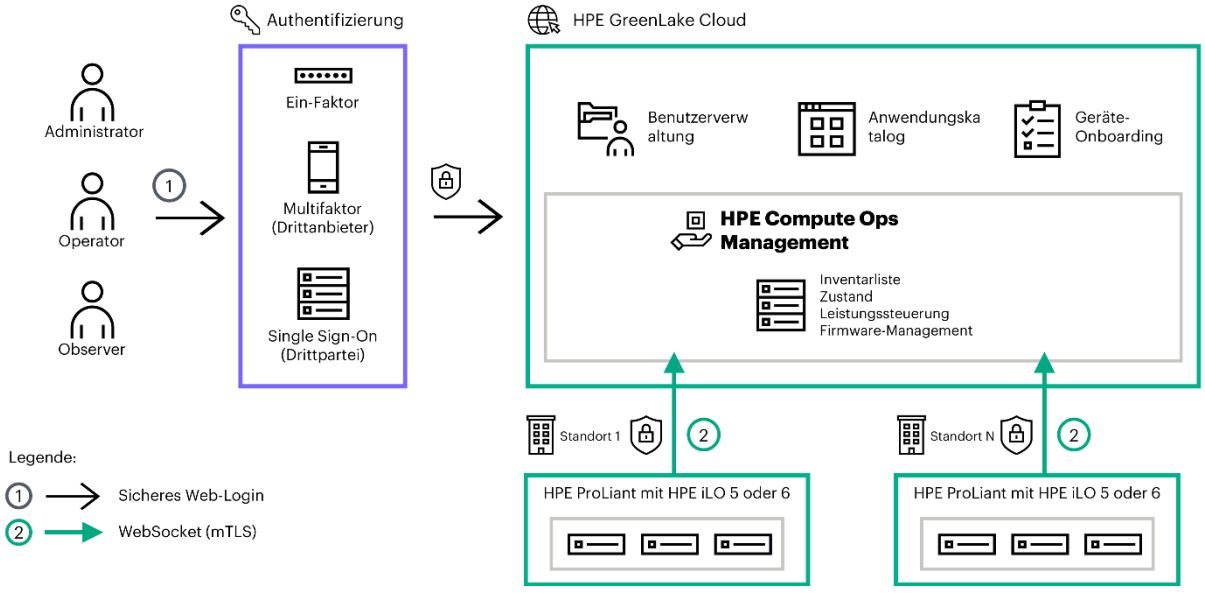


Abbildung 1. Darstellung der HPE Compute Ops Management Sicherheit

Die Sicherheit dieser Lösung basiert auf einem Modell der geteilten Verantwortung für Kunden und HPE. Dabei werden die Räumlichkeiten von Kunden und Hosting-Anbietern sowie die Rollen von Benutzern als Verbraucher und von HPE als Serviceprovider berücksichtigt. Abbildung 2 veranschaulicht dieses Modell der geteilten Sicherheitsverantwortung.
Die Kunden- und Serverinformationen in der Cloud gehören dem Kunden. HPE sichert sie in seiner Funktion als Verwalter.

