Dell EMC OpenManage Integration Version 2.0 mit Microsoft Windows Admin Center

Benutzerhandbuch

Juli 2021
Rev. A04

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.

© 2019 - 2021 Dell Inc. oder ihre Tochtergesellschaften. Alle Rechte vorbehalten. Dell, EMC und andere Marken sind Marken von Dell Inc. oder entsprechenden Tochtergesellschaften. Andere Marken können Marken ihrer jeweiligen Inhaber sein.

Inhaltsverzeichnis

Kapitel 1: Übersicht über die OpenManage Integration mit Microsoft Windows Admin Center.....5
Revisionsverlauf.....6
Was ist neu in dieser Version?.....6
Weitere Ressourcen.....7

Kapitel 2: Erste Schritte mit OpenManage Integration mit Microsoft Windows Admin Center.....9

Kapitel 3: Für Dell EMC OpenManage Integration mit Microsoft Windows Admin Center erforderliche Ports.....11

Kapitel 4: Dell EMC PowerEdge-Server verwalten..... 12
Integritätsstatus – unterstützte Ziel-Node-Komponenten..... 13
Hardwarebestand – Unterstützte Ziel-Node-Komponenten..... 13

Kapitel 5: Verwalten von Failover-Clustern, Azure Stack HCI- und Windows Server HCI-Clustern.....15
Funktionsstatus – Unterstützte Ziel-Node-Komponenten in Failover-Clustern, Windows Server HCI und Azure Stack HCI.....16
Hardware-Bestandsaufnahme – Unterstützte Ziel-Node-Komponenten in Failover-Clustern, Windows Server HCI und Azure Stack HCI.....17

Kapitel 6: iDRAC-Details der PowerEdge-Server und Nodes von HCI und Failover-Clustern anzeigen.... 19

Kapitel 7: Aktualisieren der PowerEdge-Server und -Nodes der Windows Server HCI, Azure Stack HCI und Failover-Cluster mit OpenManage Integration-Erweiterung..... 20
Konfigurieren der DSU- und IC-Einstellungen in Update Tools.....21
Proxy-Einstellungen konfigurieren.....21
Aktualisieren von Ziel-Nodes mithilfe der OpenManage Integration-Erweiterung.....22
Aktualisieren von Nodes von Windows Server-HCI, Azure Stack HCI und Failover-Clustern mit der OpenManage Integration-Erweiterung.....24
Anzeigen des Compliance-Berichts.....27

Kapitel 8: Integrierte Bereitstellung und Aktualisierung von Azure Stack HCI-Clustern..... 29
Integrierte Bereitstellung und Update eines Azure Stack HCI-Clusters mit dem OpenManage Integration-Snap-In..... 29
Hardwaresymmetrieprüfung..... 32

Kapitel 9: Clusterfähige Full-Stack-Aktualisierung für Azure Stack HCI-Cluster mithilfe des OpenManage Integration-Snap-In..... 36
Aktualisieren eines Azure Stack HCI-Clusters mithilfe des OpenManage Integration-Snap-In..... 36

Kapitel 10: Troubleshooting.....39
Aktualisieren von.....39
Lizenzierung.....39
Protokolle.....40

Funktionsstatus, Hardware und iDRAC-Bestandsaufnahme....41
Blinken und Blinken beenden....42
Cluster-fähiges Update....42
Clusterfähige Full-Stack-Aktualisierung....46
Andere....47

Kapitel 11: Identifizieren der Generation Ihres Dell EMC PowerEdge-Servers....49

Kapitel 12: Kontaktaufnahme mit Dell EMC....50

Anhang A: Glossar....51

Anhang B: Anhang....53

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 HCI-Lösungen für Microsoft Windows Server oder Dell EMC Integrated System 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. 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.
  - Dell EMC Integrated System für Microsoft Azure Stack HCI (auch als Azure Stack HCI oder als HCI bezeichnet), die mithilfe von AX-Nodes aus Dell Technologies erstellt werden.
  - Dell EMC HCI-Lösungen für Microsoft Windows Server (auch bekannt als Windows Server HCI oder WS HCI), die unter Verwendung von Storage Spaces Direct Ready-Nodes oder Kombinationen aus AX- und Storage Spaces Direct Ready-Nodes erstellt werden.
  - Microsoft Failover-Cluster, die mit Dell EMC PowerEdge-Servern erstellt wurden, auf denen ein unterstütztes Windows Serverbetriebssystem ausgeführt wird
- Bestandsaufnahme: zeigt Information zum Gesamt-Funktionszustand, dem Hardwarebestand und dem iDRAC-Bestand der Nodes an, einschließlich Informationen auf Komponentenebene für alle unterstützten Dell EMC Plattformen.
- Online-Kataloge: Unterstützung für das Erstellen einer Firmware-Baseline mithilfe der folgenden Online-Kataloge, wenn OMIMSWAC mit dem Internet verbunden ist:
  - **Dell EMC Enterprise-Katalog**: enthält Firmware-Updates für PowerEdge-Server und PowerEdge-Server-Nodes in einem Cluster.
  - **Update-Katalog für Microsoft HCI-Lösungen**: enthält Firmware-Updates für AX-Nodes und Storage Spaces Direct Ready-Nodes sowie Nodes in Windows Server HCI- und Azure Stack HCI-Clustern.
  - **Dell EMC MX Lösungskatalog** für PowerEdge MX Modular.
- Offline-Katalog: Unterstützung für die Erstellung lokaler Firmware-Baselines mithilfe von Dell EMC Repository Manager (DRM).
- Compliance-Bericht: erzeugt einen Update-Compliance-Bericht anhand der von Dell EMC verifizierten Update-Kataloge und bietet Benachrichtigungen, wenn eine neue Katalogversion verfügbar ist.
- Server-Update: unterstützt PowerEdge-Serverupdate ausgehend von der Baseline: Firmware, BIOS, Treiber und Systemmanagementanwendungen.
- Cluster-Aware Update: unterstützt Cluster-Updates ausgehend von validierten Baselines (Firmware, BIOS und Treiber) für PowerEdge-Server-basierte Failover-Cluster, Dell EMC HCI-Lösungen für Microsoft Windows Server und Dell EMC Integrated System für Microsoft Azure Stack HCI.
- Integrated Cluster Deploy and Update: unterstützt die Installation von integrierter Firmware, BIOS und Treibern bei der Erstellung von Azure Stack HCI-Clustern. Außerdem wird eine Symmetrie-Überprüfung durchgeführt, um die Hardwarekonfiguration von Cluster-Nodes in Übereinstimmung mit von Dell EMC empfohlenen Hardwarekonfiguration zu halten.
- Full Stack Cluster-Aware-Aktualisierung: unterstützt eine integrierte Cluster-Aware-Aktualisierung für Azure Stack HCI-Cluster, die Betriebssystem- und Hardware-Updates (Firmware, BIOS und Treiber) umfasst.
- iDRAC-Konsole: zeigt iDRAC-Informationen zu PowerEdge-Servern an. Für die Out-of-band-Verwaltung können Sie die iDRAC-Konsole direkt über Windows Admin Center starten.
- Dell EMC Solutions Badge:
  - Zeigt die Dell EMC Solutions Badge **Azure Stack HCI-zertifiziert** für Dell EMC Integrated System für Microsoft Azure Stack HCI aus AX-Nodes von Dell Technologies an.
  - Zeigt Dell EMC Solutions Badge **Windows Server HCI-zertifiziert** für Dell EMC HCI-Lösungen für Microsoft Windows Server an, die mit Storage Spaces Direct Ready-Nodes oder Kombinationen aus AX-Nodes und Storage Spaces Direct Ready-Nodes erstellt wurden.

- Verfügbarkeit der OMIMSWAC-Erweiterung und -Dokumentation in den Sprachen Englisch, Französisch, Deutsch, Spanisch, vereinfachtes Chinesisch und Japanisch.

Themen:

- Revisionsverlauf
- Was ist neu in dieser Version?
- Weitere Ressourcen

Revisionsverlauf

Date	Dokumentversionen	Beschreibung der Änderungen
Februar 2021	A00	Erstausgabe für OMIMSWAC 2.0
März 2021	A01	• Zusätzliche Unterstützung für Windows Admin Center 2103 GA. • Das Kapitel „Integrierte Bereitstellung und Update des Clusters“ wurde aktualisiert und mit Informationen über das Umbenennen von Nodes ergänzt. • Das Kapitel „Full-Stack CAU“ wurde aktualisiert und mit Informationen über die Deaktivierung der CAU-Clusterrollen nach Updates ergänzt.
Juni 2021	A02	• Unterstützung hinzugefügt für AX-6515- und AX-7525-Nodes in Dell EMC Integrated System für Microsoft Azure-Stack-HCI. • Unterstützung hinzugefügt für AX-7525-Nodes in Dell EMC HCI Lösungen für Microsoft Windows Server.
Juni2021	A03	Support für WAC 2103.2 hinzugefügt.
Juli 2021	A04	Unterstützung für Microsoft Failover-Cluster Tool Extension 1.280.0.nupkg-Version hinzugefügt.

Was ist neu in dieser Version?

- Unterstützt Microsoft Windows Admin Center Preview 2103.2 GA.
- Unterstützt Management und Überwachung der Azure Stack HCI-Lösung basierend auf dem neuen Betriebssystem Azure Stack HCI Version 20H2.
- Installation: bietet die Möglichkeit für die direkte Installation von Dell EMC OpenManage Integration-Snap-in bei der Erstellung eines Azure Stack HCI-Clusters mithilfe von AX-Nodes oder der Ausführung eines Full Stack-Updates auf einem Azure Stack HCI-Cluster.
- OpenManage Integration-Snap-in für integrierte Firmware- und Treiber-Updates während der Azure Stack HCI-Cluster-Erstellung oder Cluster-Aktualisierung im Windows Admin Center.
  - Integrated Cluster Deploy and Update: Diese Funktion gilt für Dell EMC Integrated System für Microsoft Azure Stack HCI (unter dem Betriebssystem Azure Stack HCI Version 20H2).

    Beim Erstellen eines Azure Stack HCI-Clusters mithilfe von AX-Nodes:

    - Unterstützt Hardware-Symmetrie-Prüfungen, die die Konfiguration des Cluster-Nodes mit den von Dell EMC empfohlenen Konfigurationen validieren. Nach der Symmetrieprüfung wird ein umfassender Bericht erstellt, der den Status aller Konfigurationen und empfohlene Aktionen für nicht unterstützte Konfigurationen anzeigt. Diese Funktion sorgt dafür, dass die Clusterkonfiguration mit Dell EMC Empfehlungen konform ist.
    - Unterstützt integrierte Firmware-, BIOS-und Treiber-Updates. Dies bietet eine einheitliche Erfahrung, bei der die Nodes nach der Aktualisierung sowohl des Betriebssystems als auch der Hardware nur einmal neu gestartet werden müssen.

        - Möglichkeit, die Voraussetzungs- und Symmetrie-Prüfungen der Hardware erneut auszuführen, wenn die Fehler behoben werden.
    - Full Stack Cluster-Aware-Aktualisierung: Diese Funktion gilt für Dell EMC Integrated System für Microsoft Azure Stack HCI (mit Betriebssystem Azure Stack HCI Version 20H2).
        - Führt zusätzlich zum Betriebssystem-Update, das im Windows Admin Center verfügbar ist, Hardware-Updates (Firmware, BIOS und Treiber) für Dell EMC Integrated System für Microsoft Azure Stack HCI-Cluster in einem einzigen Durchlauf durch. Diese Funktion unterstützt nicht nur Administratoren beim Update des Betriebssystems und der Firmware, sondern auch der BS-Treiber und Managementanwendungen, die auf dem Cluster installiert sind.
- Cluster-Aware-Aktualisierung (CAU): die Möglichkeit zur Planung von unterstützenden Updates mithilfe der OpenManage Integration-Erweiterung für Folgendes:
    - Serverbasiertes PowerEdge Failover-Cluster
    - Dell EMC HCI-Lösungen für Microsoft Windows Server
    - Dell EMC Integrated System für Microsoft Azure Stack HCI
- Unterstützt Dell EMC System Update (DSU) 1.9 zur Überprüfung der Compliance und Aktualisierung.
- Unterstützt AX-6515- und AX-7525-Nodes in Dell EMC Integrated System für Microsoft Azure Stack HCI.
- Unterstützt AX-7525-Nodes in Dell EMC HCI Lösungen für Microsoft Windows Server.
- Verbesserungen:
    - Unterstützt Ziel-Nodes, die das Betriebssystem Windows Server Core ausführen.
    - Die Lizenzdetails werden angezeigt, indem Sie im iDRAC-Bestand auf einen Lizenz-Attributnamen klicken.
    - Optimierte iDRAC-Bestandslistenattribute, um die Nutzbarkeit zu verbessern.
    - Umbenannter MX-Katalog für PowerEdge MX Modular zu „Dell EMC MX-Lösungskatalog“.
    - Die PowerEdge-Katalog-Option ist jetzt unter „Updatequelle“ für Failover-Cluster verfügbar, die mithilfe von MX Modular erstellt wurden.
    - Die Quickinfo-Informationen der Updatequelle wurden überarbeitet, um sie übersichtlicher zu machen.
    - Verbesserung der Ansicht für die Updatequelle-Katalogauswahl.
    - Verbesserungen in der Compliance-Berichtsansicht von Ringdiagramm zu Balkendiagramm, um die Compliance-Stufe anzuzeigen. Suchfeld im Compliance-Bericht hinzugefügt, um Komponenten zu suchen und auszuwählen.
    - Verbesserungen bei der Compliance-Erstellung und der Update-Leistung.
- Fehlerbehebungen:
    - Wenn zuvor ein Ziel-Node/-Cluster (mithilfe der SSO-Authentifizierung) ohne „Verwalten als“-Anmeldedaten verbunden wurde, um eine Compliance zu erzeugen, musste die Verbindung zum Ziel-Node/Cluster auf der Seite „Alle Verbindungen“ im Windows Admin Center mithilfe von „Verwalten als“-Anmeldeinformationen wiederhergestellt werden.

