

ActiveProtect Seitenwiederherstellung

Basierend auf APM 1.1

Synology

Letzte Aktualisierung: 27. Nov 2025

Inhaltsverzeichnis

Einleitung	2
Herausforderungen	2
ActiveProtect-Systemwiederherstellung	2
Serverausfälle	3
Häufige Ausfälle	3
Standort-Wiederherstellung	5
Standortkonfiguration identifizieren	5
Ausfall des Backup-Servers	6
Ausfall des Management-Servers	8
Fazit	12

Einleitung

ActiveProtect bietet zentrales Management für Ihre Backup-Infrastruktur und erleichtert so die Wiederherstellung Ihrer Umgebung bei Hardwareausfällen, Verbindungsproblemen oder Cyberangriffen. Diese Wiederherstellungsverfahren helfen, Backup-Dienste wiederherzustellen, den Schutz Ihrer Workloads aufrechtzuerhalten und das Risiko von Datenverlusten zu verringern.

Dieser Leitfaden beschreibt die häufigsten Serverausfälle und bietet Schritt-für-Schritt-Anleitungen zur Wiederherstellung.

Herausforderungen

Die Verfügbarkeit von Backups aufrechtzuerhalten, bringt verschiedene Herausforderungen mit sich. Hardwarekomponenten wie Mainboards oder Festplatten können unerwartet ausfallen, und selbst ein kurzer Ausfall des Verwaltungsservers kann die Synchronisierung und Überwachung stören. Bedrohungen der Cybersicherheit, insbesondere Ransomware, stellen zusätzliche Risiken dar, die sowohl Backup-Daten als auch Standortkonfigurationen betreffen können.

Ohne einen sekundären Verwaltungsserver oder externe Backup-Kopien können diese Ausfälle schwerwiegende Folgen haben, die Wiederherstellung verzögern und den Betrieb erschweren.

ActiveProtect-Systemwiederherstellung

ActiveProtect begegnet diesen Herausforderungen, indem das Management von Backup-Servern, externem Speicher und Workloads an einem einzigen Standort zentralisiert wird. Diese einheitliche Architektur erleichtert den Schutz von Daten und eine schnelle Wiederherstellung im Problemfall.

Um sicherzustellen, dass Daten wiederherstellbar bleiben und der normale Betrieb nach einem Serverausfall schnell wieder aufgenommen werden kann, empfehlen wir die folgenden zentralen Maßnahmen:

- Implementieren Sie eine [3-2-1-Backup-Strategie](#).
- Konfigurieren Sie einen sekundären Verwaltungsserver für das [Management-Switchover](#).

Weitere Informationen zur Einrichtung Ihres ActiveProtect-Systems finden Sie unter [Infrastrukturkomponenten](#) und [Bereitstellungsszenarien](#).

Serverausfälle

Wenn ein Backup- oder Verwaltungsserver einen Ausfall erleidet, erhalten Sie in der Regel Benachrichtigungen, die Ihnen helfen, die Probleme schnell zu erkennen. Wir empfehlen, [Benachrichtigungen einzurichten](#), um bei Problemen Hardware- und Verbindungswarnungen zu erhalten.

Nachdem Sie eine Warnung erhalten haben, besteht der nächste Schritt darin, zu verstehen, welche Art von Ausfall aufgetreten sein könnte. Im Folgenden finden Sie einige häufige Ausfallarten und deren Auswirkungen auf Ihr ActiveProtect-System.

Häufige Ausfälle

Netzwerkunterbrechung

Ein Backup-Server kann gelegentlich aufgrund von Netzwerkproblemen die Verbindung zum Verwaltungsserver verlieren. Sicherungen werden weiterhin gemäß dem konfigurierten Zeitplan durchgeführt, solange der Backup-Server die Verbindung zu den Workloads aufrechterhält.

Die Informationen zur Sicherungsversion werden aktualisiert, sobald die Verbindung zum Verwaltungsserver wiederhergestellt ist, sodass Sicherungen wie geplant fortgesetzt werden können.

Mainboard-Ausfall

Ein Mainboard-Ausfall kann dazu führen, dass der Server überhaupt nicht mehr reagiert. Da die Festplatten in der Regel intakt bleiben, wird empfohlen, so schnell wie möglich ein Ersatzgerät zu beschaffen und die Festplatten vom ausgefallenen Server in das neue Gerät zu übertragen. Erfahren Sie, wie Sie [Daten zwischen ActiveProtect-Geräten migrieren](#).