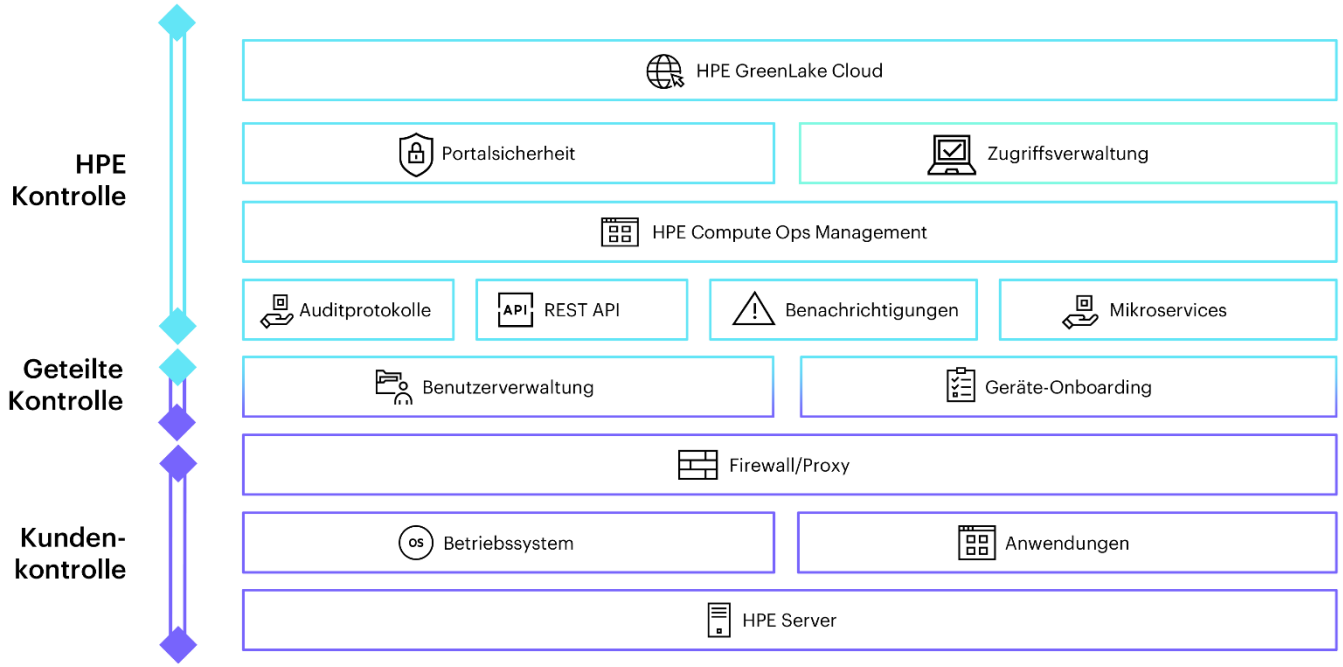


Abbildung 2. Geteiltes Sicherheitsmodell

Seien Sie vorbereitet

HPE Compute Ops Management bietet eine Reihe von Funktionen, die in die Cybersicherheitsprozesse und -pläne von Kunden integriert werden.

Für Kunden zugängliche Netzwerkverbindungen oder Endpunkte
Kunden nutzen die HPE Compute Ops Management Services über ein TLS-gesichertes Webportal und integrieren ihre lokalen Komponenten über mTLS-Verbindungen, wie in Abbildung 1 dargestellt. Ihre Cybersicherheitsprozesse und Ihre Dokumentation sollten diese Verbindungen und Port-Einstellungen berücksichtigen.

Wichtig: HPE empfiehlt dringend, die gesamte Kommunikation zwischen HPE Compute Ops Management und HPE GreenLake durch eine geeignete Firewall und HTTP-Proxy-Geräte zu schützen.

– **Webportal (TLS):** Sie können für den Zugriff auf HPE GreenLake einen Standard-Webbrowser verwenden. Der Schutz erfolgt über HTTPS mit TLS v1.3 oder 1.2 mit einem von HPE CA signierten Zertifikat für eine authentifizierte, verschlüsselte und sichere Verbindung. Zur Validierung der Authentizität müssen Benutzer von HPE GreenLake eine korrekte Kombination aus Benutzername und Passwort angeben. Darüber hinaus werden MFA und SSO mit SAML 2.0 als sicherere und bevorzugte Methoden zur Authentifizierung unterstützt. Diese werden später in diesem Dokument erläutert.

Das CA-Zertifikat verwendet SHA256 mit einer Schlüsselgröße von EC 384 Bit. In Tabelle 2 werden die unterstützten TLS v1.2- und 1.3-Chiffren-Suites erläutert.

Tabelle 2. Von öffentlichen APIs unterstützte Chiffren-Suites

Beschreibung	TLS-Version	Chiffren-Suite
Die folgenden Chiffren-Suites werden in der vom Server bevorzugten Reihenfolge unterstützt:	TLS 1.3-Chiffren	TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256v
	TLS 1.2-Chiffren	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

– **Geräteverbindung (mTLS):** Die in den On-Premises-Server des Kunden integrierten Managementprozessoren HPE iLO 5 oder HPE iLO 6 verbinden sich über eine gesicherte HTTPS-Verbindung (Port 443) mit HPE Compute Ops Management und ermöglichen so eine bidirektionale Kommunikation für Onboarding, Bestandsführung, Zustand, Energiekontrolle und Firmware-Management. Dieser WebSocket wird während der Onboarding-Schritte erstellt und bleibt mit einer dauerhaften Verbindung zur HPE Compute Ops Management Cloud geöffnet. Diese Verbindung wird über ein von HPE ausgestelltes Client-Zertifikat in HPE iLO gesichert. Die Verbindung wird immer durch das Gerät initiiert und stellt eine ausgehende Konnektivität zur HPE GreenLake Cloud her. HPE OneView nutzt denselben Ansatz für die Kommunikation mit HPE Compute Ops Management über HTTPS (Port 443) mit einem mTLS-gesicherten WebSocket.