      In dieser Version fordert die Erweiterung Sie möglicherweise auf, die „Verwalten als“-Anmeldeinformationen auf derselben Seite anzugeben, wenn Sie versuchen, einen Ziel-Node oder -Cluster zu verwalten. Aus diesem Grund müssen Sie nicht auf die Seite „Alle Verbindungen“ im Windows Admin Center zurückkehren, um den Ziel-Node oder -Cluster zu verbinden.

    - Mit Unterstützung für Microsoft-Failover-Cluster-Tool Extension 1.280.0.nupkg wurde das Problem des vollständigen Stack-Updates behoben.

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	

Tabelle 1. Weitere Ressourcen (fortgesetzt)

Dokument	Beschreibung	Verfügbarkeit
	basierten Failover-Clustern unter Verwendung von OMIMSWAC beschrieben.	
Dell EMC OpenManage Integration mit Microsoft Windows Admin Center – Sicherheitskonfigurationsleitfaden	Enthält Informationen über Sicherheitsfunktionen und Funktionen von Dell EMC OpenManage Integration in Microsoft Windows Admin Center (OMIMSWAC).	
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
Integriertes System für Azure Stack HCI	Weitere Informationen zu Dell EMC Integrated System für Microsoft Azure Stack HCI.	https://infohub.delltechnologies.com/t/microsoft-hci-solutions-from-dell-technologies-1/

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 oberen linken Ecke von Windows Admin Center **Server-Manager** oder **Cluster-Manager** aus dem Dropdown-Menü aus.

   Die unterstützte Version ist Windows Admin Center 2103.2 GA.

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 beim Herstellen einer Verbindung zu einem Ziel-Node oder -Cluster keine „Verwalten als"-Anmeldedaten vorhanden oder nicht für die Erweiterung verfügbar sind, werden Sie beim Versuch, den Ziel-Node oder -Cluster zu verwalten, zur Angabe der „Verwalten als"-Anmeldedaten aufgefordert.

   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 12.
- Für Microsoft Failover-Cluster, die mit PowerEdge-Servern erstellt wurden, Dell EMC HCI-Lösungen für Microsoft Windows Server, die mit AX-Nodes und/oder Storage Spaces Direct Ready-Nodes erstellt wurden, oder Dell EMC Integrated-System für Microsoft

Azure Stack HCI, die mit AX-Nodes erstellt wurden, siehe Verwalten von Failover-Clustern, Azure Stack HCI- und Windows Server HCI-Clustern auf Seite 15.

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

Sie können OpenManage-Integration in Microsoft Windows Admin Center (OMIMSWAC) verwenden, um Funktionsstatus, Hardware-Bestandsaufnahme, Update und iDRAC von PowerEdge-Servern anzuzeigen und zu managen.

Voraussetzungen

- Sie haben Windows Admin Center 2103.2 GA installiert.
- Sie müssen bei Microsoft Windows Admin Center als Gateway-Administrator angemeldet sein.
- Sie müssen die OMIMSWAC-Erweiterung 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.
- Stellen Sie sicher, dass Sie mithilfe der Anmeldeinformationen des Domänenadministrators remote auf Windows Admin Center zugreifen. Andernfalls verwenden Sie lokale Administrator-Anmeldedaten, um lokal auf WAC zuzugreifen. Weitere Informationen finden Sie in der Microsoft Dokumentation.

Schritte

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 beim Herstellen einer Verbindung zu einem Ziel-Node oder -Cluster keine „Verwalten als“-Anmeldedaten vorhanden oder nicht für die Erweiterung verfügbar sind, werden Sie beim Versuch, den Ziel-Node oder -Cluster zu verwalten, zur Angabe der „Verwalten als“-Anmeldedaten aufgefordert.

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 13.
   - **Bestandsaufnahme**: zum Anzeigen detaillierter Hardware-Bestandsaufnahme-Informationen der Ziel-Node-Komponenten. Informationen dazu finden Sie unter Hardwarebestand – Unterstützte Ziel-Node-Komponenten auf Seite 13.
   - **Update**: zum Anzeigen des Compliance-Berichts und Aktualisieren der Komponenten auf die Baseline-Version. Informationen dazu finden Sie unter Aktualisieren der PowerEdge-Server und -Nodes der Windows Server HCI, Azure Stack HCI und Failover-Cluster mit OpenManage Integration-Erweiterung auf Seite 20.
   - **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 19.

   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
- Hardwarebestand – Unterstützte Ziel-Node-Komponenten

Integritätsstatus – unterstützte Ziel-Node-Komponenten

Der Integritätsstatus der folgenden Serverkomponenten wird angezeigt:

- CPUs
- Accelerator

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

  ANMERKUNG: Intel **DIMM**-Speicher wird mit einem Symbol als **IntelPersistent** identifiziert.
- Speicher-Controller
- Speichergehäuse
- Physische Festplatten
- iDRAC
- Netzteile
- Lüfter
- Spannungen
- Temperaturen

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

Sie können Informationen zu den Hardware- und Firmware-Komponenten, die auf den Ziel-Nodes installiert sind, anzeigen. Um dies zu tun, wählen Sie in Dell EMC OpenManage Integration die Option **Bestand** aus. Um die neuesten Hardware-Bestandsinformationen anzuzeigen, klicken Sie in der oberen rechten Ecke der Registerkarte **Bestandsaufnahme** auf **Aktualisieren**.

Der Abschnitt „Bestandsaufnahme“ zeigt die Informationen für die folgenden Komponenten an, die auf den Ziel-Nodes verfügbar sind:

- System
- Firmware

  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.
- CPUs
- Accelerator
- Speicher

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

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.

- Netzwerkgerät
- Physische Festplatten

  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.

  Um physische Festplatten zu identifizieren, können Sie das Blinken der Festplatten-LED starten oder stoppen. Weitere Informationen finden Sie unter Blinken und Blinken beenden, physische Festplatten.

- Netzteile
- Lüfter

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 19.

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

Blinken und Blinken beenden, physische Festplatten

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:

- 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.

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.
- Blinken und Blinken beenden auf physischen Festplatten, die mit einem integrierten SATA Controller verbunden sind, ist mit einem Fehler fehlgeschlagen. `Blink/Unblibk May not be supported with - <disk_name>.`

5

Verwalten von Failover-Clustern, Azure Stack HCI- und Windows Server HCI-Clustern

Sie können OpenManage Integration mit der Microsoft Windows Admin Center (OMIMSWAC)-Erweiterung verwenden, um Funktionsstatus, Hardware-Bestandsaufnahme, Update und iDRAC von Microsoft Failover-Clustern anzuzeigen und zu managen, die mit PowerEdge-Servern, Dell EMC HCI-Lösungen für Microsoft Windows Server (Windows Server HCI) und Dell EMC Integrated System für Microsoft Azure Stack HCI (Azure Stack HCI) erstellt wurden.

Voraussetzungen

- Sie haben Windows Admin Center 2103.2 GA installiert.
- 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.
- Stellen Sie sicher, dass Sie mithilfe der Anmeldeinformationen des Domänenadministrators remote auf Windows Admin Center zugreifen. Andernfalls verwenden Sie lokale Administrator-Anmeldedaten, um lokal auf WAC zuzugreifen. Weitere Informationen finden Sie in der Microsoft Dokumentation.

Info über diese Aufgabe

So verwalten Sie die Failover-Cluster, die mit PowerEdge-Servern, mit AX-Nodes erstellten Azure Stack HCI und mit Storage Spaces Direct Ready Nodes erstellten Windows Server HCI oder Kombinationen von AX-Nodes und Storage Spaces Direct Ready Nodes erstellt wurden

Schritte

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

   ANMERKUNG: Wenn Sie von der Erweiterung dazu aufgefordert werden, die Anmeldeinformationen für „Verwalten als“ anzugeben, stellen Sie sicher, dass Sie die Option „Verwalten als“ auswählen und die entsprechenden Anmeldeinformationen für den Cluster-Administrator angeben, um die verwalteten Nodes zu authentifizieren. Aktivieren Sie anschließend das Kontrollkästchen **Diese Anmeldedaten für alle Verbindungen verwenden**. 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.

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 Funktionsstatus – Unterstützte Ziel-Node-Komponenten in Failover-Clustern, Windows Server HCI und Azure Stack HCI auf Seite 16.

- **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, Windows Server HCI und Azure Stack HCI auf Seite 17.
- **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 Aktualisieren der PowerEdge-Server und -Nodes der Windows Server HCI, Azure Stack HCI und Failover-Cluster mit OpenManage Integration-Erweiterung auf Seite 20.
- **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 19.

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:

- Funktionsstatus – Unterstützte Ziel-Node-Komponenten in Failover-Clustern, Windows Server HCI und Azure Stack HCI
- Hardware-Bestandsaufnahme – Unterstützte Ziel-Node-Komponenten in Failover-Clustern, Windows Server HCI und Azure Stack HCI

Funktionsstatus – Unterstützte Ziel-Node-Komponenten in Failover-Clustern, Windows Server HCI und Azure Stack HCI

Wählen Sie auf der Seite **Cluster – Azure Stack HCI** die Registerkarte **Integrität** aus, um den Gesamtfunktionsstatus des Failover- oder HCI-Clusters und den Funktionsstatus der folgenden Ziel-Node-Komponenten der Nodes im Failover-Cluster, Windows Server HCI 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

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

  ANMERKUNG: Intel **DIMM**-Speicher wird mit einem Symbol als **IntelPersistent** identifiziert.
- Speicher-Controller
- Speichergehäuse
- Physische Festplatten
- iDRAC
- Netzteile
- Lüfter
- Spannungen
- Temperaturen

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, Windows Server HCI und Azure Stack HCI

Sie können Informationen über die Hardware- und Firmware-Komponenten anzeigen, die auf Nodes in Failover-Clustern, Windows Server-HCI oder Azure Stack HCI installiert sind. Um dies zu tun, wählen Sie in Dell EMC OpenManage Integration die Option **Bestand** aus. Um die neuesten Hardware-Bestandsinformationen anzuzeigen, klicken Sie in der oberen rechten Ecke der Registerkarte **Bestandsaufnahme** auf **Aktualisieren**.

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

- System
- Firmware

  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.
- CPUs
- Accelerator
- Speicher

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

  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.
- Netzwerkgerät
- Physische Festplatten

  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.

  Um physische Festplatten zu identifizieren, können Sie das Blinken der Festplatten-LED starten oder stoppen. Weitere Informationen finden Sie unter Blinken und Blinken beenden, physische Festplatten.
- Netzteile
- Lüfter

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 19.

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

Blinken und Blinken beenden, physische Festplatten

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.

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.
- Blinken und Blinken beenden auf physischen Festplatten, die mit einem integrierten SATA Controller verbunden sind, ist mit einem Fehler fehlgeschlagen. `Blink/Unblibk May not be supported with - <disk_name>.`

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**.

Für Failover- und hyperkonvergente Cluster erweitern Sie die Nodes, um die folgenden Details anzuzeigen.

- DNS-Domänenname
- URL-Zeichenkette: Diese enthält die iDRAC-IP-Adresse. Sie können die iDRAC-Konsole direkt über Microsoft Windows Admin Center starten.
- IPMI-Version.
- iDRAC-Firmware-Version.
- MAC-Adresse des Geräts.
- Lizenzen: Sie können verschiedene Lizenzen sehen, die auf dem Node verfügbar sind. Beispiel: OMIWAC Premium-Lizenz für MSFT HCI-Lösungen, iDRAC9 Enterprise-Lizenz usw.

  Klicken Sie auf den Lizenznamen, um die Lizenzdetails anzuzeigen.

  Um ein Cluster mithilfe von Dell EMC OpenManage Integration zu verwalten, müssen Sie die OMIWAC Premium-Lizenz auf jedem Ziel-Node installiert haben. Weitere Informationen zur Lizenzierung finden Sie im Abschnitt zur Lizenzierung im OMIMSWAC *Installationshandbuch*.

  ANMERKUNG: Der Premium-Lizenzname für HCI Lösungen, die im OMIMSWAC iDRAC-Bestand angezeigt werden, ist „OMIWAC Premium-Lizenz für MSFT HCI-Lösungen“ Allerdings wird derselbe Lizenzname in iDRAC als „OMIWAC Premium-Lizenz für Azure Stack HCI“ angezeigt.

7

Aktualisieren der PowerEdge-Server und -Nodes der Windows Server HCI, Azure Stack HCI und Failover-Cluster mit OpenManage Integration-Erweiterung

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 Update-Quellkatalog (Online oder Offline-Katalog) aus, um die Aktualisierungsdetails für jedes Gerät abzurufen und einen Compliance-Bericht zu erstellen.
2. **Compliance-Bericht überprüfen und Komponentenauswahl bestätigen**: 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. **Aktualisieren**: 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 HCI-Lösungen für Microsoft Windows Server mit iDRAC Firmware 4.00.00.00 oder höher.
- Dell EMC Integrated System 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:

- Konfigurieren der DSU- und IC-Einstellungen in Update Tools
- Aktualisieren von Ziel-Nodes mithilfe der OpenManage Integration-Erweiterung
- Aktualisieren von Nodes von Windows Server-HCI, Azure Stack HCI und Failover-Clustern mit der OpenManage Integration-Erweiterung

Konfigurieren der DSU- und IC-Einstellungen in Update Tools

Info über diese Aufgabe

Um die neuesten Compliance-Berichte und Aktualisierungskomponenten zu erstellen, müssen Sie bei der OpenManage-Integration-Erweiterung ohne Internetzugang die in **Einstellungen** > **Update-Tools** verfügbaren DSU- und IC-Einstellungen konfigurieren. DNS- und IC-Einstellungen können auch bei der Auswahl eines Katalogs in der **Update** > **Aktualisierungsquelle** konfiguriert werden, indem Sie **Erweiterte Einstellung** auswählen. Die unterstützten Versionen der Dienstprogramme Dell System Update (DSU) und Dell Inventory Collector (IC) für OpenManage Integration Version sind:

- DSU-Version: 1.9.0 Sie können DSU unter https://downloads.dell.com/OMIMSWAC/DSU/ herunterladen.
- IC-Version: 20_09_200_921_A00. Sie können IC unter https://downloads.dell.com/OMIMSWAC/IC/ herunterladen.

