

Nerdio Manager for Enterprise-Implementierungsleitfaden

nerdio

Inhaltsverzeichnis

Implementierungsleitfaden 5
Einführung 5
In diesem Leitfaden: 5
Schritt 1 Installation 5
In diesem Abschnitt: 6
Azure-Berechtigungen und Nerdio Manager 6
Nerdio Manager Installation Guide 10
Nerdio Manager Edition Management 21
Aktivieren Sie Ihr Abonnement 22
Azure-Umgebung: verknüpfte Netzwerke und Ressourcengruppen 26
Übersicht über die Benutzeroberfläche (UI) 30
Nerdio Copilot verwalten 36
Zeitpläne für Aufgaben verwalten 42
Verwaltung von Ressourcenauswahlregeln 44
Schritt 2 Desktop-Images 49
In diesem Abschnitt: 49
Desktop-Images 49
Verwaltungs- und Lebenszyklusaufgaben für importierte Desktop-Images 50
Desktop-Image erstellen 53
Desktop-Images: Als Image festlegen 63
Scripted Actions für Desktop-Images 72
Schritt 3 Hostpools 74
In diesem Abschnitt: 74
Übersicht über Hostpools 75
Arbeitsbereiche verwalten 76
Dynamische Hostpools erstellen 78
Hostpool-Profile verwalten 87
Dynamische Hostpool-Autoskalierung aktivieren 92
Automatische Skalierung für persönliche Hostpools aktivieren 110
Autoscaling: Kostenoptimierung: Sitzungshost-VM, Betriebssystemdatenträger, Speicher 134
Fügen Sie einem dynamischen Hostpool einen neuen Sitzungshost hinzu. 136

Hostpool-AVD-Konfiguration 141
Bereitstellung von virtuellen Maschinen im Hostpool 145
Userzuweisungen für Hostpools verwalten 156
Active Directory-Einstellungen des Hostpools konfigurieren ... 156
VM beim Herstellen einer Verbindung für gepoolte Hostpools starten 158
Sitzungslimits für User konfigurieren 159
Remote-Anwendungen für User veröffentlichen 163
Schritt 4: Speicher 171
In diesem Abschnitt: 172
Erforderliche Berechtigungen zum Verbinden einer Azure Files-Freigabe mit einer Domäne (Active Directory) 172
Konfigurierte Azure Files-Datenfreigaben erstellen und verwalten 176
Auto-scale für Azure Files-Speicher 186
Verlauf des automatischen Skalierens für Azure Files-Datenfreigaben 199
Konfigurierte Azure NetApp Files erstellen und verwalten 202
Automatische Skalierung für Azure NetApp Files 205
Autoscaling-Verlauf für Azure NetApp-Datenfreigaben 209
Schritt 5: FSLogix und Userprofilverwaltung 211
In diesem Abschnitt: 211
FSLogix und Benutzerprofilverwaltung 212
FSLogix-Einstellungen und -Konfiguration 213
FSLogix-Profilanpassung pro Hostpool 219
Installierte Anwendungen auf Hostpools verwalten 223
Schritt 6: MSIX App Attach 231
In diesem Abschnitt: 231
App Attach-Images und -Pakete verwalten 231
App Attach-Zuweisungen verwalten 239
Konfigurieren von Azure Files-Berechtigungen für App Attach 242
Schritt 7: Rollenbasierte Zugriffssteuerung (RBAC) 246
In diesem Abschnitt: 246
Rollenbasierte Zugriffssteuerung (RBAC) in Nerdio Manager .. 247
Rollenbasierte Zugriffssteuerung (RBAC): Benutzerdefinierte Rollen 251

Rollenbasierte Zugriffssteuerung (RBAC): Mehrfache Gruppenzuweisungen 255

Implementierungsleitfaden

Einführung

Der *Nerdio Manager for Enterprise-Implementierungsleitfaden* bietet einen geführten Implementierungspfad durch die Dokumentation von Nerdio Manager for Enterprise – eine empfohlene Reihenfolge der Schritte für die Installation, Konfiguration und Vorbereitung einer neuen Umgebung für User, ergänzt durch die Abschnitte Knowledge Base und Setup & Settings. Er ist bewusst eng gefasst: Anstatt jedes Feature abzudecken, das Nerdio Manager bietet, verlinkt jeder Schritt auf die spezifischen Artikel, die Sie in dieser Phase benötigen.

Wenn Sie stattdessen vollständiges Referenzmaterial für jedes Feature suchen, lesen Sie die Abschnitte **Knowledge Base** und **Setup & Settings**.

Fragen während der Implementierung? Kontaktieren Sie das Support-Team unter nme.support@getnerdio.com.

In diesem Leitfaden:

- Schritt 1 Installation [5]
- Schritt 2 Desktop-Images [49]
- Schritt 3 Hostpools [74]
- Schritt 4: Speicher [171]
- Schritt 5: FSLogix und Userprofilverwaltung [211]
- Schritt 6: MSIX App Attach [231]
- Schritt 7: Rollenbasierte Zugriffssteuerung (RBAC) [246]

Schritt 1 Installation

Bevor Sie mit der Verwaltung Ihrer Azure-Umgebung beginnen können, müssen Sie die Nerdio Manager-Anwendung installieren und konfigurieren. Weisen Sie Nerdio Manager zunächst die erforderlichen Azure-Berechtigungen zu. Führen Sie dann den Installer aus und aktivieren Sie Ihr Abonnement. Machen Sie sich mit der Verwaltungskonsole vertraut, bevor Sie Ihre Umgebung aufbauen.

In diesem Abschnitt:

1. Azure-Berechtigungen und Nerdio Manager [6]
2. Nerdio Manager Installation Guide [10]
3. Nerdio Manager Edition Management [21]
4. Aktivieren Sie Ihr Abonnement [22]
5. Azure-Umgebung: verknüpfte Netzwerke und Ressourcengruppen [26]
6. UI-Übersicht [30]
7. Manage Nerdio Manager Copilot [36]
8. Zeitpläne für Aufgaben verwalten [42]
9. Verwaltung von Regeln zur Ressourcenauswahl [44]

Azure-Berechtigungen und Nerdio Manager

Nerdio Manager ist eine Azure-Anwendung, die über den Azure Marketplace bereitgestellt wird und innerhalb Ihres eigenen Entra ID Tenant sowie Ihres Azure-Abonnements ausgeführt wird. Es erfordert bestimmte Berechtigungen während der Installation, Konfiguration und laufenden Nutzung.

> **Tipp**
>
> Siehe das folgende Dokument für einen detaillierten Einblick in die Azure-Berechtigungen und Nerdio Manager: Nerdio Manager for Enterprise - Berechtigungen.

Installationsberechtigungen

Der Entra ID-Benutzer, der die Installation von Nerdio Manager durchführt, benötigt die folgenden Berechtigungen:

- **globaler Admin**-Rolle in Entra ID.
- **Owner**-Rolle im Azure-Abonnement.

> **Anmerkung**
>
> Diese erweiterten Berechtigungen werden nur für den anfänglichen Installations- und Konfigurationsprozess benötigt und sind für die laufende Nutzung von Nerdio Manager nicht erforderlich.

Wenn Nerdio Manager installiert ist, verfügt es über die folgenden API-Anwendungsberechtigungen in Azure:

Abonnement-Berechtigungen

Während der Aktivierung des Nerdio Manager-Lizenzabonnements wird ein neues Azure-Ressourcenobjekt für SaaS-Abonnements im Azure-Abonnement erstellt, das es Nerdio Manager ermöglicht, den Lizenzverbrauch als Drittanbieterdienst auf der Azure-Rechnung zu berechnen. Um ein SaaS-Abonnementobjekt zu konfigurieren, muss der User, der die Konfiguration abschließt, als **Owner** festgelegt sein für das Abonnement, da dies zu zusätzlichen Kosten auf dem Abonnement führt.

Eine neue, für die Abrechnung von Nerdio Manager spezifische Entra ID-Anwendungsregistrierung wird ebenfalls automatisch als Teil der Ressourcenbereitstellung erstellt. Dieser Anwendung werden die unten aufgeführten Berechtigungen erteilt, um sich als Ihr Benutzer im Namen Ihres Azure Tenant zu authentifizieren und das SaaS-Abonnementobjekt als mit Ihrem Azure-Abonnement verknüpft zu registrieren. Diese Berechtigungen ermöglichen es der Abrechnungsanwendung, den Lizenzierungsdienst von Nerdio Manager über die folgenden Details zu informieren:

- Wer den Kauf abschließt.
- Welches SaaS-Abonnementobjekt für die Abrechnung verwendet wird.
- Von welchem Entra ID Tenant aus Sie die Verbindung herstellen.

> **Anmerkung**
>
> Dies sind dieselben Berechtigungen, die der Abrechnungsanwendung erteilt werden, wie sie auch der primären Nerdio Manager-Anwendung oben erteilt wurden.

Dienst	Berechtigung	Funktion
Microsoft Graph	openid, Profil, User.Read (delegiert)	Ermöglicht das Anmelden des Users (Name & Azure-Mandanten-ID werden geteilt).

Konfigurationsberechtigungen

Sobald die Nerdio Manager-Anwendung installiert ist, können innerhalb von Nerdio Manager verschiedene Konfigurationsaktionen durchgeführt werden, um sie mit bestehenden Azure-Ressourcen zu „verknüpfen“ oder neue zu erstellen. Diese Aktionen erfordern, dass der anfordernde Benutzer (d. h. der Benutzer, der angemeldet ist und die Aktion über Nerdio Manager ausführt) über bestimmte Berechtigungen für die verwendeten Azure-Ressourcen verfügt.

Aktion	Erforderliche Berechtigungen
Ressourcengruppe verknüpfen	Der anfordernde Benutzer muss Owner der zu verknüpfenden Ressourcengruppe sein.
Netzwerk verknüpfen	Der anfordernde Benutzer muss Owner des zu verknüpfenden VNet (oder der Ressourcengruppe, die das VNet enthält) sein. **Anmerkung** Der angemeldete Benutzer benötigt die Rolle „Owner“ oder „User Access Administrator“; der Dienstprinzipal von Nerdio behält dann die Rolle „Contributor“ für die Ressourcengruppe oder das VNet.
Zusätzliches Azure-Abonnement verknüpfen	Der anfordernde User muss als Owner für das zu verlinkende Abonnement festgelegt sein.

Aktion	Erforderliche Berechtigungen
AVD-Objektmodell von „Klassisch“ auf „ARM“ umstellen	Der anfordernde User muss globaler Admin in Entra ID sein, um die erforderliche Admin-Zustimmung erteilen zu können.
Sepago Azure Monitoring aktivieren	Der anfordernde User muss als Owner für die ausgewählte Ressourcengruppe für die Bereitstellung der Log Analytics-Ressourcen und die Berechtigungszuweisung festgelegt sein.
Azure Files-Datenfreigaben erstellen	Der anfordernde User muss Contributor der ausgewählten Ressourcengruppe für die Bereitstellung des Storage-Kontos sein.
Azure NetApp Files-Volumes erstellen	Der anfordernde User muss Contributor der ausgewählten Ressourcengruppe für die Bereitstellung des NetApp-Kontos sowie des virtuellen Netzwerks sein, das das NetApp Files-Subnetz enthält.
AVD ARM-Hostpools erstellen	Der anfordernde User muss Contributor der Ressourcengruppe sein, in der der Hostpool erstellt wird.
Zugriff auf den Nerdio Manager für andere User hinzufügen	Der anfordernde User muss ein AVD-Admin sein.
Sitzungshost-VMs aus vorheriger AVD-Bereitstellung zuordnen	Der anfordernde User muss in der Ressourcengruppe, die die VMs enthält, Contributor sein.

Berechtigungen für die laufende Nutzung

Wenn die Nerdio Manager-Anwendung installiert und konfiguriert ist, sind keine User-Berechtigungen in Azure erforderlich, um die konfigurierte AVD-Umgebung via Nerdio Manager zu verwalten. Die meisten Aktionen in Nerdio Manager werden auf Nerdio Manager im Namen des angemeldeten Users ausgeführt.

Anmerkung

Es sind verschiedene RBAC-Rollen verfügbar. Weitere Informationen finden Sie unter Rollenbasierte Zugriffssteuerung (RBAC) in NME [247].

Nerdio Manager Installation Guide

> **Anmerkung**
>
> Stellen Sie vor dem Start sicher, dass Sie die Vorbereitungsschritte für die Installation des Nerdio Managers gelesen haben.

Dieser Abschnitt führt Sie durch den Prozess der Installation von Nerdio Manager in Ihrem Azure-Abonnement und der Initialisierung von Nerdio Manager.

Indem Sie diese Schritte befolgen, registrieren Sie eine Unternehmensanwendung in Ihrem eigenen Azure-Mandanten, in einem Abonnement Ihrer Wahl, innerhalb einer neuen Ressourcengruppe oder einer bestehenden Ressourcengruppe, sofern diese leer ist. Sobald die Installation abgeschlossen ist, erhalten Sie eine URL, um sich bei der Nerdio Manager-Webanwendung anzumelden.

Nerdio Manager wird über den Azure Marketplace installiert und abgerechnet.

Der Installationsprozess kann in die folgenden Phasen unterteilt werden:

- Bestätigen Sie, dass Sie die Voraussetzungen erfüllen, bevor Sie mit der Installation von Nerdio Manager beginnen.
- Installieren Sie die Nerdio Manager-Anwendung über den Azure Marketplace.
- Initialisieren Sie die Installation durch Ausführen eines Azure PowerShell-Skripts.
- Registrieren Sie Ihre Installation bei unseren Lizenzierungsservern und konfigurieren Sie die Nerdio Manager-Einstellungen.

Begleitvideo

Video: Install Nerdio Manager

Voraussetzungen

> **Anmerkung**
>
> Melden Sie sich vor Beginn des Installationsvorgangs als Globaler Administrator oder als Privilegierter Rollenadministrator und Cloud-Anwendungsadministrator bei Ihrem Azure-Portal an.

- Sie müssen im betreffenden Azure-Abonnement als Owner festgelegt sein, in dem Sie Nerdio Manager aus dem Azure Marketplace installieren möchten.
- Das Azure-Abonnement muss die Bereitstellung von Azure SQL, App Service, Key Vault, Application Insights und Automation Account in der Azure-Region unterstützen, die Sie während des Installationsvorgangs auswählen.
- Sie sollten über ein virtuelles Netzwerk und ein Subnetz verfügen, um AVD-Sitzungshost-VMs bereitzustellen. Sie werden während der Konfigurationsphase aufgefordert, dieses virtuelle Netzwerk und Subnetz auszuwählen.
- Bei Verwendung von Active Directory oder Entra DS muss die benutzerdefinierte Standard-DNS-Servereinstellung, die im Subnetz des virtuellen Netzwerks angegeben ist, auf einen domänenfähigen DNS-Server oder eine Azure DNS-Zone verweisen.
- Bei Verwendung von Windows Active Directory Domain Services (ADDS) muss ADDS mit Entra ID synchronisiert werden.
- Bei Verwendung von Active Directory benötigen Sie ein User-Konto mit Berechtigungen zum Hinzufügen und Entfernen von VMs zur bzw. aus der Domäne. Dieses User-Konto muss in der Lage sein, Computerobjekte in mindestens einer OU in der AD-Domäne zu erstellen und diese Computerobjekte bei Bedarf zu deaktivieren.
- Sie benötigen einen SMB-Dateispeicherort für FSLogix-Profilcontainer. Diese SMB-Freigabe kann sich auf einer Dateiserver-VM, Azure Files, Azure NetApp Files oder einem anderen Speicherort befinden, der über einen UNC-Pfad zugänglich ist (zum Beispiel \\\\server.domain.local\\share\\profiles). Der Servername muss im FQDN-Format vorliegen.

  - Um die beste Leistung zu gewährleisten, platzieren Sie den Profilspeicher in derselben Azure-Region wie die Hostpool-VMs.
  - Wenn Sie keinen Dateispeicherort zur Verfügung haben, kann dieser Schritt während der Installation übersprungen werden, und Nerdio Manager kann Azure Files oder NetApp Files nach der Konfiguration erstellen.
- Der Ressourcenanbieter Microsoft Desktop Virtualization muss in Ihrem Azure-Abonnement registriert sein.

Installation über den Azure Marketplace

Nerdio Manager wird über den Azure Marketplace installiert.

So installieren Sie Nerdio Manager:

1. Suchen Sie im Azure Marketplace nach Nerdio Manager for Enterprise.
2. Wählen Sie **Erstellen** > **NME-Plan**, um den Installationsvorgang zu starten.

   Die Seite **NME-Plan erstellen** wird geöffnet.
3. Geben Sie im Bereich **Grundlagen** die folgenden Informationen ein:
   - **Abonnement**: Wählen Sie aus der Dropdown-Liste das Abonnement aus, in dem Sie Nerdio Manager installieren möchten.
   - **Ressourcengruppe**: Wählen Sie **Neu erstellen**, um eine neue Ressourcengruppe zu erstellen. Alternativ können Sie eine vorhandene Ressourcengruppe auswählen, sofern diese leer ist.
   - **Region**: Wählen Sie aus der Dropdown-Liste die Region aus, die Ihnen am nächsten liegt oder in der sich die Mehrheit Ihrer Administratoren befindet.

     > **Anmerkung**
     >
     > In dieser Region befinden sich die Nerdio Manager-Ressourcen; sie bestimmt nicht den Standort der AVD-Sitzungshosts selbst.

   - Wählen Sie **Weiter**.
4. Führen Sie im Bereich **Ressourcennamen** Folgendes aus:
   - **Namenspräfix**: Passen Sie das für Ressourcennamen verwendete Präfix an.

- Wählen Sie **Weiter**.

5. Geben Sie im Bereich **Private Endpunkte** an, ob diese Installation private Endpunkte verwenden soll und Nerdio Manager nicht öffentlich verfügbar sein darf.

   Geben Sie die folgenden Informationen ein:

   - **Private Endpunkte aktivieren**: Aktivieren Sie diese Option, um Nerdio Manager für die Verwendung privater Endpunkte zu konfigurieren.

     > **Anmerkung**
     >
     > Wenn Nerdio Manager für die Verwendung privater Endpunkte konfiguriert ist, sind die Anwendung und ihre Abhängigkeiten (SQL-Datenbank, Storage-Konto, Key Vault, App Service, etc.) nicht mehr über ihre öffentlichen Internet-Endpunkte erreichbar. Stattdessen ist der Zugriff über private IP-Adressen auf das virtuelle Netzwerk des Kunden beschränkt. Sie können das virtuelle Netzwerk und das Subnetz für private Endpunkte sowie für den App Service anpassen, dies ist jedoch normalerweise nicht erforderlich.

   - **Virtuelles Netzwerk**: Wählen Sie aus der Dropdown-Liste das VNet aus, in dem sich die Nerdio Manager-Ressourcen befinden werden.
   - **Subnetz für private Endpunkte**: Wählen Sie aus der Dropdown-Liste das Subnetz aus, das die privaten Endpunkte hosten wird.
   - **Subnetz für App Service**: Wählen Sie aus der Dropdown-Liste das für den App Service dedizierte Subnetz aus.
   - **Öffentlichen Zugriff auf App Service einschränken**: Lassen Sie diese Option deaktiviert.

     > **Anmerkung**
     >
     > Wenn Sie **Öffentlichen Zugriff auf App Service einschränken** aktivieren, ist Nerdio Manager nach der Bereitstellung nicht verfügbar. Zusätzliche manuelle Netzwerkkonfiguration ist erforderlich.

   - Wählen Sie **Weiter**.

6. Überprüfen Sie im Bereich **Tags** alle erforderlichen benutzerdefinierten Tags und wählen Sie dann **Weiter** aus.

> **Tipp**
>
> Sie können diesen Tab überspringen.

7. Überprüfen Sie im Bereich **Review + Create** Ihre Auswahl und wählen Sie **Create** aus.

> **Anmerkung**
>
> Ein Bestätigungsfenster wird angezeigt, das Sie darüber informiert, dass die Bereitstellung läuft. Die Bereitstellung dauert in der Regel etwa 10 Minuten.

8. Wählen Sie nach Abschluss der Bereitstellung **Zu Ressourcengruppe wechseln**.
9. Suchen und wählen Sie den **App Service** aus.

> **Anmerkung**
>
> Aktivieren Sie keine Authentifizierung (Identitätsanbieter) für den App Service in Azure (**Einstellungen** > **Authentifizierung**). Nerdio Manager führt seine eigene Entra ID-Authentifizierung auf Anwendungsebene durch; die Aktivierung der Authentifizierung auf App Service-Ebene wird nicht unterstützt und kann den API-Zugriff, Webhooks und die Verarbeitung von Hintergrund-Jobs beeinträchtigen.

Initialisieren

Wenn Nerdio Manager in Ihrem Azure-Abonnement bereitgestellt ist, müssen die folgenden Schritte ausgeführt werden, um Ihre Installation von Nerdio Manager zu initialisieren.

> **Anmerkung**
>
> Wenn Sie die Entra ID-App-Registrierung oder eine geteilte Identität verwenden möchten, fahren Sie mit Nerdio Manager initialisieren (Entra ID-App-Registrierung oder geteilte Identität) [16] fort.

So initialisieren Sie Nerdio Manager (typisch):

1. Öffnen Sie die Nerdio Manager-URL vom App Service aus, indem Sie entweder die Schaltfläche **Durchsuchen** oder den Domänenlink im Bereich **Übersicht** auswählen.
2. Wählen Sie die Kopieren-Schaltfläche, um den Befehl zu kopieren.
3. Wählen Sie **Azure Cloud Shell starten** und melden Sie sich als **globaler Admin** oder **Privileged Role Administrator** in Kombination mit **Cloud Application Administrator** und dem Abonnement-**Owner** an.
4. Wählen Sie bei Bedarf **PowerShell** (nicht Bash) aus und erstellen Sie ein Storage-Konto für den Shell-Verlauf.
5. Fügen Sie den PowerShell-Befehl ein und drücken Sie **Eingabetaste**.

   > **Anmerkung**
   >
   > Mehrere Befehle werden kurz eingeblendet. Die Ausführung des Skripts sollte etwa 10 Minuten dauern.

6. Wenn das Skript abgeschlossen ist, kehren Sie zur Eingabeaufforderung zurück. Die Meldung **Deployment completed successfully** wird angezeigt.

   > **Anmerkung**
   >
   > Wenn die Installation über den Marketplace durchgeführt oder über das Automatisierungskonto aktualisiert wurde, wird die Meldung **NMW-After-Publish <Resource Group Name> <App Service Name>** angezeigt.

7. Wählen Sie die URL in der Bestätigungsmeldung aus. Alternativ kehren Sie zum geöffneten Tab im Browser zurück und aktualisieren die Seite.

Sie sind nun bereit für die nächste Phase des Installationsprozesses – Nerdio Manager-Einstellungen konfigurieren.

So initialisieren Sie den Nerdio Manager (Entra ID-App-Registrierung oder geteilte Identität):

1. Melden Sie sich bei der Nerdio Manager Webanwendung als **globaler Admin** oder **Privileged Role Administrator** in Kombination mit **Cloud Application Administrator** und dem Abonnement-**Owner** an.
2. Wählen Sie **Erweitert anzeigen**.
3. Für die Entra ID-App-Registrierung:
   - **Vorhandene Entra ID-App-Registrierung verwenden**: Wählen Sie diese Option aus.
   - **App-ID**: Geben Sie die App-ID ein.
   - **Dienstprinzipal-ID**: Geben Sie die Dienstprinzipal-ID ein.
4. Für Split Identity:
   - **Split Identity**: Wählen Sie diese Option aus.
   - **Identitäts-Mandanten-ID**: Geben Sie die Identitäts-Mandanten-ID ein.
5. Wählen Sie **Skript herunterladen (Az)**.
6. Suchen Sie auf Ihrem lokalen Computer das heruntergeladene Skript und führen Sie es aus.
7. Wählen Sie die URL in der Bestätigungsmeldung aus. Alternativ kehren Sie zum geöffneten Tab im Browser zurück und aktualisieren die Seite. Sie sind nun bereit für die nächste Phase des Installationsprozesses.

Einstellungen konfigurieren

Nerdio Manager ist jetzt installiert. Der nächste Schritt besteht darin, verschiedene Anwendungseinstellungen zu konfigurieren.

Wenn Sie zur URL navigieren, sehen Sie ein Fenster mit den folgenden Informationen:

Willkommen bei Nerdio Manager for Enterprise Willkommen bei Nerdio Manager for Enterprise

Entra ID Tenant Entra ID Tenant

Tenant: Nerdio Partner Solutions CustomerC - nerdiouniversity.net
Tenant: Nerdio Partner Solutions CustomerC - nerdiouniversity.net

ID: ID:

Azure-Abonnement Azure-Abonnement

Name: VORSCHAU NME - NUR FÜR DEN INTERNEN GEBRAUCH Name: VORSCHAU NME - NUR FÜR DEN INTERNEN GEBRAUCH

ID: ID:

Register Nerdio Manager Register Nerdio Manager

So konfigurieren Sie die Nerdio Manager-Einstellungen:

1. Im Abschnitt **Nerdio Manager-Registrierung**:
   - Wählen Sie **Registrieren Nerdio Manager**.
   - Geben Sie Ihre Registrierungsinformationen ein.
   - Sobald Sie alle Ihre Registrierungsinformationen eingegeben haben, wählen Sie **Registrieren**.
2. Wählen Sie im Abschnitt **Feature-Set** das gewünschte Feature-Set aus:
   - Azure Virtual Desktop
   - Windows 365 (Cloud-PCs)
   - Intune (Physische Endpunkte)

   > **Anmerkung**
   >
   > Sie können ein, zwei oder alle Feature-Sets gleichzeitig einrichten.

   Die Auswahl von **Azure Virtual Desktop** bietet drei Konfigurationsoptionen: **Netzwerk, Directory** und **Dateifreigabe**.

   1. Im Abschnitt **Netzwerk**:
      - Wählen Sie **keine ausgewählt**.
      - **Subnetz**: Wählen Sie aus der Dropdown-Liste das Subnetz aus.
      - Wählen Sie **OK**.
   2. Im Abschnitt **Directory**:

> **Anmerkung**
>
> Das Benutzerkonto für Active Directory, Entra Domain Services oder natives Entra ID muss über die Berechtigung verfügen, Computerobjekte in der Domäne zu erstellen. Nerdio Manager verwendet diese Anmeldedaten beim Hinzufügen von Computern zur Domäne.
>
> Darüber hinaus benötigt das Benutzerkonto bei der Verwendung von Active Directory einige zusätzliche Berechtigungen, um Azure Files-Datenfreigaben mit dem Directory zu verbinden.

- Wählen Sie **keine ausgewählt**.
- Geben Sie Ihre Informationen für Active Directory, Entra Domain Services oder Entra ID ein.
- Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

3. Im Abschnitt **Dateifreigabe**:

> **Anmerkung**
>
> Sie können Ihre FSLogix-Dateifreigabeinformationen oder einen UNC-Pfad zu einer vorhandenen Dateifreigabe angeben, auf die vom VNet aus zugegriffen werden kann. Wenn Sie keine Dateifreigabe bereit haben, wählen Sie die Option, diesen Schritt zu überspringen.

- Wählen Sie **keine ausgewählt**.
- **Diesen Schritt vorerst überspringen**: Wählen Sie diese Option, um diesen Schritt zu überspringen und die Dateifreigabe später zu konfigurieren.
- **FSLogix**: Wählen Sie die FSLogix-Version aus. Standardmäßig wird die neueste Version verwendet.
- **Cloud Cache verwenden**: Wählen Sie diese Option, um FSLogix Cloud Cache in den Hostpools und den Sitzungshosts innerhalb dieser Hostpools zu aktivieren, die dieses FSLogix-Profil verwenden.

> **Tipp**
>
> Aus Leistungsgründen wird dringend empfohlen, Premium-SSD- und ephemere Betriebssystemdatenträger zu verwenden, wenn Cloud Cache aktiviert ist. Standard-SSD-Datenträger könnten in sehr kleinen Umgebungen oder für Testszenarien ausreichen.

> **Anmerkung**
>
> Cloud Cache ermöglicht es Ihnen, mehrere Profilspeicherorte anzugeben. Es repliziert die Profile asynchron und stellt sie gleichzeitig an mehreren Speicherorten zur Verfügung. Wenn also einer der Standorte nicht verfügbar ist, wechselt der Sitzungshost automatisch zu einem der alternativen Orte.
>
> Weitere Informationen zu FSLogix Cloud Cache finden Sie unter Cloud Cache Overview.

- **Registry der Sitzungshosts für Entra ID-verbundenen Speicher konfigurieren**: Wählen Sie diese Option, um die Entra ID Kerberos-Funktionalität und das Laden von Entra ID-Anmeldedaten zu aktivieren.

> **Anmerkung**
>
> Weitere Informationen finden Sie unter Sitzungshosts konfigurieren.

- **App Service-Einstellungen verwalten**: Wählen Sie diese Option, um die Registry-Einstellungen des FSLogix App Service zu bearbeiten.
- **Protokolleinstellungen verwalten**: Wählen Sie diese Option, um die Registry-Einstellungen für das FSLogix-Protokoll zu bearbeiten.
- **FSLogix-Profilpfad (VHDLocation)**: Wählen Sie aus der Dropdown-Liste eine Azure Files-Datenfreigabe oder Azure NetApp Files-Volumes aus. Geben Sie alternativ einen UNC-Pfad ein.

> **Anmerkung**
>
> Sie können bis zu 4 Pfade angeben. Verwenden Sie außerdem die Pfeile, um die Reihenfolge der Pfade zu ändern. Die Profile werden an all diesen Orten erstellt.

- Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

4. Aktivieren Sie optional **Windows 365 & Intune** und konfigurieren Sie anschließend die Features und Scopes:
   - Wählen Sie **konfigurieren**.
   - Aktivieren Sie die erforderlichen Konfigurationsfeatures.
   - Wählen Sie **OK**.

> **Anmerkung**
>
> Einzelheiten zur Aktivierung von Windows 365 in Nerdio Manager finden Sie unter Windows 365 - Enable and Configure Cloud PCs.

So schließen Sie den Installationsprozess ab:

1. Sobald Sie alle oben genannten Einstellungen konfiguriert haben, wählen Sie **Fertig**.
2. Wählen Sie den Link des bereitgestellten Tenant aus.
3. Melden Sie sich als User mit der Rolle Global Administrator an, überprüfen Sie dann die Zustimmung und akzeptieren Sie diese.
4. Navigieren Sie zurück zu Nerdio Manager und wählen Sie **Ich habe die Admin-Zustimmung erteilt**.
5. Wählen Sie **OK**.

> **Anmerkung**
>
> Falls Fehler auftreten, wiederholen Sie bitte die Schritte zur Zustimmung. Dies dauert manchmal einige Minuten. Sie können es einige Male erneut versuchen, bis die Zustimmungen validiert sind.

Die Installation ist nun abgeschlossen und Sie können mit der Nutzung von Nerdio Manager beginnen.

Nerdio Manager Edition Management

Nerdio Manager hat zwei Editionen: **Core** und **Premium**. Die Nerdio Manager Premium-Edition enthält alle Funktionen der Core-Edition sowie viele weitere.

Bitte besuchen Sie unsere Website für Details zu den Funktionen und Preisen.

> **Warnung**
>
> Ein Herunterstufen von Premium auf Core kann zu einem Funktionsverlust führen. Beispielsweise werden erweiterte Kostenoptimierungsfunktionen in der Core-Edition nicht unterstützt. Wenn ein Kunde daher auf Core herunterstufen und Funktionen wie Azure Capacity Extender genutzt hat, sind diese Funktionen nicht mehr verfügbar.

Nerdio Manager ermöglicht es Ihnen, Ihre Edition jederzeit zu ändern.

So ändern Sie Ihre Edition von Nerdio Manager:

1. Navigieren Sie zu **System** > **Einstellungen** > **Nerdio**.
2. Wählen Sie im Bereich **Produktversion** den Namen der Produktversion aus.
3. Überprüfen Sie das Bestätigungs-Pop-up.

> **Tipp**
>
> Beim Herunterstufen auf Core zeigt das Bestätigungs-Pop-up eine detaillierte Liste der Funktionen an, auf die Sie den Zugriff verlieren. Stellen Sie sicher, dass Sie diese sorgfältig prüfen, bevor Sie fortfahren.

4. Wenn Sie bereit sind, Ihre Edition zu ändern, wählen Sie **OK**.

Ihre Edition von Nerdio Manager wurde geändert.

> **Anmerkung**
>
> Vor Version 6.0 von Nerdio Manager konnten Kunden entweder die Standard- oder die Premium-Produktversion des Produkts erwerben. Die oben beschriebenen Lizenzierungsoptionen gelten nur für neue Nerdio Manager-Installationen ab Version 6.0.

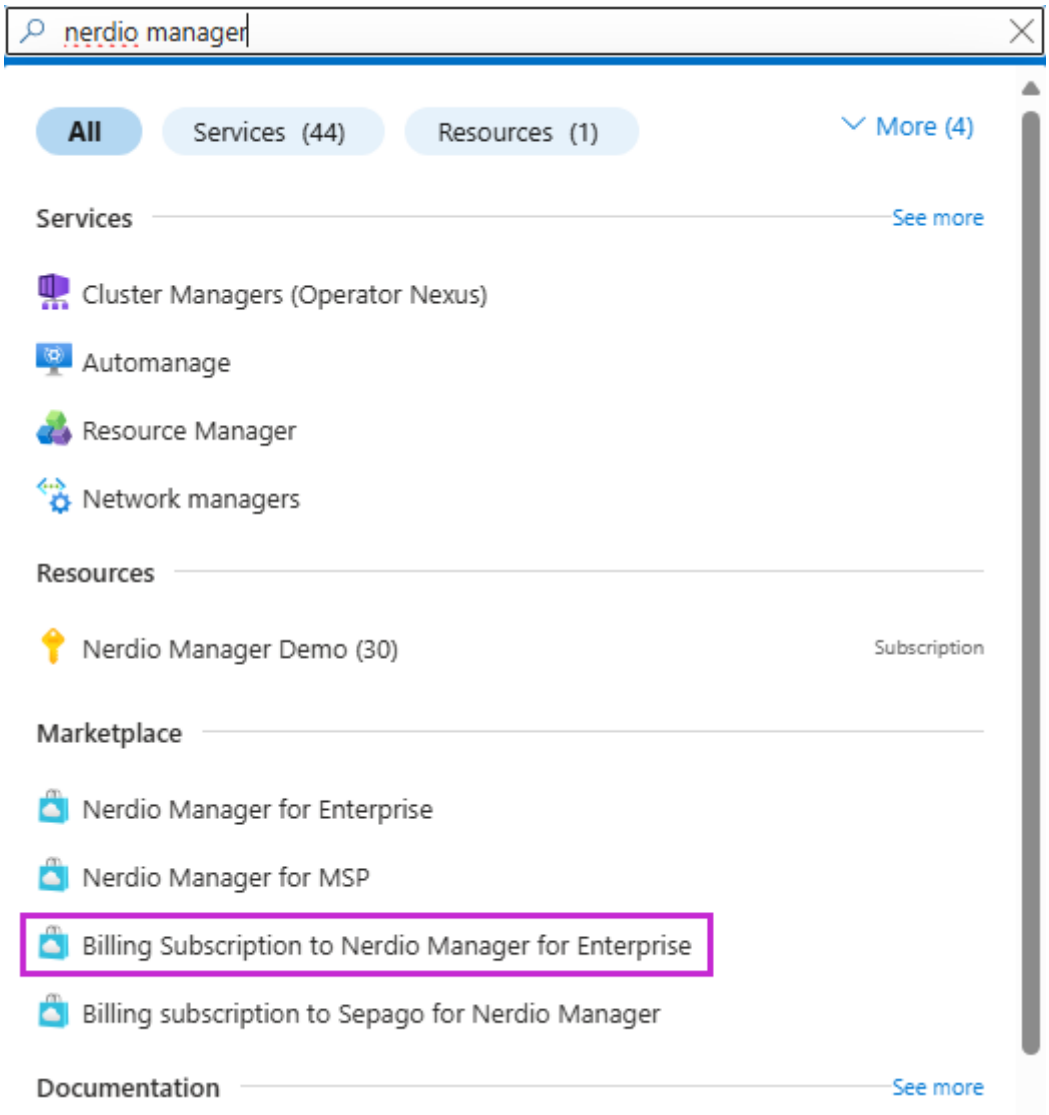
Aktivieren Sie Ihr Abonnement

Um Nerdio Manager über den Testzeitraum hinaus weiter nutzen zu können, müssen Sie das in unserem Azure Marketplace aufgeführte Abrechnungsangebot abonnieren. Dies ermöglicht es Nerdio Manager, die Nutzung an den Azure Marketplace zu melden. Basierend auf Ihrer Nutzung werden Ihnen Nerdio Manager auf Ihrer Azure-Rechnung von Microsoft in Rechnung gestellt.

> **Anmerkung**
>
> Die Aktivierung Ihres Abonnements erstellt auch eine neue App-Registrierung in Entra ID. Diese trägt standardmäßig den Namen NerdioManagerForWVD-Subscribe. Dieser Anwendung werden Azure-API-Berechtigungen erteilt, die es Ihnen ermöglichen, sich zu authentifizieren und die Lizenz zu abonnieren. Weitere Details finden Sie unter Azure-Berechtigungen und Nerdio Manager [6].

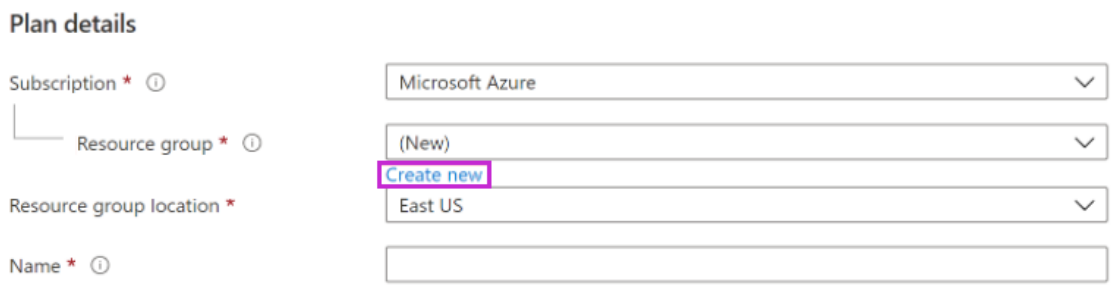
So aktivieren Sie das Nerdio Manager Abonnement:

1. Melden Sie sich bei Ihrem Azure-Portal als **Abonnementbesitzer** des Abonnements an, in dem Sie das Abrechnungsangebot für Nerdio Manager aus dem Azure Marketplace installieren möchten. Das Abonnement, das Sie auswählen, kann sich von dem Abonnement unterscheiden, in dem Sie Nerdio Manager for Enterprise installiert haben.
2. Geben Sie im Suchfeld **Nerdio Manager** ein.
3. Wählen Sie im Abschnitt **Marketplace** der Suchergebnisse die Option **Billing subscription to Nerdio Manager Enterprise** aus.



4. Geben Sie die folgenden Informationen ein:

> **Anmerkung**
>
> Möglicherweise sehen Sie in der Liste **Preis/Zahlungshäufigkeit** einen Preis von 0,00 $/Monat zuzüglich einer Gebühr für **MAU** von 3 $/Benutzer/Monat. Des Weiteren zeigt die **Zwischensumme** 0,00 $ für 1 Monat an. Sie können diesen Teil getrost ignorieren; die unter **Preis/Zahlungshäufigkeit** aufgeführten Gebühren gelten für unser internes Abrechnungssystem. Ihre Preisgestaltung basiert darauf, ob Sie sich für die Core-Edition oder die Premium-Edition anmelden, wie im Abschnitt „Plan“ auf demselben Bildschirm beschrieben. Setzen Sie den Prozess fort, und auf einer nachfolgenden Seite haben Sie die Möglichkeit, sich für die Edition Ihrer Wahl anzumelden.



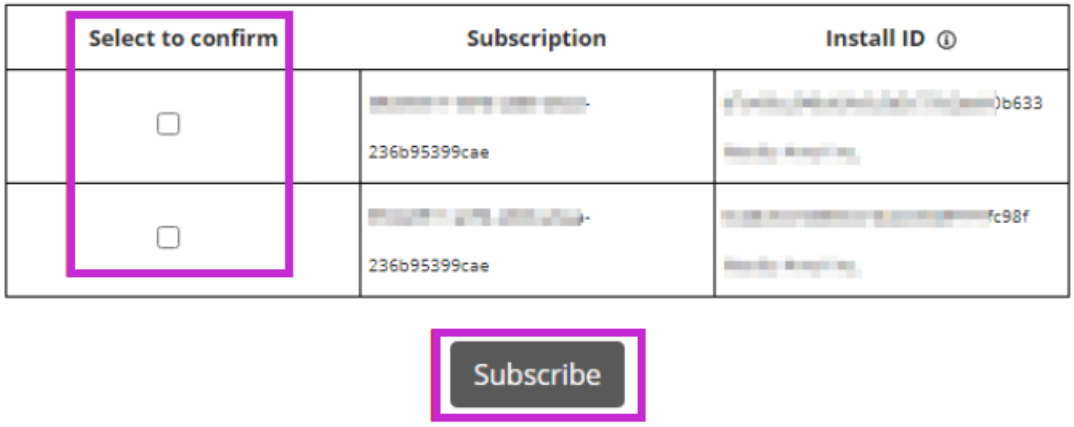
- **Abonnement**: Wählen Sie aus der Dropdown-Liste das Abonnement aus.
- **Ressourcengruppe**: Wählen Sie **Neu erstellen**, um eine neue Ressourcengruppe zu erstellen.
- **Standort der Ressourcengruppe**: Wählen Sie aus der Dropdown-Liste die Region der Ressourcengruppe aus.
- **Name**: Enter **BillingForNerdioManager**.

5. Sobald Sie alle erforderlichen Informationen eingegeben haben, wählen Sie **Überprüfen + abonnieren**.
6. Überprüfen Sie die **Nutzungsbedingungen**.
7. Wählen Sie **Abonnieren**.

   Die Bereitstellung des Angebots beginnt. Der Vorgang dauert etwa 2-3 Minuten. Eine Meldung **Abonnement wird ausgeführt** wird angezeigt.
8. Sobald die Bereitstellung abgeschlossen ist, wählen Sie **Konto jetzt konfigurieren**.

9. Wählen Sie die Installationen aus, für die Sie die Abrechnung starten möchten.

> **Anmerkung**
>
> Sie haben im Allgemeinen nur eine Installation von Nerdio Manager, daher sehen Sie ein aufgelistetes Element.
>
> Die Abrechnung basiert auf monatlich aktiven Benutzern (MAUs). MAUs sind die Anzahl der eindeutigen Benutzer, die im vergangenen Monat eine Verbindung zu einem AVD-Desktop hergestellt haben oder denen zu einem beliebigen Zeitpunkt im vergangenen Monat ein Windows 365 Enterprise Cloud PC zugewiesen wurde.
>
> *[en] For how entitlements are consumed and billed under the Windows Cloud and AVD models, see NME entitlements consumption and billing.*



10. Sobald Sie alle Installationen ausgewählt haben, wählen Sie **Abonnieren**.

Sie haben das Abrechnungsangebot nun abonniert und Ihre Nerdio Manager-Lizenz wurde aktiviert.

> **Anmerkung**
>
> Es ist wichtig, dass die wiederkehrende Abrechnung auf **On** belassen wird, was der Standardeinstellung entspricht.

Azure-Umgebung: verknüpfte Netzwerke und Ressourcengruppen

Nerdio Manager ermöglicht es Ihnen, virtuelle Netzwerke auszuwählen oder zu erstellen, die beim Hinzufügen von Desktop-Images, Hostpools und Sitzungshosts verwendet werden sollen. Die Azure-Region eines bestimmten Netzwerks bestimmt den Standort jeder in diesem Netzwerk erstellten VM.

Sie können auch Ressourcengruppen verknüpfen, die Sitzungshost-VMs und Desktop-Images enthalten können.

> **Anmerkung**
>
> Sie können auch das Standardnetzwerk und die Standardressourcengruppe für Nerdio Manager festlegen, die beim Erstellen eines neuen Desktop-Image, Hostpool oder Sitzungshost verwendet werden sollen. Sie können diese Standardwerte während des Erstellungsprozesses überschreiben.

Verknüpfte Netzwerke verwalten

Nerdio Manager ermöglicht es Ihnen, Netzwerke zu verknüpfen, die Verknüpfung aufzuheben und Netzwerke zu erstellen, die bei der Erstellung neuer Desktop-Images, Hostpools und Sitzungshosts verwendet werden können.

So verknüpfen Sie ein vorhandenes Netzwerk:

1. Navigieren Sie zum **System** > **Einstellungen** > **Azure** Blade.
2. Wählen Sie im Bereich **Verknüpfte Netzwerke** die Option **Link Azure Network** oder **Link Azure Local Network**.

3. Wählen Sie aus der Dropdown-Liste das bzw. die Subnetz(e) aus, die Sie verknüpfen möchten.
4. Wählen Sie **OK**.

   Sie haben das bzw. die angegebenen Netzwerk(e) für die Verwendung beim Erstellen neuer Desktop-Image, Hostpool und Sitzungshost verfügbar gemacht.

So erstellen und verknüpfen Sie ein neues Netzwerk:

> **Anmerkung**
>
> - Weitere Informationen zu den für Ihr Netzwerk verfügbaren Parametern und Einstellungen finden Sie im Microsoft Learn-Artikel Erstellen, Ändern oder Löschen eines virtuellen Netzwerks.
> - Einige der optionalen Konfigurationsobjekte, die Sie neben dem Netzwerk erstellen können, erfordern möglicherweise eine weitere Bearbeitung im Azure-Portal.

1. Navigieren Sie zum **System** > **Einstellungen** > **Azure** Blade.
2. Wählen Sie im Bereich **Verknüpfte Netzwerke** die Option **Create Azure Network**.
3. Geben Sie die folgenden Informationen ein:
   - **Ressourcengruppe**: Wählen Sie aus der Dropdown-Liste die Azure-Ressourcengruppe aus, die das Netzwerk verwenden soll.
   - **Region**: Wählen Sie eine verfügbare Region aus der Dropdown-Liste aus. VMs, die dieses Netzwerk verwenden, werden in dem von Ihnen ausgewählten Netzwerk erstellt.
   - **Name des virtuellen Netzwerks**: Geben Sie einen Anzeigenamen für das virtuelle Netzwerk ein.
   - **IPv6 aktivieren**: Wählen Sie aus, ob das virtuelle Netzwerk IPv6-Adressierung unterstützen soll.
   - **IP-Bereich**: Verwenden Sie die CIDR-Notation, um einen IP-Adressbereich im IPv4- oder IPv6-Adressraum einzugeben, je nachdem, ob Ihr Netzwerk IPv6 unterstützt.

- **Subnetzname**: Geben Sie einen Anzeigenamen für das Subnetz ein.
- **Subnetz**: Geben Sie eine Subnetzadresse in dem oben angegebenen Bereich an.
- **Privates Subnetz aktivieren**: Wählen Sie diese Einstellung, um den standardmäßigen ausgehenden Zugriff zu deaktivieren und sicherzustellen, dass VMs im Netzwerk explizit ausgehenden Internetzugriff erhalten.

> **Anmerkung**
>
> Am 30. September 2025 wird der standardmäßige ausgehende Zugriff für neue Deployments eingestellt. Weitere Informationen finden Sie in der offiziellen Ankündigung sowie in der Anleitung von Microsoft zum Übergang vom standardmäßigen ausgehenden Zugriff zu einer expliziten Methode der öffentlichen Konnektivität. Wir empfehlen die Verwendung eines NAT-Gateways (siehe unten), um dem Netzwerk ausgehenden Internetzugriff bereitzustellen.

- **NAT-Gateway**: Wählen Sie ein vorhandenes NAT-Gateway aus der Dropdown-Liste aus oder geben Sie einen Namen ein, um ein neues zu erstellen. Das NAT-Gateway wird zusammen mit dem Netzwerk erstellt.
- **NSG**: Wählen Sie optional eine NSG aus der Dropdown-Liste aus, um sie mit dem Netzwerk zu verknüpfen, oder geben Sie einen Namen ein, um eine neue zu erstellen. Die NSG wird zusammen mit dem Netzwerk erstellt.
- **Route Table**: Wählen Sie optional eine Route Table aus der Dropdown-Liste aus, um sie mit dem Netzwerk zu verknüpfen, oder geben Sie einen Namen ein, um eine neue zu erstellen. Die Route Table wird zusammen mit dem Netzwerk erstellt.
- **Benutzerdefinierte Tags**: Geben Sie optional die Namen und Werte für alle benutzerdefinierten Metadaten-Tags ein, die Sie mit dem Netzwerk verknüpfen möchten.

4. Klicken Sie auf **OK**. Das Netzwerk und alle zugehörigen Konfigurationsobjekte werden erstellt.

So heben Sie die Verknüpfung eines Netzwerks auf:

1. Navigieren Sie zum **System** > **Einstellungen** > **Azure** Blade.
2. Suchen Sie im Bereich **Verknüpfte Netzwerke** das Netzwerk, dessen Verknüpfung Sie aufheben möchten.
3. Wählen Sie in der Spalte **Aktionen** das Symbol **Verknüpfung aufheben** .
4. Wählen Sie bei der entsprechenden Aufforderung **OK**, um den Vorgang zu bestätigen.

> **Anmerkung**
>
> Ressourcen, die außerhalb von Nerdio Manager im Azure-Portal gelöscht wurden, verhindern nicht die Aufhebung der Verknüpfung bestimmter Netzwerke. Die Aufhebung der Verknüpfung kann erzwungen werden, selbst wenn noch „verwaiste“ Objekte vorhanden sind, die auf das Netzwerk verweisen.

So legen Sie das Standardnetzwerk fest:

1. Navigieren Sie zum Blade **System** > **Einstellungen** > **Azure**.
2. Finden Sie im Bereich **Verknüpfte Netzwerke** das Netzwerk, das Sie als Standard festlegen möchten.
3. Wählen Sie in der Spalte **Aktionen** das Symbol **Als Standard festlegen** .

Verknüpfte Ressourcengruppen verwalten

Nerdio Manager ermöglicht Ihnen das Verknüpfen, Aufheben der Verknüpfung und Erstellen von Ressourcengruppen zur Verwendung beim Erstellen neuer Desktop-Images, Hostpools und Sitzungshosts.

So verknüpfen Sie eine Ressourcengruppe:

1. Navigieren Sie zu **System** > **Einstellungen** > **Azure**.
2. Wählen Sie im Bereich **Verknüpfte Ressourcengruppen** die Option **Verknüpfen**.
3. Wählen Sie aus der Dropdownliste die Ressourcengruppe(n) aus, die Sie verknüpfen möchten.

4. Wählen Sie **OK**.

   Sie haben die angegebenen Ressourcengruppe(n) für die Verwendung beim Erstellen neuer Desktop-Images, Hostpools und Sitzungshosts verfügbar gemacht.

So heben Sie die Verknüpfung einer Ressourcengruppe auf:

1. Navigieren Sie zum Blade **System** > **Einstellungen** > **Azure**.
2. Finden Sie im Bereich **Verknüpfte Ressourcengruppen** die Ressourcengruppe, deren Verknüpfung Sie aufheben möchten.
3. Wählen Sie in der Spalte **Aktionen** das Symbol **Verknüpfung aufheben** .
4. Wählen Sie bei der entsprechenden Aufforderung **OK**, um den Vorgang zu bestätigen.

> **Anmerkung**
>
> Ressourcen, die außerhalb von Nerdio Manager im Azure-Portal gelöscht wurden, verhindern nicht die Aufhebung der Verknüpfung bestimmter Ressourcengruppen. Die Verknüpfung kann auch dann aufgehoben werden, wenn noch „verwaiste“ Objekte vorhanden sind, die auf die Ressourcengruppe verweisen.

So legen Sie die Standard-Ressourcengruppe fest:

1. Navigieren Sie zu **System** > **Einstellungen** > **Azure** Blade.
2. Finden Sie im Bereich **Verknüpfte Ressourcengruppen** die Ressourcengruppe, die Sie als Standard festlegen möchten.
3. Wählen Sie in der Spalte **Aktionen** das Symbol **Als Standard festlegen** .

Übersicht über die Benutzeroberfläche (UI)

Die Benutzeroberfläche von Nerdio Manager ist funktionsreich und anpassbar. Wenn Sie sich anmelden, sehen Sie die Startseite, auf der Ihre konfigurierten Workspaces angezeigt werden.

Zeitzone

Nerdio Manager zeigt alle Datums- und Zeitinformationen in Ihrer lokalen Zeitzone an, wie sie von Ihrem Browser konfiguriert wurde. Bitte überprüfen Sie Ihre Browsereinstellungen oder die Einstellungen Ihres persönlichen Geräts, falls die Zeitzone in Nerdio Manager nicht korrekt ist.

Linker Navigationsbereich

Über den linken Navigationsbereich können Sie die Komponente auswählen, die Sie konfigurieren möchten. Zum Beispiel Komponenten wie **Endpoints** oder **Einstellungen**.

Einige Komponenten verfügen auch über ein Untermenü, auf das durch Auswahl des Pfeils nach unten zugegriffen werden kann. Die zusätzlichen Optionen werden dann angezeigt.

Um Ihre Navigation durch die verschiedenen Menüebenen zu erleichtern, wird eine Brotkrümelnavigation erstellt, damit Sie einfach zu einer früheren Seite in Ihrem Navigationsfluss zurückkehren können.

Symbole im oberen Menü

Oben rechts in der Benutzeroberfläche befinden sich einige Symbole für die folgenden Aufgaben:

Globale Suche

Wählen Sie das Suchsymbol , um innerhalb der Benutzeroberfläche nach einem Thema zu suchen, und geben Sie den Text ein, nach dem Sie suchen möchten. Übereinstimmende Elemente werden zusammen mit einem Link angezeigt, den Sie auswählen können, um zu dieser Seite in der Benutzeroberfläche zu gelangen.

Dark Mode und Light Mode

Die Benutzeroberfläche kann mit einem Dark Mode oder einem Light Mode angezeigt werden.

Wählen Sie im Light Mode das Symbol für den Dark Mode , um zum Dark Mode zu wechseln. Wenn Sie sich im Dark Mode befinden und zum Light Mode wechseln möchten, wählen Sie das Symbol für den Light Mode .

Benachrichtigungen

Wählen Sie das Benachrichtigungssymbol, um alle Systembenachrichtigungen anzuzeigen.

Ankündigungen

Wählen Sie das Ankündigungssymbol, um Ankündigungen anzuzeigen. Sie können auch alle Ankündigungen anzeigen, die zuvor ausgeblendet wurden.

Wählen Sie das Umschlag-Symbol, um die Ankündigung als gelesen zu markieren, oder wählen Sie das Augensymbol, um weitere Details zur ausgewählten Ankündigung anzuzeigen.

Patent

Wählen Sie das Patentsymbol, um zur Seite für geistiges Eigentum von Nerdio auf der Nerdio-Website zu gelangen.

Nerdio Manager Copilot

Wählen Sie das Copilot-Symbol, um das KI-gestützte Hilfesystem zu starten. Weitere Einzelheiten finden Sie unter Nerdio Manager Copilot verwalten [36].

Wissensdatenbank

Wählen Sie das Fragezeichen-Symbol, um zu den Wissensdatenbankseiten von Nerdio auf der Nerdio-Website zu gelangen.

Abmelden

Um sich von Nerdio Manager abzumelden, wählen Sie den Abwärtspfeil neben dem Namen des aktuell angemeldeten Benutzers und wählen Sie dann **Abmelden**.

Tabellenfußzeile

Viele Tabellen verfügen über Fußzeilen, mit denen Sie schnell durch die Tabelle navigieren und die Seitengröße festlegen können. Zusätzlich zeigen einige Tabellen die Gesamtzahl der Zeilen in der Tabelle an.

Aufgaben

Innerhalb einiger konfigurierbarer Komponenten gibt es einen Bereich **Aufgaben** . Dies zeigt ein Protokoll der Aufgaben an, die mit der von Ihnen konfigurierten Komponente verbunden sind, in umgekehrter chronologischer Reihenfolge. Die Seite „Workspaces“ zeigt beispielsweise das Protokoll der Aufgaben an, die an den Workspaces ausgeführt wurden.

Aufgaben und deren Anzahl sind farblich gekennzeichnet: Grün steht für erfolgreich abgeschlossene Aufgaben, Rot für fehlgeschlagene Aufgaben und Gelb für abgebrochene Aufgaben. Aufgaben, die durch das Symbol Aktualisieren hervorgehoben sind, sind Aufgaben, die heute erstellt wurden und sich derzeit in Bearbeitung befinden.

Aufgaben filtern

Sie können Aufgaben nach ihrem Status filtern. Wählen Sie Filter und wählen Sie dann aus der Dropdown-Liste **Nach Aufgabenstatus filtern** den Status aus.

Wenn Sie weitere Details zu einer bestimmten Aufgabe sehen möchten, wählen Sie das Informationssymbol ? neben der Aufgabe aus.

Sie können eine Aufgabe aus der Liste ausblenden, indem Sie das Symbol „Ausblenden“ auswählen.

Wählen Sie für eine Aufgabe, die derzeit in Bearbeitung ist, das Symbol „Abbrechen“ ✕, um die Aufgabe abzubrechen.

Aufgabenexport

Sie können die Aufgabenprotokolle entweder in eine JSON-Datei oder eine CSV-Datei exportieren.

Wählen Sie Export, um die Aufgabenprotokolle als JSON-Datei zu exportieren.

Wählen Sie Export as CSV, um die Aufgabenprotokolle als CSV-Datei zu exportieren.

Die Dateien werden in den Ordner "Downloads" Ihres Browsers heruntergeladen.

Weitere Einzelheiten finden Sie unter Protokollmodul.

Menü „Weitere Aktionen"

Auf mehreren Seiten stehen im Menü „Weitere Aktionen“ zusätzliche Optionen zur Verfügung. Wählen Sie das Symbol „Weitere Aktionen“ ⋮, um auf diese Menüoptionen zuzugreifen.

Sie haben auch Zugriff auf zusätzliche Menüaktionen, indem Sie den Abwärtspfeil auswählen.

Suchen und Filtern

Viele Seiten verfügen über Such- und Filterfunktionen, mit denen Sie die gesuchten Informationen schnell finden können.

> **Anmerkung**
>
> Sie können auch das integrierte Suchfeld auf allen Seiten verwenden, um die in der Tabelle angezeigten Elemente zu filtern. Sie können beispielsweise Hosts finden, die ein bestimmtes Image verwenden. Die Suchergebnisse sind hervorgehoben.

Aktualisieren

Wählen Sie das Symbol Aktualisieren Refresh, um die angezeigte Tabelle zu aktualisieren.

QuickInfos

Wählen Sie das QuickInfo-Symbol ⓘ, um ein Popup-Fenster mit wertvollen Informationen zu dem Feld anzuzeigen, dem die QuickInfo zugeordnet ist.

Eine Tabelle sortieren

Wählen Sie in einer Tabellenspaltenüberschrift das Symbol **Sortieren** ⇕, um die Tabelle nach dieser Spalte auf- oder absteigend zu sortieren.