Wichtig: Der in den Server integrierte HPE iLO Managementprozessor kommuniziert mit HPE Compute Ops Management und ist vom Server isoliert.

Wenn Netzwerkprobleme auftreten, wird dieser WebSocket auf beiden Seiten geschlossen. HPE iLO versucht in regelmäßigen Abständen und mit einem Backoff-Algorithmus, die WebSocket-Verbindung zu HPE Compute Ops Management herzustellen, bis letztendlich einmal täglich versucht wird, die Verbindung herzustellen, bis die WebSocket-Verbindung wiederhergestellt ist. Dadurch hält die Lösung Netzwerkausfällen zwischen dem On-Premises-Server und der Cloud stand. Die WebSocket-Verbindung und der Wiederholungsversuch werden abgebrochen, wenn das Cloud-basierte Management in HPE iLO deaktiviert ist.

Wichtig: Beim mTLS-gesicherten Datenverkehr werden beide Endpunkte der Kommunikation zwischen Ihrem lokalen Gerät und HPE Compute Ops Management validiert. Die mTLS-Validierung eignet sich nicht gut für Prüfungen des Datenverkehrs. Jeder Versuch, eine Paketprüfung durchzuführen, führt dazu, dass die Validierung des HPE Zertifikats fehlschlägt und die Verbindung abgelehnt wird. Die Inspektion des Datenverkehrs muss so konfiguriert werden, dass eine Unterbrechung der Kommunikation mit den dokumentierten HPE Endpunkten vermieden wird.

Die Kunden müssen auf ihrer Firewall nur Port 443 für die ausgehende Kommunikation mit verschiedenen COM-Endpunkten öffnen. Zu den öffentlichen Schnittstellen-FQDN, den verwendeten Ports und dem Initiator, die auf das Internet zugreifen, gehören:

Wichtig:

Ersetzen Sie in den folgenden Tabellen 3 und 4 „<region>“ durch die Region, die Sie für die Integration Ihrer Geräte in HPE GreenLake ausgewählt haben:

„us-west2“ für die Region Nord-, Mittel- und Südamerika

„eu-central1“ für die Region Europa

„ap-northeast1“ für die Region Asien-Pazifik

Möchten Sie beispielsweise die Region EU (zentral) verwenden, wird die Variable „<region>“ in den URLS in Tabelle 3 durch „eu-central1“ ersetzt und bildet:

Eu-central1.compute.cloud.hpe.com

Eu-central1-api.compute.cloud.hpe.com

Die Kunden müssen nur auf ihrer Firewall Port 443 für die ausgehende Kommunikation mit verschiedenen COM-Endpunkten öffnen. Zu den öffentlichen Schnittstellen-FQDN, den verwendeten Ports und dem Initiator, der auf das Internet zugreift, gehören:

Tabelle 3. Firewall-Anforderungen für den Client-Browser

Öffentliche Schnittstellen-FQDN	Platzhal-ternamе	Port	Protokoll	Richtung	Beschreibung
cloud.hpe.com	*.hpe.com	443	TCP	Ausgehend	Ermöglicht die Kommunikation mit HPE GreenLake
common.cloud.hpe.com		443	TCP	Ausgehend	Ermöglicht die Anmeldung bei HPE Compute Ops Management
<region>.compute.cloud.hpe.com		443	TCP	Ausgehend	Benutzeroberflächen-Assets und Anwendungs-APIs für HPE Compute Ops Management
<region>-api.compute.cloud.hpe.com		443	TCP	Ausgehend	API-Endpunkte für HPE Compute Ops Management
client.greenlake.hpe.com		443	TCP	Ausgehend	Gemeinsam genutzte HPE GreenLake UI-Bibliotheken wie die In-App-Lader für Hilfeseiten
www.hpe.com		443	TCP	Ausgehend	UI-Assets für das Branding, z. B. Schriftarten von HPE
support.hpe.com zugänglich		443	TCP	Ausgehend	In-App-Hilfeinhalte, Ankündigungen und Benachrichtigungen
https://hpetraining.co1.qualtrics.com		443	TCP	Ausgehend	Ermöglicht den Zugriff auf Benutzer-Feedback für HPE Compute Ops Management
ccprod-hpecomputesupport-<region>.s3.amazonaws.com		443	TCP	Ausgehend	API-Endpunkt zum Hochladen von AHS-Protokolldateien zur Analyse und zum Herunterladen analysierter Inhalte, z. B. Serverinventardaten
consent.trustarc.com	-NA- *.launchdarkly.com	443	TCP	Ausgehend	Cookie-Einwilligungsverwaltung für den globalen Header **Hinweis:** Für die Region Amerika ersetzen Sie „<region>“ durch us-west-2 statt us-west2
d2ezht69fz5a7f.cloudfront.net		443	TCP	Ausgehend	UI-Assets zur Unterstützung des Karten-Widgets auf der Übersichtsseite von HPE Compute Ops Management
app.launchdarkly.com		443	TCP	Ausgehend	Launch Darkly wird verwendet, um ausgewählte Funktionen für ausgewählte Situationen zu aktivieren und hilft, dass die Site schnell auf Änderungen reagieren kann
clientstream.launchdarkly.com	*.launchdarkly.com	443	TCP	Ausgehend	Launch Darkly wird verwendet, um ausgewählte Funktionen für ausgewählte Situationen zu aktivieren und hilft, dass die Site schnell auf Änderungen reagieren kann
events.launchdarkly.com		443	TCP	Ausgehend	Ermöglicht den Zugriff auf Benutzer-Feedback für HPE Compute Ops Management

Tabelle 4. Firewall-Anforderungen für HPE iLO/HPE OneView

Öffentliche Schnittstellen-FQDN	Port	Protokoll	Richtung	Beschreibung
device.cloud.hpe.com	443	TCP	Ausgehend	Ermöglicht die Kommunikation mit HPE GreenLake
midway.ext.hpe.com	443	TCP	Ausgehend	Client-Zertifikat abrufen und Firmware herunterladen
midway-<region>.ext.hpe.com	443	TCP	Ausgehend	Client-Zertifikat abrufen und Firmware herunterladen
<Region>-devices.compute.cloud.hpe.com	443	TCP	Ausgehend	Regionaler WebSocket-Endpunkt für Geräte
<Region>-mtls.compute.cloud.hpe.com	443	TCP	Ausgehend	Regionaler API-Endpunkt für Geräte

Für die mTLS-Verbindung ist das HPE iLO Zertifikat ECDSAp384 und die Schlüsselgröße beträgt 384 Bit.

Die mTLS-Endpunkte, zu denen Geräte eine Verbindung herstellen, unterstützen eine begrenzte Reihe von Chiffren, die die Geräte verwenden müssen. Die Geräte an sich unterstützen mehr Schlüssel, als hier aufgezählt werden, allerdings legt der Cloud-Endpunkt nur die folgenden Schlüssel offen:

Tabelle 5. Von Geräten unterstützte Chiffren-Suites

Beschreibung	TLS-Version	Chiffren-Suite
Die folgenden Chiffren-Suites werden in der vom Server bevorzugten Reihenfolge unterstützt:	TLS 1.3	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256
	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Verbindungen über HPE OneView sind mittels ähnlicher Algorithmen, Chiffren und Protokolle gesichert. Weitere Details finden Sie im HPE OneView Benutzerleitfaden.

Benutzerauthentifizierung

In diesem Abschnitt werden die branchenüblichen Authentifizierungsmethoden beschrieben, die für HPE Compute Ops Management verfügbar sind. HPE bietet drei Arten von Authentifizierungen für die Anmeldung bei HPE GreenLake.

- Single Sign-On (SSO)
- Mehrfaktor-Authentifizierung (MFA)
- Ein-Faktor-Authentifizierung

Single Sign-On-Authentifizierung

SSO-Authentifizierung ermöglicht es Unternehmen, die Benutzererfahrung bei der Anmeldung in externen Portalen zu vereinfachen, indem Benutzer ihre Anmeldeinformationen für das Unternehmen eingeben können, um ihre Identität zu authentifizieren.