Schritte

Klicken Sie in der OpenManage Integration-Erweiterung auf die Registerkarte **Einstellungen** > **Update-Tools**, um Folgendes einzugeben:

1. Geben Sie den Freigabe-Speicherort ein, an dem das IC-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 Nutzerzugangsdaten 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.

Nächste Schritte

Informationen zum Erstellen von Compliance-Bericht und zum Aktualisieren von Ziel-Nodes finden Sie unter Aktualisieren von Ziel-Nodes.

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

Proxy-Einstellungen konfigurieren

OpenManage Integration-Erweiterung bietet eine Option zum Herunterladen von Katalog-, DSU- und IC-Dienstprogrammen über das Internet mithilfe von 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.

Info über diese Aufgabe

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 OMIMSWAC-**Update-Tools** nicht konfiguriert sind und das Gateway-System nicht mit dem Internet verbunden ist, wird die Internetverbindung über die Proxy-Einstellungen geprüft.

ANMERKUNG: Proxy-Einstellungen werden im OpenManage Integration Snap-In nicht unterstützt.

So stellen Sie eine Verbindung zu einem Proxyserver her:

Schritte

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)

Nächste Schritte

Informationen zum Erstellen von Compliance-Bericht und zum Aktualisieren von Ziel-Nodes finden Sie unter Aktualisieren von Ziel-Nodes.

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

Aktualisieren von Ziel-Nodes mithilfe der OpenManage Integration-Erweiterung

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

Voraussetzungen

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

- Stellen Sie sicher, dass Sie die Software- und Hardwareanforderungen erfüllen, die in der *Kompatibilitätsmatrix* des Installationshandbuchs aufgeführt sind.
- Wenn Sie von der Erweiterung zur Eingabe der Anmeldeinformationen für „Verwalten als“ aufgefordert werden, stellen Sie sicher, dass Sie die Option **Verwalten als** auswählen und entsprechende Server-Administrator- oder Cluster-Administratorkonten bereitstellen. 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.
- Wir empfehlen dringend, jeweils nur eine Compliance/Aktualisierung für einen Ziel-Node auszuführen. Das Ausführen mehrerer Compliance-/Aktualisierungsvorgänge gleichzeitige kann zu Fehlern bei den bestehenden Compliance/Aktualisierungen führt.

Schritte

Gehen Sie folgendermaßen vor, um den Compliance-Bericht zu generieren und Firmware-, BIOS- und Treiberaktualisierungen für Ziel-Nodes durchzuführen:

1. Um einen Compliance-Bericht für einen validierten Katalog zu erzeugen, wählen Sie **Aktualisieren > Aktualisierungsquelle** aus und wählen Sie eine der verfügbaren Offline- oder Online-Katalogoptionen wie folgt aus: Die entsprechenden Online-Kataloge werden standardmäßig abhängig vom Ziel-Node ausgewählt.

- Wählen Sie „Online (HTTPS) – <Katalogname>“ um den Katalog automatisch von Dell.com herunterzuladen. Standardmäßig ist der Online-Katalog ausgewählt. Sie können den Online-Katalog verwenden, wenn der OMIMSWAC mit dem Internet verbunden ist. Sie können auch über Proxyeinstellungen auf das Internet zugreifen. Siehe dazu Konfigurieren der Proxyeinstellungen.

  Die verfügbaren Kataloge sind:
  - 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.
  - Für AX-Nodes und Storage Spaces Direct Ready Nodes: Aktualisierungskatalog for Microsoft HCI-Lösungen.

- Wählen Sie „Dell EMC Repository Manager Offline-Katalog“, um den DRM-Katalog zu verwenden, der in einem CIFS-Verzeichnis konfiguriert wurde.

  OMIMSWAC mit oder ohne Internetzugang ermöglicht Ihnen die Auswahl des Dell EMC Repository Manager-Offline-Katalogs, um den Compliance-Bericht zu generieren. Sie können diesen Katalog verwenden, wenn Sie über keinen Internetzugang verfügen oder wenn Sie einen benutzerdefinierten DRM-Katalog verwenden möchten.

  a. Um DRM-Offline-Katalog zu verwenden, stellen Sie sicher, dass die neuesten Katalogdateien mithilfe der Dell EMC Repository Manager (DRM)-Anwendung erzeugt werden. Die unterstützte Version der DRM-Anwendung kann unter Dell EMC Repository Manager heruntergeladen werden. Informationen zum Erstellen eines DRM-Katalogs finden Sie im technischen Artikel.

  b. Nachdem der DRM-Katalog erstellt und in einem Freigabepfad gespeichert wurde, wählen Sie **DRM-Einstellungen** und geben Sie den CIFS-Freigabepfad an, in dem sich DRM Katalog befindet, und geben Sie die Anmeldeinformationen für den Zugriff auf den Freigabepfad ein.

  ANMERKUNG:
  - Wir empfehlen die Verwendung des Katalogs „Aktualisierungskatalog for Microsoft HCI-Lösungen“ für Azure Stack HCI und Windows Server HCI.
  - Sie müssen einzelne Katalogdateien mit den Nutzerzugangsdaten für den Server-Manager bzw. den Cluster-Manager bereitstellen.

2. Wählen Sie für die Verwendung der Dell EMC System Update (DSU-) und Inventory Collector (IC)-Tools **Erweiterte Einstellungen** aus und wählen Sie dann eine der folgenden Optionen:
   - „Automatischer Download und Konfiguration von Dell EMC System Update (DSU) und Inventory Collector (IC)“, wenn OMIMSWAC mit dem Internet verbunden ist. Diese Option ist die Standardeinstellung.
   - „Manuelle Konfiguration von DSU und IC“ und wählen Sie dann **Einstellungen**, um die DSU- und IC-Tools manuell herunterzuladen und in einem freigegebenen Speicherort zu konfigurieren. Wir empfehlen die Verwendung dieser Option, wenn OMIMSWAC nicht mit dem Internet verbunden ist.

     Die DSU- und IC-Einstellungen, die mithilfe Einstellungen unter **Update-Tools** in OpenManage Integration-Erweiterung konfiguriert wurden, sind auch unter **Erweiterte Einstellungen** verfügbar.

   Wenn Sie fertig sind, klicken Sie auf **Weiter: Compliance-Bericht**.

   OMIMSWAC lädt den Katalog herunter, erfasst die in der Registerkarte Einstellungen konfigurierten DSU- und IC-Tools und erzeugt einen Compliance-Bericht. Wenn die DSU- und IC-Tools nicht in den Einstellungen konfiguriert werden, lädt OMIMSWAC sie von https://downloads.dell.com herunter, um den Compliance-Bericht zu erzeugen.
3. Überprüfen Sie auf der Registerkarte **Compliance-Bericht** den Compliance-Bericht.
   - Standardmäßig werden alle „nicht konformen“ „aktualisierbaren“ Komponenten ausgewählt, deren Firmware, BIOS oder Treiber aktualisiert werden.

     Sie können die Auswahl der ausgewählten Komponenten aufheben oder die „nicht-konformen“ „downgradable“ Komponenten für die Aktualisierung auswählen. Wenn Sie jedoch die Standardauswahl ändern möchten, müssen Sie sicherstellen, dass die Abhängigkeiten zwischen der entsprechenden Komponenten-Firmware und den Treibern erfüllt sind.

   - Für eine genauere Auswahl können Sie jeden der im Balkendiagramm vorhandenen Farbcodes auswählen oder das Suchfeld verwenden, um die erforderlichen Komponenten zu filtern. Wählen Sie in der oberen rechten Ecke des Fensters **Compliance-Bericht** die Option zum Deaktivieren, um den Farbcode-Filter zu entfernen.

   Wenn Sie fertig sind, klicken Sie auf **Weiter: Zusammenfassung**.

4. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Komponenten, die aktualisiert werden sollen, und klicken Sie auf **Weiter: Aktualisieren**.
   - Um die Auswahl der Komponenten zu ändern, klicken Sie auf **Zurück**, um zur Registerkarte **Compliance-Bericht** zu wechseln, und aktivieren oder deaktivieren Sie die Komponentenauswahl.
   - Wenn Sie die Updatequelle ändern und die Compliance erneut ausführen möchten, klicken Sie auf **Beenden**, um zur **Updatequelle** zu wechseln.

Während die Aktualisierung auf der Registerkarte **Aktualisieren** durchgeführt wird, wird empfohlen, den Browser nicht zu beenden oder zu schließen. Wenn Sie den Browser schließen oder beenden, können Node-Aktualisierungen fehlschlagen, und der Aktualisierungsstatus wird möglicherweise nicht angezeigt.

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.

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 die Protokolldateien, die unter dem folgenden Pfad gespeichert sind, um weitere Informationen zu erhalten.
  - 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`
- Um den Compliance-Bericht erneut auszuführen, klicken Sie auf **Compliance erneut ausführen** und geben Sie die Details der Compliance-Einstellungen an.

Ergebnisse

Wenn eine Komponentenaktualisierung einen Neustart erfordert, wird der Node neu gestartet.

Aktualisieren von Nodes von Windows Server-HCI, Azure Stack HCI und Failover-Clustern mit der OpenManage Integration-Erweiterung

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

Voraussetzungen

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

- Stellen Sie sicher, dass Sie mithilfe von Domänennutzer-Zugangsdaten remote auf Windows Admin Center zugreifen. Andernfalls verwenden Sie lokale Administrator-Anmeldedaten, um lokal auf WAC zuzugreifen. Weitere Informationen finden Sie in der Microsoft Dokumentation.
- Da OMIMSWAC die Microsoft clusterfähige Aktualisierungsfunktion für Cluster-Aktualisierungen verwendet, müssen Sie sicherstellen, dass die **Failover-Clustering-Funktion** und die **Failover-Clustering-Tools** auf allen Ziel-Nodes installiert sind, bevor Sie CAU auslösen. Weitere Informationen finden Sie unter Anforderungen und Best Practices für clusterfähiges Aktualisieren in der Microsoft Dokumentation.

  ANMERKUNG: Es wird empfohlen, die Clusterbereitschaft zu testen, bevor Sie CAU starten. Weitere Informationen finden Sie in den Tests für die Aktualisierungsbereitschaft von Cluster in der Microsoft Dokumentation.
- Stellen Sie sicher, dass Sie die Software- und Hardwareanforderungen erfüllen, die in der *Kompatibilitätsmatrix* des Installationshandbuchs aufgeführt sind.
- Stellen Sie sicher, dass OMIWAC Premium-Lizenzen auf allen Cluster-Nodes installiert sind, um die CAU-Funktion zu verwenden. Um die Lizenzierung zu überprüfen, klicken Sie auf die Registerkarte **iDRAC** in der OpenManage Integration-Erweiterung, um auf jedem Node installierte Lizenzen anzuzeigen.
- 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 Domänenadministrators an. Stellen Sie außerdem sicher, dass der Benutzer Teil der lokalen Nutzergruppe von Gateway-Administratoren ist. Weitere Informationen finden Sie unter Anforderungen und Best Practices für clusterfähiges Aktualisieren in der Microsoft Dokumentation.
- 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.

Info über diese Aufgabe

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

- YX4X-Modelle der Dell EMC PowerEdge-Server und höher mit iDRAC Firmware 4.00.00.00 oder höher.
- AX-Nodes und Storage Space Direct Ready Nodes mit iDRAC-Firmware 4.00.00.00 oder höher.

ANMERKUNG:

- Wir empfehlen, das Cluster zu validieren, bevor Sie CAU auslösen. Weitere Informationen zum Validieren eines Clusters finden Sie im Microsoft-Dokument Hardware für ein Cluster validieren.
- 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.
- Wir empfehlen dringend, jeweils nur eine Compliance/Aktualisierung für einen Ziel-Node oder Cluster auszuführen. Die gleichzeitige Ausführung mehrerer Compliance-/Aktualisierungsvorgänge kann zu Fehlern bei den bestehenden Compliance/Aktualisierungen führen.
- Diese Funktion wird für YX2X- und YX3X-Modelle von Dell EMC PowerEdge-Servern nicht unterstützt.

Schritte

Gehen Sie wie folgt vor, um den Compliance-Bericht zu erzeugen und Firmware-, BIOS- und Treiberaktualisierungen für Windows Server HCI, Azure Stack HCI und Failover-Cluster auszuführen:

1. Gehen Sie auf der Registerkarte **Aktualisierungsquelle** wie folgt vor, um Compliance-Berichte für den validierten Katalog zu erstellen:
   a. Wählen Sie eine der Methoden zum Herunterladen von Katalogdateien aus:
      - **Online (HTTPS) – <Katalogname>**-Katalog zum automatischen Herunterladen des Katalogs von dell.com. Standardmäßig ist der Online-Katalog ausgewählt.

        Die verfügbaren Kataloge sind:
        - 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.
        - Für Windows Server HCI- und Azure Stack HCI-Cluster-Nodes: Katalog für Microsoft HCI-Lösungen aktualisieren, der die validierten Versionen von Komponenten für AX-Nodes und Storage Spaces Direct Ready Nodes enthält.

        Die Online-Katalogunterstützung erfordert eine direkte Internetverbindung vom Windows Admin Center-Gateway. Die Downloadzeit eines Katalogs hängt von der Netzwerkbandbreite und der Anzahl der zu aktualisierenden Komponenten ab. Sie können auch über Proxyeinstellungen auf das Internet zugreifen. Siehe dazu Konfigurieren der Proxyeinstellungen.
      - **Dell EMC Repository Manager Offline-Katalog** zur Verwendung des DRM-Katalogs, der in einem CIFS-Verzeichnis konfiguriert wurde.

        OMIMSWAC mit oder ohne Internetzugang ermöglicht Ihnen die Auswahl des Dell EMC Repository Manager-Offline-Katalogs, um den Compliance-Bericht zu generieren. Sie können diese Option verwenden, wenn Sie über keinen Internetzugang verfügen oder wenn Sie einen benutzerdefinierten DRM Katalog verwenden möchten.
        - Um den Offline-Katalog zu verwenden, wählen Sie **DRM-Einstellungen** aus, um sicherzustellen, dass der CIFS-Freigabepfad mit dem DRM-Katalog konfiguriert ist. Die unterstützte Version der DRM-Anwendung kann unter Dell EMC

Repository Manager heruntergeladen werden. Informationen zum Erstellen eines DRM-Katalogs finden Sie im technischen Artikel.