Mehrfachauswahl und Bulk-Aktionen

Nerdio Manager ermöglicht es Ihnen, mehrere Elemente aus der Liste auszuwählen und Bulk-Aktionen für die ausgewählten Elemente durchzuführen. Zum Beispiel wurden, wie unten gezeigt, drei Sitzungshosts einzeln ausgewählt. Sie können nun Bulk-Aktionen, wie z. B. Einschalten, für die 3 Sitzungshosts durchführen.

> **Anmerkung**
>
> Sie können auf mehreren Seiten mehrere Elemente auswählen. Sie können beispielsweise 2 Sitzungshosts auf der ersten Seite und 4 Sitzungshosts auf der dritten Seite auswählen. Die Bulk-Aktion wird für die 6 Sitzungshosts durchgeführt. Sie können auch alle Hosts auswählen, indem Sie das Kontrollkästchen auf der obersten Ebene neben der Spalte **Name** auswählen.

Benutzerdefinierte Ansichten

Nerdio Manager ermöglicht es Admins, Custom Views zu erstellen, die ihren spezifischen Workflows am besten entsprechen. Es können mehrere Ansichten erstellt werden, und eine der Ansichten kann als Standard festgelegt werden.

Wenn Sie beispielsweise Hostpools über mehrere Workspaces hinweg verwalten, müssen Sie nicht ständig zur Workspace-Liste zurückkehren, um von einem Workspace zum nächsten zu wechseln. Mit Custom Views können Sie ähnliche Daten auf einer einzigen Seite in der gesamten Umgebung kombinieren.

Weitere Einzelheiten finden Sie unter Custom View erstellen.

Custom Views basierend auf einer vorhandenen Seite

Nerdio Manager ermöglicht es Admins, eine Custom View von einer vorhandenen Seite zu erstellen. Sie können beispielsweise eine gefilterte Liste von Hostpools anzeigen und die Seite als Custom View speichern, um den Filter nicht jedes Mal neu erstellen zu müssen.

Weitere Informationen finden Sie unter Custom View aus einer vorhandenen Seite erstellen.

Individualisieren Sie Ihre UI-Designs

Nerdio Manager ermöglicht es Ihnen, Ihre UI-Designs zu individualisieren.

Weitere Informationen finden Sie unter Ihre UI-Designs anpassen.

Nerdio Copilot verwalten

Nerdio Copilot nutzt einen KI-basierten Assistenten, um schnell nach Informationen über Nerdio Manager, seine Features und Funktionen zu suchen.

> **Anmerkung**
>
> Die Verfügbarkeit von Azure OpenAI-Diensten ist begrenzt und variiert je nach Azure-Region.

Nerdio Copilot aktivieren

> **Wichtig**
>
> Nerdio Copilot wurde für NME 8.0 vollständig neu entwickelt und umstrukturiert. Wenn Sie Nerdio Copilot bereits in NME 7.7 oder einer früheren Version bereitgestellt haben, müssen Sie die bisherige Version von Nerdio Copilot deaktivieren.

So deinstallieren Sie die bisherige Version von Nerdio Copilot

1. Navigieren Sie in Nerdio Manager zu **System** > **Einstellungen** > **Nerdio**.
2. Scrollen Sie nach unten und erweitern Sie den Abschnitt **Nerdio Manager Copilot**.

3. Wählen Sie **Konfigurieren** aus.

   Alle Ressourcen, die für die bisherige Version von Nerdio Copilot benötigt wurden, werden angezeigt.
4. Wählen Sie **OK** aus, um diese Ressourcen zu entfernen.

So aktivieren Sie Nerdio Copilot

1. Navigieren Sie in Nerdio Manager zu **System** > **Einstellungen** > **Nerdio**.
2. Scrollen Sie nach unten und erweitern Sie den Abschnitt **Nerdio Manager Copilot**.
3. Wählen Sie **Aktiviert** aus.
4. Geben Sie die folgenden Informationen ein:
   - **Ressourcengruppe**: Wählen Sie aus der Dropdown-Liste die Ressourcengruppe aus, der Sie alle für die Ausführung von Nerdio Manager Copilot erforderlichen Ressourcen zuweisen möchten.
   - **Modell**: Wählen Sie aus den Dropdown-Listen das OpenAI-Modell basierend auf den verfügbaren Vorgaben aus.
   - **Deployment-Typ**: Wählen Sie den Deployment-Typ aus. Data Zone Standard oder Global Standard stehen zur Auswahl.
5. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

   Die Deployment-Aufgabe startet und dauert je nach Azure-Region und anderen Bedingungen etwa 2–5 Minuten. Sie können den Fortschritt der Aufgabe im Abschnitt **Tasks** verfolgen.

Nerdio Copilot verwenden

Sobald Sie alle erforderlichen Azure-Ressourcen bereitgestellt haben, können Sie Nerdio Copilot verwenden, um durch Nerdio Manager zu navigieren.

> **Anmerkung**
>
> **Nerdio Manager** Copilot speichert die KBs des Nerdio Help Centers im Cache, um Ihre Fragen zu beantworten, und aktualisiert den Cache täglich.

So verwenden Sie Nerdio Copilot

1. Wählen Sie in der oberen rechten Ecke von Nerdio Manager das Symbol **Nerdio Manager Copilot** .

   Nerdio Manager stellt eine Verbindung zum Bot her und lädt den Chatverlauf herunter.
2. Stellen Sie eine beliebige Frage zu Nerdio Manager und senden Sie diese an Copilot. Nach kurzer Zeit zeigt Copilot eine Antwort an.
3. Wählen Sie optional **Zitate**, um eine Liste der zitierten Knowledge Base-Artikel anzuzeigen.
4. Sie können entweder die Seitenleistenansicht oder die Ansicht in einem separaten Fenster auswählen.

Chat-Einstellungen von Nerdio Copilot verwalten

Sie können die Einstellungen von Nerdio Copilot jederzeit anpassen.

So verwalten Sie die Chat-Einstellungen von Nerdio Copilot

1. Wählen Sie das Symbol **Einstellungen** .
2. Geben Sie die folgenden Informationen ein:
   - **Intents-Erkennungsdienst OpenAI-Modell**: Wählen Sie aus der Dropdown-Liste das gewünschte Modell aus.
   - **Maximale Anzahl der Tage zur Aufbewahrung des Verlaufs**: Geben Sie die Anzahl der aufzubewahrenden Chatverläufe ein.
3. Sobald Sie die gewünschten Informationen eingegeben haben, wählen Sie **Speichern**.
4. Wählen Sie bei Aufforderung **Bestätigen**, um Ihre Änderungen zu bestätigen.

Feedback senden

Copilot verwendet Azure OpenAI, das auf einem Large Language Model (LLM) basiert, welches mit Nerdio-spezifischen Informationen erweitert wurde. Da es sich um ein LLM handelt, sind die Antworten nicht deterministisch. Weitere Details finden Sie unter Einführung in Large Language Models.

Wenn Sie eine falsche Antwort bemerken, können Sie auf folgende Weise Feedback geben:

- Geben Sie einen Kommentar ein (optional).
- Folgen Sie dem standardmäßigen Eskalationspfad für den Support von Nerdio.

Nerdio Copilot deaktivieren

Gehen Sie wie folgt vor, um Nerdio Copilot zu deaktivieren.

> **Anmerkung**
>
> Durch das Deaktivieren von Nerdio Copilot werden alle Azure-Ressourcen entfernt, die beim Aktivieren des Features bereitgestellt wurden, mit Ausnahme der **Regel für Smart-Detector-Warnungen**.

So deaktivieren Sie Nerdio Copilot

1. Navigieren Sie in Nerdio Manager zu **System** > **Einstellungen** > **Nerdio**.
2. Scrollen Sie nach unten, erweitern Sie den Abschnitt **Nerdio Manager Copilot** und wählen Sie **Konfigurieren**.
3. Wählen Sie bei der entsprechenden Aufforderung **OK**.

   Die Aufgabe zur Deaktivierung startet und dauert je nach Azure-Region und anderen Bedingungen etwa 2–3 Minuten. Sie können den Fortschritt der Aufgabe im Abschnitt **Tasks** verfolgen.

Skripte mit Nerdio Copilot erstellen

Nerdio Copilot enthält Script Pro, mit dem Sie Skripte mit KI-Unterstützung erstellen können.

> **Warnung**
>
> Stellen Sie sicher, dass alle KI-generierten Skripte vor der Bereitstellung in Ihren Produktionsumgebungen manuell getestet und validiert werden.

Skript mit Nerdio Copilot erstellen

1. Öffnen Sie Nerdio Copilot.
2. Stellen Sie eine Frage zur Erstellung eines Skripts. Zum Beispiel:

   ```
   Can you help me generate a management script for a Windows VM to set t
   [HKEY_LOCAL_MACHINE\SOFTWARE\MyApp]"NewFeatureEnable"=dword:1
   ```
3. Folgen Sie den Anweisungen und antworten Sie bei Bedarf.
4. Wenn das Skript generiert wurde, kopieren Sie den Code.

KQL-Abfragen mit Nerdio Copilot AnalyticsPro generieren

AnalyticsPro ist ein leistungsstarkes Tool in Nerdio Copilot, das Ihre Fragen in natürlicher Sprache in Abfragen in Kusto Query Language (KQL) umwandelt. Mit AnalyticsPro können Sie mühelos KQL-Abfragen generieren, die in Ihrem Azure Log Analytics-Workspace ausgeführt werden können. So gewinnen Sie wertvolle Insights aus Ihren Daten, ohne komplexe Abfragesyntax beherrschen zu müssen.

So generieren Sie eine KQL-Abfrage mit AnalyticsPro:

1. Öffnen Sie Nerdio Copilot.
2. Geben Sie die Details der KQL-Abfrage ein, die Sie generieren möchten. Zum Beispiel:

   ```
   Can you write me a KQL query to get the number of active users from th
   ```
3. Wählen Sie das Symbol „Senden“ aus.
4. Die KQL-Abfrage wird generiert.
5. Sie können mit AnalyticsPro interagieren und basierend auf den Ergebnissen nach zusätzlichen Informationen fragen oder Optionen bereitstellen, um Ihre Abfrage zu verfeinern. Reagieren Sie bei Bedarf auf diese Eingabeaufforderungen, um die Abfrage an Ihre spezifischen Anforderungen anzupassen.
6. Sobald der Vorgang abgeschlossen ist, können Sie die Abfrage kopieren und in Ihrem Azure Log Analytics-Workspace ausführen.

> ⚠ **Warnung**
>
> Stellen Sie sicher, dass alle KI-generierten Abfragen vor der Bereitstellung in Ihren Produktionsumgebungen manuell getestet und validiert werden.

Kosten von Nerdio Copilot

Die Kosten des Features hängen von seiner Nutzung ab. Die Kosten basieren auf den verwendeten Token, wobei die Kosten je nach gewähltem Modell und Nutzungsumfang variieren.

Wenn das Feature aktiviert, aber nicht genutzt wird, fallen keine laufenden Kosten an.

Funktionale Überlegungen

LLM-Implementierungsarbeit mit Token. Die Anzahl der Token ist eine Kombination aus System-Prompt, User-Eingabe und LLM-Ausgabe. Die Anzahl der Token definiert, wie viel „Gedächtnis“ über einen vorherigen Austausch im aktuellen Gespräch der Bot hat. Wenn ein Gespräch lang ist, also größer als die für das Modell konfigurierte maximale Token-Anzahl, werden ältere Daten verworfen. Wir zeigen jedoch den gesamten Chatverlauf in der Benutzeroberfläche an, bis der Chatverlauf über die Schaltfläche „Verlauf löschen“ gelöscht wird.

Bereitstellungsüberlegungen

Standardmäßig stellt Nerdio Copilot alle Ressourcen in derselben Region bereit. Azure OpenAI-Ressourcen können je nach Auswahl des Users in verschiedenen Regionen erstellt werden. Wo möglich, stellen wir Ressourcen der kostenlosen oder der günstigsten kostenpflichtigen Tarifstufe bereit. Diese Auswahl lässt sich nicht konfigurieren.

Bekannte Einschränkungen

- User können das Drosselungslimit pro Tag und/oder Monat nicht steuern.
- Es gibt keinen Support für Benachrichtigungen.

- Es gibt keinen Mechanismus zur Identifizierung und zum Filtern falsch positiver Ergebnisse.
- Smart-Detector-Warnregeln werden nicht gelöscht, wenn Copilot deaktiviert wird.

Zeitpläne für Aufgaben verwalten

Nerdio Manager unterstützt die Möglichkeit, Zeitpläne für Aufgaben zu konfigurieren.

Der Zeitplan kann einen oder mehrere Einträge enthalten, wie in diesen Beispielen gezeigt:

- Sie können einen Zeitplan erstellen, um einen Host heute um 18:00 Uhr auszuschalten.
- Sie können einen Zeitplan erstellen, um dieselbe Scripted Action auf einem Hostpool am Montag um 07:00 Uhr, am Dienstag um 21:00 Uhr und am Sonntag um 03:00 Uhr auszuführen.
- Sie können einen Zeitplan erstellen, um Hosts montags und donnerstags um 23:00 Uhr neu zu starten, und diesen jede Woche wiederholen lassen.

Einige der Funktionen, die Zeitpläne mit mehreren Einträgen ermöglichen, sind:

- **Desktop-Images**: Scripted Actions ausführen
- **Scripted Actions**: Run Azure Runbook
- **Hostpools**: Größe anpassen oder Reimaging vornehmen, einschalten/ausschalten, Hosts neustarten, Nachricht senden, alle Hosts abmelden, Hosts aktivieren/deaktivieren, Scripted Actions ausführen
- **Sitzungshosts** (außer Hybrid): Größe anpassen oder Reimaging vornehmen, Ein-/Ausschalten, Hosts neustarten, Nachricht senden, Hosts aktivieren/deaktivieren, Skriptaktion ausführen
- **Advisor**: Größe anpassen Sitzungshost, Größe anpassen Hostpool

Mehrere Zeitpläne für eine Aufgabe erstellen

Nerdio Manager ermöglicht es Ihnen, mehrere Zeitpläne für eine Reihe von Aufgaben zu erstellen.

So erstellen Sie mehrere Zeitpläne für eine Aufgabe:

1. Navigieren Sie zu der Aufgabe, die Sie ausführen möchten.

   > **Anmerkung**
   >
   > In diesem Beispiel starten wir einen Sitzungshost neu. Wie oben erwähnt, können für eine Reihe von Aufgaben mehrere Zeitpläne erstellt werden.

2. Wählen Sie den Bereich **Zeitplan**.
3. Geben Sie im Abschnitt **Zeitplan** den gewünschten Zeitplan ein.
   - **Startdatum**: Geben Sie das Startdatum ein.
   - **Zeitzone**: Wählen Sie aus der Dropdown-Liste die Zeitzone für die Startzeit aus.
   - **Startzeit**: Wählen Sie aus den Dropdown-Listen die Startzeit aus.
   - **Wiederholen**: Wählen Sie aus der Dropdown-Liste aus, ob dieser Vorgang einmalig ausgeführt oder in einem wiederkehrenden Zeitplan wiederholt werden soll.

     > **Anmerkung**
     >
     > Die Dropdown-Liste enthält die Option **Nach Patch Tuesday**. Dies ermöglicht es Ihnen, einen wiederkehrenden Zeitplan basierend auf Patch Tuesday zu erstellen.

   - **Wochentag**: Wählen Sie aus der Dropdown-Liste den Tag für den wiederkehrenden Zeitplan aus.
   - **Tage nach**: Wenn Sie **Nach Patch Tuesday** ausgewählt haben, geben Sie die Anzahl der Tage nach dem Patch Tuesday ein, an denen die geplante Aufgabe ausgeführt werden soll.
4. Nachdem Sie den Zeitplan eingegeben haben, wählen Sie **Speichern**.

   Zeitplan 1 wird der Aufgabe hinzugefügt.
5. Wenn Sie weitere Einträge hinzufügen möchten, wählen Sie oben rechts neben **Zeitplan** das Symbol **Zeitplan hinzufügen**.
6. Fügen Sie den nächsten Zeitplan hinzu und speichern Sie ihn, und wiederholen Sie dies für alle gewünschten Zeitplaneinträge.

Aufgabenzeitpläne verwalten

Nerdio Manager ermöglicht es Ihnen, Aufgabenzeitpläne zu verwalten. Dies umfasst das Ändern und Löschen von Zeitplaneinträgen.

So verwalten Sie Aufgabenzeitpläne:

1. Navigieren Sie zu der Aufgabe mit dem Zeitplan, mit dem Sie arbeiten möchten.
2. Wählen Sie in der Liste (zum Beispiel Hosts, Hostpool usw.) das Symbol **Zeitplan**.
3. Wählen Sie in der Zeitplanliste den Zeitplan aus, mit dem Sie arbeiten möchten.
4. Ändern oder entfernen Sie den Zeitplaneintrag wie gewünscht.
5. Alternativ öffnen Sie die Aufgabe (zum Beispiel einen Sitzungshost neu starten) und wählen Sie im Bereich **Zeitplan** aus der Dropdown-Liste den Zeitplaneintrag aus, den Sie ändern oder entfernen möchten.
6. Sobald Sie die gewünschten Änderungen vorgenommen haben, wählen Sie **Speichern**.

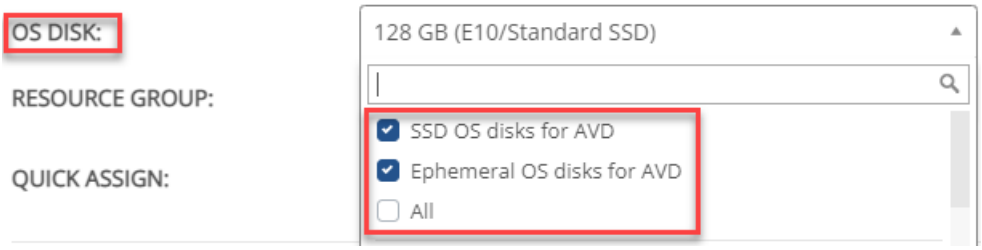
Verwaltung von Ressourcenauswahlregeln

Mit Nerdio Manager können Sie Regeln für Empfehlung und zum filtern erstellen, die Sie bei der Auswahl von VM-Größen und Betriebssystemdatenträgern beim Erstellen von Hostpools oder beim Hinzufügen von Sitzungshost-VMs unterstützen.

Ressourcenauswahlregeln können verwendet werden, um die beste VM für einen spezifischen AVD Use Case vorzuschlagen, wobei die Rechenkernverfügbarkeit berücksichtigt wird. Sie können auch verwendet werden, um die Arten von VMs und Betriebssystemdatenträgern zu begrenzen, die global in einem Workspace oder sogar auf Hostpool-Ebene verwendet werden können.

Die VMs können basierend auf der vCPU-Verfügbarkeit in einem ausgewählten Abonnement und einer Region, dem Prozessor, der VM-Familie & Version, der Anzahl der Rechenkerne & GB RAM sowie dem lokalen temporären Speicher gefiltert werden. Betriebssystemdisks können basierend auf dem Speichertyp (Premium, Standard, SSD, HDD oder Ephemeral) und der Diskgröße gefiltert werden.

Wenn Sie beispielsweise einen dynamischen Hostpool hinzufügen, können Sie die Auswahlmöglichkeiten für **VM-Größe** oder **OS Disk** filtern, indem Sie die gewünschte(n) Ressourcenauswahlregel(n) auswählen.



Erstellen Sie eine Ressourcenauswahlregel

Eine Ressourcenauswahlregel muss erstellt werden, um sie für Empfehlung und zum filtern einzusetzen.

So erstellen Sie eine Ressourcenauswahlregel:

1. Navigieren Sie zu **System** > **Einstellungen** > **Ressourcenregeln**.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie die folgenden Informationen ein:
   - **Name**: Geben Sie den Namen der Regel ein.
   - **Beschreibung**: Geben Sie die Beschreibung der Regel ein.
   - **Scope**: Wählen Sie aus der Dropdown-Liste den Scope der Regel aus.

> **Anmerkung**
> - **Anzeigen, wenn keine expliziten Regeln vorhanden sind**: Zeigen Sie die Auswahl dieser Regel in allen Dropdown-Listen für VM-Größen und OS Disks an, sofern keine Regel mit einem expliziten Scope gilt.
> - **Überall anzeigen**: Zeigen Sie die Auswahlen dieser Regel in allen Dropdown-Listen für VM-Größen und OS Disk an.
> - **Desktop-Image**: Zeigen Sie die Auswahl dieser Regel an, wenn Sie auf der Seite „Desktop-Image“ mit VMs arbeiten.
> - **Temporäre VMs**: Zeigen Sie die Auswahl dieser Regel an, wenn Sie mit temporären VMs arbeiten.
> - **Einzelner Workspace oder Hostpool**: Zeigen Sie die Auswahl dieser Regel nur für den/die ausgewählten Workspace(s) oder Hostpool(s) an.

- **Kosten anzeigen**: Wählen Sie in der Dropdown-Liste **Ja**, um in der Dropdown-Liste „VM-Größe“ die monatlichen Kosten anstelle der Größenkategorie anzuzeigen.

  > **Anmerkung**
  >
  > Dies gilt nur, wenn diese Regel als oberste Regel ausgewählt ist.

- **Standard ausgewählt**: Wählen Sie in der Dropdown-Liste **Ja**, um diese Regel automatisch zu aktivieren, wenn eine Dropdown-Auswahlliste geöffnet wird, für die diese Regel gilt. Wählen Sie **Nein**, und diese Regel wird nicht automatisch ausgewählt.
- **Regeln für die VM-Größenauswahl**: Schalten Sie um, um die VM-Größenregeln für das Filtern zu definieren.
  - **Prozessor**: Wählen Sie den Prozessorhersteller aus der Dropdown-Liste aus.
  - **VM-Familienversion**: Wählen Sie die VM-Familienversion(en) aus der Dropdown-Liste aus.
  - **VM-Familientyp**: Wählen Sie die einzelnen VM-Familien oder Use Case-optimierte VM-Familien aus der Dropdown-Liste aus.
  - **VM-Typ ausschließen**: Wählen Sie aus der Dropdown-Liste die auszuschließenden einzelnen VM-Familien aus.
  - **CPU-Kerne**: Wählen Sie aus der Dropdown-Liste die Anzahl der Rechenkerne aus.

    > **Anmerkung**
    >
    > Alle VMs, die der Anzahl der Rechenkerne entsprechen oder zwischen der Auswahl und der nächsten Zweierpotenz liegen, werden angezeigt. Wenn Sie beispielsweise 4 Rechenkerne auswählen, werden VMs mit 4 und 6 Rechenkernen berücksichtigt.

  - **RAM (GB)**: Wählen Sie aus der Dropdown-Liste die Größe des Speichers aus.

> **Anmerkung**
>
> Alle VMs, die der Größe des Speichers entsprechen oder zwischen der Auswahl und der nächsten Zweierpotenz liegen, werden angezeigt. Wenn Sie beispielsweise 4 GB Speicher auswählen, werden VMs mit 4 und 6 GB Speicher berücksichtigt.

- **Lokaler Speicher**: Wählen Sie aus der Dropdown-Liste aus, ob die VMs über temporären lokalen Speicher verfügen.

> **Anmerkung**
> - **Ja**: Filtern Sie nach VMs mit lokalem temporärem Speicher.
> - **Nein**: Filtern Sie nach VMs ohne lokalen temporären Speicher.

- **VM-Verfügbarkeit**: Wählen Sie aus der Dropdown-Liste den Verfügbarkeitstyp aus.

> **Anmerkung**
> - **Nur basierend auf Abonnement & Region**: Validieren Sie nicht die Zuweisung der Rechenkern-Vorgabe. Stellen Sie nur sicher, dass der VM-Typ im ausgewählten Abonnement und der ausgewählten Region verfügbar ist.
> - **Basierend auf CPU-Rechenkern-Vorgabe**: Überprüfen Sie dynamisch, ob im ausgewählten Abonnement und in der ausgewählten Region ausreichend Rechenkern-Vorgabe verfügbar ist, und zeigen Sie nur die VMs an, die bereitgestellt werden können.

- **Sortieren nach**: Wählen Sie aus der Dropdown-Liste das Sortierkriterium aus.

> **Anmerkung**
>
> **Alphabetisch** ist ein eigenständiges Sortierkriterium. Die anderen Optionen können kombiniert werden.

- **Regeln für die Disk-Größenauswahl über Dropdown-Liste**: Schalten Sie um, um die Disk-Größenregeln für das Filtern zu definieren.
  - **Speichertyp**: Wählen Sie aus der Dropdown-Liste den oder die Speichertypen aus.
  - **Betriebssystem-Diskgröße**: Wählen Sie aus der Dropdown-Liste die Diskgröße(n) aus.

> **Anmerkung**
>
> Bei **ephemeren Betriebssystem-Disks** entspricht die Diskgröße möglicherweise nicht exakt der Auswahl. In solchen Fällen werden die EOSD-Größen angezeigt, die zwischen der Auswahl und der nächsten Zweierpotenz liegen. Beispielsweise entspricht die Auswahl von 64 GB einem EOSD von 75 GB.

4. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

   Die Ressourcenauswahlregel wurde erstellt.

Ressourcenauswahlregeln verwalten

In der Tabelle „Ressourcenauswahlregeln“ können Sie Folgendes tun:

- **Bearbeiten**: Bearbeiten Sie die Regel.

> **Anmerkung**
>
> Integrierte Regeln können nicht bearbeitet werden. Sie müssen die Regel kopieren und die Kopie bearbeiten.

- **Klonen**: Erstellen Sie eine Kopie der Regel.

- **Deaktivieren**: Deaktivieren Sie die Regel.

> **Anmerkung**
>
> Deaktivierte Regeln werden in keinen Dropdown-Auswahllisten angezeigt.

- **Aktivieren**: Aktivieren Sie eine deaktivierte Regel.
- **Löschen**: Löschen Sie die Regel.
- **Reihenfolge ändern**: Verschieben Sie die Bänder wie gewünscht nach oben und unten.

> **Anmerkung**
>
> Dies ist die Reihenfolge, in der die Auswahlen in den Dropdown-Listen angezeigt werden, wenn Sie einen Hostpool oder eine Sitzungshost-VM erstellen.

Schritt 2 Desktop-Images

Sobald Nerdio Manager installiert ist, besteht der nächste Schritt darin, die Desktop-Images vorzubereiten, aus denen Ihre Hostpools erstellt werden – unabhängig davon, ob Sie vorhandene Images importieren oder Nerdio Manager neue für Sie verwalten lassen.

In diesem Abschnitt:

1. Desktop-Images [49]
2. Verwaltungs- und Lifecycle-Aufgaben für importierte Desktop-Images [50]
3. Desktop-Image erstellen [53]
4. Desktop-Images: als Image festlegen [63]
5. Scripted Actions für Desktop-Images [72]

Desktop-Images

Dieser Abschnitt behandelt Themen rund um Desktop-Images. Wir werden die verschiedenen Import- und Lifecycle-Management-Optionen sowie

unterschiedliche Möglichkeiten zur Automatisierung bestimmter Aufgaben in fortgeschritteneren Szenarien besprechen.

Nachdem Sie einen neuen Workspace erstellt haben, erstellen Sie als Nächstes einen oder mehrere Hostpools für Ihre virtuellen Maschinen. Weitere Informationen finden Sie unter Hostpools [75]. Virtuelle Maschinen werden auf der Grundlage eines Desktop-Images erstellt, das das Betriebssystem, Ihre Anwendungen und alles Weitere enthält, das Sie hinzufügen möchten. Damit dies funktioniert, müssen wir zunächst mindestens ein Desktop-Image erstellen.

Bevor wir fortfahren, ist es wichtig zu verstehen, dass Images auf unterschiedliche Weise erstellt oder importiert werden können. Selbst wenn keine Images in Nerdio Manager importiert wurden, können die benutzerdefinierten Azure-Images Ihres Abonnements verwendet werden, um neue Hostpools zu erstellen und bei bestehenden Hostpools Reimaging vornehmen.

Wenn Sie sich entscheiden, Ihre Images in Nerdio Manager zu importieren, können Sie viele verschiedene Verwaltungsfunktionen nutzen, die sonst nicht verfügbar wären.

Darüber hinaus werden bei importierten Images in Nerdio Manager alle Ihre Verwaltungs- und Lebenszyklusaktivitäten über ein einziges Verwaltungsportal durchgeführt.

Sobald ein Image erstellt oder importiert wurde – unabhängig vom Imagetyp (wir werden dies im weiteren Verlauf näher erläutern) – werden neue Hostpools erstellt und bei bestehenden Hostpools Reimaging vornehmen. In den folgenden Abschnitten führen wir Sie Schritt für Schritt durch den Prozess.

Verwaltungs- und Lebenszyklusaufgaben für importierte Desktop-Images

Unabhängig davon, woher Ihre Desktop-Images importiert wurden, sind deren Verwaltungs- und Lebenszyklusaufgaben identisch.

Typischer Lebenszyklus eines Desktop-Images

Der typische Lebenszyklus eines Desktop-Images sieht wie folgt aus:

1. Importieren Sie das Desktop-Image.

   Detaillierte Informationen finden Sie unter Erstellen eines Desktop-Images [53].
2. Desktop-Image einschalten:
   a. Navigieren Sie zu **Cloud-Desktop** > **Desktop-Images**.
   b. Finden Sie das Desktop-Image, das Sie einschalten möchten.
   c. Wählen Sie **Einschalten**.
3. Verwenden Sie die IP-Adresse oder den Namen der VM, um eine Verbindung über RDP herzustellen und alle gewünschten Änderungen vorzunehmen.
4. Wählen Sie **Ausschalten und als Image festlegen**.

   Einzelheiten finden Sie unter Desktop-Images als Image festlegen [63].

   > **Anmerkung**
   >
   > Ein umfassender Automatisierungsprozess beginnt, der die Änderungen an einem Image-Objekt durch "Commit ausführen" übernimmt. Dies umfasst viele Aufgaben, die Sie manuell hätten ausführen müssen, wie z. B. Sysprep durchführen und das Versiegeln des Images.
   >
   > Sie können den Fortschritt des Jobs in den Protokollen sehen. Weitere Informationen zu den Protokollen finden Sie unter Feature „Änderungsprotokoll für Desktop-Images“.
5. Sobald das Image festgelegt ist, können Sie es verwenden, um neue Hostpools zu erstellen oder bei einem vorhandenen Hostpool ein Reimaging vornehmen.

   Weitere Informationen finden Sie unter:
   - Dynamische Hostpools erstellen [78]
   - Statische Hostpools ohne automatische Skalierung erstellen
   - Größe eines Hostpools anpassen oder ein Reimaging des Hostpools vornehmen

Integration von Endpoint-Management-Software

Nerdio Manager ermöglicht es Ihnen, die Leistungsfähigkeit eines Endpoint-Management-Tools (zum Beispiel Microsoft Endpoint Configuration Manager oder Ivanti Endpoint Manager) zu nutzen, um damit mit Nerdio Manager zu arbeiten.

Beispiel für die Integration von Endpoint-Management-Software

Der Patch Tuesday, an dem Microsoft seine monatlichen Software-Updates veröffentlicht, findet am zweiten Dienstag jedes Monats gegen 10 Uhr Pacific Standard Time statt. Sie können Ihr Endpoint-Management-Tool zusammen mit Nerdio Manager verwenden, um die Windows-Updates auf das Desktop-Image vollständig zu automatisieren und bei den Hostpools mit dem aktualisierten Desktop-Image Reimaging vornehmen.

> **Anmerkung**
>
> Dies ist nur ein Beispiel für die vielen Dinge, die Sie mit diesen integrierten Automatisierungstools tun können.

- Stellen Sie in Nerdio Manager bei der Ausführung der Funktion **Als Image festlegen** sicher, dass Sie die Option **Desktop-Image-VM im Betrieb belassen** auswählen. Dadurch bleibt die VM nach Abschluss der Aufgabe **Als Image festlegen** in Betrieb, und das Endpoint-Management-Tool kann auf die VM zugreifen und das Image ändern.
- Erstellen Sie im Endpoint-Management-Tool am Patch Tuesday einen wiederkehrenden geplanten Job/Runbook, um die Windows-Updates anzuwenden.
- Konfigurieren Sie in Nerdio Manager die Funktion **Als Image festlegen** für das Desktop-Image als wiederkehrenden Job, der kurz nach Abschluss des Jobs des Endpoint-Management-Tools startet. Weitere Informationen zur Konfiguration des Jobs finden Sie unter Desktop-Images als Image festlegen [63].
- Konfigurieren Sie in Nerdio Manager die Funktion **Reimaging für Hosts vornehmen** für den Hostpool als wiederkehrenden Job, der kurz nach

Abschluss des Prozesses **Als Image festlegen** startet. Weitere Informationen zur Konfiguration des Jobs finden Sie unter Größe eines Hostpools anpassen/Reimaging vornehmen.

Durch das Erstellen von drei wiederkehrenden geplanten Jobs können Sie also jeden Monat die Windows-Updates auf die VM anwenden, das VM-Image als Image festlegen und dann den Hostpool mit dem aktualisierten Desktop-Image aktualisieren.

Desktop-Image erstellen

Nerdio Manager for Enterprise: Sie können ein Desktop-Image aus einem vorhandenen Image in der Azure-Bibliothek erstellen oder eine vorhandene Azure-VM dafür importieren.

Assistenten zum Erstellen von Desktop-Images öffnen

1. Navigieren Sie zu **Cloud-Desktops** > **Desktop-Images**.
2. Wählen Sie unten rechts auf der Seite **Erstellen** aus.

   Das Dialogfeld **Desktop-Image erstellen** wird geöffnet. Es enthält die folgenden Abschnitte: **VM**, **AD-Beitritt**, **Einstellungen**, **Bereinigung**, **Scripted Actions & Apps**, **Image**, **Replikation** und **Tags**.

VM konfigurieren

1. Wählen Sie die Tabelle aus, die zur Quelle Ihres Desktop-Images passt, und geben Sie die aufgeführten Informationen ein.

   Anmerkung

   Für einige der erforderlichen Parameter können Sie die verfügbaren Auswahlmöglichkeiten mithilfe der Ressourcenauswahlregeln filtern. Sie können beispielsweise die verfügbaren VM-Größen oder OS-Disks so filtern, dass nur Optionen für RAM-optimierte Intel-VMs angezeigt werden. Weitere Informationen finden Sie unter Verwaltung der Ressourcenauswahlregeln [44].

Azure-Bibliothek

UI-Element	Typ	Beschreibung
Quelle	Dropdown-Liste	Wählen Sie in der Dropdown-Liste **Azure-Bibliothek** aus, um das Image aus einem vorhandenen Image in Ihrer Bibliothek zu erstellen.
Name	Textfeld	Geben Sie den Namen des Desktop-Images ein.
Beschreibung	Textfeld	Geben Sie die Beschreibung ein.
Netzwerk	Dropdown-Liste	Wählen Sie das Netzwerk aus, mit dem die VM verbunden werden soll. Die VM wird in der Azure-Region erstellt, die dem Netzwerk zugeordnet ist.
Azure-Image	Dropdown-Liste	Wählen Sie ein Image aus, das Ihre Anforderungen an das Windows-Betriebssystem erfüllt und von AVD unterstützt wird, beispielsweise Windows 11 EVD Multi-Session (EVD = Enterprise Virtual Desktop). Images mit der Bezeichnung Microsoft 365 Apps enthalten eine vorinstallierte Version von Microsoft 365 Apps for Enterprise, die aktiviert wird, wenn sich lizenzierte User am Desktop anmelden. Die Liste enthält alle Standard-Azure Marketplace-Images sowie alle benutzerdefinierten verwalteten Images, die in Ihrem Azure-Abonnement verfügbar sind.
„Staged"-Image-Version verwenden	Umschalter	Wenn diese Option aktiviert ist, wird das Desktop-Image mit der „Staged"-Image-Version des ausgewählten Desktop-Images erstellt, sofern eine verfügbar ist. Diese Einstellung ist nur für Desktop-Images verfügbar, bei denen „Geografische Verteilung und Azure Compute Gallery" aktiviert ist.
VM-Größe	Dropdown-Liste	Wählen Sie die Größe aus.
OS-Disk	Dropdown-Liste	Wählen Sie die Disk aus. Sie können auch die Leistungsstufe auswählen.
Ressourcengruppe	Dropdown-Liste	Wählen Sie die Ressourcengruppe aus, die die Netzwerk-Interface-Karten der VM enthalten soll.
Disk-Typ optimieren, wenn das Desktop-Image beendet ist	Kontrollkästchen	Stuft den Betriebssystem-Disk-Typ herunter, wenn das Desktop-Image beendet ist, um Kosten zu sparen. Wenn die VM gestartet wird, wird der Betriebssystem-Disk-Typ wieder auf den ausgewählten Typ zurückgesetzt.

Azure VM

UI-Element	Typ	Beschreibung
Quelle	Dropdown-Liste	Wählen Sie aus der Dropdown-Liste **Azure-VM** aus, um eine vorhandene VM als Desktop-Image zu importieren.
SAS-URL	Textfeld	Fügen Sie die im Azure-Portal generierte SAS-URL ein. Ihre VM muss auf einer Managed Disk basieren: Beenden Sie die VM im Azure-Portal, navigieren Sie zu ihrer Betriebssystem-Disk und wählen Sie „Disk exportieren“, um die URL zu generieren.
Name	Textfeld	Geben Sie den Namen des Desktop-Images ein.
Beschreibung	Textfeld	Geben Sie die Beschreibung ein.
Netzwerk	Dropdown-Liste	Wählen Sie das Netzwerk aus, mit dem die VM verbunden werden soll. Die VM wird in der Azure-Region erstellt, die dem Netzwerk zugeordnet ist.
OS	Dropdown-Liste	Wählen Sie das Betriebssystem der VM aus. Wenn das ausgewählte Betriebssystem Hyper-V-Generation 2 erfordert (z. B. Windows 11) und Gen2 noch nicht aktiviert ist, wird eine Meldung angezeigt, die Sie auffordert, im Schritt **Einstellungen** die Option **Image-VM als Gen2 erstellen** zu aktivieren oder stattdessen ein Gen1-kompatibles Image auszuwählen.
VM-Größe	Dropdown-Liste	Wählen Sie die Größe aus.
Betriebssystem-Disk	Dropdown-Liste	Wählen Sie die Disk aus. Sie können auch die Leistungsstufe auswählen.
Ressourcengruppe	Dropdown-Liste	Wählen Sie die Ressourcengruppe aus, die die Netzwerk-Interface-Karten der VM enthalten soll.
Disk-Typ optimieren, wenn das Desktop-Image beendet ist	Kontrollkästchen	Stuft den Betriebssystem-Disk-Typ herunter, wenn das Desktop-Image beendet ist, um Kosten zu sparen. Wenn die VM gestartet wird, wird der Betriebssystem-Disk-Typ wieder auf den ausgewählten Typ zurückgesetzt.

2. Wählen Sie **Weiter** aus.

AD-Beitritt konfigurieren

1. Konfigurieren Sie Folgendes:
   - **AD-Beitritt**: Standardmäßig aktiviert. Wenn Sie diese Option deaktivieren, tritt die VM während der Erstellung nicht AD bei. Dadurch wird verhindert, dass AD-GPOs auf das Image angewendet werden, bevor

es erstellt wird. Stellen Sie sicher, dass Sie im Schritt **Einstellungen** im Feld **Benutzerdefinierte Anmeldedaten** lokale Admin-Anmeldedaten angeben, da die VM kein Mitglied der AD-Domäne sein wird.
- Wählen Sie aus der Dropdownliste die Active Directory-Domäne aus, der beigetreten werden soll, zum Beispiel **denver.int (default)**.

2. Wählen Sie **Weiter** aus.

Einstellungen konfigurieren

1. Geben Sie die folgenden Informationen ein:

UI-Element	Typ	Beschreibung
Ruhezustand wird unterstützt	Kontrollkästchen	Wählen Sie diese Option aus, wenn die VM in den Ruhezustand versetzt werden darf. Der Ruhezustand bietet die Möglichkeit, die Zuweisung der virtuellen Maschine aufzuheben und den Speicherinhalt beizubehalten, sodass Sie beim nächsten Start Ihrer VM an der Stelle weitermachen können, an der Sie aufgehört haben. Nachdem das Image erstellt wurde, kann der Ruhezustand nicht mehr aktiviert oder deaktiviert werden.
Spezialisiertes Image	Kontrollkästchen	Wählen Sie diese Option aus, wenn es sich bei dem Image um ein spezialisiertes Image handelt. Bei generalisierten Images wurden maschinen- und User-spezifische Informationen durch Ausführen eines Befehls auf der VM entfernt. Spezialisierte Images bewahren diese Informationen auf und haben den Generalisierungsprozess nicht durchlaufen.
Sysprep durchführen in	Dropdown-Liste	Wählen Sie den Kontext aus, in dem Sysprep auf der VM ausgeführt werden soll, zum Beispiel den Systemkontext.
Image-VM als Gen2 erstellen	Kontrollkästchen	Nur verfügbar, wenn im Schritt für virtuelle Maschinen Azure-VM als Quelle ausgewählt ist. Wählen Sie diese Option aus, um die VM als Gen2 zu erstellen. Standardmäßig werden Desktop-Image-VMs als Gen1 erstellt. Wenn das ausgewählte Betriebssystem Gen2 erfordert und diese Option nicht ausgewählt ist, wird eine Meldung angezeigt, die Sie auffordert, ein Gen1-kompatibles Azure-Image auszuwählen, um fortzufahren. Weitere Informationen finden Sie unter Support für VMs der Generation 2 auf Azure.

UI-Element	Typ	Beschreibung
Zeitzonen-weiterleitung	Kontrollkästchen	Wählen Sie diese Option, um die Zeitzonen-Weiterleitung auf dem Image zu aktivieren. So wird jedem User in der AVD-Desktop-Sitzung die Zeitzone des eigenen lokalen Geräts angezeigt.
Zeitzone festlegen	Umschalter	Schalten Sie diese Option ein, um die Zeitzone der VM festzulegen, und wählen Sie dann die Zeitzone aus der Dropdown-Liste aus.
Boot-Diagnose	Umschalter	Standardmäßig aktiviert. Sammelt und speichert Diagnoseprotokolle und Screenshots, während die VM hochfährt.
Storage-Konto für die Boot-Diagnose	Dropdown-Liste	Gilt nur, wenn Boot-Diagnose aktiviert ist. Lassen Sie dieses Feld auf „Verwaltetes Storage-Konto“ (empfohlen) eingestellt, um Boot-Diagnoseprotokolle in einem von Azure verwalteten Storage-Konto zu speichern, oder wählen Sie ein vom User verwaltetes Storage-Konto aus der Liste aus.
Sicherheitstyp	Dropdown-Liste	Wählen Sie die Sicherheitsoption aus, die am besten zu Ihrer Desktop-Image-VM passt. Standard ist standardmäßig festgelegt. Zusätzliche Sicherheitsoptionen sind nur für VMs der Generation 2 mit aktivierter geografischer Verteilung und Azure Compute Gallery verfügbar. Trusted Launch und vertrauliche virtuelle Maschinen verbessern die Sicherheit, haben jedoch einige Einschränkungen, wie z. B. fehlenden Support für Backups, verwaltete Datenträger und kurzlebige Betriebssystem-Disks. Weitere Informationen finden Sie unter Trusted Launch für virtuelle Maschinen in Azure und Informationen zu vertraulichen Azure-VMs.
Secure Boot	Kontrollkästchen	Nur verfügbar, wenn Trusted Launch-VMs als Sicherheitstyp ausgewählt sind. Aktiviert Secure Boot, was dazu beiträgt, Ihre VMs vor Bootkits, Rootkits und Malware auf Kernelebene zu schützen.
vTPM	Kontrollkästchen	Nur verfügbar, wenn Trusted Launch-VMs als Sicherheitstyp ausgewählt sind. Aktiviert das Virtual Trusted Platform Module (vTPM), das TPM 2.0-konform ist und die Integrität Ihres VM-Starts validiert sowie Schlüssel und Geheimnisse sicher speichert.
Integritäts-Monitoring	Kontrollkästchen	Nur verfügbar, wenn Trusted Launch-VMs als Sicherheitstyp ausgewählt sind. Ermöglicht die kryptografische Attestierung und Überprüfung der VM-Startintegrität sowie Monitoring-Warnungen, falls die VM aufgrund einer fehlgeschlagenen Attestierung anhand der definierten Baseline nicht hochgefahren ist.

UI-Element	Typ	Beschreibung
Verschlüsselung auf dem Host	Umschalter	Standardmäßig deaktiviert. Bietet eine End-to-End-Verschlüsselung für Ihre VM-Daten im Ruhezustand und bei der Übertragung, beginnend bei den Azure-Hosts.
Benutzerdefinierte Anmeldedaten	Umschalter	Standardmäßig deaktiviert. Schalten Sie den Umschalter ein, um den Admin-Benutzernamen und das Passwort für einen lokalen Admin-User einzugeben.
App Attach-Zertifikate installieren	Kontrollkästchen	Wählen Sie diese Option, um alle gespeicherten Zertifikate auf der VM zu installieren, falls zutreffend. Um die gespeicherten Zertifikate anzuzeigen, navigieren Sie zu App Attach > Zertifikate.
App-V-Clientdienst aktivieren	Kontrollkästchen	Wählen Sie diese Option, wenn die VM App Attach-Pakete verwendet, die App-V-Pakete enthalten.

2. Wählen Sie **Weiter**.

Bereinigungsoptionen konfigurieren

1. Nutzen Sie die Tabelle für die Quelle Ihres Desktop-Images und geben Sie die dort aufgeführten Informationen ein.

Azure-Bibliothek

UI-Element	Typ	Beschreibung
Entfernen lokaler Profile überspringen	Kontrollkästchen	Wählen Sie diese Option, damit lokale User-Profile nicht entfernt werden, bevor Sie Sysprep durchführen. Bei der Image-Erstellung entfernt Nerdio Manager alle lokalen User-Profile. Dies erhöht die Wahrscheinlichkeit, dass Sysprep erfolgreich ist. Durch Auswahl dieser Option wird dieser Schritt übersprungen. Wenn auf der Image-VM APPX-Apps nur teilweise installiert sind, schlägt das Entfernen durch Sysprep fehl.
Ältere VDI-Agenten deinstallieren	Kontrollkästchen	Wählen Sie diese Option, um zu versuchen, Citrix- und Omnissa-VDI-Agenten von der VM zu entfernen, bevor das Image erstellt wird. Es werden nur erkannte Agenten entfernt.
FSLogix-Apps entfernen	Kontrollkästchen	Standardmäßig ausgewählt. Wählen Sie diese Option, um den FSLogix-Agenten zu entfernen, falls er auf dem Image gefunden wird. Der FSLogix-Agent ist auf dem Desktop-Image nicht erforderlich: Der neueste FSLogix-Agent wird automatisch auf Sitzungshosts installiert, die aus diesem Desktop-Image erstellt werden.

Azure VM

UI-Element	Typ	Beschreibung
Entfernen lokaler Profile überspringen	Kontrollkästchen	Wählen Sie diese Option, damit lokale User-Profile nicht entfernt werden, bevor Sie Sysprep durchführen. Bei der Image-Erstellung entfernt Nerdio Manager alle lokalen User-Profile. Dies erhöht die Wahrscheinlichkeit, dass Sysprep erfolgreich ist. Durch Auswahl dieser Option wird dieser Schritt übersprungen. Wenn auf der Image-VM APPX-Apps nur teilweise installiert sind, schlägt das Entfernen durch Sysprep fehl.
Ältere VDI-Agenten deinstallieren	Kontrollkästchen	Wählen Sie diese Option, um zu versuchen, Citrix- und Omnissa-VDI-Agenten von der VM zu entfernen, bevor das Image erstellt wird. Es werden nur erkannte Agenten entfernt.
FSLogix-App deinstallieren	Kontrollkästchen	Standardmäßig ausgewählt. Verwenden Sie diese Option, wenn die FSLogix-App bereits im Basis-Image installiert ist und Sie sie entfernen möchten, damit Nerdio Manager FSLogix verwalten kann.
AVD-Agenten deinstallieren	Kontrollkästchen	Verwenden Sie diese Option, wenn Sie ein Image von einem vorhandenen AVD-Sitzungshost erstellen, auf dem der AVD-Agent bereits installiert ist. Stellen Sie sicher, dass Sie den AVD-Agent deinstallieren, bevor Sie diese importierte VM als Desktop-Image festlegen. Weitere Informationen finden Sie unter Desktop Images Manually Uninstall AVD Agent.

2. Wählen Sie **Weiter**.

Scripted Actions und Anwendungen konfigurieren

1. Geben Sie die folgenden Informationen ein:
   - **Führen Sie die folgenden Scripted Actions aus**: Schalten Sie diese Option auf **Ein** und wählen Sie dann aus der Dropdown-Liste die Scripted Action aus, die während der Erstellung ausgeführt werden soll.

Anmerkung

- Windows-Skripte werden über die Azure Custom Script-Erweiterung ausgeführt und laufen im Kontext des Local-System-Kontos auf dem Klon des Desktop-Image-VM, bevor das Sysprep-Durchführen beginnt. Diese Befehle werden nicht auf der Image-VM selbst ausgeführt.
- Azure-Runbooks werden über das Azure-Automatisierungskonto ausgeführt und laufen im Kontext des Nerdio Manager App Service-Dienstprinzipals.
- Mehrere Variablen werden an das Skript übergeben und können in den PowerShell-Befehlen verwendet werden.
- Geben Sie bei Bedarf die erforderlichen Parameter an.

- **AD-Anmeldeinformationen übergeben**: Wählen Sie diese Option, um AD-Anmeldeinformationen, die auf der Seite **Einstellungen** > **Integrationen** > **Active Directory** angegeben sind, an die ausgeführten Skripte zu übergeben. Verweisen Sie im Skript auf diese als **$ADUsername** und **$ADPassword**.
- **Ziel-VM**: Wählen Sie aus, ob die Scripted Action auf dem **Klon** der Desktop-Image-VM (Standard) oder auf der ursprünglichen VM (**Quelle**) ausgeführt werden soll.
- **Anwendungsverwaltung**: Schalten Sie diese Option auf **Ein**, um die Anwendungen anzugeben, die während der Erstellung bereitgestellt werden sollen.
  - **Anwendungen**: Wählen Sie in der Anwendungsliste **Neue Anwendung hinzufügen** und dann aus der Dropdown-Liste die Anwendung aus, die in diese Richtlinie aufgenommen werden soll.

    Anmerkung

    - Sie können beliebig viele Anwendungen hinzufügen.
    - Ziehen Sie eine Anwendung in der Liste per Drag & Drop, um ihre Reihenfolge in der Liste zu ändern.
    - Wählen Sie das „X“ neben einer Anwendung, um sie aus der Liste zu entfernen.

- Wählen Sie für die hinzugefügte Anwendung oder Application Group eine der folgenden Optionen aus:
  - **App installieren**: Installiert die ausgewählte Anwendung.
  - **App deinstallieren**: Deinstalliert die ausgewählte Anwendung.
  - **Gruppe installieren**: Installiert die ausgewählte Application Group.
  - **Gruppe deinstallieren**: Deinstalliert die ausgewählte Application Group.
- Wählen Sie im Feld **Anwendung suchen** die App oder Application Group aus, die je nach oben ausgewählter Option installiert oder deinstalliert werden soll.
- **Nur Favoriten anzeigen**: Wählen Sie diese Option, um nur die Anwendungen anzuzeigen, die als Favoriten markiert sind. Andernfalls können Sie die Liste der Anwendungen suchen.
- **Neustart nach Installation**: Wählen Sie diese Option, um den Klon der Desktop-Image-VM nach der Installation dieser Anwendung neu zu starten. Nachfolgende Anwendungsaufgaben werden fortgesetzt, sobald der Neustart abgeschlossen ist.
- **Ziel-VM**: Wählen Sie aus, ob die Aktion für die Anwendung auf dem **Klon** der Desktop-Image-VM (Standard) oder auf der **Quell-VM** ausgeführt werden soll.

2. Wählen Sie **Weiter**.

Image konfigurieren

1. Geben Sie die folgenden Informationen ein:

UI-Element	Typ	Beschreibung
Kein Image-Objekt erstellen	Kontrollkästchen	Wählen Sie diese Option, um nur eine Desktop-Image-VM zu erstellen, aber kein Image-Objekt. Sie müssen das Image-Objekt erstellen: Wählen Sie nach der Erstellung der VM **Ausschalten und als Image festlegen** aus, bevor dieses Desktop-Image für die Erstellung von Sitzungshosts verwendet werden kann. Wenn Sie die Image-Erstellung überspringen, können Sie Änderungen an der VM vornehmen, bevor sie in ein Image konvertiert wird.
Geografische Verteilung und Azure Compute Gallery	Schalter	Standardmäßig aktiviert. Speichert das Image in einer Azure Compute Gallery und verteilt es automatisch auf die ausgewählten Azure-Regionen.

UI-Element	Typ	Beschreibung
Azure Compute Gallery	Textfeld / Dropdown-Liste	Geben Sie einen Namen ein, um eine vorhandene Azure Compute Gallery auszuwählen oder eine neue zu erstellen. Es kann nur eine Azure Compute Gallery ausgewählt werden. Die vorhandene Galerie muss sich in einer verlinkten Ressourcengruppe im selben Azure-Abonnement wie die Image-VM befinden.
Azure-Regionen	Mehrfachauswahl	Wird automatisch mit der Region ausgefüllt, die der ausgewählten Galerie zugeordnet ist. Sie können Regionen entfernen oder hinzufügen, in denen die Version des Desktop-Images repliziert werden soll. Die aktuelle Azure-Region muss Teil der Auswahl sein.
Anzahl der Replikate (pro Region)	Textfeld	Geben Sie die Anzahl der Replikate pro Region an. Für Azure Compute Gallery-Replikate gilt ein Maximalwert von 20 gleichzeitigen Klonvorgängen pro Replikat. Bis zu 100 Replikate pro Region werden unterstützt. Replikate können nur innerhalb desselben Abonnements bereitgestellt werden.

2. Wählen Sie **Weiter**.

Replikation konfigurieren

1. Geben Sie die folgenden Informationen an:
   - **Für Cloud-PCs aktivieren**: Erfordert Windows 10/11 Enterprise. Nicht verfügbar für AVD-, EVD- oder CIS-Images.
   - **Benutzerdefinierte Standorte (Azure Local)**: Wählen Sie aus der Dropdownliste alle benutzerdefinierten Azure Local-Standorte aus, auf die das Image repliziert werden soll.
   - **Nutanix-Cluster** (nur AVD – Hybrid auf Nutanix AHV): Wählen Sie aus der Dropdownliste den Nutanix-Cluster aus, mit dem das Image synchronisiert werden soll.

   > **Anmerkung**
   >
   > Nur verwaltete Imageversionen (aktiv oder in der Staging-Phase) werden mit Nutanix synchronisiert. Nicht verwaltete (Backup-)Versionen werden nicht synchronisiert. Weitere Details finden Sie unter Erstellen einer VM-Vorlage für Nutanix-Hostpools.

2. Wählen Sie **Weiter**.

Tags konfigurieren und übermitteln

1. Geben Sie die folgenden Informationen ein:

> **Anmerkung**
>
> Sie können mehrere Tags angeben. Die angegebenen Tags werden auf die Image-VM, den Betriebssystemdatenträger, die Netzwerkschnittstelle, das Image-Objekt und das Azure Compute Gallery-Image angewendet. Weitere Informationen zur Verwendung von Tags zum Organisieren Ihrer Azure-Ressourcen finden Sie unter Verwenden von Tags zum Organisieren Ihrer Azure-Ressourcen und Verwaltungshierarchie.

   - **Tag-Gruppen**: Wählen Sie optional eine vordefinierte Tag-Gruppe aus der Dropdownliste aus, um deren Tags automatisch anzuwenden.
   - **Name** und **Wert**: Geben Sie optional einen benutzerdefinierten Tagnamen und -wert ein.
2. Wählen Sie **Übermitteln**.

Nerdio Manager for Enterprise beginnt mit der Erstellung des Desktop-Images. Dieser Schritt kann bis zu einer Stunde dauern. Sie können den Fortschritt auf dem Tab **Aufgaben** der Seite **Desktop-Images** überwachen.

Desktop-Images: Als Image festlegen

Nerdio Manager bietet ein leistungsstarkes Tool, das eine umfassende Automatisierung durchführt, um die Änderungen am Desktop-Image per Commit auszuführen und dem Image-Objekt zuzuweisen. Dies umfasst viele Aufgaben, die Sie manuell hätten ausführen müssen, wie z. B. Sysprep durchführen und das Versiegeln des Images. Dies würde normalerweise geschehen, nachdem Sie die Aktualisierungen an Ihrem Image vorgenommen haben. Sobald Sie **Als Image festlegen** ausführen, wird das Image-Objekt erstellt und steht bereit, um entweder neue Hostpools zu erstellen oder bei vorhandenen Hostpools ein Reimaging vorzunehmen.

So legen Sie ein Desktop-Image fest:

1. Navigieren Sie zu **Cloud Desktops** > **Desktop-Images**.

2. Finden Sie das Desktop-Image, mit dem Sie arbeiten möchten.
3. Wählen Sie im Aktionsmenü **Ausschalten & als Image festlegen** oder **Als Image festlegen** (je nach Energiestatus dieses Desktop-Images).
4. Geben Sie die folgenden Informationen ein:
   Nutanix-Cluster: (Nur AVD – Hybrid auf Nutanix AHV): Wählen Sie aus der Dropdown-Liste den Nutanix-Cluster aus, mit dem das Image synchronisiert werden soll.

   > **Anmerkung**
   >
   > Nur verwaltete Image-Versionen (**aktiv** oder **bereitgestellt**) werden mit Nutanix synchronisiert. Nicht verwaltete (Back-up-)Versionen werden nicht synchronisiert. Weitere Details finden Sie unter Erstellen einer VM-Vorlage für Nutanix-Hostpools.

   - **Führen Sie die folgenden Scripted Actions aus, bevor Sie das Image festlegen**: Schalten Sie diese Option auf **Ein**, um die Scripted Actions auszuführen, bevor Sie das Image festlegen.

     > **Anmerkung**
     >
     > Sie können beispielsweise Skripte ausführen, um das Image zu optimieren, Software zu installieren oder Updates zu installieren.

     - Wählen Sie aus der Dropdown-Liste die Scripted Actions aus, die Sie ausführen möchten.
     - **AD-Anmeldeinformationen übergeben**: Wählen Sie diese Option, wenn Sie diese zum Ausführen der Scripted Actions verwenden möchten.
   - **Anwendungsverwaltung**: Aktivieren Sie diese Option **Ein**, um die Anwendungen anzugeben, die während der Erstellung bereitgestellt werden sollen.
     - **Anwendungen**: Wählen Sie in der Anwendungsliste **Neue Anwendung hinzufügen** und dann aus der Dropdown-Liste die Anwendung aus, die in diese Richtlinie aufgenommen werden soll.

> **Anmerkung**
> - Sie können beliebig viele Anwendungen hinzufügen.
> - Ziehen Sie eine Anwendung in der Liste per Drag & Drop, um ihre Reihenfolge in der Liste zu ändern.
> - Wählen Sie das „X“ neben einer Anwendung, um sie aus der Liste zu entfernen.