Dieser Vorgang stellt die vorherige Systemkonfiguration ohne Datenverlust wieder her. Sobald der Ersatzserver mit dem Netzwerk verbunden ist, sind sowohl Sicherungsdaten als auch Kopien wieder verfügbar, sodass der Betrieb wie zuvor fortgesetzt werden kann.

Wenn Sie Ihre Daten nicht auf ein anderes ActiveProtect-Gerät migrieren können, müssen Sie möglicherweise [Ihr ActiveProtect-System wiederherstellen](#).

Festplattenausfall

Festplattenausfälle sind ein häufiges Risiko, aber ein vollständiger Datenverlust ist weniger wahrscheinlich, da alle Modelle RAID zur Redundanz verwenden. Weitere Informationen finden Sie in den [ActiveProtect-Gerätespezifikationen](#).

Wenn der Speicherpool degradiert wird, ersetzen Sie die ausgefallenen Laufwerke umgehend, um die Redundanz wiederherzustellen und potenziellen Datenverlust zu verhindern. Ausführliche Reparatuschritte finden Sie unter [Speicher reparieren](#). Falls der Speicherpool nicht repariert werden kann, müssen Sie möglicherweise [Ihr ActiveProtect-System wiederherstellen](#).

Ransomware-Angriff

Ransomware zielt auf die Datenintegrität und nicht auf die Hardware ab. Wenn ein Backup- oder Verwaltungsserver kompromittiert wurde, besteht die erste Priorität darin, das betroffene Gerät vom Netzwerk zu isolieren, um die Ausbreitung der Schadsoftware zu verhindern. Die Wiederherstellung erfolgt dann entweder durch das Wiederherstellen von einem sauberen sekundären Verwaltungsserver oder durch die vollständige Bereitstellung eines neuen Servers, abhängig von Ihrer Systemkonfiguration. Ausführliche Wiederherstellungsschritte finden Sie unter [Site Recovery](#).

Um das Risiko durch Ransomware zu verringern, empfehlen wir die Verwendung eines unveränderlichen Plans für Ihre Backups. Backups, die mit einem unveränderlichen Plan erstellt wurden, sind durch WORM (auf dem ActiveProtect-Gerät oder ActiveProtect Vault) oder Object Lock (auf AWS S3) geschützt, sodass Daten nicht verändert oder gelöscht werden können. Dadurch bleiben Backups und Kopien, die auf externem Speicher oder einem anderen Gerät gespeichert sind, sicher und unbeschädigt, sodass Daten im Falle eines Ransomware-Angriffs wiederhergestellt werden können.

Sie können unter **Schutzpläne > Plan erstellen** einen unveränderlichen Schutzplan erstellen. Ausführliche Anweisungen finden Sie unter [Schutzpläne verwalten](#).

