Dell EMC OpenManage Integration Version 1.1.1 mit Microsoft Windows Admin Center

Benutzerhandbuch

February 2021
Rev. A01

Hinweise, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.

WARNUNG: Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.

Inhaltsverzeichnis

1

Übersicht über die OpenManage Integration mit Microsoft Windows Admin Center

Dell EMC OpenManage Integration mit Microsoft Windows Admin Center (OMIMSWAC) ermöglicht IT-Administratoren die Verwaltung der PowerEdge-Server als Hosts, mit PowerEdge-Servern erstellte Microsoft Failover-Cluster und mit Dell EMC Lösungen für Microsoft Azure Stack HCI erstellte hyperkonvergente Infrastruktur (HCI; Storage Space Direct Ready-Nodes or AX-Nodes). OMIMSWAC vereinfacht die Aufgaben von IT-Administratoren durch die Remote-Verwaltung der PowerEdge-Server und -Cluster während des gesamten Lebenszyklus. Weitere Informationen zu den Funktionen und Vorteilen von OMIMSWAC finden Sie in der Dokumentation unter Dell.com/OpenManageManuals.

Hauptmerkmale der OMIMSWAC

- OMIMSWAC bietet IT-Administratoren eine vereinfachte Lösung, um Folgendes effizient zu managen:
  - Dell EMC PowerEdge-Server, die auf unterstützten Windows-Betriebssystemen ausgeführt werden.
  - Azure Stack HCI Cluster auf Basis von AX-Nodes oder Storage Spaces Direct Ready Nodes von Dell EMC.
  - Microsoft-Failover-Cluster, die mit Dell EMC PowerEdge-Servern erstellt wurden.
- Anzeigen des Gesamt-Funktionszustands, des Hardwarebestands und des iDRAC-Bestands der Nodes, einschließlich Informationen auf Komponentenebene für alle unterstützten Dell EMC Plattformen.
- Stellt Aktualisierungs-Compliance-Berichte für von Dell EMC verifizierte Aktualisierungskataloge und Benachrichtigungen für neue Katalogversionen bereit.
- Unterstützung für verschiedene Baselines in OMIMSWAC, wenn sie mit dem Internet verbunden sind:
  - Dell EMC Enterprise Katalog für PowerEdge Server und Cluster, die PowerEdge Server enthalten.
  - Dell EMC Azure Stack HCI Lösungskatalog für Dell EMC Lösungen für Microsoft Azure Stack HCI.
  - Dell EMC MX Lösungskatalog für PowerEdge MX Modular.
- Unterstützung für lokale Baselines, die mithilfe von Dell EMC Repository Manager (DRM) erstellt wurden.
- Aktualisieren von PowerEdge-Servern anhand einer Baseline – BIOS, Treiber, Firmware und/oder Systemmanagementanwendungen.
- Clusterfähiges Update anhand validierter Baseline (BIOS, Treiber, Firmware und/oder Systemmanagementanwendung) für serverbasierte PowerEdge Failover-Cluster und Dell EMC-Lösungen für Microsoft Azure Stack HCI.
- Zeigt iDRAC-Informationen zu PowerEdge-Servern an. Für die Out-of-band-Verwaltung können Sie die iDRAC-Konsole direkt über Windows Admin Center starten.
- Verfügbarkeit der OMIMSWAC-Erweiterung und -Dokumentation in den Sprachen Englisch, Französisch, Deutsch, Spanisch, vereinfachtes Chinesisch und Japanisch.

Themen:

Versionsverlauf

Date	Dokumentversion	Beschreibung der Änderungen
August 2020	A00	Erste Version für OMIMSWAC 1.1.1
Januar 2021	A01	• Zusätzliche Unterstützung für Windows Admin Center 2009 GA. • Ziel-Nodes, die Windows Server Core Betriebssystem ausführen, werden nicht unterstützt.

Was ist neu in dieser Version?

Release 1.1.1

- Unterstützung für Microsoft Windows Admin Center Version 2007 GA und 2009 GA.
- Unterstützung für PowerEdge XE2420 Edge Server mit iDRAC Firmware 4.00.129.00 oder höher.
- Fehlerbehebungen und Verbesserungen:
  - Sie können auf OMIMSWAC über die Konsole von Windows Admin Center (WAC) zugreifen, nachdem Sie sich mit den Gateway-Nutzeranmeldedaten ohne Administratorrechte beim WAC angemeldet haben.

    In der vorherigen Version wurde der Zugriff auf OMIMSWAC von der WAC-Konsole verweigert, wenn Sie sich mit den Gateway-Nutzeranmeldedaten ohne Administratorrechte angemeldet haben.
  - Ermöglicht OMIMSWAC das Abrufen von Bestandsinformationen für Cluster, die über Single Sign-On verbunden sind.

    In der vorherigen Version schlug das Abrufen von Bestandsinformationen fehl, wenn ein Cluster über Single Sign-On verbunden war, und WAC reagierte nicht mehr.
  - Ermöglicht das Erstellen eines Compliance-Berichts für Ziel-Nodes oder Cluster, die über ein Kennwort mit bestimmten Sonderzeichen verbunden sind.

    In der vorherigen Version schlug die Compliance-Generierung fehl, wenn ein Server oder Cluster über ein Kennwort verbunden war, das Sonderzeichen wie z. B. doppelte Anführungszeichen ("), Accent grave (`) und Semikolon (;) enthält.
- Zurücksetzen des Parameters `CauClusterRole`, um die Selbstaktualisierungsfunktion des angegebenen Clusters zu ermöglichen, nachdem das Cluster-Aware-Update (CAU) abgeschlossen wurde.

Version 1.1.0

- Zusätzliche Unterstützung für Dell EMC Online Kataloge:
  - Dell EMC Enterprise Katalog für PowerEdge Server und Cluster, die PowerEdge Server enthalten.
  - Dell EMC Azure Stack HCI Lösungskatalog für Dell EMC Lösungen für Microsoft Azure Stack HCI.
  - Dell EMC MX Lösungskatalog für PowerEdge MX Modular.
- Möglichkeit zum Durchführen von Server-Updates einschließlich selektiver Komponenten-Updates.
- Möglichkeit zur Durchführung von Cluster-Aware-Updates anhand der validierten Baseline (BIOS, Treiber, Firmware und Systemmanagementanwendungen) auf folgenden Systemen:
  - Serverbasiertes PowerEdge Failover-Cluster
  - Dell EMC Lösungen für Microsoft Azure-Stack-HCI

    ANMERKUNG: Für die Cluster-Aware-Updatefunktion muss auf jedem Node in einem Cluster eine Premium-Lizenz installiert werden.
- Um physische Laufwerke zu lokalisieren oder fehlerhafte physische Laufwerke zu identifizieren, besteht die Möglichkeit, die Blinkfunktion für Leuchtdioden (LEDs) der physische Laufwerke zu nutzen oder diese Funktion zu beenden.
- Unterstützung für neuere Plattformen:
  - Plattformen auf Basis von AX-Nodes – Dell EMC Lösungen für Microsoft Azure Stack HCI Nodes: AX-640, AX-6515 und AX-740xd.
  - Plattformen auf Basis von Storage Spaces Direct Ready-Nodes von Dell EMC – Dell EMC Lösungen für Microsoft Azure Stack-HCI: R440, R640, R740xd und R740xd2.
- Unterstützung für Microsoft Windows Admin Center Version 1910,2.
- Möglichkeit zur Überwachung des Funktionszustands und der Bestandsaufnahme von Accelerators (GPU) mit den neuesten iDRAC9-basierten PowerEdge-Servern.
- Verbesserungen der Benutzeroberfläche für die Überwachung und Bestandsaufnahme von Intel persistenten Speicher.
- Verbesserungen bei der Performance der Update-Compliance.
- Korrelation zwischen Storage-Controller und physischen Laufwerken mit den dazugehörigen Laufwerken.
- Möglichkeit zum Aktualisieren der Funktionszustands-, Bestandsaufnahme-und iDRAC Informationen der verwalteten Ziel-Nodes, um sicherzustellen, dass die angezeigte Inventarinformationen die neuesten sind.
- Verbesserung der Nutzbarkeit durch Herunterladen von DSU und IC, die für das Update der Komponenten automatisch erforderlich sind.
- Möglichkeit zum Herunterladen von Katalog-, DSU- und IC-Dienstprogrammen über das Internet mithilfe der Proxy-Einstellungen, um den Compliance-Bericht zu erzeugen.
- Dell EMC Solutions Badge **Azure Stack HCI Certified** für Dell EMC-Lösungen für Microsoft Azure Stack HCI Cluster besteht aus AX-Nodes oder Storage Spaces Direct Ready-Nodes.

Weitere Ressourcen

Tabelle 1. Weitere Ressourcen

Dokument	Beschreibung	Verfügbarkeit
Dell EMC OpenManage Integration mit Microsoft Windows Admin Center – Installationshandbuch	Enthält Informationen zur Installation und Konfiguration von OpenManage Integration mit Microsoft Windows Admin Center.	1. Gehen Sie zu Dell.com/OpenManageManuals. 2. Wählen Sie **OpenManage Integration mit Microsoft Windows Admin Center** aus. 3. Klicken Sie auf **DOKUMENTATION** > **HANDBÜCHER UND DOKUMENTE**, um auf diese Dokumente zuzugreifen.
Dell EMC OpenManage Integration mit Microsoft Windows Admin Center – Versionshinweise	Enthält Informationen zu neuen Funktionen, bekannten Problemen und Workarounds in OpenManage Integration mit Microsoft Windows Admin Center.	
Dell EMC Infrastructure Compliance-Bericht für PowerEdge-Server und Azure Stack HCI Cluster mithilfe von OMIMSWAC	In diesem Whitepaper wird der Prozess zur Generierung eines Aktualisierungs-Compliance-Berichts für PowerEdge-Server, Microsoft Azure Stack HCI Cluster und Hyper-V basierten Failover-Clustern unter Verwendung von OMIMSWAC beschrieben.	
Microsoft Windows Admin Center – Dokumentation	Darin finden Sie weitere Informationen zur Verwendung von Microsoft Windows Admin Center.	https://www.microsoft.com/en-us/cloud-platform/windows-admin-center

2

Erste Schritte mit OpenManage Integration mit Microsoft Windows Admin Center

Bevor Sie Dell EMC OpenManage Integration-Erweiterung in Windows Admin Center unter Verwendung des NuGet-Feeds starten, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Sie sind bei Windows Admin Center als Gateway-Administrator angemeldet.

Nachdem Sie OpenManage Integration mit Microsoft Windows Admin Center (OMIMSWAC) installiert haben, führen Sie die folgenden Schritte aus, um die Erweiterung zu starten:

1. Wählen Sie in der linken oberen Ecke von Windows Admin Center:
   - Für die Version 1910.2 GA, Version 2007 GA oder 2009 GA von Windows Admin Center: **Server-Manager** oder **Cluster-Manager** aus dem Drop-Down-Menü.
2. Wählen Sie in der Liste eine Server- oder Clusterverbindung aus und klicken Sie dann auf **Verbinden**.
3. Geben Sie die Anmeldeinformationen für den Server oder das Cluster ein.

   ANMERKUNG: Wenn Sie nicht zur Eingabe der Anmeldeinformationen aufgefordert werden, stellen Sie sicher, dass Sie die Option „Verwalten als“ auswählen und entsprechende Server-Administrator- oder Cluster-Administratorkonten eingeben.

   ANMERKUNG: OMIMSWAC unterstützt keine Single-Sign-On- und Smartcard-Authentifizierungsmethoden.
4. Klicken Sie im linken Bereich des Microsoft Windows Admin Center unter **ERWEITERUNGEN** auf **Dell EMC OpenManage Integration**.

Wenn Sie OpenManage Integration zum ersten Mal starten, wird ein Kundenhinweis angezeigt, um die Vorgänge anzugeben, die von OpenManage Integration durchgeführt werden, wie z. B. das Aktivieren der USB-NIC und das Erstellen eines iDRAC-Benutzers auf dem Ziel-Node. Klicken Sie auf **Akzeptieren**, um die PowerEdge-Server weiterhin mithilfe von OpenManage Integration zu verwalten.

ANMERKUNG: Nachdem die Informationen aus den verwalteten Nodes gesammelt wurden, wird der zuvor erstellte iDRAC-Nutzer von OMIMSWAC gelöscht.

Um die ordnungsgemäße Funktionsweise von OpenManage Integration mit Microsoft Windows Admin Center zu gewährleisten, stellen Sie Folgendes sicher:

- Die Firewall in Ihrer Unternehmensumgebung ermöglicht die Kommunikation über KMU-Port 445.
- Redfish-Service ist auf dem Ziel-Node aktiviert.
- Auf dem Ziel-Node ist ein iDRAC-Benutzersteckplatz verfügbar.
- Stellen Sie sicher, dass der Ziel-Node nicht zum Lifecycle Controller gestartet wird.
- Der Ziel-Node befindet sich nicht im Neustartstatus oder ist ausgeschaltet.
- Der USB-NIC-Adapter ist auf dem Ziel-Node-Betriebssystem nicht deaktiviert.
- Der Sperrmodus ist auf dem Ziel-Node deaktiviert.
- Die PowerShell-Ausführungsrichtlinie ist auf dem System mit installiertem Windows Admin Center und auf dem Ziel-Node-Betriebssystem auf RemoteSigned festgelegt. Weitere Informationen finden Sie unter https://www.dell.com/support/article/sln318718/dell-emc-openmanage-integration-with-microsoft-windows-admin-center-omimswac-fails-to-query-host-information.

ANMERKUNG: Für die Verwaltung von PowerEdge-Servern verwendet OMIMSWAC ein internes Betriebssystem zur iDRAC Passthrough-Schnittstelle. Standardmäßig kann auf iDRAC über die IP-Adresse 169.254.0.1/<Subnetz> oder 169.254.1.1/<Subnetz> zugegriffen werden. Wenn der Host jedoch eine andere Netzwerkschnittstelle im selben Subnetz hat (z. B. wenn ein Tool wie VMFleet installiert ist), ist OMIMSWAC möglicherweise nicht in der Lage, über das Hostbetriebssystem mit der iDRAC zu kommunizieren. Melden Sie sich zur Behebung des Konflikts bei iDRAC an, und ändern Sie die USB-NIC-IP-Adresse unter dem Abschnitt „BS-zu-iDRAC-Passthrough“. Weitere Informationen über die Zuweisung dieser IP-Adresse finden Sie in der iDRAC-Dokumentation auf der Dell EMC Support-Website.