Die Benutzer können sich mittels der Anmeldeinformationen ihres Unternehmens bei HPE GreenLake anmelden. Nach der Anmeldung verifiziert HPE GreenLake diese Anmeldeinformationen, indem es eine SAML-Anfrage (digital signiertes XML) an den vertrauenswürdigen IdP des Unternehmens des Benutzers sendet, der die Anmeldeinformationen verifiziert und eine SAML-Antwort zurücksendet, die die Gültigkeit der Daten bestätigt.

Mehrfaktor-Authentifizierung

Die Mehrfaktor-Authentifizierung implementiert mehrere Authentifizierungsebenen für einen Benutzer, um Zugang zu HPE GreenLake zu erhalten. HPE unterstützt softwarebasierte Authentifikatoren (Okta-Verifizierung, Sicherheitsschlüssel oder biometrischer Authentifikator, Google Authenticator™), die in Kombination mit einer herkömmlichen Benutzeranmeldung eine zusätzliche Sicherheitsebene bilden.

Ein-Faktor-Authentifizierung

Die Ein-Faktor-Authentifizierung erfordert einen Benutzernamen und ein Passwort, um die Identität eines Benutzers zu überprüfen. Die Passwörter müssen folgende Kriterien erfüllen:

- Sie müssen zwischen 8 und 255 Zeichen enthalten, mit mindestens fünf eindeutigen Zeichen
- Nicht mehr als zwei Zeichen dürfen wiederholt werden
- Sie müssen mindestens ein Sonderzeichen, ein numerisches Zeichen, einen Großbuchstaben und einen Kleinbuchstaben enthalten
- Sie dürfen keine Benutzerkontendaten enthalten und werden mit einer Liste häufig verwendeter Passwörter abgeglichen

Alle validierten Passwörter unterliegen einer strengen Richtlinie:

- Neue Passwörter dürfen nicht mit den letzten sechs Passwörtern übereinstimmen, die innerhalb der letzten 365 Tage verwendet wurden.
- Passwörter verfallen automatisch nach 182 Tagen.
- Konten mit mehrfachen fehlgeschlagenen Anmeldeversuchen werden automatisch für eine bestimmte Zeit gesperrt.

Rollenbasierte Zugriffssteuerung für Benutzer

HPE GreenLake

HPE GreenLake Benutzerberechtigungen werden mithilfe rollenbasierter Zugriffskontrolle (RBAC) durchgesetzt, um sicherzustellen, dass jeder Benutzer den benötigten Zugriff erhält. Der Administrator einer Organisationseinheit hat die Möglichkeit, vordefinierte, von HPE GreenLake bereitgestellte Rollen zuzuweisen oder eigene Rollen für Benutzer zu erstellen. Informationen dazu finden Sie im HPE GreenLake Cloud Benutzerhandbuch.

Hinweis: Dem Ersteller der Organisationseinheit innerhalb von HPE GreenLake werden automatisch Administratorrechte zugewiesen.

HPE Compute Ops Management

Dieser Abschnitt beschreibt die rollenbasierte Zugriffskontrolle (RBAC) für HPE Compute Ops Management. Wir empfehlen, dass Sie sich im HPE GreenLake Cloud Benutzerhandbuch genauer über die RBAC-Funktionen in HPE GreenLake informieren. HPE Compute Ops Management unterstützt drei Rollen, die in Ihren Cybersicherheitsprozessen und -plänen klar definiert sein sollten.

Tabelle 6. RBAC-Rollen in HPE Compute Ops Management

Typ	Zugewiesene Berechtigungen
Administrator	Diese Rolle gewährt alle Berechtigungen für die Kundenorganisation, einschließlich Onboarding, Asset-Management, Rollenerstellung, Benutzereinladungen sowie der Zuweisung von Benutzerrollen
Bediener	Gewährt Berechtigungen für das Bearbeiten von Servern, Zeitplänen und Benutzergruppen. Bei allen anderen Ressourcen ist der Zugriff schreibgeschützt
Beobachter	Gewährt Berechtigungen zur Ansicht von Komponenten in der zugewiesenen Organisation, ohne die Möglichkeit, Änderungen vorzunehmen

Geräte-Onboarding in HPE Compute Ops Management

In diesem Abschnitt werden Sicherheitsaspekte beschrieben, die Sie beim Geräte-Onboarding beachten müssen.