ANMERKUNG:

- Wir empfehlen die Verwendung des Katalogs „Aktualisierungskatalog for Microsoft HCI-Lösungen“ für Azure Stack HCI und Windows Server HCI.
- Sie müssen einzelne Katalogdateien mit den Nutzerzugangsdaten für den Server-Manager bzw. den Cluster-Manager bereitstellen.

b. Um die Dell EMC System Update (DSU)- und die Inventory Collector (IC)-Tools zu verwenden, wählen Sie **Erweiterte Einstellungen** aus und wählen Sie dann eine der folgenden Optionen:

- „Automatischer Download und Konfiguration von Dell EMC System Update (DSU) und Inventory Collector (IC)“, wenn OMIMSWAC mit dem Internet verbunden ist. Diese Option ist die Standardeinstellung.
- „Manuelle Konfiguration von DSU und IC“ und wählen Sie dann **Einstellungen**, um die DSU- und IC-Tools manuell herunterzuladen und in einem freigegebenen Speicherort zu konfigurieren. Wir empfehlen die Verwendung dieser Option, wenn OMIMSWAC nicht mit dem Internet verbunden ist.

  Die DSU- und IC-Einstellungen, die mithilfe Einstellungen unter **Update-Tools** in OpenManage Integration-Erweiterung konfiguriert wurden, sind auch unter **Erweiterte Einstellungen** im OpenManage Integration-Snap-In verfügbar.

Wenn Sie fertig sind, klicken Sie auf **Weiter: Compliance-Bericht**.

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

2. Überprüfen Sie auf der Registerkarte **Compliance-Bericht** den Compliance-Bericht. Weitere Informationen über den Compliance-Bericht finden Sie unter Anzeigen des Compliance-Berichts.

- Die aktualisierbaren Komponenten, die nicht konform sind, werden standardmäßig für die Aktualisierung ausgewählt.

  Sie können die Auswahl der ausgewählten Komponenten aufheben oder die „nicht-konformen“ „downgradable“ Komponenten für die Aktualisierung auswählen. Wenn Sie jedoch die Standardauswahl ändern möchten, stellen Sie sicher, dass die Abhängigkeiten zwischen der entsprechenden Komponenten-Firmware und den Treibern erfüllt sind.

- Für eine genauere Auswahl können Sie jeden der im Balkendiagramm vorhandenen Farbcodes auswählen oder das Suchfeld verwenden, um die erforderlichen Komponenten zu filtern. Wählen Sie in der oberen rechten Ecke des Fensters **Compliance-Bericht** die Option zum Deaktivieren, um den Farbcode-Filter zu entfernen.

  Sie können auch auf das Symbol „Alle erweitern“ in der oberen rechten Ecke des Bereichs **Compliance-Bericht** klicken, um die Nodes zu erweitern, auf denen Sie die Komponenten auswählen oder deren Auswahl aufheben können.

Wenn Sie fertig sind, klicken Sie auf **Weiter: Zusammenfassung**.

3. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Komponenten, die aktualisiert werden sollen, und geben Sie an, ob die Aktualisierung jetzt ausgeführt oder für später geplant werden soll.

- **Jetzt ausführen**: Dadurch wird die Clusteraktualisierung sofort ausgeführt, und die Nodes werden bei Bedarf neu gestartet.
- **Später planen**: Wählen Sie einen zukünftigen Zeitpunkt aus, zu dem die Clusteraktualisierung durchgeführt werden soll. Dadurch werden die erforderlichen Dateien heruntergeladen und kopiert und das Cluster zur angegebenen Zeit zur Aktualisierung bereitgehalten.

  Zu einem gegebenen Zeitpunkt kann pro Cluster nur ein einziger Job geplant werden. Jeder neue CAU-Job (Jetzt ausführen oder Später planen) ersetzt den vorhandenen geplanten Job.

Um die Auswahl der Komponenten zu ändern, wählen Sie **Zurück**, um zur Registerkarte **Compliance-Bericht** zu wechseln, und aktivieren oder deaktivieren Sie die Komponentenauswahl. 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 mit Microsoft Windows Admin Center-Integration erzeugt wird.

4. Wenn Sie fertig sind, klicken Sie auf **Weiter: Clusterfähige Aktualisierung**.

Eine Meldung wird angezeigt, die Sie dazu auffordert, CredSSP zu aktivieren. Klicken Sie auf **Ja**, um CredSSP zu aktivieren, und fahren Sie mit der Aktualisierung der ausgewählten Komponenten fort. Sie werden zur Registerkarte **Clusterfähige Aktualisierung** weitergeleitet, um den Status der Aktualisierung anzuzeigen. Um die Sicherheit zu verbessern, deaktivieren Sie CredSSP, nachdem der Update-Vorgang abgeschlossen ist.

ANMERKUNG: Während die Aktualisierung auf der Registerkarte **Clusterfähige Aktualisierung** durchgeführt wird, wird empfohlen, den Browser nicht zu beenden oder zu schließen. Wenn Sie den Browser schließen oder beenden, können Node-Aktualisierungen fehlschlagen, und der Aktualisierungsstatus wird möglicherweise nicht angezeigt.

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.

- Wenn der Update-Vorgang fehlschlägt, überprüfen Sie zum Troubleshooting die Protokolldateien, die unter dem folgenden Pfad gespeichert sind.
  - 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`
  - Nachdem die geplante Cluster-Aktualisierung abgeschlossen ist, sind die Protokolle für einzelne Nodes im Ordner `<Windows Directory>\Temp\OMIMSWAC` auf den entsprechenden Nodes zu finden.
- Um den Compliance-Bericht erneut auszuführen, klicken Sie auf **Compliance erneut ausführen** und geben Sie bei Bedarf die Details der Compliance-Einstellungen an.

Ergebnisse

Wenn für die Aktualisierung einer Komponente ein Neustart erforderlich ist, werden die Nodes nacheinander neu gestartet. Dabei werden Cluster-Rollen wie VMS zwischen Nodes verschoben, um Ausfallzeiten zu vermeiden.

Anzeigen des Compliance-Berichts

Die Update-Compliance-Details werden berechnet und der Compliance-Bericht wird angezeigt. Im Balkendiagramm 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.

Sie können auf das Symbol **Alle erweitern** oder **Alle ausblenden** (nur für clusterfähige Aktualisierung in der OpenManage Integration-Erweiterung) in der oberen rechten Ecke des Bereichs **Compliance-Bericht** klicken, um die Nodes zu erweitern, für die Sie Komponenten auswählen oder die Auswahl aufheben können. Für eine genauere Auswahl können Sie jeden der im Balkendiagramm vorhandenen Farbcodes auswählen oder das Suchfeld verwenden, um die erforderlichen Komponenten zu filtern. Wählen Sie in der oberen rechten Ecke des Fensters **Compliance-Bericht** die Option zum Deaktivieren, um den Farbcode-Filter zu entfernen.

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 (OMIWAC Premium-Lizenz) für jeden Node angezeigt.

ANMERKUNG: 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.

ANMERKUNG: Wenn ein Katalog keine Updates für eine Komponente enthält, wird die Komponente nicht im generierten Compliance-Bericht angezeigt.

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` - Ziel-Nodes in dieser Kategorie haben dieselben Firmware-, BIOS- und Treiberversionen wie der importierte Katalog. • `Non-Compliant` - Ziel-Nodes in dieser Kategorie erfordern Firmware-, BIOS- und Treiberaktualisierungen.
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` Das Update enthält Funktionsverbesserungen oder -änderungen, anhand derer Sie sicherstellen können, dass die Systemsoftware auf dem neusten Stand und mit anderen Systemmodulen (Firmware, BIOS und Treiber) 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.

ANMERKUNG: Im Compliance-Bericht kann für den Compliance-Typ **Microsoft basic display adapter Driver** (Grundlegender Microsoft Bildschirmadaptertreibers) angezeigt werden, dass ein Downgrade möglich ist. Nach der Aktualisierung (Downgrade) ändert sich der Name des Treibers in **Matrox G200eW3 (Nuvoton) WDDM <Versionsnr.> Driver**. Hierbei handelt es sich um erwartetes Verhalten.

8

Integrierte Bereitstellung und Aktualisierung von Azure Stack HCI-Clustern

In diesem Abschnitt erfahren Sie, wie Sie das OpenManage Integration Snap-In verwenden, um eine integrierte Bereitstellung und Aktualisierung von Azure Stack (AS HCI)-Clustern durchzuführen.

Während der Bereitstellung eines Azure Stack HCI-Clusters mit AX-Nodes im Windows Admin Center, verwenden Sie das OpenManage Integration-Snap-In, um Folgendes für eine optimale Cluster-Leistung und Unterstützung sicherzustellen:

- Hardwaresymmetrieprüfungen: stellt sicher, dass die für einen Azure Stack HCI-Cluster ausgewählten Nodes unterstützt werden und über symmetrische Hardwarekonfigurationen verfügen, wie von Dell EMC empfohlen.
- Update: stellt sicher, dass Firmware, BIOS und Treiber der ausgewählten Nodes auf dem neuesten Stand sind.

Da diese Funktion in den Workflow zur Erstellung eines Azure Stack HCI-Clusters integriert ist, werden die Nodes nur einmal neu gestartet, wenn dies erforderlich ist, nachdem sowohl Betriebssystem- als auch Hardware-Updates abgeschlossen sind.

Themen:

- Integrierte Bereitstellung und Update eines Azure Stack HCI-Clusters mit dem OpenManage Integration-Snap-In
- Hardwaresymmetrieprüfung

Integrierte Bereitstellung und Update eines Azure Stack HCI-Clusters mit dem OpenManage Integration-Snap-In

Die Funktion zur integrierten Bereitstellung und Update eines Clusters in OpenManage Integration ermöglicht es Ihnen, Ziel-Nodes zu aktualisieren, während Sie einen Azure Stack HCI-Cluster mithilfe von Windows Admin Center erstellen. Mit dieser Funktion können Sie außerdem die Hardwarekonfigurationen ausgewählter Nodes mit von Dell EMC empfohlenen Hardwarekonfigurationen einhalten.

Voraussetzungen

Bevor Sie beginnen, überprüfen Sie Folgendes:

- Stellen Sie sicher, dass Sie Windows Admin Center 2103.2 GA installiert haben.
- Stellen Sie sicher, dass Sie die Erweiterung für Microsoft Cluster Creation Version 1.556.0.nupkg installiert haben. Diese finden Sie im öffentlichen NuGet Feed auf Windows Admin Center von Micrsoft.
- Stellen Sie sicher, dass Sie mithilfe der Anmeldeinformationen des Domänenadministrators remote auf Windows Admin Center zugreifen. Andernfalls verwenden Sie lokale Administrator-Anmeldedaten, um lokal auf WAC zuzugreifen. Weitere Informationen finden Sie unter Windows Admin Center-Installationstypen.
- Stellen Sie sicher, dass alle Voraussetzungen, die unter Erstellen eines Azure Stack HCI-Clusters mit Windows Admin Center in den Microsoft Dokumenten erwähnt werden, erfüllt sind.
- Stellen Sie sicher, dass alle ausgewählten Nodes AX-Nodes sind, auf denen das Betriebssystem Azure Stack HCI Version 20H2 ausgeführt wird. Weitere Informationen über die unterstützte Hardware finden Sie unter *Kompatibilitätsmatrix* im OMIMSWAC-Installationshandbuch.
- Um ein Cluster zu erstellen, stellen Sie eine Verbindung mit den Nodes her, indem Sie die entsprechenden Node-Administrator-Anmeldedaten angeben. 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 Nodes nicht zu einem vorhandenen Cluster gehören.
- Stellen Sie sicher, dass die OMIWAC Premium-Lizenz für MSFT HCI-Lösungen auf jedem Node verfügbar ist.
- Stellen Sie sicher, dass OMIMSWAC mit dem Internet verbunden ist, um Online-Kataloge verwenden zu können. Sie können auch Proxyeinstellungen zum Herunterladen von Katalog-, DSU- und IC-Dienstprogrammen über das Internet verwenden, um nur Compliance-Berichte zu erstellen. Weitere Informationen zu den Proxyeinstellungen finden Sie unter Konfigurieren von Proxyeinstellungen.
- Um den DRM-Offline-Katalog zu verwenden, stellen Sie sicher, dass die Einstellungen wie unter Konfigurieren der Einstellungen des Updatetools beschrieben konfiguriert werden.

Info über diese Aufgabe

ANMERKUNG:

- Wenn eine der oben genannten Voraussetzungen nicht erfüllt ist, stellen Sie sicher, dass Sie sie nach Bedarf überprüfen und beheben. Sie können auch den OpenManage Integration-Snap-In-Ablauf überspringen und mit dem Workflow zur Erstellung von Clustern von Microsoft fortfahren. Allerdings kann das Überspringen des Workflows Hardwareaktualisierungen installieren Auswirkungen auf die Performance des Clusters haben. Aus diesem Grund wird empfohlen, beim Erstellen von Clustern Hardware-Aktualisierungen zu installieren.
- Dell EMC OpenManage Integration in Windows Admin Center bietet keine Unterstützung für die Erstellung eines stretched Clusters.

Schritte

Gehen Sie bei der Bereitstellung eines Azure Stack HCI-Clusters wie folgt vor, um eine symmetrische Hardwarekonfiguration beizubehalten und Firmware/Treiber für Azure Stack HCI-Cluster-Nodes zu aktualisieren:

1. Bei der Bereitstellung eines Azure Stack HCI-Clusters in Windows Admin Center mit dem Assistenten **Erste Schritte** führen Sie die Vorgänge auf den Registerkarten **1.1 Voraussetzungen überprüfen** , **1.2 Server hinzufügen**, **1.3 Einer Domäne beitreten**, **1.4 Funktionen installieren** und **1.5 Updates installieren** nach Bedarf aus.