  - **Installieren/Deinstallieren**: Wählen Sie aus, ob die Bereitstellungsrichtlinie die ausgewählten Anwendungen installieren oder deinstallieren soll.
  - **Neustart nach Installation**: Wählen Sie diese Option, um den Klon der Desktop-Image-VM nach der Installation dieser Anwendung neu zu starten. Nachfolgende Anwendungsaufgaben werden fortgesetzt, sobald der Neustart abgeschlossen ist.
  - **Nur Favoriten anzeigen**: Wählen Sie diese Option, um nur die Anwendungen anzuzeigen, die als Favoriten markiert sind. Andernfalls können Sie die Liste der Anwendungen durchsuchen.
- **Zeitplan**: Schalten Sie die Option **Zeitplan** auf **Ein**, um die Vorgänge zu einem oder mehreren ausgewählten Zeitpunkten auszuführen. Weitere Informationen zum Erstellen eines Zeitplans finden Sie unter Zeitpläne für Aufgaben verwalten [42].
- **Azure Marketplace-Image aktualisieren**: Schalten Sie diese Option auf **Ein**, um das vorhandene Image-Objekt zu entfernen und durch die neueste Version des ausgewählten Azure Marketplace-Images zu ersetzen.

> **Anmerkung**
>
> Durch Aktivieren dieser Option wird die vorhandene Desktop-Image-VM entfernt und aus der neuesten Version des ausgewählten Azure Marketplace-Images neu erstellt.

- **Sicherheitstyp**: Diese Option ist gesperrt, basierend auf der Auswahl, die bei der Erstellung oder dem Import des Images in Nerdio Manager getroffen wurde.

> **Anmerkung**
>
> - **Standard** ist standardmäßig eingestellt. Zusätzliche Sicherheitsoptionen sind nur für Generation-2-VMs verfügbar, bei denen die Option **Geografische Verteilung & Azure Compute Gallery** aktiviert ist.
> - Die Sicherheitsoptionen **Trusted Launch** und **Confidential Virtual Machines** tragen dazu bei, die Sicherheit von Azure-VMs der Generation 2 zu verbessern. Die zusätzlichen Sicherheitsfunktionen, die sie bieten, weisen jedoch auch einige Einschränkungen auf, wie z. B. die fehlende Unterstützung für Backup, verwaltete Datenträger und kurzlebige Betriebssystemdatenträger. Weitere Informationen finden Sie unter:
>   - Trusted Launch für Azure-VMs
>   - Informationen zu vertraulichen Azure-VMs

- **Geografische Verteilung & Azure Compute Gallery**: Wählen Sie diese Option, um das Image in der Azure Compute Gallery zu speichern und automatisch auf die ausgewählten Azure-Regionen zu verteilen.
  - **Azure Compute Gallery**: Diese Option ist gesperrt, basierend auf der Auswahl, die bei der Erstellung oder dem Import des Images in Nerdio Manager getroffen wurde.

    > **Anmerkung**
    >
    > Es kann nur eine Azure Compute Gallery ausgewählt werden. Die vorhandene Azure Compute Gallery muss sich in einer verknüpften Ressourcengruppe im selben Azure-Abonnement wie das Image-VM befinden.

  - **Azure-Regionen**: Wählen Sie aus der Dropdownliste die Azure-Regionen aus, in denen die Desktop-Imageversion repliziert werden soll.

> **Anmerkung**
>
> Die aktuelle Azure-Region muss Teil der Auswahl sein.

- **Version Increment Type**: Wählen Sie aus der Dropdownliste eine der folgenden Optionen aus:
  - **Major**
  - **Minor**
  - **Revision**

> **Anmerkung**
>
> Versionsnummern haben das Format **Major**.**Minor**.**Revision**. Wenn Sie beispielsweise Version 1.4.3 aktualisieren, wird die höhere Version je nach der im Dropdownmenü **Version Increment Type** gewählten Option wie folgt numeriert:
>
> - **Major**: 2.0.0
> - **Minor**: 1.5.0
> - **Revision**: 1.4.4.

- **Spezialisiertes Image**: Wählen Sie diese Option, wenn es sich bei dem Image um ein spezialisiertes Image handelt.

> **Anmerkung**
>
> Bei generalisierten Images wurden maschinen- und user-spezifische Informationen durch Ausführen eines Befehls auf der VM entfernt. Spezialisierte Images behalten diese Informationen bei und haben den Generalisierungsprozess nicht durchlaufen.

- **Ruhezustand unterstützt**: Wählen Sie diese Option, wenn Sie der VM das Ruhezustands-Feature ermöglichen möchten.

> **Anmerkung**
>
> Der Ruhezustand bietet die Möglichkeit, die Zuweisung der virtuellen Maschine aufzuheben und dabei den Speicherinhalt beizubehalten. Auf diese Weise können Sie beim nächsten Start Ihrer VM an der Stelle weitermachen, an der Sie aufgehört haben. Beachten Sie, dass der Ruhezustand nach der Erstellung des Images nicht mehr aktiviert oder deaktiviert werden kann.

- **Neue Imageversion als inaktiv anlegen**: Wählen Sie diese Option, um die neue Imageversion zu erstellen, ohne sie als aktiv festzulegen.

> **Anmerkung**
>
> Alle vorhandenen Konfigurationen verwenden weiterhin die aktuelle Version des Images. Weitere Informationen zum Aktivieren von Desktop-Images in der Staging-Phase finden Sie unter Desktop-Images in die Staging-Phase versetzen.

- **Bereitgestelltes Image aktivieren nach**: Wählen Sie diese Option, um das Image automatisch einige Tage nach der Bereitstellung zu aktivieren. Alle verknüpften Pools erhalten ein Update ihres zugehörigen Images.
- **Aktion für aktuelles Image**: Wählen Sie eine der folgenden Optionen:
  - **Aktuelle Version als Backup beibehalten**: Diese Option behält die aktuelle Image-Version als eigenständiges Objekt bei. Diese Image-Version ist über Nerdio Manager nicht sichtbar oder verwaltbar. Löschen Sie sie daher manuell, wenn sie nicht mehr benötigt wird, um unnötige Azure-Speicherkosten zu vermeiden. Sie können weiterhin frühere Versionen von Azure Compute Gallery-Images im Menü **Desktop-Image (Vorlage)** unter **Nicht verwaltete ACG-Image-Versionen** verwenden.
  - **Aktuelle Version nach Aktivierung entfernen**: Diese Option entfernt die aktuelle Image-Version automatisch nach der Aktivierung.

- **Replikaanzahl (pro Region)**: Geben Sie die Anzahl der Replikate pro Region an.

  > **Anmerkung**
  > - Replikate der Azure Compute Gallery unterstützen maximal 20 gleichzeitig ablaufende Klonvorgänge pro Replikat.
  > - Stellen Sie sicher, dass die angegebene Anzahl an Replikaten Ihre Bereitstellungsanforderungen erfüllt. Es werden bis zu 100 Replikate pro Region unterstützt.
  > - Replikate können nur innerhalb desselben Abonnements bereitgestellt werden.

- **Limit für Backup-Versionen**: Geben Sie die maximale Anzahl der aufzubewahrenden Backup-Image-Versionen an.

  > **Anmerkung**
  >
  > Wenn eine neue Image-Version erstellt und die alte als Backup gespeichert wird, verwaltet und begrenzt das System die Anzahl dieser Backups automatisch gemäß dem festgelegten Limit. Wenn das Limit erreicht ist, werden die ältesten Versionen gelöscht. Sie können diese Einstellung in den Desktop-Image-Einstellungen unter der Option **Versionen verwalten** konfigurieren.

- **Aktuelles Image als Backup speichern**: Wählen Sie dieses Image aus, um das vorhandene Image als eigenständiges Objekt beizubehalten und es nicht mit dem neuen zu überschreiben.

> **Anmerkung**
>
> - Dieses Image ist über Nerdio Manager nicht sichtbar oder verwaltbar. Löschen Sie es daher manuell, wenn es nicht mehr benötigt wird, um unnötige Azure Storage-Kosten zu vermeiden.
> - Wenn das aktuelle Image in der Azure Compute Gallery gespeichert ist, wird es mit einer älteren Versionsnummer beibehalten. Wenn das Image nicht in der Azure Compute Gallery gespeichert ist, finden Sie es im Azure-Portal unter **Images**. In den Image-Auswahllisten von Nerdio Manager wird es unter **Benutzerdefinierte Images** aufgeführt.

- **App Attach-Zertifikate installieren**: Wählen Sie diese Option, um alle gespeicherten Zertifikate auf der Image-VM zu installieren, sofern vorhanden.
- **App-V-Clientdienst aktivieren**: Wählen Sie diese Option, wenn die VM App Attach-Pakete verwendet, die App-V-Pakete enthalten.
- **Entfernen lokaler Profile überspringen**: Wählen Sie diese Option, um das Entfernen aller lokalen Benutzerprofile zu umgehen.

> **Anmerkung**
>
> Während des Image-Erstellungsprozesses entfernt Nerdio Manager alle lokalen Benutzerprofile. Dies erhöht die Wahrscheinlichkeit, dass Sysprep durchgeführt werden kann. Die Auswahl dieser Option überspringt diesen Schritt. Wenn auf der Image-VM teilweise installierte APPX-Apps vorhanden sind, entfernt Sysprep diese nicht.

- **Für Cloud PCs aktivieren**: Wählen Sie diese Option, um dieses Image im Windows 365 Cloud-PC-Dienst verfügbar zu machen.

> **Anmerkung**
>
> Das Image wird hochgeladen und auf Kompatibilität mit Cloud-PCs getestet. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Es gibt ein Limit von 20 Images, die in Windows 365 hochgeladen werden können.

- **Desktop-Image-VM weiterlaufen lassen**: Wählen Sie diese Option, um die VM nach Abschluss der Aufgabe **Als Image festlegen** weiterlaufen zu lassen.

> **Anmerkung**
>
> Dies ist vor allem dann hilfreich, wenn Sie OS- und Anwendungsupdates auf die laufende VM übertragen möchten.

- **Änderungsprotokoll**: Geben Sie die Liste der am Image vorgenommenen Änderungen ein.
- **Tags anwenden**: Geben Sie optional den **Namen** und den **Wert** des Azure-Tags ein.

> **Anmerkung**
>
> Sie können mehrere Tags angeben. Die angegebenen Tags werden auf die Image-VM, den Betriebssystemdatenträger, die Netzwerkschnittstelle, das Image-Objekt und das Azure Compute Gallery-Image angewendet. Weitere Informationen zur Verwendung von Tags zum Organisieren Ihrer Azure-Ressourcen finden Sie unter Verwenden von Tags zum Organisieren Ihrer Azure-Ressourcen und Verwaltungshierarchie.

5. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Jetzt ausführen** (nicht geplant) oder **Speichern und schließen** (geplant).

Sie können den Fortschritt des Jobs in den Protokollen einsehen. Weitere Informationen zu den Protokollen finden Sie unter Feature für das Änderungsprotokoll von Desktop-Images.

Scripted Actions für Desktop-Images

Nerdio Manager ermöglicht es Ihnen, Skripte auf Desktop-Images auszuführen.

> **Anmerkung**
>
> Sie können Scripted Actions sofort ausführen oder diese nach einem Zeitplan ausführen.

So führen Sie Scripted Actions aus:

1. Wählen Sie im Hauptmenü **Desktop Images** aus.
2. Wählen Sie im Aktionsmenü **Skript ausführen** aus.
3. Geben Sie die folgenden Informationen ein:
   - **Zeitplan**: Schalten Sie den Zeitplaner auf **Ein**/**Aus**. Weitere Informationen zum Erstellen eines Zeitplans finden Sie unter Zeitpläne für Aufgaben verwalten [42].
   - **Scripted Actions**: Wählen Sie aus der Dropdown-Liste das Skript aus, das Sie ausführen möchten.

Anmerkung

- Windows-Skripte werden über die Azure Custom Script-Erweiterung ausgeführt und laufen im Kontext des Local-System-Kontos.
- Azure-Runbooks werden über das Azure-Automatisierungskonto ausgeführt und laufen im Kontext des Nerdio Manager App Service-Dienstprinzipals.
- Die folgenden Variablen werden an das Skript übergeben und können in den PowerShell-Befehlen verwendet werden:
  - $AzureSubscriptionId
  - $AzureSubscriptionName
  - $AzureResourceGroupName
  - $AzureRegionName
  - $AzureVMName
  - $ADUsername (bei Übergabe von AD-Anmeldeinformationen)
  - $ADPassword (bei Übergabe von AD-Anmeldeinformationen)
  - $SATrigger = "RunOnce"
  - $SATriggerMode = \"Manual\" | \"Schedule\"
  - $DesktopImageVmName
  - $DesktopImageActiveVersion
  - $DesktopImageStagedVersion

- **Eingabeparameter für Scripted Actions**: Geben Sie bei Bedarf die erforderlichen Parameter an.
- **AD-Anmeldeinformationen übergeben**: Wählen Sie diese Option, um Ihre AD-Anmeldeinformationen an das ausgeführte Skript zu übergeben.
- **VM nach Skriptausführung neu starten**: Wählen Sie diese Option, um die VM nach der Skriptausführung neu zu starten.

> **Anmerkung**
>
> Es ist vorzuziehen, diese Option zu wählen, anstatt die VM in Ihren PowerShell-Befehlen neu zu starten, da die Custom Script-Erweiterung fehlschlägt, wenn das Skript die VM neu startet.

4. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie entweder **Jetzt ausführen**, um den Vorgang sofort auszuführen, oder **Speichern und schließen**, um das Skript zu speichern und gemäß dem Zeitplan auszuführen.

Schritt 3 Hostpools

Mit Ihren Desktop-Images besteht der nächste Schritt darin, Hostpools zu erstellen – die Pools von Sitzungshosts, mit denen Ihre User tatsächlich eine Verbindung herstellen – und zu konfigurieren, wie diese erstellt, skaliert und zugewiesen werden.

In diesem Abschnitt:

1. Übersicht über Hostpools [75]
2. Workspace-Verwaltung [76]
3. Dynamische Hostpools erstellen [78]
4. Hostpool-Profile verwalten [87]
5. Auto-scale für dynamische Hostpools aktivieren [92]
6. Auto-scale für persönliche Hostpools aktivieren [110]
7. Auto-scale: Kostenoptimierung für den Speicher der Betriebssystem-Disk von Sitzungshost-VMs [134]
8. Einen neuen Sitzungshost zu einem dynamischen Hostpool hinzufügen [136]
9. AVD-Konfiguration für Hostpools [141]
10. Hostpool-VM-Deployment [145]
11. Hostpool-User-Zuweisungen verwalten [156]
12. Active Directory-Einstellungen des Hostpools konfigurieren [156]
13. VM bei Verbindung für gepoolte Hostpools starten [158]
14. Zeitlimits für User-Sitzungen konfigurieren [159]

15. Remote-Anwendungen für User veröffentlichen [163]

Übersicht über Hostpools

> ⚠ **Warnung**
>
> Nerdio Manager installiert die BgInfo Azure-Erweiterung während keiner Automatisierungs- oder Verwaltungsprozesse. Die BgInfo-Erweiterung kann jedoch entweder direkt über eine skriptgesteuerte Aktion oder unbeabsichtigt installiert werden, wie im Bericht zu Problemen mit dem Azure PowerShell-Modul angegeben.

Nachdem Sie die Desktop-Images erstellt haben, besteht der nächste Schritt im Nerdio Manager AVD-Bereitstellungsablauf darin, Hostpools aus den Desktop-Images zu erstellen.

Hostpools sind Gruppen identischer Azure-VMs, die die Azure Virtual Desktops hosten, bei denen sich Endbenutzer anmelden. Alle VMs im Hostpool teilen sich eine Reihe von Konfigurationsoptionen: VM-Größe, Betriebssystem-Datenträgergröße, Basis-Image, AD-Domäne, Speicherort für Benutzerprofile und mehr.

Hostpools können auf folgende Weise konfiguriert werden:

Ob Auto-scale aktiviert ist:

- **Statisch**: Ein statischer Hostpool enthält eine festgelegte Anzahl von Sitzungshosts, die der Admin konfiguriert. Das heißt, Auto-scale ist nicht aktiviert. Auto-scale kann bei Bedarf nach der Erstellung für einen statischen Hostpool aktiviert werden.

  > **Anmerkung**
  >
  > Wenn Nerdio Manager erstmals in einer **bestehenden** Umgebung bereitgestellt wird, sind die erstellten Hostpools statisch. Auto-scale kann nachträglich für sie aktiviert werden.

- **Auto-scale aktiviert**: Sitzungshosts werden basierend auf Ihrer Auto-scale-Konfiguration automatisch entsprechend dem Bedarf der Workload erstellt und entfernt.

> **Anmerkung**
>
> Dies wurde zuvor als „dynamischer" Hostpool bezeichnet. Während der Umstellung der Terminologie kann dieser Begriff in einigen Bereichen des Produkts noch vorkommen.

Wo Sitzungshosts ausgeführt werden:

- **Azure**: Sitzungshosts werden vollständig in Azure ausgeführt.
- **AVD – Hybrid**: Sitzungshosts werden auf einer Infrastruktur ausgeführt, die via Azure Virtual Desktop für Azure Local oder Nutanix AHV angebunden ist.

Siehe auch

- Statische Hostpools ohne Auto-scale erstellen
- Dynamische Hostpools erstellen [78]
- Hosts, Hostpools und Workspaces löschen
- Einen statischen Hostpool in einen dynamischen konvertieren
- AVD für Azure Local und Nerdio Manager
- AVD – Hybrid-Support

Arbeitsbereiche verwalten

Ein Arbeitsbereich ist ein Container für Hostpools und Sitzungshosts, die Benutzern Desktops und RemoteApps bereitstellen. Dieses Thema behandelt das Erstellen und Verwalten von Arbeitsbereichen.

Einen Arbeitsbereich erstellen

Ein Arbeitsbereich muss erstellt werden, bevor Sie Hostpools und Sitzungshosts erstellen können.

So erstellen Sie einen Arbeitsbereich:

1. Navigieren Sie zu **Cloud Desktops** > **Azure Virtual Desktop** > **Workspaces**.

2. Wählen Sie **Arbeitsbereich hinzufügen**.
3. Geben Sie die folgenden Informationen ein:
   - **Name**: Geben Sie den Namen des Arbeitsbereichs ein.

     > **Anmerkung**
     >
     > Der Name wird dem Arbeitsbereich bei der Erstellung zugewiesen und kann später nicht mehr geändert werden. Standardmäßig ist er für den Endbenutzer sichtbar. Die Angabe eines Anzeigenamens überschreibt das, was für den Endbenutzer sichtbar ist.

   - **Anzeigename**: Geben Sie den Anzeigenamen ein.
   - **Beschreibung**: Geben Sie die Beschreibung ein, die nur für Administratoren sichtbar ist.
   - **Ressourcengruppe**: Wählen Sie aus der Dropdownliste die Ressourcengruppe aus, in der der Arbeitsbereich angelegt werden soll.
   - **Ort**: Wählen Sie aus der Dropdownliste den Azure-Ort für die Objekte und die zugehörigen Metadaten des Arbeitsbereichs aus.
   - **Tags anwenden**: Geben Sie optional den **Namen** und den **Wert** des Azure-Tags ein, der auf den Arbeitsbereich angewendet werden soll.

     > **Anmerkung**
     >
     > Sie können mehrere Tags angeben. Weitere Informationen zur Verwendung von Tags zum Organisieren Ihrer Azure-Ressourcen finden Sie in diesem Microsoft-Artikel.

4. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

   Der Arbeitsbereich wird erstellt.

Arbeitsbereiche verwalten

In der Tabelle „Arbeitsbereiche“ können Sie Folgendes tun:

- **Hostpools**: Verwalten Sie die dynamischen Hostpools des Arbeitsbereichs.
- **Statische Hostpools**: Verwalten Sie die statischen Hostpools des Arbeitsbereichs.

- **Zuweisung aufheben**: Heben Sie die Zuweisung des Arbeitsbereichs von Nerdio Manager auf.
- **Löschen**: Löschen Sie einen Arbeitsbereich.

> **Anmerkung**
>
> Sie können nur einen Arbeitsbereich löschen, der keine Hostpools enthält.

- **Benutzersitzungen**: Verwalten Sie die User-Sitzungen des Arbeitsbereichs.

Dynamische Hostpools erstellen

> **Warnung**
>
> Nerdio Manager installiert die BgInfo Azure-Erweiterung während keiner Automatisierungs- oder Verwaltungsprozesse. Die BgInfo-Erweiterung kann jedoch entweder direkt über eine skriptgesteuerte Aktion oder unbeabsichtigt installiert werden, wie im Bericht zu Problemen mit dem Azure PowerShell-Modul angegeben.

Das folgende Verfahren ermöglicht es Ihnen, einen neuen dynamischen Hostpool zu erstellen.

So erstellen Sie einen neuen dynamischen Hostpool:

> **Anmerkung**
>
> Neben der Beschriftung vieler Felder in diesem Assistenten finden Sie eine QuickInfo. Ziehen Sie diese QuickInfos für weitere Informationen zu den einzelnen Optionen heran.

Assistenten zum Hinzufügen von Hostpools öffnen

1. Navigieren Sie zu **Cloud Desktops** > **Azure Virtual Desktop** > **Workspaces**.
2. Wählen Sie den Workspace aus, mit dem Sie arbeiten möchten.
3. Wählen Sie **Neuer Hostpool**.

   Ein Dialogfeld mit dem Titel *Hostpool hinzufügen* wird geöffnet. Es enthält die folgenden Abschnitte: Grundlagen, VM-Vorlage, Active Directory, FSLogix, RDP, Tags, Anwendungsrichtlinien.

Grundlagen konfigurieren

Geben Sie die folgenden Informationen ein:

> **Anmerkung**
>
> Für einige der erforderlichen Parameter können Sie die verfügbaren Optionen mithilfe der Ressourcenauswahlregeln filtern. Sie können beispielsweise die verfügbaren VM-Größen oder Betriebssystem-Disks so filtern, dass nur Optionen für Intel-RAM-optimierte VMs angezeigt werden. Weitere Informationen finden Sie unter Verwaltung von Ressourcenauswahlregeln [44].

- **Name**: Geben Sie den Namen des Hostpools ein.
- **Beschreibung**: Geben Sie die Beschreibung des Hostpools ein.

  > **Anmerkung**
  >
  > Wählen Sie optional **Mit KI generieren**, damit die KI die Beschreibung erstellt. Weitere Informationen finden Sie unter Übersicht über die KI-gestützte Beschreibungsgenerierung.

- **Ressourcengruppe**: Wählen Sie aus der Dropdown-Liste die Ressourcengruppe für den Hostpool aus.
- **Hosttyp**: Wählen Sie aus der Dropdown-Liste den Hosttyp aus (Azure Cloud, Azure Local oder Nutanix).

- **Hostpool-Typ**: Wählen Sie **Dynamisch**.
- **Desktop-Erfahrung**: Wählen Sie aus der Dropdown-Liste die Desktop-Erfahrung aus.
  - **AVD-Multi-Session-Desktop (gepoolt)**: Dies ist die vollständige Desktop-Erfahrung. User werden keinen einzelnen Sitzungshosts zugewiesen. Stattdessen werden sie je nach Last einem Host zugewiesen. Mehrere User werden auf einer Gruppe von Hosts zusammengefasst.
  - **AVD-Multi-Session-RemoteApp (gepoolt)**: Dies sind nur veröffentlichte Anwendungen, keine vollständige Desktop-Erfahrung. Veröffentlichte RemoteApps werden Usern als native Apps angezeigt, die auf ihrem lokalen Computer ausgeführt werden. Die RemoteApps werden über einen Pool von Sitzungshosts angeboten.
  - **AVD-Single-Session-Desktop (gepoolt)**: Dies ist die vollständige Desktop-Erfahrung. User werden individuellen Desktop-VMs zugewiesen (ein User pro Sitzungshost), und eine vorkonfigurierte Anzahl freier (verfügbarer) Desktops wird vorgehalten.
  - **AVD-Single-Session-Desktop (persönlich)**: Dies ist eine persönliche (persistente) vollständige Desktop-Erfahrung. Jedem User wird eine eigene Sitzungshost-VM zugewiesen.
- Wenn Sie **AVD Single-Session-Desktop (persönlich)** als **Desktop-Erfahrung** auswählen, müssen Sie die folgenden zusätzlichen Funktionen konfigurieren:
  - **Zuweisungstyp**: Wählen Sie aus, wie der Desktop dem User zugewiesen wird.

    > **Anmerkung**
    >
    > Bevor sich User bei einem persönlichen Desktop anmelden können, müssen sie der VM vorab zugewiesen werden.

  - Wählen Sie optional **Mehrere Desktops einem einzelnen User zuweisen**.

> **Anmerkung**
>
> Durch Auswahl dieser Option können einem einzelnen User für diesen Hostpool mehrere Desktops zugewiesen werden. Diese Einstellung kann nach der Aktivierung NICHT mehr deaktiviert werden und ist nur für direkte Zuweisungen verfügbar. Weitere Details finden Sie unter Persönliche Desktopzuweisung konfigurieren.

- **Name der App Group**: Geben Sie optional den Namen der App Group des Hostpools ein.
- **Validierungsumgebung**: Wählen Sie diese Option, um Service-Updates in einem schnelleren Rhythmus als bei Nicht-Validierungs-Hostpools zu erhalten, sodass Sie Serviceänderungen testen können, bevor diese umfassend in der Produktion bereitgestellt werden.
- **Schnellzuweisung**: Wählen Sie aus der Dropdown-Liste die User oder Gruppen aus, die den neu erstellten Desktops vorab zugewiesen werden sollen.

Wählen Sie **Weiter**.

VM-Vorlage konfigurieren

- **Name**: Geben Sie den Namen der neu hinzugefügten Hosts für Präfix oder das Präfix+Muster ein.
  - **Präfix/Muster**: Wählen Sie aus der Dropdown-Liste aus, ob Sie ein Präfix oder ein Muster verwenden möchten.
    - **Präfix** kann beim Erstellen mehrerer Sitzungshosts verwendet werden. Das Präfix-Limit beträgt 10 gültige Windows-Computernamenzeichen. Bei Verwendung eines Präfixes wird automatisch ein eindeutiges Suffix im Format „-xxxx“ angehängt, wobei xxxx für 4 zufällige alphanumerische Zeichen steht. Zum Beispiel: AVDHOST-s72h. Fügen Sie dem Präfix kein „-“ hinzu.
    - **Muster** kann verwendet werden, um eine erweiterte Namenskonvention für neue Hosts festzulegen. Musterzeichen müssen in {} eingeschlossen werden und können # (für fortlaufende Nummern) und/oder ? (für zufällige alphanumerische Zeichen) sein. Ein # steht für Zahlen von 0 bis 9, zwei # stehen für Zahlen von 0 bis 99 usw.

    - Beispiel 1: AVDHOST{###} (AVDHOST000..AVDHOST999).
    - Beispiel 2: AVDHOST-{???} (AVDHOST-d83, AVDHOST-7sl, etc.).
- **Netzwerk**: Wählen Sie das Netzwerk aus der Dropdown-Liste aus. Das Netzwerk bestimmt die Azure-Region der VM.

> **Anmerkung**
>
> Nerdio Manager überprüft, ob eine ausreichende Anzahl an verfügbaren IP-Adressen im ausgewählten Netzwerk vorhanden ist, bevor neue Hostpool-VMs bereitgestellt werden. Wenn nicht genügend IP-Adressen verfügbar sind, wird eine Fehlermeldung angezeigt und Sie können den neuen Hostpool nicht hinzufügen.

- **Desktop-Image**: Wählen Sie aus der Dropdown-Liste das Desktop-Image aus, das als Golden Image für neu erstellte Sitzungshosts verwendet wird.
- **VM-Größe**: Wählen Sie aus der Dropdown-Liste die VM-Disk-Größe und den Typ für neu erstellte Sitzungshosts aus.

> **Anmerkung**
>
> Wenn eine VM-Größe für ein Abonnement oder eine Region nicht verfügbar ist, wird sie nicht in der Liste angezeigt. Manchmal kann eine VM-Größe, selbst wenn sie in einer bestimmten Azure-Region verfügbar ist, nicht verwendet werden, da das Abonnement Einschränkungen für eine bestimmte Größe aufweist. In solchen Fällen zeigen wir die VM-Größe in der Dropdown-Liste an, erlauben Usern jedoch nicht, sie auszuwählen (die Größe ist deaktiviert).

- **Betriebssystemdatenträger**: Wählen Sie aus der Dropdown-Liste den Typ und die Größe des Betriebssystemdatenträgers für neu erstellte Sitzungshosts aus.

> **Anmerkung**
>
> Dieser muss gleich oder größer als die Größe des oben ausgewählten Desktop-Images sein. Die Verwendung von Standard HDD (S-Typ) wird nicht empfohlen. Premium-SSD bietet die beste Leistung.

- **Ressourcengruppe**: Wählen Sie aus der Dropdown-Liste die Ressourcengruppe aus, die die VMs enthalten soll.

Wählen Sie **Weiter**.

Active Directory konfigurieren

- **Directory-Profil**: Wählen Sie aus der Dropdown-Liste **Standard**, eine der **Vordefinierten** globalen Konfigurationen oder **Benutzerdefiniert** aus.

> **Anmerkung**
>
> Standard verwendet immer die globale Standard-AD-Konfiguration der Anwendung, sodass sie synchron bleibt, falls dieser Standard später geändert wird. Wenn Sie eine vordefinierte Konfiguration auswählen, bleibt diese gespeicherte Konfiguration erhalten, auch wenn sich der globale Standard später ändert. Wählen Sie Benutzerdefiniert aus, um eine eigene Konfiguration für diesen Hostpool anzubieten.

- **Directory-Typ**, **Domäne (FQDN)**, **Dienstkonto (UPN)**, **Dienstkonto-Passwort** und **Organisationseinheit**: Diese Felder werden automatisch aus dem ausgewählten Directory-Profil aufgefüllt und bleiben schreibgeschützt, sofern für das Directory-Profil nicht **Benutzerdefiniert** ausgewählt wird; in diesem Fall können sie bearbeitet werden. Geben Sie die Organisationseinheit als Distinguished-Name-Pfad (DN-Pfad) an, wenn Sitzungshosts in einer bestimmten OU erstellt werden sollen; lassen Sie das Feld leer, um den Computers-Container zu verwenden.

Wählen Sie **Weiter**.

Configure FSLogix

- **FSLogix**: Wählen Sie aus der Dropdown-Liste das FSLogix-Konfigurationsprofil aus, das beim Erstellen oder Neu-Imaging von Hosts in diesem Hostpool verwendet werden soll.
- **FSLogix-Profile**: Wählen Sie den Umschalter aus, um FSLogix-Profile zu aktivieren.

  > **Anmerkung**
  >
  > Wenn diese Option nicht aktiviert ist, installiert Nerdio Manager die FSLogix-Profilcontainer-Anwendung nicht auf neu erstellten VMs, wenn diese in diesem Hostpool bereitgestellt werden.

- **Konfiguration**: Wählen Sie aus der Dropdown-Liste ein vorhandenes Profil aus oder wählen Sie **Benutzerdefiniert**, um die unten stehenden Einstellungen selbst zu konfigurieren.

  > **Anmerkung**
  >
  > Die Auswahl eines vorhandenen Profils vervollständigt die Konfiguration automatisch mit den Einstellungen dieses Profils, die hier nicht bearbeitet werden können. Durch die Auswahl von Benutzerdefiniert können Sie das Profil nach Bedarf konfigurieren.

- **Version**: Wählen Sie aus der Dropdown-Liste die FSLogix-Version aus.
- **Sitzungshost-Registry für Entra ID-verbundenen Speicher konfigurieren**, **Konten lokaler Admins von FSLogix ausschließen** und **Domänenkonten von FSLogix ausschließen**: Wählen Sie bei Bedarf eine dieser Optionen aus und geben Sie die entsprechenden Domänenkonten in das Feld **Domänenkonten** ein.
- **Pfad für FSLogix-Profile (VHDLocation)**: Wählen Sie **Überschreiben**, um statt des Standards einen eigenen Ort für den Profilspeicher anzugeben.
- **Office-Container konfigurieren, um Userdaten von Microsoft Office automatisch weiterzuleiten (ODFC)**: Wählen Sie diese Option, um Office-Containerdaten automatisch weiterzuleiten, und geben Sie den **Pfad für FSLogix Office-Container (VHDLocation)** an, falls Sie den Standard überschreiben.

- **FSLogix Cloud Cache**: Wählen Sie den Umschalter, um FSLogix Cloud Cache zu aktivieren, der Profile für Ausfallsicherheit asynchron über mehrere Speicherorte hinweg repliziert.

  > **Tipp**
  >
  > Aus Leistungsgründen empfehlen wir dringend die Verwendung von Premium-SSD-Disks und ephemeren Betriebssystem-Disks, wenn Cloud Cache aktiviert ist.

- **App Service-Einstellungen verwalten** und **Protokolleinstellungen verwalten**: Wählen Sie eine der Optionen, um die entsprechenden FSLogix-Registry-Einstellungen zu bearbeiten.
- **FSLogix-Registryoptionen**: Wählen Sie aus der Dropdown-Liste **Bearbeitungsmodus** die Option **Alle Einstellungen** oder **Erweitert** aus und konfigurieren Sie dann die einzelnen Registry-Werte in den Tabs Profileinstellungen, ODFC-Einstellungen, Cloud Cache-Einstellungen, App Service-Einstellungen und Protokolleinstellungen. Verwenden Sie das Feld **Einstellungen nach Namen suchen**, um zu filtern.

  > **Anmerkung**
  >
  > Die vollständige Liste der konfigurierbaren Registry-Einstellungen finden Sie unter FSLogix-Anpassung pro Hostpool.

Wählen Sie **Weiter**.

RDP konfigurieren

- **RDP-Profil**: Wählen Sie das RDP-Profil aus der Dropdown-Liste aus.

  > **Anmerkung**
  >
  > Dieser Schritt umfasst auch RDP Shortpath-Netzwerkeinstellungen und für ein benutzerdefiniertes Profil individuelle Umleitungs- und Sitzungsoptionen. Weitere Informationen finden Sie unter Benutzerdefinierte RDP-Konfiguration für Hostpools.

Wählen Sie **Weiter**.

Tags konfigurieren

- **Tag-Gruppen**: Wählen Sie optional aus der Dropdown-Liste eine vorhandene Tag-Gruppe aus. Die Auswahl einer Tag-Gruppe füllt die Felder „Name“ und „Wert“ unten automatisch mit ihren vordefinierten Werten aus.
- **Tag anwenden**: Geben Sie optional den **Namen** und den **Wert** des Azure-Tag ein, das auf den Hostpool angewendet werden soll.

> **Anmerkung**
>
> Sie können mehrere Tags angeben. Weitere Informationen zur Verwendung von Tags zum Organisieren Ihrer Azure-Ressourcen finden Sie in diesem Microsoft Artikel.

- **Tag „cm-resource-parent“ hinzufügen**: Wählen Sie diese Option, um dem Hostpool das Tag „cm-resource-parent“ hinzuzufügen.

Wählen Sie **Weiter**.

Assistenten abschließen

- **Anwendungsrichtlinien**: Wählen Sie optional die Anwendungsrichtlinien aus, die dem Hostpool zugewiesen werden sollen.

> **Anmerkung**
>
> Dieser Schritt zeigt einen Hinweis an, dass die Erstellung des Hostpools als Hintergrundaufgabe ausgeführt wird.

Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Absenden**.

Sie werden automatisch zur Seite mit den Auto-scale-Einstellungen des neuen Hostpools weitergeleitet. Konfigurieren Sie bei Bedarf die automati-

sche Skalierung des Hostpools. Weitere Informationen finden Sie unter Dynamische automatische Skalierung für Hostpools aktivieren [92].

Ergebnis

Der Prozess der Hostpool-Erstellung beginnt. Wenn das Autoscaling aktiviert wurde, kann der Abschluss einige Zeit in Anspruch nehmen. Andernfalls wird der Hostpool sofort erstellt. Dadurch wird ein „leerer" Hostpool erstellt – in diesem Hostpool befinden sich keine Sitzungshosts. Ein Endbenutzer, der versucht, eine Verbindung mit dem leeren Hostpool herzustellen, wird darüber informiert, dass keine Ressourcen (d. h. Sitzungshosts) zur Bereitstellung eines Desktops verfügbar sind. Sie können den Fortschritt im Abschnitt **Hostpool-Aufgaben** überwachen.

Verwandte Themen

- Dynamische automatische Skalierung für Hostpools aktivieren [92]
- Hostpools [75]
- Statische Hostpools ohne automatische Skalierung erstellen
- Hosts, Hostpools und Workspaces löschen

Hostpool-Profile verwalten

Hostpool-Profile vereinfachen die Erstellung neuer Hostpools: Sie können wiederverwendbare Profile für Auto-scale-Einstellungen, FSLogix-Einstellungen, RDP-Einstellungen, Directory-Einstellungen und Sitzungszeitlimits definieren. Wenn Sie eine dieser Einstellungen für einen Hostpool konfigurieren, können Sie ein vordefiniertes Profil auswählen. Dies macht eine manuelle Konfiguration für jeden Pool oder Zeitplan überflüssig.

> **Anmerkung**
>
> Autoscaling-Profile sind nur in der Nerdio Manager**Premium-Edition** verfügbar.

Um Ihre FSLogix-Konfiguration beim Verschieben von Usern in einen neuen Hostpool mithilfe eines Hostpool-Profils konsistent zu halten, lesen Sie User

mit FSLogix-Kontinuität von Windows 10- zu Windows 11-AVD-Hostpools migrieren.

Hostpool-Profil erstellen

Führen Sie die folgenden Schritte aus, um ein neues Hostpool-Profil zu erstellen.

So erstellen Sie ein Profil:

1. Navigieren Sie zu **Cloud-Desktops**> **Azure Virtual Desktop** > **Hostpool-Profile**.
2. Wählen Sie im Tab **Hostpool-Profile** (Standard) die Option **Neues Profil** aus.
3. Wählen Sie das Profil aus, das Sie erstellen möchten:
   - **Autoscaling**: Geben Sie die folgenden Informationen ein:
     - **Autoscaling-Modus**: Wählen Sie aus der Dropdownliste den Autoscaling-Modus aus.

       Die folgenden Modi sind verfügbar:
       - **Freigegeben**: Für alle gepoolten dynamischen Hostpools.
       - **Zeitplanbasiert (Persönlich)**: Für Single-User-Desktop (persönlich) Hostpools mit Autoscaling, das gemäß dem festgelegten Zeitplan durchgeführt wird.
       - **User-gesteuert (persönlich)**: Für Single-User-Desktop (persönlich) Hostpools mit Autoscaling, das durchgeführt wird, wenn keine aktiven oder getrennten Sitzungen vorhanden sind.
     - **Name**: Eingeben Sie den Profilnamen.
     - **Beschreibung**: Eingeben Sie die Profilbeschreibung.
     - Für alle anderen Parameter siehe den entsprechenden Artikel:
       - Für gepoolte dynamische Hostpools: Dynamische automatische Skalierung für Hostpools aktivieren [92]
       - Für persönliche Hostpools mit Single-User-Desktop (persönlich): Auto-scale für persönliche Hostpools aktivieren [110].
   - **Directory**: Führen Sie die Schritte wie unter Active Directory-Einstellungen des Hostpools konfigurieren [156] beschrieben aus.
   - **RDP**: Führen Sie die Schritte wie unter RDP-Einstellungsprofile konfigurieren beschrieben aus.

- **FSLogix**: Führen Sie die Schritte wie unter FSLogix-Einstellungen und -Konfiguration [213] beschrieben aus.
- **Sitzungszeitlimits**: Führen Sie die Schritte wie unter Sitzungszeitlimit-Profil erstellen beschrieben aus.

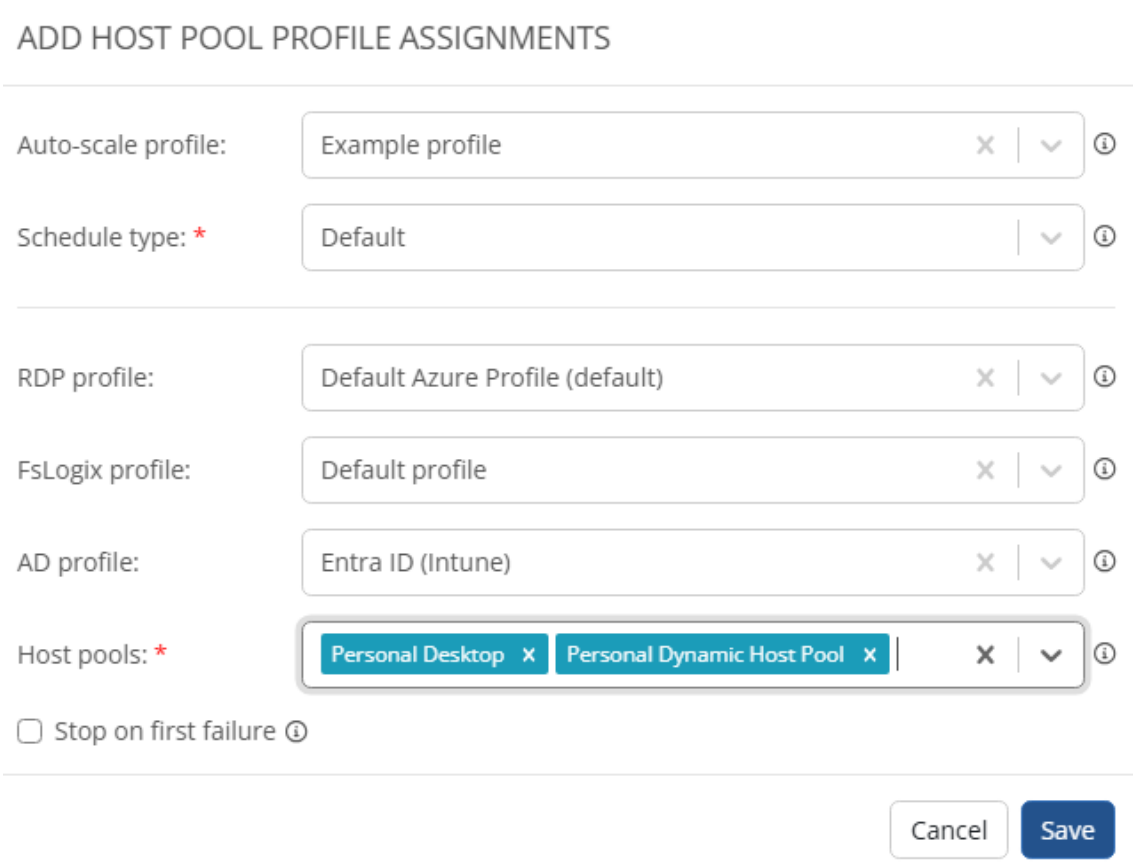
4. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern**.

Hostpool-Profil zuweisen

Sobald Sie ein Hostpool-Profil erstellt haben, können Sie es den entsprechenden Hostpools zuweisen.

So weisen Sie einem Hostpool ein Profil zu:

1. Navigieren Sie zu **Cloud-Desktops** > **Azure Virtual Desktop** > **Hostpool-Profile**.
2. Wählen Sie im Aktionsmenü **Zuweisungen** und dann **Neue Zuweisungen**.
3. Geben Sie die folgenden Informationen ein:
   - **Autoscaling-Profil**: Wählen Sie aus der Dropdown-Liste das Autoscaling-Profil aus.
   - **Zeitplantyp**: Wählen Sie aus der Dropdown-Liste den Zeitplantyp aus.
   - **RDP-Profil**: Wählen Sie aus der Dropdown-Liste den RDP-Profiltyp aus.
   - **FSLogix-Profil**: Wählen Sie aus der Dropdown-Liste den FSLogix-Profiltyp aus.
   - **AD-Profil**: Wählen Sie aus der Dropdown-Liste das AD-Profil aus.
   - **Hostpools**: Wählen Sie aus der Dropdown-Liste den/die Hostpool(s) aus.
   - **Bei erstem Fehler beenden**: Jeder Hostpool wird einzeln verarbeitet. Wählen Sie diese Option, um die verbleibenden Vorgänge beim ersten Fehler abzubrechen.



4. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern**.

> **Anmerkung**
>
> Sie können für Zuweisungen von Autoscaling-Profilen Folgendes ausführen:
>
> - **Ausgewählte Alternative bearbeiten**: Wählen Sie dies aus, um einen alternativen Zeitplan zu bearbeiten.
> - **Auswahl entfernen**: Wählen Sie diese Option, um ausgewählte Zuweisungen zu entfernen.

Hostpool-Profile verwalten

Sie können vorhandene Hostpool-Profile verwalten.

So verwalten Sie Profile:

1. Navigieren Sie zu **Cloud-Desktops** > **Azure Virtual Desktop** > **Hostpool-Profile**.

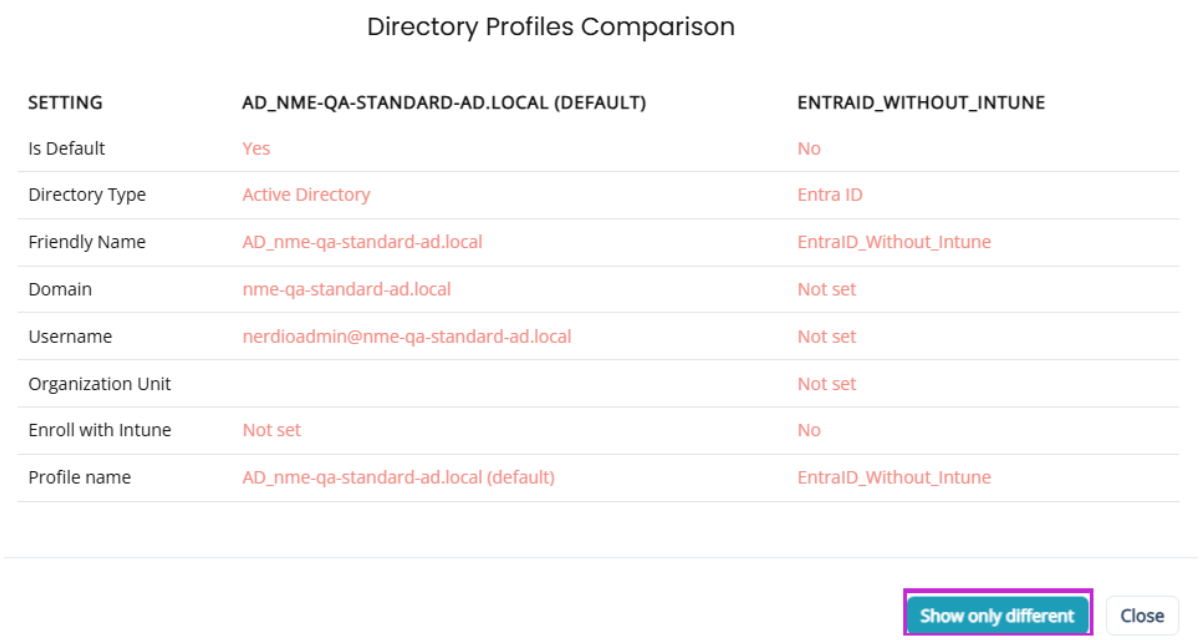
2. Finden Sie das Hostpool-Profil, mit dem Sie arbeiten möchten.
3. Wählen Sie aus dem Folgenden aus:
   - Wählen Sie das Stift-Symbol, um das Profil zu bearbeiten.
   - Wählen Sie das Menü für weitere Aktionen für die folgenden Optionen:
     - **Zuweisungen**: Bearbeiten Sie die Zuweisungen.
     - **Als Standard festlegen**: Legt das Profil als Standard fest.
     - **Klonen**: Erstellen Sie einen Klon des Profils.
     - **Löschen**: Löschen Sie das Profil.

Hostpool-Profile vergleichen

Sie können zwei bestehende Hostpool-Profile vergleichen.

So vergleichen Sie Profile:

- Wählen Sie die Profile aus, die Sie vergleichen möchten.
- Wählen Sie **Vergleichen**.
- Wählen Sie optional **Nur Unterschiede anzeigen**, um nur die Eigenschaften anzuzeigen, die sich zwischen den beiden Profilen unterscheiden. Wählen Sie **Alle anzeigen**, um wieder alle Eigenschaften anzuzeigen, einschließlich derer, die bei beiden Profilen identisch sind.



Dynamische Hostpool-Autoskalierung aktivieren

Die Autoscaling-Funktion stellt sicher, dass nur so viele Sitzungshost-VMs aktiv sind, wie zur Deckung des aktuellen Bedarfs erforderlich sind. Bei Nichtgebrauch werden VMs beendet oder gelöscht. Wenn die Nachfrage steigt oder zu bestimmten Tageszeiten werden zusätzliche VMs im Hostpool gestartet oder erstellt. Dies ermöglicht Kosteneinsparungen.

Wenn ein Unternehmen beispielsweise während der Geschäftszeiten 300 User virtueller Desktops online hat und nach Feierabend nur 50 User, kann der Hostpool, der diese User bedient, so konfiguriert werden, dass während der Geschäftszeiten mehr VMs eingeschaltet sind und diese VMs nach Feierabend, wenn sie nicht benötigt werden, heruntergefahren werden. Dies ermöglicht es Unternehmen, Kosten zu sparen und gleichzeitig den Bedarf zu decken.

Sie können dynamische Hostpools automatisch skalieren und diese Funktion aktivieren und konfigurieren. Dieser Artikel behandelt die Einstellungen für das automatische Skalieren dynamischer Hostpools, einschließlich der Skalierungsoptionen (wie Auslöser, Hostpool-Dimensionierung und Einschränkungen beim horizontalen Herunterskalieren), der Aggressivität beim horizontalen Herunterskalieren, des Rolling Drain Mode und des Pre-Stagings von Hosts.

> **Anmerkung**
>
> Standardmäßig ist die Option **Autoscaling** deaktiviert. Wenn Sie das Autoscaling aktivieren, können Sie das Desktop-Image, die VM-Größe und die Vorlage für den Betriebssystemdatenträger konfigurieren sowie die Kriterien für die Größe des Hostpools, die Skalierungslogik und Pre-Staging-Hosts festlegen.

So aktivieren Sie das Autoscaling für dynamische Hostpools:

1. Finden Sie den dynamischen Hostpool, mit dem Sie arbeiten möchten.

2. Fahren Sie im Menü „Weitere Optionen“ ⋮ mit der Maus über **Autoscaling** und wählen Sie **konfigurieren**.
3. Geben Sie die folgenden grundlegenden Informationen zum Autoscaling ein:
   - **Autoscaling-Zeitzone**: Wählen Sie aus der Dropdownliste die Zeitzone für den Autoscaling-Prozess aus.
   - **Name**: Geben Sie den Namen der neu hinzugefügten Hosts für das Präfix oder das Präfix+Muster ein.
     - **Präfix/Muster**: Wählen Sie aus der Dropdownliste aus, ob ein Präfix oder ein Muster verwendet werden soll.

       Anmerkung
       - **Präfix** kann beim Erstellen mehrerer Sitzungshosts verwendet werden. Das Präfix ist auf 10 gültige Zeichen für Windows-Computernamen begrenzt. Bei Verwendung eines Präfixes wird automatisch ein eindeutiges Suffix im Format „-xxxx“ angehängt, wobei xxxx für 4 zufällige alphanumerische Zeichen steht. Zum Beispiel: AVDHOST-s72h. Fügen Sie dem Präfix kein „-“ hinzu.
       - **Muster** kann verwendet werden, um eine erweiterte Namenskonvention für neue Hosts festzulegen. Musterzeichen müssen in {} eingeschlossen werden und können # (für fortlaufende Nummern) und/oder ? (für zufällige alphanumerische Zeichen) sein. Ein # steht für Zahlen von 0 bis 9, zwei # stehen für Zahlen von 0 bis 99 usw.
         - Beispiel 1: AVDHOST{###} (AVDHOST000..AVDHOST999).
         - Beispiel 2: AVDHOST-{???} (AVDHOST-d83, AVDHOST-7sl usw.).
   - **Netzwerk**: Wählen Sie aus der Dropdown-Liste das Netzwerk aus, mit dem die VM verbunden werden soll.

> **Anmerkung**
>
> Die VM, die im ausgewählten Netzwerk erstellt wird, wird in der dem Netzwerk zugeordneten Azure-Region erstellt.

- **Zusätzliche Subnetze**: Wählen Sie aus der Dropdown-Liste zusätzliche Subnetze innerhalb desselben virtuellen Netzwerks aus.

> **Anmerkung**
>
> Wenn ein bestimmtes Subnetz beim Scale-out nicht über genügend IP-Adressen verfügt, wird beim Erstellen zusätzlicher Sitzungshosts automatisch das nächste Subnetz ausgewählt.

- **Netzwerkverteilung**: Wählen Sie aus der Dropdown-Liste aus, wie die Last über das Netzwerk verteilt werden soll.

> **Anmerkung**
>
> Wählen Sie **Tiefensuche**, um die Last nacheinander in einer festen Reihenfolge auf die Knoten zu verteilen, oder wählen Sie für eine optimale Verteilung **Breitensuche**, um die Last proportional basierend auf der aktuellen Ressourcennutzung auszugleichen.

- **Desktop-Image (Vorlage)**: Wählen Sie aus der Dropdown-Liste ein Desktop-Image aus, das als Golden Image für neue Sitzungshosts verwendet werden soll.
- **„Staged"-Imageversion verwenden**: Wählen Sie diese Option, um die „staged" Imageversion zu verwenden, falls verfügbar, wenn der Hostpool skaliert wird.
- **VM-Größe (Vorlage)**: Wählen Sie aus der Dropdownliste die VM-Größe für neue Sitzungshosts aus.
- **Ausgeführter Betriebssystemdatenträger (Vorlage)**: Wählen Sie aus der Dropdownliste den Typ und die Größe des Betriebssystemdatenträgers für neue Sitzungshosts aus.

- **Typ des Betriebssystemdatenträgers bei Beendigung**: Wählen Sie aus der Dropdownliste den Typ des Betriebssystemdatenträgers aus, wenn Sitzungshost-VMs beendet sind.

> **Anmerkung**
>
> Weitere Informationen zur Konfiguration des automatischen Skalierens von Betriebssystem-Disks finden Sie unter Auto-scale-Kostenoptimierung für Betriebssystem-Disk-Speicher [134].

- **Ressourcengruppe**: Wählen Sie aus der Dropdownliste die Ressourcengruppe aus, in der VMs erstellt werden sollen.
- **VM-Benennung**: Wählen Sie aus der Dropdownliste die zu verwendende VM-Benennung aus.

> **Anmerkung**
>
> Host-VMs, die automatisch durch den Prozess des horizontalen Hochskalierens oder Auto-Grow erstellt werden, erhalten Namen basierend auf dem ausgewählten VM-Benennungsmodus. Weitere Informationen finden Sie unter Wie Sitzungshost-VM-Namen generiert werden.
>
> - **Namen wiederverwenden**: Versuchen Sie immer, Namen wiederzuverwenden, die zuvor im Pool verwendet wurden, sofern verfügbar.
> - **Standardnamen**: Verwenden Sie den nächsten verfügbaren Namen.
> - **Eindeutige Namen**: Versuchen Sie immer, einen eindeutigen Namen für neue Hosts zu verwenden.

- **Automatisches Reimaging für benutzte Hosts**: Wählen Sie eine der folgenden Optionen aus dem Dropdown-Menü:
  - **Deaktiviert**: Es findet kein Reimaging statt.
  - **Immer**: Hosts, an denen sich mindestens ein User angemeldet hat, werden einem Reimaging unterzogen. Bei Multi-Session-Hosts erfolgt das Reimaging, sobald sich der letzte User abmeldet.

  - **Nur während horizontal herunterskalierenden Beschränkungen**: Das Reimaging erfolgt nur innerhalb des konfigurierten Zeitraums der horizontal herunterskalierenden Beschränkungen, wodurch das Risiko einer reduzierten Sitzungskapazität im Hostpool zu anderen Zeiten gemindert wird.
- **Skalierungsintervall**: Wählen Sie das Zeitintervall aus der Dropdown-Liste aus.
- **Zeitplantyp**: Wählen Sie den **Standardplan** oder den **alternativen Zeitplan** aus.
- Wählen Sie den **Standardplan** oder den **alternativen Zeitplan** aus.

> **Anmerkung**
>
> Nerdio Manager ermöglicht es Ihnen, separate Einstellungen für die automatische Skalierung für einen Standardplan (normaler Betrieb) und einen alternativen Zeitplan (außerhalb des normalen Betriebs) zu konfigurieren. Sie möchten beispielsweise möglicherweise an Wochenenden oder Feiertagen weniger Sitzungshosts zur Verfügung haben. Alternativ möchten Sie möglicherweise zwei Wochen vor Weihnachten mehr Sitzungshosts zur Verfügung haben, wenn Sie eine große Anzahl temporärer Kunden-Support-Agenten beschäftigen. In beiden Fällen würden Sie den Bereich **alternativer Zeitplan** verwenden, um die Einstellungen für die automatische Skalierung für Zeiträume außerhalb des normalen Betriebs zu konfigurieren.

- Um einen alternativen Zeitplan zu erstellen, wählen Sie **alternativen Zeitplan** und geben Sie die folgenden Informationen ein:

> **Anmerkung**
>
> Die oben auf dieser Seite angezeigten geschätzten monatlichen Kosten berücksichtigen nur die Einstellungen des Standardplans.

  - **Zeitplan**: Schalten Sie diese Option auf **Aktiviert**.

- **Tage**: Wählen Sie aus der Dropdownliste den/die Nebenzeittag(e) aus.
- **Daten**: Wählen Sie das/die spezifische(n) Nebenzeitsdatum/-daten aus.
- Wählen Sie **+** oder **-**, um Nebenzeitsdaten hinzuzufügen oder zu entfernen.

> **Anmerkung**
>
> Tage und Datumsangaben werden kombiniert und nicht als Alternativen behandelt. Wenn Sie beides auswählen, gilt der alternative Zeitplan nur an den ausgewählten Wochentagen innerhalb der ausgewählten Datumsangaben. Es gilt nicht einmalig für den gesamten Datumsbereich. Beispiel:
>
> - Um den alternativen Zeitplan nur während der Feiertage anzuwenden, wählen Sie die Datumsangaben für diesen Zeitraum aus (zum Beispiel 24. bis 27. Dezember) und lassen Sie **Tage** leer.
> - Um ihn auf jedes Wochenende anzuwenden, wählen Sie Samstag und Sonntag aus und lassen Sie **Datumsangaben** leer.
> - Um ihn nur an den Wochenenden innerhalb eines Teils des Monats anzuwenden, wählen Sie Samstag und Sonntag sowie die Datumsangaben aus (zum Beispiel 10. bis 24. Dezember). Der Zeitplan gilt dann für die Samstage und Sonntage zwischen dem 10. und 24. Dezember.

- Wählen Sie das **Autoscaling-Profil (nur Premium)**:
  - Wählen Sie aus der Dropdownliste das zu verwendende Autoscaling-Profil aus. Wählen Sie alternativ **Benutzerdefiniert**, um eine benutzerdefinierte Autoscaling-Konfiguration zu erstellen.