Wichtig: Die gesamte Kommunikation für das Geräte-Onboarding wird immer von HPE iLO initiiert. Es wird nie eine von der Cloud initiierte Anfrage zur Erkennung von Geräten beim Onboarding geben. Die Netzwerkkommunikation ist mit mTLS gesichert.

Verbindungen zu HPE GreenLake werden mit HTTPS und TLS v1.3 hergestellt. RBAC stellt sicher, dass Sie zur richtigen Instanz mit den richtigen Berechtigungen geleitet werden.

Wenn die Cloud-basierte Verwaltung in HPE iLO aktiviert ist, wird eine WebSocket-Verbindung mit mTLS zwischen HPE iLO und HPE Compute Ops Management hergestellt. Dieser WebSocket ist permanent und wird nur dann dauerhaft deaktiviert, wenn das Cloud-basierte Management deaktiviert ist.

Onboarding von HPE OneView Appliances in HPE Compute Ops Management – OneView Edition

Das Onboarding von HPE OneView Appliances in HPE Compute Ops Management kann über ein etwas anderes Verfahren erfolgen, jedoch unter Anwendung der gleichen robusten Sicherheitsmechanismen. So bleiben vertrauenswürdige private Verbindungen gewährleistet. Die einzigartige HPE OneView Appliance ID wird aus der HPE OneView Instanz entnommen und in HPE Compute Ops Management eingegeben. Wird die Appliance-ID in die Benutzeroberfläche von HPE Compute Ops Management eingegeben, dann gibt sie einen Aktivierungsschlüssel aus. Dieser Schlüssel ist für jede Appliance eindeutig und kann nur für das Onboarding der jeweiligen Appliance verwendet werden.

Wenn der Aktivierungsschlüssel in die HPE OneView Benutzeroberfläche eingegeben wurde, um das Cloud-Management zu ermöglichen, dann stellt die HPE OneView Instanz eine dauerhafte mTLS-WebSocket-Verbindung mit dem Endpunkt von HPE Compute Ops Management in der Cloud her. Diese Verbindung wird mit einem von HPE ausgegebenen Sicherheitszertifikat gesichert, ähnlich dem, das beim Onboarding von HPE iLO in HPE Compute Ops Management genutzt wird. Schließlich wird, wenn Zertifizierung und Aktivierung fertiggestellt sind, eine mTLS-Verbindung hergestellt.

Wichtig: Der Zugriff auf Geräte mit HPE Compute Ops Management – OneView Edition wird über Serviceabonnements verwaltet. Ein Abonnement für HPE Compute Ops Management – OneView Edition ist zum Verwalten von Geräten mit HPE Compute Ops Management – OneView Edition innerhalb von HPE Compute Ops Management nötig. Außerdem wird der Zugriff auf die Verwaltung von Geräten mit HPE Compute Ops Management – OneView Edition über Benutzerrechte geregelt. Wird einem Benutzer-Account nicht der passende Zugriff für HPE Compute Ops Management – OneView Edition hinzugefügt, dann kann der Benutzer Geräte mit HPE Compute Ops Management – OneView Edition innerhalb von HPE Compute Ops Management nicht sehen.

RBAC für HPE iLO

HPE iLO verfügt auch über RBAC für die lokalen Benutzer. In HPE iLO sind vier Rollen definiert, wie in Tabelle 7 dargestellt. Diese Rollen werden nur für den lokalen direkten Zugriff auf HPE iLO verwendet und nicht für die Kommunikation mit HPE Compute Ops Management.

Tabelle 7. RBAC-Rollen in HPE iLO

Typ	Zugewiesene Berechtigungen
Administrator	Alle Berechtigungen mit Ausnahme des Recovery Sets (für das Onboarding verwendbar)
Operator	Erlaubt alle Privilegien außer: Konfiguration von HPE iLO 5 Einstellungen, Verwaltung von Benutzerkonten und Recovery Set (für das Onboarding verwendbar)
Lesezugriff	Nur Anmeldeberechtigung
Benutzerdefiniert (Standard)	Ermöglicht dem Benutzer, individuelle Berechtigungen zu definieren (verwendbar für Onboarding mit erforderlichen benutzerdefinierten Rolleneinstellungen)

Hinweis: Nur von HPE autorisierte Techniker haben mit Zustimmung des Kunden Zugang zu Kunden-Accounts für die Fehlerbehebung.