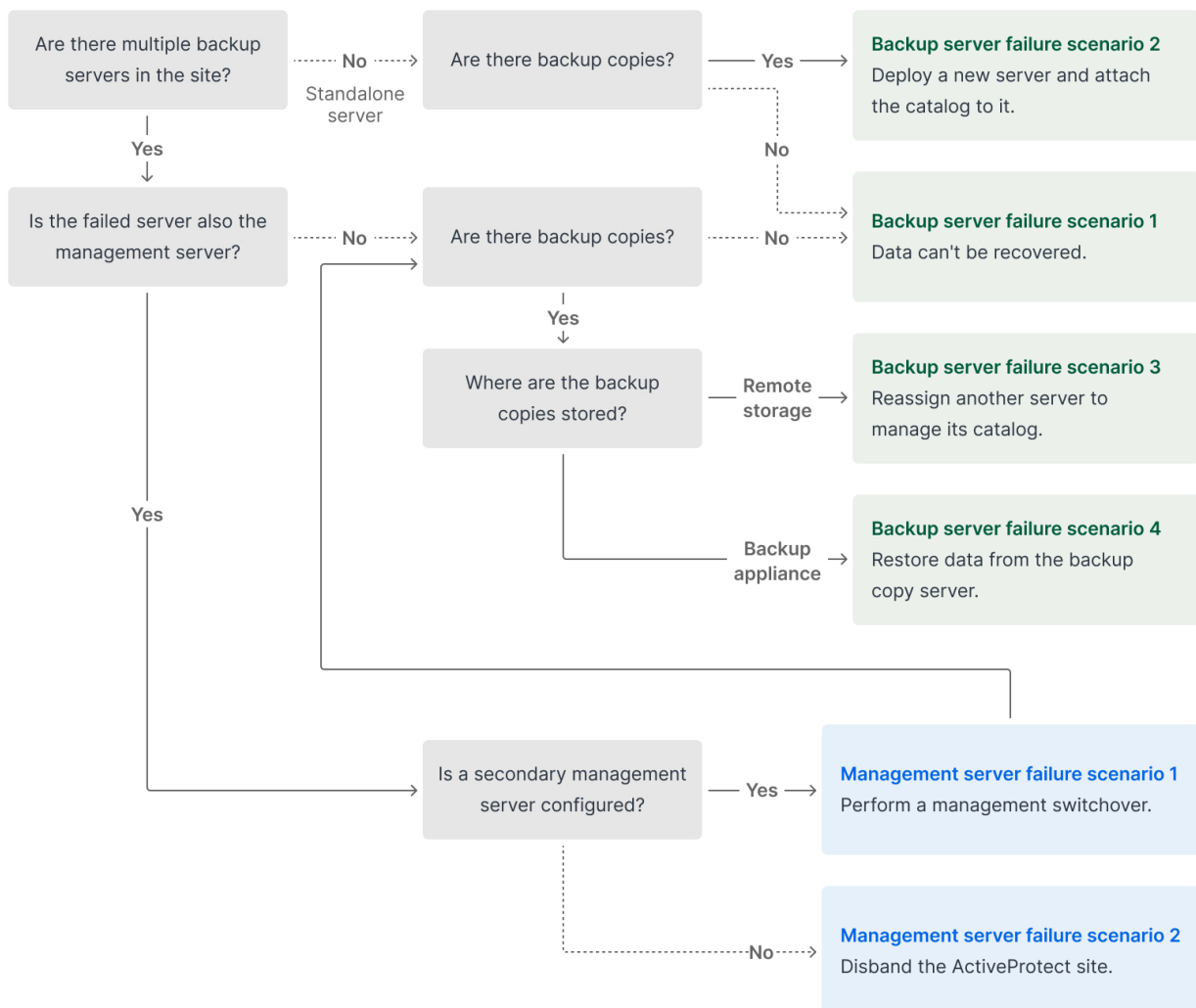
Erfahren Sie mehr über [unveränderlichen Schutz](#).

Standort-Wiederherstellung

Wenn Sie Ihr Backup-Gerät nicht reparieren können (z. B. durch HDD-Migration oder Speicherreparatur), verwenden Sie die Wiederherstellungsverfahren in diesem Abschnitt, um Backups wiederherzustellen und den Betrieb für jeden betroffenen Server fortzusetzen – unabhängig davon, ob dieser als Verwaltungs- oder Backup-Server fungiert.

Standortkonfiguration identifizieren

Bevor Sie mit dem Wiederherstellungsprozess beginnen, ist es wichtig, die Struktur Ihrer Backup-Infrastruktur zu verstehen. Das folgende Diagramm hilft Ihnen, Ihre Standortkonfiguration schnell zu identifizieren, sodass Sie die für Ihr Szenario passenden Wiederherstellungsschritte befolgen können.



Ausfall des Backup-Servers

Wenn ein Backup-Server nicht mehr verfügbar ist, orientieren Sie sich an dem Szenario, das Ihrer Konfiguration entspricht, um die Backups fortzusetzen. Dies gilt auch, wenn der Server zuvor als Verwaltungsserver fungierte.

Szenario 1: Keine Backup-Kopien verfügbar

Wenn ein Backup-Server ausfällt und dessen Backup-Daten weder auf Remote-Speicher noch auf anderen Backup-Geräten gespeichert wurden, können die betroffenen Backups nicht wiederhergestellt werden. Da die Backup-Daten nur auf dem ausgefallenen Server gespeichert waren, sind sie dauerhaft verloren und der Schutz für diese Workloads muss von Grund auf neu eingerichtet werden.

Nachdem Sie den ausgefallenen Server ersetzt haben, führen Sie die folgenden Schritte aus, um den Schutz für die betroffenen Workloads entsprechend Ihrer Standortkonfiguration wieder aufzunehmen:

Für eigenständige Server

Schutzpläne, Hypervisoren und Workloads müssen auf dem neuen Server neu erstellt werden:

- Um Schutzpläne zu erstellen, gehen Sie zu **Pläne > Schutzpläne > Plan erstellen**.
- Um Hypervisoren hinzuzufügen, gehen Sie zu **Infrastruktur > Hypervisoren > Hinzufügen**.
- Um Workloads hinzuzufügen, gehen Sie zu **Maschinen** oder **Cloud-Anwendungen**, wählen Sie den Workload-Typ aus und klicken Sie auf **Hinzufügen**.

