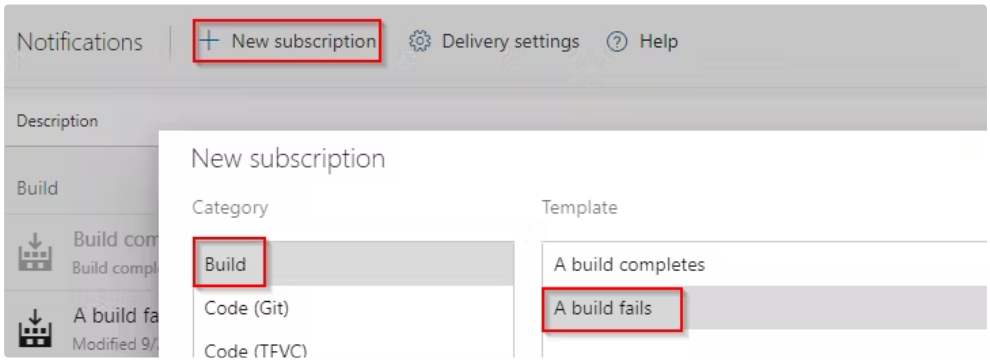
Intune-CaC-Automation Advanced View

Was macht die Azure Pipline

- IntuneCD Tool installieren
- Intune-Konfigurationssicherung in den Ordner prod-backup exportieren
- Wenn eine Änderung in der Konfiguration erkannt wird
  - **Finde für jede geänderte Datei heraus, wer sie geändert hat**
    - Suche dazu im Intune-Auditprotokoll nach bestimmten ResourceId-Änderungen seit dem Datum des letzten Konfigurations-Commits
- Gruppiere die geänderten Dateien nach den Autor(en), die sie geändert haben
- Committe jede Gruppe separat, wobei der/die Name(n) des/der Autors/Autoren auch als Commit-Autor(en) verwendet werden
- Erstelle eine Intune-Konfigurationsdokumentationsdatei (als Markdown)
  - (nur wenn du die Aufgabe "Markdown-Dokument generieren & committen" auskommentierst)
- Git TAG erstellen
  - Der Name aller Änderungsautoren wird in die TAG-Beschreibung aufgenommen
- HTML- und PDF-Dateien aus der Intune-Konfigurationsdokumentationsdatei generieren und als Pipeline-Artefakte speichern
  - (nur wenn du die Aufgaben "Markdown-Dokument generieren & committen" und "As-built-Artefakte veröffentlichen" auskommentierst und den Ordner md2pdf (aus diesem Repository) zu deinem Repository-Root hinzufügst) Wenn keine Änderungen vorhanden sind
- Pipeline endet

Benachrichtigung bei Pipeline-Fehlern senden

Es ist hilfreich, benachrichtigt zu werden, wenn die Pipeline fehlschlägt. Dies kann zum Beispiel passieren, wenn ein Anwendungsgeheimnis abgelaufen ist. Um dies einzurichten, gehen Sie zu **Projekteinstellungen** > **Benachrichtigungen** > **Neues Abonnement**. Wählen Sie dann **Build** > **Ein Build schlägt fehl** aus und schliessen Sie den Assistenten ab.



Wiederherstellungsprozess

Beim Wiederherstellen des Backups haben Sie grundsätzlich zwei Möglichkeiten:

1. Verwenden der IntuneCD-Updatefunktion:

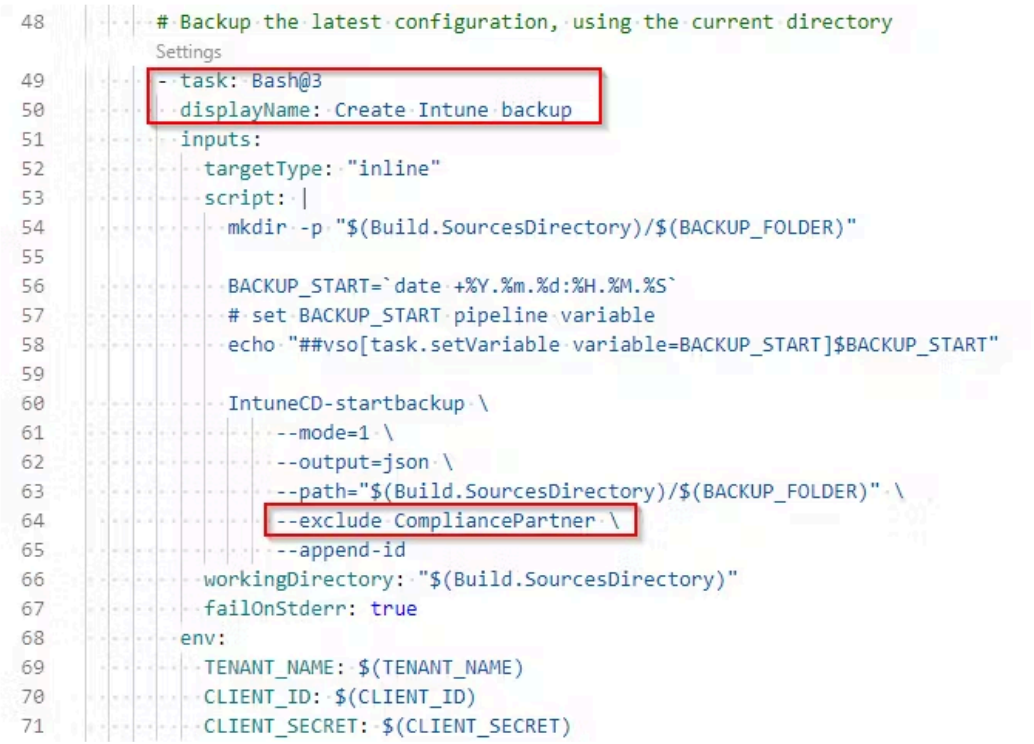
- Erstellen Sie einen neuen Ordner.
- Kopieren Sie nur die Ordnerstruktur mit den JSON-Dateien, die Sie wiederherstellen möchten, in diesen Ordner.
- Führen Sie "IntuneCD-startupdate" mit dem Argument "--path "PfadZumBackupOrdner"" aus.