Informationen zum Verwalten von:

- PowerEdge-Servern finden Sie unter Dell EMC PowerEdge-Server verwalten auf Seite 10.
- Mit PowerEdge-Servern erstellte Microsoft Failover-Cluster oder mit Dell EMC Storage Spaces Direct Ready Nodes erstellte Azure Stack HCI finden Sie unter Verwalten von Failover-Clustern und Azure Stack HCI auf Seite 13.

3

Für Dell EMC OpenManage Integration mit Microsoft Windows Admin Center erforderliche Ports

Tabelle 2. Für Dell EMC OpenManage Integration mit Microsoft Windows Admin Center erforderliche Ports

Funktionen von OpenManage Integration mit Windows Admin Center	System mit installiertem Windows Admin Center	Ziel-Node/Cluster-Node	System, auf dem der DRM-Katalog verfügbar ist	System, auf dem die DSU- und IC-Dienstprogramme verfügbar sind	iDRAC des Ziel-Node/ Cluster-Node
Installation	-	-	-	-	-
Deinstallation	-	-	-	-	-
Integrität, Hardware und iDRAC-Bestandsaufnahme	445 – ausgehend	445 – eingehend	-	-	443 (Standardport)
Einstellungen der Aktualisierungstools – Verbindung testen	445 – ausgehend	-	-	445 – eingehend	-
Updatecompliance	-	445 – eingehend	445 – ausgehend	445 – ausgehend	-
Benachrichtigungen zur Updatecompliance	445 – ausgehend	-	445 – eingehend	-	-
Ziel-Node-Update und Cluster-Aware-Update	-	Von Microsoft bereitgestellte Standard-WinRM-Ports	445 – ausgehend	445 – ausgehend	443 (Standardport)

Weitere Informationen zum KMU-Port 445 finden Sie unter https://go.microsoft.com/fwlink/?linkid=2101556.

Weitere Informationen über WinRM-Ports finden Sie unter https://docs.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management.

4

Dell EMC PowerEdge-Server verwalten

Voraussetzungen:

- Sie müssen bei Microsoft Windows Admin Center als Gateway-Administrator angemeldet sein.
- Sie müssen die Dell EMC OpenManage Integration mit Microsoft Windows Admin Center-Erweiterung (OMIMSWAC) installiert haben. Weitere Informationen über das Installationsverfahren finden Sie im *Dell EMC OpenManage Integration mit Microsoft Windows Admin Center-Installationshandbuch unter Dell.com/OpenManageManuals*.
- Serververbindungen werden in Microsoft Windows Admin Center hinzugefügt. Weitere Informationen über das Hinzufügen von Serververbindungen finden Sie unter https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center.

So verwalten Sie PowerEdge-Server:

1. Wählen Sie in der oberen linken Ecke von Windows Admin Center **Server-Manager** aus dem Dropdown-Menü aus.
2. Wählen Sie in der Liste eine Serververbindung aus und klicken Sie dann auf **Verbinden**.

   ANMERKUNG: Wenn Sie beim Hinzufügen der Verbindung keine Serveranmeldeinformationen eingegeben haben, müssen Sie die Anmeldedaten eingeben, wenn Sie eine Verbindung zum Server herstellen, indem Sie die Option „Verwalten als“ auswählen.

3. Klicken Sie im linken Bereich des Microsoft Windows Admin Center unter **ERWEITERUNGEN** auf **Dell EMC OpenManage Integration**.
4. Wählen Sie:
   - **Integrität**: zum Anzeigen des Integritätsstatus der Ziel-Node-Komponenten. Ein Statussymbol zeigt den Gesamt-Integritätsstatus des Ziel-Nodes an. Informationen dazu finden Sie unter Integritätsstatus – unterstützte Ziel-Node-Komponenten auf Seite 11.
   - **Bestandsaufnahme**: zum Anzeigen detaillierter Hardware-Bestandsaufnahme-Informationen der Ziel-Node-Komponenten. Informationen dazu finden Sie unter Hardwarebestand – Unterstützte Ziel-Node-Komponenten auf Seite 11.
   - **Update**: zum Anzeigen des Compliance-Berichts und Aktualisieren der Komponenten auf die Baseline-Version. Informationen dazu finden Sie unter PowerEdge-Server und -Nodes von HCI- und Failover-Clustern aktualisieren auf Seite 17.
   - **iDRAC**: zum Anzeigen der iDRAC-Details der Ziel-Nodes. Sie können die iDRAC-Konsole direkt über Windows Admin Center starten, indem Sie die OpenManage-Integration verwenden. Informationen dazu finden Sie unter iDRAC-Details der PowerEdge-Server und Nodes von HCI und Failover-Clustern anzeigen auf Seite 16.

ANMERKUNG: Integrität, Hardware-Bestandsaufnahme und iDRAC-Details werden zwischengespeichert und werden nicht jedes Mal geladen, wenn die Erweiterung geladen wird. Klicken Sie zum Anzeigen des aktuellen Integritäts- und Bestandsaufnahmestatus sowie der iDRAC-Details in der oberen rechten Ecke des Integritätsstatus auf **Aktualisieren**.

ANMERKUNG: Für modulare Server (YX2X, YX3X, YX4X, YX5X und höhere Modelle von PowerEdge-Servern) werden die folgenden Informationen in Verbindung mit Lüftern und Netzteilen nicht angezeigt:

- Funktionsstatus
- Attributwerte in der Tabelle „Hardware-Bestandsaufnahme“

ANMERKUNG: Für YX2X- und YX3X-Modelle des PowerEdge-Servers mit Firmware-Version vor 2.60.60.60 werden Informationen zu den folgenden Komponenten nicht angezeigt:

- Integritätsstatus: Beschleuniger, Arbeitsspeicher, Speicher-Controller, Speichergehäuse und physische Laufwerke.
- Hardware-Bestandsaufnahme: Beschleuniger, Arbeitsspeicher, Speicher-Controller, Speichergehäuse, physische Laufwerke, Netzwerkgeräte und Firmware.

Themen:

Integritätsstatus – unterstützte Ziel-Node-Komponenten

Der Integritätsstatus der folgenden Serverkomponenten wird angezeigt:

- CPUs
- Accelerator
- Speicher
- Speicher-Controller
- Speichergehäuse
- Physische Laufwerke
- iDRAC
- Netzteile
- Lüfter
- Spannungen
- Temperaturen

ANMERKUNG: Informationen zum Integritätsstatus sind für Beschleuniger in PowerEdge-Servermodellen YX4X und höher mit iDRAC-Version 4.00.00.00 oder höher verfügbar.

ANMERKUNG: Intel **DIMM**-Speicher wird mit einem Symbol als **IntelPersistent** identifiziert.

Die Funktionsstatus werden mit einem Ringdiagramm dargestellt. Sie können verschiedene Abschnitte im Ringdiagramm auswählen, um den Funktionsstatus der Komponenten zu filtern. Wenn Sie z. B. den roten Abschnitt auswählen, werden nur Komponenten mit kritischem Funktionsstatus angezeigt.

Um den aktuellen Integritätsstatus anzuzeigen, klicken Sie in der oberen rechten Ecke der Registerkarte **Integrität** auf **Aktualisieren**.

ANMERKUNG: Bei Software-Speicher-Controllern und physikalischen Laufwerke, die mit dem integrierten SATA Controller verbunden sind, wird der Status der Bestandsaufnahme als „Unbekannt“ angezeigt.

Hardwarebestand – Unterstützte Ziel-Node-Komponenten

Die Hardware-Bestandsliste der folgenden Ziel-Node-Komponenten wird angezeigt:

- System
- Firmware
- CPUs
- Accelerator
- Speicher
- Speicher-Controller

  Klicken Sie zum Anzeigen des physischen Laufwerks in einem Speicher-Controller unter **Zugehörige Laufwerke** auf den Link **Laufwerke anzeigen**. Die physischen Laufwerke werden auf der Registerkarte **Physische Laufwerke** aufgeführt.

- Speichergehäuse
- Netzwerkgerät
- Physische Laufwerke

  Um die zusätzlichen Eigenschaften eines Laufwerks anzuzeigen, wählen Sie das Laufwerk aus und klicken Sie dann auf **Erweiterte Eigenschaften**. Um den zugehörigen Speicher-Controller anzuzeigen, klicken Sie auf den Speicher-Controller-Link unter **Erweiterte Eigenschaften**. Der zugehörige Speicher-Controller wird auf der Registerkarte **Speicher-Controller** angezeigt. Wenn physische Laufwerke an die CPU angeschlossen sind, ist der Speicher-Controller-Link unter **Erweiterte Eigenschaften** nicht verfügbar.

  Blinken und Blinken beenden (physische Laufwerke)

  Wählen Sie ein physisches Laufwerke aus und klicken Sie auf **Blinken**, um das Blinken der LEDs auf dem physischen Laufwerk zu aktivieren. Die LEDs stehen für den Zustand der physischen Laufwerke. Das Bilnken der physischen Laufwerke hilft, die fehlerhaften physikalischen Laufwerke in Ihrem Rechenzentrum zu finden und zu identifizieren. Um das Blinken der physischen Laufwerke zu deaktivieren, wählen Sie ein Laufwerk aus und klicken Sie auf **Blinken beenden**.

ANMERKUNG: Die Vorgänge „Blinken“ und „Blinken beenden“ sind nicht verfügbar für:

- Laufwerk, die BOSS-Karten (Boot Optimized Storage Subsystem) zugeordnet sind.
- Geräte mit iDRAC-Firmware-Version vor 3.30.30.30. Aktualisieren Sie die iDRAC-Firmware auf die neueste Version, um „Blinken“ und „Blinken beenden“ zu aktivieren.

ANMERKUNG:

- Wenn der Vorgang „Blinken“ oder „Blinken beenden“ ausgeführt wird, wird die Schaltfläche **Aktualisieren** zum Laden der neuesten Integritätsstatus- und Hardwarebestandsaufnahmedaten deaktiviert. Wenn der Integritätsstatus und die Hardwarebestandsaufnahme in OMIMSWAC geladen werden, sind die Vorgänge „Blinken“ und „Blinken beenden“ ebenfalls deaktiviert.
- Der Vorgang „Blinken“ oder „Blinken beenden“ schlägt auf physischen Laufwerken mit dem Fehler `Blinken/Blinken beenden wird möglicherweise nicht von - <Laufwerkname> unterstützt` fehl, die an einen integrierten SATA-Controller angeschlossen sind.

- Netzteile
- Lüfter

Um die neuesten Hardware-Bestandsinformationen anzuzeigen, klicken Sie in der oberen rechten Ecke der Registerkarte **Bestandsaufnahme** auf **Aktualisieren**.

Informationen zum Anzeigen der iDRAC-Details des Ziel-Node finden Sie unter iDRAC-Details der PowerEdge-Server und Nodes von HCI und Failover-Clustern anzeigen auf Seite 16.

ANMERKUNG: Unter **Bestandsaufnahme** werden die Attributwerte einiger Ziel-Node-Komponenten leer angezeigt, weil der Wert auf dem Ziel-Node möglicherweise nicht verfügbar ist.

ANMERKUNG: Unter Firmware-Bestandsaufnahme werden für einige Netzwerkgeräte mit mehreren Ports nur ein einziger Port mit der Firmware-Version angezeigt, da die jeweils zutreffende Firmwareversion für alle Ports identisch ist.

ANMERKUNG: Informationen über einige Attribute von Speichergehäusen, Firmware-Bestandsaufnahme und Speicherkomponente sind möglicherweise nicht verfügbar für:

- YX2X- und YX3X-Modelle des PowerEdge-Servers.
- YX4X-Modelle des PowerEdge-Servers mit iDRAC-Version unter 3.30.30.30.

ANMERKUNG: Für die PCIe-SSD-Rückwandplatine von Speichergehäusen stehen einige Attributwerte möglicherweise nicht zur Verfügung.

ANMERKUNG: Informationen zum Integritätsstatus sind für Beschleuniger in PowerEdge-Servermodellen YX4X und höher mit iDRAC-Version 4.00.00.00 oder höher verfügbar.

ANMERKUNG: Intel **DIMM**-Speicher wird mit einem Symbol als **IntelPersistent** identifiziert.

5

Verwalten von Failover-Clustern und Azure Stack HCI

Voraussetzungen:

- Sie sind bei Microsoft Windows Admin Center als Gateway-Administrator angemeldet.
- Sie müssen die Dell EMC OpenManage Integration mit Microsoft Windows Admin Center-Erweiterung (OMIMSWAC) installiert haben. Weitere Informationen über das Installationsverfahren finden Sie im *Dell EMC OpenManage Integration mit Microsoft Windows Admin Center-Installationshandbuch unter Dell.com/OpenManageManuals*.
- Sie haben Failover- oder hyperkonvergente Clusterverbindungen in Microsoft Windows Admin Center hinzugefügt. Weitere Informationen zum Hinzufügen von Failover- oder hyperkonvergenten Clusterverbindungen finden Sie unter https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center.
- Stellen Sie sicher, dass alle Cluster-Nodes über IP-Adresse, Hostname oder FQDN (vollständig qualifizierter Domainname) erreichbar sind, bevor Sie das Cluster mit OMIMSWAC verwalten.

So verwalten Sie die mit PowerEdge-Servern erstellten Microsoft Failover-Cluster und mit Dell EMC Storage Spaces Direct Ready Nodes erstellte Azure-Stack-HCI:

1. Wählen Sie in der linken oberen Ecke von Windows Admin Center:
   - Für Version 1910.2 GA, Version 2007 GA oder Version 2009 GA von Windows Admin Center: **Cluster Manager** vom Dropdown-Menü.
2. Wählen Sie in der Liste eine Failover- oder hyperkonvergente Clusterverbindung aus und klicken Sie dann auf **Verbinden**.
3. Klicken Sie im linken Bereich des Microsoft Windows Admin Center unter **ERWEITERUNGEN** auf **Dell EMC OpenManage Integration**.
4. Um das Failover- oder hyperkonvergente Cluster zu verwalten, wählen Sie Folgendes aus:
   - **Integrität**: zum Anzeigen des Integritätsstatus der Serverkomponenten der einzelnen Nodes im Cluster.
     - Der Abschnitt **Gesamt-Integritätsstatus** zeigt den Gesamt-Integritätsstatus des Clusters an. Wählen Sie verschiedene Abschnitte im Ringdiagramm aus, um den Integritätsstatus der Komponenten der Cluster-Nodes zu filtern.

       ANMERKUNG: Der Gesamt-Integritätsstatus des Clusters wird möglicherweise als „Kritisch“ oder „Warnung“ angezeigt, obwohl die Komponenten der Nodes, die im Windows Admin Center angezeigt werden, fehlerfrei sind. Weitere Informationen zu den Komponenten mit dem Funktionsstatus „Kritisch“ finden Sie in der entsprechenden iDRAC-Konsole.