   ANMERKUNG: Das Umbenennen von Nodes in der Registerkarte **1.3 Einer Domäne beitreten** wird nicht unterstützt und kann bei der Installation von Hardwareupdates zu einem Voraussetzungsfehler führen. Um Server umzubenennen (falls erforderlich), empfiehlt es sich, die Umbenennung außerhalb des Cluster-Bereitstellungsworkflows durchzuführen. Verwenden Sie beispielsweise das Azure Stack HCI OS Serverkonfigurationstool (Sconfig) oder den Windows Admin Center, um einen Node umzubenennen. Stellen Sie vor dem Start des Clustererstellungsassistenten sicher, dass der neue Node-Name gültig ist.

2. Klicken Sie auf der Registerkarte **Hardwareaktualisierungen installieren** auf **Installieren**, um das OpenManage Integration-Snap-In zu installieren. Wenn Sie die OpenManage Integration-Erweiterung Version 2.0 bereits installiert haben, klicken Sie auf **Nach Updates suchen**, um zur Seite „Hardwareaktualisierungen installieren“ zu wechseln.

   ANMERKUNG: Wenn Sie vom Snap-In dazu aufgefordert werden, die Anmeldeinformationen für „Verwalten als“ anzugeben, stellen Sie sicher, dass Sie die Option „Verwalten als“ auswählen und die entsprechenden Anmeldeinformationen für den Cluster-Administrator angeben, um den verwalteten Node zu authentifizieren. Aktivieren Sie anschließend das Kontrollkästchen „Diese Anmeldedaten für alle Verbindungen verwenden“. 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.

   Wenn das OpenManage Integration Snap-In installiert ist, wird die eigenständige OpenManage Integration-Erweiterung im Menü **Extras** im Windows Admin Center angezeigt. Sie werden in der Lage sein, alle Funktionen der OpenManage Integration-Erweiterung zusammen mit den Snap-In-spezifischen Funktionen zu verwenden.

3. Überprüfen Sie die auf der Seite aufgeführten Voraussetzungen, um sicherzustellen, dass alle Nodes für die Durchführung von Hardwaresymmetrieprüfungen und Updates bereit sind.
   - Wenn einer der Nodes kein gültiges Modell ist, können Sie nicht mit dem nächsten Schritt fortfahren. Weitere Informationen zu unterstützten Modellen finden Sie unter AS HCI-Supportmatrix.
   - Wenn einer der Nodes keine OMIWAC Premium-Lizenz enthält, können Sie fortfahren, Nodes zu aktualisieren. Sie können jedoch keine Hardwaresymmetrieprüfungen ausführen.

   Klicken Sie auf **Erneut ausführen**, um die Voraussetzungen erneut auszuführen.

   Wenn Sie fertig sind, klicken Sie auf **Weiter: Hardwaresymmetrieprüfung**.

4. Für **Hardwaresymmetrieprüfung** prüfen Sie die unter jeder Kategorie aufgeführten Konfigurationen, um sicherzustellen, dass alle Node-Konfigurationen den von Dell EMC empfohlenen Konfigurationen entsprechen. Weitere Informationen zu den für die Hardwaresymmetrie erforderlichen Hardwarekonfigurationen finden Sie unter Hardwaresymmetriekonfigurationen.
   - (Optional) Wenn keine Internetverbindung verfügbar ist, führen Sie die folgenden Schritte aus, um Hardwaresymmetrieprüfungen im Offlinemodus auszuführen:
     a. Laden Sie die Dateien *asHCISolutionSupportMatrix.json* und *asHCISolutionSupportMatrix.json.sign* von http://downloads.dell.com/omimswac/supportmatrix/ herunter.
     b. Legen Sie diese Dateien im Ordner `C:\Users\Dell\SymmetryCheck` im Gateway-System, auf dem Windows Admin Center installiert ist, ab.
     c. Führen Sie die Hardwaresymmetrieprüfung aus.

ANMERKUNG: Die Hardwaresymmetrie schlägt fehl, wenn eine der erforderlichen Konfigurationen mit einem „kritischen“ Fehler fehlschlägt. Überprüfen Sie die Empfehlungen und Details zum Beheben von Problemen, um Hardwaresymmetrie zu erzielen, und fahren Sie mit dem nächsten Schritt fort.

Wenn die Konfiguration mit einer Warnung fehlschlägt, bedeutet dies, dass die Konfiguration für die Cluster-Bereitstellung unterstützt werden kann, aber möglicherweise zu einer suboptimalen Cluster-Performance führt. Daher sollte sie überprüft werden.

Klicken Sie auf **Erneut ausführen**, um die Hardwaresymmetrieprüfung erneut auszuführen.

Wenn Sie fertig sind, klicken Sie auf **Weiter: Aktualisierungsquelle**.

5. Gehen Sie auf der Seite **Aktualisierungsquelle** wie folgt vor, um Compliance-Berichte für den validierten Azure Stack HCI-Katalog zu erstellen:
   a. Wählen Sie eine der Methoden zum Herunterladen von Katalogdateien aus:
      - **Online (HTTPS) – Updatekatalog für Microsoft HCI-Lösungen** zum automatischen Herunterladen des Katalogs von dell.com. Standardmäßig ist der Online-Katalog ausgewählt.

        Die Online-Katalogunterstützung erfordert eine direkte Internetverbindung vom Windows Admin Center-Gateway. Die Downloadzeit eines Katalogs hängt von der Netzwerkbandbreite und der Anzahl der zu aktualisierenden Komponenten ab.

        ANMERKUNG: Der Zugriff auf das Internet über Proxyeinstellungen wird nicht unterstützt.

      - **Dell EMC Repository Manager-Offline-Katalog** zur Verwendung des DRM-Katalogs, der in einem CIFS-Verzeichnis konfiguriert wurde.

        OMIMSWAC mit oder ohne Internetzugang ermöglicht Ihnen die Auswahl des Dell EMC Repository Manager-Offline-Katalogs, um den Compliance-Bericht zu generieren. Sie können diese Option verwenden, wenn Sie über keinen Internetzugang verfügen oder wenn Sie einen benutzerdefinierten DRM-Katalog verwenden möchten.

        - Um den Offline-Katalog zu verwenden, wählen Sie **DRM-Einstellungen** aus, um sicherzustellen, dass der CIFS-Freigabepfad mit dem DRM-Katalog konfiguriert ist. Informationen zum Erstellen eines DRM-Katalogs finden Sie im technischen Artikel.

   b. Um die Dell EMC System Update (DSU)- und die Inventory Collector (IC)-Tools zu verwenden, wählen Sie **Erweiterte Einstellungen** aus und wählen Sie dann eine der folgenden Optionen:
      - **Automatischer Download und Konfiguration von Dell EMC System Update (DSU) und Inventory Collector (IC)**, wenn OMIMSWAC mit dem Internet verbunden ist.
      - **Manuelle Konfiguration von DSU und IC** und wählen Sie dann **Einstellungen**, um die DSU- und IC-Tools manuell herunterzuladen und in einem freigegebenen Speicherort zu konfigurieren. Wir empfehlen die Verwendung dieser Option, wenn OMIMSWAC nicht mit dem Internet verbunden ist.

        Die DSU- und IC-Einstellungen, die mithilfe Einstellungen unter **Update-Tools** in OpenManage Integration-Erweiterung konfiguriert wurden, sind auch unter **Erweiterte Einstellungen** im OpenManage Integration-Snap-In verfügbar.

   Wenn Sie fertig sind, klicken Sie auf **Weiter: Compliance-Bericht**.

   OMIMSWAC lädt den Katalog herunter, erfasst die in der Registerkarte **Einstellungen** konfigurierten DSU- und IC-Tools und erzeugt einen Compliance-Bericht. Wenn die DSU- und IC-Tools nicht in den **Einstellungen** konfiguriert werden, lädt OMIMSWAC sie von https://downloads.dell.com herunter, um den Compliance-Bericht zu erzeugen.
6. Überprüfen Sie auf der Registerkarte **Compliance-Bericht** den Compliance-Bericht. Weitere Informationen über den Compliance-Bericht finden Sie unter Anzeigen des Compliance-Berichts.
   - Die aktualisierbaren Komponenten, die nicht konform sind, werden standardmäßig für das Update ausgewählt.

     Sie können die Auswahl der ausgewählten Komponenten aufheben oder die „nicht konformen“ Komponenten, für die ein Downgrade möglich ist, auswählen. Wenn Sie jedoch die Standardauswahl ändern möchten, stellen Sie sicher, dass die Abhängigkeiten zwischen der entsprechenden Komponenten-Firmware und den Treibern erfüllt sind.

   Wenn Sie fertig sind, klicken Sie auf **Weiter: Zusammenfassung**.
7. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die zu aktualisierenden Komponenten und klicken Sie dann auf **Weiter: Aktualisieren**, um die Cluster-Nodes zu aktualisieren.

   Eine Meldung wird angezeigt, die Sie dazu auffordert, CredSSP zu aktivieren.
   a. Klicken Sie auf **Ja**, um CredSSP zu aktivieren, und fahren Sie mit der Aktualisierung der ausgewählten Komponenten fort. Sie werden zum Fenster **Aktualisieren** weitergeleitet. Um die Sicherheit zu verbessern, deaktivieren Sie CredSSP, nachdem der Update-Vorgang abgeschlossen ist.

ANMERKUNG: Während das Update auf der Seite **Aktualisieren** durchgeführt wird, wird empfohlen, den Browser nicht zu beenden oder zu schließen. Wenn Sie den Browser schließen oder beenden, können Node-Updates fehlschlagen, und der Updatestatus wird möglicherweise nicht angezeigt.

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.

- Wenn der Update-Vorgang fehlschlägt, überprüfen Sie zum Troubleshooting die Protokolldateien, die unter dem folgenden Pfad gespeichert sind.
  - 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`
- Um den Compliance-Bericht erneut auszuführen, klicken Sie auf **Compliance erneut ausführen** und geben Sie bei Bedarf die Details der Compliance-Einstellungen an.

Ergebnisse

Nachdem die Hardwareaktualisierungen abgeschlossen sind, können Sie die Anweisungen im Windows Admin Center weiter befolgen, um den Azure Stack HCI-Cluster zu erstellen.

Hardwaresymmetrieprüfung

Eine Hardwaresymmetrieprüfung stellt sicher, dass die für einen Azure Stack HCI-Cluster ausgewählten Nodes unterstützt werden und über symmetrische Hardwarekonfigurationen verfügen, wie von Dell EMC empfohlen.

Azure Stack HCI Cluster funktioniert am besten, wenn die Hardwarekonfigurationen aller ausgewählten Nodes mit Dell EMC Empfehlungen konform sind.

Die Funktion „Integrierte Bereitstellung und Aktualisierung“ in OMIMSWAC hilft Ihnen bei der Verwaltung der Hardwaresymmetrie und der Aktualisierung von Nodes bei der Erstellung eines Azure Stack HCI-Clusters mithilfe von AX-Nodes (auf denen das Azure Stack HCI-Betriebssystem ausgeführt wird) in Windows Admin Center. Die Hardwaresymmetrieprüfung führt eine Reihe von Regeln auf Nodes aus und hilft Ihnen dabei, ihre Hardwarekonfigurationen an Dell EMC Empfehlungen auszurichten.

Bevor Sie einen Azure Stack HCI-Cluster erstellen, stellen Sie sicher, dass Sie alle Regeln der Hardwaresymmetrieprüfungen ausführen und einhalten.

Die Hardwaresymmetrieprüfungen dienen Folgendem:

- Ermitteln von Hardware- oder Konfigurationsproblemen, bevor ein Azure Stack HCI-Cluster in Produktion geht.
- Sicherstellen, dass der von Ihnen bereitgestellte Azure Stack HCI-Cluster zuverlässig ist und die Cluster-Performance optimal ist.

In diesem Thema werden die Hardwaresymmetrieregeln erläutert und Beispiele für unterstützte und nicht unterstützte Konfigurationen bereitgestellt. Informationen zu unterstützten und validierten Komponenten, die für die Hardwaresymmetrie erforderlich sind, finden Sie unter AS HCI-Supportmatrix. Wenn eine der Hardwaresymmetrieprüfungen mit dem Fehler „Kritisch“ oder „Warnung“ fehlschlägt, überprüfen Sie die Empfehlungen und zeigen Sie Details an, und wenden Sie sich an das Dell Support-Team, um das Problem zu beheben, bevor Sie mit dem nächsten Schritt fortfahren.

Der kritische Fehlerstatus besagt, dass dieser Aspekt der Node-Konfiguration nicht unterstützt wird. Sie müssen das Problem beheben, bevor Sie einen symmetrischen Azure Stack HCI-Cluster bereitstellen können. Und die Warnstatus besagen, dass dieser Aspekt der Node-Konfiguration für die Cluster-Bereitstellung unterstützt werden kann, aber möglicherweise zu einer suboptimalen Cluster-Performance führt. Daher sollte sie überprüft werden.

Symmetrieregeln

Prozessor

- Es wird empfohlen, dass sich in allen Nodes Prozessoren desselben Modells befinden. Die Verwendung von Nodes mit unterschiedlichen Prozessormodellen führt zu einer Warnmeldung.

  Beispiel: Wenn ein Node über einen Prozessor des x-Modells verfügt, sollten alle Prozessoren des x-Modells verwenden.

- Alle Nodes müssen die gleiche Anzahl an Prozessorsockeln haben. Die Verwendung von Nodes mit unterschiedlichen Prozessorsockeln führt zu Hardwaresymmetriefehlern.

Wenn beispielsweise ein Node über 2 Prozessorsockel verfügt, sollten alle 2 Prozessorsockel haben.

Speicher

- Wenn ein Node über persistenten Speicher verfügt, wird empfohlen, dass alle den persistenten Speicher mit derselben Anzahl und Kapazität haben. Die Verwendung von Nodes mit unterschiedlichen Anzahlen oder Kapazitäten des persistenten Speichers führt zu einer Warnmeldung.
- Es wird empfohlen, die gleiche Menge an physischem Speicher für alle Nodes zu haben. Wenn Sie physischen Speicher unterschiedlicher Kapazität verwenden, wird eine Warnung angezeigt.