Sobald die Workloads erneut hinzugefügt wurden, führt das System eine vollständige Sicherung durch, bevor die inkrementellen Backups fortgesetzt werden.

Für Multi-Server-Standorte

Da standortweite Konfigurationen wie Schutzpläne, Hypervisoren und SaaS-Mandantenkonten in der gesamten Umgebung geteilt werden, müssen nur die Workloads erneut hinzugefügt werden:

1. Gehen Sie zu **Maschinen** oder **Cloud-Anwendungen**, wählen Sie den Workload-Typ aus und klicken Sie auf **Hinzufügen**.
2. Sobald die Workloads erneut hinzugefügt wurden, führt das System eine vollständige Sicherung durch, bevor die inkrementellen Backups fortgesetzt werden.

Weitere Anweisungen finden Sie im [Admin Guide für das ActiveProtect-Gerät](#).

Szenario 2: Eigenständiger Server mit Backup-Kopien auf Remote-Speicher

Wenn ein eigenständiger Backup-Server Backup-Kopien auf Remote-Speicher ablegt, ist eine Wiederherstellung möglich, erfordert jedoch eine umfangreiche Neukonfiguration.

Nachdem Sie einen Ersatzserver bereitgestellt haben, führen Sie die folgenden Schritte aus:

Vorherige Backup-Daten wiederherstellen

1. Gehen Sie auf Ihrem Ersatzserver zu **Infrastruktur > Remote-Speicher > Hinzufügen**.
2. Nachdem Sie Ihren Remote-Speicher hinzugefügt haben, doppelklicken Sie darauf und gehen Sie zu **Backup-Katalog**.
3. [Anhängen](#) Sie alle Kataloge, die mit dem ausgefallenen Server verbunden sind.
4. Wählen Sie den Backup-Server und den Archivierungsplan für den Katalog aus.
5. Sobald der Katalog angehängt ist, gehen Sie zur Workload-Liste und wählen Sie im oberen Dropdown-Menü **Archiviert** aus, um Backup-Versionen anzuzeigen und wiederherzustellen.

Konfigurationen neu erstellen und Workloads erneut hinzufügen, um Backups fortzusetzen

Da Schutzpläne, Hypervisoren und Workloads nicht auf dem Remote-Speicher gespeichert werden, müssen sie auf dem neuen Server neu erstellt werden:

- Um Schutzpläne zu erstellen, gehen Sie zu **Pläne > Schutzpläne > Plan erstellen**.
- Um Hypervisoren hinzuzufügen, gehen Sie zu **Infrastruktur > Hypervisoren > Hinzufügen**.
- Um Workloads hinzuzufügen, gehen Sie zu **Maschinen** oder **Cloud-Anwendungen**, wählen Sie den Workload-Typ aus und klicken Sie auf **Hinzufügen**.

Sobald die Workloads erneut hinzugefügt wurden, führt das System eine vollständige Sicherung durch, bevor die inkrementellen Backups fortgesetzt werden. Weitere Anweisungen finden Sie im [Admin Guide für das ActiveProtect-Gerät](#).

Szenario 3: Multi-Server-Standort mit Backup-Kopien auf Remote-Speicher

In einem ActiveProtect-System mit mehreren Backup-Servern, bei dem Backup-Kopien auf Remote-Speicher abgelegt werden, ist die Wiederherstellung effizienter. Fällt ein Server aus, kann dessen Katalog einem anderen funktionierenden Server zugewiesen werden.

Vorherige Backup-Daten wiederherstellen

1. Entfernen Sie den ausgefallenen Backup-Server aus dem Standort und weisen Sie einem anderen Backup-Server die Verwaltung seines Katalogs zu. Wählen Sie gegebenenfalls einen Archivierungsplan für verbleibende Backup-Kopien aus.

2. Um den Zuweisungsprozess anzuzeigen, gehen Sie zu **Infrastruktur > Remote-Speicher**, wählen Sie den Remote-Speicher aus und klicken Sie auf **Backup-Katalog**.
3. Sobald der Zuweisungsprozess abgeschlossen ist, ändert sich der Katalogstatus zu **Verwaltet (Archiviert)**.
4. Sie können zur Workload-Liste gehen und im oberen Dropdown-Menü **Archiviert** auswählen, um Backup-Versionen anzuzeigen und wiederherzustellen.