     Informationen dazu finden Sie unter Integritätsstatus – Unterstützte Ziel-Node-Komponenten in Failover-Clustern und Azure Stack HCI auf Seite 14.
   - **Bestandsaufnahme**: zum Anzeigen detaillierter Hardware-Bestandsaufnahme-Informationen der Komponente. Auf der Seite **Übersicht** werden die grundlegenden Details der Nodes des Failover- oder hyperkonvergenten Clusters aufgelistet. Wählen Sie den erforderlichen Node aus, um die detaillierte Hardware-Bestandsaufnahme der Serverkomponenten anzuzeigen. Informationen dazu finden Sie unter Hardware-Bestandsaufnahme – Unterstützte Ziel-Node-Komponenten in Failover-Clustern und Azure Stack HCI auf Seite 14.
   - **Update**: zum Anzeigen der Compliance-Tabellen der Nodes und Komponenten. Erweitern Sie den erforderlichen Node, um einen detaillierten Compliance-Bericht der Komponenten anzuzeigen. Informationen dazu finden Sie unter PowerEdge-Server und -Nodes von HCI- und Failover-Clustern aktualisieren auf Seite 17.
   - **iDRAC**: zum Anzeigen der iDRAC-Details der einzelnen Nodes. Sie können die iDRAC-Konsole direkt über Windows Admin Center starten, indem Sie die OpenManage-Integration verwenden. Informationen dazu finden Sie unter iDRAC-Details der PowerEdge-Server und Nodes von HCI und Failover-Clustern anzeigen auf Seite 16.

ANMERKUNG: Integrität, Hardware-Bestandsaufnahme und iDRAC-Details werden zwischengespeichert und werden nicht jedes Mal geladen, wenn die Erweiterung geladen wird. Klicken Sie zum Anzeigen des aktuellen Integritäts- und Bestandsaufnahmestatus sowie der iDRAC-Details in der oberen rechten Ecke des Integritätsstatus auf **Aktualisieren**.

Themen:

Integritätsstatus – Unterstützte Ziel-Node-Komponenten in Failover-Clustern und Azure Stack HCI

Wählen Sie auf der Seite **Cluster – Azure Stack HCI** die Registerkarte **Integrität** aus, um den Gesamt-Integritätsstatus des Failover- oder HCI-Clusters und den Integritätsstatus der folgenden Ziel-Node-Komponenten der Nodes im Failover-Cluster oder Azure Stack HCI anzuzeigen. Bei Auswahl von „Kritisch“ oder „Warnung“ im Ringdiagramm „Gesamt-Funktionsstatus“ werden die entsprechenden Nodes und die Komponenten im Status „Kritisch“ oder „Warnung“ angezeigt.

- CPUs
- Accelerator
- Speicher
- Speicher-Controller
- Speichergehäuse
- Physische Laufwerke
- iDRAC
- Netzteile
- Lüfter
- Spannungen
- Temperaturen

ANMERKUNG: Informationen zum Integritätsstatus sind für Beschleuniger in PowerEdge-Servermodellen YX4X und höher mit iDRAC-Version 4.00.00.00 oder höher verfügbar.

ANMERKUNG: Intel **DIMM**-Speicher wird mit einem Symbol als **IntelPersistent** identifiziert.

Die Funktionsstatus werden mit einem Ringdiagramm dargestellt. Sie können verschiedene Abschnitte im Ringdiagramm auswählen, um den Funktionsstatus der Komponenten zu filtern. Wenn Sie z. B. den roten Abschnitt auswählen, werden nur Komponenten mit kritischem Funktionsstatus angezeigt.

Wenn in einem Failover- oder HCI-Cluster die verschiedenen Abschnitte des Ringdiagramms für einzelne Komponenten ausgewählt sind, werden die entsprechenden Nodes mit dem Integritätsstatus der Komponente aufgeführt. Blenden Sie die Nodes ein, um die Komponenten mit einem bestimmten Funktionsstatus anzuzeigen.

Um den aktuellen Integritätsstatus anzuzeigen, klicken Sie in der oberen rechten Ecke der Registerkarte **Integrität** auf **Aktualisieren**.

ANMERKUNG: Bei Software-Speicher-Controllern und physikalischen Laufwerken, die mit dem integrierten SATA Controller verbunden sind, wird der Status der Bestandsaufnahme immer als „Unbekannt“ angezeigt.

Hardware-Bestandsaufnahme – Unterstützte Ziel-Node-Komponenten in Failover-Clustern und Azure Stack HCI

Die Hardware-Bestandsaufnahme der folgenden Ziel-Node-Komponenten der Nodes in Failover-Clustern oder Azure Stack HCI wird angezeigt:

- System
- Firmware
- CPUs
- Accelerator
- Speicher
- Speicher-Controller

  Klicken Sie zum Anzeigen der physischen Laufwerke in einem Speicher-Controller unter **Zugehörige Laufwerke** auf den Link **Laufwerke anzeigen**. Die physischen Laufwerke werden auf der Registerkarte **Physische Laufwerke** aufgeführt.

  Speichergehäuse
- Netzwerkgerät
- Physische Laufwerke

Um die zusätzlichen Eigenschaften eines Laufwerks anzuzeigen, wählen Sie das Laufwerk aus und klicken Sie dann auf **Erweiterte Eigenschaften**. Um den zugehörigen Speicher-Controller anzuzeigen, klicken Sie auf den Speicher-Controller-Link unter **Erweiterte Eigenschaften**. Der zugehörige Speicher-Controller wird auf der Registerkarte **Speicher-Controller** angezeigt. Wenn physische Laufwerke an die CPU angeschlossen sind, ist der Speicher-Controller-Link unter **Erweiterte Eigenschaften** nicht verfügbar.

Blinken und Blinken beenden (physische Laufwerke)

Wählen Sie einen Node und anschließend ein physisches Laufwerk aus und klicken Sie auf **Blinken**, um das Blinken der LEDs auf dem physischen Laufwerk zu aktivieren. Die LEDs stehen für den Zustand der physischen Laufwerke. Das Bilnken der physischen Laufwerke hilft, die fehlerhaften physikalischen Laufwerke in Ihrem Rechenzentrum zu finden und zu identifizieren. Um das Blinken der physischen Laufwerke zu deaktivieren, wählen Sie ein Laufwerk aus und klicken Sie auf **Blinken beenden**. In einem Cluster muss der Vorgang „Blinken“ oder „Blinken beenden“ eines ausgewählten Nodes abgeschlossen werden, bevor Sie den Vorgang „Blinken“ oder „Blinken beenden“ auf einem anderen Node durchführen.

ANMERKUNG: Die Vorgänge „Blinken“ und „Blinken beenden“ sind nicht verfügbar für:

- Laufwerke, die BOSS-Karten (Boot Optimized Storage Subsystem) zugeordnet sind.
- Geräte mit iDRAC-Firmware-Version vor 3.30.30.30. Aktualisieren Sie die iDRAC-Firmware auf die neueste Version, um „Blinken“ und „Blinken beenden“ zu aktivieren.
  - Wenn die Vorgänge „Blinken“ und „Blinken beenden“ für ausgewählte unterstützte Laufwerke trotz vorhandener iDRAC-Firmware-Version 3.30.30.30 und höher nicht verfügbar ist, führen Sie ein Upgrade der iDRAC-Firmware auf die neueste Version durch, um „Blinken“ und „Blinken beenden“ zu aktivieren.

ANMERKUNG:

- Wenn der Vorgang „Blinken“ oder „Blinken beenden“ ausgeführt wird, wird die Schaltfläche **Aktualisieren** zum Laden der neuesten Integritätsstatus- und Hardwarebestandsaufnahmedaten deaktiviert. Wenn der Integritätsstatus und die Hardwarebestandsaufnahme in OMIMSWAC geladen werden, sind die Vorgänge „Blinken“ und „Blinken beenden“ ebenfalls deaktiviert.
- Der Vorgang „Blinken“ oder „Blinken beenden“ schlägt auf physischen Laufwerken mit dem Fehler `Blinken/Blinken beenden wird möglicherweise nicht von - <Laufwerkname> unterstützt` fehl, die an einen integrierten SATA-Controller angeschlossen sind.

- Netzteile
- Lüfter

Um die neuesten Hardware-Bestandsinformationen anzuzeigen, klicken Sie in der oberen rechten Ecke der Registerkarte **Bestandsaufnahme** auf **Aktualisieren**.

Informationen zum Anzeigen der iDRAC-Details des Ziel-Node finden Sie unter iDRAC-Details der PowerEdge-Server und Nodes von HCI und Failover-Clustern anzeigen auf Seite 16.

ANMERKUNG: Unter **Bestandsaufnahme** werden die Attributwerte einiger Ziel-Node-Komponenten leer angezeigt, weil der Wert auf dem Ziel-Node möglicherweise nicht verfügbar ist.

ANMERKUNG: Unter Firmware-Bestandsaufnahme werden für einige Netzwerkgeräte mit mehreren Ports nur ein einziger Port mit der Firmware-Version angezeigt, da die jeweils zutreffende Firmwareversion für alle Ports identisch ist.

ANMERKUNG: Informationen über einige Attribute von Speichergehäusen, Firmware-Bestandsaufnahme und Speicherkomponente sind möglicherweise nicht verfügbar für:

- YX2X- und YX3X-Modelle des PowerEdge-Servers.
- YX4X-Modelle des PowerEdge-Servers mit iDRAC-Version unter 3.30.30.30.

ANMERKUNG: Für die PCIe-SSD-Rückwandplatine von Speichergehäusen stehen einige Attributwerte möglicherweise nicht zur Verfügung.

ANMERKUNG: Informationen zum Integritätsstatus sind für Beschleuniger in PowerEdge-Servermodellen YX4X und höher mit iDRAC-Version 4.00.00.00 oder höher verfügbar.

ANMERKUNG: Intel **DIMM**-Speicher wird mit einem Symbol als **IntelPersistent** identifiziert.

6

iDRAC-Details der PowerEdge-Server und Nodes von HCI und Failover-Clustern anzeigen

Um die folgenden iDRAC-Details zum Ziel-Node anzuzeigen, wählen Sie in der linken oberen Ecke von Microsoft Windows Admin Center **Server-Manager** oder **Cluster-Manager** aus und wählen Sie dann einen Server oder eine Clusterverbindung aus der Liste aus. Klicken Sie im linken Bereich unter „ERWEITERUNGEN“ auf **Dell EMC OpenManage Integration** und navigieren Sie zur Registerkarte **iDRAC**.

ANMERKUNG: Blenden Sie für Failover- und hyperkonvergente Cluster die Nodes ein, um die folgenden Details anzuzeigen.

- iDRAC-IP-Adresse. Sie können die iDRAC-Konsole direkt über Microsoft Windows Admin Center starten.
- IPMI-Version.
- iDRAC-Firmware-Version.

7

PowerEdge-Server und -Nodes von HCI- und Failover-Clustern aktualisieren

OpenManage-Integration in Microsoft Windows Admin Center (OMIMSWAC) ermöglicht es Ihnen, Compliance-Details zu erzeugen und Komponenten zu aktualisieren, z. B. BIOS, Treiber, Firmware und/oder Systemmanagementanwendungen von Ziel-Nodes und-Nodes in HCI- und Failover-Clustern. Sie können entweder einen Online- oder Offline-Katalog verwenden, um Compliance-Details zu generieren und Komponenten zu aktualisieren.

Klicken Sie in OMIMSWAC auf **Update**. Das Update-Fenster wird angezeigt.

Auf dieser Seite können Sie einen Compliance-Bericht generieren und die Komponenten wie folgt aktualisieren:

1. Compliance-Bericht erstellen: Wählen Sie den Updatequellen-Katalog (Online oder Offline-Katalog) aus, um die Aktualisierungsdetails für jedes Gerät abzurufen und einen Compliance-Bericht zu erstellen.
2. Überprüfen Sie den Compliance-Bericht und bestätigen Sie die Komponentenauswahl: Überprüfen Sie den generierten Compliance-Bericht. Standardmäßig sind alle nicht konformen Komponenten (außer zurückstufbarer Komponenten) ausgewählt. Aktivieren oder deaktivieren Sie die Komponenten, die Sie aktualisieren möchten, und bestätigen Sie die Auswahl der Komponenten.
3. Update: Aktualisieren Sie den Ziel-Node oder das Cluster.

Informationen zum Erstellen eines Compliance Berichts und zum Aktualisieren eines Ziel-Nodes finden Sie unter Aktualisiere von Ziel-Nodes. Informationen zum Erstellen von Compliance-Berichten und Aktualisieren von Nodes von HCI- und Failover-Clustern finden Sie unter Aktualisieren von Nodes von HCI- und Failover-Clustern.

OpenManage Integration verwendet Online- oder Offline-Kataloge zur Erstellung von Baselines. Der Katalog enthält die neuesten BIOS-, Treiber-, Firmware- und/oder Systemmanagementanwendungs-Versionen. Die Systemmanagementanwendung kann IC, Treiberpaket, iSM, OMSA usw. enthalten. OpenManage Integration verwendet außerdem die Tools Dell EMC System Update Utility (DSU) und Dell EMC Inventory Collector (IC), um die Update-Details für jedes Gerät abzurufen. Die Tools DSU und IC helfen bei der Erstellung von Compliance-Berichten und der Aktualisierung der nicht konformen Geräte.

Wenn Offline- oder Online-Katalog ausgewählt ist, erfasst OMIMSWAC die in **Einstellungen** > **Update-Tools** konfigurierten Tools DSU und IC. Informationen zum Konfigurieren der Update-Tools finden Sie unter Einstellungen der Update-Compliance-Tools konfigurieren. Wenn die Tools DSU und IC nicht in den Einstellungen konfiguriert sind, werden Sie von OMIMSWAC mit Internetzugang von `www.downloads.dell.com` heruntergeladen.

Im Abschnitt **Benachrichtigungen** des Windows Admin Center werden Sie benachrichtigt, wenn eine neue Online- oder Offline-Katalog-Datei verfügbar ist. Um den neuesten Compliance-Bericht zu erstellen, führen Sie auf der Registerkarte **Update** den Update-Compliance-Bericht aus.

ANMERKUNG: Die CAU-Funktion (Cluster-Aware-Update) wird für die folgenden Plattformen mit gültiger Lizenz unterstützt:

- YX4X-Modelle der Dell EMC PowerEdge-Server (und höher) mit iDRAC Firmware 4.00.00.00 oder höher.
- Dell EMC Lösungen für Microsoft Azure Stack HCI mit iDRAC Firmware 4.00.00.00 oder höher.

Weitere Informationen zu Lizenzen finden Sie unter *Lizenzierung für OpenManage Integration in Windows Admin Center* im OMIMSWAC-Installationshandbuch.