Plattform

- Alle Nodes müssen über einen BOSS-Adapter verfügen. Die Verwendung von Nodes ohne BOSS-Adapter führt zu Hardwaresymmetriefehlern.

Storage

- Es wird empfohlen, für alle Nodes kompatible Laufwerke desselben Medientyps wie SSD, NVMe und HDD zu haben. Die Verwendung von Nodes mit inkompatiblen Laufwerken führt zu einer Warnmeldung.
- Alle Nodes müssen denselben Hostbusadapter (HBA) haben, mit Ausnahme von All-NVMe-Konfigurationen. Die Verwendung von Nodes mit unterschiedlichen HBA führt zu Hardwaresymmetriefehlern.

  Wenn beispielsweise ein Node HBA 330 hat, sollten alle denselben HBA 330 haben.

Netzwerk

- Es wird empfohlen, dass alle Nodes über kompatible Netzwerkadapter verfügen. Die Verwendung von Nodes mit inkompatiblen Netzwerkadaptern führt zu einer Warnmeldung.
- Mindestens ein RDMA-Netzwerkadapter muss auf allen Nodes gemeinsam sein. Die Verwendung von Nodes ohne gemeinsame Netzwerkadapter führt zu Hardwaresymmetriefehlern.

  Wenn beispielsweise ein Node QLogic Netzwerkadapter hat und andere Nodes Mellanox Netzwerkadapter haben, wird diese Konfiguration nicht unterstützt. In diesem Fall sollte mindestens ein gemeinsamer RDMA-Netzwerkadapter (QLogic oder Mellanox) in allen Nodes vorhanden sein.

Laufwerke

- Es wird empfohlen, dass alle Nodes kompatible Festplatten enthalten, wie in der AS HCI-Supportmatrixbeschrieben. Die Verwendung von Nodes mit inkompatiblen Festplatten führt zu einer Warnmeldung.
- Es wird empfohlen, dass alle Nodes bis zu zwei Medientypen enthalten sollten. Folgende Kombinationen von Medientypen werden unterstützt:
  - Persistenter Speicher und NVMe
  - Persistenter Speicher und SSD
  - NVMe und SSD
  - NVMe und HDD
  - SSD und HDD
  - All-NVMe
  - All-SSD

  Bei Verwendung einer Kombination von drei Medientypen, wie z. B. NVMe, SSD und HDD, werden Hardwaresymmetriefehler angezeigt.

- Es wird empfohlen, dass alle Nodes die Mindestanzahl an Laufwerken haben, die pro Medientyp benötigt werden.

  Wenn z. B. ein Node nur über 1 Medientyp SSD verfügt, sind mindestens 4 SSD-Laufwerke für die Kapazität erforderlich.

  Wenn ein Node 2 Medientypen hat, wie z. B. SSD und HDD, sind 2 SSD-Festplatten für Cache und 4 HDD-Laufwerke für die Kapazität erforderlich.

  Die Verwendung von Medientypen mit unterschiedlichen Laufwerken führt zu einer Warnmeldung.

- Es wird empfohlen, dass alle Laufwerke jedes Medientyps, wie z. B. SSD, NVMe und HDD, das gleiche Bus-Protokoll verwenden, wie z. B. SAS, SATA oder PCIe.

  Wenn beispielsweise ein Node über SSD- und HDD-Laufwerke mit SAS-Bus-Protokoll verfügt, sollten andere Nodes ebenfalls SSD- und HDD-Laufwerke mit SAS-Bus-Protokoll haben. Die Verwendung von Laufwerken mit unterschiedlichen Bus-Protokollen führt zu einer Warnung.

  ANMERKUNG: Es wird empfohlen, dass Laufwerke über ausgewählte Nodes hinweg dasselbe Bus-Protokoll haben, um eine symmetrische Konfiguration zu erhalten. Beispielsweise sind Nodes mit Laufwerkten wie SSD und HDD mit SATA- und SAS-Bus-Protokollen keine unterstützte Konfiguration.

- Es wird empfohlen, dass alle Nodes über Laufwerke gleicher Größe und Anzahl pro Medientyp verfügen.

  Wenn beispielsweise ein Node über 4 SSD-Festplatten mit einer Größe von 2 TB verfügt, sollten andere Nodes ebenfalls über 4 SSD-Laufwerke mit einer Größe von 2 TB verfügen. Wenn Nodes mit unterschiedlicher Anzahl und Kapazität verwendet werden, wird eine Warnung ausgegeben.

- Es wird empfohlen, dass die Laufwerke des SSD- oder NVMe-Medientyps für jeden Node die gleiche Lebensdauer haben.

  Wenn beispielsweise ein Node den 4 Mixed-Use-SSD-Festplattentyp verwendet, sollten andere Nodes ebenfalls den 4 Mixed-Use-SSD-Festplattentyp verwenden.

  Bei Verwendung von Nodes mit Laufwerken mit unterschiedlicher Lebensdauer, wie z. B. Leseintensiv, Mixed Use und schreibintensiv, wird eine Warnung ausgegeben.

- Wenn persistenter Speicher auf mindestens einem Node vorhanden ist, sollten alle verbleibenden Nodes, die für das Cluster ausgewählt werden, ebenfalls die gleiche Anzahl und Kapazität der persistenten Speichermodule enthalten. Die Verwendung von Nodes mit unterschiedlichen persistenten Speichermodulen führt zu einer Warnmeldung.

Beispielkonfigurationen

Hier sehen Sie einige unterstützte und nicht unterstützte Konfigurationen:

Nicht unterstützt: unterschiedliche Modelle zwischen Nodes

Die ersten beiden Nodes verwenden das AX-640-Modell, aber der dritte Node verwendet AX-740xd.

Node 1	Node 2	Node 3
AX-640	AX-640	AX-740xd

Dieser Vorgang wird nicht unterstützt. Alle Nodes sollten vom gleichen Modell sein.

Unterstützt: höchstens zwei Medientypen

Die unterstützte Konfiguration für zwei Medientypen lautet wie folgt:

Node 1	Node 2	Node 3	Node 4	Node 5
NVMe+SSD	NVMe+HDD	SSD+HDD	All-NVMe	All-SSD

Nicht unterstützt: mindestens die minimale Anzahl an Laufwerken

Wenn zwei Medientypen vorhanden sind:

Node 1	Node 2	Node 3
2 × SSD für Cache	2 × SSD für Cache	2 × SSD für Cache
3 × HDD für Kapazität	3 × HDD für Kapazität	3 × HDD für Kapazität

Dieser Vorgang wird nicht unterstützt. Nodes mit zwei Medientypen sollten 2 SSD-Festplatten für Cache und 4 HDD-Laufwerke für Kapazität haben.

Unterstützt: mindestens die minimale Anzahl an Laufwerken

Wenn zwei Medientypen vorhanden sind, werden folgende Konfigurationen unterstützt:

Node 1	Node 2	Node 3
2 × SSD für Cache	2 × SSD für Cache	2 × SSD für Cache
4 x HDD für Kapazität	4 x HDD für Kapazität	4 x HDD für Kapazität

Dies wird unterstützt. Nodes mit zwei Medientypen sollten 2 Cachelaufwerke (SSD/NVMe/AEP) und 4 Kapazitätslaufwerke (HDD/SSD/NVMe) haben.

Nicht unterstützt: Laufwerke mit unterschiedlichen Bus-Protokollen

Die ersten beiden Nodes verwenden die SSD-Festplatten mit SAS Bus-Protokoll. der dritte Node verwendet jedoch die SSD-Festplatte mit SATA Bus-Protokoll.

Node 1	Node 2	Node 3
SSD mit SAS-Protokoll	SSD mit SAS-Protokoll	SSD mit SATA-Protokoll

Die ersten beiden Nodes verwenden SSD- und HDD-Laufwerke mit SAS Bus-Protokoll. Der dritte Node verwendet jedoch das HDD-Laufwerk mit SATA Bus-Protokoll.

Node 1	Node 2	Node 3
SSD mit SAS-Protokoll	HDD mit SAS-Protokoll	HDD mit SATA-Protokoll

Diese werden nicht unterstützt. Laufwerke über Nodes hinweg sollten das gleiche Bus-Protokoll für die symmetrische Konfiguration verwenden.

Nicht unterstützt: Laufwerke mit gleicher Kapazität und unterschiedlicher Anzahl

Die ersten beiden Knoten verwenden 2 TB SSD und der letzte Node verwendet 3 TB SSD. Jeder Node verfügt über insgesamt 4 SSD-Laufwerke.

Node 1	Node 2	Node 3
4 x 2 TB-SSD	4 x 2 TB-SSD	4 x 3 TB-SSD

Dieser Vorgang wird nicht unterstützt. Alle Laufwerke jedes Medientyps (SSD/NVMe/HDD) sollten die gleiche Anzahl und Kapazität haben.

Nicht unterstützt: mindestens ein gleicher RDMA-Netzwerkadapter in allen Nodes vorhanden

Die ersten beiden Nodes verwenden den Qlogic Netzwerkadapter und der letzte Node verwendet einen Mellanox Netzwerkadapter.

Node 1	Node 2	Node 3
Qlogic Netzwerkadapter	Qlogic Netzwerkadapter	Mellanox Netzwerkadapter

Dieser Vorgang wird nicht unterstützt. Es sollte auf allen Nodes ein gemeinsamer Netzwerkadapter vorhanden sein.

Anzeigen der Ergebnisse der Hardwaresymmetrieprüfung

Nachdem die Hardwaresymmetrieprüfung abgeschlossen wurde, wird der Zusammenfassungsbericht angezeigt. Alle Regeln müssen mit einem grünen Häkchen oder in einigen Fällen einem gelben Dreieck (Warnung) übergeben werden. In der folgenden Tabelle werden die Symbole in der Zusammenfassung gezeigt und ihre Bedeutung erläutert:

Symbole	Beschreibung
	Die Hardwaresymmetrieprüfung wurde erfolgreich durchgeführt, was darauf hinweist, dass dieser Aspekt der Node-Konfiguration für die Clusterbereitstellung unterstützt wird.
	Die Hardwaresymmetrieprüfung produzierte eine Warnmeldung, die darauf hinweist, dass dieser Aspekt der Node-Konfiguration für die Clusterbereitstellung unterstützt werden kann, aber möglicherweise zu einer suboptimalen Cluster Performance führt. Daher sollte sie überprüft werden.
	Die Hardwaresymmetrieprüfung ist fehlgeschlagen und dieser Aspekt der Node-Konfiguration wird nicht unterstützt. Sie müssen das Problem beheben, bevor Sie einen symmetrischen Azure Stack HCI-Cluster bereitstellen können.

9

Clusterfähige Full-Stack-Aktualisierung für Azure Stack HCI-Cluster mithilfe des OpenManage Integration-Snap-In

Durch die Verwendung der clusterfähigen Full-Stack-Aktualisierungsfunktion im OpenManage Integration-Snap-In können Sie Hardware-Updates (Firmware, BIOS und Treiber) auf Dell EMC Integrated System für Microsoft Azure Stack HCI (auch bekannt als Azure Stack HCI)-Cluster-Nodes zusätzlich zum im Windows Admin Center verfügbaren Betriebssystem-Update durchführen.

Um die neuesten Funktionen zu erhalten, die neuesten Sicherheitskorrekturen anzuwenden und die Infrastruktur fehlerfrei zu halten, müssen Sie sicherstellen, dass die Ziel-Nodes mit den neuesten Betriebssystem- und Hardware-Updates wie Firmware, BIOS und Treiber aktualisiert werden. Viele Betriebssystem- und Hardware-Updates erfordern möglicherweise einen Neustart der Nodes, um die Änderungen zu übernehmen. Der Neustartvorgang kann sich auf die Workload oder Anwendungen auswirken, die auf dem Node ausgeführt werden.

Durch die Verwendung von OpenManage Integration-Snap-In, das in den Workflow für die Windows Admin Center-Clusteraktualisierung integriert ist, können Sie die Firmware, das BIOS und die Treiber auf Ziel-Nodes zusätzlich zum im WAC verfügbaren Betriebssystem-Update nahtlos aktualisieren. Außerdem wird die Anzahl der nach der Aktualisierung erforderlichen Neustarts mithilfe der CAU-Funktion für den vollständigen Stack reduziert.

Um die Funktion für die Aktualisierung des vollständigen Stacks aufzurufen, wählen Sie in Windows Admin Center im Menü **Extras** die Option **Aktualisierungen** aus.

Um Hardware-Updates separat auf dem Cluster durchzuführen, verwenden Sie die clusterfähige Aktualisierungsfunktion, die in OpenManage Integration im Windows Admin Center-Erweiterungstool verfügbar ist. Informationen dazu finden Sie unter Aktualisieren der PowerEdge-Server und -Nodes der Windows Server HCI, Azure Stack HCI und Failover-Cluster mit OpenManage Integration-Erweiterung auf Seite 20.

Themen:

- Aktualisieren eines Azure Stack HCI-Clusters mithilfe des OpenManage Integration-Snap-In

Aktualisieren eines Azure Stack HCI-Clusters mithilfe des OpenManage Integration-Snap-In

Voraussetzungen

Bevor Sie mit dem Firmware-, BIOS- und Treiberupdate beginnen, überprüfen Sie, ob die folgenden Voraussetzungen erfüllt sind:

- Stellen Sie sicher, dass Sie Windows Admin Center 2103.2 GA installiert haben.
- Stellen Sie sicher, dass Sie mithilfe der Anmeldeinformationen des Domänenadministrators remote auf Windows Admin Center zugreifen. Andernfalls verwenden Sie lokale Administrator-Anmeldedaten, um lokal auf WAC zuzugreifen. Weitere Informationen finden Sie in der Microsoft Dokumentation.
- Stellen Sie sicher, dass das Dell EMC Integrated System für Microsoft Azure Stack HCI (auch bekannt als Azure Stack HCI)-Cluster von AX-Nodes erstellt wird, auf denen das Betriebssystem Azure Stack HCI Version 20H2 ausgeführt wird.
- Stellen Sie sicher, dass die OMIWAC Premium-Lizenz auf jedem AX-Node installiert ist.
- Stellen Sie sicher, dass Sie die Microsoft Failover-Cluster-Tool Extension 1.280.0.nupkg im Microsoft NuGet-Windows Admin Center-Feed installiert haben.
- Stellen Sie sicher, dass das Skript vor dem Update und das Skript nach dem Update nicht als Teil der Clusterrolle vorhanden ist. Wenn es vorhanden ist, wird empfohlen, das Skript vor dem Auslösen von Aktualisierungen zu entfernen. Weitere Informationen finden Sie auf der Seite Übersicht über Tests im *Abschnitt „Troubleshooting“*.
- Stellen Sie sicher, dass OMIMSWAC mit dem Internet verbunden ist, um Online-Kataloge verwenden zu können. Sie können auch Proxyeinstellungen zum Herunterladen von Katalog-, DSU- und IC-Dienstprogrammen über das Internet verwenden, um nur Compliance-Berichte zu erstellen. Weitere Informationen zu den Proxyeinstellungen finden Sie unter Konfigurieren von Proxyeinstellungen.