So schützen HPE Compute Ops Management und HPE GreenLake Sie in der Cloud

Risikobewertungen
HPE Compute Ops Management nimmt eine regelmäßige Überprüfung der Anwendungsarchitektur sowie eine Bedrohungsanalyse vor, um jegliche im System vorhandenen Risiken zu erkennen und zu ermitteln, wie diese Risiken gemindert oder beseitigt werden können. Mithilfe dieser Analyse kann HPE Compute Ops Management alle Schwachstellen beheben, bevor ein Angriff erfolgt, Schutz vor Systemdiebstahl und -beschädigung bieten sowie Strafzahlungen aufgrund nicht eingehaltener Vorschriften vermeiden.

Schutz vor Schwachstellen
Wenn eine Schwachstelle entdeckt wird, analysieren die Techniker von HPE die CVEs und bestimmen, inwieweit die Schwachstelle das Cloud-Design von HPE Compute Ops Management betrifft. CVEs, die das Cloud-Modell von HPE Compute Ops Management betreffen, werden entschärft oder mit Umgehungslösungen behandelt, die die erkannten CVEs in dem von HPE Compute Ops Management kontrollierten Bereich abschwächen. Wenn der Kunde zusätzliche Maßnahmen On-Premises durchführen muss, bietet HPE ein Bulletin, das die Anforderungen detailliert erläutert.

HPE Compute Ops Management hat die Anwendungssicherheit in den Software Development Lifecycle integriert, um Verstöße und Vorfälle auf Webanwendungsebene zu verhindern. HPE Compute Ops Management testet Anwendungen kontinuierlich auf Schwachstellen unter Verwendung von Standards wie dem OWASP Application Security Verification Standard (ASVS). Dabei werden Anwendungen auf Remote-Code-Ausführung, SQL-Injektion, Cross-Site-Scripting (XSS), Identität und Zugriff, Sitzungsvalidierung, Code-Injektionen, Kryptografie und mehr geprüft.

Sichere Architektur
HPE Compute Ops Management wird mit containerisierten Microservices entwickelt und implementiert. Die Container werden mit von HPE kontrollierten minimalen Basis-Images erstellt. Container, die mit Basis-Images erstellt werden, bieten Entwicklern die volle Kontrolle über den Inhalt, was es wiederum den Technikern von HPE ermöglicht, Sicherheitsprobleme schnell zu beheben und Microservices mit behobenen Fehlern auf hocheffiziente Weise neu bereitzustellen.

HPE Compute Ops Management setzt Tools ein, die infrastrukturelle Schwachstellen, Fehlkonfigurationen und Compliance-Verstöße in den Code-Vorlagen, Container-Images und Git-Repositorys identifizieren. Ebenso führt es regelmäßig Architekturprüfungen sowie Netzwerk- und Anwendungspenetrationstests vor.

API-Gateway und Amazon CloudFront
Durch Authentifizierung auf Anwendungsebene bietet das API-Gateway Schutz vor DDoS-Angriffen, um gefälschte Anfragen zu verhindern. Zugleich verhindert der Übertragungsgrenzschutz SYN-Flood-Angriffe. Darüber hinaus bietet das API-Gateway eine Verschleierung der Lösungskomponenten, ermöglicht die Autorisierung von APIs und kontrolliert den Zugriff auf ausgewählte Endpunkte. Amazon CloudFront stellt den Caching-Layer und die Integration mit einer Webanwendungs-Firewall für zusätzliche Sicherheitsebenen bereit.

Gespeicherte Kundendaten
HPE GreenLake speichert und verwendet Daten für HPE Compute Ops Management. Hierzu zählen HPE iLO Bestandsdaten, Statusinformationen sowie HPE OneView Daten für verwaltete physische Geräte und logische Ressourcen. HPE GreenLake speichert keine HPE OneView Anmeldeinformationen. Bei Inaktivität sind alle Daten verschlüsselt.