Themen:

Einstellungen der Updatecompliance-Tools konfigurieren

Um den neuesten Update-Compliance-Bericht und Gerätekomponenten-Details zu generieren, müssen Sie bei OpenManage Integration ohne Internetzugang die Einstellungen für die Update-Compliance-Tools konfigurieren. Die unterstützten Versionen der Dienstprogramme Dell System Update (DSU) und Dell Inventory Collector (IC) für OpenManage Integration Version 1.1.1 sind:

- DSU-Version: 1.8.1. Sie können DSU unter https://downloads.dell.com/OMIMSWAC/DSU/ herunterladen.
- IC-Version: Laden Sie den IC unter https://downloads.dell.com/OMIMSWAC/IC/ herunter.

Die folgende Konfiguration ist erforderlich, wenn OMIMSWAC nicht mit dem Internet verbunden ist und Sie den Dell EMC Repository Manager (DRM)-Katalog offline verwenden, um den Compliance-Bericht zu erzeugen und die Komponenten zu aktualisieren.

1. Geben Sie auf der Registerkarte **Einstellungen** den Freigabe-Speicherort ein, an dem das DSU-Dienstprogramm abgelegt wurde.

   DSU wird verwendet, um die Dell Update Packages für Ziel-Nodes bereitzustellen.
2. Geben Sie den Freigabe-Speicherort ein, an dem das IC-Dienstprogramm abgelegt wurde.

   Das IC-Dienstprogramm wird verwendet, um die Hardware-Bestandsaufnahmedaten von Ziel-Nodes zu erfassen.
3. Geben Sie die Nutzeranmeldedaten ein, um auf den Freigabe-Speicherort zuzugreifen.

   ANMERKUNG: Bei der Deinstallation von OMIMSWAC werden die auf der Seite „Einstellungen“ vorhandenen Daten nicht gelöscht. Wenn OMIMSWAC später neu installiert wird, sind die zuvor konfigurierten Daten auf der Seite „Einstellungen“ weiterhin verfügbar. Das Kennwort ist jedoch nicht mehr verfügbar.
4. Um zu überprüfen, ob die Dienstprogramme verfügbar sind, klicken Sie auf **Verbindung testen**.
5. Klicken Sie auf **Speichern**, um die Einstellung des Aktualisierungstools zu speichern.

   Die Kennwörter für die Aktualisierungstool-Einstellungen werden nur für die aktuelle Browsersitzung aufbewahrt. Geben Sie das Kennwort nach dem Öffnen einer neuen Browsersitzung erneut ein, damit die Update-Compliance-Funktion von OpenManage Integration mit Microsoft Windows Admin Center ordnungsgemäß funktioniert.

   Informationen zum Erzeugen des neuesten Update-Compliance-Berichts finden Sie unter Generieren von Compliance-Berichten – Ziel-Node und Generieren von Compliance-Berichten – Ziel-Node-Komponenten in Failover-Clustern und Azure-Stack-HCI.

Proxy-Einstellungen konfigurieren

OMIMSWAC bietet eine Option zum Herunterladen von Katalog-, DSU- und IC-Dienstprogrammen über das Internet mithilfe der Proxy-Einstellungen, um den Compliance-Bericht zu erzeugen. Allerdings unterstützt OMIMSWAC, das mit dem Internet über einen Proxy verbunden ist, das Aktualisieren von Ziel-Nodes oder Clustern über Online-Kataloge nicht. In diesem Fall werden Compliance und Aktualisierungen, die den Offlinekatalog verwenden, unterstützt.

Sie können die Proxy-Einstellungen so konfigurieren, dass Sie eine Verbindung zu einem Proxyserver herstellen, der als Vermittler zwischen Ihrem Gateway-System und dem Internet fungiert. Wenn die Einstellungen für das OMIMSWAC-Aktualisierungs-Compliance-Tool nicht konfiguriert sind und das Gateway-System nicht mit dem Internet verbunden ist, wird die Internetverbindung über die Proxy-Einstellungen geprüft.

So stellen Sie eine Verbindung zu einem Proxyserver her:

1. Geben Sie die IP-Adresse des Proxyservers in folgendem Format ein:

   `https://<IP-Adresse>` oder **`http://<IP-Adresse>`**
2. Geben Sie die Portnummer des Proxyservers im folgenden Format ein und klicken Sie auf **Speichern**.

   `<Portnummer> (HTTPS)` oder **`<Portnummer> (http)`**

   Beispiel: 443 (HTTPS) oder 80 (http)

   Informationen zum Erzeugen des neuesten Update-Compliance-Berichts finden Sie unter Generieren von Compliance-Berichten – Ziel-Node und Generieren von Compliance-Berichten – Ziel-Node-Komponenten in Failover-Clustern und Azure-Stack-HCI.

Aktualisieren von Ziel-Nodes

Mithilfe von OpenManage Integration in Windows Admin Center können Sie den Compliance-Bericht (BIOS, Treiber, Firmware und/oder Systemmanagementanwendung) anzeigen und die Komponenten der Ziel-Nodes aktualisieren.

Compliance- und Update-Voraussetzungen

Bevor Sie einen Compliance-Bericht generieren und Komponenten aktualisieren, stellen Sie Folgendes sicher:

- Die in der *Kompatibilitätsmatrix* des Installationshandbuchs aufgelisteten Software- und Hardwareanforderungen sind erfüllt.
- Um einen Ziel-Node zu verwalten, stellen Sie eine Verbindung mit dem Ziel-Node über die Option **Verwalten als** her und geben Sie die entsprechenden Anmeldeinformationen des Ziel-Node-Administrators ein. Stellen Sie außerdem sicher, dass der Benutzer Teil der lokalen Nutzergruppe von Gateway-Administratoren ist. Weitere Informationen zur Auswahl von „Verwalten als“ finden Sie im Abschnitt „Erste Schritte mit Windows Admin Center“ in der Microsoft Dokumentation.

- Achten Sie auf den Workload, bevor Sie den Ziel-Node aktualisieren.
- Stellen Sie sicher, dass die Bestandsinformationen für den Ziel-Node abgerufen wurden.
- Stellen Sie sicher, dass der iDRAC-Sperrmodus deaktiviert ist. Informationen zum Deaktivieren des iDRAC-Systemsperrmodus finden Sie in den iDRAC-Dokumenten.
- Für SAS-RAID_Driver stellen Sie Folgendes sicher:
  - Setzen Sie den SATA-Controller auf RAID-Modus.
  - Setzen Sie die NVMe PCIe SSDs auf RAID-Modus.

  Weitere Informationen zur Einstellung des RAID-Modus finden Sie im Anhang
- Stellen Sie sicher, dass der WAC nicht auf dem Zielknoten installiert ist, den Sie aktualisieren möchten.
- Stellen Sie sicher, dass der Ziel-Node über IP-Adresse, Hostname und den FQDN (Fully Qualified Domain Name) des Ziel-Node erreichbar ist.

  ANMERKUNG: Wenn der Ziel-Node nicht erreichbar ist und das Ziel-Node-Update durchgeführt wird, wird der Updatestatus möglicherweise als fehlgeschlagen angezeigt. Wenn Sie in diesem Fall den Ziel-Node unmittelbar nach dem Update neu starten und die Compliance erneut ausführen, wird der Status der Ziel-Node-Komponenten möglicherweise als konform angezeigt, während der Gesamtstatus des Ziel-Node-Updates möglicherweise weiterhin fehlgeschlagen ist.

ANMERKUNG: Das Aktualisieren eines Ziel-Node, auf dem WAC installiert ist, wird nicht empfohlen. Um dieses Szenario zu unterstützen, installieren Sie den WAC auf einem anderen (nicht WAC-bezogenen) Ziel-Node und schließen Sie das Update ab.

ANMERKUNG: Während die Compliance oder das Update im Gange ist, ist es nicht zulässig, weitere Compliance- oder Update-Aufgaben für denselben Ziel-Node auszuführen, der die Update-Anforderungen von den MS WAC-Update-Tools enthält.

Schritt 1: Erstellen eines Compliance Berichts – Ziel-Node-Komponenten

Um einen Compliance-Bericht für einen Ziel-Node zu erzeugen, wählen Sie **Update > Updatequelle** aus und wählen Sie eine der verfügbaren Offline- oder Online-Katalog-Optionen wie folgt aus:

Erzeugen eines Compliance-Berichts mithilfe des Online-Katalogs

Zur Verwendung des Online-Katalogs muss OMIMSWAC mit oder ohne Proxy-Einstellungen mit dem Internet verbunden sein. OMIMSWAC mit Internetzugang ermöglicht es Ihnen, die Online-Katalog-Option in der Drop-down-Liste **Updatequelle** zu verwenden, um den Katalog automatisch herunterzuladen.

Um die Update-Compliance-Details anzuzeigen, müssen Sie die folgenden Aktionen ausführen:

1. Wählen Sie unter **Update > Updatequelle** eine der verfügbaren Online-Katalogoptionen aus.

   Die entsprechenden Online-Kataloge werden standardmäßig abhängig vom Ziel-Node ausgewählt.

   Die verfügbaren Online-Kataloge variieren je nach Ziel-Node/Cluster, mit dem Sie verbunden sind, wie folgt:
   - Für PowerEdge-Server und Cluster mit PowerEdge-Server: Dell EMC Enterprise-Katalog, der die validierten Versionen von Komponenten für PowerEdge-Server enthält.
   - MX-Server: Dell EMC MX-Lösungskatalog, der die validierten Versionen von Komponenten für PowerEdge MX Modular enthält.
   - Azure-Stack-HCI-Cluster-Nodes: Dell EMC Azure-Stack-HCI-Lösungskatalog, der die validierten Versionen von Komponenten für AX-Nodes und Storage Spaces Direct Ready-Nodes enthält.

   Weitere Informationen über verfügbare Kataloge finden Sie im Anhang.

2. Klicken Sie auf **Weiter: Compliance-Details:**, um den Compliance-Bericht zu erzeugen.

OMIMSWAC lädt den Katalog herunter, erfasst die in der Registerkarte **Einstellungen** konfigurierten DSU- und IC-Tools und erzeugt einen Compliance-Bericht. Wenn die Tools DSU und IC nicht in den **Einstellungen** konfiguriert werden, lädt OMIMSWAC sie von `www.downloads.dell.com` herunter, um den Compliance-Bericht zu erzeugen.

Die Compliance-Details werden berechnet und der Bericht steht unter **Update-Compliance** > **Compliance-Details** zur Verfügung. Weitere Informationen über den Compliance-Bericht finden Sie unter Compliance-Bericht anzeigen.

Erzeugen eines Compliance-Berichts mithilfe des Offline-Katalogs

OMIMSWAC mit oder ohne Internetzugang ermöglicht Ihnen die Auswahl des Dell EMC Repository Manager-Offline-Katalogs, um den Compliance-Bericht zu generieren.

Bevor Sie den neuesten Compliance-Bericht von Ziel-Node-Komponenten erstellen, stellen Sie Folgendes sicher: Die folgenden Voraussetzungen sind erforderlich, wenn der OMIMSWAC nicht mit dem Internet verbunden ist und der Dell EMC Repository Manager (DRM)-Offline-Katalog verwendet wird, um einen Compliance-Bericht zu generieren und Komponenten zu aktualisieren.

- Konfigurieren Sie die Informationen zum Freigabe-Speicherort, an denen die Anwendungen DSU und IC platziert werden. Siehe Einstellungen der Update-Compliance-Tools konfigurieren.
- Erzeugen Sie die neuesten Katalogdateien mithilfe der Anwendung Dell EMC Repository Manager (DRM). Die unterstützte Version des DRM kann unter Dell EMC Repository Manager heruntergeladen werden.

Um die Update-Compliance-Details anzuzeigen, müssen Sie die folgenden Aktionen ausführen:

1. Wählen Sie unter **Update** > **Updatequelle** in der Drop-down-Liste **Offline – Dell EMC Repository Manager-Katalog** aus. Standardmäßig ist der Online-Katalog ausgewählt.

   Offline – Dell EMC Repository Manager-Katalog: wenn die DRM-Repositorys an einem Freigabespeicherort verfügbar sind und für alle verwalteten Nodes durch OMIMSWAC in Rechenzentren ohne Internetverbindung anwendbar sind.

2. Geben Sie den CIFS-Freigabepfad, in dem die Katalogdateien abgelegt werden, und die Nutzeranmeldedaten für den Zugriff auf den CIFS-Freigabepfad ein und wählen Sie dann **Weiter: Compliance-Details:**.

   Die Katalogdateien können mithilfe der Anwendung Dell EMC Repository Manager (DRM) erzeugt werden. Stellen Sie sicher, dass alle erforderlichen Dell Update Packages (DUP) im freigegebenen Katalog-Repository für den Ziel-Node zur Verfügung stehen.

   Wenn ein neuer Katalogpfad angegeben wird, ist der vorherige, zur Berechnung der Update-Compliance verwendete Pfad möglicherweise nicht verfügbar.

OMIMSWAC erfasst den Katalog aus dem freigegebenen Pfad, erfasst die in der Registerkarte **Einstellungen** konfigurierten DSU- und IC-Tools und erzeugt einen Compliance-Bericht. Wenn die Tools DSU und IC nicht in den **Einstellungen** konfiguriert sind, werden Sie von OMIMSWAC mit Internetzugang von `www.downloads.dell.com` heruntergeladen, um den Compliance-Bericht zu erzeugen.

ANMERKUNG: Sie müssen einzelne Katalogdateien mit den Nutzeranmeldedaten für den Server-Manager bzw. den Cluster-Manager bereitstellen.

Die Compliance-Details werden berechnet und der Bericht steht unter **Update-Compliance** > **Compliance-Details** zur Verfügung. Weitere Informationen über den Compliance-Bericht finden Sie unter Compliance-Bericht anzeigen.

Schritt 2: Anzeigen des Compliance-Berichts und Auswahl von Komponenten – Ziel-Node-Komponenten

Die Update-Compliance-Details werden berechnet und der Compliance-Bericht wird angezeigt. Im Ringdiagramm sind die Anzahl der Komponenten im Zustand „Compliant“ (Konform), „Urgent“ (Dringend), „Recommended“ (Empfohlen) oder „Optional“ farbcodiert aufgeführt. Der Compliance-Bericht bietet eine detaillierte Ansicht aller Komponenten, die den Komponentennamen, die aktuelle Version, den Typ, die Baseline-Version, den Compliance-Status, die Dringlichkeit und den Compliance-Typ enthalten.