- Um den DRM-Offline-Katalog zu verwenden, stellen Sie sicher, dass die Einstellungen wie unter Konfigurieren der Einstellungen des Updatetools beschrieben konfiguriert werden.
- Wenn Sie vom Snap-In dazu aufgefordert werden, die Anmeldeinformationen für „Verwalten als“ anzugeben, geben Sie die entsprechenden Anmeldeinformationen für den Cluster-Administrator an, um den verwalteten Node zu authentifizieren. Aktivieren Sie anschließend das Kontrollkästchen **Diese Anmeldedaten für alle Verbindungen verwenden**. Stellen Sie außerdem sicher, dass der Benutzer Teil der lokalen Nutzergruppe von Gateway-Administratoren ist. Weitere Informationen finden Sie unter Anforderungen und Best Practices für clusterfähiges Aktualisieren in der Microsoft Dokumentation.

Info über diese Aufgabe

Die clusterfähige Full-Stack-Aktualisierungsfunktion wird für Dell EMC Integrated System für Microsoft Azure Stack HCI mit Azure Stack HCI Version 20H2-Betriebssystem unterstützt.

Schritte

So führen Sie Betriebssystem- und Hardware-Updates auf Azure Stack HCI Cluster-Nodes aus:

1. Wählen Sie in Windows Admin Center im Menü **Extras** die Option **Updates** aus.
   a. Sie müssen den Credential Security Service Provider (CredSSP) aktivieren und explizite Anmeldeinformationen bereitstellen. Wenn Sie gefragt werden, ob CredSSP aktiviert werden soll, klicken Sie auf **Ja**.

   Die Seite **Updates** wird angezeigt.
2. Informationen zum Aktualisieren des Betriebssystems finden Sie in der Azure Stack HCI-Dokumentation unter Microsoft.
3. Wählen Sie auf der Seite **Updates installieren** nach dem Überprüfen der Betriebssystem-Updates die Option **Weiter: Hardware-Updates** aus.
4. Windows Admin Center prüft, ob die unterstützte Dell EMC OpenManage Integration-Erweiterung installiert wurde.
   - Wenn die Erweiterung nicht installiert ist, klicken Sie auf **Installieren**, um die Lizenzvereinbarungen zu akzeptieren und das OpenManage Integration-Snap-In zu installieren.
   - Wenn die OpenManage Integration-Erweiterung Version 2.0 bereits installiert ist oder nachdem das OpenManage Integration-Snap-In installiert ist, klicken Sie auf **Aktualisierungen erhalten**, um zur Seite „Hardwareaktualisierungen“ zu wechseln.

   Nach der Installation des OpenManage Integration-Snap-In wird die OpenManage Integration-Erweiterung Version 2.0 im Menü **Extras** im Windows Admin Center angezeigt. Sie werden in der Lage sein, alle Funktionen der OpenManage Integration-Erweiterung zusammen mit den Snap-In-spezifischen Funktionen zu verwenden.
5. Überprüfen Sie auf der Seite **Hardwareaktualisierungen** die aufgeführten Voraussetzungen, um sicherzustellen, dass alle Nodes für die Hardwareaktualisierungen bereit sind. Wenn Sie fertig sind, klicken Sie auf **Weiter: Updatequelle**. Klicken Sie auf **Erneut ausführen**, um die Voraussetzungen erneut auszuführen.

   Sie müssen alle Voraussetzungen erfüllen, die auf der Registerkarte **Voraussetzungen** aufgeführt sind. Andernfalls können Sie nicht mit dem nächsten Schritt fortfahren.
6. Gehen Sie auf der Seite **Updatequelle** wie folgt vor, um Compliance-Berichte für den validierten Azure Stack HCI-Katalog zu erstellen:
   a. Wählen Sie eine der Methoden zum Herunterladen von Katalogdateien aus:
      - **Online (HTTPS) – Updatekatalog für Microsoft HCI-Lösungen** zum automatischen Herunterladen des Katalogs von Dell.com. Der Online-Katalog ist standardmäßig ausgewählt.

        Die Online-Katalogunterstützung erfordert eine direkte Internetverbindung vom Windows Admin Center-Gateway. Die Downloadzeit eines Katalogs hängt von der Netzwerkbandbreite und der Anzahl der zu aktualisierenden Komponenten ab.

        ANMERKUNG: Der Zugriff auf das Internet über Proxyeinstellungen wird nicht unterstützt.

      - **Dell EMC Repository Manager-Offline-Katalog** zur Verwendung des DRM-Katalogs, der in einem CIFS-Verzeichnis konfiguriert wurde.

        OMIMSWAC mit oder ohne Internetzugang ermöglicht Ihnen die Auswahl des Dell EMC Repository Manager-Offline-Katalogs, um den Compliance-Bericht zu generieren. Sie können diese Option verwenden, wenn Sie über keinen Internetzugang verfügen oder wenn Sie einen benutzerdefinierten DRM-Katalog verwenden möchten.

        - Um den Offline-Katalog zu verwenden, wählen Sie **DRM-Einstellungen** aus, um sicherzustellen, dass der CIFS-Freigabepfad mit dem DRM-Katalog konfiguriert ist. Informationen zum Erstellen eines DRM-Katalogs finden Sie im technischen Artikel.

   b. Um die Dell EMC System Update (DSU)- und die Inventory Collector (IC)-Tools zu verwenden, wählen Sie **Erweiterte Einstellungen** aus und wählen Sie dann eine der folgenden Optionen:
      - „Automatischer Download und Konfiguration von Dell EMC System Update (DSU) und Inventory Collector (IC)“, wenn OMIMSWAC mit dem Internet verbunden ist.

- „Manuelle Konfiguration von DSU und IC“ und wählen Sie dann **Einstellungen**, um die DSU- und IC-Tools manuell herunterzuladen und in einem freigegebenen Speicherort zu konfigurieren. Wir empfehlen die Verwendung dieser Option, wenn OMIMSWAC nicht mit dem Internet verbunden ist.

  Die DSU- und IC-Einstellungen, die mithilfe Einstellungen unter **Update-Tools** in OpenManage Integration-Erweiterung konfiguriert wurden, sind auch unter **Erweiterte Einstellungen** im OpenManage Integration-Snap-In verfügbar.

Wenn Sie fertig sind, klicken Sie auf **Weiter: Compliance-Bericht**.

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

7. Überprüfen Sie auf der Registerkarte **Compliance-Bericht** den Compliance-Bericht. Weitere Informationen über den Compliance-Bericht finden Sie unter Anzeigen des Compliance-Berichts.
   - Die aktualisierbaren Komponenten, die nicht konform sind, werden standardmäßig für das Update ausgewählt.

     Sie können das Kontrollkästchen neben den ausgewählten Komponenten deaktivieren oder die „nicht konformen“ Komponenten, für die ein Downgrade möglich ist, auswählen. Wenn Sie jedoch die Standardauswahl ändern möchten, stellen Sie sicher, dass die Abhängigkeiten zwischen der entsprechenden Komponenten-Firmware und den Treibern erfüllt sind.

   Wenn Sie fertig sind, klicken Sie auf **Weiter: Zusammenfassung**.

8. Überprüfen Sie auf der Registerkarte **Zusammenfassung** die Komponenten, die aktualisiert werden sollen, und klicken Sie dann auf **Weiter: Aktualisierungen herunterladen**, um die Aktualisierungen für die ausgewählten Komponenten herunterzuladen.

   ANMERKUNG: Während der Download durchgeführt wird, wird empfohlen, den Browser nicht zu beenden oder zu schließen. Wenn Sie den Browser schließen oder beenden, schlägt der Download des Updatevorgangs möglicherweise fehl.

   Der Download-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 Download-Vorgang abgeschlossen ist.

   - Wenn der Download-Vorgang fehlschlägt, überprüfen Sie zum Troubleshooting die Protokolldateien, die unter dem folgenden Pfad gespeichert sind.
     - 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`
     - Nachdem das Clusterupdate abgeschlossen ist, sind die Protokolle für einzelne Nodes im Ordner `<Windows Directory>\Temp\OMIMSWAC` auf den entsprechenden Nodes zu finden.
   - Um den Compliance-Bericht erneut auszuführen, klicken Sie auf **Compliance erneut ausführen** und wiederholen Sie die Schritte 4 bis 7.

9. Nachdem die Updates heruntergeladen wurden, befolgen Sie die Anweisungen im Windows Admin Center, um Betriebssystem- und Hardwareaktualisierungen zu installieren.

   Wenn die UI-Sitzung aktiv ist, wird der Fortschrittsstatus auf Node-Ebene angezeigt. Windows Admin Center benachrichtigt, sobald das Update abgeschlossen ist.

Ergebnisse

Wenn für eine der Aktualisierungen ein Neustart erforderlich ist, werden die Nodes nacheinander neu gestartet. Dabei werden Cluster-Rollen wie VMS zwischen Nodes verschoben, um Ausfallzeiten zu vermeiden.

Nächste Schritte

ANMERKUNG: Die CAU-Clusterrolle ist standardmäßig so konfiguriert, dass die selbst aktualisierenden Funktionen des Clusters am Dienstag in der dritten Woche jedes Monats ausgelöst werden. Stellen Sie daher nach Abschluss des Updates sicher, dass die CAU-Clusterrolle in einem Cluster-Node deaktiviert wird, um die selbst aktualisierbare Funktion des Clusters zu unterbinden. Weitere Informationen über die Deaktivierung der CAU-Clusterrolle finden Sie unter https://docs.microsoft.com/en-us/powershell/module/clusterawareupdating/disable-cauclusterrole?view=win10-ps

10

Troubleshooting

Themen:

- Aktualisieren von
- Lizenzierung
- Protokolle
- Funktionsstatus, Hardware und iDRAC-Bestandsaufnahme
- Blinken und Blinken beenden
- Cluster-fähiges Update
- Clusterfähige Full-Stack-Aktualisierung
- Andere

Aktualisieren von

Installation der Erweiterung fehlgeschlagen

Wenn Sie versuchen, OpenManage Integration Snap-In während der Erstellung oder dem Update des Azure Stack HCI Cluster zu installieren, kann die Installation der Erweiterung fehlschlagen.

Grund: Eine ältere Version der Erweiterung (OMIMSWAC 1.1.1 oder früher) wurde möglicherweise bereits installiert.

Auflösung:

- Deinstallieren Sie die ältere Version und installieren Sie dann das OpenManage Integration-Snap-In während der Erstellung oder des Updates des Azure Stack HCI-Clusters. Weitere Informationen finden Sie im Abschnitt *Installieren von Dell EMC OpenManage Integration in Microsoft Windows Admin Center* im OMIMSWAC-Installationshandbuch.
- Wechseln Sie zur Registerkarte **Erweiterungen** > **Installierte Erweiterungen**, um von früheren Versionen auf das OpenManage Integration-Snap-In zu aktualisieren. Wählen Sie die Dell EMC OpenManage Integration-Erweiterung mit dem Status „Update verfügbar (Version)“ aus und klicken Sie dann auf **Aktualisieren**.

Lizenzierung

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 einer 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.

Protokolle

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 Updatebenachrichtigungen: `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 des Updates 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.

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`

Funktionsstatus, Hardware und iDRAC-Bestandsaufnahme

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.
- Der USB-NIC-Adapter ist auf dem Ziel-Node-Betriebssystem nicht deaktiviert.

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

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

- YX3X- und YX2X-Modelle von PowerEdge-Servern werden mit der neuesten iDRAC-Version von 2.60.60.60 oder höher aktualisiert.
- YX4X-Modelle von PowerEdge-Servern werden mit der neuesten iDRAC-Version von 3.30.30.30 oder höher aktualisiert.
- 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.

Funktionszustand und Hardware-Bestandsaufnahme von YX2X-, YX3X- und YX4X-Modellen von PowerEdge-Servern werden nicht angezeigt

- Stellen Sie sicher, dass YX3X- und YX2X-Modelle von PowerEdge-Servern mit der neuesten iDRAC-Version von 2.60.60.60 oder höher aktualisiert werden.
- Stellen Sie sicher, dass die YX4X-Modelle der PowerEdge-Server mit der neuesten iDRAC-Version von 3.30.30.30 oder höher aktualisiert werden.

Der Gesamtfunktionszustand zeigt „Warnung“ oder „kritisch“ an, während der Funktionszustand der Node-Komponenten fehlerfrei ist

Der Gesamtfunktionsstatus der PowerEdge-Server, Failover-Cluster und HCI-Cluster wird möglicherweise als „Kritisch“ oder „Warnung“ angezeigt, obwohl die Komponenten der Nodes, die im Windows Admin Center angezeigt werden, fehlerfrei sind. Der Funktionszustand von physischen Festplatten, die mit dem integrierten SATA-Controller verbunden sind, wird möglicherweise als unbekannt angezeigt, da iDRAC die Integritätsinformationen für diese Festplatten nicht erhalten kann.

Weitere Informationen zu den Komponenten mit dem Funktionsstatus „Kritisch“ finden Sie in der entsprechenden iDRAC-Konsole.