Workloads erneut hinzufügen, um Sicherungen fortzusetzen

Da standortweite Konfigurationen wie Schutzpläne, Hypervisoren und SaaS-Mandantenkonten in der gesamten Umgebung geteilt werden, müssen nur die Workloads erneut hinzugefügt werden.

1. Um Workloads hinzuzufügen, gehen Sie zu **Maschinen** oder **Cloud-Anwendungen**, wählen Sie den Workload-Typ aus und klicken Sie auf **Hinzufügen**.
2. Sobald die Workloads erneut hinzugefügt wurden, führt das System eine vollständige Sicherung durch, bevor inkrementelle Sicherungen fortgesetzt werden.

Weitere Anweisungen finden Sie im [Admin-Handbuch des ActiveProtect-Geräts](#).

Szenario 4: Multi-Server-Standort mit Sicherungskopien auf einem anderen Backup-Gerät

Wenn Sicherungskopien auf einem anderen Backup-Gerät statt auf Remote-Speicher gespeichert sind, ist die Wiederherstellung einfacher. Fällt ein Server aus, kann das andere Backup-Gerät direkt aus seinen Sicherungskopien wiederherstellen, ohne einen Katalog anzuhängen. Hinweise zur Wiederherstellung finden Sie unter [Datenwiederherstellung](#).

Workloads erneut hinzufügen, um Sicherungen fortzusetzen

Da standortweite Konfigurationen wie Schutzpläne, Hypervisoren und SaaS-Mandantenkonten in der gesamten Umgebung geteilt werden, müssen nur die Workloads erneut hinzugefügt werden.

1. Um Workloads hinzuzufügen, gehen Sie zu **Maschinen** oder **Cloud-Anwendungen**, wählen Sie den Workload-Typ aus und klicken Sie auf **Hinzufügen**.
2. Sobald die Workloads erneut hinzugefügt wurden, führt das System eine vollständige Sicherung durch, bevor inkrementelle Sicherungen fortgesetzt werden.

Weitere Anweisungen finden Sie im [Admin-Handbuch des ActiveProtect-Geräts](#).

Ausfall des Management-Servers

Wenn ein Management-Server ausfällt, hängt der Wiederherstellungsprozess davon ab, ob ein sekundärer Management-Server im System konfiguriert wurde.

Szenario 1: Sekundärer Management-Server konfiguriert

Wenn bereits ein sekundärer Management-Server eingerichtet wurde, können Sie eine Management-Übergabe auslösen.

Wenn Ihre Backup-Server über einen FQDN verbunden sind (empfohlen)

1. Gehen Sie zu Ihrem DNS-Server. Leiten Sie die externe Adresse des primären Management-Servers auf die IP-Adresse Ihres sekundären Servers um.
2. Melden Sie sich mit einem APM-Administratorkonto am sekundären Server an.
3. Klicken Sie auf **Management wechseln**.

Wenn Ihre Server über eine IP-Adresse verbunden sind

1. Melden Sie sich mit einem APM-Administratorkonto am sekundären Server an.
2. Klicken Sie auf **Management wechseln**.
3. Melden Sie sich an jedem Ihrer verwalteten Backup-Server an. Klicken Sie auf das Stiftsymbol neben dem **Management-Server** und geben Sie die IP-Adresse Ihres sekundären Servers ein.

Weitere Details finden Sie unter [Management-Übergabe initiieren](#). Nach der Übergabe wird der ursprüngliche Management-Server zum sekundären Management-Server. Folgen Sie den Schritten aus den Szenarien unter [Ausfall des Backup-Servers](#), um Sicherungen fortzusetzen und Sicherungskopien wiederherzustellen.