Attributnamen	Beschreibung
Komponentenname	Gibt den Komponentennamen an. Beispiel: `Serial-ATA_Firmware_6FGD4_WN64_E012_A00`
Compliance	Gibt den Compliance-Typ unabhängig davon an, ob der Status konform oder nicht konform ist. • `Konform`: Ziel-Nodes in dieser Kategorie haben die gleichen Versionen von BIOS, Treibern, Firmware und Systemmanagementanwendung wie der importierte Katalog. • `Nicht konform`: Ziel-Nodes in dieser Kategorie benötigen BIOS-, Treiber-, Firmware-oder Systemmanagementanwendungs-Updates.
Kritischer Zustand	Gibt an, ob die Compliance dringend, empfohlen oder optional ist.

	• `Dringend`: Das Update enthält Änderungen zur Erhöhung der Zuverlässigkeit und Verfügbarkeit des Dell EMC Systems. Führen Sie dieses Update daher sofort aus. • `Empfohlen`: Das Update enthält Funktionsverbesserungen oder -änderungen, anhand derer Sie sicherstellen können, dass die Systemsoftware auf dem neusten Stand und mit anderen Systemmodulen (Firmware, BIOS, Treiber und Anwendung) kompatibel ist. • `Optional`: Das Update enthält Änderungen, die sich nur auf bestimmte Konfigurationen auswirken, oder stellt neue Funktionen zur Verfügung, die auf Ihre Umgebung anwendbar bzw. nicht anwendbar sind. Überprüfen Sie die Einzelheiten zum Update, um festzustellen, ob diese auf das System zutreffen.
Aktuelle Version	Gibt die aktuelle Version der Komponente an. Beispiel: `E012`
Baseline-Version	Gibt an, dass die Version zum importierten Katalog gehört. Beispiel: `E013`
Typ	Gibt den Typ der Komponente an. Beispiel: `Firmware`, `BIOS`, `Treiber`, `Anwendung`
Compliance-Typ	Gibt an, ob die Komponente aktualisierbar, Downgrade-fähig oder identisch ist. • `Aktualisierbar`: Die Komponente kann von der aktuellen Version aktualisiert werden. • `Zurückstufbar`: Die Komponente kann von der aktuellen Version zurückgestuft werden. • `Identisch`: Die aktuelle Version der Komponente ist mit der Baseline-Version identisch.

1. Standardmäßig werden alle nicht konformen erweiterbaren Komponenten ausgewählt.

   Löschen Sie die ausgewählten Komponenten oder wählen Sie die nicht konformen Downgrade-fähigen Komponenten aus, die Sie aktualisieren möchten. Wenn Sie jedoch die Standardauswahl ändern möchten, stellen Sie sicher, dass die Abhängigkeiten zwischen der entsprechenden Komponenten-Firmware und den Treibern erfüllt sind.

2. Klicken Sie nach Auswahl der Komponenten zum Aktualisieren unter **Compliance-Details** auf **Weiter: Zusammenfassung**, um die Seite „Zusammenfassungsbericht“ zur Bestätigung aufzurufen.

   ANMERKUNG: Wenn Komponenten ausgewählt und bestätigt werden und der Sperrmodus auf dem Ziel-Node in iDRAC aktiviert ist, tritt ein Fehler auf und Sie können mit dem Update nicht fortfahren. Deaktivieren Sie den Sperrmodus auf dem Ziel-Node, der von OMIMSWAC verwaltet wird, bevor Sie den Ziel-Node aktualisieren. Informationen zum Deaktivieren des iDRAC-Systemsperrmodus finden Sie in den iDRAC-Dokumenten.

   - Um die Auswahl der Komponenten während des Update-Vorgangs zu ändern, klicken Sie auf der Registerkarte **Zusammenfassung** auf **Zurück**, um zur Registerkarte **Compliance-Details** zu wechseln und Komponenten auszuwählen oder die Auswahl aufzuheben.
   - Wenn Sie die Updatequelle ändern und die Compliance erneut ausführen möchten, klicken Sie auf **Beenden**, um zur **Updatequelle** zu wechseln.

ANMERKUNG: Wenn ein Katalog keine Updates für eine Komponente enthält, wird die Komponente nicht im Compliance-Bericht angezeigt, der mithilfe von OpenManage Integration in Microsoft Windows Admin Center erzeugt wird.

Schritt 3: Aktualisieren – Ziel-Node-Komponenten

Nachdem Sie den Compliance-Bericht auf der Registerkarte **Compliance-Details** erstellt und die Auswahl der Komponenten in der Registerkarte **Zusammenfassung** bestätigt haben, können Sie mit dem Update der Ziel-Node-Komponenten wie folgt fortfahren:

1. Klicken Sie zum Aktualisieren der BIOS-, Treiber-, Firmware- und/oder Systemmanagementanwendung des PowerEdge-Servers auf die neueste Version unter **Zusammenfassung** auf **Weiter: Update**. Sie werden zum Fenster **Aktualisierungsstatus** weitergeleitet.

ANMERKUNG: Während das Update durchgeführt wird, wird empfohlen, den Browser nicht zu beenden oder zu schließen. Wenn Sie den Browser schließen oder beenden, schlägt das Ziel-Node-Update möglicherweise fehl.

2. Sie werden von OMIMSWAC benachrichtigt, sobald der Update-Vorgang abgeschlossen ist.
   - Nach erfolgreicher Aktualisierung wird der Compliance-Bericht (basierend auf den vorherigen Auswahlen) automatisch neu berechnet und auf der Registerkarte **Update** angezeigt.
   - Wenn der Update-Vorgang fehlschlägt, überprüfen Sie die Protokolldateien, die unter dem folgenden Pfad gespeichert sind, um weitere Informationen zu erhalten.
     - Gateway-System: `<Windows-Verzeichnis>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs`
     - Windows 10 Gateway-System: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs`
   - Um den Compliance-Bericht erneut auszuführen, klicken Sie auf **Compliance erneut ausführen** und geben Sie die Details der Compliance-Einstellungen an.

Nodes von HCI- und Failover-Clustern aktualisieren

Mithilfe der Funktion „Cluster-Aware-Update (CAU)“ in OpenManage Integration in Windows Admin Center (OMIMSWAC) können Sie den Compliance-Bericht (BIOS, Treiber, Firmware und/oder Systemmanagementanwendung) anzeigen und die Komponenten von Nodes von HCI- und Failover-Clustern aktualisieren, ohne die Workloads zu beeinträchtigen.

ANMERKUNG: Die CAU-Funktion wird für die folgenden Plattformen mit gültiger Lizenz unterstützt:

- YX4X-Modelle der Dell EMC PowerEdge-Server (und höher) mit iDRAC Firmware 4.00.00.00 oder höher.
- Dell EMC Lösungen für Microsoft Azure Stack HCI mit iDRAC Firmware 4.00.00.00 oder höher.

Compliance- und Update-Voraussetzungen

Bevor Sie einen Compliance-Bericht generieren und Komponenten aktualisieren, stellen Sie Folgendes sicher:

- Die in der *Kompatibilitätsmatrix* des Installationshandbuchs aufgelisteten Software- und Hardwareanforderungen sind erfüllt.
- Stellen Sie sicher, dass der Cluster-Dienst aktiv ist, bevor Sie die Update-Compliance ausführen. Wenn der Cluster-Dienst inaktiv ist, wird möglicherweise kein Update-Compliance-Bericht für einen Ziel-Node erzeugt.
- Um ein Cluster zu verwalten, stellen Sie mithilfe der Option **Verwalten als** eine Verbindung mit dem Cluster her und geben Sie die entsprechenden Anmeldeinformationen des Cluster-Administrators an. Stellen Sie außerdem sicher, dass der Benutzer Teil der lokalen Nutzergruppe von Gateway-Administratoren ist. Weitere Informationen zur Auswahl von „Verwalten als“ finden Sie im Abschnitt „Erste Schritte mit Windows Admin Center“ in der Microsoft Dokumentation.
- Stellen Sie sicher, dass die Failover Cluster Management Tools (RSAT-Clustering-Mgmt) auf den Ziel-Nodes installiert sind.
- Stellen Sie sicher, dass die Bestandsinformationen für den Ziel-Node abgerufen wurden.
- Stellen Sie sicher, dass sich die physischen und virtuellen Laufwerke vor dem Start des CAU in einem fehlerfreien Zustand befinden.
- Stellen Sie sicher, dass der iDRAC-Sperrmodus deaktiviert ist. Informationen zum Deaktivieren des iDRAC-Systemsperrmodus finden Sie in den iDRAC-Dokumenten.
- Für SAS-RAID_Driver stellen Sie Folgendes sicher:
  - Setzen Sie den SATA-Controller auf RAID-Modus.
  - Setzen Sie die NVMe PCIe SSDs auf RAID-Modus.

  Weitere Informationen zur Einstellung des RAID-Modus finden Sie im Anhang
- Stellen Sie sicher, dass der Ziel-Node über IP-Adresse, Hostname und den FQDN (Fully Qualified Domain Name) des Ziel-Node erreichbar ist.

  ANMERKUNG: Wenn der Ziel-Node nicht erreichbar ist und das Ziel-Node-Update durchgeführt wird, wird der Updatestatus möglicherweise als fehlgeschlagen angezeigt. Wenn Sie in diesem Fall den Ziel-Node unmittelbar nach dem Update neu starten und die Compliance erneut ausführen, wird der Status der Ziel-Node-Komponenten möglicherweise als konform angezeigt, während der Gesamtstatus des Server-Updates möglicherweise weiterhin fehlgeschlagen ist.
- Stellen Sie sicher, dass OMIMSWAC Premium-Lizenzen auf allen Cluster-Nodes installiert sind, um die CAU-Funktion zu verwenden. Um die Lizenzierung zu überprüfen, können Sie einen Compliance-Bericht erzeugen und die auf jedem Node installierte Lizenz anzeigen.

ANMERKUNG: Es wird empfohlen, das Cluster zu validieren, bevor Sie CAU starten. Weitere Informationen zum Validieren eines Clusters finden Sie im Microsoft-Dokument Hardware für ein Cluster validieren.

ANMERKUNG: Das Aktualisieren eines Clusters, auf dem WAC installiert ist, wird nicht empfohlen. Um dieses Szenario zu unterstützen, installieren Sie das WAC auf einem anderen System, das nicht Teil des Clusters ist, und schließen Sie das Update ab.

ANMERKUNG: Während die Compliance oder das Update im Gange ist, ist es nicht zulässig, weitere Compliance- oder Update-Aufgaben für dasselbe Cluster auszuführen, das die Update-Anforderungen von den MS WAC-Update-Tools enthält.

ANMERKUNG: Diese Funktion wird für YX2X- und YX3X-Modelle von Dell EMC PowerEdge-Servern nicht unterstützt.

Schritt 1: Erstellen eines Compliance Berichts – Ziel-Node-Komponenten in Failover-Clustern und Azure-Stack-HCI

Um einen Compliance-Bericht für Ziel-Node-Komponenten in Failover-Clustern und Azure-Stack-HCI zu erstellen, wählen Sie **Update > Updatequelle** aus und wählen Sie eine der verfügbaren Offline- oder Online-Katalogoptionen wie folgt aus:

Erzeugen eines Compliance-Berichts mithilfe des Online-Katalogs

Zur Verwendung des Online-Katalogs muss OMIMSWAC mit dem Internet verbunden sein. OMIMSWAC mit Internetzugang ermöglicht es Ihnen, die Online-Katalog-Option in der Drop-down-Liste **Updatequelle** zu verwenden, um den Katalog automatisch herunterzuladen.

Um die Update-Compliance-Details anzuzeigen, müssen Sie die folgenden Aktionen ausführen:

1. Wählen Sie unter **Update > Updatequelle** eine der verfügbaren Online-Katalogoptionen aus. Die entsprechenden Online-Kataloge werden standardmäßig abhängig vom Cluster ausgewählt.

   Die verfügbaren Online-Kataloge variieren je nach Cluster/Ziel-Node, mit dem Sie verbunden sind, wie folgt:
   - Für PowerEdge-Server und Cluster mit PowerEdge-Server: Dell EMC Enterprise-Katalog, der die validierten Versionen von Komponenten für PowerEdge-Server enthält.
   - MX-Server: Dell EMC MX-Lösungskatalog, der die validierten Versionen von Komponenten für PowerEdge MX Modular enthält.
   - Azure-Stack-HCI-Cluster-Nodes: Dell EMC Azure-Stack-HCI-Lösungskatalog, der die validierten Versionen von Komponenten für AX-Nodes und Storage Spaces Direct Ready-Nodes enthält.

   Weitere Informationen über verfügbare Kataloge finden Sie im Anhang.

2. Klicken Sie auf **Weiter: Compliance-Details:**, um den Compliance-Bericht zu erzeugen.

OMIMSWAC lädt den Katalog herunter, erfasst die in der Registerkarte **Einstellungen** konfigurierten DSU- und IC-Tools und erzeugt einen Compliance-Bericht. Wenn die Tools DSU und IC nicht in den **Einstellungen** konfiguriert werden, lädt OMIMSWAC sie von `www.downloads.dell.com` herunter, um den Compliance-Bericht zu erzeugen.

Sie werden zu dem im Fenster **Compliance-Details** generierten Compliance-Bericht weitergeleitet. Weitere Informationen über den Compliance-Bericht finden Sie unter Compliance-Bericht anzeigen.

Erzeugen eines Compliance-Berichts mithilfe des Offline-Katalogs

OMIMSWAC mit oder ohne Internetzugang ermöglicht Ihnen die Auswahl des Dell EMC Repository Manager-Offline-Katalogs, um den Compliance-Bericht zu generieren.

Bevor Sie den neuesten Compliance-Bericht für ein Cluster erstellen, stellen Sie Folgendes sicher: Die folgenden Voraussetzungen sind erforderlich, wenn der OMIMSWAC nicht mit dem Internet verbunden ist und der Dell EMC Repository Manager (DRM)-Offline-Katalog verwendet wird, um einen Compliance-Bericht zu generieren und Komponenten zu aktualisieren.

- Konfigurieren Sie die Informationen zum Freigabe-Speicherort, an denen die Anwendungen DSU und IC platziert werden. Siehe Einstellungen der Update-Compliance-Tools konfigurieren.
- Erzeugen Sie die neuesten Katalogdateien mithilfe der Anwendung Dell EMC Repository Manager (DRM). Die unterstützte Version des DRM kann unter Dell EMC Repository Manager heruntergeladen werden.

Um die Update-Compliance-Details anzuzeigen, müssen Sie die folgenden Aktionen ausführen:

1. Wählen Sie unter **Update** > **Updatequelle** in der Drop-down-Liste **Offline – Dell EMC Repository Manager-Katalog** aus. Standardmäßig ist der Online-Katalog ausgewählt.