> **Anmerkung**
>
> Weitere Details finden Sie unter Auto-scale Profile verwalten [87].

4. Geben Sie die folgenden **Hostpool-Eigenschaften** Informationen ein:
   - **Sitzungslimit je Host**: Geben Sie den Maximalwert für die Anzahl der Sitzungen je Host ein. Sobald dieses Sitzungslimit erreicht ist und keine Hosts mehr verfügbar sind, wird automatisch ein neuer Host gestartet (sofern vorhanden).
   - **Lastenausgleich**: Wählen Sie den gewünschten Lastenausgleich aus der Dropdownliste aus.

     > **Anmerkung**
     > - **Breitensuche** bedeutet, dass der Algorithmus für das Load-Balancing die User gleichmäßig auf alle verfügbaren Sitzungshosts verteilt.
     > - **Tiefensuche** bedeutet, dass der Algorithmus für das Load-Balancing alle User auf dem ersten Sitzungshost platziert, bis das Sitzungslimit des Hosts erreicht ist. Erst dann platziert er die User auf dem nächsten Sitzungshost. Bei Bedarf schaltet er den virtuellen Computer ein und stellt ihn den Usern zur Verfügung.

   - **VM beim Herstellen der Verbindung starten**: Wählen Sie diese Option, um die Sitzungshost-VMs beim Herstellen der Verbindung zu starten.
5. Geben Sie die folgenden Informationen zur **Hostpool-Kapazität** ein:
   - **Messverfahren**: Wählen Sie aus der Dropdown-Liste aus, wie der Mindestwert für die Kapazität aktiver Hosts und die Burst-Kapazität gemessen werden.
     - **Anzahl**: Geben Sie **Min. aktive Hostkapazität** und **Burst über Basiskapazität** als Anzahl der Hosts ein.
     - **Prozent**: Die Felder ändern sich zu **Min. aktive Hostkapazität in Prozent** und **Burst über Basiskapazität in Prozent**. Geben Sie jeden Wert als Prozentsatz der **Basis-Hostpool-Kapazität** ein. Die Anzahl der Hosts wird aufgerundet und das Ergebnis unter jedem Feld angezeigt.

Bei einer **Basis-Hostpool-Kapazität** von beispielsweise 9 Hosts wird eine **Min. aktive Hostkapazität in Prozent** von 30 als 3 von 9 Hosts angezeigt, und ein **Burst über Basiskapazität in Prozent** von 70 wird als Burst 7, insgesamt 16, angezeigt.

- **Aktiver Host definiert als**: Wählen Sie aus der Dropdown-Liste die Definition für den aktiven Host aus.

> **Anmerkung**
>
> Bei der Einstellung „VM gestartet“ identifiziert das System eine Sitzungshost-VM als aktiv, solange die VM in Azure ausgeführt wird. Es gibt nur sehr wenige Fälle, in denen „VM gestartet“ ausgewählt werden sollte.
>
> Bei der Einstellung „AVD-Agent verfügbar“ identifiziert das System eine Sitzungshost-VM nur dann als aktiv, wenn das AVD-Backend Heartbeats empfängt und den Sitzungshost als „Verfügbar“ erkennt. Im Allgemeinen sollten Sie „AVD-Agent verfügbar“ auswählen.

- **Basis-Hostpool-Kapazität**: Geben Sie die Anzahl der Sitzungshost-VMs ein, die immer Teil dieses Hostpools sein sollen. Diese Sitzungshosts können gestoppt oder ausgeführt werden.
- **Minimale aktive Host-Kapazität**: Geben Sie die Mindestanzahl an laufenden Sitzungshosts ein, die immer verfügbar sind. Normalerweise muss ein Sitzungshost ausgeführt werden, damit sich User anmelden können oder das Feature „Beim Herstellen der Verbindung starten“ aktiviert ist. Andere VMs können entweder gestoppt oder eingeschaltet sein, wie durch die Logik zum automatischen Skalieren konfiguriert.
- **Burst über die Basis-Kapazität**: Geben Sie die Kapazität ein, um bei User-Bedarf über die Standardanzahl an Sitzungshost-VMs hinaus zu skalieren. Das System erstellt bei Bedarf automatisch bis zu dieser Anzahl neuer Sitzungshost-VMs über die **Basis-Hostpool-Kapazität** hinaus. Diese Sitzungshosts werden als erste entfernt, wenn das System nach den Geschäftszeiten horizontal herunterskaliert.

6. Geben Sie die folgenden Informationen zur **Skalierungslogik** ein:
   - **Mehrere Auslöser für das automatische Skalieren verwenden**: Wählen Sie diese Option, um mehrere Nutzungs-Auslöser für das horizontale Hoch- und Herunterskalieren zu aktivieren. Wenn aktiviert, können

Sie die Anzahl der Hosts in einer Gruppe für das horizontale Hoch- oder Herunterskalieren konfigurieren.

> **Anmerkung**
>
> Das Feature für mehrere Autoscaling-Auslöser ist nur in der Nerdio Manager **Premium**-Edition verfügbar.

> **Anmerkung**
>
> - Automatisches Skalieren fügt Kapazität hinzu, wenn **irgendeine** der Bedingungen für das horizontale Hochskalieren erfüllt ist. Kapazität wird nur entfernt, wenn **alle** Bedingungen für das horizontale Herunterskalieren erfüllt sind.
> - Verwenden Sie die + und - Buttons, um Auslöser für das horizontale Hochskalieren hinzuzufügen oder zu entfernen. Sie können bis zu 3 Auslöser auswählen.
> - Sie können beispielsweise mehrere CPU-Auslastungsauslöser verwenden, um bei einer CPU-Auslastung von 65 %, die 15 Minuten lang anhält, oder bei einer CPU-Auslastung von 90 %, die 5 Minuten lang anhält, horizontal hochzuskalieren, je nachdem, welcher Wert zuerst erreicht wird. So können Sie das horizontale Hochskalieren anhand mehrerer Schwellenwerte für Auslöser genauer steuern.

- **Autoscaling-Auslöser auswählen**: Wählen Sie den Auslöser für das horizontale Hochskalieren aus der Dropdown-Liste aus.

> **Anmerkung**
>
> Die verfügbaren Auslöser sind:
>
> - **CPU-Auslastung** oder **RAM-Auslastung**: Dies wird horizontal hochskaliert, wenn die durchschnittliche CPU- oder RAM-Auslastung über alle laufenden Sitzungshosts im Pool hinweg einen vordefinierten Wert für eine vordefinierte Dauer überschreitet.
> - **Durchschnittliche aktive Sitzungen**: Dies wird horizontal hochskaliert, wenn die durchschnittliche Anzahl aktiver Sitzungen pro Host einen vordefinierten Wert überschreitet.
> - **Verfügbare Sitzungen**: Die Anzahl der verfügbaren Hosts wird gewartet, indem innerhalb der Grenzen der Hostpool-Dimensionierung und des Maximalwerts an Sitzungen pro Host horizontal hoch- und herunterskaliert wird.
> - **Benutzergesteuert**: Hosts werden gestartet, wenn sich User verbinden, und nach einer definierten Zeitspanne automatisch beendet, nachdem sich alle User abgemeldet haben.

- Für **CPU-Auslastung oder RAM-Auslastung**:
  - **Starten oder Erstellen (horizontal hochskalieren) bis zu**: Skalieren Sie horizontal hoch, indem Sie Sitzungshosts starten (falls angehaltene VMs vorhanden sind) oder erstellen (falls keine angehaltenen VMs vorhanden sind), wenn der Auslöser überschritten wird.
  - **Beenden oder Entfernen (horizontal herunterskalieren) bis zu**: Skalieren Sie horizontal herunter, indem Sie Sitzungshosts beenden (falls keine Burst-VMs vorhanden sind) oder entfernen (falls Burst-VMs vorhanden sind), wenn der Auslöser für das horizontale Herunterskalieren erfüllt ist.
- Für **Durchschnittliche aktive Sitzungen**:
  - **Starten oder Erstellen (horizontal hochskalieren) bis zu**: Skalieren Sie horizontal hoch, indem Sie Sitzungshosts starten (falls angehaltene VMs vorhanden sind) oder erstellen (falls keine angehaltenen VMs vorhanden sind), wenn die durchschnittliche Anzahl aktiver Sitzungen über alle Hosts hinweg überschritten wird.

- **Beenden oder Entfernen (horizontal herunterskalieren) bis zu**: Horizontal herunterskalieren durch Beenden (falls keine Burst-VMs vorhanden sind) oder Entfernen (falls Burst-VMs vorhanden sind) von Sitzungshosts, wenn die durchschnittliche Anzahl aktiver Sitzungen über alle Hosts hinweg unter der angegebenen Zahl liegt.

- Für **Verfügbare Sitzungen**:
  - **Maximalwert für die Anzahl der Hostpool-Sitzungen**: Zeigt den Maximalwert für die Anzahl der Sitzungen an, die der Hostpool unterstützen kann. Sie können diesen Wert nicht bearbeiten.
  - **Warten Sie bis zu X verfügbare Sitzungen**: Geben Sie die Anzahl der Sitzungen ein, die entweder immer oder während der Arbeitszeiten verfügbar sein müssen.

    > **Anmerkung**
    >
    > Dies stellt sicher, dass während der Arbeitszeiten oder jederzeit diese Anzahl an Sitzungen verfügbar ist. Die Arbeitszeiten beginnen um den im Abschnitt **Pre-Staging Hosts** angegebenen Arbeitsbeginn und enden zu Beginn des Herunterskalierungszeitraums, der im Abschnitt „Einschränkungen für das Herunterskalieren“ weiter unten angegeben ist.

  - **Außerhalb der Arbeitszeiten**: Geben Sie die Anzahl der Sitzungen ein, die außerhalb der Arbeitszeiten gewartet werden sollen.

    > **Anmerkung**
    >
    > Dieser Wert darf die Anzahl der während der Arbeitszeiten verfügbaren Desktops nicht überschreiten.

  - **Arbeitszeiten**: Wählen Sie aus den Dropdown-Listen die Start- und Endzeiten für die Arbeitszeiten aus.

- Für **User-gesteuert**:
  - **Desktops beenden nach**: Wählen Sie aus der Dropdown-Liste aus, nach wie vielen Minuten nach der Abmeldung aller User horizontal herunterskaliert werden soll.

> **Anmerkung**
>
> Desktops werden nur dann automatisch beendet, wenn keine aktiven oder getrennten Sitzungen vorhanden sind. Um getrennte User nach einer bestimmten Zeit automatisch abzumelden, verwenden Sie die Einstellungen für User-Sitzungslimits in den Hostpool-Eigenschaften.

  - **Burst-Hosts, wenn die Anzahl der verfügbaren Sitzungen unter folgenden Wert fällt**: Wenn die Anzahl der verfügbaren Sitzungen unter den angegebenen Wert fällt, wird automatisch ein neuer Sitzungshost hinzugefügt, bis der Maximalwert der Burst-Kapazität erreicht ist.
- **Einschränkungen beim Herunterskalieren**:
  - **Hosts nur beenden oder entfernen (horizontal herunterskalieren) ab**: Wählen Sie aus der Dropdown-Liste den Zeitpunkt für die Durchführung des Herunterskalierungsvorgangs aus. Wählen Sie **<any time>**, um das Herunterskalieren zu jeder Zeit zu ermöglichen.
  - **Aggressivität beim horizontalen Herunterskalieren**: Wählen Sie aus der Dropdown-Liste die Aggressivität beim horizontalen Herunterskalieren aus.

Anmerkung

- **Hohe Aggressivität**: Die Aggressivität beim horizontalen Herunterskalieren ist standardmäßig auf **Hoch** eingestellt. Das bedeutet, dass nach Geschäftsschluss Hosts, auf denen aktive oder getrennte Sitzungen ausgeführt werden, garantiert automatisch gelöscht oder ausgeschaltet werden, um die Kapazität zu reduzieren. Nach Geschäftsschluss entfernt die automatisch skalierende Logik zuerst die Hosts, auf denen keine Sitzungen ausgeführt werden. Die verbleibenden Hosts werden basierend auf der geringsten Anzahl der darauf ausgeführten Sitzungen sortiert. Die User mit aktiven Sitzungen werden dann zusammengefasst und auf einen einzigen Host verschoben, während die anderen Hosts durch das automatische Skalieren entfernt werden. Vor dem Entfernen der Sitzungshosts wird eine Warnmeldung an die User mit aktiven Sitzungen gesendet.
- **Mittlere Aggressivität**: Wenn die Aggressivität beim horizontalen Herunterskalieren auf **Mittel** eingestellt ist, entfernt die Skalierungslogik nach Geschäftsschluss nur die Hosts, auf denen getrennte Sitzungen ausgeführt werden. Die Sitzungshosts, auf denen aktive Sitzungen ausgeführt werden, werden nicht entfernt. In diesem Fall wird der Hostpool in gewissem Umfang horizontal herunterskaliert.
- **Geringe Aggressivität**: Wenn die Aggressivität beim horizontalen Herunterskalieren auf **Gering** eingestellt ist, entfernt die Skalierungslogik nach Geschäftsschluss nur diejenigen Sitzungshosts, auf denen absolut keine Sitzungen ausgeführt werden. Die automatisch skalierende Logik entfernt keinen der Sitzungshosts, auf denen Sitzungen ausgeführt werden – weder aktive noch getrennte. Obwohl diese Option für die User weniger störend ist, gibt es keine Garantie dafür, dass der Hostpool jemals horizontal herunterskaliert wird.

- **Hosts deaktivieren (Drain-Modus)**: Optional können Sie die Engine für das automatische Skalieren anweisen, alle Hosts zu Beginn des Fensters für das horizontale Herunterskalieren zu deaktivieren. Sie lässt die Mindestanzahl an Hosts übrig, wie in **Mindestwert aktive Hostkapazität** im Abschnitt **Hostpool-Größe** angegeben.

7. Geben Sie die folgenden Informationen zum **Rolling Drain Mode** ein:

> **Anmerkung**
>
> - Sie können mehrere Drain-Fenster erstellen und einen bestimmten Prozentsatz Ihrer Hosts außerhalb des Fensters für die Einschränkungen beim Herunterskalieren in den Drain-Modus versetzen. Dieses Feature ermöglicht es Ihnen, neue Verbindungen zu einem Prozentsatz der Hosts zu verhindern und diese Hosts schneller herunterzufahren, wodurch Ressourcenkosten eingespart werden.
> - Der Rolling Drain Mode wählt Hosts zum horizontalen Herunterskalieren wie folgt aus:
>   - Zuerst beginnt er mit den Hosts mit den wenigsten aktiven Sitzungen.
>   - Dann skaliert er Hosts herunter, die sich bereits im Drain-Modus befinden,
>   - Schließlich skaliert er Hosts mit der geringsten Anzahl an Gesamtsitzungen (aktiv + getrennt) herunter.
> - Wenn eine VM ephemeren Speicher verwendet, wird sie beim Herunterskalieren im Rolling Drain Mode deaktiviert, anstatt beendet zu werden.

- **Rolling Drain Mode**: Schalten Sie diese Option auf **Aktiviert**, um den Rolling Drain Mode zu aktivieren.
- **Fenstername**: Geben Sie den Namen für dieses Drain-Fenster ein.
- **Startzeit**: Wählen Sie aus den Dropdown-Listen die Startzeit aus, zu der dieses Drain-Fenster in Kraft tritt.

> **Anmerkung**
>
> Das letzte Drain-Fenster bleibt bis 23:59 Uhr in Kraft.

- **% Hosts im Drain Mode**: Geben Sie den Prozentsatz der Hosts im Drain Mode während dieses Fensters ein.

> **Anmerkung**
>
> Verwenden Sie , um Drain-Fenster hinzuzufügen oder zu entfernen.

- **Lastausgleich**: Wählen Sie aus der Dropdown-Liste den bevorzugten Algorithmus für das Load-Balancing aus.

> **Anmerkung**
>
> - **Tiefensuche**: Der Algorithmus für das Load-Balancing platziert User auf einem einzelnen Host, bis das Sitzungslimit erreicht ist. Anschließend werden User auf dem nächsten Host platziert, bis das Sitzungslimit dort ebenfalls erreicht ist.
> - **Breitensuche**: Der Algorithmus für das Load-Balancing verteilt User gleichmäßig auf die verfügbaren Sitzungshosts.

- **Aggressivität beim Herunterskalieren**: Wählen Sie aus der Dropdown-Liste die Aggressivität beim Herunterskalieren aus.

8. Geben Sie die folgenden Informationen für **Pre-Staging-Hosts** ein:

> **Anmerkung**
>
> Konfigurieren Sie das System so, dass einige Hosts in Bezug auf die Geschäftszeiten automatisch als verfügbare Kapazität für das Pre-Staging bereitgestellt werden. Sie können beispielsweise Hosts zu Beginn des Arbeitstages für das Pre-Staging bereitstellen, damit das System nicht in Echtzeit automatisch skalieren muss, wenn sich alle User gleichzeitig anmelden, wenn sie mit der Arbeit beginnen.

- **Mehrere Zeitpläne verwenden**: Wählen Sie diese Option, um die Verwendung mehrerer, sich nicht überschneidender Pre-Staging-Zeitplä-

ne zu aktivieren. Verwenden Sie , um Zeitpläne hinzuzufügen oder zu entfernen.

> **Anmerkung**
>
> Dies ist für den Auslöser „Verfügbare Sitzungen“ nicht verfügbar, wenn die Option „Während der Arbeitszeit“ festgelegt ist.

- **Arbeitstage**: Wählen Sie aus der Dropdown-Liste die Arbeitstage aus, an denen Pre-Staging-Aufgaben ausgeführt werden sollen.
- **Beginn der Arbeitszeit**: Wählen Sie aus der Dropdown-Liste die Anfangsstunde aus, zu der Pre-Staging-Aufgaben ausgeführt werden sollen.
- **Hosts müssen bei Arbeitsbeginn aktiv sein**: Geben Sie die Anzahl der Sitzungshosts ein, die zu diesem Zeitpunkt bereit sein sollen, Verbindungen von Usern anzunehmen.
- **Verzögerung beim horizontalen Herunterskalieren**: Wählen Sie aus den Dropdownlisten die Verzögerung in Stunden und Minuten aus, um das horizontale Herunterskalieren nach Beginn der Arbeitszeit einzuschränken. Hosts mit Pre-Staging werden während dieser Zeit nicht horizontal herunterskaliert, selbst wenn sie nicht verwendet werden.

9. Geben Sie die folgenden **Messaging**-Informationen ein:

> **Anmerkung**
>
> Das System sendet Nachrichten an alle User, die mit einem Sitzungshost verbunden sind, der für das Herunterskalieren ausgewählt wurde.

- **Send a Warning Message to User on the host**: Wählen Sie aus der Dropdown-Liste die Anzahl der Minuten vor dem Herunterskalieren aus, nach denen die Nachricht gesendet werden soll.
- **Nachrichteninhalt**: Geben Sie den Text der Warnmeldung ein.

10. Geben Sie die folgenden **Auto-Heal Broken Hosts**-Informationen ein:

> **Anmerkung**
>
> Sitzungshosts können aufgrund von Problemen mit dem Domänenvertrauen oder der FSLogix-Konfiguration beeinträchtigt werden. Der AVD-Agent meldet den Status solcher Hosts als nicht verfügbar. Administratoren müssen solche Hosts dann manuell aus dem Pool entfernen. Allerdings ermöglicht Nerdio Manager es Ihnen, eine Reihe von Aktionen zu konfigurieren, um diese Sitzungshosts während des Autoscaling-Prozesses zu reparieren. Autoscaling kann versuchen, „defekte“ Sitzungshosts automatisch durch Neustarten und Löschen/Neuerstellen zu reparieren. Es können einige Versuche unternommen werden, den Host neu zu starten, um ihn wieder in einen betriebsbereiten Zustand zu versetzen, und ihn anschließend entweder unverändert zu lassen oder zu löschen und neu zu erstellen.

- **Auto-Heal Broken Hosts**: Schalten Sie diese Option auf **Aktiviert**, um Auto-Heal zu aktivieren.
- **AVD-Agentenstatus**: Wählen Sie aus den Dropdown-Listen die gewünschten Status sowie den Sitzungsstatus aus.

> **Anmerkung**
>
> Der Status wird dem AVD-Dienst von dem auf der Sitzungshost-VM installierten AVD-Agenten gemeldet. Wenn etwas nicht stimmt, lautet der Status nicht „Verfügbar“. Allerdings bedeutet das im Umkehrschluss nicht unbedingt, dass ein Problem vorliegt. Weitere Details finden Sie in diesem Microsoft-Artikel. Hosts mit aktiven Sitzungen sind u. U. noch teilweise funktionsfähig und werden nicht als defekt behandelt. Nur Hosts, die entweder gar keine Sitzungen oder keine aktiven Sitzungen (d. h. nur getrennte Sitzungen) aufweisen, werden von Autoscaling als defekt eingestuft.

- **Timeout der ersten Aktion**: Geben Sie die Anzahl der Minuten ein, die gewartet werden soll, bevor die erste Aktion ausgeführt wird.

- **Wiederherstellungsmaßnahmen**: Wählen Sie aus der Dropdown-Liste die Wiederherstellungsmaßnahme(n) aus.

  > **Anmerkung**
  > - Sie können eine VM-Aktion (z. B. VM neu starten oder VM entfernen) oder eine skriptbasierte Aktion (z. B. SxS neu installieren, Host erneut bei AVD registrieren usw.) auswählen.
  > - Die Wiederherstellungsmaßnahmen werden in der angezeigten Reihenfolge ausgeführt. Sie können eine beliebige Aktion per Drag-and-Drop verschieben, um deren Position in der Liste und damit die Ausführungsreihenfolge zu ändern.

- **Timeout zwischen Wiederherstellungsaktionen**: Geben Sie die Anzahl der Minuten ein, die nach jedem Neustartversuch gewartet werden soll, bevor mit dem nächsten Schritt fortgefahren wird (zum Beispiel VM neu starten, dann VM entfernen, dann usw.).

  > **Anmerkung**
  >
  > Wenn der Auto-Heal-Vorgang das Löschen und Neuerstellen einer defekten Host-VM erfordert, wird eine Ersatz-VM eingeschaltet, um die Kapazität zu ersetzen, sofern verfügbar.

11. Schalten Sie die Option **Auto-scale** auf **Aktiviert**. Der Umschalter befindet sich unten im Dialogfeld.
12. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern**.

Verwandte Themen:

- Dynamische Hostpools erstellen [78]
- Auto-scale für persönliche Hostpools aktivieren [110]

Automatische Skalierung für persönliche Hostpools aktivieren

Nerdio Manager ermöglicht es Ihnen, eine automatische Skalierung für persönliche Hostpools durchzuführen. Dies ermöglicht Ihnen Folgendes:

- Persönliche Desktops können basierend auf einem Zeitplan automatisch ein- und ausgeschaltet werden. Alternativ können persönliche Desktops beendet werden, wenn keine aktiven oder getrennten Sitzungen vorhanden sind.
- Der Typ des Host-Betriebssystemdatenträgers kann in einen kostengünstigeren Speichertyp geändert werden, wenn der persönliche Desktop nicht ausgeführt wird.
- Auto-Heal versucht automatisch, „defekte“ Sitzungshosts zu reparieren. Darüber hinaus ermöglicht sie die Ausführung von Scripted Actions, wie z. B. eine SxS-Neuinstallation oder eine AVD-Host-Neuregistrierung, für diese.

So konfigurieren Sie die grundlegenden Autoscaling-Informationen:

1. Finden Sie den persönlichen Hostpool, mit dem Sie arbeiten möchten.
2. Fahren Sie im Menü ⋮ mit der Maus über **Autoscaling** und wählen Sie **konfigurieren**.
3. Schalten Sie unten auf der Seite **Autoscaling** auf **Enabled**.
4. Geben Sie die folgenden grundlegenden Autoscaling-Informationen ein:
   - **Autoscaling-Zeitzone**: Wählen Sie aus der Dropdownliste die Zeitzone für den Autoscaling-Prozess aus.
   - **Name**: Geben Sie den Namen der neu erstellten Hosts für das Präfix oder das Präfix+Muster ein.
     - **Präfix/Muster**: Wählen Sie aus der Dropdownliste aus, ob ein Präfix oder ein Muster verwendet werden soll.

> **Anmerkung**
>
> - **Präfix** kann beim Erstellen mehrerer Sitzungshosts verwendet werden. Das Präfix ist auf 10 gültige Zeichen für Windows-Computernamen begrenzt. Bei Verwendung eines Präfixes wird automatisch ein eindeutiges Suffix im Format „-xxxx“ angehängt, wobei xxxx für 4 zufällige alphanumerische Zeichen steht. Zum Beispiel: AVDHOST-s72h. Fügen Sie dem Präfix kein „-“ hinzu.
> - **Muster** kann verwendet werden, um eine erweiterte Namenskonvention für neue Hosts zu erstellen. Musterzeichen müssen in {} eingeschlossen werden und können # (für fortlaufende Nummern) und/oder ? (für zufällige alphanumerische Zeichen) sein. Ein # steht für Zahlen von 0 bis 9, zwei # stehen für Zahlen von 0 bis 99 usw.
>   - Beispiel 1: AVDHOST{###} (AVDHOST000..AVDHOST999).
>   - Beispiel 2: AVDHOST-{???} (AVDHOST-d83, AVDHOST-7sl, etc.).

- **Netzwerk**: Wählen Sie aus der Dropdown-Liste das Netzwerk aus, mit dem die VM verbunden werden soll.

> **Anmerkung**
>
> Die VM, die im ausgewählten Netzwerk erstellt wird, wird in der dem Netzwerk zugeordneten Azure-Region erstellt.

- **Zusätzliche Subnetze**: Wählen Sie aus der Dropdown-Liste ein zusätzliches Subnetz aus demselben virtuellen Netzwerk aus.

> **Anmerkung**
>
> Wenn beim horizontalen Hochskalieren ein bestimmtes Subnetz nicht über genügend IP-Adressen verfügt, wird beim Erstellen zusätzlicher Sitzungshosts automatisch das nächste Subnetz ausgewählt.

- **Netzwerkverteilung**: Wählen Sie aus der Dropdown-Liste aus, wie die Netzwerklast verteilt werden soll. Wählen Sie entweder **Tiefensuche** oder **Breitensuche**.

> **Anmerkung**
>
> Wählen Sie **Tiefensuche**, um die Netzwerklast nacheinander in einer festen Reihenfolge auf Knotenpunkten zu verteilen, oder wählen Sie **Breitensuche**, um die Netzwerklast proportional basierend auf der aktuellen Ressourcennutzung auszugleichen.

- **Desktop-Image (Vorlage)**: Wählen Sie aus der Dropdown-Liste ein Desktop-Image aus, das als Golden Image für neue Sitzungshosts verwendet werden soll.
- **VM-Größe (Vorlage)**: Wählen Sie aus der Dropdownliste die VM-Größe für neue Sitzungshosts aus.
- **Betriebssystemdatenträger (Vorlage)**: Wählen Sie aus der Dropdownliste den Typ und die Größe des Betriebssystemdatenträgers für neue Sitzungshosts aus.
- **Typ des Betriebssystemdatenträgers bei Beendigung**: Wählen Sie aus der Dropdownliste den Typ des Betriebssystemdatenträgers aus, wenn Sitzungshost-VMs beendet sind.
- **Ressourcengruppe**: Wählen Sie aus der Dropdownliste die Ressourcengruppe aus, in der VMs erstellt werden sollen.
- **VM-Benennung**: Wählen Sie aus der Dropdownliste die zu verwendende VM-Benennung aus.

> **Anmerkung**
>
> Host-VMs, die automatisch durch horizontales Hochskalieren oder den Auto-Grow-Prozess erstellt werden, verwenden Namen, die auf dem ausgewählten VM-Namensmodus basieren. Weitere Informationen finden Sie unter Wie Sitzungshost-VM-Namen generiert werden.
>
> - **Namen wiederverwenden**: Versuchen Sie immer, Namen wiederzuverwenden, die zuvor im Pool verwendet wurden, sofern verfügbar.
> - **Standardnamen**: Verwenden Sie den nächsten verfügbaren Namen.
> - **Eindeutige Namen**: Versuchen Sie immer, einen eindeutigen Namen für neue Hosts zu verwenden.

5. Wählen Sie **Standardplan** oder **alternativer Zeitplan**.

> **Anmerkung**
>
> Nerdio Manager ermöglicht es Ihnen, separate Autoscaling-Einstellungen für einen Standardplan (normaler Betrieb) und einen alternativen Zeitplan (außerhalb des normalen Betriebs) zu konfigurieren. Sie möchten beispielsweise möglicherweise an Wochenenden oder Feiertagen weniger Sitzungshosts zur Verfügung haben. Alternativ benötigen Sie möglicherweise zwei Wochen vor einem Feiertag mehr verfügbare Sitzungshosts, wenn Sie eine große Anzahl von Usern haben. In beiden Fällen würden Sie den Bereich **Alternativer Zeitplan** verwenden, um die Autoscaling-Einstellungen für Zeiträume außerhalb des normalen Betriebs zu konfigurieren.

- Um einen alternativen Zeitplan zu erstellen, wählen Sie den Bereich **Alternativer Zeitplan** und geben Sie die folgenden Informationen ein:
  - **Zeitplan**: Wählen Sie den Umschalter, um den alternativen Zeitplan zu aktivieren.
  - **Tage**: Wählen Sie aus der Dropdownliste die Tage mit geringer Auslastung aus.

- **Daten**: Wählen Sie das Datumsfeld und wählen Sie das Datum aus dem angezeigten Kalender aus.
- Wählen Sie das Plus-Symbol ⊕, um ein weiteres Datum hinzuzufügen, oder wählen Sie das Minus-Symbol ⊖, um Daten zu entfernen.

> **Anmerkung**
>
> Tage und Datumsangaben werden kombiniert und nicht als Alternativen behandelt. Wenn Sie beides auswählen, gilt der alternative Zeitplan nur an den ausgewählten Wochentagen innerhalb der ausgewählten Datumsangaben. Es gilt nicht einmalig für den gesamten Datumsbereich. Beispiel:
>
> - Um den alternativen Zeitplan nur während der Feiertage anzuwenden, wählen Sie die Datumsangaben für diesen Zeitraum aus (zum Beispiel 24. bis 27. Dezember) und lassen Sie **Tage** leer.
> - Um ihn auf jedes Wochenende anzuwenden, wählen Sie Samstag und Sonntag aus und lassen Sie **Datumsangaben** leer.
> - Um ihn nur an den Wochenenden innerhalb eines Teils des Monats anzuwenden, wählen Sie Samstag und Sonntag sowie die Datumsangaben aus (zum Beispiel 10. bis 24. Dezember). Der Zeitplan gilt dann für die Samstage und Sonntage zwischen dem 10. und 24. Dezember.

6. **Autoscaling-Modus**: Wählen Sie aus der Dropdownliste den gewünschten Autoscaling-Modus aus.

> **Anmerkung**
>
> - **Benutzergesteuert**: Die automatische Skalierung wird durchgeführt, wenn keine aktiven oder getrennten Sitzungen vorhanden sind.
> - **Zeitplanbasiert**: Die automatische Skalierung wird gemäß dem festgelegten Zeitplan durchgeführt.

7. **Autoscaling-Profil**: Wählen Sie optional aus der Dropdownliste das zu verwendende Autoscaling-Profil aus. Wählen Sie alternativ **Benutzerdefiniert**, um eine benutzerdefinierte Autoscaling-Konfiguration zu erstellen.

   > **Anmerkung**
   >
   > Weitere Informationen zum Erstellen und Verwenden von Auto-scale-Profilen finden Sie unter Auto-scale-Profile verwalten [87].

8. Setzen Sie den Konfigurationsprozess mit dem entsprechenden Autoscaling-Modus fort:
   - **Benutzergesteuert**: Zum Aktivieren der benutzergesteuerten Autoscaling für persönliche Hostpools. [115]
   - **Zeitplanbasiert**: Zum Aktivieren der zeitplanbasierten Autoscaling für persönliche Hostpools. [124]

Zum Aktivieren der benutzergesteuerten Autoscaling für persönliche Hostpools:

1. **Autoscaling-Modus**: Wählen Sie aus der Dropdown-Liste **Benutzergesteuert** aus.
2. Geben Sie die folgenden Informationen zu **Hostpool-Eigenschaften** ein:
   - **VM beim Verbinden starten**: Wählen Sie diese Option, um den Desktop bei Verbindungsaufbau zu starten.
3. Geben Sie die folgenden Informationen zu **Desktop-Start und -Stopp** ein:
   - **Desktop-Start und -Stopp**: Aktivieren Sie diese Option, um den Desktop-Start und -Stopp zu ermöglichen.
   - **Desktops werden gestoppt nach**: Wählen Sie aus der Dropdown-Liste die Anzahl der Minuten oder Stunden aus, nach denen horizontal herunterskaliert wird, nachdem sich alle User abgemeldet haben.

> **Anmerkung**
>
> - Desktops werden automatisch gestartet, wenn Benutzer eine Verbindung herstellen.
> - Desktops werden nur dann automatisch gestoppt, wenn keine aktiven oder getrennten Sitzungen vorhanden sind. Um getrennte User nach einer bestimmten Zeit automatisch abzumelden, verwenden Sie die Einstellungen für Sitzungslimits in den Hostpool-Eigenschaften.

- **Drain-Modus für Desktops in diesem Pool umgehen**: Wählen Sie diese Option, damit Desktops vor dem Herunterfahren nicht in den Drain-Modus wechseln.

4. Geben Sie die folgenden Informationen zu **Pre-stage hosts** ein:
   - **Pre-stage hosts**: Aktivieren Sie diese Option, um Pre-stage hosts zu aktivieren.

> **Anmerkung**
>
> Wenn „Pre-stage hosts“ aktiviert ist, hat dies Vorrang vor anderen User-gesteuerten Konfigurationen. Gestoppte Hosts werden gestartet, Hosts im Drain-Modus werden aktiviert, gestoppte Datenträgertypen werden auf „running“ umgestellt und Hosts werden nicht gestoppt oder deaktiviert, selbst wenn keine User-Sitzungen vorhanden sind.

   - Aktivieren Sie das Kontrollkästchen, um Hosts ohne zugewiesene User einzubeziehen.
   - **Arbeitstage**: Wählen Sie aus der Dropdown-Liste die Arbeitstage aus, an denen sich eine große Anzahl von Usern gleichzeitig bei ihren virtuellen Desktops oder Anwendungen anmeldet.
   - **Beginn der Arbeitszeit**: Wählen Sie die Uhrzeit am Morgen aus, zu der sich User bei ihren virtuellen Desktops oder Anwendungen anmelden.
   - **Verzögerung für horizontal herunterskalieren**: Wählen Sie eine Verzögerung, um horizontales Herunterskalieren nach Beginn der Arbeitszeit einzuschränken.

- > **Anmerkung**
  >
  > Pre-stage Hosts werden während dieser Zeit nicht horizontal herunterskaliert, selbst wenn sie nicht verwendet werden.

5. Geben Sie die folgenden Informationen zu **Pre-stage Host OS Disks** ein:

   > **Anmerkung**
   >
   > Weitere Details und Beispiele zum intelligenten Pre-Staging von Disks finden Sie unter Intelligentes Pre-Staging von Disks für persönliche Hostpools

   - **Pre-stage host OS Disks**: Aktivieren Sie diese Option, um Pre-stage Host OS Disks zu aktivieren.
   - Wählen Sie aus den Dropdown-Listen die **Tage** und **Zeiten** aus, zu denen die Host OS Disks der Sitzungshost-VMs per Pre-stage bereitgestellt werden sollen.
   - **Lassen Sie Desktops, die keinem User zugewiesen sind, mit dem OS-Disk-Typ STOPPED**: Wählen Sie diese Option, damit Desktop-VMs, die keinem User zugewiesen sind, der OS-Disk nicht von STOPPED auf RUNNING umgestellt wird.
   - **Intelligentes Disk-Pre-Staging für User verwenden**: Wählen Sie diese Option, damit intelligentes Disk-Pre-Staging das User-Verhalten lernt und die Zeiten für das Disk-Pre-Staging automatisch anpasst.

     > **Anmerkung**
     >
     > Diese Funktion erfordert, dass AVD Insights für den Hostpool aktiviert und konfiguriert ist.

     - **Modus**: Wenn **Intelligentes Disk-Pre-Staging für User verwenden** ausgewählt ist, wählen Sie den Modus aus der Dropdown-Liste **Modus** aus.

Anmerkung

- **Hybrid Modus**: Disks werden immer basierend auf dem definierten Zeitplan vorab bereitgestellt. Das Verhalten von Usern, deren Arbeitsmuster erlernt werden, und zusätzliche Pre-stage-Aktivitäten werden geplant. Diese Funktion ist als „Lernmodus“ konzipiert und bietet die Vorteile sowohl der Standard Pre-stage-Funktion als auch der erlernten Anforderungen.
- **Automatisierter Modus**: Disks werden für bestehende User nur gemäß dem erlernten Zeitplan als Pre-stage bereitgestellt. Neue User berücksichtigen den definierten Zeitplan, bis das intelligente Pre-stage über genügend Daten verfügt, um diesen Prozess zu automatisieren. Disks werden 30 Minuten vor erwarteten User-Logon-Ereignissen als Pre-stage bereitgestellt.

6. Geben Sie die folgenden **Auto-Grow** Informationen ein:

Anmerkung

Desktops automatisch zum Hostpool hinzufügen, wenn die Anzahl der verbleibenden nicht zugewiesenen Desktops unter einen festgelegten Schwellenwert fällt.

- **Auto-Grow**: Aktivieren Sie diese Option, um Auto-Grow zu aktivieren.
- **Einen neuen Host hinzufügen, wenn die Anzahl der verfügbaren (nicht einem User zugewiesenen) Hosts unter folgenden Wert fällt**: Geben Sie den Schwellenwert ein und wählen Sie aus der Dropdown-Liste aus, ob der Schwellenwert eine Anzahl von Desktops oder ein Prozentsatz der gesamten Desktops ist.

7. Geben Sie die folgenden **Auto-Shrink** Informationen ein:

Anmerkung

Das System entfernt automatisch Desktops, die längere Zeit nicht verwendet wurden.

- **Auto-Shrink**: Aktivieren Sie diese Option, um Auto-Shrink zu aktivieren.
- **Delete VM if the User hasn't logged in for**: Geben Sie die Anzahl der Tage ein, die gewartet werden soll, bevor das System die VM automatisch löscht.

> **Anmerkung**
>
> Die Aktivität von Usern auf dieser Sitzungshost-VM wird basierend auf Nerdio Manager dem Verlauf der automatischen Skalierung und den AVD-Diagnosedaten bestimmt. Jedes Mal, wenn der Desktop durch die automatische Skalierung verarbeitet wird, wird ein Azure-Tag mit Datum und Uhrzeit der letzten Verwendung des Desktops gesetzt. Wenn der Desktop die hier angegebene Anzahl an Tagen nicht verwendet wird, wird die Sitzungshost-VM beendet und mit einem „Wird demnächst gelöscht"-Tag versehen.

- **Der Desktop wechselt in den Status „Wird demnächst gelöscht" und wird anschließend gelöscht nach**: Wählen Sie aus der Dropdown-Liste die Zeitdauer aus, bevor ein Desktop gelöscht wird.

> **Anmerkung**
>
> Der Desktop wird durch den automatischen Skalierungsprozess auf den Status „Wird demnächst gelöscht" gesetzt. Dazu wird die VM mit einem Tag versehen. Dabei wird eine Aufgabe protokolliert, die auch als Benachrichtigung an den Administrator verwendet werden kann, wenn ein Desktop in den Status „Wird demnächst gelöscht" wechselt. In der Nerdio Manager Benutzeroberfläche werden auch Benachrichtigungsbanner angezeigt, die darauf hinweisen, dass ein persönlicher Hostpool VMs enthält, die demnächst gelöscht werden. Nach Ablauf der Löschfrist (Standardwert: 24 Stunden) wird die VM dauerhaft gelöscht.

- **Folgende Gruppen (oder einzelne User) ausschließen**: Aktivieren Sie diese Option und wählen Sie dann die Gruppe(n) oder den/die einzelnen User aus, die von der automatischen Verkleinerung ausgeschlossen werden sollen.

> **Anmerkung**
>
> Desktops, die den hier aufgeführten Usern zugewiesen sind, werden **nicht** automatisch entfernt, auch nicht nach längerer Inaktivität.

- **Nicht zugewiesene Desktops bei Auto-Shrink ausschließen**: Wählen Sie diese Option, um Desktops, die keinem User zugewiesen wurden, von Auto-Shrink-Vorgängen auszuschließen.

> **Anmerkung**
>
> Verwenden Sie diese Einstellung in Kombination mit Auto-Grow, um einen Puffer freier, nicht zugewiesener Desktops zu warten.

- **Scripted Actions bei geplanter Host-Verkleinerung**: Wählen Sie aus der Dropdown-Liste die Scripted Actions aus, die ausgeführt werden sollen, nachdem die VM für Auto-Shrink markiert wurde.
- **User über geplante Löschung benachrichtigen**: Wählen Sie diese Option, um den User per E-Mail über die Löschung seines Desktops zu benachrichtigen, wenn der Zeitraum der Inaktivität überschritten wurde.

> **Anmerkung**
>
> Benachrichtigungen auf der Seite **System** > **Einstellungen** > **Nerdio** müssen aktiviert sein, damit diese Funktion funktioniert.

  - **Nachrichtenbetreff**: Erweitern Sie diese Option, um die Betreffzeile der Auto-Shrink-Nachricht einzugeben.
  - **Nachrichtentext**: Erweitern Sie diese Option, um den Editor zum Erstellen einer benutzerdefinierten Auto-Shrink-Nachricht für User zu öffnen.

Anmerkung

Die folgenden Variablen stehen für die Verwendung im Nachrichtentext zur Verfügung:

- **%HOSTPOOL%**: Gibt den Namen des betroffenen Hostpools zurück.
- **%HOSTNAME%**: Gibt den spezifischen Hostnamen zurück.
- **%HOST_IDLE_DAYS_THRESHOLD%**: Gibt den konfigurierten Maximalwert der Leerlauftage zurück, bevor Auto-Shrink gestartet wird.
- **%SHRINK_TIME_UTC%**: Gibt die genaue Uhrzeit in UTC zurück, zu der die Auto-Shrink-Aufgabe stattfinden soll.
- **%SHRINK_DATE%**: Gibt das genaue Datum zurück, an dem die Auto-Shrink-Aufgabe stattfinden soll.
- **%SHRINK_DATE_EUR%**: Gibt das genaue Datum zurück, an dem die Auto-Shrink-Aufgabe im Format TT/MM/JJJJ (europäisch) stattfinden soll.
- **%IMAGE_NAME%**: Gibt den Image-Namen der VM zurück.
- **%FRIENDLY_WORKSPACE_NAME%**: Gibt den Anzeigenamen des Workspace zurück.
- **%FRIENDLY_HOSTPOOL_NAME%**: Gibt den Anzeigenamen des Hostpools zurück.
- **%VM_SIZE%**: Gibt die Größe der VM zurück.
- **%DISK_SKU%**: Gibt die Disk-SKU der VM zurück.
- **%USER_NAME%**: Gibt den Namen des Users zurück, der bei der VM angemeldet ist.

- **Zusätzlichen E-Mail-Empfänger benachrichtigen, wenn Desktops zur Löschung geplant sind**: Wählen Sie diese Option, um einen zusätzlichen E-Mail-Empfänger zu benachrichtigen, wenn Desktops zur Löschung geplant sind.
  - **Benachrichtigungs-E-Mails senden an**: Geben Sie die E-Mail-Adresse des zusätzlichen Empfängers ein.

- **Benachrichtigungs-E-Mails senden von**: Geben Sie die E-Mail-Adresse des Absenders ein.
- **Häufigkeit der Benachrichtigungen**: Wählen Sie aus der Dropdown-Liste aus, wie häufig die E-Mail-Erinnerungen an den User gesendet werden sollen.

> **Anmerkung**
>
> Einen Tag vor der planmäßigen Löschung wird immer eine finale E-Mail verschickt.

8. Geben Sie die folgenden **Auto-Heal defekter Hosts** Informationen ein:

> **Anmerkung**
>
> Sitzungshosts können aufgrund von Problemen mit dem Domänenvertrauen oder der FSLogix-Konfiguration beeinträchtigt werden. Der AVD-Agent meldet den Status solcher Hosts als nicht verfügbar. Admins müssen solche Hosts dann manuell aus dem Pool entfernen. Nerdio Manager ermöglicht es Ihnen jedoch, eine Reihe von Aktionen zu konfigurieren, um diese Sitzungshosts während des Autoscaling-Prozesses zu reparieren. Das Autoscaling kann versuchen, „defekte“ Sitzungshosts automatisch durch Neustarten und Löschen/Neuerstellen zu reparieren. Es können einige Versuche unternommen werden, den Host neu zu starten, um ihn wieder in einen betriebsbereiten Zustand zu versetzen, und ihn anschließend entweder in Ruhe zu lassen oder den Host zu löschen und neu zu erstellen.

- **Auto-Heal defekter Hosts**: Aktivieren Sie diese Option, um Auto-Heal zu ermöglichen.
  - Geben Sie im Feld **Anzeichen eines defekten Hosts** die folgenden Informationen ein:
  - **AVD-Agentenstatus**: Wählen Sie aus der Dropdown-Liste den AVD-Agentenstatus und anschließend aus der Dropdown-Liste darunter den Sitzungsstatus aus.

> **Anmerkung**
>
> Der Status wird dem AVD-Dienst von dem auf der Sitzungshost-VM installierten AVD-Agenten gemeldet. Wenn etwas nicht stimmt, lautet der Status anders als „Verfügbar“. Nicht jeder Status außer „Verfügbar“ bedeutet, dass ein Problem vorliegt. Weitere Details finden Sie in diesem Microsoft-Artikel. Hosts mit aktiven Sitzungen sind u. U. noch teilweise funktionsfähig und solche Hosts werden nicht als defekt behandelt. Nur Hosts, die entweder überhaupt keine Sitzungen oder keine aktiven Sitzungen (d. h. nur getrennte Sitzungen) aufweisen, werden vom Autoscaling als defekt eingestuft.

- **Erste Aktion**: Geben Sie die Anzahl der Minuten ein, die gewartet werden soll, bevor die erste Aktion ausgeführt wird.
- **Wiederherstellungsmaßnahmen**: Wählen Sie aus der Dropdown-Liste die Wiederherstellungsmaßnahme(n) aus.

> **Anmerkung**
>
> - Sie können eine VM-Aktion (z. B. VM neu starten oder VM entfernen) oder eine Scripted Action (z. B. SxS neu installieren, Host erneut bei AVD registrieren usw.) auswählen.
> - Die Wiederherstellungsaktionen werden in der angezeigten Reihenfolge ausgeführt. Sie können eine beliebige Aktion per Drag & Drop verschieben, um deren Position in der Liste und damit die Reihenfolge der Ausführung zu ändern.

- **Zeitüberschreitung zwischen Wiederherstellungsaktionen**: Geben Sie die Anzahl der Minuten ein, die nach jedem Wiederherstellungsschritt gewartet werden soll, bevor mit dem nächsten Schritt fortgefahren wird (zum Beispiel VM neu starten, dann VM entfernen, dann etc.).

> **Anmerkung**
>
> Wenn der Auto-Heal-Vorgang das Löschen und Neuerstellen einer defekten Host-VM erfordert, wird eine Ersatz-VM eingeschaltet, um die Kapazität zu ersetzen, sofern verfügbar.

- Um ein weiteres Anzeichen eines defekten Hosts hinzuzufügen, wählen Sie das Plus-⊕-Symbol.

9. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern**.

So aktivieren Sie das zeitplanbasierte Autoscaling für den persönlichen Hostpool:

1. Wählen Sie aus der Dropdownliste **Autoscaling-Modus** die Option **Zeitplanbasiert** aus.
2. Wählen Sie aus der Dropdownliste **Autoscaling-Profil** das Autoscaling-Profil aus.
3. Geben Sie die folgenden **Hostpool-Eigenschaften** Informationen ein:
   - **VM beim Verbindung herstellen starten**: Wählen Sie diese Option, um den Desktop beim Herstellen der Verbindung zu starten.
4. Geben Sie die folgenden Informationen zu den **Arbeitszeiten** ein:
   - Wählen Sie aus den Dropdownlisten die **Arbeitstage** und **Arbeitszeiten** aus, zu denen die Betriebssystem-Disks der Sitzungshost-VMs Pre-Staging durchlaufen sollen.
   - **Aggressivität beim Ausschalten**: Wählen Sie aus der Dropdownliste die Aggressivität beim Ausschalten aus. (Nur zeitplanbasiert)

> **Anmerkung**
>
> - **Hoch**: Schalten Sie alle Sitzungshost-VMs aus, einschließlich derer mit aktiven und getrennten Sitzungen. Usern mit aktiven Sitzungen wird eine unten definierte Nachricht gesendet, und sie erhalten Zeit, sich abzumelden, bevor ihre Sitzungshost-VM ausgeschaltet wird.
> - **Mittel**: Schalten Sie nur die Sitzungshost-VMs aus, die keine aktive User-Sitzung haben, einschließlich derer mit getrennten Sitzungen.
> - **Niedrig**: Schalten Sie nur die Sitzungshost-VMs aus, die keine aktiven oder getrennten Sitzungen haben.

- **Einschaltzeitpunkt**: Wählen Sie aus der Dropdown-Liste den Einschaltzeitpunkt aus. (Nur zeitplanbasiert)

> **Anmerkung**
>
> - **Nie**: Schalten Sie Sitzungshost-VMs nicht zu Beginn der oben definierten Arbeitszeiten ein. User müssen ihre Sitzungshost-VMs manuell einschalten.
> - **Einmal**: Alle Sitzungshost-VMs werden nur einmal zu Beginn der Arbeitszeiten eingeschaltet. Wenn eine Sitzungshost-VM nach Beginn der Arbeitszeiten ausgeschaltet wird, wird sie nicht automatisch durch Autoscaling wieder eingeschaltet.
> - **Kontinuierlich**: Alle Sitzungshost-VMs werden zu Beginn der Arbeitszeiten eingeschaltet. Zusätzlich schaltet Auto-Scale während der Arbeitszeiten automatisch alle Sitzungshost-VMs ein, die manuell ausgeschaltet wurden.

- **Ausschaltzeitpunkt**: Wählen Sie aus der Dropdown-Liste den Ausschaltzeitpunkt aus.

> **Anmerkung**
>
> - **Nie**: Schalten Sie Sitzungshost-VMs nicht am Ende der oben definierten Arbeitszeiten aus.
> - **Einmal**: Am Ende der Arbeitszeiten werden alle Sitzungshost-VMs ausgeschaltet, abhängig von der oben definierten Aggressivität. Wenn Sitzungshost-VMs außerhalb der Arbeitszeiten manuell eingeschaltet werden, schaltet Autoscaling sie nicht automatisch aus.
> - **Kontinuierlich**: Am Ende der Arbeitszeiten werden alle Sitzungshost-VMs ausgeschaltet, abhängig von der oben definierten Aggressivität. Wenn Sitzungshost-VMs außerhalb der Arbeitszeiten manuell eingeschaltet werden, schaltet Autoscaling sie unter Berücksichtigung der oben definierten Aggressivität automatisch aus.

- **Hosts ohne zugewiesenen User einbeziehen**: Wählen Sie diese Option, um während des automatischen Skalierungsprozesses auch nicht zugewiesene Desktops zu starten.

> **Anmerkung**
>
> Dies kann für Organisationen nützlich sein, die während des Arbeitstages geplante Aufgaben auf Desktops ausführen möchten.

5. Geben Sie die folgenden Informationen zu **Host-OS-Disks** ein:
   - **Alle Hosts während der Arbeitszeiten auf den Betriebssystem-Disktyp „Ausgeführt“ setzen**: Wählen Sie diese Option, um alle angehaltenen Host-VM-Betriebssystem-Disks während der oben definierten Arbeitszeiten in den Disktyp „Ausgeführt“ zu konvertieren.

> **Anmerkung**
>
> Dies ist erforderlich, um sicherzustellen, dass eine VM, die über „Azure Start VM on Connect“ gestartet wird, über den korrekten Hochleistungs-Disktyp verfügt. Wenn diese Einstellung aktiviert ist, werden alle Warnungen vom Typ „Disktyp entspricht nicht der Richtlinie“ für diesen Pool ausgeblendet.

- **Intelligentes Disk-Pre-Staging für User verwenden**: Wählen Sie diese Option, damit das intelligente Disk-Pre-Staging das User-Verhalten lernt und die Zeiten für das Disk-Pre-Staging automatisch anpasst.

> **Anmerkung**
>
> Diese Funktion erfordert, dass AVD Insights für den Hostpool aktiviert und konfiguriert sind.

  - **Modus**: Wenn Sie die Option **Intelligentes Desktop-Pre-Staging für User verwenden** ausgewählt haben, wählen Sie den Modus aus der Dropdown-Liste aus.

Anmerkung

- **Hybrid**: Disks werden immer basierend auf dem festgelegten Zeitplan im Pre-Staging vorbereitet. Das Verhalten von Usern, deren Arbeitsmuster erlernt werden, sowie zusätzliche Pre-Staging-Aktivitäten werden geplant. Diese Funktion ist als „Lernmodus“ konzipiert und bietet die Vorteile sowohl der Standard-Pre-Staging-Funktionalität als auch der erlernten Anforderungen.
- **Automatisierter Modus**: Disks werden für vorhandene User nur gemäß dem erlernten Zeitplan im Pre-Staging vorbereitet. Neue User halten sich an den definierten Zeitplan, bis das intelligente Pre-Staging über genügend Daten verfügt, um diesen Prozess zu automatisieren. Disks werden 30 Minuten vor erwarteten User-Anmeldeereignissen im Pre-Staging vorbereitet.

6. Geben Sie die folgenden **Auto-grow** Informationen ein:

Anmerkung

Fügen Sie dem Hostpool automatisch Desktops hinzu, wenn die Anzahl der verbleibenden nicht zugewiesenen Desktops unter einen festgelegten Schwellenwert fällt.

- **Auto-grow**: Aktivieren Sie diese Option, um Auto-grow zu aktivieren.
- **Einen neuen Host hinzufügen, wenn die Anzahl der verfügbaren (nicht einem User zugewiesenen) Desktops unter folgenden Wert fällt**: Geben Sie den Schwellenwert ein und wählen Sie aus der Dropdown-Liste aus, ob es sich bei dem Schwellenwert um eine Anzahl von Desktops oder einen Prozentsatz der Gesamtzahl der Desktops handelt.

7. Geben Sie die folgenden **Auto-Shrink** Informationen ein:

> **Anmerkung**
>
> Das System entfernt Desktops, die längere Zeit nicht verwendet wurden, automatisch.

- **Auto-Shrink**: Aktivieren Sie diese Option, um Auto-Shrink zu aktivieren.
- **VM löschen, wenn sich der User nicht angemeldet hat für**: Geben Sie die Anzahl der Tage ein, die gewartet werden soll, bevor das System die VM automatisch löscht.

  > **Anmerkung**
  >
  > Die User-Aktivität auf dieser Sitzungshost-VM wird basierend auf dem Nerdio Manager Auto-Scale-Verlauf und den AVD-Diagnose-Daten bestimmt. Jedes Mal, wenn der Desktop durch Auto-Scale verarbeitet wird, wird ein Azure-Tag mit Datum/Uhrzeit der letzten Verwendung des Desktops gesetzt. Wenn der Desktop die hier angegebene Anzahl an Tagen nicht verwendet wird, wird die Sitzungshost-VM ausgeschaltet und ein "ausstehend löschen"-Tag gesetzt.

- **Der Desktop wechselt in den Status „ausstehend löschen“ und wird anschließend gelöscht nach**: Wählen Sie aus der Dropdown-Liste die Dauer für „ausstehend löschen“ aus.

> **Anmerkung**
>
> Der Desktop wird durch den Auto-Scale-Prozess in den Status „ausstehend löschen“ versetzt, indem der VM ein Tag hinzugefügt wird. Dabei wird eine Aufgabe protokolliert, die als Benachrichtigung an den Administrator verwendet werden kann, wenn ein Desktop in den Status „ausstehend löschen“ wechselt. In der Nerdio Manager-Benutzeroberfläche werden auch Banner angezeigt, die darauf hinweisen, dass ein persönlicher Hostpool VMs enthält, die als ausstehend löschen markiert sind. Nach Ablauf der ausstehend löschen-Periode (Standard: 24 Stunden) wird die VM dauerhaft gelöscht.

- **Folgende Gruppen (oder einzelne User) ausschließen**: Aktivieren Sie diese Option und wählen Sie dann die Gruppe(n) oder den/die einzelnen User aus, die von der automatischen Verkleinerung ausgeschlossen werden sollen.

  > **Anmerkung**
  >
  > Desktops, die den hier aufgeführten Usern zugewiesen sind, werden **nicht** automatisch entfernt, auch nicht nach längerer Inaktivität.

- **User benachrichtigen, wenn ihr Desktop demnächst gelöscht wird**: Wählen Sie diese Option, um den User per E-Mail über die Löschung seines Desktops zu benachrichtigen, wenn der Zeitraum der Inaktivität überschritten wurde.

  > **Anmerkung**
  >
  > Benachrichtigungen auf der Seite **System** > **Einstellungen** > **Nerdio** müssen aktiviert sein, damit diese Funktion funktioniert.

  - **Nachrichtenbetreff**: Erweitern Sie diese Option, um die Betreffzeile der Auto-Shrink-Nachricht einzugeben.

- **Nachrichtentext**: Erweitern Sie diese Option, um den Editor zum Erstellen einer benutzerdefinierten Auto-Shrink-Nachricht für User zu öffnen.

  > **Anmerkung**
  >
  > Die folgenden Variablen stehen für die Verwendung im Nachrichtentext zur Verfügung:
  >
  > - **%HOSTPOOL%**: Gibt den Namen des betroffenen Hostpools zurück.
  > - **%HOSTNAME%**: Gibt den spezifischen Hostnamen zurück.
  > - **%HOST_IDLE_DAYS_THRESHOLD%**: Gibt den konfigurierten Maximalwert an Leerlauftagen zurück, bevor Auto-Shrink gestartet wird.
  > - **%SHRINK_TIME_UTC%**: Gibt die genaue Uhrzeit in UTC zurück, zu der die Auto-Shrink-Aufgabe stattfinden soll.
  > - **%SHRINK_DATE%**: Gibt das genaue Datum zurück, an dem die Auto-Shrink-Aufgabe stattfinden soll.

- **Zusätzlichen E-Mail-Empfänger benachrichtigen, wenn Desktops zur Löschung geplant sind**: Wählen Sie diese Option, um weitere User über die Auto-Shrink-Aktivität zu benachrichtigen.
  - **Benachrichtigungs-E-Mails senden an**: Geben Sie die zusätzlichen E-Mail-Adressen ein.
- **Benachrichtigungs-E-Mails senden von**: Wählen Sie aus der Dropdown-Liste die „Absender"-E-Mail-Adresse aus.