Auf dem Ziel-iDRAC-Gerät können keine Benutzer erstellt werden.

Wenn der Sperrmodus auf dem YX4X-Modell der PowerEdge-Server und höher aktiviert ist, schlägt die Bestandsaufnahme von Integrität, Hardware und iDRAC mit folgendem Fehler fehl: „Auf dem Ziel-iDRAC-Gerät können keine Benutzer erstellt werden."

Lösung: Deaktivieren Sie den Sperrmodus auf dem Ziel-Node, der von Dell EMC OpenManage Integration verwaltet wird.

Die OMIMSWAC-Erweiterung kann nicht initialisiert werden.

Das Abrufen der Bestandsaufnahme von Servern und Cluster-Nodes kann mit folgendem Fehler fehlschlagen: „Die OMIMSWAC-Erweiterung kann nicht initialisiert werden."

Lösung: Stellen Sie sicher, dass der IPMI-Treiber installiert ist und der IPMI-Dienst auf dem Ziel-Node ausgeführt wird. Weitere Informationen zu den Anforderungen und Lösungen finden Sie unter Dell Information Center.

Blinken und Blinken beenden

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.

Cluster-fähiges Update

Job fehlgeschlagen, während die erforderlichen Komponenten für den Aktualisierungs-Compliance-Vorgang heruntergeladen wurden

Beim Herunterladen der DSU- und IC-Tools können die Updatejobs aus verschiedenen Gründen fehlschlagen. Die möglichen Ursachen und Lösungen werden nachfolgend aufgeführt:

- **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.

Die DUP(s) kann/können nicht heruntergeladen werden.

- Stellen Sie sicher, dass Sie mithilfe von Domänennutzer-Zugangsdaten remote auf Windows Admin Center zugreifen. Andernfalls verwenden Sie lokale Administrator-Anmeldedaten, um lokal auf WAC zuzugreifen. Weitere Informationen finden Sie in der Microsoft Dokumentation.
- Überprüfen Sie die Internetverbindung oder die Proxy-Konfiguration.

Compliance-Bericht kann nicht erzeugt werden

- **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.

- **Ursache**: Bei der Erstellung von Compliance-Berichten erscheint möglicherweise folgende Fehlermeldung: `Unable to install Dell System Update(DSU) package for the server/cluster because DSU installation operation is already in progress for another server/cluster`. Dies kann passieren, wenn ein Nutzer versucht, Compliance in zwei verschiedenen Instanzen/Sitzungen gleichzeitig auszuführen. Beispiel: Die erste Instanz wäre das Klicken auf die Popup-Schaltfläche und die zweite die gleichzeitige Verwendung eines Browsers im gleichen Gateway. Die zuerst ausgelöste Instanz/Sitzung führt Compliance/Update wie gewohnt aus, während die zweite zu einer Fehlermeldung führt.

  Lösung: Führen Sie jeweils nur eine Instanz von Compliance/Update für einen Ziel-Node/-Cluster in einer Gateway-Instanz aus.

Seite „Compliance-Bericht“ über einen langen Zeitraum im Ladestatus

Während der Erstellung eines Compliance-Berichts wird die Seite „Compliance-Bericht“ möglicherweise auch nach der Benachrichtigung des erfolgreich erzeugten Update-Compliance-Berichts im Ladestatus angezeigt.

In diesem Fall wechseln Sie zu einer der anderen Registerkarten, wie z. B. „Einstellungen“, „Bestandsaufnahme“ usw., und gehen Sie dann zurück zur Registerkarte „Aktualisieren“, auf der Sie nun den erzeugten Compliance-Bericht sehen können.

Job ist beim Aktualisieren der ausgewählten Komponenten fehlgeschlagen

Manchmal können CAU oder die Ziel-Node-Aktualisierungen aus verschiedenen Gründen fehlschlagen. Mögliche Ursachen und Lösungen sind nachfolgend aufgeführt:

- **Ursachen**: Wenn die Ziel-Nodes vor dem Auslösen von CAU nicht validiert wurden, kann CAU fehlschlagen.

  Lösung: Stellen Sie für eine clusterfähige Aktualisierung sicher, dass Sie das Cluster validieren, bevor Sie CAU auslösen. Weitere Informationen zum Validieren eines Clusters finden Sie im Microsoft-Dokument Hardware für ein Cluster validieren.

- **Ursachen**: Wenn die Failover-Clustering-Funktion und die Failover-Clustering-Tools nicht auf den Ziel-Nodes installiert sind, kann CAU fehlschlagen.

  Lösung: Da OMIMSWAC die Microsoft clusterfähige Aktualisierungsfunktion für Cluster-Aktualisierungen verwendet, müssen Sie vor dem Aktualisieren eines Clusters über OMIMSWAC sicherstellen, dass die Failover-Clustering-Funktion und die Failover-Clustering-Tools auf allen Ziel-Nodes installiert sind. Weitere Informationen finden Sie unter CAU-Anforderungen und Best Practices in der Microsoft Dokumentation.

  Um zu überprüfen, ob die Failover-Clustering-Tools auf allen Ziel-Nodes ausgeführt werden, führen Sie im Fenster „PowerShell“ des Ziel-Node den PowerShell-Befehl `Get-CauClusterRole` aus.

- **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 das Serverupdate 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 Funktionszustand aufweist, finden Sie in der Microsoft Dokumentation Anleitungen, wie Sie es in einen fehlerfreien Zustand 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.

- **Ursache**: CAU schlägt fehl, wenn die Failover-Clustering-Funktion und die Failover-Clustering-Tools nicht auf allen Ziel-Nodes installiert sind.

  Lösung: Stellen Sie sicher, dass die Failover-Clustering-Funktion und die Failover-Clustering-Tools auf allen Ziel-Nodes installiert sind, bevor Sie CAU durchführen. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/windows-server/failover-clustering/cluster-aware-updating-requirements.

Ausfall von CredSSP

Überprüfen Sie die Ereignisanzeigeprotokolle im Gateway-System, um sicherzustellen, dass CredSSP während der clusterfähigen Aktualisierung nicht fehlgeschlagen ist. Wenn der CredSSP fehlschlägt, sind im Folgenden die wahrscheinlichen Ursachen und Lösungen aufgeführt:

- **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` im PowerShell aus.

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 (zum Update 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 unter `<Windows Directory>\Dell\UpdatePackage\log\<Package Name>` angegebenen Rückgabecode. 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 das Komponentenupdate von OMIMSWAC erneut aus. Weitere Informationen zur Deinstallation von Treibern finden Sie im Microsoft-Dokument.
- Nach dem Cluster-Update werden möglicherweise Komponenten als nicht konform angezeigt. Dies geschieht aufgrund eines DUP-Fehlers.

  Lösung: Überprüfen Sie in diesem Fall die Bereinigungsprotokolle mit den DSU-Protokollen, um festzustellen, ob für die Komponenten 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.

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.

Clusterfähige Full-Stack-Aktualisierung

Clusterfähige Aktualisierungen konnten nicht konfiguriert werden

Ursache: Beim Durchführen von Full-Stack-Aktualisierungen kann in Windows Admin Center ein Fehler auftreten, wenn Sie **Updates** im Menü **Extras** auswählen: `Couldn't configure cluster aware updates`. Dieser Fehler tritt auf, weil die CAU-Clusterrolle nicht zum Cluster zum Update hinzugefügt werden konnte.

Lösung: Um dieses Problem zu umgehen, können Sie die Clusterrolle mithilfe des folgenden PowerShell-Befehls manuell hinzufügen, bevor Sie das Full-Stack-Update auslösen: `Add-CauClusterRole -StartDate "02-03-2021 3:00:00 AM" -DaysOfWeek Tuesday -WeeksOfMonth 3 -EnableFirewallRules -RequireAllNodesOnline -Force`

Weitere Informationen finden Sie unter Konfigurieren der Nodes für die Remote-Verwaltung in der Microsoft Dokumentation.

Bereitschaft für clusterfähige Aktualisierungen konnte nicht abgefragt werden

Ursache: Beim Durchführen von Full-Stack-Aktualisierungen kann in Windows Admin Center ein Fehler auftreten, wenn Sie **Updates** im Menü **Extras** auswählen: `Couldn't query readiness for cluster aware updates`. Dieser Fehler tritt aufgrund eines Ausfalls von CredSSP auf.

Lösung: Um dieses Problem zu umgehen, suchen Sie unter Ausfall von CredSSP nach Ursache und Lösung.

Weitere Informationen finden Sie in der Microsoft Dokumentation.

Die Seite „Testzusammenfassung“ wird angezeigt.

Beim Auslösen von Full-Stack-Aktualisierungen wird möglicherweise die Seite „Testzusammenfassung“ angezeigt.

Lösung: Um dieses Problem zu umgehen, überprüfen Sie, ob das Skript „Vor dem Update“ oder „Nach dem Update“ zur Clusterrolle gehört. Falls vorhanden, entfernen Sie die Skripte aus dem Cluster-Node, indem Sie den folgenden Befehl in PowerShell ausführen: `Set-CauClusterRole -PreUpdateScript $null -PostUpdateScript $null`. Weitere Informationen zu den Voraussetzungen, die für das Clusterupdate erforderlich sind, finden Sie in der Microsoft Dokumentation.

Aktualisierung des Updatestatus dauert länger

Während der Aktualisierung des Full-Stack-Clusters kann der Aktualisierungsstatus, der auf der Seite **Updates** angezeigt wird, länger dauern. In diesem Fall wird empfohlen, auf der Seite „Updates“ zu bleiben und zu warten, bis die Aktualisierung abgeschlossen ist. Der Updatestatus wird automatisch angezeigt, sobald das Update abgeschlossen ist. Weitere Information zur Microsoft Empfehlungen finden Sie in der Microsoft Dokumentation.

Das vollständige Stapelupdate schlägt möglicherweise mit Failover-Cluster-Toolerweiterung 1.271.0 nupkg fehl.

Bei vollständigen Stapel-Cluster-Updates in Azure Stack HCI-Clustern schlägt das Update möglicherweise fehl und ein Ausnahmefehler wird angezeigt: RemoteException: Exception calling "Add" with "2" argument(s): "Item has already been added. Key in dictionary: 'PreUpdateScript' Key being added: 'PreUpdateScript'". Dieses Problem tritt auf, wenn Microsoft Failover-Cluster-Toolerweiterung 1.271.0 installiert ist. Aufgrund dieses Problems können sowohl Hardware- als auch Betriebssystem-Cluster-fähige (vollständiges Stapelupdate) nicht zusammen durchgeführt werden.

Lösung: Aktualisieren Sie auf die neueste Microsoft Failover-Cluster-Tool-Erweiterung 1.280.0.nupkg, die im Microsoft-Feed verfügbar ist, um ein vollständiges Stack-Cluster-Update durchzuführen.

Andere

Zugriff auf OpenManage Integration verweigert

Ursache: Wenn Sie sich beim Windows Admin Center (WAC) mit Gateway-Nutzerzugangsdaten 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.

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.

Speichern der Annahme fehlgeschlagen: Dell EMC Softwarelizenzvereinbarung und Kundenhinweis

Ursache: Beim Speichern der Annahme von Dell EMC Softwarelizenzvereinbarung und Kundenhinweisen tritt möglicherweise ein Fehler auf. Dies kann passieren, wenn Sie mehrere Instanzen der Dell EMC OpenManage Integration-Erweiterung von demselben Gateway

starten und Bedingungen und Bestimmungen in einer Instanz akzeptieren. Dieser Fehler tritt auf, wenn Sie in den verbleibenden Instanzen versuchen, die Bedingungen und Bestimmungen zu akzeptieren.

Lösung: Verlassen Sie die Dell EMC OpenManage Integration-Erweiterung, in der dieses Problem auftritt, und wechseln Sie wieder zu ihr, um dieses Problem zu beheben.

11

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

12

Kontaktaufnahme mit Dell EMC

Info über diese Aufgabe

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:

Schritte

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 in Microsoft Windows Admin Center-Erweiterung (auch bekannt als OpenManage Integration-Erweiterung)	Mit Dell EMC OpenManage Integration in Microsoft Windows Admin Center (OMIMSWAC) können IT-Administratoren die PowerEdge-Server als Hosts, Microsoft Failover-Cluster (erstellt mit PowerEdge-Servern), Dell EMC HCI-Lösungen für Microsoft Windows Server (erstellt mithilfe von AX-Nodes und/oder Storage Spaces Direct Ready Nodes) und Dell EMC Integrated System für Microsoft Azure Stack HCI (erstellt mithilfe von AX-Nodes) verwalten. OMIMSWAC vereinfacht die Aufgaben von IT-Administratoren durch die Remote-Verwaltung der PowerEdge-Server und -Cluster während des gesamten Lebenszyklus.
OpenManage-Integration-Snap-In	Das OpenManage Integration Snap-In ist in den Windows Admin Center-Cluster-Erstellungs- oder Cluster-Aktualisierungsworkflow integriert, um die Erstellung und Aktualisierung von Clustern zu verbessern und die Anzahl der erforderlichen Neustarts bei der Erstellung eines Clusters zu reduzieren. Nachdem das OpenManage Integration Snap-In installiert wurde, wird die OpenManage Integration-Erweiterung im Menü **Extras** im Windows Admin Center angezeigt. Sie werden in der Lage sein, alle Funktionen der OpenManage Integration-Erweiterung zusammen mit den Snap-In-spezifischen Funktionen zu verwenden.
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.

Tabelle 4. Glossar (fortgesetzt)

Abkürzungen/Akronyme	Definition
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.
iDRAC	Integrated Dell Remote Access Controller
IPMI	Intelligent Platform Management Interface
LED	Leuchtdiode (Light-Emitting Diode; LED)
Netzwerkadapter	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) – Aktualisierungskatalog für Microsoft HCI-Lösungen	Empfohlen für Windows Server (erstellt mithilfe von AX-Nodes und/oder Storage Spaces Direct Ready Nodes) und Azure Stack HCI-Clustern (erstellt mithilfe von AX-Nodes).
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	Universeller serieller Bus
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) – Aktualisierungskatalog für Microsoft HCI-Lösungen
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)