   Offline – Dell EMC Repository Manager-Katalog: wenn die DRM-Repositorys an einem Freigabespeicherort verfügbar sind und für alle verwalteten Geräte durch OMIMSWAC in Rechenzentren ohne Internetverbindung anwendbar sind.

ANMERKUNG: Es wird empfohlen, dass die Azure-Stack-HCI-Katalogdateien verwendet werden, um einen Compliance-Bericht für Azure-Stack-HCI zu generieren.

2. Geben Sie den CIFS-Freigabepfad, in dem die Katalogdateien abgelegt werden, und die Nutzeranmeldedaten für den Zugriff auf den CIFS-Freigabepfad ein und wählen Sie dann **Weiter: Compliance-Details:** zum Erstellen eines Compliance Berichts.

   Die Katalogdateien können mithilfe der Anwendung Dell EMC Repository Manager (DRM) erzeugt werden. Stellen Sie sicher, dass alle erforderlichen Dell Update Packages (DUP) im freigegebenen Katalog-Repository für den Ziel-Node zur Verfügung stehen.

   Wenn ein neuer Katalogpfad angegeben wird, ist der vorherige, zur Berechnung der Update-Compliance verwendete Pfad möglicherweise nicht verfügbar.

OMIMSWAC erfasst den Katalog aus dem freigegebenen Pfad, erfasst die in der Registerkarte **Einstellungen** konfigurierten DSU- und IC-Tools und erzeugt einen Compliance-Bericht. Wenn die Tools DSU und IC nicht in den **Einstellungen** konfiguriert sind, werden Sie von OMIMSWAC mit Internetzugang von `www.downloads.dell.com` heruntergeladen, um den Compliance-Bericht zu erzeugen.

ANMERKUNG: Sie müssen einzelne Katalogdateien mit den Nutzeranmeldedaten für den Server-Manager bzw. den Cluster-Manager bereitstellen.

Sie werden zu dem im Fenster **Compliance-Details** generierten Compliance-Bericht weitergeleitet. Weitere Informationen über den Compliance-Bericht finden Sie unter Compliance-Bericht anzeigen.

Schritt 2: Anzeigen des Compliance-Berichts und Auswahl von Komponenten – Ziel-Node-Komponenten in Failover-Clustern und Azure-Stack-HCI

Die Update-Compliance-Details werden berechnet und der Compliance-Bericht wird angezeigt. Im Ringdiagramm sind die Anzahl der Komponenten im Zustand „Compliant“ (Konform), „Urgent“ (Dringend), „Recommended“ (Empfohlen) oder „Optional“ farbcodiert aufgeführt. Der Compliance-Bericht bietet eine detaillierte Ansicht aller Komponenten, die den Komponentennamen, die aktuelle Version, den Typ, die Baseline-Version, den Compliance-Status, die Dringlichkeit und den Compliance-Typ enthalten.

Bei HCI-und Failover-Clustern werden die Update-Compliance der einzelnen Ziel-Nodes und der Komponenten mithilfe von zwei Ringdiagrammen dargestellt: Node-Zusammenfassung und Komponenten-Zusammenfassung. Erweitern Sie zur weiteren Analyse die einzelnen Nodes im Compliance-Bericht, um die aktuelle Version, die Baseline-Versionen und den Compliance-Typ der Komponenten abzurufen, und um alle Nodes und Komponenten mit dem Status „Nicht konform“, „Dringend“, „Empfohlen“ oder „Optional“ anzuzeigen.

Neben Compliance-Informationen wird auch der Lizenzstatus (OMIMSWAC Premium License) für jeden Node angezeigt. Alle Ziel-Nodes, die Teil des Clusters sind, müssen über gültige Lizenzen verfügen. andernfalls können Sie mit dem Update des Clusters nicht fortfahren. Weitere Informationen zur OMIMSWAC-Lizenzierung finden Sie im OMIMSWAC-Installationshandbuch.

Attributnamen	Beschreibung
Komponentenname	Gibt den Komponentennamen an. Beispiel: `Serial-ATA_Firmware_6FGD4_WN64_E012_A00`
Compliance	Gibt den Compliance-Typ unabhängig davon an, ob der Status konform oder nicht konform ist. • `Compliant` Konform: Ziel-Nodes in dieser Kategorie haben die gleichen Versionen von BIOS, Treibern, Firmware und Systemmanagementanwendung wie der importierte Katalog. • `Non-Compliant` Nicht konform: Ziel-Nodes in dieser Kategorie benötigen BIOS-, Treiber-, Firmware-oder Systemmanagementanwendungs-Updates.
Kritischer Zustand	Gibt an, ob die Compliance dringend, empfohlen oder optional ist. • `Urgent` Dringend: Das Update enthält Änderungen zur Erhöhung der Zuverlässigkeit und Verfügbarkeit des Dell EMC Systems. Führen Sie dieses Update daher sofort aus. • `Recommended` Empfohlen: Das Update enthält Funktionsverbesserungen oder -änderungen, anhand derer Sie sicherstellen können, dass die Systemsoftware auf dem neusten Stand und mit anderen Systemmodulen (Firmware,

	BIOS, Treiber und Systemmanagementanwendung) kompatibel ist. • `Optional` Optional: Das Update enthält Änderungen, die sich nur auf bestimmte Konfigurationen auswirken, oder sie stellt neue Funktionen zur Verfügung, die auf Ihre Umgebung anwendbar bzw. nicht anwendbar sind. Überprüfen Sie die Einzelheiten zum Update, um festzustellen, ob diese auf das System zutreffen.
Aktuelle Version	Gibt die aktuelle Version der Komponente an. Beispiel: `E012`
Baseline-Version	Gibt an, dass die Version zum importierten Katalog gehört. Beispiel: `E013`
Typ	Gibt den Typ der Komponente an. Beispiel: `Firmware` , `BIOS` , `Driver` , `Application`
Compliance-Typ	Gibt an, ob die Komponente aktualisierbar, Downgrade-fähig oder identisch ist. • `Upgradable`Aktualisierbar: Die Komponente kann von der aktuellen Version aktualisiert werden. • `Downgradable`Zurückstufbar: Die Komponente kann von der aktuellen Version zurückgestuft werden. • `Same`Identisch: Die aktuelle Version der Komponente ist mit der Baseline-Version identisch.

1. Standardmäßig werden alle nicht konformen erweiterbaren Komponenten für zur Aktualisierung ausgewählt.

   Löschen Sie die ausgewählten Komponenten oder wählen Sie die nicht konformen Downgrade-fähigen Komponenten aus, die Sie aktualisieren möchten. Wenn Sie jedoch die Standardauswahl ändern möchten, stellen Sie sicher, dass die Abhängigkeiten zwischen der entsprechenden Komponenten-Firmware und den Treibern erfüllt sind.

2. Klicken Sie nach Auswahl der Komponenten unter **Compliance-Details** auf **Weiter: Zusammenfassung**, um die Seite „Zusammenfassungsbericht“ zur Bestätigung aufzurufen.

   ANMERKUNG: Wenn Komponenten ausgewählt und bestätigt werden und der Sperrmodus auf einem Ziel-Node in iDRAC aktiviert ist, tritt ein Fehler auf und Sie können mit dem Update nicht fortfahren. Deaktivieren Sie den Sperrmodus auf dem Ziel-Node, der von OMIMSWAC verwaltet wird, bevor Sie das Cluster aktualisieren. Informationen zum Deaktivieren des iDRAC-Systemsperrmodus finden Sie in den iDRAC-Dokumenten.

   - Um die Auswahl der Komponenten während des Update-Vorgangs zu ändern, klicken Sie auf der Registerkarte **Zusammenfassung** auf **Zurück**, um zur Registerkarte **Compliance-Details** zu wechseln und Komponenten auszuwählen oder die Auswahl aufzuheben.
   - Wenn Sie die Updatequelle ändern und die Compliance erneut ausführen möchten, klicken Sie auf **Beenden**, um zur **Updatequelle** zu wechseln.

ANMERKUNG: Wenn ein Katalog keine Updates für eine Komponente enthält, wird die Komponente nicht im Compliance-Bericht angezeigt, der mithilfe von OpenManage Integration in Microsoft Windows Admin Center erzeugt wird.

Schritt 3 Aktualisieren – Ziel-Node-Komponenten in Failover-Clustern und Azure Stack-HCI

Nachdem Sie den Compliance-Bericht auf der Registerkarte **Compliance-Details** erstellt und die Auswahl der Komponenten in der Registerkarte **Zusammenfassung** bestätigt haben, fahren Sie wie folgt mit dem Update der Ziel-Node-Komponenten in Failover-Clustern und Azure-Stack-HCI fort:

1. Klicken Sie zum Aktualisieren der BIOS-, Treiber-, Firmware- und/oder Systemmanagementanwendung der Ziel-Node-Komponenten in Azure Stack-HCI und Failover-Cluster auf die neueste Version unter **Zusammenfassung** auf **Weiter: Cluster-Aware-Update**.

   Eine Meldung wird angezeigt, die Sie dazu auffordert, CredSSP zu aktivieren.

2. Klicken Sie auf **Ja**, um CredSSP zu aktivieren, und fahren Sie mit der Aktualisierung der ausgewählten Komponenten fort. Sie werden zum Fenster **Aktualisierungsstatus** weitergeleitet.

Um die Sicherheit zu verbessern, deaktivieren Sie CredSSP, nachdem der Update-Vorgang abgeschlossen ist.

ANMERKUNG: Während das Update im Fenster **Update-Status** durchgeführt wird, wird empfohlen, den Browser nicht zu beenden oder zu schließen. Wenn Sie den Browser schließen oder beenden, schlägt das Cluster-Update möglicherweise fehl.

Der Update-Job wird im Hintergrund fortgesetzt, unabhängig davon, ob die UI-Sitzung aktiv ist oder nicht. Wenn die UI-Sitzung aktiv ist, wird der Fortschrittsstatus auf Node-Ebene angezeigt. Sie werden von OMIMSWAC benachrichtigt, sobald der Update-Vorgang abgeschlossen ist.

- Nach erfolgreicher Aktualisierung wird der Compliance-Bericht (basierend auf den vorherigen Auswahlen) automatisch neu berechnet und auf der Registerkarte **Update** angezeigt.
- Wenn der Update-Vorgang fehlschlägt, überprüfen Sie zur Fehlerbehebung die Protokolldateien, die unter dem folgenden Pfad gespeichert sind.
  - Gateway-System: `<Windows-Verzeichnis>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs`
  - Windows 10 Gateway-System: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs`
- Um den Compliance-Bericht erneut auszuführen, klicken Sie auf **Compliance erneut ausführen** und geben Sie die Details der Compliance-Einstellungen an.

ANMERKUNG: Wenn ein Update-Job fehlschlägt, werden die aktualisierten Komponenten nicht auf die alte Version zurückgesetzt. Aus diesem Grund sind manchmal das BIOS, die Firmware oder die Treiberversion zwischen den Knoten im Cluster nicht auf dem gleichen Stand. In diesem Fall führen Sie die Update erneut aus, indem Sie die aktualisierte Komponente ausschließen.

8

Troubleshooting

Themen:

Verfügbarkeit der OMIMSWAC-Erweiterungsprotokolle

Die OpenManage Integration in Microsoft Windows Admin Center (OMIMSWAC)-Erweiterungsprotokolle von Ziel-Nodes und Cluster-Nodes finden Sie unter `<Windows Directory>\Temp\OMIMSWAC` auf Ziel-Nodes. Die Protokolle erfassen Informationen, wenn die OMIMSWAC-Funktionen ausgeführt werden, und stellen außerdem Fehlerbehebungsinformationen zu Fehlern bereit, die bei der Durchführung von OMIMSWAC-Vorgängen auftreten. Die Protokolle der verschiedenen OMIMSWAC-Funktionen können mit Hilfe der folgenden Benennungskonvention problemlos aufgerufen werden:

- Für die Hardware- und Funktionsstatus-Bestandsliste: `Inventory<ID*>`
- Für Updatecompliance: `FirmwareCompliance<ID*>`
- Für Aktualisierungsbenachrichtigungen: `Notification<ID*>`

Verfügbarkeit der Update-Vorgangsprotokolle

Die Anwendungsprotokolle für die Update-Compliance-Funktion sind unter folgendem Pfad verfügbar:

- Gateway-System: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs`
- Windows 10 Gateway-System: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs`

Der Downloadstatus der Online-Kataloge wird in den Anwendungsprotokollen erfasst und kann auf Fehlerbehebung bei Downloadfehlern in den Online-Katalogen verweisen.

Wenn die Online-Katalog-Quelle ausgewählt ist und wenn DSU und IC nicht im Voraus in den Einstellungen konfiguriert sind, lädt OMIMSWAC den Katalog sowie die Dienstprogramme DSU und IC in folgendem Pfad herunter:

- Gateway-System: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\Share\temp\<server/cluster_name>`
- Windows 10 Gateway-System: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\Share\temp\<server/cluster_name>`

Stellen Sie sicher, dass die heruntergeladene Katalogdatei, DSU und IC während der Compliance-Generierung und Aktualisierung nicht geändert werden. Die Katalogdatei sowie die Dienstprogramme DSU und IC werden nach Erzeugung und Update des Compliance-Berichts automatisch entfernt.

Protokolle für das Skript, das auf HCI-Clustern vor dem Update ausgeführt wird, um den Speicher in den Wartungsmodus zu versetzen, sind unter `<Windows Directory>\Temp\precau.log` auf jedem Node verfügbar. Protokolle für das Skript, das auf HCI-Clustern nach dem Update ausgeführt wird, um den Speicher aus dem Wartungsmodus wiederherzustellen, sind unter `<Windows Directory>\Temp\postcau.log` auf jedem Node verfügbar.

Die erforderlichen Dateien können nicht auf den Ziel-Node kopiert werden, um Bestandsinformationen abzurufen.

Stellen Sie folgende Punkte sicher:

- Der Ziel-Node befindet sich nicht im Neustartstatus und ist eingeschaltet.
- Die Firewall blockiert die Kommunikation über KMU-Port 445 nicht. Weitere Informationen finden Sie unter Umgebung für Windows Admin Center vorbereiten.

Funktionsstatus und Hardware-Bestandsaufnahme kann nicht von iDRAC abgerufen werden.

Um die Informationen zu Integrität und Hardware-Bestandsaufnahme von iDRAC abzurufen, stellen Sie Folgendes sicher:

- Für die Verwaltung von PowerEdge-Servern verwendet OMIMSWAC ein internes Betriebssystem zur iDRAC Passthrough-Schnittstelle. Standardmäßig ist iDRAC über die IP-Adresse 169.254.0.1/<*Subnetz*> oder 169.254.1.1/<*Subnetz*> erreichbar. Wenn der Host jedoch eine andere Netzwerkschnittstelle im selben Subnetz hat (z. B. wenn ein Tool wie VMFleet installiert ist), ist OMIMSWAC möglicherweise nicht in der Lage, über das Hostbetriebssystem mit der iDRAC zu kommunizieren.