Szenario 2: Kein sekundärer Management-Server konfiguriert

Wenn der Management-Server vollständig funktionsunfähig wird (z. B. durch einen Laufwerksausfall oder Ransomware) und kein sekundärer Management-Server verfügbar ist, müssen Sie ein neues ActiveProtect-System einrichten:

Neues ActiveProtect-System bereitstellen

1. Führen Sie auf jedem verwalteten Server einen [Mode 2-Reset](#) durch, um das System aufzulösen.
2. Stellen Sie einen neuen Management-Server bereit und gehen Sie zu **Systemeinstellungen > Allgemein**, um ein neues System zu erstellen.
3. Konfigurationen wiederherstellen:
 - Um Schutzpläne zu erstellen, gehen Sie zu **Pläne > Schutzpläne > Plan erstellen**.
 - Um Hypervisoren hinzuzufügen, gehen Sie zu **Infrastruktur > Hypervisoren > Hinzufügen**.
 - Um Remote-Speicher hinzuzufügen, gehen Sie zu **Infrastruktur > Remote-Speicher > Hinzufügen**.

Sicherungskopien wiederherstellen

So stellen Sie Sicherungskopien aus dem Remote-Speicher wieder her

1. Gehen Sie zu **Infrastruktur > Remote-Speicher**.
2. Doppelklicken Sie auf den Remote-Speicher und gehen Sie zu **Backup-Katalog**.
3. Wählen Sie den Katalog aus, den Sie wiederherstellen möchten, und klicken Sie auf **Anfügen**.
4. Wählen Sie den Backup-Server und den Archivierungsplan für den Katalog aus.
5. Sobald die Verbindung hergestellt ist, gehen Sie zur Workload-Liste und wählen Sie im oberen Dropdown-Menü **Archiviert** aus, um Sicherungsversionen anzuzeigen und wiederherzustellen.

So stellen Sie Sicherungskopien von einem Backup-Appliance wieder her

1. Gehen Sie zu **Maschinen** oder **Cloud-Anwendungen** und wählen Sie Ihren Workload-Typ aus.
2. Fahren Sie mit der Maus über den Workload und klicken Sie auf das Detailsymbol > **Wiederherstellungsportal öffnen**.

Weitere Anweisungen finden Sie unter [Wiederherstellungsportal navigieren](#).

Workloads erneut hinzufügen, um Sicherungen fortzusetzen

1. Gehen Sie zu **Maschinen** oder **Cloud-Anwendungen**, wählen Sie Ihren Workload-Typ aus und fügen Sie Ihre Workloads erneut hinzu.
2. Sobald die Workloads erneut hinzugefügt wurden, führt das System eine vollständige Sicherung durch, bevor die inkrementellen Sicherungen fortgesetzt werden.

Hinweise:

- Beim Durchführen eines **Mode 2**-Resets:
 - Der Management-Server verlässt die Site und wird zu einem eigenständigen Server.
 - Sicherungsdaten bleiben erhalten, aber alle Workloads werden nicht mehr verwaltet und Site-Konfigurationen wie Schutzpläne, Hypervisoren und Verbindungen zu Remote-Speichern werden entfernt.
 - Mit WORM verknüpfte Tiering-Pläne bleiben bestehen, werden jedoch nicht mehr ausgeführt, da ihr Ziel (d. h. der Remote-Speicher) entfernt wurde.
- Wenn Sie einen verwalteten Server zurücksetzen, während der Management-Server noch online ist, betrachtet der Management-Server den zurückgesetzten Server als dauerhaft offline. Jeder Schutzplan, der den zurückgesetzten Server als Sicherungsziel verwendet, schlägt fehl.
- Für Synology NAS ist kein Reset erforderlich. Um die Site zu verlassen, gehen Sie zu **Active Backup for Business > Zentrales Management > Bearbeiten > Verlassen erzwingen**. Nach dem Verlassen bleiben die Sicherungsdaten erhalten und Synology NAS sichert die Workloads weiterhin gemäß dem zuletzt synchronisierten Plan.

Fazit

Durch die Umsetzung einer 3-2-1-Backup-Strategie, die Bereitstellung eines sekundären Management-Servers und die Speicherung von Sicherungskopien auf einem entfernten Speicher oder einem dedizierten Backup-Gerät stellen Sie sicher, dass Daten wiederherstellbar bleiben und der Betrieb auch bei Hardwareausfällen, Cyberangriffen oder unerwarteten Ausfällen fortgesetzt werden kann.

Wenn Vorfälle auftreten, unterstützen Sie ein schneller Austausch, das Anhängen von Katalogen und die Neukonfiguration von Workloads bei einer zügigen Wiederherstellung, während unveränderliche oder isolierte Backups Ihre Daten vor Ransomware schützen. Die Befolgung dieser Maßnahmen trägt dazu bei, die Resilienz aufrechtzuerhalten, Ausfallzeiten zu minimieren und kritische Daten zu schützen.