8. Geben Sie die folgenden **Messaging**-Informationen ein:

> **Anmerkung**
>
> Das System sendet Nachrichten an alle User, die mit einem Sitzungshost verbunden sind, der für das horizontale Herunterskalieren ausgewählt wurde.

- **Warnmeldung an aktive User senden**: Wählen Sie aus der Dropdown-Liste die Anzahl der Minuten aus, bevor das horizontale Herunterskalieren erfolgt, in denen die Nachricht gesendet werden soll.
- **Der Nachrichtentext sollte lauten**: Geben Sie den Text der Warnmeldung ein.

9. Geben Sie die folgenden **Auto-Heal defekter Hosts** Informationen ein:

> **Anmerkung**
>
> Sitzungshosts können aufgrund von Problemen mit dem Domänenvertrauen oder der FSLogix-Konfiguration beeinträchtigt werden. Der AVD-Agent meldet den Status solcher Hosts als nicht verfügbar. Admins müssen solche Hosts dann manuell aus dem Hostpool entfernen. Nerdio Manager ermöglicht es Ihnen jedoch, eine Reihe von Aktionen zu konfigurieren, um diese Sitzungshosts während des automatischen Skalierungsprozesses zu reparieren. Die automatische Skalierung kann versuchen, defekte Sitzungshosts durch Neustarten sowie Löschen und Neuerstellen zu reparieren. Es können einige Versuche unternommen werden, den Host neu zu starten, um ihn wieder in einen betriebsbereiten Zustand zu versetzen, und ihn anschließend entweder in Ruhe zu lassen oder den Host zu löschen und neu zu erstellen.

- **Auto-Heal defekter Hosts**: Aktivieren Sie diese Option, um Auto-Heal zu ermöglichen.
- **AVD-Agentenstatus**: Wählen Sie aus der Dropdown-Liste die gewünschten Status zusammen mit dem Sitzungsstatus aus.

> **Anmerkung**
>
> Der Status wird dem AVD-Dienst von dem auf der Sitzungshost-VM installierten AVD-Agenten gemeldet. Wenn etwas nicht stimmt, lautet der Status anders als „Verfügbar“. Nicht jeder Status außer „Verfügbar“ bedeutet, dass ein Problem vorliegt. Weitere Details finden Sie in diesem Microsoft-Artikel. Hosts mit aktiven Sitzungen können weiterhin funktionsfähig sein und werden nicht als defekt behandelt. Nur Hosts, die entweder überhaupt keine Sitzungen oder keine aktiven Sitzungen (d. h. nur getrennte Sitzungen) aufweisen, werden von der automatischen Skalierung als defekt eingestuft.

- **Timeout der ersten Aktion**: Geben Sie die Anzahl der Minuten ein, die gewartet werden soll, bevor die erste Aktion ausgeführt wird.
- **Wiederherstellungsaktionen**: Wählen Sie aus der Dropdown-Liste die Wiederherstellungsaktion(en) aus.

> **Anmerkung**
>
> - Sie können eine VM-Aktion (z. B. VM neustarten oder VM entfernen) oder eine Skript-Aktion (z. B. SxS neu installieren, Host erneut bei AVD registrieren, etc.) auswählen.
> - Die Wiederherstellungsaktionen werden in der angezeigten Reihenfolge ausgeführt. Sie können eine beliebige Aktion per Drag & Drop verschieben, um deren Position in der Liste und damit die Reihenfolge der Ausführung zu ändern.

- **Zeitüberschreitung zwischen Wiederherstellungsaktionen**: Geben Sie die Anzahl der Minuten ein, die nach jeder Wiederherstellungsaktion gewartet werden soll, bevor mit dem nächsten Schritt fortgefahren wird (zum Beispiel VM neustarten, dann VM entfernen, etc.).

> **Anmerkung**
>
> Wenn der Auto-Heal-Vorgang das Löschen und Neuerstellen einer defekten Host-VM erfordert, wird eine Ersatz-VM eingeschaltet, um die Kapazität bereitzustellen, sofern verfügbar.

10. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern**.

Verwandte Themen

Dynamische Hostpools erstellen [78]

Auto-scale für dynamische Hostpools aktivieren [92]

Autoscaling: Kostenoptimierung: Sitzungshost-VM, Betriebssystemdatenträger, Speicher

Es gibt zwei Arten von Kosten, die mit einer VM verbunden sind: Compute-Kosten und Speicherkosten. Compute-Kosten fallen nur an, wenn die VM in Gebrauch ist, während Speicherkosten auch dann anfallen, wenn die VM angehalten ist.

Die Einstellungen **Größe der Betriebssystem-Disk im laufenden Betrieb** und **Typ der Betriebssystem-Disk im ausgeschalteten Zustand** (zusammen mit anderen Auto-scale-Einstellungen) ermöglichen Einsparungen von bis zu 75 % bei den Speicherkosten. Die Auto-scale-Logik kann den Typ der Betriebssystem-Disk von VMs sowohl in gepoolten als auch in persönlichen Hostpools automatisch auf eine kostengünstigere Speicherstufe (von Premium-SSD auf Standard-HDD) umstellen, während die Host-VM ausgeschaltet ist, und unmittelbar vor dem Start wieder auf die höhere Leistungsstufe zurücksetzen.

So konfigurieren Sie die Einstellungen Größe der Betriebssystem-Disk im laufenden Betrieb und Typ der Betriebs-

system-Disk im ausgeschalteten Zustand auf Ihren Sitzungshosts:

1. Suchen Sie den Hostpool, mit dem Sie arbeiten möchten.
2. Wählen Sie im Aktionsmenü **Auto-scale** > **Konfigurieren**.
3. Konfigurieren Sie im Abschnitt **Auto-scale** Folgendes:
   - **OS-Disk bei laufender VM (Vorlage**): Wählen Sie aus der Dropdownliste den Disk-Typ für die laufende VM aus.
   - **OS-Disk-Typ bei gestoppter VM**: Wählen Sie aus der Dropdownliste den Disk-Typ für die gestoppte VM aus.
4. Nachdem Sie die oben genannten Parameter geändert haben, wählen Sie **Speichern und schließen**.

> **Anmerkung**
>
> Mit dem Azure-Feature **VM beim Herstellen einer Verbindung starten** können VMs außerhalb von Nerdio Manager eingeschaltet werden. Dadurch werden die Einstellungen **Größe der Betriebssystem-Disk im laufenden Betrieb** und **Typ der Betriebssystem-Disk im ausgeschalteten Zustand** möglicherweise überschrieben. Das bedeutet, dass eine VM, die über das Feature **VM beim Herstellen einer Verbindung starten** eingeschaltet wird, die Disk-Leistung nicht ändern kann. Stattdessen empfehlen wir, **Pre-Staging** so zu konfigurieren, dass „Alle Hosts auf den OS-Disk-Typ für laufende VMs einstellen“ aktiviert ist, wenn **VM beim Herstellen einer Verbindung starten** zusammen mit der Speicherskalierung aktiviert ist.

Für einen Single-User-Hostpool mit zeitplanbasiertem Auto-scale können Sie die **Host-OS-Disks** innerhalb und außerhalb der Arbeitszeiten konfigurieren. Sie können beispielsweise Premium SSD angeben, wenn die VM läuft, und Standard SSD, wenn die VM beendet ist. So sparen Sie Kosten für Azure Storage.

So konfigurieren Sie Host-OS-Disks

1. Navigieren Sie zu **Cloud-Desktops** > **Azure Virtual Desktop** > **Workspaces** > **Hostpools**.

2. Finden Sie den Single-User-Hostpool, den Sie ändern möchten.
3. Wählen Sie im Aktionsmenü **Auto-scale**> **Konfigurieren**.
4. Konfigurieren Sie im Abschnitt **Host OS Disks** Folgendes:
   - **Running**: Wählen Sie aus der Dropdown-Liste den Disk-Typ für die laufende VM aus.
   - **Gestoppt**: Wählen Sie aus der Dropdown-Liste den Disk-Typ aus, wenn die VM gestoppt ist.
5. Nachdem Sie die oben genannten Parameter geändert haben, wählen Sie **Speichern und schließen**.

   Für einen Multi-User-Hostpool, bei dem **Mindestwert für die Kapazität aktiver Hosts** auf 0 festgelegt ist, können Sie konfigurieren, dass während der Pre-Staging-Zeiten alle OS-Disks beendeter VMs automatisch in den Typ **OS-Disk für laufende VMs** konvertiert werden. Dies ist erforderlich, um sicherzustellen, dass eine VM, die via **Azure Start VM on Connect** gestartet wird, über den richtigen Hochleistungs-Disk-Typ verfügt.

So konfigurieren Sie die Konvertierung des OS-Disk-Typs für das Pre-Staging

1. Finden Sie den Single-User-Hostpool, mit dem Sie arbeiten möchten.
2. Wählen Sie im Aktionsmenü **Auto-scale** > **Konfigurieren** aus.
3. Konfigurieren Sie im Abschnitt **Hosts für Pre-Staging** Folgendes:
   - Aktivieren Sie bei Bedarf **Pre-Staging für Hosts**.
   - **Alle Hosts auf den OS-Disk-Typ für laufende VMs einstellen**: Wählen Sie diese Option aus.
   - Stellen Sie die Pre-Staging-Zeit wie gewünscht ein.
4. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern und schließen**.

Fügen Sie einem dynamischen Hostpool einen neuen Sitzungshost hinzu.

Sobald ein Hostpool erstellt wurde, können Sie manuell Sitzungshosts hinzufügen.

Tipp

Wenn Sie dynamische Hostpools verwenden, empfehlen wir, die Hosts mit konfigurierter automatischer Skalierung zu erstellen. Weitere Informationen finden Sie unter Dynamisches Auto-Scaling für Hostpools aktivieren [92].

So fügen Sie einem dynamischen Hostpool einen Sitzungshost hinzu:

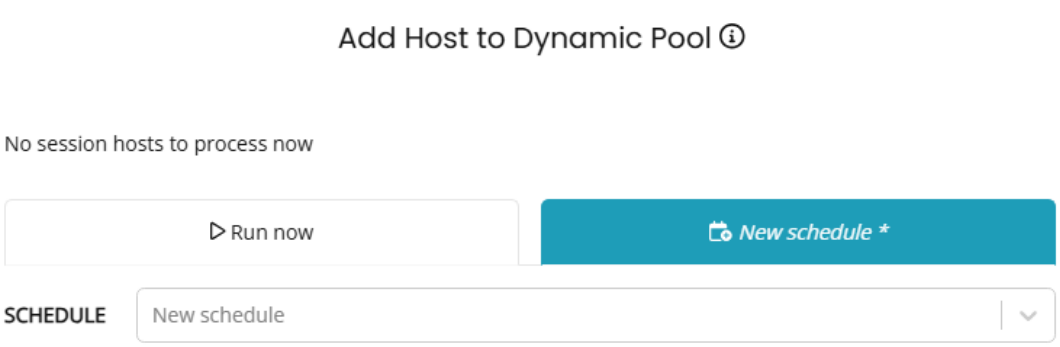
1. Suchen Sie den dynamischen Hostpool, mit dem Sie arbeiten möchten.
2. Gehen Sie wie folgt vor:

   Wählen Sie im Menü „Weitere Optionen“ die Option **Hosts** > **Neu hinzufügen**.
3. Geben Sie die folgenden Informationen ein:

   Anmerkung

   Für einige der erforderlichen Parameter können Sie die verfügbaren Optionen mithilfe der Ressourcenauswahlregeln filtern. Sie können beispielsweise die verfügbaren VM-Größen oder OS-Disks so filtern, dass nur Optionen für RAM-optimierte Intel-VMs angezeigt werden. Weitere Informationen finden Sie unter Verwaltung von Ressourcenauswahlregeln [44].

   - Wählen Sie **Jetzt ausführen** oder **Zeitplan**.
     - Im Bereich **Zeitplan** können Sie die Aufgabe während eines oder mehrerer ausgewählter Zeiträume ausführen. Andernfalls startet die Aufgabe, sobald Sie **OK** auswählen. Weitere Informationen zum Erstellen eines Zeitplans finden Sie unter Zeitpläne für Aufgaben verwalten [42]. Wählen Sie den Zeitplan aus der Dropdown-Liste aus oder erstellen Sie einen neuen Zeitplan.



- **Hostanzahl**: Geben Sie die Anzahl der Sitzungshosts ein, die während der Erstellung zum Hostpool hinzugefügt werden sollen.
- **Hostname**: Geben Sie den Namen der neu hinzugefügten Hosts für den exakten Namen, ein Präfix oder das Präfix+Muster ein.
  - **Exakt/Präfix/Muster**: Wählen Sie aus der Dropdownliste aus, ob Sie einen exakten Namen, ein Präfix oder ein Muster verwenden möchten.

Anmerkung

- **Exakt** gilt beim Hinzufügen eines einzelnen Hosts und der Angabe eines exakten Namens. Zum Beispiel MYADVHOST.
- **Präfix** kann beim Erstellen mehrerer Sitzungshosts verwendet werden. Das Präfix ist auf 10 gültige Windows-Computernamenzeichen begrenzt. Bei Verwendung eines Präfixes wird automatisch ein eindeutiges Suffix im Format „-xxxx“ angehängt, wobei xxxx für 4 zufällige alphanumerische Zeichen steht. Zum Beispiel: AVDHOST-s72h. Fügen Sie dem Präfix kein „-“ hinzu.
- **Muster** kann verwendet werden, um eine erweiterte Namenskonvention für neue Hosts festzulegen. Musterzeichen müssen in {} eingeschlossen werden und können # (für fortlaufende Nummern) und/oder ? (für zufällige alphanumerische Zeichen) sein. Ein # steht für Zahlen von 0 bis 9, zwei # stehen für Zahlen von 0 bis 99 usw.
  - Beispiel 1: AVDHOST{###} (AVDHOST000..AVDHOST999).
  - Beispiel 2: AVDHOST-{???} (AVDHOST-d83, AVDHOST-7sl usw.).

- **Netzwerk**: Wählen Sie das Netzwerk aus der Dropdownliste aus. Das Netzwerk bestimmt die Azure-Region der VM.
- **Desktop-Image**: Wählen Sie aus der Dropdown-Liste das Desktop-Image aus, das als Golden Image für neu erstellte Sitzungshosts verwendet wird.

> **Anmerkung**
>
> Der Abschnitt **Nicht verwaltete Azure Compute Gallery-Imageversionen** befindet sich am Ende der Liste. Dies sind nicht verwaltete Backup-Versionen von Images, die während der Aktivierung von Staging-Images erstellt wurden. Diese Images können verwendet werden, um Änderungen an Sitzungshosts wiederherzustellen.

- **VM-Größe**: Wählen Sie aus dem Dropdown-Menü den VM-Typ für neu erstellte Sitzungshosts aus.
- **Betriebssystem-Datenträger**: Wählen Sie aus der Dropdown-Liste den Typ und die Größe des Betriebssystem-Datenträgers für neu erstellte Sitzungshosts aus. Wählen Sie bei Bedarf optionale Filter aus, um bestimmte Betriebssystem-Datenträgertypen anzuzeigen. Wählen Sie beispielsweise **Alle Datenträger-Leistungsstufen**, um die Premium-SSD-Datenträger anzuzeigen.

> **Anmerkung**
>
> Dies muss gleich oder größer als die Größe des oben ausgewählten Desktop-Images sein. Die Verwendung von Standard-HDD (S-Typ) wird nicht empfohlen. Premium-SSD bietet die beste Leistung.

- **Ressourcengruppe**: Wählen Sie aus der Dropdown-Liste die Ressourcengruppe aus, die die VMs enthalten soll.
- **Tags anwenden**: Geben Sie optional den **Namen** und den **Wert** des Azure-Tags ein, das auf den Sitzungshost angewendet werden soll.

> **Anmerkung**
>
> Sie können mehrere Tags angeben. Weitere Informationen zur Verwendung von Tags zum Organisieren Ihrer Azure-Ressourcen finden Sie in diesem Microsoft-Artikel.

4. Wenn Sie eine **Hostanzahl** eingegeben haben, die größer als 1 ist, geben Sie die folgenden Informationen ein:

- **Hosts gruppieren in Gruppen von**: Geben Sie die Anzahl der gleichzeitigen Vorgänge beim Hinzufügen der neuen Hosts ein.
- **Anzahl der Fehler vor dem Abbruch**: Geben Sie die Anzahl der fehlgeschlagenen Aufgaben ein, bevor der Vorgang gestoppt wird.

5. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Jetzt ausführen** (nicht geplant) oder **Speichern und schließen** (geplant).

Hostpool-AVD-Konfiguration

> ⚠ **Warnung**
>
> Nerdio Manager installiert die BgInfo Azure-Erweiterung während keiner Automatisierungs- oder Verwaltungsprozesse. Die BgInfo-Erweiterung kann jedoch entweder direkt über eine skriptgesteuerte Aktion oder unbeabsichtigt installiert werden, wie im Bericht zu Problemen mit dem Azure PowerShell-Modul angegeben.

Nerdio Manager ermöglicht es Ihnen, die AVD-Einstellungen des Hostpools anzupassen.

So konfigurieren Sie die AVD-Einstellungen des Hostpools:

1. Finden Sie den Hostpool, mit dem Sie arbeiten möchten.
2. Wählen Sie im Aktionsmenü **Einstellungen** > **AVD**.
3. Geben Sie die folgenden Informationen ein:
   - **Anzeigename**: Geben Sie den Anzeigenamen ein, der für die Endbenutzer sichtbar ist.
   - **Beschreibung**: Geben Sie die Beschreibung ein, die für die Admins sichtbar ist.

> **Anmerkung**
>
> Sowohl der Anzeigename als auch die Beschreibung können jederzeit geändert werden.

- **Lastenausgleich**: Wählen Sie die gewünschte Option für den Lastenausgleich aus.

> **Anmerkung**
>
> Der Algorithmus für das Load-Balancing wird vom AVD-Verwaltungsdienst verwendet, um zu bestimmen, wie die Desktop- oder RemoteApp-Verbindung eines bestimmten Users über die Route weitergeleitet wird.
>
> **Breitensuche** bedeutet, dass der Algorithmus für das Load-Balancing die User gleichmäßig auf alle verfügbaren Sitzungshosts verteilt.
>
> **Tiefensuche** bedeutet, dass der Algorithmus für das Load-Balancing alle User auf dem ersten Sitzungshost platziert, bis das Sitzungslimit des Hosts erreicht ist. Erst dann platziert er die User auf dem nächsten Sitzungshost. Bei Bedarf schaltet er die VM ein und stellt sie den Usern zur Verfügung.

  - **Session Limit**: Geben Sie die Anzahl der Sitzungen ein, die ein einzelner Host im Hostpool akzeptieren kann.
- **Validierungsumgebung**: Wählen Sie diese Option, um diesen Hostpool als Validierungshostpool festzulegen.

> **Anmerkung**
>
> Validierungshostpools erhalten Dienstupdates in einem schnelleren Rhythmus als Nicht-Validierungshostpools, wodurch Sie Dienständerungen testen können, bevor diese umfassend in der Produktion bereitgestellt werden.

- **Benutzern das manuelle Starten eines Sitzungshosts erlauben, wenn keiner gestartet ist**: Wählen Sie diese Option, um einem User das Anmelden bei Nerdio Manager zu ermöglichen und Dienstaktionen durchzuführen. Zum Beispiel das Einschalten der Sitzungshosts innerhalb des Hostpools. Nur bestimmte User, die über die Berechtigungen zur Anmeldung bei Nerdio Manager verfügen, können die Sitzungshost-VM auf diese Weise starten.

- **VM beim Herstellen einer Verbindung starten**: Die VM wird automatisch eingeschaltet, wenn der User eine Verbindung herstellt. Jeder User kann die VM starten, wenn er sich anmeldet.
- **User beim Entfernen eines Hosts vom Hostpool abmelden**: Wählen Sie bei persönlichen Hostpools diese Option, um den User vom Hostpool abzumelden, wenn der Host gelöscht wird.
- **CPU-Auslastung der Hosts erfassen**: Wählen Sie diese Option, damit der Prozess zur automatischen Skalierung die CPU-Auslastung unabhängig vom Auslöser für die automatische Skalierung des Hostpools immer erfasst.
- **RAM-Auslastung der Hosts erfassen**: Wählen Sie diese Option, damit der Prozess zur automatischen Skalierung die RAM-Auslastung unabhängig vom Auslöser für die automatische Skalierung des Hostpools immer erfasst.
- **Durchschnittliche aktive Sitzungen der Hosts erfassen**: Wählen Sie diese Option, damit der Prozess zur automatischen Skalierung die Daten zu den durchschnittlichen aktiven Sitzungen unabhängig vom Auslöser für die automatische Skalierung des Hostpools immer erfasst.
- **Geplantes AVD-Agent-Update aktivieren**: Schalten Sie diese Option ein, um den Tag und die Uhrzeit für das Update des AVD-Agenten festzulegen.

> **Anmerkung**
>
> Die Bereitstellung von Updates zu günstigen Zeiten oder außerhalb der Hauptgeschäftszeiten gewährleistet eine höhere Zuverlässigkeit und Business Continuity und verbessert gleichzeitig die Darstellung, ohne dass geschäftskritische Arbeiten unterbrochen werden.

  - **Zeitzone**: Wählen Sie aus der Dropdown-Liste die Zeitzone für das geplante Update aus.

> **Anmerkung**
>
> Die Einstellung der Zeitzone stellt sicher, dass Updates für die Sitzungshost-VMs im Hostpool zur gleichen Zeit gemäß der ausgewählten Zeitzone erfolgen, unabhängig von den lokalen Zeitzonen der Sitzungshost-VMs. Weitere Informationen finden Sie in diesem Microsoft Artikel.

- **Lokale Zeitzone des Sitzungshosts verwenden**: Wählen Sie diese Option, um das Agent-Update unter Verwendung der lokalen Zeitzone jeder Sitzungshost-VM im Hostpool durchzuführen.

> **Anmerkung**
>
> . Verwenden Sie diese Einstellung, wenn sich alle Sitzungshost-VMs in Ihrem Hostpool oder deren zugewiesene User in unterschiedlichen Zeitzonen befinden.

- **Wartungsfenster**: Geben Sie über die Dropdown-Listen den Tag und die Uhrzeit für das Agent-Update an.

> **Anmerkung**
>
> Alle Wartungsfenster sind zwei Stunden lang.

- **Weiteres Wartungsfenster konfigurieren**: Wählen Sie optional diese Option, um ein zweites Wartungsfenster festzulegen.

> **Anmerkung**
>
> Das Erstellen von zwei Wartungsfenstern bietet den Agent-Komponenten eine zusätzliche Möglichkeit zur Aktualisierung, falls das erste Update nicht erfolgreich war.

- **Alle Hosts während des/der Fenster(s) einschalten**: Wählen Sie optional diese Option, um alle Hosts in einem Hostpool während der Wartungsfenster-Vorgänge einzuschalten und so die Installation des neuesten AVD-Agent sicherzustellen.

> **Anmerkung**
>
> Hosts, die als Teil dieses Prozesses gestartet werden, werden nach 2 Stunden heruntergefahren. Hosts, die bereits laufen, behalten ihren Energiezustand unverändert.

- **Hosts im Drain-Modus ausschließen**: Wählen Sie optional diese Option, um Hosts im Drain-Modus von den AVD-Agent-Wartungsfensteraufgaben auszuschließen, die in den Hostpool-Eigenschaften konfiguriert sind.

4. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern** oder **Speichern und schließen**.

Bereitstellung von virtuellen Maschinen im Hostpool

> **Warnung**
>
> Nerdio Manager installiert die BgInfo Azure-Erweiterung während keiner Automatisierungs- oder Verwaltungsprozesse. Die BgInfo-Erweiterung kann jedoch entweder direkt über eine skriptgesteuerte Aktion oder unbeabsichtigt installiert werden, wie im Bericht zu Problemen mit dem Azure PowerShell-Modul angegeben.

Nerdio Manager ermöglicht es Ihnen, die Art und Weise anzupassen, wie Sitzungshost-virtuelle Maschinen in einem Hostpool bereitgestellt werden. Dies ist ein funktionsreiches Feature, das unten detailliert beschrieben wird.

So konfigurieren Sie die Bereitstellung von Hostpool-VMs:

1. Finden Sie den Hostpool, mit dem Sie arbeiten möchten.
2. Wählen Sie im Aktionsmenü **Einstellungen** > **virtuelle Maschinen**.
3. Geben Sie die folgenden Informationen ein:
4. Geben Sie die folgenden **Betriebssystem**-Optionen ein:
   - **Zeitzone festlegen**: Aktivieren Sie diese Option und wählen Sie aus der Dropdown-Liste die Zeitzone aus, um die Zeitzone auf der virtuellen Maschine bei der Bereitstellung festzulegen.

- **Zeitzonenumleitung**: Aktivieren Sie diese Option, damit Benutzer die Zeitzone ihres lokalen Geräts innerhalb ihrer Sitzung sehen können.
- **Immer zur Passworteingabe auffordern**: Wählen Sie diese Option, um den Benutzer immer zur Eingabe eines Passworts aufzufordern.

> **Anmerkung**
>
> Diese Richtlinie gibt an, ob der Remotedesktopdienst den Client bei der Verbindung immer zur Eingabe eines Passworts auffordert. Sie können diese Einstellung verwenden, um eine Passwortabfrage für Benutzer zu erzwingen, die sich beim Remotedesktopdienst anmelden, selbst wenn sie das Passwort bereits im Remote-Desktop-Verbindungsclient eingegeben haben.
>
> Standardmäßig ermöglicht der Remotedesktopdienst Benutzern, sich automatisch anzumelden, indem sie ein Passwort im Remote-Desktop-Verbindungsclient eingeben.
>
> - Wenn Sie diese Option auswählen, können sich Benutzer nicht automatisch beim Remotedesktopdienst anmelden, indem sie ihre Passwörter im Remote-Desktop-Verbindungsclient angeben. Sie werden zur Eingabe eines Passworts für die Anmeldung aufgefordert.
> - Wenn Sie diese Option nicht auswählen, können sich User immer automatisch beim Remotedesktopdienst anmelden, indem sie ihre Passwörter im Remote-Desktop-Verbindung-Client eingeben.

- **Ausgeschaltete VMs automatisch Zuweisung aufheben**: Wählen Sie diese Option, damit eine periodische Aufgabe überprüft, ob sich Sitzungshost-VMs in einem ausgeschalteten, aber noch nicht deallokierten Zustand befinden, und hebt die Zuweisung dieser VMs automatisch auf, um Azure Compute-Kosten zu sparen.
- **Bootdiagnose**: Aktivieren Sie diese Option, um das Bootdiagnose-Feature auf Desktops in diesem Pool anzuwenden.

> **Anmerkung**
>
> Diese Einstellung gilt nur für neu erstellte Desktops.

- **Storage-Konten für Bootdaten**: Wählen Sie optional aus der Dropdownliste ein verfügbares Storage-Konto aus, das zum Speichern von Bootdaten verwendet werden soll.

  > **Anmerkung**
  >
  > Standardmäßig verwendet Azure ein automatisch verwaltetes Storage-Konto für Screenshots und andere Daten. Um die Standardeinstellung zu verwenden, lassen Sie dies leer.

- **Optionen für die Patch-Orchestrierung**: Wählen Sie aus der Dropdownliste die Option für die Patch-Orchestrierung aus, mit der Sie steuern können, wie Patches auf Ihre virtuelle Maschine angewendet werden.

  > **Anmerkung**
  >
  > Nerdio Manager berücksichtigt die Azure-Standardeinstellung, die „Automatisch durch Betriebssystem“ (Windows-Updates automatisch) lautet.

- **Accelerated Networking (falls unterstützt)**: Aktivieren Sie diese Option, um Accelerated Networking zu aktivieren, sofern verfügbar.

> **Anmerkung**
>
> Das Feature Accelerated Networking von Azure-VMs ist in einigen der größeren Azure-VMs verfügbar. Dieses Feature ist nützlich für Unternehmensorganisationen und IT-Experten, die große Mengen an Azure Virtual Desktops bereitstellen, verwalten und optimieren müssen. Es beschleunigt die Netzwerkleistung einzelner VMs.
>
> Wenn dieses Feature auf Ihrer Azure-VM nicht unterstützt wird, ist es nicht aktiviert. Weitere Informationen finden Sie in diesem Microsoft-Dokument.

- **NVMe (falls unterstützt)**: Aktivieren Sie diese Option, um NVMe zu aktivieren, falls verfügbar.

> **Anmerkung**
>
> NVMe ist ein Speicherprotokoll, das höhere IOPs und einen höheren Durchsatz bietet und Ihrer Arbeitslast eine insgesamt höhere Leistung ermöglicht. Weitere Informationen finden Sie in diesem Microsoft-Dokument.

- **GPU-Treiber (falls unterstützt)**: Aktivieren Sie diese Option, um entweder NVidia- oder AMD-Treiber zu installieren.

> **Anmerkung**
>
> GPU-Treiber können auf VMs der N-Serie installiert werden.

- **H.265-Codierung (falls unterstützt)**: Aktivieren Sie diese Option, um die Hardwarebeschleunigung für H.265 High Efficiency Video Coding zu aktivieren.

> **Anmerkung**
>
> Die H.265-Hardwarebeschleunigung ist nur bei VM-Größen der N-Serie mit NVidia-GPUs verfügbar.

- **VMs in Kapazitätsreservierungsgruppen bereitstellen**: Aktivieren Sie diese Option, um die VMs in einer Kapazitätsreservierungsgruppe zu platzieren.

  > **Anmerkung**
  >
  > Weitere Einzelheiten finden Sie unter Kapazitätsreservierungsgruppen verwalten.

  - **Kapazitätsreservierungsgruppen**: Wählen Sie die Kapazitätsreservierungsgruppe(n) aus der Dropdownliste aus.
- **VMs über Verfügbarkeitszonen hinweg bereitstellen**: Aktivieren Sie diese Option, um neu erstellte oder nach einem Reimaging bereitgestellte Sitzungshost-VMs automatisch über Verfügbarkeitszonen in der ausgewählten Azure-Region zu verteilen.

  > **Anmerkung**
  >
  > - Schalten Sie **Verfügbarkeitszonen-Berücksichtigung** in der Konfiguration des Azure Capacity Extender für den Hostpool an, damit Nerdio Manager bei der Neuinstanziierung von VMs alle möglichen Verfügbarkeitszonen berücksichtigt.
  > - Weitere Informationen zu Azure-Regionen und Verfügbarkeitszonen finden Sie in diesem Microsoft-Artikel.

  - **Verfügbarkeitszone**: Wählen Sie die Verfügbarkeitszone(n) aus der Dropdownliste aus.
- **VMs auf dedizierten Hosts bereitstellen**: Aktivieren Sie diese Option, um die VMs auf physischen Servern bereitzustellen.

  > **Anmerkung**
  >
  > Weitere Informationen zu dedizierten Azure-Hosts finden Sie in diesem Microsoft-Artikel.

  - **Dedizierte Hostgruppe**: Wählen Sie aus der Dropdown-Liste die dedizierte Hostgruppe aus.

- **Dedizierter Host**: Wählen Sie aus der Dropdown-Liste den dedizierten Host für die VMs aus.

  > **Anmerkung**
  >
  > Wenn **Automatische Zuweisung** ausgewählt ist, werden die VMs beim Einschalten automatisch den entsprechenden Hosts zugewiesen.

- **VMs in einer Näherungsplatzierungsgruppe bereitstellen**: Aktivieren Sie diese Option, um VMs in einer Näherungsplatzierungsgruppe bereitzustellen.

  > **Anmerkung**
  >
  > VMs, die in einer Näherungsplatzierungsgruppe platziert sind, befinden sich physisch nahe beieinander in einem Azure-Rechenzentrum, wodurch die geringstmögliche Netzwerklatenz zwischen den VMs sichergestellt wird. Siehe Learn Microsoft: Näherungsplatzierungsgruppen für Details.

  - **Näherungsplatzierungsgruppe**: Wählen Sie aus der Dropdown-Liste die Näherungsplatzierungsgruppe aus.
  -

    > **Anmerkung**
    >
    > Die ausgewählte Gruppe wird der VM bei der Erstellung automatisch zugewiesen. Wenn keine geeignete Ressource gefunden wird, schlägt die VM-Erstellung fehl.

- **VM nach Bereitstellung neustarten**: Wählen Sie diese Option, um die VM nach ihrer Erstellung neustarten.

> **Anmerkung**
>
> Wenn während der Bereitstellung bestimmte Erweiterungen installiert werden (FSLogix, Sepago, Virtual Desktop Optimizations oder User Sessions Time Limits), wird die VM automatisch neu gestartet, auch wenn diese Option nicht ausgewählt ist.

- **App Attach-Zertifikate installieren**: Wählen Sie diese Option, um alle gespeicherten Zertifikate zu installieren, wenn die App Attach-Pakete diesem Hostpool hinzugefügt werden.
- **App-V-Clientdienst**: Aktivieren Sie diese Option, um den App-V-Clientdienst zu aktivieren, der erforderlich ist, wenn die VM App Attach-Pakete verwendet, die ein App-V-Paket enthalten.
- **Anwendungen installieren**: Aktivieren Sie diese Option, um Anwendungen, die durch wiederkehrende UAM-Richtlinien konfiguriert wurden, zu installieren, bevor der Host aus dem Drain-Modus genommen wird.
- **Entra ID-Gruppe(n)**: Wählen Sie aus der Dropdown-Liste die Entra ID-Standardgruppe(n) aus, der/denen die Sitzungshosts hinzugefügt werden sollen.
- **Entra Connect-Replikations-Timeout (Minuten)**: Geben Sie bei Hybrid-Registrierungen eine maximale Verzögerung für die Replikation von Computerkonten aus dem Active Directory über Entra Connect ein.

> **Anmerkung**
>
> Standardmäßig sind dies 30 Minuten. Es kann ein Wert von bis zu 120 Minuten angegeben werden.

- **Intune-Compliance erzwingen**: Wählen Sie diese Option aus der Dropdown-Liste aus, um Hosts für Benutzer erst dann verfügbar zu machen, wenn die Intune-Compliance-Anforderungen erfüllt sind.

> **Anmerkung**
>
> - Wählen Sie optional **Nur Compliance-Richtlinien** oder **Alle Richtlinien** aus. Die Option **Alle Richtlinien** erfordert zudem, dass Intune-verwaltete Apps erfolgreich installiert wurden, bevor der Host aus dem Drain-Modus freigegeben wird.
> - Die Intune-Integration muss aktiviert sein, um diese Funktion nutzen zu können, wobei folgende Optionen zur Verfügung stehen:
>   - Die Einstellung **Nur Compliance-Richtlinien** erfordert Leseberechtigungen für **Intune-verwaltete Geräte**.
>   - Die Einstellung **Alle Richtlinien** erfordert zusätzlich Leseberechtigungen für **Geräterichtlinien & App-Richtlinien**.
> - Das Aktivieren einer dieser Optionen kann je nach den konfigurierten Intune-Compliance-Anforderungen zu einer erheblichen Erhöhung der Bereitstellungszeit führen.

- **Nicht-Administratoren das Shadowing von Sitzungen erlauben**: Aktivieren Sie diese Option, um ausgewählten Nicht-Administratoren oder Gruppen das Shadowing von Sitzungen zu erlauben.

> **Anmerkung**
>
> Sitzungsshadowing ist nur bei Multi-Session-Versionen des Windows-Betriebssystems verfügbar. Diese Funktion funktioniert nicht mit Windows 10 Enterprise (Single-Session).

  - **Benutzer- oder Gruppenname**: Wählen Sie aus der Dropdownliste die Benutzer oder Gruppen aus, denen das Shadowing von Sitzungen erlaubt werden soll.
- **Sicherheitstyp**: Wählen Sie aus der Dropdownliste den Sicherheitstyp aus.

> **Anmerkung**
>
> Der Sicherheitstyp bezieht sich auf die verschiedenen Sicherheitsfunktionen, die für eine virtuelle Maschine verfügbar sind. Sicherheitsfunktionen wie Trusted Launch und vertrauliche virtuelle Maschinen verbessern die Sicherheit von Gen2-VMs. Zusätzliche Sicherheitsfunktionen haben jedoch einige Einschränkungen, darunter die fehlende Unterstützung für das Sichern, verwaltete Datenträger und ephemere Betriebssystemdatenträger.

- **Verschlüsselung auf dem Host**: Wählen Sie diese Option, damit auf den Sitzungshost-VMs gespeicherte Daten im Ruhezustand verschlüsselt werden und verschlüsselt an den Speicherdienst übertragen werden.

> **Anmerkung**
>
> - Diese Einstellung gilt nur für neu erstellte Desktops.
> - Verschlüsselungssätze gelten pro Abonnement/Region. Sie können Hosts in verschiedenen Abonnements/Regionen erstellen, und basierend auf dem Abonnement/der Region des Hosts wählen wir den entsprechenden Verschlüsselungssatz aus.
> - Weitere Informationen zur Funktion „Verschlüsselung auf dem Host“ finden Sie in diesem Microsoft-Artikel.

- **Datenträgerverschlüsselungssätze**: Wählen Sie aus der Dropdownliste die Datenträgerverschlüsselungssätze aus, die für die Funktionalität der vom Kunden verwalteten Schlüssel verwendet werden sollen.

> **Anmerkung**
>
> Standardmäßig verwendet Nerdio Manager plattformverwaltete Schlüssel. Um die Standardeinstellung zu verwenden, lassen Sie die Datenträgerverschlüsselungssätze leer. Wenn Disk-Verschlüsselungssätze erforderlich sind, erstellen Sie diese über das Azure-Portal in derselben Region wie den Desktop-Pool. Verfügbare Datenträgerverschlüsselungssätze können aus der Dropdown-Liste ausgewählt werden. Weitere Informationen zu Schlüsseloptionen finden Sie unter Serverseitige Verschlüsselung von Azure Disk Storage.

- **Anwendungssicherheitsgruppe**: Wählen Sie aus der Dropdown-Liste die Anwendungssicherheitsgruppen (ASGs) aus, mit denen Sie Netzwerksicherheit als natürliche Erweiterung der Anwendungsstruktur konfigurieren können.

> **Anmerkung**
>
> Dies ermöglicht es Ihnen, virtuelle Maschinen zu gruppieren und Netzwerksicherheitsrichtlinien basierend auf diesen Gruppen zu definieren. Diese Funktion ermöglicht es Ihnen, Ihre Sicherheitsrichtlinie in großem Maßstab wiederzuverwenden, ohne explizite IP-Adressen manuell verwalten zu müssen. VMs mit Netzwerkschnittstellen in anderen Regionen als die ASG werden ohne ASG-Unterstützung erstellt. Die maximale Anzahl unterstützter ASGs beträgt 10.
>
> Weitere Informationen finden Sie unter Anwendungssicherheitsgruppen.

- **Wasserzeichen**: Aktivieren Sie diese Option, um Wasserzeichen zu aktivieren.

> **Anmerkung**
>
> Wasserzeichen helfen dabei, die Erfassung sensibler Informationen auf Client-Endpunkten zu verhindern. Wenn Sie Wasserzeichen aktivieren, erscheinen QR-Code-Wasserzeichen als Teil der Remote-Desktops. Der QR-Code enthält die Verbindungs-ID einer Remotesitzung, die Administratoren zur Nachverfolgung der Sitzung verwenden können.

- **Skalierung**: Wählen Sie die Skalierung aus, die der Größe jedes QR-Code-Punkts in Pixeln entspricht. Dieser Wert bestimmt die Anzahl der Quadrate pro Punkt im QR-Code.
- **Deckkraft**: Wählen Sie die Deckkraft aus, die angibt, wie transparent das Wasserzeichen ist, in Prozent, wobei 0 vollständig transparent bedeutet.
- **Breitenfaktor**: Wählen Sie den Breitenfaktor aus, der den Abstand zwischen den QR-Codes in Prozent bestimmt. In Kombination mit dem Höhenfaktor würde ein Wert von 0 dazu führen, dass die QR-Codes nebeneinander erscheinen und den gesamten Bildschirm ausfüllen.
- **Höhenfaktor**: Wählen Sie den Höhenfaktor aus, der den Abstand zwischen den QR-Codes in Prozent bestimmt. In Kombination mit dem Breitenfaktor würde ein Wert von 0 dazu führen, dass die QR-Codes nebeneinander erscheinen und den gesamten Bildschirm ausfüllen.

- **Skriptsignierung**: Aktivieren Sie diese Option, um die Skriptsignierung zu aktivieren.

> **Anmerkung**
>
> Nerdio Manager kann automatisch alle PowerShell-Erweiterungen und skriptbasierten Aktionen, die auf Sitzungshost-VMs ausgeführt werden, mithilfe eines angegebenen Signaturzertifikats signieren. Bitte beachten Sie, dass das ausgewählte Zertifikat auf den VMs installiert sein muss, damit die Skripte funktionieren.

5. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern** oder **Speichern und schließen**.

Userzuweisungen für Hostpools verwalten

Nerdio Manager ermöglicht es Ihnen, User anzuzeigen, die verschiedenen Hostpools zugeordnet sind. Darüber hinaus können Sie User dem Hostpool zuweisen oder die Zuweisung aufheben.

So verwalten Sie Userzuweisungen für Hostpools:

1. Finden Sie den Hostpool, mit dem Sie arbeiten möchten.
2. Wählen Sie im Aktionsmenü **Verwalten** > **User und Gruppen** aus.
3. Alternativ wählen Sie in der Spalte **Status** die Zahl neben **Zugewiesene User**, um die User und Gruppen anzuzeigen.
4. Im Fenster **Zuweisungen** können Sie die User und Gruppen suchen, sortieren und filtern. Filtern Sie beispielsweise nach allen Usern, die dem Hostpool nicht zugewiesen sind.
5. Um die Zuweisung von Usern zum Hostpool aufzuheben, wählen Sie das Symbol neben dem/den User(n), deren Zuweisung Sie aufheben möchten.
6. Wenn Sie alle User ausgewählt haben, wählen Sie **Zuweisung aufheben**.
7. Um User dem Hostpool zuzuweisen, wählen Sie das Symbol neben den Usern, denen Sie zuweisen möchten.
8. Wenn Sie alle User ausgewählt haben, wählen Sie **Zuweisen**.

Active Directory-Einstellungen des Hostpools konfigurieren

Standardmäßig verwendet jeder Hostpool die globale Active Directory-Standardkonfiguration, die bei der Installation von Nerdio Manager verwendet wurde. Nerdio Manager ermöglicht es Ihnen, bei Bedarf mehrere Active Directory-Profile mit unterschiedlichen Dienstkonten und OUs zu erstellen. Wir können diese mehreren Profile dann für verschiedene Hostpools verwenden.

So konfigurieren Sie Active Directory für einen Hostpool:

1. Finden Sie den Hostpool, mit dem Sie arbeiten möchten.
2. Wählen Sie im Aktionsmenü **Einstellungen** > **Directory** aus.

3. Geben Sie die folgenden Informationen ein:
   - **AD-Konfiguration**: Wählen Sie aus der Dropdown-Liste die Active Directory-Konfiguration aus.

     Geben Sie für eine **benutzerdefinierte** Konfiguration Folgendes ein:
     - **Directory**: Wählen Sie aus der Dropdown-Liste das Directory aus.
     - **AD-Domäne**: Geben Sie die Domäne, der die Sitzungshost-VMs beitreten sollen, im FQDN-Format (Fully Qualified Domain Name) ein.
     - **AD-Benutzername**: Geben Sie den Benutzernamen im FQDN-Format ein.

       > **Anmerkung**
       >
       > Dieser User muss über Berechtigungen zur Erstellung von Computerobjekten in der unten angegebenen OU sowie über die Möglichkeit verfügen, diese AD-Computerobjekte zu deaktivieren, wenn die VM die AD-Domäne verlässt.

     - **AD-Passwort**: Geben Sie das Passwort ein.
     - **Organisationseinheit**: Geben Sie den Namen der Organisationseinheit im DN-Format (Distinguished Name) ein.

       > **Anmerkung**
       >
       > Dies ist die Organisationseinheit, in der standardmäßig alle Sitzungshost-VMs und Desktop-Images-AD-Computerobjekte erstellt werden. Wenn Sie dieses Feld unausgefüllt lassen, werden alle Computerobjekte im AD-Container des Computers platziert.

4. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern** oder **Speichern und schließen**.

Verwandte Themen

Azure Active Directory – Definition von Begriffen

Konfigurieren von Entra Domain Services zur Verwendung mit AVD

VM beim Herstellen einer Verbindung für gepoolte Host-pools starten

Nerdio Manager ermöglicht es Ihnen, die Funktion „VM beim Herstellen einer Verbindung starten“ zu nutzen. Diese Funktion schaltet eine Sitzungshost-VM in einem Hostpool ein, in dem alle Sitzungshost-VMs derzeit ausgeschaltet sind. Wenn sich der User also anmeldet, wird eine VM eingeschaltet, um diesem User eine Sitzung bereitzustellen.

> **Anmerkung**
>
> Endbenutzer können eine Sitzungshost-VM auf mehr als eine Weise starten. Dies hängt von den Berechtigungen des Users ab.
>
> - **Erlauben Sie den Usern, einen Sitzungshost manuell zu starten, wenn keiner gestartet ist**: Dies ermöglicht es dem User, sich bei Nerdio Manager anzumelden und Dienstaktionen auszuführen. Zum Beispiel das Einschalten der Sitzungshosts innerhalb des Hostpools. Nur bestimmte User, die über die Berechtigungen zur Anmeldung bei Nerdio Manager verfügen, können die Sitzungshost-VM auf diese Weise starten.
> - **VM beim Herstellen einer Verbindung starten**: Die VM wird automatisch eingeschaltet, wenn der User eine Verbindung herstellt. Jeder User kann die VM starten, wenn er sich anmeldet.

So konfigurieren Sie „VM beim Herstellen einer Verbindung starten“ für gepoolte Hostpools:

1. Finden Sie den Hostpool, mit dem Sie arbeiten möchten.
2. Wählen Sie im Menü **Einstellungen** > **AVD**.
3. Wählen Sie die Option **VM beim Herstellen einer Verbindung starten** aus.
4. Wählen Sie **Speichern** oder **Speichern und schließen**.

Sitzungslimits für User konfigurieren

Nerdio Manager ermöglicht es Ihnen, Sitzungslimits auf einzelne Hostpools auf Hostpool-Ebene anzuwenden. Dies ermöglicht Ihnen Folgendes:

- Optimieren Sie Ihr AVD-Deployment und die automatische Skalierung.
- Schonen Sie Ressourcen, indem Sie User abmelden, die ihre Sitzungen offen lassen oder sich in einem getrennten Zustand befinden.

> **Anmerkung**
>
> - Standardmäßig ist die Option für Sitzungslimits deaktiviert. Sitzungslimits gelten nicht, und das System akzeptiert alle Änderungen, die User an einem einzelnen Image oder über die Gruppenrichtlinie vornehmen.
> - Nerdio Manager wendet Sitzungslimits durch lokale Richtlinienänderungen auf dem Sitzungshost-VM an. Sitzungsstatus werden vom Windows-Betriebssystem verwaltet und nicht von Nerdio Manager.

Um Sitzungszeitlimits einmalig zu definieren und in Hostpools wiederzuverwenden, erstellen Sie ein Profil für Sitzungszeitlimits. Weitere Informationen finden Sie unter Erstellen eines Profils für Sitzungszeitlimits.

So legen Sie die Sitzungslimits für User für vollständige Desktops fest:

1. Finden Sie den Hostpool, mit dem Sie arbeiten möchten.
2. Wählen Sie im Aktionsmenü **Einstellungen** > **Sitzungszeitlimits**.
3. Geben Sie die folgenden Informationen ein:
   - **Sitzungslimits für User aktivieren**: Schalten Sie diese Option **ein**.
   - **Getrennte Sitzungen abmelden nach**: Wählen Sie aus der Dropdown-Liste die Zeit aus, nach der getrennte User abgemeldet werden sollen.

> **Anmerkung**
>
> Standardmäßig können User die Verbindung zu einer AVD-Sitzung trennen, ohne sich abzumelden und die Sitzung zu beenden. Wenn sich eine Sitzung in einem getrennten Zustand befindet, bleiben ausgeführte Programme aktiv, auch wenn der User nicht mehr aktiv verbunden ist. Standardmäßig werden diese getrennten Sitzungen unbegrenzt lange auf dem Server gewartet.
>
> Wenn Sie diese Richtlinieneinstellung aktivieren, werden getrennte Sitzungen nach der angegebenen Zeitdauer vom Server gelöscht. Um das Standardverhalten zu erzwingen, dass getrennte Sitzungen unbegrenzt lange auf dem Server gewartet werden, wählen Sie **Nie**. Wenn Sie eine Konsolensitzung haben, gelten die Sitzungslimits für getrennte Sitzungen nicht.

- **Inaktive Sitzung trennen nach**: Wählen Sie aus der Dropdownliste den Maximalwert aus, wie lange eine aktive Sitzung ohne Benutzereingabe inaktiv sein kann, bevor sie automatisch getrennt wird.

  > **Anmerkung**
  >
  > Wenn Sie diese Richtlinieneinstellung aktivieren, wird die inaktive Sitzung nach der angegebenen Zeitdauer getrennt. Der User erhält zwei Minuten vor der Trennung der Sitzung eine Warnung, die es ihm ermöglicht, eine Taste zu drücken oder die Maus zu bewegen, um die Sitzung aktiv zu halten. Wenn Sie eine Konsolensitzung haben, gelten keine Zeitlimits für inaktive Sitzungen.

- **Aktive Sitzung trennen nach**: Wählen Sie aus der Dropdownliste die maximale Zeitdauer aus, die eine Sitzung aktiv sein kann, bevor sie automatisch getrennt wird. Die empfohlene Einstellung: **Nicht konfiguriert**.

> **Anmerkung**
>
> Wenn Sie diese Richtlinieneinstellung aktivieren, werden aktive Sitzungen nach der angegebenen Zeitdauer automatisch getrennt. Der User erhält zwei Minuten vor der Trennung der Sitzung eine Warnung, die es ihm ermöglicht, geöffnete Dateien zu speichern und Programme zu schließen. Wenn Sie eine Konsolensitzung haben, gelten keine Zeitlimits für aktive Sitzungen.

- **Leere RemoteApp-Sitzungen abmelden nach**: Wählen Sie aus der Dropdownliste die Zeitdauer aus, die eine RemoteApp-Sitzung eines User nach dem Schließen aller RemoteApp-Programme im getrennten Zustand verbleibt, bevor die Sitzung abgemeldet wird.

> **Anmerkung**
>
> Standardmäßig wird die Sitzung getrennt, aber nicht abgemeldet, wenn ein User ein RemoteApp-Programm schließt. Wenn ein User das letzte ausgeführte RemoteApp-Programm, das mit einer Sitzung verknüpft ist, schließt, verbleiben die RemoteApps in einem getrennten Zustand, bis das von Ihnen angegebene Zeitlimit erreicht ist. Wenn das angegebene Zeitlimit erreicht ist, wird die RemoteApp-Sitzung abgemeldet. Wenn der User ein RemoteApp-Programm startet, bevor das Zeitlimit erreicht ist, stellt der User eine Verbindung zur getrennten Sitzung auf der AVD-Sitzungshost-VM wieder her.
>
> Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird die Sitzung getrennt, aber nicht abgemeldet, wenn ein User das letzte RemoteApp-Programm schließt.

- **Abmelden statt Trennen von inaktiven und aktiven Sitzungen**: Wählen Sie aus der Dropdown-Liste die Option aus, um festzulegen, ob eine aktive oder inaktive Sitzung, deren Zeitlimit abgelaufen ist, beendet statt getrennt werden soll.

> **Anmerkung**
>
> Sie können diese Einstellung verwenden, um eine Sitzung abzumelden, nachdem Zeitlimits für aktive oder inaktive Sitzungen erreicht wurden. Standardmäßig werden Sitzungen getrennt (nicht abgemeldet), wenn sie ihre Zeitlimits erreichen.
>
> Wenn Sie diese Richtlinieneinstellung deaktivieren, werden inaktive und aktive Sitzungen, die ihr Zeitlimit erreichen, getrennt, auch wenn vom Serveradministrator etwas anderes festgelegt wurde.
>
> Diese Richtlinie gilt nur für Timeout-Limits, die explizit vom Admin festgelegt wurden. Diese Richtlinie gilt nicht für Timeout-Ereignisse, die aufgrund von Konnektivitäts- oder Netzwerkbedingungen auftreten.

- **Auf bestehende Hostpools anwenden**: Wählen Sie diese Option, um die geänderten Sitzungslimits auf bestehende Hostpools anzuwenden.
  - **VMs neustarten**: Wählen Sie diese Option, um Sitzungshost-VMs nach der Aktualisierung der Sitzungs-Timeouts neustarten.
  - **Verarbeiten Sie Hostpools in Gruppen von**: Geben Sie die Anzahl der gleichzeitigen Vorgänge beim Anwenden der Änderung ein.
  - **Anzahl der Fehler vor dem Abbruch**: Geben Sie die Anzahl der fehlgeschlagenen Aufgaben ein, bevor der Prozess beendet wird.
  - **Zeitplan**: Schalten Sie den Zeitplan ein, um die Änderungen zu einem ausgewählten Zeitpunkt anzuwenden.
    - **Startdatum**: Geben Sie das Startdatum ein.
    - **Zeitzone**: Wählen Sie aus der Dropdown-Liste die Zeitzone für die Startzeit aus.
    - **Startzeit**: Wählen Sie aus den Dropdown-Listen die Startzeit aus.
    - **Wiederholen**: Wählen Sie bei Bedarf aus der Dropdown-Liste den wiederkehrenden Zeitplan aus.

> **Anmerkung**
>
> Die Dropdown-Liste enthält die Option **After Patch Thursday**. Dies ermöglicht Ihnen das Erstellen eines wiederkehrenden Zeitplans auf Basis von Patch Thursday.

- **Tage danach**: Wenn Sie **After Patch Thursday** ausgewählt haben, geben Sie die Anzahl der Tage nach dem Patch Thursday ein, an denen die geplante Aufgabe ausgeführt werden soll.

4. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern** oder **Speichern und schließen**.

Remote-Anwendungen für User veröffentlichen

User werden oft in eine Cloud-Umgebung verschoben, weil eine Anwendung lokal nicht mehr ausgeführt werden kann. Es lassen sich jedoch große Kosteneinsparungen erzielen, indem man einfach eine oder mehrere Anwendungen remote ausführt. Dieser Leitfaden führt Sie durch das Wie und Warum der Einrichtung eines AVD-Hostpools mit Remote-Anwendungen.

Sie können Nerdio Manager verwenden, um Anwendungen (RemoteApp) innerhalb von Azure Virtual Desktop einfach zu veröffentlichen. Diese Anwendungen können bei Bedarf durch Application Groups eingeschränkt werden, wodurch Admins verschiedenen Usern vom selben Hostpool aus unterschiedliche Anwendungen bereitstellen können.

Was sind Remote-Anwendungen?

Wie der Name schon sagt, sind RemoteApp Anwendungen, die remote ausgeführt werden. Entgegen der landläufigen Meinung erfordern RemoteApps jedoch einen Multi-Session-AVD-Hostpool, um die Anwendung remote nutzen zu können. Sie installieren Ihre Anwendungen genau wie bei einer herkömmlichen Remote-Desktop-Lösung. Wenn Sie die Anwendung jedoch für Remote-User veröffentlichen, können Sie auswählen, auf welche Anwendungen der User Zugriff hat. Dies wird über Application Groups gesteuert.

> **Anmerkung**
>
> Wenn Sie Usern eine vollständige Desktop-Erfahrung anstelle von RemoteApp bereitstellen, können Sie den Zugriff der User auf Anwendungen mit FSLogix App Masking begrenzen.

Warum RemoteApp?

RemoteApp ist weniger ressourcenintensiv als eine vollständige Desktop-Erfahrung, wodurch Sie mehr User auf einem bestimmten Host unterbringen und somit Kosten senken können.

Was sind Application Groups?

In Azure Virtual Desktop (AVD) definieren Application Groups, worauf User innerhalb eines Hostpools zugreifen können – entweder auf einen vollständigen Desktop oder auf bestimmte Anwendungen. User können für einen flexiblen Zugriff mehreren Application Groups in verschiedenen Hostpools zugewiesen werden.

Es gibt die folgenden Typen:

- **Desktop**: Ermöglicht den Zugriff auf einen vollständigen Windows-Desktop (gepoolter oder persönlicher Hostpool).
- **RemoteApp**: Bietet Zugriff auf ausgewählte Anwendungen (nur gepoolter Hostpool).

Sie können beide Typen demselben gepoolten Hostpool zuweisen, jedoch nur eine Desktop-App-Gruppe pro Pool. Es können mehrere RemoteApp-Gruppen zugewiesen werden, und User sehen alle Anwendungen aus diesen Gruppen.

Wenn einem User im selben Pool sowohl eine Desktop-App-Gruppe als auch eine RemoteApp-Gruppe zugewiesen sind, sieht er nur den bevorzugten Typ der Application Group, basierend auf den Einstellungen des Pools.

Konfigurieren Sie Ihren Hostpool

Wie bereits erwähnt, benötigen Sie einen Multi-Session-Hostpool, um Remote-Anwendungen nutzen zu können. Idealerweise sollten Sie einen neuen

Hostpool erstellen. Wenn Sie jedoch bereits über einen bestehenden Hostpool verfügen, können Sie problemlos eine RemoteApp-Gruppe hinzufügen und/oder zu einer RemoteApp-Gruppe wechseln.

Bereitstellen Ihres Desktop-Images und Ihrer Hosts

Nachdem Sie Ihren Hostpool erstellt haben, erstellen oder aktualisieren Sie Ihr Desktop-Image und stellen es anschließend im Hostpool bereit. Weitere Informationen finden Sie unter Desktop-Images: als Image festlegen [63].

Hinzufügen von App-Gruppen zu Hostpools

App-Gruppen ermöglichen die Zuweisung von Usern und Gruppen zu Desktops und RemoteApps. Dies vereinfacht die Anwendungsverwaltung, da Anwendungen nach App-Gruppen statt nach einzelnen Benutzern verwaltet werden können.

> **Anmerkung**
>
> Einem Hostpool muss mindestens eine App-Gruppe zugeordnet sein.

So fügen Sie einem Hostpool eine App-Gruppe hinzu:

1. Wählen Sie den Hostpool aus, mit dem Sie arbeiten möchten.
2. Wählen Sie im Menü „Weitere Optionen“ ⋮ die Option **Verwalten** > **App-Gruppen**.
3. Geben Sie die folgenden Informationen ein:
   - **RemoteApp-App-Gruppen**: Geben Sie die Namen der App-Gruppen für RemoteApps ein.

     > **Anmerkung**
     >
     > Ein Hostpool kann über mehrere RemoteApp-App-Gruppen verfügen.

- **Desktop-App-Gruppe**: Geben Sie den Namen der Desktop-App-Gruppe ein.

> **Anmerkung**
>
> Ein Hostpool darf nur eine Desktop-App-Gruppe haben.