  Melden Sie sich zur Behebung des Konflikts bei iDRAC an, und ändern Sie die USB-NIC-IP-Adresse unter dem Abschnitt „Betriebssystem-zu-iDRAC-Passthrough“. Weitere Informationen über die Zuweisung dieser IP-Adresse finden Sie in der iDRAC-Dokumentation auf der Support-Website.

- Zur Verwaltung von Clustern sind alle Cluster-Nodes über IP-Adresse, Hostname oder FQDN (vollständig qualifizierter Domainname) erreichbar, bevor das Cluster mit OMIMSWAC verwaltet wird.
- Wenn der Refish-Dienst deaktiviert ist, aktivieren Sie den ihn mithilfe der iDRAC-Benutzeroberfläche. Weitere Informationen finden Sie in der iDRAC-Dokumentation auf der Dell EMC Support-Website.
- Auf iDRAC stehen Benutzer-Slots zum Erstellen neuer Benutzer zur Verfügung.

Es war nicht möglich, die Vorgänge „Blinken“ oder „Blinken beenden“ abzuschließen oder die Datenträger dafür auszuwählen.

- **Ursache**: Der Redfish-Service ist nicht aktiviert.

  Lösung: Aktivieren Sie den Redfish-Service mithilfe der iDRAC-Benutzeroberfläche. Weitere Informationen finden Sie in der iDRAC-Dokumentation auf der Dell EMC Support-Website.

- **Ursache**: Wenn nach dem Laden der Hardware-Bestandsaufnahme in OMIMSWAC das physische Laufwerk entfernt wird, schlagen die Vorgänge „Blinken“ und blinken beenden“ `Blink may not be supported with <Disk_Name>` fehl:

  Lösung: Legen Sie das physische Laufwerke ein, und klicken Sie auf **Aktualisieren**, um die Bestandsdaten in OMIMSWAC erneut zu laden, und führen Sie die Vorgänge „Blinken“ und „Blinken beenden“ aus.

- **Ursache**: Wenn die iDRAC-Firmware-Version niedriger als 3.30.30.30 ist, können die physischen Laufwerke nicht für „Blinken“ und „Blinken beenden“ ausgewählt werden.

  Lösung: Aktualisieren Sie die iDRAC-Firmware auf die neueste Version und wiederholen Sie dann die Vorgänge „Blinken“ und „Blinken beenden“.

- Die Vorgänge „Blinken“ und „Blinken beenden“ schlagen fehl, wenn ein physisches Laufwerk an einen integrierten SATA-Controller angeschlossen und der Integritätsstatus `Unknown` ist. Dies weist darauf hin, dass „Blinken“ und „Blinken beenden“ von dem Laufwerk möglicherweise nicht unterstützt wird.

Der Lizenzierungsstatus ist „Unbekannt“ oder „Nicht lizenziert“.

Wenn der Lizenzstatus `Unknown` oder `Non-licensed` ist, stellen Sie Folgendes sicher:

- Die Lizenz ist nicht abgelaufen.
- Auf jedem Ziel-Node sind Lizenzen vorhanden.
- Der Ziel-Node befindet sich nicht im Neustartstatus und ist eingeschaltet.
- Redfish ist aktiviert.
- Die Azure-Stack-HCI-Lizenz oder die PowerEdge-Server-Lizenz wird auf die entsprechende Hardware importiert. Das Importieren der Azure-Stack-HCI-Lizenz auf einen PowerEdge-Server oder PowerEdge-Server-Lizenz auf einen Azure-Stack-HCI-Server wird nicht unterstützt.

Falls das Problem weiterhin besteht:

1. Navigieren Sie zu iDRAC.
2. Stellen Sie sicher, dass der Redfish-Dienst aktiviert ist.
3. Deaktivieren Sie Betriebssystem-zu-iDRAC-Passthrough und aktivieren Sie es wieder.

   Weitere Informationen über Betriebssystem-zu-iDRAC-Passthrough finden Sie im iDRAC-Benutzerhandbuch.

Verfügbarkeit von Lizenzierungsprotokollen

Die lizenzbezogenen Protokolle sind unter folgendem Pfad verfügbar und können durch Durchsuchen von *DellLicenseCollection* in der Datei *Cleanup* gefunden werden.

- Gateway-System: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs\CleanupXXXXXXXXXXXXXX.log`
- Windows 10 Gateway-System: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs\CleanupXXXXXXXXXXXXXX.log`

Job während des Herunterladens der erforderlichen Komponenten für die Server- und Cluster-bewussten Aktualisierungsvorgänge fehlgeschlagen.

Ursache: Beim Export des Repositorys mit dem Dell EMC Repository Manager (DRM) wird der Export-Job möglicherweise mit dem Status „Teilweise erfolgreich“ abgeschlossen. In diesem Fall fehlen möglicherweise ein oder mehrere DUPs im Repository.

Lösung: Führen Sie den Export des Repositorys in DRM erneut aus und stellen Sie sicher, dass der Job erfolgreich abgeschlossen wird.

Ursache: Eine oder mehrere Komponenten werden möglicherweise nicht heruntergeladen, wenn als Updatequelle eine Online-Quelle ausgewählt wird.

Lösung: Stellen Sie sicher, dass eine Internetverbindung vorhanden ist, und versuchen Sie erneut, den Katalog von der Online-Quelle herunterzuladen. Weitere Informationen finden Sie im Dell EMC Repository Manager-Benutzerhandbuch.

CredSSP während der Aktualisierung fehlgeschlagen

- **Ursache**: Beim Update eines Clusters kann die Delegierung von Anmeldedaten unter Verwendung von CredSSP fehlschlagen.

  Lösung: Verbinden Sie das Cluster erneut über den FQDN (vollqualifizierter Domainname) und aktivieren Sie das Kontrollkästchen **Diese Anmeldedaten für alle Server verwenden**.

  Beispiel: Wenn der Domainname „test.dev.com“ ist, verwenden Sie **`test.dev.com\administrator`** als Domainnamen und klicken Sie dann auf **Diese Anmeldedaten für alle Server verwenden**.

- **Ursache**: Wenn die CredSSP-Authentifizierung zum Ausführen von Skripts auf einer Remote-Maschine verwendet wird, kann der Update-Job mit einem Fehler fehlschlagen.

  Das Problem ist, dass CredSSP auf dem Gateway-Rechner deaktiviert wurde.

  Lösung: Um dieses Problem zu beheben, führen Sie die folgenden Schritte aus:

1. Führen Sie im PowerShell-Fenster gpedit aus. `gpedit`
2. Im Gruppenrichtlinien-Editor, **Computer-Konfigurationen** > **Administrative Vorlagen** > **System** > **Anmeldedaten delegieren**
3. Wählen Sie **Delegieren neuer Anmeldedaten mit Server-Authentifizierung nur über NTLM zulassen** und aktivieren Sie es.
4. Führen Sie `gpupdate /force` in der PowerShell aus.

Job fehlgeschlagen, während der Compliance-Bericht generiert wurde

Ursache: Wenn Sie eine Verbindung zu einem Ziel-Node oder Cluster über Single Sign-On statt der Option „Verwalten als“ herstellen und den Compliance-Bericht mit OMIMSWAC erstellen, kann die Compliance-Generierung fehlschlagen.

Lösung: Bevor Sie eine Verbindung zum Ziel-Node oder Cluster herstellen, stellen Sie sicher, dass Sie „Verwalten als“ auswählen und entsprechende Server-Administrator- oder Cluster-Administratorkonten bereitstellen.

Ursache: Bei der Erstellung eines Compliance-Berichts kann die Generierung des Compliance-Berichts mit dem folgenden Fehler im Protokoll fehlschlagen:

```
Starting a command on the remote server failed with the following error message : The
WinRM client sent a request to the remote WS-Management service and was notified that the
request size exceeded the configured MaxEnvelopeSize quota. For more information, see the
about_Remote_Troubleshooting Help topic.
```

Lösung: Stellen Sie sicher, dass:

- Die Netzwerkverbindung zwischen dem Gateway-System und dem Ziel-Node ist intakt.
- Das Kopieren von Dateien zwischen dem Gateway-System und dem Ziel-Node funktioniert. So können Sie dies überprüfen:
  1. Erstellen Sie eine Sitzung basierend auf Ziel-Node-Anmeldedaten, indem Sie den folgenden PowerShell-Befehl ausführen:

     ```
     $SecurePassword = convertto-securestring <password> -asplaintext -force

     $credential = New-Object System.Management.Automation.PSCredential -ArgumentList <userid>,
     $SecurePassword

     $session = New-PSSession -ComputerName <MN FQDN> -Credential $credential -ErrorAction
     SilentlyContinue
     ```

  2. Kopieren Sie eine Testdatei auf den fehlgeschlagenen Ziel-Node unter der Annahme, dass sich "Test.txt" auf Laufwerk C:\ befindet

     ```
     Copy-Item -Path "C:\Test.txt" -Destination "C:\" -Recurse -Force -ToSession $session
     ```

- Wenn das Problem weiterhin besteht, nachdem Sie die obigen Aktionen durchgeführt haben, versuchen Sie, den Windows Remote Management (WS-Management)-Dienst auf dem Ziel-Node zu starten (Datei-Kopieren schlägt fehl), und führen Sie die Compliance erneut aus.

Ursache: Wenn Sie einen Compliance-Bericht für ein Cluster erstellen, schlägt die Erstellung des Compliance-Berichts für Cluster-Nodes möglicherweise fehl.

Lösung: Stellen Sie sicher, dass:

- der Clusterdienst auf dem Cluster-Node ausgeführt wird, indem Sie den PowerShell-Befehl `Get-ClusterService` verwenden.
- der Cluster-Node nicht neu gestartet wird oder sich im ausgeschalteten Zustand befindet.
- Stellen Sie beim Hinzufügen eines Clusters zum Windows Admin Center sicher, dass Sie den Clusternamen im FQDN-Format verwenden.

Ursache: Wenn Sie einen Compliance-Bericht mit dem Microsoft Edge-Browser in Windows 10 erstellen, kann die Generierung des Compliance-Berichts mit dem folgenden Fehler fehlschlagen: `Unable to generate compliance report. The Manage As credentials have not been set or are not in domain\user format.`

Lösung: Führen Sie einen der folgenden Schritte aus:

- Verbinden Sie den Ziel-Node mit den Anmeldedaten unter Verwendung des vollqualifizierten Domainnamens (z. B **`Domäne.lab\Nutzername`**) oder der Top-Level-Domäne (z. B. **`Domäne\Nutzername`**).
- Löschen Sie den Cache-Speicher des Browsers und führen Sie die Compliance erneut aus.
- Stellen Sie sicher, dass der DNS im WAC-installierten System richtig konfiguriert ist, um eine Verbindung zum Ziel-Node mit den richtigen Anmeldedaten herzustellen.

Job ist beim Aktualisieren der ausgewählten Komponenten fehlgeschlagen.

Manchmal kann CAU oder das Ziel-Node-Update fehlschlagen. Mögliche Ursachen und Lösungen sind nachfolgend aufgeführt:

- Validieren Sie im Fall von CAU den Cluster, bevor Sie das Cluster-Aware-Update starten. Weitere Informationen zum Validieren eines Clusters finden Sie im Microsoft-Dokument Hardware für ein Cluster validieren.
- **Ursache**: Die Compliance-Bestandsaufnahmedatei ist für einige Nodes nicht verfügbar oder das Kopieren von Dateien von Node zu Gateway ist nach der Compliance-Generierung fehlgeschlagen.

  Lösung: Erneutes Ausführen der Compliance
- **Ursache**: Aufgrund von Problemen mit der Internetverbindung können die folgenden Fehler auftreten:
  - Signatur-Überprüfung von DSU oder IC
  - Download des Online-Katalogs
  - Download der DUPs

  Wenn einer der oben aufgeführten Schritte fehlschlägt, schlägt auch die Serveraktualisierung fehl.

  Lösung: Stellen Sie sicher, dass eine Internetverbindung vorhanden ist und führen Sie Compliance und Update erneut aus.
- **Ursache**: Das DSU-Installationsprogramm wird nicht von einem Node gelöscht, weil die Installationsdatei manchmal durch den Windows Admin Center-Prozess (sme.exe) gesperrt wird.

  Lösung: Starten Sie den Windows Admin Center-Dienst über die Windows-Dienste-Konsole neu.
- **Ursache**: CAU schlägt fehl, wenn sich ein Laufwerk nicht im fehlerfreien Zustand befindet.

  Lösung: Stellen Sie sicher, dass sich die physischen und virtuellen Laufwerke vor dem Start des CAU in einem fehlerfreien Zustand befinden. Wenn ein Laufwerk einen fehlerhaften Integritätsstatus aufweist, finden Sie im Microsoft-Dokument Informationen, um sie in einen fehlerfreien Zustand zu versetzen.
- **Ursache**: CAU schlägt fehl, wenn einer der Cluster-Nodes angehalten wurde.

  Lösung: Stellen Sie Cluster-Nodes (Failover-Rollen) wieder her, bevor Sie CAU starten.

Komponente wird nach Update als nicht konform angezeigt

Nach dem Update werden möglicherweise Komponenten als nicht konform angezeigt.

Auflösung: Überprüfen Sie in diesem Fall die Bereinigungsprotokolle mit den DSU-Protokollen, um festzustellen, ob für die Komponente ein FEHLER vorliegt. Wenn Voraussetzungen für die Komponente vor der Update erfüllt werden müssen, erfüllen Sie die Voraussetzungen und führen Sie das Update erneut aus.

Zugriff auf OpenManage Integration verweigert

Ursache: Wenn Sie sich beim Windows Admin Center (WAC) mit Gateway-Nutzeranmeldedaten ohne Administratorrechte anmelden und versuchen, OpenManage Integration von der WAC-Konsole aus zu starten, erscheint möglicherweise der Fehler „Zugriff verweigert“.

Lösung: Bevor Sie die Dell EMC OpenManage Integration-Erweiterung in Windows Admin Center starten, stellen Sie sicher, dass Sie sich als Gateway-Administrator am WAC anmelden.

Dell Update Package-(DUP-)Fehler

Das Dell EMC Update Package (DUP) kann Komponenten nach dem Starten des Updates möglicherweise nicht aktualisieren. Es gibt verschiedene Gründe, warum das DUP während des Updates fehlschlagen kann. Sehen Sie sich die folgenden möglichen Lösungen an, um das Problem zu beheben:

- Überprüfen Sie auf dem Node, auf dem Windows Admin Center (WAC) installiert ist, die Protokolldateien, um weitere Informationen zum Herunterladen von DUP-Fehlern und zur Komponentenzuordnung zu erhalten. Die Komponentenzuordnung erfolgt, um die (zur Aktualisierung ausgewählte) Komponente im DUP-Katalog zu identifizieren. Die Protokolldateien befinden sich unter folgendem Pfad.