RBAC prüft, ob die Benutzer den richtigen Zugriff auf die einzelnen Ressourcen in der Anwendung haben. Mit HPE Compute Ops Management können Kunden ihre IT-Geschäftsprozesse mithilfe von RBAC planen. Daten im Zusammenhang mit Benutzer-Accounts und Kundendetails für jeden HPE Compute Ops Management Kunden werden von anderen Mandantenunternehmen auf HPE GreenLake Ebene isoliert. Dadurch wird ein konsistenter Datenschutz und Datenzugriffsschutz über alle Anwendungen hinweg sichergestellt.

Die in HPE Compute Ops Management gespeicherten Daten bleiben in der Region, die bei der Ersteinrichtung angegeben wurde. Weitere Informationen finden Sie in der HPE Datenschutzerklärung unter hpe.com/de/de/legal/privacy.html.

Daten, auf die HPE Mitarbeiter oder -Partner zugreifen können
Forschungs- und Entwicklungsteams und Partner von HPE haben keinen Zugriff auf kundenbezogene Daten und Anwendungsdaten. Allerdings hat eine minimale Anzahl von Technikern mit Kundengenehmigung schreibgeschützten Zugriff auf Kundendaten (z. B. Benutzernamen, Adressen sowie Informationen zum Servernetzwerk). Wir pflegen eine separate Umgebung für die interne Entwicklung, in der keine Kundendaten gespeichert werden dürfen.

Gewährleistung von Sicherheit und Compliance
HPE Compute Ops Management hat kürzlich CSA STAR Level 1 abgeschlossen: Selbsteinschätzungen für mehr Transparenz bei den zur Sicherung der Kundendaten eingerichteten Sicherheitskontrollen. Weitere Informationen finden Sie im CAIQ für HPE Compute Ops Management.

HPE Compute Ops Management hat auch die SOC 2 Typ 1 und Typ 2 Bescheinigung.

HPE arbeitet aktiv an der Zertifizierung nach FIPS 140-2 Level 1. Alle Daten, die zwischen den Kundengeräten vor Ort und dem HPE Compute Ops Management Geräteportal übertragen werden, sind durch FIPS 140-2-konforme Verschlüsselung und Chiffren geschützt. Ebenso werden alle Daten bei der Übertragung und bei Inaktivität innerhalb der Softwareanwendung mit FIPS 140-2 Verschlüsselung und Ciphers geschützt. Die gesamte Verschlüsselung innerhalb der Anwendung erfolgt durch OpenSSL 1.1.1, und wir arbeiten aktiv an der Implementierung eines FIPS-zertifizierten OpenSSL 3.0-Anbieters. Die HPE Compute Ops Management Anwendung wurde entwickelt, um von Grund auf FIPS 140-2-Compliance zu gewährleisten.

Kunden müssen keine Änderungen an ihrer Software oder ihrem Account vornehmen, um die FIPS 140-2-Compliance zu gewährleisten.

Lizenzerklärung für Open Source-Software
Erklärungen zu Open Source-Softwarelizenzen finden Sie im HPE GreenLake Cloud Benutzerhandbuch und der Online-Hilfe zu HPE Compute Ops Management.

Erklärung zur Datensicherheit und zum Datenschutz für HPE GreenLake und HPE Computing Ops-Management
HPE respektiert und berücksichtigt die weltweit wichtigsten Datenschutzgrundsätze und -rahmenwerke, darunter die OECD-Richtlinien zum Datenschutz und zum grenzüberschreitenden Datenverkehr [OECD Guidelines on the Protection of Privacy and Transborder Flows], die Datenschutz-Grundverordnung 2016/679 (DSGVO) [GDPR] und das APEC-Datenschutzrahmenwerk [APEC Privacy Framework]. Die in dieser Datenschutzerklärung beschriebenen Datenschutzpraktiken von HPE entsprechen auch dem APEC Cross Border Privacy Rules (CBPR) System [APEC-System zur grenzüberschreitenden Datenschutzregulierung]. Weitere Informationen finden Sie in der HPE Datenschutzerklärung unter hpe.com/de/de/legal/privacy.html.

Weitere Details zu den Sicherheitsrichtlinien, Verfahren und der regulatorischen Compliance von HPE finden Sie im Referenzhandbuch zur HPE Computing-Sicherheit.

Weitere Informationen unter

HPE.com/info/COM

HPE.com besuchen

Jetzt chatten

a50004539DEE

HEWLETT PACKARD ENTERPRISE

hpe.com