2. Manuelles Erstellen der gewünschten Intune-Konfigurationen:
   - Füllen Sie die Werte in den JSON-Dateien Ihres Backups ein.

Ändern der Datensicherungselemente

Um festzulegen, welche Intune-Konfigurationen gesichert werden sollen, müssen Sie den Abschnitt "Create Intune backup task" im Pipeline-Konfigurationscode bearbeiten.

Gehen Sie zu **Pipelines** > **<IhrPipelineName>** > klicken Sie auf **Bearbeiten** > Suchen Sie nach einer Aufgabe mit dem Namen **Create Intune backup** und ändern Sie deren Abschnitt **Skript**, indem Sie den Parameter **--exclude** modifizieren.



Standardmässig schließe ich **CompliancePartner** aus, da sich dessen Daten täglich ändern und ich nur bei echten Änderungen neue Commits erstellen möchte.

Wie der Änderungsautor ermittelt wird

Wenn eine Änderung im erstellten Backup (eine JSON-Konfigurationsdatei) erkannt wird, führt die Pipeline die folgenden Schritte aus:

1. **Liste aller geänderten Dateien abrufen**
2. **Datum des letzten Konfigurations-Backup-Commits abrufen ($lastCommitDate)**
   - Falls kein Commit vorhanden ist, wird das gesamte Intune-Auditprotokoll durchsucht.
3. **Für jede geänderte Datei den Autor ermitteln**
   - Die Ressourcen-ID aus dem Dateinamen extrahieren

    - Diese ID im Intune-Auditprotokoll suchen (zwischen den in $lastCommitDate gespeicherten Daten und der Startzeit dieses Backup-Laufs)
    - Alle Autoren notieren, die dort Änderungen vorgenommen haben
4. **Geänderte Dateien nach Autoren gruppieren und Commits erstellen**
    - Für jede Gruppe einen Commit erstellen.
    - Im Commit-Namen und als Commit-Autor werden alle Autoren verwendet, die diese Dateien geändert haben.
5. **Alle gefundenen Autoren auch in die Git-Tag-Beschreibung aufnehmen**

Ungenauigkeiten bei der Ermittlung des Änderungsautors

Die Liste der ermittelten Autoren ist nicht zwingend zu 100 % korrekt. Wenn Sie absolute Genauigkeit benötigen (z. B. bei Sicherheitsvorfällen), verwenden Sie den Befehl "Get-MgDeviceManagementAuditEvent".

Dies ist zum Beispiel hilfreich, wenn jemand direkt nach dem Start des Backups eine Änderung in Intune vornimmt. Die Änderung selbst wird zwar erfasst, der Autor jedoch nicht, da das Intune-Protokoll nur zwischen dem Datum des letzten Commits und dem Startzeitpunkt des aktuellen Backups durchsucht wird. Würde die Suche stattdessen bis zum Abschluss des Backups laufen, könnte im umgekehrten Fall ein Autor in der Liste aufgeführt sein, der die im Backup erfasste Änderung gar nicht vorgenommen hat.

Beachte Folgendes:

- Die Liste der Commit-Autoren zeigt lediglich, wer Änderungen an den commiteten Dateien vorgenommen hat (seit dem letzten Commit). Sie gibt nicht an, wer welche bestimmte Änderung vorgenommen hat.
- Wurde eine Änderung von einer Anwendung (anstatt von einem Benutzer) vorgenommen, wird der Name der Anwendung mit dem Suffix "(SP)" als Autorenname verwendet (z. B. "Modern Workplace Management (SP)").
- Bestimmte Intune-Konfigurationsänderungen werden im Intune-Auditprotokoll überhaupt nicht erfasst! Dies gilt beispielsweise für Änderungen am ESP-Profil usw. Wenn der Autor der geänderten Konfiguration im Auditprotokoll nicht gefunden wird, wird stattdessen "unbekannt" verwendet.
- Intune verwendet verschiedene ID-Formate! Nicht nur "<GUID>" wie man vermuten könnte, sondern zum Beispiel verwenden ESP-Profile, Apple-Konfiguratorprofile und App-Schutzrichtlinien Formate wie "<GUID>_<GUID>", "<GUID>_<Zeichenfolge>", "T_<GUID>" und wahrscheinlich gibt es noch weitere exotische Formate.