4. Sobald Sie die gewünschten Informationen eingegeben haben, wählen Sie **OK**.

Veröffentlichen von RemoteApps für User

RemoteApps bieten dem User die Möglichkeit, eine einzelne Anwendung zu starten, ohne die vollständige Desktop-Erfahrung starten zu müssen. Der User kann beispielsweise Excel starten, ohne sich bei einem Desktop anzumelden zu müssen. Dies spart Ressourcen auf dem Sitzungshost, da die User keinen vollständigen Desktop verwenden müssen. In unserem Excel-Beispiel könnten Sie also möglicherweise 10 User haben, die mit Excel als RemoteApp arbeiten. Hätten sich die User jedoch als vollständiger Desktop verbunden, hätte der Sitzungshost möglicherweise weniger User verarbeiten können. Das bedeutet, dass Sie zusätzliche Sitzungshosts bereitstellen müssten, um alle Excel-User zu verarbeiten.

Sie können RemoteApps mit den folgenden Methoden für User veröffentlichen:

- Veröffentlichen einer auf einem Host installierten Remoteanwendung für User [166]
- Veröffentlichen einer Remoteanwendung aus einem App Attach-Paket für User [169]
- Veröffentlichen einer Remoteanwendung über einen Dateipfad für User [170]

Veröffentlichen einer auf einem Host installierten Remoteanwendung für User

Nerdio Manager ermöglicht es Ihnen, auf einem Host installierte Anwendungen für Ihre User bereitzustellen.

So veröffentlichen Sie eine auf einem Host installierte Remoteanwendung für User:

1. Wählen Sie den Hostpool aus, mit dem Sie arbeiten möchten. Dies ist ein Hostpool, der für die Desktop-Erfahrung **RemoteApp (gepoolt)** konfiguriert ist.
2. Wählen Sie im Menü „Weitere Optionen“ ⋮ die Option **Anwendungen** > **RemoteApps**.
3. Wählen Sie **Neue RemoteApp**.

> **Anmerkung**
> - Beim Hinzufügen der RemoteApp muss der Host eingeschaltet sein und die Anwendungen, die Sie veröffentlichen möchten, müssen bereits installiert sein.
> - Wenn der Hostpool über mehrere RemoteApp-App-Gruppen verfügt, muss eine bestimmte RemoteApp-App-Gruppe ausgewählt werden. Durch das Veröffentlichen verschiedener Anwendungen in verschiedenen App-Gruppen können Administratoren den Zugriff auf diese Anwendungen über die Gruppenmitgliedschaft steuern. Dies ermöglicht es, User-Gruppen verschiedene Anwendungen aus demselben Hostpool bereitzustellen.

4. Geben Sie im Dialogfeld **App-Gruppe auswählen** die folgenden Informationen ein:
   - Wählen Sie aus der Dropdownliste die App-Gruppe aus.
   - Wählen Sie **OK** aus.
5. Geben Sie im Dialogfeld **Anwendung veröffentlichen** die folgenden Informationen ein:
   - **Anwendungsquelle**: Wählen Sie aus der Dropdown-Liste **Auf Host installiert** aus.

Anmerkung

Anmerkung

Hinweis: Sie können einen der folgenden Anwendungsquelltypen auswählen:Auf Host installiert: Die Apps sind lokal auf der Sitzungshost-VM installiert. App Attach-Paket: Ein MSIX App Attach-Paket. Dateipfad: Sie können einen spezifischen Dateipfad zur Zielanwendung auswählen. Dies kann in Szenarien hilfreich sein, in denen die Zielanwendung sich nicht selbst beim Windows-Installer registriert oder in denen portable Anwendungen erforderlich sind.

- **Anwendung**: Wählen Sie die Anwendung aus der Dropdown-Liste aus.
- **Name**: Geben Sie den Namen der RemoteApp ein.

Anmerkung

Der **Name** ist für den Benutzer sichtbar, sofern er nicht durch den **Anzeigenamen** überschrieben wird.

- **Anzeigename**: Geben Sie optional den Anzeigenamen ein, der für den Benutzer sichtbar ist.
- **Beschreibung**: Geben Sie die Beschreibung ein, die für den Admin sichtbar ist.
- **Dateipfad**: Geben Sie den Pfad zur ausführbaren Anwendungsdatei auf dem Sitzungshost ein.
- **Symbolpfad**: Geben Sie optional den Pfad zu einer Symboldatei ein, die für diese RemoteApp verwendet werden soll, wenn sie im Remote Desktop-Feed des Benutzers erscheint.
- **Symbolindex**: Geben Sie optional den numerischen Symbolindex in der Symboldatei ein.
- **Befehlszeileneinstellung**: Wählen Sie diese Option, um eine Befehlszeileneinstellung zu erfordern.

- **Befehlszeile**: Geben Sie die Befehlszeile ein, die beim Starten der RemoteApp an die ausführbare Datei übergeben werden soll.

6. Sobald Sie die gewünschten Informationen eingegeben haben, wählen Sie **OK**.

Die autorisierten Hostpool-Benutzer müssen nun der RemoteApp-Gruppe zugewiesen werden, die die neu veröffentlichte RemoteApp enthält.

> **Anmerkung**
>
> - Hostpool-Benutzer werden nicht automatisch den RemoteApp-Gruppen dieses Hostpools zugewiesen. Jeder Benutzer muss der entsprechenden RemoteApp-Gruppe einzeln zugewiesen werden.
> - Über das Aktionsmenü können Sie veröffentlichte Apps **bearbeiten** oder **löschen**.

Veröffentlichen Sie eine RemoteApp aus einem App Attach-Paket für User.

Nerdio Manager ermöglicht es Ihnen, App Attach-paketierte Anwendungen an Ihre User bereitzustellen.

So veröffentlichen Sie eine RemoteApp aus einem App Attach-Paket für User:

1. Wählen Sie den Hostpool aus, mit dem Sie arbeiten möchten. Dies ist ein Hostpool, der für die **RemoteApp (gepoolt)** Desktop-Erfahrung konfiguriert ist.
2. Wählen Sie im Menü „Weitere Optionen“ ⋮ die Option **Anwendungen** > **RemoteApps**.
3. Wählen Sie **Neue RemoteApp**.
4. Geben Sie im Dialogfeld **App-Gruppe auswählen** die folgenden Informationen ein:
   - Wählen Sie aus der Dropdownliste die App-Gruppe aus.
   - Wählen Sie **OK** aus.

5. Geben Sie im Dialogfeld **Anwendung veröffentlichen** die folgenden Informationen ein:
   - **Anwendungsquelle**: Wählen Sie aus der Dropdown-Liste **App Attach-Paket** aus.
   - **App Attach-Paket**: Wählen Sie das App Attach-Paket aus der Dropdown-Liste aus.
   - **MSIX-Anwendung**: Wählen Sie aus der Dropdown-Liste die MSIX-Anwendung aus.
   - **Anzeigename**: Geben Sie optional den Anzeigenamen ein, der für den User sichtbar ist.
   - **Beschreibung**: Geben Sie die Beschreibung ein, die für den Administrator sichtbar ist.
   - **Symbolpfad**: Geben Sie optional den Pfad zu einer Symboldatei ein, die für diese RemoteApp verwendet werden soll, wenn sie im Remote-Desktop-Feed des Users erscheint.
   - **Symbolindex**: Geben Sie optional den numerischen Symbolindex in der Symboldatei ein.
6. Sobald Sie die gewünschten Informationen eingegeben haben, wählen Sie **OK**.

Veröffentlichen Sie eine RemoteApp von einem Dateipfad für User

Nerdio Manager ermöglicht Ihnen die Bereitstellung von Anwendungen von einem Dateipfad für Ihre User.

So veröffentlichen Sie eine RemoteApp von einem Dateipfad für User:

1. Wählen Sie den Hostpool aus, mit dem Sie arbeiten möchten. Dies ist ein Hostpool, der für die **RemoteApp (gepoolt)** Desktop-Erfahrung konfiguriert ist.
2. Wählen Sie im Menü „Weitere Optionen“ ⋮ die Option **Anwendungen** > **RemoteApp**.
3. Wählen Sie **Neue RemoteApp**.
4. Geben Sie im Dialogfeld **App-Gruppe auswählen** die folgenden Informationen ein:
   - Wählen Sie aus der Dropdownliste die App-Gruppe aus.
   - Wählen Sie **OK** aus.

5. Geben Sie im Dialogfeld **Anwendung veröffentlichen** die folgenden Informationen ein:
   - **Anzeigename**: Geben Sie optional den Anzeigenamen ein, der für den User sichtbar ist.
   - **Beschreibung**: Geben Sie die Beschreibung ein, die für den Administrator sichtbar ist.
   - **Dateipfad**: Geben Sie den Pfad zur ausführbaren Anwendung auf dem Sitzungshost ein
   - **Symbolpfad**: Geben Sie optional den Pfad zu einer Symboldatei ein, die für diese RemoteApp verwendet werden soll, wenn sie im Remote-Desktop-Feed des Users erscheint.
   - **Symbolindex**: Geben Sie optional den numerischen Symbolindex in der Symboldatei ein.
   - **Befehlszeileneinstellung**: Wählen Sie diese Option, um eine Befehlszeileneinstellung zu erfordern.
   - **Befehlszeile**: Geben Sie die Befehlszeile ein, die beim Starten der RemoteApp an die ausführbare Datei übergeben werden soll
6. Sobald Sie die gewünschten Informationen eingegeben haben, wählen Sie **OK**.

Verwandte Themen

Wartungsmodus für Remote-Anwendungen

Schritt 4: Speicher

Sobald Ihre Hostpools in Betrieb sind, besteht der nächste Schritt darin, den Speicher für User-Daten und -Profile zu konfigurieren. Nerdio Manager arbeitet sowohl mit Azure Files als auch mit Azure NetApp Files zusammen: nativen Azure-Diensten, die häufig anstelle einer dedizierten Datei-Server-VM verwendet und oft mit einer Profilverwaltungslösung wie FSLogix kombiniert werden.

Sie können Nerdio Manager mit einer vorhandenen Azure Files- oder Azure NetApp Files-Datenfreigabe verlinken oder Nerdio Manager eine neue für Sie erstellen und konfigurieren lassen, einschließlich Berechtigungen und Domain Join. Nerdio Manager kann beide Speichertypen außerdem automatisch skalieren. So bezahlen Sie nur für die Kapazität, die Sie tatsächlich nutzen, statt im Voraus Überkapazitäten bereitzustellen.

In diesem Abschnitt:

1. Für den Domain Join einer Azure Files-Datenfreigabe erforderliche Berechtigungen (Active Directory) [172]
2. Konfigurierte Azure Files-Datenfreigaben erstellen und verwalten [176]
3. Auto-scale für Azure Files Storage Premium [186]
4. Auto-scale-Verlauf für Azure Files-Datenfreigaben [199]
5. Erstellen und Verwalten von konfigurierten Azure NetApp Files [202]
6. Auto-scale für Azure NetApp Files [205]
7. Auto-scale-Verlauf für Azure NetApp-Datenfreigaben [209]

Erforderliche Berechtigungen zum Verbinden einer Azure Files-Freigabe mit einer Domäne (Active Directory)

Dieser Artikel erläutert die Berechtigungen, die für ein delegiertes Domänenbenutzer-Dienstkonto ohne Administratorrechte erforderlich sind, das verwendet wird, um eine Azure Files-Freigabe mit einer Active Directory-Domäne zu verbinden. Wenn diese Berechtigungen nicht korrekt sind, erhalten Sie während des Schritts zum Domänenbeitritt eine Fehlermeldung. Fehler können unter anderem „Zugriff verweigert“ oder „Ein erforderliches Privileg wird vom Client nicht gehalten“ umfassen.

Dies gilt nicht für Entra Domain Services-Umgebungen. Entra Domain Services-Umgebungen benötigen lediglich das aktivierte Feature und müssen der Domäne nicht als spezielles Dienstkonto beitreten. Stellen Sie in Nerdio Manager sicher, dass Sie in der Dropdown-Liste **Join to AD** die Option **Entra Domain Services** auswählen.

Anmerkung

Zur Vereinfachung der Bereitstellung können Sie einen Domänenadministrator verwenden oder das delegierte Dienstkonto vorübergehend auf Domänenadministratorrechte erweitern.

Ein Domänenadministratorkonto reicht aus, um die Azure Files-Freigabe mit Ihrer Domäne zu verbinden. Wenn Sie jedoch ein Dienstkonto verwenden und diesem Konto bestimmte Berechtigungen delegieren, *reichen die für AVD-Sitzungshosts verwendeten delegierten Berechtigungen „Computerkonten hinzufügen/entfernen“ nicht aus, um Azure Files-Freigaben hinzuzufügen*.

Anmerkung

- Der Domänenbeitrittsprozess für Azure Files muss im Kontext eines Domänenbenutzers ausgeführt werden. Nerdio Manager schließt diesen Prozess unter Verwendung der bereitgestellten Domänenadministrator-Anmeldedaten oder Benutzeranmeldedaten ab, denen nach den unten aufgeführten Schritten ausreichende Berechtigungen delegiert wurden. Wenn Sie keine Domänenadministrator-Anmeldedaten verwenden oder wenn der Domänenadministrator-Benutzer keine **lokalen** Administratorrechte erhält, kann die Automatisierung von Nerdio Manager den Domänenbeitritt möglicherweise nicht abschließen.
- Damit Nerdio Manager diese Befehle als der angegebene Benutzer ausführen kann, ist ein Befehl zum Ändern des Benutzerkontexts erforderlich. Damit dies erfolgreich ist, müssen dem angegebenen Benutzer die **lokalen** Administratorrechte auf der temporären VM gewährt werden, die von Nerdio Manager bereitgestellt wird, um diesen Prozess abzuschließen. Wenn der angegebene User nicht über lokale Adminrechte verfügt, erhalten Sie möglicherweise eine Fehlermeldung mit dem Hinweis *„Verbindung zum Remote-Server azfilestmp-* fehlgeschlagen mit der folgenden Fehlermeldung: Zugriff verweigert.“* Bitte stellen Sie sicher, dass dem angegebenen Userkonto lokale Administratorrechte (nur für die azfilestmp-* VM) gewährt werden.
- Domänen-Adminrechte (oder delegierte Rechte) sind eine Anforderung für das Azure Files-Domain Join-Modul. Lokale Adminberechtigungen sind nur erforderlich, damit Nerdio Manager den Domain Join-Prozess automatisch ausführen kann.

Azure Files tritt der Domäne als delegiertes Dienstprinzipal-Userobjekt bei. Um das Azure Files Storage-Konto der Domäne beizutreten, benötigt das bereitgestellte Dienstkonto Berechtigungen für die Ziel-Organisationseinheit (OU), die das Erstellen und Schreiben neuer Userobjekte ermöglichen. Darüber hinaus benötigt das Dienstkonto auch die Berechtigung, das Azure Files-Anmeldekonto als delegierten Dienst festzulegen. Standardmäßig wird dieses Privileg nur AD-Domänen-Admins gewährt.

Berechtigung zum Erstellen von Userobjekten delegieren

Das folgende Verfahren beschreibt, wie Sie die Berechtigung zum Erstellen und Schreiben von Userobjekten mithilfe von Active Directory-Benutzer und -Computer (ADUC oder dsa.msc) delegieren.

So delegieren Sie die Berechtigung zum Erstellen von Userobjekten:

1. Finden Sie die OU, in der Azure Files beigetreten werden soll.
2. Klicken Sie mit der rechten Maustaste auf die OU und wählen Sie **Steuerung delegieren** aus.
3. Fügen Sie das Dienstkonto hinzu, das für den Beitritt von Azure Files zur Domäne verwendet werden soll.
4. Delegieren Sie Berechtigungen zum **Erstellen, Löschen und Verwalten von Userkonten**.
5. Wählen Sie **Fertig stellen** aus, um die Änderungen anzuwenden.

Berechtigung zum Erstellen delegierter User delegieren

Das folgende Verfahren beschreibt, wie Sie dem Dienstkonto, das für den Beitritt von Azure Files zur Domäne verwendet wird, erlauben, das neue Objekt für Azure Files als delegierten Dienst zu markieren. Dies erfordert das Ändern des Gruppenrichtlinienobjekts „Standard-Domänencontroller“ in der Gruppenrichtlinienverwaltung (gpmc.msc).

So löschen Sie die Berechtigung zum Erstellen delegierter User:

1. Klicken Sie mit der rechten Maustaste auf die Richtlinie für den Standard-Domänencontroller und wählen Sie **bearbeiten**.
2. Navigieren Sie zu **Computerkonfiguration** > **Richtlinien** > **Windows-Einstellungen** > **Sicherheitseinstellungen** > **Lokale Richtlinien** > **Zuweisung von Benutzerrechten**.
3. Finden Sie die Richtlinie **Computer- und Benutzerkonten dürfen für die Delegierung als vertrauenswürdig eingestuft werden**.
4. Fügen Sie der Richtlinie den Namen des Dienstkontos hinzu, das für den Beitritt von Azure Files zur Domäne verwendet wird.
5. Schließen Sie den Editor.
6. Führen Sie **gpupdate /force** auf allen Domänencontroller aus.

> **Anmerkung**
>
> Die Änderung der Richtlinie kann nach Abschluss von gpupdate einige Minuten dauern, bis sie angewendet wird.

Fügen Sie das Dienstkonto in Nerdio Manager hinzu.

Sie müssen das Dienstkonto unter AD-Profile in Nerdio Manager angeben. Weitere Informationen finden Sie unter Entra ID Join-Feature.

Konfigurierte Azure Files-Datenfreigaben erstellen und verwalten

Die Seite **Azure Files** enthält eine Liste aller konfigurierten und verknüpften Azure Files-Datenfreigaben. Sie können verschiedene Aktionen für die Azure Files-Datenfreigaben ausführen, wie z. B. das Erstellen, Verknüpfen oder Verwalten von Datenfreigaben. Dies umfasst Optionen wie Autoscaling, Verknüpfung aufheben, Festlegen/Ändern von Berechtigungen, Schließen von Dateihandles und Kopieren des Azure Files-UNC-Pfads.

Verknüpfung mit einer bestehenden Azure Files-Datenfreigabe herstellen

Nerdio Manager ermöglicht es Ihnen, eine Verknüpfung mit einer bestehenden Azure Files-Datenfreigabe herzustellen.

So stellen Sie eine Verknüpfung mit einer bestehenden Azure Files-Datenfreigabe her:

1. Navigieren Sie zu **Cloud-Desktop** > **Speicher** > **Azure Files**.
2. Wählen Sie **Link Azure Files**.
3. Geben Sie die folgenden Informationen ein:
   - **Storage-Konto**: Wählen Sie das Storage-Konto aus der Dropdown-Liste aus.
   - **Datenfreigabe**: Wählen Sie die Datenfreigabe aus der Dropdown-Liste aus.
4. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

Nach wenigen Augenblicken wird die Azure Files-Datenfreigabe zu Nerdio Manager hinzugefügt.

Erstellen einer neuen Azure Files-Datenfreigabe und/oder eines neuen Storage-Kontos

Nerdio Manager ermöglicht es Ihnen, eine neue Azure Files-Datenfreigabe und/oder ein neues Storage-Konto zu erstellen.

Netzwerkanforderungen

Um eine ordnungsgemäße Konnektivität zu Azure Files-Freigaben sicherzustellen, stellen Sie sicher, dass die folgenden Ports geöffnet sind.

Die zusätzlichen Ports können für Azure Government-Umgebungen gelten.

Port	Protokoll	Zweck
53	TCP/UDP	DNS-Namensauflösung für Active Directory
88	TCP/UDP	Kerberos-Authentifizierung (für AD DS-Integration)
135	TCP RPC	Endpoint Mapper (für AD DS-Integration)
389	TCP/UDP	LDAP für die Kommunikation mit dem Domänencontroller (für AD DS-Integration)
443	TCP HTTPS	REST-API-Zugriff, Azure Files-Synchronisierung, SMB über QUIC
445	TCP	SMB-Datenfreigabezugriff
636	TCP	Sicheres LDAP (LDAPS)
2049	TCP	NFS-Protokollzugriff
3268	TCP	Globaler Katalog (LDAP)
3269	TCP	Sicherer globaler Katalog (LDAPS)
49152–65535	TCP	Dynamische RPC-Ports (für AD DS-Integration)

So erstellen Sie eine neue Azure Files-Datenfreigabe und/oder ein neues Storage-Konto:

1. Navigieren Sie zu **Cloud-Desktop** > **Speicher** > **Azure Files**.
2. Wählen Sie **Azure Files hinzufügen**.
3. Geben Sie die folgenden Informationen ein:
   - **Storage-Konto**: Geben Sie zum Erstellen eines neuen Storage-Kontos einen Namen ein, der global eindeutig ist, maximal 24 Zeichen enthält und nur Kleinbuchstaben und Zahlen verwendet (keine Sonderzeichen oder Leerzeichen). Wählen Sie dann unter dem Feld **[*Ihr Kontoname*]**

als neues Storage-Konto erstellen aus. Um ein vorhandenes Storage-Konto zu verwenden, wählen Sie es aus der Dropdown-Liste aus.

> **Anmerkung**
>
> Wenn der Name diese Anforderungen nicht erfüllt, wird die Option **Erstellen** nicht angezeigt und es wird keine Validierungsmeldung ausgegeben.

- **Beschreibung des Storage-Kontos**: Geben Sie die Beschreibung des Storage-Kontos ein.
- **Leistung**: Wählen Sie aus der Dropdownliste die Leistungsstufe für die Datenfreigabe aus.

> **Anmerkung**
>
> Premium-Storage-Konten werden durch Solid-State-Laufwerke unterstützt und bieten eine konsistente Leistung mit geringer Latenz. Sie können nur mit den Datenträgern virtueller Maschinen in Azure verwendet werden und eignen sich insbesondere für I/O-intensive Anwendungen, wie z. B. Datenbanken. Darüber hinaus qualifizieren sich virtuelle Maschinen, die Premium-Storage für alle Datenträger verwenden, für eine SLA von 99,9 %, selbst wenn sie außerhalb einer Verfügbarkeitsgruppe ausgeführt werden. Diese Einstellung kann nach der Erstellung des Storage-Kontos nicht mehr geändert werden.

-

> **Tipp**
>
> Wir empfehlen dringend, für die beste Benutzererfahrung **Premium** auszuwählen.

- **Replikation**: Wählen Sie aus der Dropdownliste den Typ der Speicherreplikation aus.

> **Anmerkung**
>
> Weitere Informationen finden Sie unter Azure Storage-Redundanz.

- **Azure Files-Datenfreigabe**: Geben Sie den Namen der Datenfreigabe ein.
- **Beschreibung der Dateifreigabe**: Geben Sie die Beschreibung der Datenfreigabe ein.
- **Bereitgestellte Kapazität (GiB)**: Geben Sie die Größe der bereitgestellten Kapazität ein.

4. Geben Sie die folgenden Informationen im Abschnitt **Konfiguration des Storage-Kontos** ein:
   - **Freigabeberechtigungen**: Wählen Sie diese Option, um Standard-Freigabeberechtigungen für das Storage-Konto festzulegen.

> **Anmerkung**
>
> - Mit der Berechtigung **SMB Share Contributor** erhalten alle authentifizierten Benutzer Lese-/Schreibzugriff auf die Datenfreigabe.
> - **SMB Share Reader** kann verwendet werden, um allen authentifizierten Benutzern Lesezugriff auf die Datenfreigabe zu gewähren (z. B. MSIX App Attach).
>
> Weitere Informationen finden Sie unter Berechtigungen auf Freigabeebene für alle authentifizierten Identitäten.

   - **Beitritt zu AD oder Entra ID**: Wählen Sie diese Option und anschließend aus der Dropdown-Liste ein Entra ID- oder AD-Profil aus, um der Datenfreigabe direkt beizutreten.
   - **Computer-verbundene Datenfreigabe erstellen**: Wählen Sie diese Option, um Azure Files-Speicherkonten mit AD zu verbinden, indem Sie entweder ein Benutzerobjekt oder ein Computerobjekt in Active Directory erstellen.

> **Anmerkung**
>
> Wir empfehlen, für den Domain-Join-Prozess ein User-Objekt zu verwenden. Vergewissern Sie sich, dass keine Richtlinien in Kraft sind, durch die das Konto deaktiviert oder entfernt oder durch die sein Passwort zurückgesetzt wird. Wird ein Computerobjekt ausgewählt, muss das Konto von jedem automatisierten Bereinigungsprozess ausgeschlossen werden. Alle Datenfreigaben werden mit aktivierter AES256-Verschlüsselung erstellt.

- **SMB Multichannel aktivieren**: Zur Aktivierung auswählen.

> **Anmerkung**
>
> Azure Files SMB Multichannel ermöglicht es Clients, mehrere Netzwerkverbindungen zu nutzen, was die Leistung steigert. Die Leistungssteigerung wird durch Bandbreitenbündelung über mehrere Netzwerkkarten (NICs) und die Nutzung der Receive Side Scaling (RSS)-Unterstützung für Netzwerkkarten erreicht, um die E/A-Last auf mehrere CPUs zu verteilen.

5. Geben Sie die folgenden Informationen im Abschnitt **Datenfreigabenkonfiguration** ein:
   - **Berechtigungen (SMB Share Contributors)**: Geben Sie Benutzer und Gruppen an, denen die Rolle 'Storage File Data SMB Share Contributor' für die Datenfreigabe zugewiesen ist.
   - **Benutzer/Gruppen aus Hostpools hinzufügen**: Wählen Sie aus der Dropdown-Liste Benutzer und Gruppen aus, die derzeit den Hostpools zugewiesen sind, um ihnen die Rolle 'Storage File Data SMB Share Contributor' für die Datenfreigabe zu erteilen.

- > **Anmerkung**
  >
  > Um eine Azure Files-Freigabe als Speicherort für FSLogix-Profile und MSIX App Attach-Images zu verwenden, muss das Speicherkonto in Active Directory, Entra Domain Services oder Entra ID integriert sein. Wenn Sie sich entscheiden, das Storage-Konto nicht mit Active Directory oder Entra ID zu verbinden, können Sie dies später nachholen. Das Verbinden des Storage-Kontos mit Active Directory erstellt eine temporäre VM und verwendet die Anmeldedaten des Active Directory-Profils, um das Storage-Konto als Computerobjekt im ausgewählten Active Directory hinzuzufügen. Die Integration des Storage-Kontos mit Entra Domain Services setzt das entsprechende Flag in Azure. Die Entra Domain Services-Profil-Anmeldedaten sind erforderlich, um eine temporäre VM zu erstellen, die in Domäne eingebunden wird und die AES-256-Verschlüsselung aktiviert. Das Verbinden des Storage-Kontos mit Entra ID erstellt die erforderliche App-Registrierung und bietet Ihnen die Möglichkeit, die benötigte Zustimmung zu erteilen.

- **NTFS-Berechtigungen auf Dateiebene zuweisen**: Wählen Sie diese Option, damit Nerdio Manager NTFS-Berechtigungen auf Dateiebene für neu erstellte Datenfreigaben zuweist.

  > **Anmerkung**
  >
  > - Dies erfolgt zusätzlich zur Zuweisung der oben ausgewählten Azure RBAC-Rollen.
  > - Dieser Prozess erstellt automatisch eine temporäre VM, um die Aufgabe der Zuweisung von Berechtigungen auszuführen.
  > - Weitere Informationen zu den Standard-Berechtigungen auf Dateiebene für neue Azure Files-Datenfreigaben finden Sie in diesem Microsoft-Artikel.

- **App Attach**: Wählen Sie diese Option, um authentifizierten Benutzern Leseberechtigung für Unterverzeichnisse in der Datenfreigabe zu

erteilen. Dies wird für Freigaben empfohlen, die App Attach-Anwendungen enthalten.

- **FSLogix**: Wählen Sie diese Option, um authentifizierten Benutzern die Berechtigung zum Ändern für das Stammverzeichnis der Datenfreigabe zu erteilen, was die Erstellung von FSLogix-Profilordnern ermöglicht.

> **Anmerkung**
>
> Dies wird für Datenfreigaben empfohlen, die FSLogix-Profile enthalten.

6. **Erweiterte Einstellungen anzeigen**: Um Azure Files mit dem Active Directory zu verbinden, erstellt Nerdio Manager eine temporäre VM, um den Vorgang auszuführen. Wählen Sie die Einstellungen aus, die für diese temporäre VM verwendet werden sollen.

> **Tipp**
>
> Wir empfehlen dringend, Nerdio Manager bei der Erstellung der temporären VM die Standardeinstellungen verwenden zu lassen. Das heißt, wir empfehlen, die erweiterten Einstellungen nicht zu verwenden.

7. **Tags anwenden**: Geben Sie optional den **Name** und den **Wert** des Azure-Tags ein, das auf die Azure Files-Datenfreigabe angewendet werden soll.
8. Wählen Sie **OK**, um die Konfiguration zu speichern.

> **Anmerkung**
>
> Sie können mehrere Tags angeben. Weitere Informationen zur Verwendung von Tags zur Organisation Ihrer Azure-Ressourcen finden Sie in diesem Microsoft-Artikel.

Konfigurierte Azure Files-Datenfreigaben verwalten

Nerdio Manager ermöglicht Ihnen die Verwaltung vorhandener Azure Files-Datenfreigaben.

So verwalten Sie konfigurierte Azure Files-Datenfreigaben:

1. Navigieren Sie zu **Cloud Desktops** > **Storage** > **Azure Files**.
2. Finden Sie die Azure Files-Dateifreigabe, die Sie verwalten möchten.
3. Das Aktionsmenü ermöglicht Ihnen die Ausführung der folgenden Funktionen:
   - **Speicherkonto verwalten**: Ermöglicht Ihnen die Aktivierung der Entra ID-Hostunterstützung. Weitere Informationen finden Sie unter Entra ID-verbundene Hostunterstützung aktivieren [184].
   - **Auto-scale**: Weitere Informationen finden Sie unter Auto-scale für Azure Files Premium-Speicher [186].
   - **Datei-Handles**: Dateien entsperren/Geöffnete Datei-Handles schließen.
   - **FSLogix-Profile erzwingen**: Dies erzwingt eine Erfassung von FSLogix-Daten auf allen verknüpften Dateifreigaben.
   - **UNC-Pfad kopieren**: Kopieren Sie den UNC-Pfad in die Zwischenablage.
   - **Verknüpfung aufheben**: Entfernen Sie die Azure Files-Dateifreigabe von Nerdio Manager.
   - **FSLogix-Profile löschen**: Löschen Sie ein ausgewähltes FSLogix-Profil.
   - **FSLogix-Profile wiederherstellen**: Stellen Sie ein ausgewähltes FSLogix-Profil wiederher, das zuvor gelöscht wurde.
4. Wählen Sie im Aktionsmenü **Verwalten**, um die Parameter und Berechtigungen der Azure Files-Dateifreigabe zu ändern.

So erfassen Sie FSLogix-Daten in großen Mengen:

Nerdio Manager ermöglicht Ihnen die Auswahl mehrerer Dateifreigaben, sodass Sie FSLogix-Daten in großen Mengen und on demand erfassen können.

1. Navigieren Sie zu **Cloud Desktops** > **Storage** > **Azure Files**.
2. Wählen Sie die Datenfreigaben aus, für die Sie FSLogix-Daten erfassen möchten.

3. Wählen Sie im Menü **Bulk-Aktion** die Option **Sammeln von FSLogix-Profilen für ausgewählte Datenfreigaben erzwingen (x)**.

> **Anmerkung**
>
> Das **(x)** gibt die Anzahl der Azure Files-Datenfreigaben an, auf die die Bulk-Aktion angewendet wird. Im Beispiel wurden 4 Azure Files-Datenfreigaben ausgewählt.

Unterstützung für in Entra ID eingebundene Hosts aktivieren

In Entra ID eingebundene Hosts können jetzt von der Verwendung von App Attach-Anwendungen profitieren, was die Optionen für die Anwendungsbereitstellung erweitert.

Voraussetzungen

- Sie sollten mit App Attach vertraut sein. Weitere Informationen finden Sie in diesem Microsoft-Artikel App attach und MSIX app attach in Azure Virtual Desktop.

Nützliche Informationen

App Attach unterstützt die folgenden Identitätsanbieter:

- Microsoft Entra ID
- Active Directory Domain Services (AD DS)

Standard-NTFS-Berechtigungen für Dateifreigaben:

- BUILTIN\\Administrators:(OI)(CI)(F)
- BUILTIN\Users:(RX)
- BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
- NT AUTHORITY\\Authenticated Users:(OI)(CI)(M)
- NT AUTHORITY\\SYSTEM:(OI)(CI)(F)
- NT AUTHORITY\\SYSTEM:(F)
- CREATOR OWNER:(OI)(CI)(IO)(F)

NTFS-Berechtigungen für Datenfreigaben für App Attach:

- BUILTIN\Users:(RX)
- BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
- NT AUTHORITY\\Authenticated Users:(OI)(CI)(M)
- CREATOR OWNER:(OI)(CI)(IO)(F)

Einsatzbereich

Hosts, die App Attach verwenden sollen, sind in Microsoft Entra ID eingebunden

Die einzige zwingende Voraussetzung für das Funktionieren von App Attach auf solchen Hosts ist, dass das Speicherkonto, in dem die App Attach-Images gespeichert sind, im selben Abonnement vorhanden ist und über eine **Reader and Data Access**-Rollenzuweisung mit den Mitgliedern **Azure Virtual Desktop** und **Windows Virtual Desktop ARM Provider** verfügt. Das Speicherkonto kann in einen beliebigen Identitätsanbieter (Microsoft Entra ID, AD DS) integriert oder überhaupt nicht integriert sein.

Hosts, die App Attach verwenden sollen, sind in AD DS eingebunden

Zwingende Voraussetzungen:

- Das Speicherkonto, in dem App Attach-Images gespeichert sind, ist in AD DS eingebunden
- App Attach NTFS-Berechtigungen sind auf der Datenfreigabe konfiguriert
- Berechtigungen auf Freigabeebene sind konfiguriert

Variationen der Konfiguration von Berechtigungen auf Freigabeebene:

- **Schreibgeschützter Zugriff für alle authentifizierten Identitäten**: Standardberechtigung auf Freigabeebene mit mindestens der Rolle **Storage File Data SMB Share Reader** für alle authentifizierten Identitäten im Speicherkonto.
- **Schreibgeschützter Zugriff für Domänencomputer**:

  1. Erstellen Sie in Active Directory eine neue globale Sicherheitsgruppe in einer Organisationseinheit (OU), die mit ADConnect mit Entra ID synchronisiert wird.
  2. Fügen Sie die Domänencomputer der neuen Gruppe hinzu.
  3. Fügen Sie die neu erstellte Sicherheitsgruppe mit mindestens der Rolle **Storage File Data SMB Share Reader** über die Zugriffssteuerung im Azure-Portal zur Datenfreigabe hinzu.

- Einige benutzerdefinierte Konfigurationen.

Verwandte Themen:

- Erstellen und Verwalten konfigurierter Azure NetApp Files [202]

Auto-scale für Azure Files-Speicher

Azure Files Premium-Speicher unterstützt zwei Generationen von Datenfreigaben, die jeweils unterschiedlich abgerechnet – und automatisch skaliert – werden:

- **Provisioned V1**: Abrechnung nur nach bereitgestellter Datenfreigabegröße, unabhängig von der genutzten Kapazität. Die Größe der Datenfreigaben kann zwischen 100 GiB und 102.400 GiB liegen. E/A- und Netzwerkbandbreitenlimits skalieren automatisch mit der bereitgestellten Größe, sind jedoch nicht separat konfigurierbar.
- **Provisioned V2**: Abrechnung nach drei unabhängig bereitgestellten Werten – Datenfreigabegröße, IOPS und Durchsatz. Azure unterstützt Datenfreigabegrößen von bis zu 262.144 GiB. Im Feld **Maximales Vorgabenlimit** wird derzeit jedoch nur ein Maximalwert von 102.400 GiB akzeptiert. Diese bekannte Produkteinschränkung wird voraussichtlich in einer zukünftigen Version behoben. Die bereitgestellten IOPS reichen von 3.000 bis 102.400 und der bereitgestellte Durchsatz von 100 bis 10.340 MiB/s. Die Abrechnungssätze für alle drei hängen von der Region und weiteren Parametern ab. Einzelheiten finden Sie unter Azure Files-Preise.

Ist Auto-scale für Speicher aktiviert, erhöht die Funktion die bereitgestellten Werte bei geplantem Bedarf (siehe **Geplante Vorgabenerhöhung** / **Geplante Leistungserhöhung**) oder gemessener Speicherlatenz (siehe **Skalierungslogik**). Auto-scale senkt die Werte auch, um Kosten zu sparen, wenn die zusätzliche Leistung nicht mehr benötigt wird. Jeder Wert kann jedoch erst 24 Stunden nach seiner letzten Erhöhung gesenkt werden. Für Erhöhungen gibt es keine Wartezeit.

Mit Auto-scale für Speicher in Azure Files können Sie auch eine festgelegte Kapazitätsreserve vorhalten, damit der Speicherplatz auf der Datenfreigabe nicht knapp wird.

Anmerkung

Auto-scale ist für Azure Files-Datenfreigaben mit nutzungsabhängiger Abrechnung (Standard, nicht bereitgestellt) nicht verfügbar. Diese Datenfreigaben werden nach genutzter Kapazität und Transaktionen abgerechnet, nicht nach bereitgestellten Werten. Auto-scale kann daher keine Werte anpassen. Auto-scale **ist** für Provisioned V2-Datenfreigaben sowohl auf der SSD-Ebene (Premium) als auch auf der HDD-Ebene (Standard) verfügbar. Beide werden nach bereitgestellter Größe, IOPS und Durchsatz abgerechnet.

Anmerkung

Bei einer neu verknüpften Datenfreigabe ist Auto-scale standardmäßig deaktiviert. Eine Umstellung zwischen Provisioned V1 und Provisioned V2 ist nicht möglich. Die Generation wird beim Erstellen des zugrunde liegenden Storage-Kontos festgelegt. Jede Freigabe gehört dauerhaft einer der beiden Generationen an.

Sie müssen diese Autoscaling-Parameter konfigurieren:

- Bereitgestellte Größe (Vorgabe), IOPS und Durchsatz *(die skalierten Werte hängen davon ab, ob die Freigabe Provisioned V1 oder Provisioned V2 ist – siehe unten)*
- Geplante Erhöhung der Vorgabe (Provisioned V1) oder geplante Leistungserhöhung (Provisioned V2) (optional)
- Skalierungslogik

So konfigurieren und verwalten Sie das Autoscaling für Azure Files Premium:

1. Navigieren Sie zu **Cloud-Desktops** > **Speicher** > **Azure Files**.
2. Finden Sie die Datenfreigabe, die Sie verwalten möchten.

3. Wählen Sie im Aktionsmenü **Autoscaling** > **konfigurieren**.
4. Schalten Sie die Option **Auto-scale** auf **Ein**.
5. Wählen Sie die Tabelle für die Generation Ihrer Freigabe (Provisioned V1 oder Provisioned V2) aus und geben Sie die dort aufgeführten Einstellungen für **Bereitgestellte Größe (Vorgabe), IOPS und Durchsatz** ein.

> **Anmerkung**
>
> Liegt ein Wert außerhalb des konfigurierten Bereichs, wird er beim nächsten automatischen Skalieren auf den **Mindestwert** des Bereichs gesetzt – unabhängig davon, ob er zuvor zu hoch oder zu niedrig war. Wenn Sie beispielsweise das automatische Skalieren für eine Freigabe aktivieren, die bereits größer als der konfigurierte Maximalwert ist, wird sie auf die Mindestgröße verkleinert – nicht auf den Maximalwert.

Provisioned V1

UI-Element	Typ	Beschreibung
Einheit der Vorgabe	Dropdown-Liste	Wählen Sie die Einheit aus, die für **Mindestgröße** und **Maximalgröße** verwendet wird: **Relativ (%)**: Der Puffer wird als Prozentsatz der aktuell genutzten Kapazität angegeben. **Absolut (GiB)**: Derselbe Puffer wird als feste Anzahl von GiB zusätzlich zur aktuell genutzten Kapazität angegeben. In beiden Fällen verfolgen die Felder die genutzte Kapazität nach. Die Einheit bestimmt nur, wie der Puffer angegeben wird.
Mindestgröße	Textfeld	Die kleinste Größe, die beim automatischen Skalieren beibehalten wird, eingegeben in GiB oder % über der genutzten Kapazität. Der Mindestwert beträgt 100 GiB und kann nicht niedriger als die aktuell genutzte Kapazität der Freigabe eingestellt werden. Dieser Wert definiert den Puffer an freiem Speicherplatz, der beim automatischen Skalieren auch bei wachsender genutzter Kapazität stets verfügbar bleibt.
Maximalgröße	Textfeld	Die größte Größe, auf die die Freigabe automatisch skaliert wird. Geben Sie den Wert in GiB oder als Prozentsatz über der genutzten Kapazität ein. Der im Feld **Kleiner als** eingegebene Grenzwert darf nicht überschritten werden. Auto-scale erhöht die Größe der Freigabe nur bis zu diesem Maximalwert, damit sie nicht unkontrolliert wächst.

UI-Element	Typ	Beschreibung
Leistung	Schreibgeschützte Anzeige	Zeigt die Mindest- und Maximalwerte der Leistungsmerkmale an, die sich aus dem konfigurierten Größenbereich ergeben. Diese Werte werden von Azure anhand der bereitgestellten Größe berechnet und können nicht direkt konfiguriert werden: • **IO/S**: Basis-IOPS, berechnet als 3.000 + 1 pro bereitgestelltem GiB, bis zu einem Maximalwert für die Basisrate von 100.000 IO/s. • **Burst-IO/S**: der höhere Wert aus 10.000 IO/s oder der 3-fachen Basis-IO/s-Rate. Nicht genutzte Basis-IOs sammeln sich als Burst-Guthaben an (bis zu einem Limit), das aufgebraucht wird, wenn der Bedarf die Basisrate übersteigt, bis zu einem Maximalwert für die Burst-Rate von 100.000 IO/s. • **Egress-Rate**: zulässiger ausgehender Netzwerkdatenverkehr pro Sekunde, berechnet als 60 plus (Vorgabe für die Freigabe × 0,06 MiByte/s). • **Ingress-Rate**: zulässiger eingehender Netzwerkdatenverkehr pro Sekunde, berechnet als 40 plus (Vorgabe für die Freigabe × 0,04 MiByte/s).

Provisioned V2

> **Anmerkung**
>
> Die Abrechnungssätze für die bereitgestellte Größe, IOPS und Durchsatz variieren je nach Region und anderen Parametern. Weitere Informationen finden Sie unter Azure Files-Preise.

UI-Element	Typ	Beschreibung
Einheit der Vorgabe	Dropdown-Liste	Wählen Sie die Einheit aus, die für **Mindestgröße** und **Maximalgröße** verwendet wird: **Relativ (%)**: Der Puffer wird als Prozentsatz der aktuell genutzten Kapazität angegeben. **Absolut (GiB)**: Derselbe Puffer wird als feste Anzahl von GiB zusätzlich zur aktuell genutzten Kapazität angegeben. In beiden Fällen verfolgen die Felder die genutzte Kapazität nach. Die Einheit bestimmt nur, wie der Puffer angegeben wird.

UI-Element	Typ	Beschreibung
Mindestgröße	Textfeld	Die kleinste Größe, die beim automatischen Skalieren beibehalten wird, eingegeben in GiB oder % über der genutzten Kapazität. Der Mindestwert beträgt 32 GiB und kann nicht kleiner als die aktuell genutzte Kapazität der Freigabe eingestellt werden. Dieser Wert definiert den Puffer an freiem Speicherplatz, der beim automatischen Skalieren bei wachsender genutzter Kapazität immer vorgehalten wird. Beim automatischen Skalieren wird die Freigabe zudem nie unter ihre **Größenuntergrenze** verkleinert – die kleinste Größe, deren IOPS-/Durchsatzobergrenze die aktuell bereitgestellten IOPS und den Durchsatz der Freigabe noch abdecken kann. Beispielsweise wird eine SSD-Tier-Freigabe mit 20.000 bereitgestellten IOPS nicht auf unter etwa 1.000 GiB horizontal herunterskaliert, da diese Größe erforderlich ist, um die Obergrenze bei oder über 20.000 IOPS zu halten. Da die Formel für empfohlene IOPS bei HDD pro GiB langsamer wächst als bei SSD, erfordert derselbe Wert für bereitgestellte IOPS eine wesentlich größere HDD-Freigabe, um die Obergrenze zu erreichen.
Maximalgröße	Textfeld	Die größte Größe, auf die die Freigabe automatisch skaliert wird. Geben Sie den Wert in GiB oder als Prozentsatz über der genutzten Kapazität ein. Der im Feld **Kleiner als** eingegebene Grenzwert darf nicht überschritten werden. Obwohl Azure Freigabegrößen von bis zu 262.144 GiB unterstützt, akzeptiert dieses Feld derzeit einen Maximalwert von 102.400 GiB – eine bekannte Produkteinschränkung, die voraussichtlich in einer zukünftigen Version korrigiert wird. Auto-scale erhöht die Größe der Freigabe nur bis zu diesem Maximalwert, damit sie nicht unkontrolliert wächst.

UI-Element	Typ	Beschreibung
Bereitgestellte IOPS	Textfelder (von / bis)	Der Bereich, innerhalb dessen Auto-scale die bereitgestellten IOPS hält. Azure erzwingt ein Limit für bereitgestellte IOPS: Es begrenzt sie auf das Fünffache des Werts, den Microsoft für die aktuelle Größe der Freigabe empfiehlt, und auf den absoluten Maximalwert der Speicherklasse. Der empfohlene Wert und damit die Obergrenze unterscheiden sich je nach Medientier: • **SSD (Premium)**: Die empfohlenen IOPS betragen 3.000 + 1 pro bereitgestelltem GiB; die bereitgestellten IOPS sind auf das 5-Fache dieses Wertes begrenzt, jedoch niemals auf mehr als den absoluten Maximalwert von 102.400 IOPS. Bei 32 GiB liegt die Obergrenze bei 15.160 IOPS und erreicht bei etwa 17.480 GiB den absoluten Maximalwert von 102.400 IOPS. • **HDD (Standard)**: Die empfohlenen IOPS betragen 1.000 + 0,2 pro bereitgestelltem GiB; die bereitgestellten IOPS sind auf das 5-Fache dieses Wertes begrenzt, jedoch niemals auf mehr als den absoluten Maximalwert von 50.000 IOPS. Bei 32 GiB liegt die Obergrenze bei etwa 5.030 IOPS und erreicht bei etwa 45.000 GiB den absoluten Maximalwert von 50.000 IOPS. So oder so steigt die Obergrenze mit der Größe der Freigabe (weit unter den 102.400 GiB, die das Feld **Limit für die maximale Vorgabe** derzeit zulässt). Auto-scale vergrößert die Freigabe nicht allein, um eine höhere IOPS-Obergrenze zu erreichen. Wenn Sie die **Mindestgröße** erhöhen, steigt die Obergrenze früher. Diese Begrenzung blockiert nur weitere Erhöhungen, nicht den Betrieb: Eine Freigabe, die schon vor Einführung dieser Schutzmaßnahme mit mehr als dem 5-Fachen bereitgestellt wurde, läuft unverändert weiter. Beim automatischen Skalieren kann das Verhältnis von IOPS zu Größe lediglich nicht weiter steigen.

UI-Element	Typ	Beschreibung
Bereitgestellter Durchsatz (MiB/s)	Textfelder (von / bis)	Der Bereich, innerhalb dessen Auto-scale den bereitgestellten Durchsatz hält. Azure erzwingt eine Schutzmaßnahme, die den bereitgestellten Durchsatz auf das 5-Fache des von Microsoft für die aktuelle Größe der Freigabe empfohlenen Wertes begrenzt, jedoch niemals über den absoluten Maximalwert der Stufe hinaus. Der empfohlene Wert und damit die Obergrenze unterscheiden sich je nach Speichermedium: • **SSD (Premium)**: Der empfohlene Durchsatz beträgt 100 + 0,1 MiB/s pro bereitgestelltem GiB, begrenzt auf das 5-Fache dieses Wertes, niemals über 10.340 MiB/s. Bei 32 GiB liegt die Obergrenze bei 520 MiB/s und erreicht den absoluten Maximalwert von 10.340 MiB/s bei etwa 19.680 GiB. • **HDD (Standard)**: Der empfohlene Durchsatz beträgt 60 + 0,02 MiB/s pro bereitgestelltem GiB, begrenzt auf das 5-Fache dieses Wertes, jedoch niemals über 5.120 MiB/s. Bei 32 GiB liegt die Obergrenze bei etwa 303 MiB/s und erreicht den absoluten Maximalwert von 5.120 MiB/s bei etwa 48.200 GiB. So oder so steigt die Obergrenze mit der Größe der Freigabe (weit unter den 102.400 GiB, die das Feld **Limit für die maximale Vorgabe** derzeit zulässt). Auto-scale vergrößert die Freigabe nicht allein, um eine höhere Durchsatzobergrenze zu erreichen; eine Erhöhung der **Mindestgröße** hebt die Obergrenze früher an. Diese Begrenzung blockiert nur weitere Erhöhungen, nicht den Betrieb: Eine Freigabe, die schon vor Einführung dieser Schutzmaßnahme mit mehr als dem 5-Fachen bereitgestellt wurde, läuft unverändert weiter. Beim automatischen Skalieren kann das Verhältnis von Durchsatz zu Größe lediglich nicht weiter steigen.

6. Stellen Sie bei Bedarf **Geplante Vorgabenerhöhung** (Provisioned V1) oder **Geplante Leistungserhöhung** (Provisioned V2) auf **Ein**. Dies legt eine vorübergehende Erhöhung während eines wiederkehrenden Zeitfensters fest – zum Beispiel, wenn Sie Tage mit vorhersehbarem Spitzenbedarf haben. Solange der Zeitplan aktiv ist, werden die geplanten Werte beibehalten und die latenzbasierten Skalierungsregeln gelten nicht für sie. Nutzen Sie die Tabelle für die Generation Ihrer Freigabe und geben Sie die aufgeführten Einstellungen ein.

Provisioned V1

> **Anmerkung**
>
> Die bereitgestellte Größe (Vorgabe) wird zu Beginn des geplanten Zeitraums erhöht. Die Rückkehr in den normalen Bereich danach ist eine **Verringerung**, daher unterliegt sie weiterhin der 24-Stunden-Sperre – sie erfolgt nicht einfach deshalb, weil der geplante Zeitraum abgelaufen ist.
>
> Die Vorgabe kann noch lange nach dem geplanten Tag erhöht bleiben. Sie wird zu Beginn jedes ausgewählten Tages erhöht und kann erst 24 Stunden später, also zu Beginn des folgenden Tages, wieder herunterskaliert werden. Bei einem wiederkehrenden Zeitplan von Montag bis Freitag kann dies bedeuten, dass die Vorgabe zwischen aufeinanderfolgenden geplanten Tagen nie in ihren normalen Bereich zurückkehrt, was als potenzielle Kostenauswirkung bei der Planung berücksichtigt werden sollte.

UI-Element	Typ	Beschreibung
Tage	Dropdown-Liste	Wählen Sie den Bereich der Tage aus, für die der Zeitplan gilt.
Stunden	Zeitbereich und Dropdown-Liste	Wählen Sie die Zeitzone aus, für die der Zeitplan gilt. Obwohl dieses Feld auch einen Zeitraum mit Start- und Endzeit anzeigt, gilt der Zeitplan derzeit für jeden ausgewählten Tag vollständig, unabhängig von den hier eingegebenen Zeiten.
Bereitgestellte Größe (Vorgabe) einstellen auf	Textfeld	Die Vorgabe, die für die Freigabe während des geplanten Fensters gilt. Sie muss über der aktuell genutzten Kapazität liegen.

Provisioned V2

Anmerkung

Die bereitgestellten IOPS und der bereitgestellte Durchsatz werden zu Beginn des geplanten Zeitraums erhöht. Die anschließende Rückführung auf ihre normalen Werte ist eine **Verringerung**, daher unterliegt jeder Wert weiterhin seiner eigenen 24-Stunden-Sperre – sie erfolgt nicht einfach deshalb, weil der geplante Zeitraum abgelaufen ist. (Die Größe hat ebenfalls eine eigene, unabhängige 24-Stunden-Sperre, aber dieser Zeitplan legt die Größe nicht fest – siehe **Bereitgestellte Größe (Vorgabe), IOPS und Durchsatz**.)

IOPS und Durchsatz können noch lange nach dem geplanten Tag erhöht bleiben. Sie werden zu Beginn jedes ausgewählten Tages erhöht und können erst 24 Stunden später, also zu Beginn des folgenden Tages, wieder herunterskaliert werden. Bei einem wiederkehrenden Zeitplan von Montag bis Freitag kann dies bedeuten, dass sie zwischen aufeinanderfolgenden geplanten Tagen nie auf ihre normalen Bereiche zurückkehren, was als potenzielle Kostenauswirkung eingeplant werden sollte.

UI-Element	Typ	Beschreibung
Tage	Dropdown-Liste	Wählen Sie den Bereich der Tage aus, für die der Zeitplan gilt.
Stunden	Zeitbereich und Dropdown-Liste	Wählen Sie die Zeitzone aus, für die der Zeitplan gilt. Obwohl dieses Feld auch einen Zeitraum mit Start- und Endzeit anzeigt, gilt der Zeitplan derzeit für jeden ausgewählten Tag vollständig, unabhängig von den hier eingegebenen Zeiten.
Bereitgestellte IOPS einstellen auf	Textfeld	Der Wert, der für die bereitgestellten IOPS der Freigabe während des geplanten Fensters gilt.
Bereitgestellten Durchsatz (MiB/s) einstellen auf	Textfeld	Der Wert, der für den bereitgestellten Durchsatz der Freigabe während des geplanten Fensters gilt.

7. Diese Bedingungen bestimmen, wann die bereitgestellten Werte durch automatisches Skalieren erhöht oder verringert werden: Jede Regel, die eine Erhöhung vorschlägt, bewirkt eine Erhöhung, und eine Verringerung wird angewendet, wenn eine Regel dies vorschlägt. Nutzen Sie die Tabelle für die Generation Ihrer Freigabe und geben Sie die aufgeführten Einstellungen unter **Skalierungslogik** ein.

Provisioned V1

> **Anmerkung**
>
> Die bereitgestellte Größe (Vorgabe) kann frühestens 24 Stunden nach der letzten Erhöhung der Vorgabe verringert werden. Für Erhöhungen gibt es keine Wartezeit.

Provisioned V1 unterstützt bis zu zwei Regeln, die beide die Größe (Vorgabe) als Ziel haben. Jede Regel enthält **sowohl** eine Bedingung für das horizontale Hochskalieren als auch eine Bedingung für das horizontale Herunterskalieren – die beiden Regeln sind nicht „eine für das horizontale Hochskalieren, eine für das horizontale Herunterskalieren“. Stattdessen werden sie durch den Auslöser unterschieden: Eine Regel kann die durchschnittliche Latenz verwenden, die andere die maximale Latenz; jeder Auslöser kann einmal verwendet werden.

Wenn die Bedingungen mehrerer Regeln gleichzeitig erfüllt sind, werden ihre Vorschläge beim automatischen Skalieren wie folgt kombiniert: Jede vorgeschlagene Erhöhung hat Vorrang vor jeder vorgeschlagenen Verringerung. Wenn zwei Regeln eine Verringerung vorschlagen, wird der höhere (weniger aggressive) resultierende Wert angewendet. Eine Regel, deren Latenz zwischen ihren eigenen Schwellenwerten für das horizontale Hochskalieren und das horizontale Herunterskalieren liegt, schlägt keine Änderung vor. Sie verhindert nicht, dass eine andere Regel eine Änderung vorschlägt.

UI-Element	Typ	Beschreibung
Auslöser für die automatische Skalierung auswählen	Dropdown-Liste	Die Latenzmetrik, die die Skalierung steuert: **Latenz bei erfolgreichen Serveranfragen (Durchschnitt)** (Standard) oder **Latenz bei erfolgreichen Serveranfragen (Maximalwert)** – die durchschnittliche Zeit oder der Maximalwert der Zeit, die Azure Storage benötigt, um eine erfolgreiche Anforderung zu verarbeiten.
Vorgabe erhöhen (horizontal hochskalieren) um	Textfeld (% oder GiB)	Die Schrittweite, um die die Vorgabe jedes Mal erhöht wird (in der unter **Einheit der Vorgabe** festgelegten Einheit), wenn die unten stehende Bedingung für das horizontale Hochskalieren erfüllt ist. Solange der Latenzschwellenwert überschritten wird, skaliert das System weiter horizontal hoch, bis es entweder den konfigurierten Maximalwert für die Größe erreicht oder die Latenz wieder unter den Schwellenwert fällt.
wenn die Latenz bei erfolgreichen Serveranfragen ... überschreitet	Textfeld (ms)	Der Latenzschwellenwert in Millisekunden, der ein horizontales Hochskalieren auslöst.
für ... Minuten (horizontal hochskalieren)	Dropdown-Liste	Das Messfenster, über das der Latenzschwellenwert für das horizontale Hochskalieren überschritten bleiben muss: 5, 15, 30 oder 60 Minuten.
Vorgabe senken (horizontal herunterskalieren) um	Textfeld (% oder GiB)	Die Schrittweite, um die die Vorgabe jedes Mal gesenkt wird, wenn die unten stehende Bedingung für das horizontale Herunterskalieren erfüllt ist.
wenn die Latenz bei erfolgreichen Serveranfragen unter ... fällt	Textfeld (ms)	Der Latenzschwellenwert in Millisekunden, der ein horizontales Herunterskalieren auslöst.
für ... Minuten (horizontal herunterskalieren)	Dropdown-Liste	Das Messfenster, über das der Latenzschwellenwert für das horizontale Herunterskalieren unterschritten bleiben muss: 5, 15, 30 oder 60 Minuten.

Provisioned V2

> **Anmerkung**
>
> Bereitgestellte IOPS und bereitgestellter Durchsatz können jeweils erst 24 Stunden nach der letzten Erhöhung des jeweiligen Werts gesenkt werden. Für Erhöhungen gibt es keine Wartezeit. (Die Größe hat ebenfalls eine eigene, unabhängige 24-Stunden-Sperre, die getrennt von IOPS und Durchsatz nachverfolgt wird.)

Provisioned V2 unterstützt bis zu vier Regeln – eine für jede Kombination aus Ziel (bereitgestellte IOPS oder bereitgestellter Durchsatz) und Auslöser (durchschnittliche oder maximale Latenz); jede Kombination kann einmal verwendet werden. Jede Regel enthält **sowohl** eine Bedingung für das horizontale Hochskalieren als auch eine Bedingung für das horizontale Herunterskalieren – eine Regel ist nicht nur „für das horizontale Hochskalieren“ oder „für das horizontale Herunterskalieren“ gedacht. Wählen Sie **+**, um eine Regel hinzuzufügen und auszuwählen, welcher Wert und welcher Auslöser verwendet werden sollen.

Wenn die Bedingungen mehrerer Regeln gleichzeitig erfüllt sind, werden sie beim automatischen Skalieren wie folgt kombiniert: Jede vorgeschlagene Erhöhung hat Vorrang vor jeder vorgeschlagenen Verringerung; wenn zwei Regeln für dasselbe Ziel beide eine Verringerung vorschlagen, wird der höhere (weniger aggressive) resultierende Wert angewendet; das Ergebnis wird dann auf den Höchstwert des Ziels begrenzt; und eine Verringerung wird vollständig verworfen, wenn das Ziel derzeit gesperrt ist. Eine Regel, deren Latenz zwischen ihren eigenen Schwellenwerten für das horizontale Hochskalieren und das horizontale Herunterskalieren liegt, schlägt keine Änderung vor. Sie verhindert nicht, dass eine andere Regel eine Änderung vorschlägt.