  Gateway-System:

- Serverupdate: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs\<PrepareUpdate XXXX>`
- CAU: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs\Update XXXX`

Windows 10 Gateway-System:

- Serverupdate: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs\<PrepareUpdate XXXX>`
- CAU: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs\Update XXXX`

- Beispiele für Protokollmeldungen sind unten angegeben:
  - DUP-Download-Fehlerprotokoll

    ```
    28-Apr-2020 12:19:18 AM::: Error >>> Message : DUPs for some of the selected components are not present in DRM repository.
    ```

  - Komponentenzuordnungs-Protokolldatei

    ```
    ## Format: :>> Component Name -> Package Name

    :>> [0001] Broadcom NetXtreme Gigabit Ethernet ->
    Network_Firmware_RG25N_WN64_21.60.2_01.EXE
    ```

- Überprüfen Sie auf dem Ziel-Node die Komponentenzuordnung, suchen Sie nach der komponentenbezogenen DUP-Protokolldatei und überprüfen Sie den Rückgabecode unter `<Windows Directory>\Dell\UpdatePackage\log\<Package Name>`. Im Dell EMC Update Package-Benutzerhandbuch finden Sie Informationen zu Ursache und möglicher Lösung.

  Ein Beispiel für einen Rückgabecode in einem DUP-Fehlerszenario ist unten angegeben:

  ```
  Exit code = 1 (Failure)

  2020-04-21 23:48:27

  Update Package finished. Exit code = 1
  ```

- Das DUP kann fehlschlagen, wenn versucht wird, eine Treiberkomponente auf eine niedrigere Version zurückzustufen. Deinstallieren Sie in diesem Fall den Treiber vom Betriebssystem und führen Sie dann die Komponentenaktualisierung von OMIMSWAC erneut aus. Weitere Informationen zur Deinstallation von Treibern finden Sie im Microsoft-Dokument.

Alternativ können Sie auch Folgendes versuchen:

- Setzen Sie iDRAC auf Version 4.20.20.20 oder höher zurück und führen Sie das Update erneut aus. Weitere Informationen zum Zurücksetzen oder Aktualisieren von iDRAC finden Sie in der iDRAC-Dokumentation.
- Führen Sie die Update manuell im Ziel-Node aus, indem Sie es vom in `<Windows Directory>\Dell\UpdatePackage\log\<Package Name>` im DUP-Protokoll angegebenen Pfad herunterladen. Ein Beispiel für eine Netzwerk-Firmware ist https://downloads.dell.com/FOLDER06091050M/1/Network_Firmware_TWFF6_WN64_16.26.60.00.EXE.
- Stellen Sie sicher, dass das ausgewählte DUP auf dem ausgewählten Betriebssystem und auf der Plattform unterstützt wird, indem Sie den Komponentennamen auf der Dell Support-Website suchen. URL der Dell Support-Website: https://www.dell.com/support/home/in/en/inbsd1/?app=products.

Test-Cluster schlägt mit Netzwerkkommunikationsfehlern fehl

Ursache: Wenn USB-NIC in iDRAC aktiviert ist, wird bei der Ausführung des Test-Cluster-Befehls zur Überprüfung der Bereitschaft zur Cluster-Erstellung oder der Cluster-Integrität möglicherweise ein Fehler im Validierungsbericht angezeigt. Die Fehlermeldung besagt, dass die IPv4-Adressen, die der USB-NIC des Hostbetriebssystems zugewiesen sind, nicht für die Kommunikation mit den anderen Clusternetzwerken verwendet werden können. Sie können diesen Fehler ignorieren.

Lösung: Deaktivieren Sie die USB-NIC (standardmäßig als „Ethernet“ bezeichnet) vorübergehend, bevor Sie den Test-Cluster-Befehl ausführen.

USB-NIC-Netzwerk als partitioniertes Clusternetzwerk angezeigt

Ursache: Wenn die USB-NIC in iDRAC aktiviert ist, zeigen Clusternetzwerke im Failover-Cluster-Manager die Netzwerke an, die der USB-NIC gemäß der Partitionierung zugeordnet sind. Dieses Problem tritt auf, weil die Clusterkommunikation standardmäßig auf allen

Netzwerkadaptern aktiviert ist und USB-NIC IPv4 Adressen nicht für die externe Kommunikation verwendet werden können, wodurch die Clusterkommunikation auf diesen NICs unterbrochen wird. Sie können diesen Fehler ignorieren.

Auflösung: Deaktivieren Sie über den Cluster-Manager die Clusterkommunikation mit den Netzwerken, die den USB-NICs zugeordnet sind.

9

Identifizieren der Generation Ihres Dell EMC PowerEdge-Servers

Um eine Reihe von Servermodellen abzudecken, werden PowerEdge-Server jetzt mithilfe der generischen Benennungskonvention anstelle ihrer Generation benannt.

In diesem Thema wird erläutert, wie Sie die Generation eines PowerEdge-Servers identifizieren, der mithilfe der generischen Benennungskonvention benannt wurde.

Beispiel:

Beim R740-Servermodell handelt es sich um ein Rack-System mit zwei Prozessoren der 14. Generation von Servern mit Intel-Prozessoren. In der Dokumentation wird für R740 die generische Benennungskonvention **YX4X** verwendet. Dabei gilt Folgendes:

- Der Buchstabe **Y** (Alphabet) steht für den Servertyp (Formfaktor: Cloud (C), Flexibel (F), Modular (M oder MX), Rack (R), Tower (T)).
- Der Buchstabe **X** (Ziffer) steht für die Klasse (Anzahl der Prozessoren) des Servers.
- Die Ziffer **4** steht für die Generation des Servers.
- Der Buchstabe **X** (Ziffer) steht für die Bauart des Prozessors.

Tabelle 3. Benennungskonvention für PowerEdge-Server und Beispiele

YX5X-Server	YX4X-Server	YX3X-Server
PowerEdge R7515	PowerEdge M640	PowerEdge M630
PowerEdge R6515	PowerEdge R440	PowerEdge M830
	PowerEdge R540	PowerEdge T130

10

Kontaktaufnahme mit Dell EMC

Dell EMC bietet verschiedene Optionen für Online- und Telefonsupport an. Die Verfügbarkeit ist abhängig von Land und Produkt und einige Dienste sind in Ihrem Gebiet möglicherweise nicht verfügbar.

ANMERKUNG: Wenn Sie nicht über eine aktive Internetverbindung verfügen, können Sie Kontaktinformationen auch auf Ihrer Auftragsbestätigung, dem Lieferschein, der Rechnung oder im Dell EMC Produktkatalog finden.

So erreichen Sie den Vertrieb, den Technischen Support und den Kundendienst von Dell EMC:

1. Rufen Sie die Website Dell.com/support auf.
2. Wählen Sie aus der Liste unten rechts auf der Seite das bevorzugte Land oder die bevorzugte Region aus.
3. Klicken Sie auf **Kontakt** und wählen Sie den entsprechenden Support-Link aus.

A

Glossar

In der folgenden Tabelle sind wichtige Abkürzungen und Akronyme definiert, die in diesem Dokument verwendet werden.

Tabelle 4. Glossar

Abkürzungen/Akronyme	Definition
OMIMSWAC – OpenManage Integration mit Microsoft Windows Admin Center	Dell EMC OpenManage Integration mit Microsoft Windows Admin Center (OMIMSWAC) ermöglicht IT-Administratoren die Verwaltung der PowerEdge-Server als Hosts, mit PowerEdge-Servern erstellte Microsoft Failover-Cluster und mit Dell EMC Lösungen für Microsoft Azure Stack HCI erstellte hyperkonvergente Infrastruktur (HCI). OMIMSWAC vereinfacht die Aufgaben von IT-Administratoren durch die Remote-Verwaltung der PowerEdge-Server und -Cluster während des gesamten Lebenszyklus.
BIOS	Basic Input/Output System (Grundlegendes Eingabe-/Ausgabesystem) BIOS ist Firmware, die auf einem kleinen Speicherchip auf der Systemplatine oder Hauptplatine des Computers integriert ist. Sie fungiert als Schnittstelle zwischen der Computerhardware und dem Betriebssystem. Das BIOS enthält außerdem Anweisungen, die der Computer zum Durchführen von grundlegenden Anweisungen verwendet, z. B. ob von einem Netzwerk oder einer Festplatte aus gestartet werden soll.
Konsole	Die Verwaltungsanwendung, die ein Benutzer zur Durchführung von Remote-Plattformverwaltungsaufgaben verwendet.
DRM – Dell EMC Repository Manager	Dell EMC Repository Manager (DRM) ist eine Anwendung aus dem Dell OpenManage-Portfolio, die IT-Administratoren eine problemlose Verwaltung von Systemaktualisierungen ermöglicht. Dell Repository Manager bietet eine durchsuchbare Benutzeroberfläche, die zum Erstellen benutzerdefinierter Sammlungen verwendet wird. Diese werden auch als Pakete und Repositories von Dell Update Packages (DUPs) bezeichnet.
DSU – Dell EMC System Update Utility	Dell EMC System Update (DSU) ist ein Skript-optimiertes Update-Bereitstellungstool für die Anwendung von Dell Update Packages (DUP) auf Dell EMC Ziel-Nodes.
FQDN	FQDN (Fully Qualified Domain Name, vollqualifizierter Domainname)
Gateway-Administratoren	Gateway-Administratoren können konfigurieren, wer Zugriff auf das Gateway erhält und wie sich Benutzer beim Gateway authentifizieren. Nur Gateway-Administratoren können die Zugriffseinstellungen in Windows Admin Center anzeigen und konfigurieren. Lokale Administratoren auf dem Gateway-Computer sind immer Administratoren des Windows Admin Center Gateway-Services.
Gateway-System	Windows Admin Center ist als Gateway auf einem Windows-Server installiert.
Gateway-Benutzer	Gateway-Benutzer können eine Verbindung mit dem Windows Admin Center Gateway-Dienst herstellen, um Server über dieses Gateway zu verwalten, sie können jedoch weder die Zugriffsberechtigungen noch die Authentifizierungsmethode ändern, die für die Authentifizierung am Gateway verwendet wird.
Windows 10 Gateway-System	Windows Admin Center als Gateway auf einem Windows 10-Betriebssystem installiert.
HCI	Hyperkonvergente Infrastruktur
IC – Dell EMC Inventory Collector	Inventory Collector wird verwendet, um das Zielsystem zu inventarisieren, die Ergebnisse mit einem Repository oder Katalog zu vergleichen und nur die erforderlichen Updates bereitzustellen.

Tabelle 4. Glossar (fortgesetzt)

Abkürzungen/Akronyme	Definition
iDRAC	Integrated Dell Remote Access Controller
IPMI	Intelligent Platform Management Interface
LED	Leuchtdiode (Light-Emitting Diode; LED)
NIC	Netzwerkschnittstellenkarte, auch bekannt als Netzwerkschnittstellen-Controller (NIC)
Offline – Dell EMC Repository Manager-Katalog	Empfohlen, wenn die DRM-Repositorys an einem freigegebenen Speicherort verfügbar sind, und gilt für alle von OMIMSWAC verwalteten Geräte in Rechenzentren ohne Internetverbindung.
Online (HTTPS) – Dell EMC Azure Stack HCI-Lösungskatalog	Die Firmware- und Treiber-Update-Kataloge für Dell EMC Lösungen für Azure Stack-HCI-Katalog enthalten einen Katalog aller validierten Versionen der Ready Node- und AHCI-Komponenten. Empfohlen für Azure-Stack-HCI-Cluster (erstellt mit Dell EMC Microsoft Storage Spaces Direct Ready-Nodes und Dell EMC-Appliance für Azure-Stack-HCI) und für Azure-Stack-HCI-Server.
Online (HTTPS) – Dell EMC Enterprise-Katalog	Empfohlen für PowerEdge-Server.
Online (HTTPS) – Dell EMC MX-Lösungskatalog	Empfohlen für MX-Modelle von PowerEdge-Servern.
SATA	Serial Advanced Technology Attachment – Schnittstelle, die die alternde **PATA**-Technologie ersetzen soll.
USB-Anschluss	USB
UI	Benutzeroberfläche
<Windows Directory>	C:\Windows

B

Anhang

SAS-RAID_Driver

Stellen Sie bei der Durchführung des Update-Compliance-Vorgangs für SAS-RAID_Driver sicher, dass *SATA-Controller* und *NVMe-PCIe-SSDs* auf den RAID-Modus eingestellt sind. So konfigurieren Sie den RAID-Modus:

1. Drücken Sie die F2-Taste, wenn der Bildschirm **Dell Power-On Self-Test (POST)** angezeigt wird.

   Das Fenster **Dell PowerEdge System-Setup** wird angezeigt.

   - Konfigurieren Sie unter **System-BIOS-Einstellung** den RAID-Modus in **SATA-Einstellungen** > **Integriertes SATA**.
   - Konfigurieren Sie unter **System-BIOS-Einstellungen** den RAID-Modus in **NVMe-Einstellungen** > **NVMe-Modus**.

Empfohlener Katalog für Ziel-Nodes oder Cluster

Die folgende Tabelle enthält den empfohlenen Katalog für einen Ziel-Node oder ein Cluster unter „Updatequelle“.

Ziel-Nodes oder Cluster	Empfohlener Katalog
PowerEdge-Server (Rack, modular und Tower)	Online (HTTPs) – Dell EMC Enterprise Katalog (für PowerEdge-Server)
MX-Server	Online (HTTPS) – Dell EMC MX-Lösungskatalog (für PowerEdge-Server)
AHCI Cluster Ready Nodes (S2D oder AX-Appliance)	Online (HTTPS) – Dell EMC Azure Stack HCI-Lösungskatalog
Cluster mit MX- und PowerEdge-Server	Online (HTTPs) – Dell EMC Enterprise Katalog (für PowerEdge-Server)
Cluster mit AHCI Ready Nodes und PowerEdge-Server	Online (HTTPs) – Dell EMC Enterprise Katalog (für PowerEdge-Server)
Cluster mit PowerEdge-, MX- und AHCI Ready-Node-Server	Online (HTTPs) – Dell EMC Enterprise-Katalog (für PowerEdge-Server).
PowerEdge XE2420 Edge-Server oder Cluster	Online (HTTPs) – Dell EMC Enterprise Katalog (für PowerEdge-Server)