UI-Element	Typ	Beschreibung
Typ	Dropdown-Liste	• **Provisioned IOPS**: Diese Regel skaliert die bereitgestellten IOPS. • **Provisioned throughput**: Diese Regel skaliert den bereitgestellten Durchsatz (MiB/s). Jede Regel zielt auf einen Wert ab und verwendet einen Auslöser, deckt jedoch beide Richtungen (horizontal hochskalieren und horizontal herunterskalieren) für diesen Wert ab. Es können bis zu vier Regeln gleichzeitig existieren – eine für jede Kombination aus Ziel (IOPS oder Durchsatz) und Auslöser (durchschnittliche oder maximale Latenz). Im Gegensatz zur Größe, für die entweder % oder GiB verwendet werden kann (festgelegt unter **Vorgabeeinheit** im vorherigen Schritt), werden IOPS- und Durchsatz-Skalierungsschritte immer als absolute Werte (IOPS oder MiB/s) eingegeben – für beide gibt es keine Prozentoption.
Auslöser für automatisches Skalieren auswählen	Dropdown-Liste	Die Latenzmetrik, die die Skalierung steuert – die durchschnittliche oder maximale Zeit, die Azure Storage benötigt, um eine erfolgreiche Anforderung zu verarbeiten. Die verfügbaren Optionen hängen vom oben ausgewählten **Typ** ab: • **Typ: Provisioned IOPS** – sowohl **Success Server Latency (avg)** (Standard) als auch **Success Server Latency (max)** sind verfügbar. • **Typ: Provisioned throughput** – nur **Success Server Latency (max)** ist verfügbar.
Bereitgestellte IOPS / bereitgestellten Durchsatz um folgenden Wert erhöhen (horizontal hochskalieren)	Textfeld (IOPS oder MiB/s)	Die Schrittweite, um die der unter **Typ** ausgewählte Wert jedes Mal erhöht wird, wenn die unten stehende Bedingung für das horizontale Hochskalieren erfüllt ist. Die Erhöhung ist durch das Limit des Werts begrenzt (siehe **Provisioned IOPS** / **Provisioned throughput** im vorherigen Schritt).
wenn Success Server Latency folgenden Wert überschreitet	Textfeld (ms)	Der Latenzschwellenwert in Millisekunden, der ein horizontales Hochskalieren auslöst.

UI-Element	Typ	Beschreibung
für ... Minuten (horizontal hochskalieren)	Dropdown-Liste	Das Messfenster, über das der Latenzschwellenwert für das horizontale Hochskalieren hinweg überschritten bleiben muss: 5, 15, 30 oder 60 Minuten.
Bereitgestellte IOPS / bereitgestellten Durchsatz um folgenden Wert verringern (horizontal herunterskalieren)	Textfeld (IOPS oder MiB/s)	Die Schrittweite, um die der unter **Typ** ausgewählte Wert jedes Mal verringert wird, wenn die unten stehende Bedingung für das horizontale Herunterskalieren erfüllt ist.
wenn Success Server Latency unter folgenden Wert fällt	Textfeld (ms)	Der Latenzschwellenwert in Millisekunden, der ein horizontales Herunterskalieren auslöst.
für ... Minuten (horizontal herunterskalieren)	Dropdown-Liste	Das Messfenster, über das der Latenzschwellenwert für das horizontale Herunterskalieren hinweg unterschritten bleiben muss: 5, 15, 30 oder 60 Minuten.

8. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern** oder **Speichern und schließen**.

   Die konfigurierte Datenfreigabe erscheint in der **Azure Files**-Liste.

Verwandte Themen

Auto-scale für Azure NetApp Files [205]

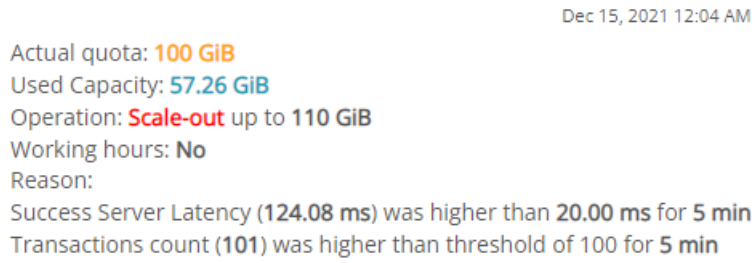
Verlauf des automatischen Skalierens für Azure Files-Datenfreigaben

Die Visualisierung des Verlaufs des automatischen Skalierens hilft Ihnen, das Verhalten des automatischen Skalierens und dessen Auswirkungen auf Ihr Deployment zu verstehen.

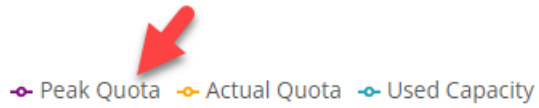
Im Folgenden finden Sie wichtige Features des Verlaufs des automatischen Skalierens.

- **Zeitbereich**: Wählen Sie oben im Fenster den gewünschten Zeitraum für die Anzeige aus.

- **Anzeigen**: Wählen Sie oben im Fenster das oder die gewünschten Diagramme für die Anzeige aus.
- **Einsparungen**: Oben im Fenster können Sie die Einsparungen durch die automatische Skalierung anzeigen.
- **Vergrößern**: Klicken und ziehen Sie die Maus im Diagramm **Vorgabe (GiB)** über den Bereich, den Sie vergrößern möchten. Wenn Sie vergrößert haben, wählen Sie **Verkleinern**, um das vollständige Diagramm wiederherzustellen.
- **Darüberfahren**: Sie können mit der Maus über einen beliebigen Teil eines Diagramms fahren, um dessen Details anzuzeigen. Zum Beispiel:



- **Aktionspunkte**:
  - **Horizontal hochskalieren**: Dieser Aktionspunkt zeigt an, dass ein Ereignis zum horizontalen Hochskalieren stattgefunden hat. (Rot zeigt an, dass das Ereignis zum horizontalen Hochskalieren Kosten verursacht.)
  - **Horizontal herunterskalieren**: Dieser Aktionspunkt zeigt an, dass ein Ereignis zum horizontalen Herunterskalieren stattgefunden hat. (Grün bedeutet, dass das Ereignis zum horizontalen Herunterskalieren Kosten spart.)
  - **Azure Issue**: Dies zeigt an, dass ein Issue bei der Kommunikation mit Azure aufgetreten ist. Wenn dies häufig auftritt, wenden Sie sich bitte an den Nerdio Manager Support.
- Wählen Sie am unteren Rand eines Diagramms den Namen des Datensatzes aus, um die zugehörige Anzeigelinie ein- oder auszuschalten. Wählen Sie beispielsweise **Spitzenvorgabe** aus, um diese Linie im Diagramm auszublenden. Wählen Sie sie erneut aus, um sie anzuzeigen.



So zeigen Sie den Verlauf des automatischen Skalierens für eine Azure Files-Datenfreigabe an:

1. Navigieren Sie zu **Cloud-Desktop** > **Speicher** > **Azure Files**.
2. Finden Sie die Datenfreigabe, mit der Sie arbeiten möchten.
3. Wählen Sie im Aktionsmenü **Autoscaling** > **Verlauf** aus.
4. Wählen Sie den gewünschten Zeitraum und die spezifischen Diagramme aus, die angezeigt werden sollen.
   - **Vorgabe (GiB)**: Das Vorgabediagramm zeigt die folgenden Informationen zur Datenfreigabe-Vorgabe an:
     - **Spitzenvorgabe**: Der Maximalwert der Vorgabe.
     - **Tatsächliche Vorgabe**: Die tatsächliche Vorgabegröße, wie sie derzeit konfiguriert ist.
     - **Genutzte Kapazität**: Der tatsächlich genutzte Speicher.
   - **Latenz (ms)**: Das Latenzdiagramm zeigt die folgenden Informationen an:
     - **Server-Latenz (Durchschnitt)**: Die durchschnittliche Zeit, die Azure Storage benötigt, um eine erfolgreiche Anforderung zu verarbeiten. Dieser Wert beinhaltet nicht die Netzwerklatenz, die in der End-to-End-Latenz angegeben ist.
     - **End-to-End-Latenz (Durchschnitt)**: Die durchschnittliche End-to-End-Latenz erfolgreicher Anforderungen an einen Speicherdienst oder den angegebenen API-Vorgang. Dieser Wert umfasst die erforderliche Zeit innerhalb von Azure Storage, um die Anforderung zu lesen, die Antwort zu senden und den Erhalt der Antwort zu bestätigen.
   - **Transaktionen**: Das Transaktionsdiagramm zeigt die Anzahl der Transaktionen an.
   - **Einsparungen %**: Das Einsparungsdiagramm zeigt den Prozentsatz der Einsparungen an.

Verwandte Themen

Auto-scale-Verlauf für Azure NetApp Shares [209]

Konfigurierte Azure NetApp Files erstellen und verwalten

> **Anmerkung**
>
> Diese Funktion ist nur in der Nerdio Manager**Premium**-Edition verfügbar.

Die Seite **Azure NetApp Files** enthält eine Liste aller konfigurierten und verknüpften Azure NetApp Files-Freigaben. Sie können verschiedene Aktionen für die Datenfreigaben ausführen, wie z. B. das Erstellen oder Verwalten von Datenfreigaben.

Azure-Abonnement und Ressourcengruppe mit Nerdio Manager verknüpfen

Sie müssen das Azure-Abonnement und die Ressourcengruppe, in der sich die Azure NetApp Files befinden, mit Nerdio Manager verknüpfen, bevor Sie mit den nächsten Schritten fortfahren können.

So verknüpfen Sie das Azure-Abonnement mit der Ressourcengruppe für Nerdio Manager:

1. Navigieren Sie zu **System** > **Einstellungen** > **Azure**.
2. Erweitern Sie **Azure-Abonnements**.
3. Wählen Sie entweder **Mit aktuell angemeldetem Benutzer verknüpfen** oder **Mit App-Anmeldeinformationen verknüpfen**, um das Azure-Abonnement zu verknüpfen.
4. Erweitern Sie **Verknüpfte Ressourcengruppen**.
5. Wählen Sie **Verknüpfen**, um die Ressourcengruppe zu verknüpfen.

Mit einer vorhandenen Azure NetApp Files-Datenfreigabe verknüpfen

Sie können eine Verknüpfung mit einer vorhandenen Azure NetApp Files-Datenfreigabe herstellen.

So stellen Sie eine Verknüpfung mit einer vorhandenen Azure NetApp Files-Datenfreigabe her:

1. Navigieren Sie zu **Cloud-Desktops** > **Speicher** > **Azure NetApp Files**.
2. Wählen Sie **ANF-Volume verknüpfen**.
3. Wählen Sie aus der Dropdown-Liste das **NetApp Files-Konto** aus.
4. Wählen Sie **OK**.

   Nach wenigen Augenblicken wird die Azure NetApp Files-Dateifreigabe zu Nerdio Manager hinzugefügt.

Azure NetApp Files-Volumen erstellen

Sie können ein neues Azure NetApp Files-Volumen erstellen.

So erstellen Sie ein Azure NetApp Files-Volumen

> **Anmerkung**
>
> Überprüfen Sie vor dem Fortfahren, ob ANF in Ihrer Azure-Region verfügbar ist und ob Ihr Azure-Abonnement für diesen Dienst zugelassen ist.

1. Navigieren Sie zu **Cloud-Desktops** > **Speicher** > **Azure NetApp Files**.
2. Wählen Sie **Neues ANF-Volumen**.
3. Geben Sie im Bereich **Konto** die folgenden Informationen ein:
   - **Konto**: Wählen Sie ein vorhandenes ANF-Konto aus der Dropdown-Liste aus oder geben Sie einen Namen ein, um ein neues zu erstellen.
   - **Ressourcengruppe**: Wählen Sie aus der Dropdown-Liste eine Ressourcengruppe aus, die die Azure NetApp Files-Kontoobjekte enthalten soll.
4. Wählen Sie den Bereich **Netzwerk** aus und geben Sie die folgenden Informationen ein:
   - **Active Directory**: Wählen Sie aus der Dropdown-Liste das Active Directory aus.
   - **SMB-Serverpräfix**: Geben Sie das Präfix der Computerobjekte ein, die der AD-Domäne hinzugefügt und für den UNC-Pfad verwen-

det werden sollen. Zum Beispiel: **SMB-PREFIX**-random\\volume\\share\\folder.
- **AD-Site-Name**: Geben Sie den Namen der Active Directory-Site ein.
- **Subnetz**: Wählen Sie aus der Dropdown-Liste das Subnetz aus.

> **Anmerkung**
>
> Das an ANF delegierte Subnetz muss leer sein.

- **AD-fähiger DNS-Server**: Geben Sie die Adresse des AD-fähigen DNS-Servers ein.

5. Wählen Sie den Bereich **Kapazitätspool** aus und geben Sie die folgenden Informationen ein:
   - **Kapazitätspool**: Wählen Sie einen vorhandenen Kapazitätspool aus der Dropdown-Liste aus oder geben Sie einen Namen ein, um einen neuen zu erstellen.
   - **Kapazität (TiB)**: Geben Sie die Kapazität in TiB ein.

   > **Anmerkung**
   >
   > Die Mindestkapazität eines ANF-Kapazitätspools beträgt 1 TiB.

   - **Leistungsstufe**: Wählen Sie aus der Dropdown-Liste die Leistungsstufe des neuen Kapazitätspools aus.

   > **Anmerkung**
   >
   > Leistungsstufen unterscheiden sich in Preis und Durchsatz (IOPS). Weitere Informationen finden Sie im folgenden Microsoft-Dokument.

6. Wählen Sie den Bereich **Volume** aus und geben Sie die folgenden Informationen ein:
   - **Volumename**: Geben Sie den Namen des Volumes ein, das auf dem oben angegebenen SMB-Server erstellt werden soll.

> **Anmerkung**
>
> Es können mehrere Volumes im selben ANF-Konto vorhanden sein.

7. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Absenden** aus.

Verwandte Themen

Konfigurierte Azure Files-Datenfreigaben erstellen und verwalten [176]

Automatische Skalierung für Azure NetApp Files

> **Anmerkung**
>
> Diese Funktion ist nur in der Nerdio Manager**Premium-Edition** verfügbar.

In Azure Storage NetApp Files verfügen Sie über ein ANF-Konto, das mehrere Kapazitätspools enthalten kann. Kapazitätspools werden mit einem Servicelevel (Standard, Premium, Ultra) erstellt, das die Leistung bestimmt. Innerhalb jedes Kapazitätspools können Sie ein oder mehrere Volumes haben, die in der Summe die Größe dieses Kapazitätspools nicht überschreiten dürfen. Die Kosten für den ANF-Speicher werden durch die Größe des Kapazitätspools bestimmt, wobei der Mindestwert 4 TiB beträgt. Sie können einen Kapazitätspool in Schritten von 1 TiB vergrößern und verkleinern, jedoch nicht unter die Summe der Volumes, die in diesem Kapazitätspool enthalten sind.

Das Durchsatzlimit des ANF-Speichersystems wird durch eine Kombination aus der dem Volume zugewiesenen Vorgabe und dem ausgewählten Servicelevel bestimmt.

Die automatische Speicherskalierung mit ANF ist erforderlich, wenn Sie die Leistung eines bestimmten Volumes während Zeiten hoher Auslastung des Speichersystems erhöhen und diese dann planmäßig wieder verringern

müssen, wenn die Leistung nicht mehr benötigt wird. Zum Beispiel während Anmelde-/Abmeldestürmen von Azure VD-Maschinen. Oder es könnte erforderlich sein, wenn mitten am Tag eine starke Aktivität auf dem Speichersystem vorliegt und die Latenz dieses Volumes als hoch erkannt wird.

Die automatische Speicherskalierung mit ANF kann auch verwendet werden, um eine festgelegte Kapazitätsreserve beizubehalten, damit der Speicherplatz auf dem Volume oder im Kapazitätspool nicht ausgeht.

So konfigurieren und verwalten Sie die automatische Skalierung für Azure NetApp Files:

1. Navigieren Sie zu **Cloud-Desktops** > **Speicher** > **Azure NetApp Files**.
2. Finden Sie das ANF, das Sie verwalten möchten.
3. Wählen Sie im Aktionsmenü **Automatische Skalierung** > **Konfigurieren**.
4. Schalten Sie die Option **Automatische Skalierung** auf **Ein**.
5. Geben Sie die **Einstellungen für die bereitgestellte Größe** ein.

> **Anmerkung**
>
> Wenn der freie Speicherplatz des Volumes unter den Mindestwert fällt, versucht das System, das Volume zu vergrößern. Wenn das Volume innerhalb des aktuellen Kapazitätspools nicht vergrößert werden kann, wird der Kapazitätspool immer um 1 TiB erweitert und das Volume wächst um mindestens 1 TiB.
>
> Das Volume wächst nicht über den konfigurierten Maximalwert hinaus.

- **Modus**: Wählen Sie aus der Dropdown-Liste den Modus aus:
  - **Nur Volume**: Skaliert das Volume automatisch, ohne den Kapazitätspool, der es enthält. Das Volume ist auf den verfügbaren freien Speicherplatz innerhalb des Kapazitätspools begrenzt, und der Kapazitätspool wird nicht automatisch vergrößert.
  - **Volume und Kapazitätspool**: Skaliert das Volume und den Kapazitätspool, der es enthält, automatisch (Standard).
- Für **Nur Volume**:

- **Größeneinheit**: Wählen Sie aus der Dropdown-Liste die Einheit (Relative % oder Absolute GiB) aus. Relativ ist ein Prozentsatz der aktuell genutzten Kapazität.
- **Mindestgröße**: Geben Sie beim Herunterskalieren die Mindestgröße ein, die auf dem Volume beibehalten werden soll. Dies wird als aktuell genutzte Kapazität plus Kapazitätsreserve ausgewertet.

> **Anmerkung**
>
> Wenn der verfügbare Speicherplatz unter den konfigurierten Mindestwert für freien Speicherplatz fällt, wird das Volume vergrößert, um den Mindestwert für verfügbaren Speicherplatz zu erreichen. Wenn die Kapazitätspoolgröße überschritten wird und die Kapazitätspool-Skalierung aktiviert ist, wird der Kapazitätspool um weitere 1 TiB erweitert, um das Volume zu vergrößern – bis zur konfigurierten maximalen Gesamtgröße.

- **Maximale Größe**: Geben Sie beim Hochskalieren den Maximalwert ein, um den das Volume vergrößert werden soll. Dies wird als aktuell genutzte Kapazität + Skalierungsbetrag ausgewertet.
  - **Weniger als**: Definieren Sie den Maximalwert, auf den das Volume anwachsen darf, um ein unkontrolliertes Systemwachstum zu verhindern. Dies ist durch die verfügbare Kapazitätspoolgröße begrenzt.
- Für **Volume und Kapazitätspool**:
  - **Minimaler freier Speicherplatz des Volumes**: Geben Sie den minimalen freien Speicherplatz ein, der auf dem Volume beibehalten werden soll. Wenn der aktuelle freie Speicherplatz unter diesen Schwellenwert fällt, wächst das Volume automatisch zusammen mit dem Kapazitätspool.
  - **Maximale Gesamtgröße des Volumes**: Geben Sie den Maximalwert der Volumegröße des Volumes in TiB ein. Die Kombination aus Volume und Kapazitätspool kann nicht größer als dieser Wert werden.
- **Das Überschreiten des Limits sollte einen Fehler auslösen**: Wählen Sie diese Option, damit der Auto-Scale-Prozess einen Fehler auslöst, wenn die berechnete Größe den Maximalwert überschreitet.

> **Anmerkung**
>
> So können Sie diese Fehler über Benachrichtigungen nachverfolgen. Weitere Informationen finden Sie unter E-Mail-Benachrichtigungen konfigurieren.

Der **Größen- und Leistungsrechner** zeigt die minimalen und maximalen Konfigurationswerte sowie die Leistungsmerkmale an.

6. Schalten Sie optional **Zeitplanbasierte SkalierungEin** und konfigurieren Sie die Einstellungen.

> **Anmerkung**
>
> Dies ist nützlich, wenn Sie Bedarfsspitzen im Speichersystem haben (zum Beispiel, wenn sich mehrere User zur gleichen Zeit anmelden und abmelden). Sie können mehr als einen Zeitraum für die Spitzen-Autoskalierung angeben, nach dem das System automatisch auf die Mindestgröße horizontal herunterskaliert. Stellen Sie sicher, dass sich die Zeitpläne nicht überschneiden.

- **Zeitzone**: Wählen Sie die Zeitzone aus der Dropdown-Liste aus.
- **Tage**: Wählen Sie die Tage aus der Dropdown-Liste aus.
- **Stunden**: Wählen Sie den Stundenbereich aus der Dropdown-Liste aus.
- **Bereitgestellte Größe festlegen auf**: Geben Sie die zusätzliche Kapazität ein, die dem Volume über die aktuelle Kapazität hinaus hinzugefügt werden soll.

7. Schalten Sie optional **Latenzbasierte SkalierungEin** und konfigurieren Sie die Einstellungen.
   - **Auto-Skalierungsauslöser auswählen**: Wählen Sie den Auslöser aus der Dropdown-Liste aus.

> **Anmerkung**
>
> Dies ist die durchschnittliche oder maximale Zeit, die von Azure Storage für die Verarbeitung einer erfolgreichen Anforderung benötigt wird.

- **Volume-Größe erhöhen (Scale-Out)**: Das System erhöht die Volume-Größe um den von Ihnen festgelegten Wert, wenn die Serverlatenz den angegebenen Schwellenwert überschreitet.
- **Volume-Größe verringern (Scale-In)**: Das System verringert die Volume-Größe um den von Ihnen festgelegten Wert, wenn die Serverlatenz unter den angegebenen Schwellenwert fällt.

8. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern** oder **Speichern und schließen**.

   Die konfigurierte Datei erscheint in der Liste der Dateien in der **Azure NetApp Files**-Liste.

Verwandte Themen

- Auto-scale für Azure Files Premium-Speicher [186]

Autoscaling-Verlauf für Azure NetApp-Datenfreigaben

> **Anmerkung**
>
> Diese Funktion ist nur in der Nerdio Manager**Premium-Edition** verfügbar.

Die Visualisierung des Autoscaling-Verlaufs hilft Ihnen, das Verhalten des Autoscalings und dessen Auswirkungen auf Ihr Deployment zu verstehen.

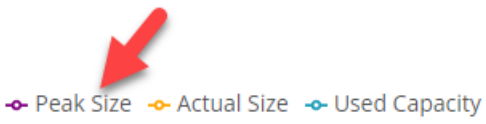
Im Folgenden finden Sie wichtige Autoscaling-Verlauf-Features.

- **Zeitbereich**: Wählen Sie oben im Fenster den gewünschten Zeitraum für die Anzeige aus.

- **Anzeigen**: Wählen Sie oben im Fenster das oder die gewünschten Diagramme für die Anzeige aus.
- **Einsparungen**: Oben im Fenster können Sie die Einsparungen durch die automatische Skalierung anzeigen.
- **Vergrößern**: Klicken und ziehen Sie die Maus nur für das Diagramm **Größe (GiB)** über den Bereich des Diagramms, den Sie vergrößern möchten. Wenn Sie vergrößert haben, wählen Sie **Verkleinern**, um das vollständige Diagramm wiederherzustellen.
- **Darüberfahren**: Sie können mit der Maus über einen beliebigen Teil eines Diagramms fahren, um dessen Details anzuzeigen. Zum Beispiel:



- **Aktionspunkte**:
  - **Horizontal hochskalieren**: Dieser Aktionspunkt zeigt an, dass ein Ereignis des horizontalen Hochskalierens stattgefunden hat. (Rot zeigt an, dass das Ereignis des horizontalen Hochskalierens Kosten verursacht.)
  - **Horizontal herunterskalieren**: Dieser Aktionspunkt zeigt an, dass ein Ereignis des horizontalen Herunterskalierens stattgefunden hat. (Grün bedeutet, dass das Ereignis des horizontalen Herunterskalierens Kosten spart.)
  - **Azure Issue**: Dies zeigt an, dass ein Problem bei der Kommunikation mit Azure aufgetreten ist. Wenn dies häufig auftritt, wenden Sie sich bitte an den Nerdio Manager technischen Support.
- Wählen Sie am unteren Rand eines Diagramms den Namen des Datensatzes aus, um die zugehörige Anzeigelinie ein- oder auszuschalten. Wählen Sie beispielsweise **Spitzengröße**, um diese Linie im Diagramm auszublenden. Wählen Sie sie erneut aus, um sie anzuzeigen.



So zeigen Sie den Autoscaling-Verlauf für eine Azure NetApp Files-Datenfreigabe an:

1. Navigieren Sie zu **Cloud-Desktops** > **Speicher** > **Azure NetApp Files**.
2. Finden Sie die Datenfreigabe, mit der Sie arbeiten möchten.
3. Wählen Sie im Aktionsmenü **Autoscaling** > **Verlauf**.
4. Wählen Sie den gewünschten Zeitraum und die spezifischen Diagramme aus, die angezeigt werden sollen.
   - **Größe (GiB)**: Das Größendiagramm zeigt die folgenden Informationen zur Größe der Datenfreigabe an:
     - **Spitzengröße**: Der Maximalwert der Datenfreigabe.
     - **Tatsächliche Größe**: Die tatsächliche Größe der Datenfreigabe.
     - **Genutzte Kapazität**: Die aktuell in der Datenfreigabe genutzte Kapazität.
   - **Latenz (ms)**: Das Latenzdiagramm zeigt die folgenden Informationen an.
     - **Leselatenz (Durchschnitt)**: Die durchschnittliche Leselatenz.
     - **Schreiblatenz (Durchschnitt):** Die durchschnittliche Schreiblatenz.
   - **Einsparungen %**: Das Einsparungsdiagramm zeigt den Prozentsatz der Einsparungen an.

Verwandte Themen

Auto-scale-Verlauf für Azure Files-Datenfreigaben [199]

Schritt 5: FSLogix und Userprofilverwaltung

Nachdem der Speicher eingerichtet ist, besteht der nächste Schritt darin, **FSLogix** zu konfigurieren, die Profilverwaltungslösung, mit der Usereinstellungen, Daten und installierte Anwendungen den Usern zwischen Sitzungshosts folgen können. Dieser Abschnitt behandelt die Einrichtung von FSLogix, die Anpassung der Konfiguration pro Hostpool und die Verwaltung der Anwendungen, die den Usern zur Verfügung stehen.

In diesem Abschnitt:

1. FSLogix und Userprofilverwaltung [212]
2. FSLogix-Einstellungen und -Konfiguration [213]

3. FSLogix-Anpassung pro Hostpool [219]
4. Installierte Anwendungen auf Hostpools verwalten [223]

FSLogix und Benutzerprofilverwaltung

FSLogix ist eine Profilcontainer-Technologie, die es Usern ermöglicht, zwischen virtuellen Desktop-Sitzungshosts zu wechseln, ohne den Zugriff auf ihre eigenen Anpassungen zu verlieren. Mit FSLogix können Sie OneDrive und die indizierte Suchfunktion in virtuellen Desktops verwenden. Diese Option war für ältere RDS-Benutzerprofil-Datenträger (UPDs) nicht verfügbar.

FSLogix ist in AVD integriert und bietet eine nahtlose, on demand Profilspeicherlösung. Die Funktionsebene von AVD für Business und SharePoint entspricht der eines stationären Desktops – zum Beispiel auf einem physischen PC oder einem Laptop.

FSLogix unterstützt die aktive Cache-Synchronisierung in der AVD-Umgebung, sodass Benutzer ihre aktualisierten Dateien von jedem der verbundenen Hosts erhalten.

FSLogix behält die Anmeldedaten der User bei. Sie müssen sich nicht jedes Mal bei OneDrive anmelden, wenn Sie eine Sitzung starten.

Die Windows-Benutzerprofile von AVD-Desktopbenutzern sind in VHD-Dateien gekapselt und auf einem Dateiserver gespeichert, der von den Sitzungshost-VMs getrennt ist. Wenn einem Benutzer ein gepoolter (d. h. nicht persistenter) Desktop zugewiesen ist, folgt das Profil einschließlich des Windows Search-Caches dem Benutzer, unabhängig von der virtuellen Desktop-VM, bei der er sich anmeldet.

Nerdio Manager stellt sicher, dass das Einrichten, Konfigurieren und Verwalten von FSLogix-Profilcontainern einfach ist. Sie können mehrere FSLogix-Konfigurationsprofile erstellen und diese auf Hostpool-Basis anwenden. Dies bedeutet, dass Sie unterschiedliche FSLogix-Konfigurationen haben können, bei denen beispielsweise die Speicherorte unterschiedlich sind oder bei denen Sie unterschiedliche Registry-Parameter auf Hostpool-Ebene festgelegt haben.

Anmerkung

- Die gängigste Speicherlösung für FSLogix-Profile, die im Allgemeinen für neue Deployments/Profile empfohlen wird, ist Azure Files-Speicher. Detaillierte Konfigurationsanweisungen finden Sie unter Erstellen und Verwalten konfigurierter Azure Files-Datenfreigaben [176].
- Wenn Sie sich nicht sicher sind, welche Speicherlösung Sie für Ihre Umgebung wählen sollen, lesen Sie Welche FSLogix-Profilspeicheroption sollte ich wählen?

Wir stellen sicher, dass der richtige Agent auf Ihrem Image installiert ist, oder erklären, wie dies manuell durchgeführt wird, und dass das korrekte Konfigurationsprofil angewendet wird. Dies stellt sicher, dass, wenn eine Sitzungshost-VM dem Hostpool beitritt oder ein Reimaging vorgenommen wird, all dies automatisch erledigt wird.

Verwandte Themen

FSLogix-Einstellungen und -Konfiguration [213]

Problembehandlung, wenn FSLogix-Profilcontainer trotz Speicherung auf OneDrive weiter wachsen

User von Windows 10- zu Windows 11-AVD-Hostpools migrieren und dabei ihre FSLogix-Profile beibehalten

FSLogix-Einstellungen und -Konfiguration

Der FSLogix-Profilcontainer basiert auf zwei Komponenten:

- Installation of the FSLogix application (https://aka.ms/fslogix_download)
- Konfiguration von FSLogix über GPO oder Registry. Weitere Informationen finden Sie in diesem Microsoft-Artikel.

Nerdio Manager installiert standardmäßig automatisch die FSLogix-Anwendung, wenn eine neue Sitzungshost-VM erstellt wird oder bei einer bestehenden ein Reimaging vorgenommen wird. Dies ist der häufigste Use Case.

Erstellen einer FSLogix-Profilspeicherkonfiguration

Nerdio Manager ermöglicht es Ihnen, FSLogix-Profilspeicherkonfigurationen zu erstellen.

So fügen Sie eine FSLogix-Profilspeicherkonfiguration hinzu:

1. Navigieren Sie zu **Cloud-Desktops** > **Azure Virtual Desktop** > **Hostpool-Profile**.
2. Wählen Sie unten rechts **New profile** und aus den Menüoptionen **FSLogix** aus.
3. Wählen Sie im Bereich **FSLogix Profiles storage** die Option **Add**.
4. Geben Sie die folgenden Informationen ein:
   - **Name**: Geben Sie den Profilnamen ein.
   - **Version** Wählen Sie aus der Dropdown-Liste die FSLogix-Version aus.
   - **Use Cloud Cache**: Wählen Sie diese Option, um FSLogix Cloud Cache zu aktivieren.

> **Tipp**
>
> Aus Leistungsgründen empfehlen wir dringend die Verwendung von Premium-SSD-Disks und ephemeren Betriebssystem-Disks, wenn Cloud Cache aktiviert ist. (Standard-SSD-Disks können in sehr kleinen Umgebungen oder Testszenarien ausreichen.)

> **Anmerkung**
>
> Weitere Informationen zu FSLogix Cloud Cache finden Sie im folgenden Microsoft-Artikel.
>
> Cloud Cache ermöglicht es Ihnen, mehrere Profilspeicherorte anzugeben. Es repliziert die Profile asynchron und stellt die Profile gleichzeitig an mehreren Speicherorten zur Verfügung. Wenn also einer der Standorte nicht verfügbar ist, führt der Sitzungshost automatisch ein Failover auf einen der alternativen Standorte durch.

- **Registry der Sitzungshosts für Entra ID-verbundenen Speicher konfigurieren**: Wählen Sie diese Option, um die Entra ID Kerberos-Funktionalität und das Laden von Entra ID-Anmeldedaten zu aktivieren.

  > **Anmerkung**
  >
  > Weitere Informationen finden Sie in diesem Microsoft-Artikel.

- **Lokale Admin-Konten von FSLogix ausschließen**: Wählen Sie diese Option, um die Erstellung lokaler Admin-Profile im FSLogix-Speicherort zu verhindern.
- **Domänenkonto von FSLogix ausschließen**: Wählen Sie diese Option, um zu verhindern, dass Domänenkontoprofile im FSLogix-Speicherort erstellt werden, und geben Sie dann die Domänendetails in das Feld unten ein.

  > **Anmerkung**
  >
  > Wenn FSLogix auf einem Sitzungshost Probleme verursacht, gibt es immer noch eine Möglichkeit, sich zu Fehlerbehebungszwecken mit einem ausgeschlossenen Benutzer anzumelden.

- **App Service-Einstellungen verwalten**: Wählen Sie diese Option, um die Registry-Einstellungen des FSLogix App Service zu bearbeiten.
- **Protokolleinstellungen verwalten**: Wählen Sie diese Option, um Protokolleinstellungen zu verwalten.
- **FSLogix-Profilpfad (VHDLocation)**: Wählen Sie aus der Dropdown-Liste eine Azure Files-Freigabe aus. Alternativ geben Sie einen UNC-Pfad ein.

  > **Anmerkung**
  >
  > Sie können bis zu 4 Pfade angeben. Verwenden Sie außerdem die Pfeile, um die Reihenfolge der Pfade zu ändern. Die Profile werden an all diesen Speicherorten erstellt.

- **FSLogix Registry-Optionen**: Wählen Sie aus der Dropdown-Liste **Bearbeitungsmodus** aus, ob Sie mit **Allen Einstellungen** oder **Erweitert** arbeiten möchten.
  - Für **Alle Einstellungen**:
    - Geben Sie in der Spalte **Konfiguration** den Wert der Einstellung ein.
    - Wählen Sie **Löschen**, um eine bestimmte Einstellung auf **Nicht konfiguriert** zu setzen.
    - Wählen Sie **Alle löschen**, um alle Einstellungen auf **Nicht konfiguriert** zu setzen.
  - Für **Erweitert**:
    - Sie können DWORD-Werte im folgenden Format hinzufügen: **"ValueName":dword:ValueData**. Zum Beispiel: **"ProfileType"=dword:00000003**.
    - Sie können Zeichenfolgenwerte im folgenden Format hinzufügen: **"ValueName":"ValueData**". Zum Beispiel: **"VolumeType":"vhdx"**.
- **FSLogix Office Container zur automatischen Weiterleitung von Microsoft Office-Benutzerdaten konfigurieren**: Aktivieren Sie diese Option, um nur die Bereiche des Profils umzuleiten, die spezifisch für Microsoft Office sind.

> **Anmerkung**
>
> FSLogix Office Container trennen Microsoft Office-Daten (zum Beispiel OST-Dateien) vom allgemeinen Benutzerprofil, um die Fehlerbehebung zu erleichtern. FSLogix Office Container und FSLogix-Profilcontainer werden in separaten VHDX-Dateien gespeichert und können auf verschiedenen Datenfreigaben abgelegt werden. Weitere Einzelheiten finden Sie in diesem Microsoft-Artikel.

  - **FSLogix Office Container-Pfad (VHDLocation)**: Nach Bedarf ändern.
  - **FSLogix Office Container Registry-Optionen**: Wählen Sie aus der Dropdown-Liste **Bearbeitungsmodus**, ob Sie mit **Allen Einstellungen** oder **Erweitert** arbeiten möchten, und konfigurieren Sie dann die Einstellungen wie erforderlich.

- **Umleitungen**: Aktivieren Sie diese Option, wenn Sie Umleitungen in das globale Profil zur Wiederverwendung bei Kunden einbeziehen möchten.

> **Anmerkung**
>
> Weitere Informationen zu Umleitungen finden Sie in diesem Microsoft-Artikel.

- **Installation von FSLogix-Apps erzwingen, auch wenn diese bereits installiert sind**: Wählen Sie diese Option, um die Neuinstallation des FSLogix-Agenten und der Anwendungen zu erzwingen.

5. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

Eine FSLogix-Profilspeicherkonfiguration als Standard festlegen

Nerdio Manager ermöglicht es Ihnen, eine FSLogix-Profilspeicherkonfiguration als Standard festzulegen.

So legen Sie Nerdio Manager fest, um die FSLogix-Anwendung automatisch zu installieren:

1. Navigieren Sie zu **System** > **Einstellungen** > **Integrationen**.
2. Fügen Sie im Bereich **FSLogix Profiles storage** Profile nach Bedarf hinzu, ändern oder entfernen Sie diese.

> **Anmerkung**
>
> Stellen Sie sicher, dass Sie die folgenden Optionen für FSLogix-Profile auswählen, die mit hybrid Hostpools verknüpft sind.
>
> - **Use Cloud Cache**: Wählen Sie diese Option, um FSLogix Cloud Cache in den Hostpools und den Sitzungshosts innerhalb dieser Hostpools zu aktivieren, die dieses FSLogix-Profil verwenden.
> - **Azure-Seitenblobs verwenden**: Wählen Sie diese Option, um Blob-Container von Speicherkonten zum Speichern von Benutzerprofilen zu verwenden. Auf diese Container wird mithilfe von Zugriffsschlüsseln für Storage-Konten zugegriffen.

3. Finden Sie das gewünschte FSLogix-Speicherkonfigurationsprofil und wählen Sie **Als Standard festlegen**.

> **Anmerkung**
>
> - Wenn Sie die Option **FSLogix-Profile verwenden** auf **Aus** setzen, wird die FSLogix-App automatisch installiert, wenn neue Hosts erstellt oder bei denen ein Reimaging vorgenommen wurde.
> - Die FSLogix-Einstellungen jedes Hostpools können angepasst werden.
> - FSLogix ist nicht auf dem Desktop-Image installiert.
> - Die FSLogix-Registry-Einstellungen sind auf dem Desktop-Image nicht festgelegt.
> - Sitzungshosts sollten keine widersprüchlichen FSLogix-Konfigurationen von GPOs erhalten.

Verwandte Themen

FSLogix und Userprofilverwaltung [212]

FSLogix-Anpassung pro Hostpool [219]

Welche FSLogix-Profilspeicheroption sollte ich wählen?

FSLogix-Profilanpassung pro Hostpool

Sie können FSLogix mit Nerdio Manager konfigurieren und dessen Einstellungen auf jeden Hostpool in der AVD-Bereitstellung anwenden.

Weitere Informationen finden Sie unter Hostpools [75].

Das Hinzufügen eines Servers umfasst die Installation von FSLogix und das Anwenden der erforderlichen Einstellungen, die für den Hostpool ausgewählt wurden. Sie können die globalen Standardeinstellungen verwenden oder die Einstellungen für jeden Hostpool anpassen.

So konfigurieren Sie benutzerdefinierte FSLogix-Einstellungen für einen Hostpool:

> **Anmerkung**
>
> Alle hier konfigurierten Einstellungen werden nur auf neu erstellte Hosts oder auf Hosts angewendet, bei denen ein Reimaging vorgenommen wurde.

1. Navigieren Sie zur Liste der Hostpools und finden Sie den Hostpool, den Sie ändern möchten.
2. Wählen Sie das Menü „Weitere Optionen“ ⋮ und dann **Einstellungen** .
3. Wählen Sie in den Menüoptionen auf der linken Seite **FSLogix**.
4. Geben Sie die folgenden Informationen ein:
   - **FSLogix-Profile aktivieren**: Wählen Sie den Umschalter, um FSLogix-Profile zu aktivieren.

     > **Anmerkung**
     >
     > Wenn diese Option nicht aktiviert ist, installiert Nerdio Manager die FSLogix-Profilcontainer-Anwendung nicht auf neu erstellten VMs, wenn diese in diesem Hostpool bereitgestellt werden. Vorhandene VMs sind davon nicht betroffen.

- Wählen Sie aus der Dropdown-Liste einen vorhandenen Profilnamen aus. Wählen Sie alternativ **Benutzerdefiniert**, um ein benutzerdefiniertes Profil für diesen Hostpool zu erstellen.

> **Anmerkung**
>
> Wenn Sie ein vorhandenes Profil auswählen, wird die Konfiguration automatisch mit den Details des ausgewählten Profils vervollständigt, das nicht bearbeitet werden kann. Wenn Sie **Benutzerdefiniert** auswählen, können Sie das Profil nach Bedarf konfigurieren.

- **Version** Wählen Sie aus der Dropdown-Liste die FSLogix-Version aus.
- **Registry der Sitzungshosts für Entra ID-verbundenen Speicher konfigurieren**:
- **Lokale Admin-Konten von FSLogix ausschließen**:
- **Domänenkonten von FSLogix ausschließen**:
- Pfad für FSLogix-Profile (VHDLocation).
- Konfigurieren Sie den Office-Container zur Umleitung von Microsoft Office-Benutzerdaten (ODFC):
  - Pfad für FSLogix Office-Container (VHDLocation):
- **Cloud Cache verwenden**: Wählen Sie diese Option, um FSLogix Cloud Cache zu aktivieren.

> **Tipp**
>
> Aus Leistungsgründen empfehlen wir dringend die Verwendung von Premium-SSD-Disks und ephemeren Betriebssystem-Disks, wenn Cloud Cache aktiviert ist (Standard-SSD-Disks können in sehr kleinen Umgebungen oder Testszenarien ausreichen).

> **Anmerkung**
>
> Weitere Informationen zu FSLogix Cloud Cache finden Sie im folgenden Microsoft-Artikel.
>
> Cloud Cache ermöglicht es Ihnen, mehrere Profilspeicherorte anzugeben. Es repliziert die Profile asynchron und stellt die Profile gleichzeitig an mehreren Speicherorten zur Verfügung. Wenn also einer der Orte nicht verfügbar ist, führt der Sitzungshost automatisch ein Failover auf einen der alternativen Orte durch.

- **App Service Einstellungen verwalten**: Wählen Sie diese Option, um die FSLogix App Service Registry-Einstellungen zu bearbeiten.
- **Protokolleinstellungen verwalten**: Wählen Sie diese Option, um die Registry-Einstellungen für Protokolle zu verwalten.
- **FSLogix-Registry-Optionen**: Wählen Sie aus der Dropdown-Liste **Bearbeitungsmodus** aus, ob Sie mit **Allen Einstellungen** oder **Erweitert** arbeiten möchten.
  - Für **Alle Einstellungen**:
    - Wählen Sie über die Tabs die Komponente aus, die Sie konfigurieren möchten. Wählen Sie aus **Profileinstellungen**, **ODFC-Einstellungen**, **Cloud Cache-Einstellungen**, **App-Diensteinstellungen** oder **Protokolleinstellungen**.
    - Geben Sie in der Spalte **Konfiguration** den Wert der Einstellung ein. Um beispielsweise Profileinstellungen zu konfigurieren, wählen Sie den Bereich **Profileinstellungen**, wählen Sie das Feld in der Spalte **Konfiguration** und geben Sie die Einstellung ein.
    - Wählen Sie **Tab-Konfigurationswerte löschen**, um alle Werte für diese bestimmte Komponente auf **Nicht konfiguriert** zu setzen.
    - Wählen Sie **Alle Konfigurationswerte löschen**, um alle Einstellungen auf **Nicht konfiguriert** zu setzen.
      - Optional können Sie im Feld **Einstellungen nach Namen suchen** die Einstellungen filtern, indem Sie den Namen oder einen Teil des Namens der Einstellung eingeben.
  - Für **Erweitert**:

  - Sie können DWORD-Werte im folgenden Format hinzufügen: *\"ValueName\":dword:ValueData (Beispiel: "Profile-Type"=dword:00000003)*.
  - Sie können Zeichenfolgenwerte im folgenden Format hinzufügen: *\"ValueName\":\"ValueData\" (Beispiel: "VolumeType":"vhdx")*.
- **Umleitungen**: Wenn Sie Umleitungen in das globale Profil zur Wiederverwendung bei Kunden einbeziehen möchten, aktivieren Sie den Schalter, um diese Funktion zu aktivieren.

> **Anmerkung**
>
> Weitere Details finden Sie unter Containertypen.

- **Installation von FSLogix-Apps erzwingen, auch wenn diese bereits installiert sind**: Wählen Sie diese Option, um die Neuinstallation des FSLogix-Agents und der Anwendungen zu erzwingen.
- **Auf bestehende Hosts anwenden**: Wählen Sie diese Option, um diese Änderungen auf bestehende Hosts anzuwenden. Andernfalls wirkt sich die Änderung nur auf neue Hosts oder auf Hosts aus, bei denen ein Reimaging vorgenommen wurde.
  - **Hosts in Gruppen verarbeiten**: Geben Sie die Anzahl der gleichzeitigen Aktionen ein, die während dieses Massenvorgangs ausgeführt werden sollen.
  - **Anzahl der Fehler vor dem Abbruch**: Geben Sie die Anzahl der Fehler ein, die zum Stoppen des Prozesses führen.
  - **Messaging**: Um Nachrichten an aktive User zu senden, aktivieren Sie den Schalter, um diese Funktion zu aktivieren, und geben Sie die folgenden Details ein:
    - **Verzögerung**: Wählen Sie aus der Dropdown-Liste die Anzahl der Minuten aus, die nach dem Senden der Nachricht gewartet werden soll, bevor der Prozess gestartet wird.
    - **Nachricht**: Geben Sie die Nachricht ein, die Sie an die Benutzer senden möchten.
  - **Zeitplan**:Um die Änderungen zu einem ausgewählten Zeitpunkt anzuwenden, aktivieren Sie den Schalter, um diese Funktion zu aktivieren, und geben Sie die folgenden Details ein:
    - **Name**: Geben Sie einen Namen für den Zeitplan ein.
    - **Beschreibung**: Geben Sie eine Beschreibung für den Zeitplan ein.

- **Startdatum**: Wählen Sie das Feld **Startdatum** aus und wählen Sie im Kalender das gewünschte Startdatum aus.
- **Zeitzone**: Wählen Sie aus der Dropdown-Liste die Zeitzone für die Startzeit aus.
- **Startzeit**: Wählen Sie aus den Dropdown-Listen für Stunden und Minuten die Startzeit aus.
- **Wiederholung**: Wählen Sie bei Bedarf aus der Dropdown-Liste den wiederkehrenden Zeitplan aus.

> **Anmerkung**
>
> Die Dropdown-Liste enthält die Option **Nach dem Patch Thursday**. Dies ermöglicht Ihnen das Erstellen eines wiederkehrenden Zeitplans basierend auf Patch Thursday.

- **Tage danach**: Wenn Sie **Nach dem Patch Thursday** ausgewählt haben, geben Sie die Anzahl der Tage nach dem Patch Thursday ein, an denen die geplante Aufgabe ausgeführt werden soll.

5. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Speichern** oder **Speichern und schließen**.

Verwandte Themen

Hostpools [75]

https://www.youtube.com/watch?v=HJMLL3ZthPs

Installierte Anwendungen auf Hostpools verwalten

Nerdio Manager ermöglicht es Ihnen, die FSLogix App Masking-Technologie zu nutzen, um automatisch eine Discovery durchzuführen, die auf einem Hostpool installierten Anwendungen zu entdecken, und Regeln zu konfigurieren, um zu bestimmen, welche User auf welche Anwendungen zugreifen können. Der Userzugriff kann auf der Ebene der einzelnen Anwendung gesteuert und pro User oder Sicherheitsgruppe zugewiesen werden. Mehrere Anwendungen können für eine konsolidierte Zugriffsverwaltung gruppiert werden. Installieren Sie einfach alle erforderlichen Anwendungen auf dem Desktop-Image, aktualisieren Sie die Sitzungshosts und definieren Sie, welche User auf welche Anwendungen zugreifen können.

Anmerkung

FSLogix App Masking wird derzeit in AAD-verbundenen Hostpool-Szenarien nicht unterstützt.

Anmerkung

Dieser Prozess funktioniert nicht durch einfaches Ausblenden von Verknüpfungen. Er verbirgt tatsächlich alle Komponenten der Anwendung. Wenn Sie beispielsweise eine Regel erstellen, um Chrome für alle User auszublenden:

- Der Chrome-Ordner in den Programmdateien erscheint für den User als leer. Tatsächlich ist der Ordner nicht leer, er ist lediglich vor dem User verborgen.
- Chrome wird bei Bedarf von der Taskleiste gelöst.
- Die Chrome-Desktopverknüpfung wird bei Bedarf entfernt.
- Der User findet Chrome nicht, wenn er eine Cortana-Suche durchführt.

Die folgenden Schritte müssen ausgeführt werden, um die installierten Apps zu verwalten:

- **Discovery durchführen und installierte Anwendungen bearbeiten**: Die Discovery wird automatisch durchgeführt, sobald ein Hostpool erstellt oder ein Reimaging vorgenommen wird. Darüber hinaus wird sie alle paar Tage ausgeführt, um Anwendungen zu finden, die möglicherweise hinzugefügt wurden (nicht durch einen Reimaging-Prozess). Alternativ kann die Discovery manuell durchgeführt werden.
- **Regelsätze erstellen**: Erstellen Sie Regelsätze, um zu bestimmen, welche User Zugriff auf welche Anwendungen haben.
- **Wenden Sie die Regelsätze auf die Sitzungshost-VMs an**: Wenden Sie die ausgewählten Regelsätze auf alle Sitzungshost-VMs an. Sie können damit warten, bis ein Sitzungshost erstellt oder ein Reimaging vorgenommen

wird. Alternativ können Sie die ausgewählten Regelsätze sofort manuell anwenden.

Diese Schritte werden unten ausführlich erläutert.

Discovery durchführen und installierte Anwendungen bearbeiten

Der erste Schritt zur Verwaltung der installierten Anwendungen besteht darin, eine Discovery durchzuführen. Darüber hinaus ermöglicht Ihnen Nerdio Manager, Anwendungen zu bearbeiten und manuell hinzuzufügen.

So führen Sie eine Discovery durch und bearbeiten die installierten Anwendungen:

1. Finden Sie den Hostpool, mit dem Sie arbeiten möchten.
2. Wählen Sie im Aktionsmenü **Anwendungen**> **Installierte Apps** aus.
3. Notieren Sie sich Datum und Uhrzeit der letzten Discovery.

> **Anmerkung**
>
> Wenn der Hostpool vor Kurzem erstellt wurde, sehen Sie möglicherweise keine entdeckten Anwendungen, da noch keine Discovery durchgeführt wurde. Möglicherweise müssen Sie bis zu 48 Stunden warten oder eine manuelle Discovery durchführen.

4. Wählen Sie bei Bedarf (**nn Apps)**, um eine Liste der entdeckten Anwendungen und weitere Details anzuzeigen.
5. Wählen Sie bei Bedarf **Discovery durchführen**, um eine manuelle Discovery durchzuführen.
   - Geben Sie die folgenden Informationen ein:
   - **Sitzungshost-VM**: Wählen Sie aus der Dropdown-Liste die Sitzungshost-VM aus, die Sie für die Discovery verwenden möchten.
   - Wählen Sie **Erweitert**, um eine der folgenden Aktionen durchzuführen:
     - Wählen Sie ✖, um eine entdeckte Anwendung zu entfernen.
     - Bearbeiten Sie bei Bedarf den Namen oder das Installationsdirectory für jede entdeckte Anwendung.

- Wählen Sie +, um eine Anwendung und ihr Installationsdirectory hinzuzufügen. Der Discovery-Prozess sucht in diesem Directory nach allen Komponenten dieser Anwendung und erkennt sie automatisch.
- Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Jetzt ausführen**.
- Verfolgen Sie den Fortschritt des Discovery-Prozesses im Aufgabenbereich. Warten Sie unbedingt, bis die Aufgabe abgeschlossen ist, bevor Sie fortfahren.

> **Anmerkung**
>
> Wenn der Sitzungshost ausgeschaltet ist, schaltet das System den Sitzungshost ein, um die Discovery durchzuführen.

Regelsätze erstellen

Der nächste Schritt zur Verwaltung der installierten Anwendungen ist das Erstellen von Regelsätzen. Im Wesentlichen legen Sie fest, welche User Zugriff auf welche Anwendungen haben.

So erstellen Sie Regelsätze:

1. Finden Sie den Hostpool, mit dem Sie arbeiten möchten.
2. Wählen Sie im Aktionsmenü **Anwendungen**> **Installierte Apps** aus.
3. Wählen Sie **Regelsatz hinzufügen**.
4. Geben Sie die folgenden Informationen ein:
   - **Regelsatzname**: Geben Sie den Namen des Regelsatzes ein.
   - **Aktiviert**: Wählen Sie diese Option, um den Regelsatz zu aktivieren.

> **Anmerkung**
>
> Nur aktivierte Regelsätze werden auf Hosts angewendet.

   - **Anwendungen**: Wählen Sie aus der Dropdown-Liste die entdeckten Anwendungen aus, die dem Regelsatz hinzugefügt werden sollen.
     - Erweitern Sie bei Bedarf die Anwendung, um deren Details anzuzeigen.

- Bearbeiten, hinzufügen oder löschen Sie die Komponenten der Anwendung nach Wunsch.
- **Regeltyp: App-Maskierung**: Dies ermöglicht Ihnen die Verwaltung des Zugriffs auf installierte Komponenten.
- **Regeltyp: Umleitung**: Dies ermöglicht Ihnen die dynamische Umleitung eines Ordners, einer Datei, eines Registry-Schlüssels oder eines Werts auf eine Alternative basierend auf dem User oder der Gruppe. Beispiel: Wie oben dargestellt, können Sie eine Anwendung dazu bringen, eine andere Lizenzdatei für das Vertriebsteam zu verwenden.
- **Regeltyp: App-Container**: Dies ermöglicht Ihnen die dynamische Umleitung eines Ordners auf ein anderes angeschlossenes Laufwerk. Beispiel: Wie oben dargestellt, leiten Sie auf ein anderes Laufwerk um, das die Lizenzen für das Vertriebsteam enthält.

- **Auf alle User anwenden**: Wenn diese Option ausgewählt ist (Standard), sind die Anwendungen nur für die User verfügbar, die Sie im Feld **Ausgeschlossene User und Gruppen** angeben. Die Anwendungen sind für alle anderen User ausgeblendet und nicht verfügbar.

  > **Anmerkung**
  > - Deaktivieren Sie diese Option, wenn Sie die Anwendungen für alle User verfügbar machen müssen.
  > - Wenn Sie den Zugriff für einige User oder Gruppen weiterhin einschränken müssen, fügen Sie diese im Feld **Nur auf die folgenden User und Gruppen anwenden** hinzu.
  >
  > Beachten Sie, dass das Feld **Nur auf die folgenden User und Gruppen anwenden** erst verfügbar wird, wenn die Option **Auf alle User anwenden** deaktiviert ist.

- **Lokale Admin ausschließen**: Wählen Sie diese Option, um diese Regel nicht auf die Gruppe der lokalen Admin anzuwenden.
- **Ausgeschlossene User und Gruppen**: Wählen Sie die User aus, die von der Liste zulässiger User oder der Blocklist ausgeschlossen werden sollen.

5. Wählen Sie **Speichern und anwenden**, um die Regel zu speichern und sofort auf alle Sitzungshost-VMs anzuwenden. Wählen Sie **Speichern und schließen**, um die Regel zu speichern.

> **Anmerkung**
>
> Wenn Sie **Speichern und schließen** auswählen, wird die Regel angewendet, wenn Sitzungshosts erstellt werden oder ein Reimaging für sie vorgenommen wird. Sie können die Regel bei Bedarf auch später manuell anwenden.

Regelsätze verwalten und anwenden

Nerdio Manager ermöglicht Ihnen das Verwalten von Regelsätzen. Dies umfasst das Anwenden von Regelsätzen, das Löschen, Bearbeiten usw.

So verwalten Sie Regelsätze:

1. Finden Sie den Hostpool, mit dem Sie arbeiten möchten.
2. Wählen Sie im Aktionsmenü **Anwendungen**> **Installierte Apps** aus.
3. Sie können mehrere Regeln auswählen und dann **Bulk-Aktion auswählen**, um eine Bulk-Aktion für die ausgewählten Regeln durchzuführen.
4. Über das Aktionsmenü neben jedem Regelsatz können Sie:
   - Wählen Sie **Bearbeiten**, um den Regelsatz zu bearbeiten.
   - Wählen Sie **Auf Hosts anwenden**, um den Regelsatz sofort auf alle Sitzungshosts anzuwenden. (siehe unten)
   - Wählen Sie **Deaktivieren**, um den Regelsatz zu deaktivieren.
   - Wählen Sie **Löschen**, um den Regelsatz zu löschen.
   - Wählen Sie **Zuweisen**, um die Regelsatzzuweisungen zu ändern.
5. Zusätzlich können Sie:
   - Wählen Sie **Discovery durchführen**, um den Application Discovery-Prozess sofort zu starten. (siehe oben)
   - Wählen Sie **Regelsatz hinzufügen**, um einen neuen Regelsatz hinzuzufügen. (siehe oben)
   - Wählen Sie **Alle Regelsätze anwenden**, um sofort alle Regelsätze auf alle Sitzungshosts anzuwenden. (siehe unten)

So wenden Sie Regelsätze an:

1. Wählen Sie **Auf Hosts anwenden** (für eine einzelne Regel oder ausgewählte Regeln) oder **Alle Regelsätze anwenden** (für alle Regeln).

2. Geben Sie die folgenden Informationen ein:
   - **Anwendungsmethode**: Wählen Sie aus der Dropdown-Liste aus, wie der Regelsatz angewendet werden soll.
     - **Alle vorhandenen FSLogix-Regelsätze auf Hosts löschen**: Wählen Sie diese Option, um alle FSLogix-Regelsätze auf den Hosts zu löschen, bevor dieser Regelsatz angewendet wird.
     - **Nur Nerdio Manager erstellte Regelsätze auf Hosts löschen**: Wählen Sie diese Option, um alle Regelsätze, die von Nerdio Manager erstellt wurden, auf den Hosts zu löschen, bevor dieser Regelsatz angewendet wird.
     - **Keine Regelsätze löschen, nur die angewendeten Regelsätze überschreiben**: Wählen Sie diese Option, um alle vorhandenen Regelsätze beizubehalten und nur den Regelsatz zu überschreiben, der gerade angewendet wird.
   - **Verarbeiten Sie Hosts in Gruppen von**: Geben Sie die Anzahl der gleichzeitigen Aktionen ein, die während dieses Massenvorgangs ausgeführt werden sollen.
   - **Anzahl der Fehler vor dem Abbruch**: Geben Sie die Anzahl der Fehler ein, die zum Stoppen des Prozesses führen.
   - **Messaging**: Schalten Sie Messaging ein, um Nachrichten an aktive User zu senden.
     - **Verzögerung**: Wählen Sie aus der Dropdown-Liste die Anzahl der Minuten aus, die nach dem Senden der Nachricht gewartet werden soll, bevor der Prozess gestartet wird.
     - **Nachricht**: Geben Sie die Nachricht ein, die Sie an die User senden möchten.
3. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

   Der Prozess zur Anwendung der Regelsätze beginnt.

Regelsätze exportieren

Nerdio Manager ermöglicht es Ihnen, Regelsätze entweder in eine JSON-Datei oder in einen Hostpool zu exportieren.

So exportieren Sie Regelsätze:

1. Finden Sie den Hostpool, mit dem Sie arbeiten möchten.

2. Wählen Sie im Aktionsmenü **Anwendungen**> **Installierte Apps** aus.
3. Wählen Sie den oder die Regelsätze aus, die Sie exportieren möchten.
4. Wählen Sie im Aktionsmenü **Bulk-Aktion auswählen** die Option **Regelsätze exportieren** aus.
5. Geben Sie die folgenden Informationen ein:
   - **Exportieren nach**: Wählen Sie aus der Dropdown-Liste das Exportziel aus.

     > **Anmerkung**
     >
     > Beim Export in eine JSON-Datei wird die Datei in den Standard-Downloadordner des Browsers heruntergeladen.

   - **Ziel-Hostpool**: Wählen Sie beim Exportieren in einen Hostpool den Hostpool aus der Dropdown-Liste aus.
6. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

   Der Regelsatz-Exportvorgang beginnt.

Regelsätze importieren

Nerdio Manager ermöglicht es Ihnen, Regelsätze zu importieren, die zuvor in eine JSON-Datei oder aus einem Hostpool exportiert wurden.

So importieren Sie Regelsätze:

1. Finden Sie den Hostpool, mit dem Sie arbeiten möchten.
2. Wählen Sie im Aktionsmenü **Anwendungen**> **Installierte Apps** aus.
3. Wählen Sie im Aktionsmenü **Regelsatz hinzufügen** die Option **Regelsätze importieren**.
4. Geben Sie die folgenden Informationen ein:
   - **Importieren von**: Wählen Sie den Importort aus der Dropdown-Liste aus.
   - **Hostpool**: Wählen Sie beim Importieren aus einem Hostpool den Hostpool aus der Dropdown-Liste aus.
   - **JSON-Datei**: Wählen Sie beim Importieren aus einer JSON-Datei die Datei aus.
   - **Importierte Regelsätze aktivieren**: Wählen Sie diese Option, um die importierten Regelsätze nach dem Import zu aktivieren.

5. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Installieren**.

   Der Regelsatz-Importvorgang beginnt.

Schritt 6: MSIX App Attach

Konfigurieren Sie als Nächstes **MSIX App Attach**. Damit stellt Nerdio Manager Anwendungen auf Sitzungshosts bereit, ohne sie direkt auf dem Image zu installieren.

Ein MSIX App Attach-Image ist ein erweiterter Container (eine VHD-, VHDX- oder CIM-Datei), der ein oder mehrere extrahierte MSIX-Pakete enthält. Nerdio Manager bindet diese Images auf den Sitzungshosts im Hostpool ein. So stehen die paketierten Anwendungen den Usern zur Verfügung, sobald sie sich anmelden.

In diesem Abschnitt:

1. App Attach-Images und -Pakete verwalten [231]
2. App Attach-Zuweisungen verwalten [239]
3. Azure Files-Berechtigungen für App Attach konfigurieren [242]

App Attach-Images und -Pakete verwalten

Nerdio Manager ermöglicht Ihnen die Verwaltung von App Attach-Images und -Paketen.

Beispiel-Workflow

Dies ist ein Beispiel-Workflow:

- Laden Sie das App Attach-Image in die Nerdio Manager-verwaltete Image-Bibliothek hoch. Siehe App Attach-Image-Datei hochladen [233] und MSIX-Paketdatei hochladen [234].
- Fügen Sie die App Attach-Images in der Nerdio Manager-verwalteten Image-Bibliothek als App Attach-Pakete in Azure hinzu. Siehe Den App Attach-Paket-Assistenten verwenden [235].

> **Anmerkung**
>
> Der App Attach-Paket-Assistent ermöglicht es Ihnen, Usern und Gruppen in Hostpools das App Attach-Paket zuzuweisen.

- Sie können Image-Versionen nach Bedarf verwalten. Siehe Eine neue Version einer App hochladen [237] und Nerdio App Attach-Image-Versionen verwalten [238].
- Sie können Zuweisungen nach Bedarf verwalten. Siehe App Attach-Zuweisungen verwalten [239].

Beispiel-VHD(X)-Pakete und Zertifikat

Um Ihnen den Einstieg zu erleichtern, haben wir einige VHD(X)-Pakete für beliebte Anwendungen erstellt, die Sie herunterladen und zu Testzwecken in Ihrer AVD-Umgebung verwenden können.

> **Anmerkung**
>
> Diese Pakete sind nicht für Produktionszwecke bestimmt. Sie sollten für Proof-of-Concept-Tests verwendet werden.

Google Chrome

- VHD-Datei MSIX-Paket
- MSIX-Datei

Mozilla Firefox

- VHD-Datei MSIX-Paket
- MSIX-Datei

Notepad++

- VHD-Datei MSIX-Paket
- MSIX-Datei

PuTTY

- VHD-Datei MSIX-Paket
- MSIX-Datei

VLC

- VHD-Datei MSIX-Paket
- MSIX-Datei

Zertifikat

- Das Zertifikat kann hier heruntergeladen werden.
- Das Zertifikat ist für alle Pakete identisch.

Laden Sie eine App Attach-Image-Datei hoch

Sie können ein VHD/VHDX/CIM-Image in die Nerdio Manager-verwaltete Image-Bibliothek hochladen.

So laden Sie ein Image hoch:

1. Navigieren Sie zu **Anwendungen** > **Katalog** > **App Attach**.
2. Wählen Sie den Bereich **Nerdio App Attach-Images** aus.
3. Wählen Sie **Image hochladen** aus.
4. Geben Sie die folgenden Informationen ein:
   - **Anzeigename**: Geben Sie den Namen ein, der in der Image-Liste angezeigt werden soll.
   - **Beschreibung**: Geben Sie eine Beschreibung ein.
   - **Version**: Geben Sie die Image-Versionsnummer an, die hochgeladen werden soll. Diese muss eindeutig sein.
   - **Speicherorte**: Wählen Sie aus der Dropdown-Liste den oder die verknüpften App-Speicherorte in der AD-integrierten Azure Files-Freigabe aus.

> **Anmerkung**
> - App Attach unterstützt keine Entra Domain Services. Dies muss Active Directory Domain Services (ADDS) sein.
> - Damit App Attach in Entra ID funktioniert, sollten Sie **Entra ID-Hostunterstützung** aktivieren. Navigieren Sie zu **Speicher** > **Azure Files** > **Speicherkonto verwalten**.

- **Image-Dateien**: Wählen Sie die VHD(X)-/CIM-Datei(en) aus, die die aus dem MSIX-Installer erweiterte App Attach-Anwendung enthält, oder laden Sie die App-V-Paketdatei(en) hoch.
- **Zertifikatsdateien (.cer)**: Wählen Sie die Zertifikatsdatei(en) aus.

> **Anmerkung**
>
> Ein Zertifikat, das zum Erstellen des Pakets verwendet wurde, muss auf allen Sitzungshost-VMs installiert sein. Wenn Sie zum Erstellen des Pakets ein selbstsigniertes Zertifikat verwendet haben, laden Sie es hier hoch; es wird dann automatisch für Sie installiert. Alternativ können Sie das Zertifikat auf dem Desktop-Image installieren und bei den Sitzungshost-VMs ein Reimaging vornehmen.

5. Nachdem Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Hochladen** aus.

Das Image wird in den Nerdio Manager hochgeladen.

Laden Sie eine MSIX-Paketdatei hoch

Wenn Sie noch keine VHD/VHDX/CIM mit dem Image haben, können Sie mit Nerdio Manager die MSIX-Datei hochladen, und Nerdio Manager erstellt automatisch eine VHD-Datei für Sie. Das VHD-Image wird der Nerdio Manager-verwalteten Image-Bibliothek hinzugefügt.

So laden Sie eine MSIX-Paketdatei hoch:

1. Navigieren Sie zu **Anwendungen** > **Katalog** > **App Attach**.
2. Wählen Sie den Bereich **Nerdio App Attach-Images** aus.

3. Wählen Sie **MSIX-App(s) hochladen** aus.
4. Geben Sie die folgenden Informationen ein:
   - **Image-Name**: Geben Sie den Image-Namen ein.
   - **Speicherorte**: Wählen Sie aus der Dropdown-Liste die Speicherorte aus, in denen die App Attach-Anwendungen gespeichert sind.

     > **Anmerkung**
     > - Der Speicherort sollte sich in derselben Azure-Region wie die Sitzungshost-VMs befinden, die auf die App zugreifen.
     > - Nur in den Editionen **Premium** und **Core** gilt der erste ausgewählte Standort als primär. Der Hauptstandort enthält alle Versionen der Anwendung.

   - **MSIX-Datei(en)**: Wählen Sie die MSIX-Datei(en) aus.
   - **Zertifikatsdateien (.cer)**: Wählen Sie optional die Zertifikatsdatei(en) aus.

     > **Anmerkung**
     >
     > Um die MSIX-App in einen VHDX-Container zu erweitern, wird eine temporäre VM erstellt, um den Vorgang auszuführen, und anschließend gelöscht. Wir empfehlen, dass Sie Nerdio Manager einfach die Konfiguration der temporären VM übernehmen lassen. Wählen Sie andernfalls **Erweiterte Einstellungen anzeigen**, um die Details der temporären VM anzugeben.

5. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

   Die MSIX-Datei wird hochgeladen und Nerdio Manager beginnt mit dem Prozess der Erstellung einer VM, um die Datei in ein VHDX-Image zu paketieren.

Verwenden Sie den App Attach-Paket-Assistenten

Der App Attach-Paket-Assistent fügt die ausgewählten App Attach-Images in der von Nerdio Manager verwalteten Image-Bibliothek als App

Attach-Pakete in Azure hinzu. Darüber hinaus können Sie die Pakete allen gewünschten Usern und Gruppen in den angegebenen Hostpools zuweisen.

So verwenden Sie den App Attach-Paket-Assistenten:

1. Navigieren Sie zu **Anwendungen** > **Katalog** > **App Attach**.
2. Wählen Sie den Bereich **App Attach-Pakete** aus.
3. Wählen Sie **+ App Attach-Paket hinzufügen** aus.
4. Alternativ dazu im Bereich **Nerdio App Attach-Images**:
   - Suchen Sie das Image, mit dem Sie arbeiten möchten.
   - Wählen Sie im Aktionsmenü **Paket-Assistent** aus.
5. Geben Sie die Informationen im App Attach-Assistenten ein.
6. Geben Sie im Bereich **Image** die folgenden Informationen ein:
   - **Image-Quelle**: Wählen Sie aus der Dropdown-Liste die Image-Quelle aus.
   - **App Attach Image**: Wählen Sie aus der Dropdown-Liste das Anwendungs-Image aus.
   - **Image-Version**: Wählen Sie aus der Dropdown-Liste die Version des Anwendungs-Image aus.
   - **Temporäres Replikat**: Wählen Sie aus der Dropdown-Liste das Versionsreplikat aus, das zum Extrahieren von Metadaten aus dem ausgewählten App Attach-Image verwendet wird.
   - **Temporärer Hostpool**: Wählen Sie aus der Dropdown-Liste den temporären Hostpool aus, der zum Erweitern des Images verwendet wird.

> **Anmerkung**
>
> - Der temporäre Hostpool ist als Proxy erforderlich, um Metadaten aus dem ausgewählten App Attach-Image zu extrahieren. Es werden keine Änderungen an der Pool-Konfiguration vorgenommen, und es kann jeder beliebige Hostpool verwendet werden. Als bewährte Methode empfehlen wir jedoch die Erstellung eines dedizierten App Attach-Hostpools. Mindestens ein Desktop muss im Pool ausgeführt werden, um fortzufahren.
> - Der temporäre Hostpool wird auch verwendet, um das Image zu erweitern und zu testen, ob das Image gültig ist.

7. Geben Sie im Bereich **Paket** die folgenden Informationen ein:
   - **Ressourcengruppe**: Wählen Sie aus der Dropdown-Liste die Ressourcengruppe aus, in der das App Attach-Paket erstellt wird.

     > **Anmerkung**
     >
     > Diese Ressourcengruppe muss sich nicht in derselben Region wie die Poolzuweisungen befinden, wir empfehlen dies jedoch als bewährte Vorgehensweise.

   - **Pakete**: Wählen Sie aus der Dropdown-Liste ein oder mehrere MSIX-Pakete aus, die Usern auf den ausgewählten Hostpools zur Verfügung gestellt werden sollen.
8. Geben Sie im Bereich **Zuweisungen** die folgenden Informationen ein:
   - **Hostpools**: Wählen Sie aus der Dropdown-Liste einen oder mehrere Hostpools aus dem Abonnement der ausgewählten Ressourcengruppe aus, die dem Paket bzw. den Paketen zugewiesen sind.
   - **User und Gruppen**: Wählen Sie aus der Dropdown-Liste die autorisierten User und Gruppen aus, die die Anwendungen in den ausgewählten Paketen ausführen können.
9. Überprüfen Sie im Bereich **Zusammenfassung** die Auswahl.
10. Sobald Sie die gewünschten Auswahlmöglichkeiten überprüft haben, wählen Sie **Ausführen**.

Die Aufgabe des App Attach-Assistenten wird gestartet. Sie können den Fortschritt der Aufgabe im Fenster **Aufgaben** sehen.

Eine neue Version einer App hochladen

Nerdio Manager ermöglicht es Ihnen, mehrere Versionen einer App zu haben. Daher können Sie nach Belieben neue Versionen einer App hochladen.

So laden Sie eine neue Version einer App hoch:

1. Navigieren Sie zu **Anwendungen** > **Katalog** > **App Attach**.
2. Wählen Sie den Bereich **Nerdio App Attach-Images** aus.
3. Suchen Sie das Image, mit dem Sie arbeiten möchten.
4. Wählen Sie im Aktionsmenü **Version hochladen** aus.

5. Geben Sie die folgenden Informationen ein:
   - **Version**: Geben Sie die Image-Versionsnummer an, die hochgeladen werden soll. Diese muss eindeutig sein.
   - **Speicherorte**: Wählen Sie die Speicherorte aus, an denen die App Attach-App gespeichert werden soll.

     > **Anmerkung**
     >
     > Der Speicherort sollte sich in derselben Azure-Region wie die Sitzungshost-VMs befinden, die auf die App zugreifen.

   - **Image-Dateien**: Wählen Sie aus der Dropdownliste das Anwendungs-Image aus.
   - **Zertifikatsdateien (.cer)**: Wählen Sie optional die Zertifikatsdatei(en) aus.

     > **Anmerkung**
     >
     > Ein Zertifikat, das zum Erstellen des Pakets verwendet wurde, muss auf allen Sitzungshost-VMs installiert sein. Wenn Sie zum Erstellen des Pakets ein selbstsigniertes Zertifikat verwendet haben, laden Sie es hier hoch; es wird dann automatisch für Sie installiert. Alternativ können Sie das Zertifikat auf dem Desktop-Image installieren und ein Reimaging der Sitzungshost-VMs vornehmen.

6. Nachdem Sie alle gewünschten Informationen eingegeben haben, wählen Sie **Hochladen** aus.

Nerdio App Attach-Image-Versionen verwalten

Nerdio Manager ermöglicht es Ihnen, Image-Versionen zu verwalten. Dies umfasst das Hochladen eines neuen Images, das Ändern seines Speicherorts oder das Aktualisieren der Hostpools mit der gewünschten Version.

So verwalten Sie Image-Versionen:

1. Navigieren Sie zu **Anwendungen** > **Katalog** > **App Attach**.
2. Wählen Sie den Bereich **Nerdio App Attach-Images** aus.

3. Suchen Sie das Image, mit dem Sie arbeiten möchten.
4. Wählen Sie das Symbol **Image-Versionen**.
5. Suchen Sie die Image-Version, die Sie als Standard festlegen möchten.
6. Führen Sie einen der folgenden Schritte für die Image-Version aus:
   - Wählen Sie das Symbol **Hostpools aktualisieren**, um die zugewiesenen Hostpools mit der ausgewählten Version zu aktualisieren.
   - Wählen Sie im Aktionsmenü **Speicherorte ändern**, um den Speicherort des Images zu ändern.
7. Alternativ auswählen Sie **+ Neue Version hochladen**, um eine neue Version hochzuladen.

Verwandte Themen

App Attach-Zuweisungen verwalten [239]

App Attach-Zuweisungen verwalten

Nerdio Manager ermöglicht es Ihnen, Usern und Gruppen in Hostpools App Attach-Pakete zuzuweisen. Sie müssen zuerst ein App Attach-Image hochladen und ein App Attach-Paket hinzufügen, bevor Sie die Zuweisungen durchführen können. Weitere Informationen finden Sie unter App Attach-Images und -Pakete verwalten [231].

> **Anmerkung**
>
> Diese Zuweisungen können mithilfe des App Attach-Paket-Assistenten durchgeführt werden. Weitere Informationen finden Sie unter App Attach-Images und -Pakete verwalten [231].

MSIX App Attach-Paket zu einem Hostpool hinzufügen

Sie können einem Hostpool ein MSIX App Attach-Paket zuweisen.

> ⚠ **Warnung**
>
> MSIX App Attach ist veraltet. Microsoft aktualisiert das Feature nicht mehr. Wir empfehlen, dass Sie alle neuen Pakete als App Attach erstellen.

So fügen Sie einem Hostpool ein MSIX App Attach-Paket hinzu:

1. Finden Sie den Hostpool, dem Sie die App zuweisen möchten.
2. Wählen Sie im Menü für weitere Aktionen ⋮ das Symbol **Anwendungen** > **Katalog** > **App Attach** aus.
3. Wenn das Fenster **App Attach** angezeigt wird, wählen Sie im Menü für weitere Aktionen ⋮ das Symbol **MSIX App Attach-Paket hinzufügen** aus.
4. Geben Sie die folgenden Informationen ein:
   - **Image-Quelle**: Wählen Sie aus der Dropdown-Liste den Ort des Images aus, das MSIX-Pakete enthält.

     > **Anmerkung**
     >
     > Das Image kann in der Image-Bibliothek von Nerdio Manager oder in einer SMB-Datenfreigabe gespeichert werden, auf die Sitzungshost-VMs Zugriff haben. Wenn Sie MSIX-Images mit Nerdio Manager hochgeladen oder erstellt haben, wählen Sie **Image-Bibliothek** aus.

   - **MSIX App Attach Image**: Wählen Sie aus der Dropdown-Liste ein MSIX App Attach Image aus, das die MSIX-Pakete enthält.
   - **Image-Version**: Wählen Sie aus der Dropdown-Liste die Version des Images aus, die dem Hostpool hinzugefügt werden soll.
   - **Pakete**: Wählen Sie aus der Dropdown-Liste ein oder mehrere MSIX-Pakete/-Apps aus, die im Image vorhanden sind, um sie Usern in diesem Hostpool zur Verfügung zu stellen.
5. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

Zuweisen eines App Attach-Pakets an User und Gruppen in Hostpools

Sie können das Paket Usern und Gruppen in Hostpools zuweisen.

So weisen Sie ein App Attach-Paket Usern und Gruppen zu:

1. Navigieren Sie zu **Anwendungen** > **Katalog** > **App Attach**.
2. Wählen Sie den Bereich **App Attach-Pakete** aus.
3. Finden Sie das App Attach-Paket, mit dem Sie arbeiten möchten.
4. Wählen Sie das Symbol **Zuweisungen** aus.
5. Geben Sie die folgenden Informationen ein:
   - **User und Gruppen**: Wählen Sie aus der Dropdown-Liste die User und Gruppen aus, denen das Paket zugewiesen werden soll.

     > **Anmerkung**
     >
     > Sie müssen User und/oder Gruppen angeben.

   - **Hostpools**: Wählen Sie aus der Dropdown-Liste die Hostpools aus, denen das Paket zugewiesen werden soll.
6. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

App Attach-Pakete einem Hostpool zuweisen

Sie können App Attach-Pakete einem Hostpool zuweisen.

So weisen Sie einem Hostpool eine App zu:

1. Finden Sie den Hostpool, dem Sie die App zuweisen möchten.
2. Wählen Sie im Menü für weitere Aktionen das Symbol **Anwendungen** > **Katalog** > **App Attach** aus.
3. Wenn das Fenster **App Attach** angezeigt wird, wählen Sie **App Attach-Pakete zuweisen**.
4. Geben Sie die folgenden Informationen ein:
   - **App Attach-Pakete**: Wählen Sie aus der Dropdown-Liste das oder die App Attach-Paket(e) aus.
5. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK**.

Konfigurieren von Azure Files-Berechtigungen für App Attach

Nerdio Manager verwendet die Azure Files-Freigabetechnologie, um App Attach-Pakete und die zugehörigen Metadaten zu speichern. Sie können eine vorhandene Azure Files-Freigabe verwenden oder mit Nerdio Manager eine neue erstellen.

> **Anmerkung**
>
> Was Sie konfigurieren müssen, hängt davon ab, wie Ihre Sitzungshosts eingebunden sind. Mit Entra ID verbundene Hosts und mit AD DS verbundene Hosts haben unterschiedliche, sich nicht überschneidende Anforderungen. Arbeiten Sie den Abschnitt durch, der zu Ihren Hosts passt.

App Attach unterstützt die folgenden Identitätsanbieter:

- Microsoft Entra ID
- Active Directory Domain Services (AD DS)

Hintergrundinformationen zu App Attach selbst finden Sie im Microsoft-Artikel App attach and MSIX app attach in Azure Virtual Desktop.

Sitzungshosts, die mit Microsoft Entra ID verbunden sind

Mit Entra ID verbundene Hosts können App Attach-Anwendungen verwenden. Die einzigen Anforderungen betreffen das Storage-Konto, das die App Attach-Images enthält:

- Es muss sich im selben Abonnement wie die Sitzungshosts befinden.
- Es muss über eine Rollenzuweisung **Reader and Data Access** verfügen, zu deren Mitgliedern **Azure Virtual Desktop** und **Windows Virtual Desktop ARM Provider** gehören.

Nerdio Manager erstellt diese Rollenzuweisung für Sie, wenn Sie **Entra ID host support** für das Storage-Konto aktivieren. Sie können dies für eine neue Freigabe oder eine bereits vorhandene Freigabe tun.

Anmerkung

Das Storage-Konto kann mit Active Directory verbunden, mit Entra ID verbunden oder gar nicht verbunden sein. Sie müssen für Hosts, die mit Entra ID verbunden sind, weder Berechtigungen auf Freigabeebene noch Berechtigungen für New Technology File System konfigurieren.

So aktivieren Sie die Entra ID-Hostunterstützung für eine vorhandene Azure Files-Freigabe:

1. Navigieren Sie zu **Cloud-Desktops > Speicher > Azure Files**.
2. Finden Sie die Azure Files-Freigabe, in der Ihre App Attach-Images gespeichert sind.
3. Wählen Sie im Aktionsmenü der Freigabe **Verwalten** aus.
4. Wechseln Sie im Assistenten zum Tab **Storage-Konto** und wählen Sie **Entra ID host support** aus.
5. Wählen Sie **SPEICHERN** aus.

Anmerkung

Durch Aktivieren dieser Option wird dem Storage-Konto die Rollenzuweisung **Reader and Data Access** mit **Azure Virtual Desktop** und **Windows Virtual Desktop ARM Provider** als Mitgliedern hinzugefügt. Wenn Sie die Zuweisung lieber selbst vornehmen möchten, fügen Sie dem Storage-Konto unter **Zugriffssteuerung (IAM)** im Azure-Portal die Rolle mit denselben zwei Mitgliedern hinzu.

Sitzungshosts, die mit AD DS verbunden sind

Alle drei der folgenden Bedingungen sind zwingend erforderlich:

1. Das Storage-Konto, in dem die App Attach-Images gespeichert sind, ist mit AD DS verbunden.

2. Auf der Datenfreigabe sind die App Attach-Berechtigungen für New Technology File System konfiguriert.
3. Freigabeberechtigungen sind konfiguriert.

App Attach-Berechtigungen im New Technology File System

New Technology File System-Standardberechtigungen für Datenfreigaben

- `BUILTIN\Administrators:(OI)(CI)(F)`
- `BUILTIN\Users:(RX)`
- `BUILTIN\Users:(OI)(CI)(IO)(GR,GE)`
- `NT AUTHORITY\Authenticated Users:(OI)(CI)(M)`
- `NT AUTHORITY\SYSTEM:(OI)(CI)(F)`
- `NT AUTHORITY\SYSTEM:(F)`
- `CREATOR OWNER:(OI)(CI)(IO)(F)`

New Technology File System-Berechtigungen für App Attach-Datenfreigaben

- `BUILTIN\Users:(RX)`
- `BUILTIN\Users:(OI)(CI)(IO)(GR,GE)`
- `NT AUTHORITY\Authenticated Users:(OI)(CI)(M)`
- `CREATOR OWNER:(OI)(CI)(IO)(F)`

Tipp

Lassen Sie Nerdio Manager diese Berechtigungen zuweisen, statt sie manuell festzulegen. Wählen Sie im Azure Files-Assistenten **New Technology File System-Dateiberechtigungen zuweisen** und dann **App Attach**, wodurch authentifizierten Usern Leseberechtigungen für Unterverzeichnisse in der Datenfreigabe erteilt werden. Dies ist die empfohlene Option für Datenfreigaben mit App Attach-Anwendungen.

Anmerkung

Beim Zuweisen von New Technology File System-Dateiberechtigungen wird automatisch eine temporäre VM erstellt, die die Aufgabe der Berechtigungszuweisung ausführt.

Freigabeberechtigungen

Wählen Sie eine der folgenden Konfigurationen.

Option 1: Schreibgeschützter Zugriff für alle authentifizierten Identitäten

Legen Sie die Standardfreigabeberechtigung für das Storage-Konto für alle authentifizierten Identitäten auf mindestens **Storage File Data SMB Share Reader** fest.

Verwenden Sie in Nerdio Manager die Option **Freigabeberechtigungen** im Azure Files-Assistenten, um dies festzulegen. **SMB Share Reader** gewährt allen authentifizierten Usern schreibgeschützten Zugriff auf die Datenfreigabe. Dies ist für App Attach erforderlich.

Option 2: Schreibgeschützter Zugriff für Domänencomputer

1. Erstellen Sie in Active Directory eine neue globale Sicherheitsgruppe in einer Organisationseinheit (OU), die mit ADConnect mit Entra ID synchronisiert wird.
2. Fügen Sie **Domain Computers** der neuen Gruppe hinzu.
3. Öffnen Sie im Azure-Portal die **Zugriffssteuerung** der Datenfreigabe und fügen Sie die neue Sicherheitsgruppe mit mindestens der Rolle **Storage File Data SMB Share Reader** hinzu.

Anmerkung

Möglicherweise müssen Sie auf den nächsten Synchronisierungszyklus warten, damit neue Gruppen in Entra ID verfügbar sind.

Option 3: Eine benutzerdefinierte Konfiguration

Jede Konfiguration, die den Sitzungshost-Computerobjekten mindestens Lesezugriff auf die Datenfreigabe gewährt, wird unterstützt. Passen Sie die oben genannten Optionen an die Sicherheitsrichtlinien Ihrer Organisation an.

Verwandte Themen

- Erstellen und Verwalten konfigurierter Azure Files-Datenfreigaben [176]
- App Attach
- Verwalten von App Attach-Images und -Paketen [231]
- Erstellen und Verwalten konfigurierter Azure NetApp Files [202]

Schritt 7: Rollenbasierte Zugriffssteuerung (RBAC)

Konfigurieren Sie zum Schluss die **rollenbasierte Zugriffssteuerung (RBAC)**. So erhalten alle in Ihrem Team den passenden Zugriff auf Nerdio Manager: von Admins mit vollen Berechtigungen bis hin zu Helpdesk-Mitarbeitenden, die nur bestimmte Aufgaben ausführen müssen.

In diesem Abschnitt:

1. Rollenbasierte Zugriffssteuerung (RBAC) in Nerdio Manager [247]
2. Rollenbasierte Zugriffssteuerung (RBAC): Benutzerdefinierte Rollen [251]
3. Rollenbasierte Zugriffssteuerung (RBAC): Mehrfache Gruppenzuweisungen [255]

Rollenbasierte Zugriffssteuerung (RBAC) in Nerdio Manager

> **Anmerkung**
>
> Es gibt eine Entra ID-Einschränkung: Die Owner-Rolle für eine Enterprise-Anwendung wird nur automatisch einem direkten User zugewiesen und kann nicht mithilfe von Nerdio Manager einer Gruppe zugewiesen werden. Daher müssen Administratoren in Nerdio Manager direkt zugewiesen werden, damit Nerdio Manager die Owner-Rolle automatisch zuweist.

Sie können rollenbasierte Zugriffssteuerung (RBAC) verwenden, um Usern in Ihrer Organisation das Anmelden bei Nerdio Manager zu ermöglichen und zu steuern, welche Aktionen sie nach der Anmeldung ausführen können.

Die folgenden Rollen sind verfügbar:

- **AVD-Administrator**: Ein User mit der Rolle „AVD-Administrator“ hat vollständigen Zugriff auf alle Bereiche von Nerdio Manager. Nur AVD-Administratoren können User und Rollen verwalten.
- **Desktop-Admin**: Ein User mit der Rolle „Desktop-Admin“ hat vollständigen Zugriff auf Benutzersitzungen, die Möglichkeit, Hostpools anzuzeigen sowie Sitzungshosts ein-/auszuschalten und neu zu starten, hat jedoch nicht die Möglichkeit, Hosts hinzuzufügen oder zu entfernen oder Hostpool-Einstellungen zu ändern. Diese Rolle ermöglicht außerdem den vollständigen Zugriff auf Desktop-Images und Scripted Actions.
- **Helpdesk**: Ein User mit der Rolle „Helpdesk“ hat nur Zugriff auf die Verwaltung von Benutzersitzungen.
- **Reviewer**: Ein User mit der Rolle „Reviewer“ hat nur Anzeigezugriff auf alle Bereiche von Nerdio Manager. Sie können keine Bearbeitungen vornehmen und keine Änderungen speichern.
- **Endbenutzer**: Ein User mit der Rolle „Endbenutzer“ kann seine eigenen Sitzungen anzeigen und verwalten (Nachricht senden, abmelden, Verbindung trennen). User persönlicher Desktops können ihre persönlichen Desktops neustarten, ausschalten und einschalten.

Weitere Informationen zu benutzerdefinierten Rollen finden Sie unter Benutzerdefinierte Rollen für die rollenbasierte Zugriffssteuerung (RBAC) [251].

Begleitvideo

https://fast.wistia.net/embed/iframe/e1e4p9ff5r?seo=false&videoFoam=true

Verwaltung von Usern und Rollen

Nerdio Manager ermöglicht es Ihnen, die konfigurierten rollenbasierten Zugriffszuweisungen anzuzeigen.

So zeigen Sie RBAC-Rollenzuweisungen an:

- Navigieren Sie zu **System** > **RBAC** > **Zuweisungen**. Die Liste der User und ihrer RBAC-Rollenzuweisungen wird angezeigt.

> **Anmerkung**
>
> - Der Suchbereich oben ermöglicht Ihnen die Suche nach verschiedenen Feldern, einschließlich Name, Benutzername, Rolle und Workspace.
> - Sie können das System anweisen, bis zu 1.000 Zeilen auf einer einzigen Seite aufzulisten. Dies ist besonders nützlich, wenn Sie eine Liste von Endbenutzern betrachten, die oft Hunderte oder Tausende umfassen kann.
> - Wählen Sie den Abwärtspfeil neben **Bearbeiten**, um ein Aktionenmenü anzuzeigen.

User zu Rollen hinzufügen

Sie können User zu Rollen/Workspaces hinzufügen.

So fügen Sie User zu Rollen/Workspaces hinzu:

1. Navigieren Sie zu **System** > **RBAC** > **Zuweisungen**.

2. Gehen Sie wie folgt vor:

   Wählen Sie **Neue Zuweisung** aus.
3. Geben Sie im Dialogfeld **Rolle hinzufügen** die folgenden Informationen ein:
   - **Rolle**: Wählen Sie aus der Dropdown-Liste eine Rolle aus.
   - **User/Gruppen**: Wählen Sie aus der Dropdown-Liste die User/Gruppen aus, denen Sie Zugriff gewähren möchten.
   - **AVD-Tenant**: Wählen Sie aus der Dropdown-Liste den/die AVD-Tenant(s) aus, denen Sie Zugriff gewähren möchten.
   - **Workspace**: Wählen Sie für Workspace-Rollen aus der Dropdown-Liste den/die Workspace(s) aus, auf den/die der User Zugriff haben soll.
   - **Images**: Wählen Sie für Desktop-Image-Rollen aus der Dropdown-Liste das/die Desktop-Image(s) aus, auf das/die der User Zugriff haben soll.
   - **Hostpools**: Wählen Sie für Hostpool-Rollen aus der Dropdown-Liste den/die Hostpool(s) aus, auf den/die der User Zugriff haben soll.
4. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK** aus.

> **Anmerkung**
> - Die Änderungen werden als Aufgabe protokolliert. Sie können den Status der Aufgabe überprüfen, um sicherzustellen, dass die Aufgabe erfolgreich abgeschlossen wurde.
> - Sobald der Zugriff gewährt wurde, können sich User mit ihrem Entra ID-Benutzernamen und Passwort bei Nerdio Manager anmelden. Teilen Sie dem User einfach die URL für Nerdio Manager aus der Adressleiste Ihres Browsers mit. Wenn MFA erzwungen wird, muss der User während der Anmeldung den MFA-Prozess durchlaufen.

Rolle eines User bearbeiten

Sie können die Rolle eines User oder die Workspaces, auf die der User Zugriff hat, ändern.

So bearbeiten Sie einen User:

1. Navigieren Sie zu **System** > **RBAC** > **Zuweisungen**.
2. Gehen Sie wie folgt vor:

   Suchen Sie den User, den Sie bearbeiten möchten, und wählen Sie das Symbol „Bearbeiten“ .
3. Sobald Sie die Änderungen vorgenommen haben, wählen Sie **OK**.

> **Anmerkung**
>
> Die Änderungen werden als Aufgabe protokolliert. Sie können den Status der Aufgabe überprüfen, um sicherzustellen, dass die Aufgabe erfolgreich abgeschlossen wurde.

User-Zugriff entfernen

Sie können verhindern, dass ein User auf Nerdio Manager zugreift, indem Sie den Zugriff des Users entfernen.

So entfernen Sie den Zugriff eines User:

1. Navigieren Sie zu **System** > **RBAC** > **Zuweisungen**.
   - Gehen Sie wie folgt vor:

     Suchen Sie den User, dem Sie den Zugriff entziehen möchten, und wählen Sie im Menü „Weitere Aktionen“ die Option **Zugriff entfernen**.
2. Wählen Sie im Bestätigungsfenster **OK**.

> **Anmerkung**
>
> Die Änderungen werden als Aufgabe protokolliert. Sie können den Status der Aufgabe überprüfen, um sicherzustellen, dass die Aufgabe erfolgreich abgeschlossen wurde.

Rollenbasierte Zugriffssteuerung (RBAC): Benutzerdefinierte Rollen

Sie können benutzerdefinierte Rollendefinitionen erstellen, um den Zugriff auf alle Bereiche von Nerdio Manager zu steuern. Benutzerdefinierte Rollen definieren den Scope und die Zugriffsebene und können Usern und Sicherheitsgruppen zugewiesen werden. User können auf Module im Lesezugriffs- oder Verwaltungsmodus zugreifen.

So erstellen Sie eine benutzerdefinierte Rollendefinition:

1. Navigieren Sie zu **System** > **RBAC** > **Definitionen**.
2. Wählen Sie **Neue Definition**.
3. Geben Sie die folgenden Informationen ein:
   - **Name**: Geben Sie den Namen der benutzerdefinierten Rolle ein.
   - **Beschreibung**: Geben Sie eine Beschreibung der benutzerdefinierten Rolle ein.
   - **Module**: Wählen Sie alle zutreffenden Module und Modi aus.

Tabelle 1.

Module	Modi
OBSERVABILITY	
Insights	• **Lesezugriff**: Bietet Usern Lesezugriff auf die Insights-Dashboards. • **Verwalten**
Observability > Advisor > Modeler	• **Lesezugriff** • **Verwalten**
Observability > Advisor > Empfehlungen	• **Lesezugriff** • **Verwalten**
Observability > Advisor > Regeln	• **Lesezugriff** • **Verwalten**
AVD UND SITZUNGEN	

Module	Modi
Workspaces	• **Lesezugriff** • **Verwalten** • **Hosts verwalten**: Ermöglicht Usern das Verwalten von Hosts innerhalb zugewiesener Hostpools. • **Zuweisungen verwalten**: Ermöglicht Usern das Verwalten von Zuweisungen innerhalb zugewiesener Hostpools. • **Sitzungen verwalten**: Ermöglicht Usern, Sitzungen innerhalb zugewiesener Hostpools zu verwalten. • **Betriebszustand verwalten**: Ermöglicht Usern, den Betriebszustand von Sitzungen innerhalb zugewiesener Hostpools zu verwalten. • **Drain-Modus verwalten**: Ermöglicht Usern, den Drain-Modus für Sitzungen innerhalb zugewiesener Hostpools zu verwalten. • **Scripted Actions ausführen**: Ermöglicht Usern, Scripted Actions innerhalb zugewiesener Hostpools auszuführen. • **Console Connect-Bediener**: Ermöglicht Usern, Console Connect-Rollen zu verwalten.
Desktop-Images	• **Lesezugriff** • **Verwalten**
App Attach	• **Lesezugriff** • **Verwalten**
Portal	• **Verwalten**
ENDPOINT MANAGEMENT	
Intune (Globale Rollen)	• **Lesezugriff** • **Verwalten**
Intune (Schreibgeschützte Rollen)	• **Geräte lesen** • **Richtlinien lesen** • **Anwendungen und App-Richtlinien lesen** • **Update-Ringe und Richtlinien lesen** • **Skripte lesen** • **Read BitLocker** • **Antivirus-Einstellungen lesen** • **Benutzererfahrung lesen** • **User-Gruppen lesen** • **Ort des Geräts lesen** • **Genehmigungen lesen**

Module	Modi
Intune (Rollen verwalten)	• **Geräte verwalten** • **Privilegierte Geräte verwalten** • **Manage BitLocker** • **Antivirus-Einstellungen verwalten** • **Gerätegruppen verwalten** • **User-Gruppen verwalten** • **„Gerät finden" verwalten** • **Richtlinien verwalten** • **Anwendungen und App-Richtlinien verwalten** • **Update-Ringe und Richtlinien verwalten** • **Console Connect-Bediener** • **Genehmigungen verwalten** • **Skripte verwalten** • **Microsoft-Lizenzen verwalten**
Intune > Windows 365	• **Lesezugriff** • **Verwalten**
ANWENDUNGSVERWALTUNG (Unified Application Management)	
Unified Application Management > Deployment-Richtlinien	• **Lesezugriff** • **Verwalten**
Unified Application Management > Application Groups	• **Lesezugriff** • **Verwalten**
Unified Application Management > Unified Catalog	• **Katalog lesen** • **Katalog verwalten**: Ermöglicht Usern, Kataloge von Unified Application Management zu verwalten und Aufgaben wie das Importieren und Bereitstellen von Anwendungen auszuführen. • **Shell-App-Parameter verwalten**: Ermöglicht Usern das Verwalten von Shell-App-Parametern.
AUTOMATISIERUNG	
Scripted Actions	• **Lesezugriff** • **Verwalten**
Scripted Sequences	• **Lesezugriff** • **Verwalten**
Scripted Sequences > Ausführungen	• **Lesezugriff** • **Verwalten**
Task Worker Analytics	• **Lesezugriff** • **Verwalten**
SPEICHER	

Module	Modi
Cloud-Desktops > Speicher > Azure Files	• **Lesezugriff** • **Verwalten** • **Profile verwalten**: Ermöglicht Usern das Verwalten von FSLogix-Profilen, ohne dass eine aktive User-Sitzung erforderlich ist und ohne dass Vollzugriff auf die Datenfreigabe gewährt werden muss.
Cloud-Desktops > Speicher > Azure NetApp Files	• **Lesezugriff** • **Verwalten**
Cloud-Desktops > Speicher > Log Analytics	• **Lesezugriff** • **Verwalten**
VORGÄNGE	
Monitoring	• **Lesezugriff**
Protokolle	• **Lesezugriff**
Migrieren	• **Lesezugriff** • **Verwalten**
Sichere Variablen	• **Lesezugriff** • **Verwalten** • **Geheimnis anzeigen**

4. Sobald Sie alle gewünschten Informationen eingegeben haben, wählen Sie **OK** aus.

> **Anmerkung**
>
> In der Liste der Definitionen können Sie eine benutzerdefinierte Rolle bearbeiten oder löschen.

Weitere Informationen finden Sie unter Rollenbasierte Zugriffssteuerung (RBAC) in Nerdio Manager.

Wie benutzerdefinierte Rollen in Microsoft Entra ID angezeigt werden

Eine benutzerdefinierte Rolle hat kein Gegenstück in Microsoft Entra ID. Wenn Sie einem User eine benutzerdefinierte Rolle zuweisen, schreibt Nerdio Manager die Entra-App-Rollenzuweisung für die Nerdio Manager-Enterprise-Anwendung als Zuweisung der integrierten Rolle **Endbenutzer**, der integrierten Rolle mit den geringsten Berechtigungen nach dem Prinzip Least Privilege. Nerdio Manager erzwingt dann die Berechtigungen der benutzerdefinierten Rolle, wenn sich der User anmeldet. Infolgedessen sehen Sie in

Entra ID nur die integrierten Rollen und können dort keine benutzerdefinierte Rolle anhand ihres Namens finden.

Damit Nerdio Manager diese Entra ID-Zuweisung automatisch vornehmen kann, muss die Nerdio Manager App-Registrierung über die Berechtigungen **Application.ReadWrite.All** und **AppRoleAssignment.ReadWrite.All** verfügen. Wenn diese Berechtigungen nicht erteilt wurden, weisen Sie dem User manuell die Rolle **Endbenutzer** zu, bevor Sie die benutzerdefinierte Rolle in Nerdio Manager zuweisen. Die Zuweisung der benutzerdefinierten Rolle funktioniert erst, wenn Sie dies getan haben.

So weisen Sie die Rolle „Endbenutzer“ manuell zu:

1. Navigieren Sie im Microsoft Entra Admin Center zu **Enterprise-Anwendungen** und wählen Sie Ihre Nerdio Manager Enterprise-Anwendung aus.
2. Wählen Sie **Benutzer und Gruppen** und dann **Benutzer/Gruppe hinzufügen** aus.
3. Wählen Sie den User und dann die Rolle **Endbenutzer** aus.
4. Wählen Sie **Zuweisen** aus.

Rollenbasierte Zugriffssteuerung (RBAC): Mehrfache Gruppenzuweisungen

Bei Verwendung eines der integrierten Konten wird der administrative Zugriff auf Nerdio Manager durch die Zuweisung einzelner Benutzer oder Gruppen zu der in Entra ID registrierten Anwendung von Nerdio Manager gesteuert. Ab Nerdio Manager v6.4 wurde die Unterstützung für kumulative RBAC für benutzerdefinierte Rollen eingeführt. Bitte lesen Sie dieses Dokument sorgfältig durch, um die Auswirkungen dieser Änderung zu verstehen. Details zum neuen und bisherigen Verhalten werden unten beschrieben.

Obwohl es für einen Benutzer möglich ist, durch mehrere Gruppenzugehörigkeiten zu Nerdio Manager berechtigt zu sein, ist dies bei Verwendung integrierter Konten oder einer Kombination aus integrierten Konten und benutzerdefinierten Rollen keine unterstützte Konfiguration. Es sollte darauf geachtet werden, dass Benutzer nur eine Zuweisung haben, die Zugriff auf Nerdio Manager gewährt, wenn integrierte Konten verwendet werden.

RBAC-Überlegungen ab Nerdio Manager v6.4 und höher

> **Anmerkung**
>
> Das hier beschriebene Verhalten ist der Standard für Neuinstallationen von Nerdio Manager. Bei bestehenden Installationen muss, falls kumulative RBAC-Funktionalität gewünscht ist, diese durch die App-Diensteinstellung **Features:CumulativeRbac** mit dem Wert **True** aktiviert werden.

Mit der Veröffentlichung von Nerdio Manager v6.4 wurde das Konzept der kumulativen RBAC für benutzerdefinierte Rollen eingeführt. Diese neue Funktionalität ermöglicht es, dass unterschiedliche Berechtigungen, die über separate individuelle Zuweisungen von Benutzer- oder Gruppenmitgliedschaften vergeben werden können, kumulativ innerhalb der Nerdio Manager-Konsole angewendet werden.

Wenn Konflikte innerhalb der zugewiesenen Rollen bestehen, wird die höhere Berechtigungszuweisung angewendet. Stellen Sie sicher, dass die Berechtigungen, die Sie Benutzern und Gruppen über benutzerdefinierte Rollen zuweisen, die Sicherheitsanforderungen Ihres Unternehmens erfüllen oder übertreffen.

> **Anmerkung**
>
> Mehrfache direkte Zuweisungen werden nicht unterstützt. Eine einzelne direkte Zuweisung kann mit mehreren **indirekten (Gruppen-)** Zuweisungen kombiniert werden. Diese neue Funktionalität gilt nur für benutzerdefinierte Rollen, die innerhalb der Nerdio Manager-Anwendung definiert sind. Integrierte Rollen sind von dieser neuen Funktionalität vollständig ausgeschlossen.

Grundlegende Prinzipien der Berechtigungszuweisung

Im Folgenden werden die Grundprinzipien erläutert, wie Berechtigungszuweisungen über Entra ID angewendet werden und wie Nerdio Manager diese interpretiert.

- Benutzer können der Anwendung direkt mit einer spezifischen Kombination aus Rolle und Workspace zugewiesen werden, oder sie können direktes Mitglied einer Gruppe sein, der die Anwendung zugewiesen ist. Zuweisungen sowohl als User als auch als Gruppenmitglied werden unterstützt.
- Mitglieder einer Gruppe, die ein verschachteltes Mitglied einer anderen Gruppe ist, welche der Entra ID-Anwendung zugewiesen ist, werden nicht berücksichtigt. Dies ist ein Limit von Entra ID. Weitere Details finden Sie in diesem Microsoft-Artikel.
- Die integrierten Standardrollen von Nerdio Manager sind in Stufen mit abnehmender Berechtigung angeordnet. Wenn ein User Mitglied von Gruppen mit mehreren gleichwertigen integrierten Rollenebenen ist, stellt Entra ID nur eine dieser Zuweisungen für Nerdio Manager bereit. Im Allgemeinen erfolgt die Bereitstellung in alphabetischer Reihenfolge, sodass die Zuweisungen der ersten alphabetischen Gruppe in den meisten Situationen gelten, technisch gesehen kann die Verarbeitung jedoch in beliebiger Reihenfolge erfolgen.

Zusätzliche Prinzipien

- Die benutzerdefinierten Rollen von Nerdio Manager bieten eine gefilterte Erfahrung auf Anwendungsebene. Daher bieten benutzerdefinierte Rollen die Möglichkeit, eine oder mehrere benutzerdefinierte Rollen per direkter Zuweisung oder Gruppenmitgliedschaft zuzuweisen, und diese Rollen werden innerhalb der Nerdio Manager-Anwendung kombiniert, um die umfangreichste Menge an Berechtigungen bereitzustellen.
- Eine direkte Userzuweisung gilt als höchste Priorität. Daher wird jeder User, der direkt Nerdio Manager zugewiesen ist, vor anderen Berechtigungen zugewiesen, die möglicherweise durch Gruppen zugewiesen wurden.

Beispielszenario

- Das Konto eines Users ist Mitglied der **ABC-ADM Group** und der **DEF-ADM Group**.

- **ABC-ADM Group** ist unter der Gruppe **XYZ-NerdioSupport-Admin** verschachtelt.
- **ABC-ADM Group** ist Workspace A mit einer benutzerdefinierten Rolle in Nerdio Manager zugewiesen.
- **DEF-ADM Group** ist Workspace B mit einer benutzerdefinierten Rolle in Nerdio Manager zugewiesen.
- **XYZ-NerdioSupport-Admin** ist den Workspaces C und D als AVD-Administrator in Nerdio Manager zugewiesen.

1. Die verschachtelte Mitgliedschaft spielt keine Rolle. Daher existiert aus Sicht von Entra ID die **ABC-ADM Group** als Mitglied von **XYZ-NerdioSupport-Admin** nicht. Nur User, die direkte Mitglieder der Gruppe **XYZ-NerdioSupport-Admin** sind, werden berücksichtigt. Da der User kein direktes Mitglied von **XYZ-NerdioSupport-Admin** ist, hat er keinen Zugriff auf die Workspaces C oder D.
2. Da der User ein direktes Mitglied sowohl der **ABC-ADM Gruppe** als auch der **DEF-ADM Gruppe** ist und beide Gruppen einer benutzerdefinierten Rolle zugewiesen sind, also derselben Berechtigungsebene gemäß Entra ID, entsprechen die effektiven Berechtigungen des Users der kumulativen Summe der Berechtigungen, die der **ABC-ADM Gruppe** und der **DEF-ADM Gruppe** zugewiesen sind.

Feature-Einschränkungen

In dieser ersten Version des kumulativen RBAC-Features gibt es einige funktionale Einschränkungen. Diese werden nach Möglichkeit in Zukunft behandelt.

- Integrierte Rollen werden für dieses Feature nicht unterstützt. Es dürfen nur benutzerdefinierte Rollen verwendet werden.
- Das Feature unterstützt nicht das Mischen verschiedener Zugriffsebenen für das Workspace-Modul über separate Zuweisungen hinweg. Sie können beispielsweise die Berechtigungen „Hosts verwalten“ und „Sitzungen verwalten“ im Workspace-Modul nicht über separate Zuweisungen mischen, da global nur eine Zugriffsebene für das Workspace-Modul unterstützt wird.
- Sie können eingeschränkte Berechtigungen nicht mit Vollzugriff mischen, selbst wenn Sie den Scope auf bestimmte Workspaces beschränken, da die Benutzeroberfläche für Vollzugriff mit den festgelegten Limits in Konflikt stehen würde.

- Sie können eingeschränkte Berechtigungen nicht mit Read Only mischen, selbst wenn Sie den Scope auf bestimmte Workspaces beschränken, da die Benutzeroberfläche für Read Only mit den festgelegten Limits in Konflikt stehen würde.
- Der Maximalwert der unterstützten Zuweisungen beträgt 10. Zusätzliche Zuweisungen werden gefiltert.

RBAC-Überlegungen vor Nerdio Manager v6.4

Dieser Abschnitt erörtert die Situation, in der ein User möglicherweise Mitglied verschiedener Gruppen für Umgebungen vor v6.4 ist. Einige davon können direkte Zuweisungen oder eine verschachtelte Gruppenzuweisung sein.

- Die Gruppen sind verschiedenen benutzerdefinierten Rollen zugewiesen. Zum Beispiel gewähren zwei Zuweisungen Zugriff auf Workspace A mit unterschiedlichen benutzerdefinierten Berechtigungen (das heißt, derselbe Workspace), und eine Zuweisung gewährt Zugriff auf die Workspaces B, C und D.
- Wenn sich der User anmeldet, sieht er nur den Workspace A. Er sieht **nicht** die Workspaces B, C und D.
- Tatsächlich möchten Sie, dass der User Zugriff auf alle Workspaces (A, B, C und D) hat.

Rechenkern-Berechtigungszuweisungsprinzipien

Im Folgenden werden die Rechenkernprinzipien erläutert, wie Berechtigungszuweisungen über Entra ID angewendet werden und wie Nerdio Manager diese interpretiert.

- Die User-Zuweisung zu Entra ID-Anwendungen unterstützt keine verschachtelte Gruppenmitgliedschaft. Das heißt, User können nur direkt mit einer spezifischen Rollen- und Workspace-Kombination der Anwendung zugewiesen werden, oder sie können direktes Mitglied einer Gruppe sein, die der Anwendung zugewiesen ist. Die Zuweisung sowohl als User als auch als Gruppenmitglied wird unterstützt, aber Nerdio Manager priorisiert zuerst die User-Zuweisung (siehe unten).
- Mitglieder einer Gruppe, die ein verschachteltes Mitglied einer anderen Gruppe ist, welche der Entra ID-Anwendung zugewiesen ist, werden nicht

berücksichtigt. Dies ist ein Limit von Entra ID. Weitere Details finden Sie in diesem Microsoft-Artikel.
- Die integrierten Standardrollen von Nerdio Manager sind in Stufen mit abnehmender Berechtigung angeordnet. Wenn ein User Mitglied von Gruppen mit mehreren gleichwertigen Rollenebenen ist, bietet Entra ID nur eine dieser Zuweisungen für Nerdio Manager an. Im Allgemeinen wird sie alphabetisch angeboten, sodass die Zuweisungen der ersten alphabetischen Gruppe in den meisten Situationen gelten, technisch gesehen kann die Verarbeitung jedoch in beliebiger Reihenfolge erfolgen.

Zusätzliche Prinzipien

- Alle in Nerdio Manager erstellten benutzerdefinierten Rollen werden hinsichtlich der Rollenberechtigungen von Entra ID als auf derselben Ebene befindlich betrachtet. Nerdio Manager kann Berechtigungen nicht zusammenführen oder konsolidieren, um den Zugriff auf die umfangreichste Kombination von Berechtigungen zu ermöglichen.
- Selbst wenn es eine benutzerdefinierte Rolle gäbe, die alle Berechtigungen aktiviert, und eine zweite Rolle, die nur eine einzige Berechtigung enthält, sind sie aus der Perspektive der Azure-Anwendung gleichwertig auf derselben Ebene, da beide als benutzerdefinierte Rolle betrachtet werden.
- Eine direkte User-Zuweisung gilt als höchste Priorität. Daher umgeht jeder User, der direkt Nerdio Manager zugewiesen ist, alle alternativen Berechtigungen, die möglicherweise per Gruppe zugewiesen sind. User sollten jedoch nur eine einzige Zuweisung haben, da sie sonst denselben Verarbeitungsproblemen wie bei mehreren Gruppenmitgliedschaften unterliegen.

Beispielszenario

- Das Konto eines Users ist Mitglied der **ABC-ADM Group** und der **DEF-ADM Group**.
- **ABC-ADM Gruppe** ist unter der Gruppe **XYZ-NerdioSupport-Admin** verschachtelt.
- **ABC-ADM Gruppe** ist dem Workspace A mit einer benutzerdefinierten Rolle in Nerdio Manager zugewiesen.
- **DEF-ADM Gruppe** ist dem Workspace B mit einer benutzerdefinierten Rolle in Nerdio Manager zugewiesen.
- **XYZ-Nerdio-Support-Admin** ist den Workspaces C und D als AVD-Administrator in Nerdio Manager zugewiesen.

1. Die verschachtelte Mitgliedschaft spielt keine Rolle. Daher existiert aus Sicht von Entra ID die **ABC-ADM Gruppe** als Mitglied von **XYZ-Nerdio-Support-Admin** nicht. Es werden nur User berücksichtigt, die direkte Mitglieder der Gruppe **XYZ-Nerdio-Support-Admin** sind. Da der User kein direktes Mitglied von **XYZ-Nerdio-Support-Admin** ist, hat er keinen Zugriff auf die Workspaces C oder D.
2. Da der User ein direktes Mitglied sowohl der **ABC-ADM Gruppe** als auch der **DEF-ADM Gruppe** ist und beide Gruppen einer benutzerdefinierten Rolle zugewiesen sind (daher dieselbe Berechtigungsebene gemäß Entra ID), sind die effektiven Berechtigungen des Users eine Glückssache zwischen den Workspaces/Pools, denen diese Gruppen zugewiesen sind. In diesem Beispiel ist das entweder Workspace A oder Workspace B.
3. Normalerweise erfolgt die Zuweisung alphabetisch, aber es gibt keine offizielle Definition dafür, wie dies von Entra ID interpretiert wird. Daher könnte der User heute den Workspace A sehen, der durch **ABC-ADM Gruppe** aktiviert wird. Morgen sieht der User möglicherweise Workspace B, der durch **DEF-ADM Gruppe** aktiviert wird. Entra ID nimmt die Auswertung vor und gewährt dem User Zugriff auf Nerdio Manager unter dieser Gruppe. Nerdio Manager sieht lediglich, dass sich ein Mitglied einer bestimmten Gruppe angemeldet hat, und erteilt die Berechtigungen entsprechend.

> **Anmerkung**
>
> Dies könnte auch auf zwei verschiedene RBAC-Rollenzuweisungen in Nerdio Manager zutreffen, bei denen zwei verschiedene Gruppen demselben Workspace (zum Beispiel Workspace A) zugewiesen sind, aber zwei unterschiedliche Definitionen für benutzerdefinierte Rollen aufweisen. Eine Zuweisung gewährt möglicherweise Berechtigungen für eine Reihe von Hostpools, während die andere Gruppe möglicherweise einer anderen Reihe von Hostpools zugewiesen ist.
>
> Da alle benutzerdefinierten Rollen auf einer gleichwertigen Ebene liegen, können sich die spezifischen Hostpools, die für den User sichtbar sind, je nachdem ändern, welche Gruppenauswertung Entra ID bei der Anmeldung bei Nerdio Manager vornimmt.

Empfehlungen

> **Tipp**
>
> Befolgen Sie diese Empfehlungen, um eine klare und konsistente Darstellung zu gewährleisten.

- **Option #1**: Ändern Sie entweder die Gruppenmitgliedschaft oder die Zuweisungen, die verwendet werden, um dem User Zugriff auf Nerdio Manager zu gewähren, sodass nur eine Gruppenmitgliedschaft mit einer einzigen benutzerdefinierten Rolle angewendet wird, die Zugriff auf alle erforderlichen Workspaces gewährt, zu denen der User berechtigt sein sollte.

  > **Anmerkung**
  >
  > Wenn nicht mehrere Gruppen für Entra ID ausgewertet werden müssen, wird sichergestellt, dass nur die eine korrekte Zuweisung angewendet wird.

- **Option #2**: Weisen Sie das Konto des User explizit und nicht als Gruppenmitgliedschaft direkt der benutzerdefinierten Rolle zu und gewähren Sie Zugriff auf alle Workspaces, zu denen eine Berechtigung bestehen sollte.

  > **Anmerkung**
  >
  > Eine einzelne direkte Zuweisung stellt sicher, dass genau die erforderlichen Berechtigungen angewendet werden.

Tipp

Obwohl beide Lösungen funktionieren würden, empfehlen wir die Verwendung von Option Nr. 1. Dies hilft zu verhindern, dass die Berechtigungsliste mit einer großen Anzahl einzelner User überladen wird.