Synology

Synology Administrator-Handbuch für

Synology Directory Server

Basierend auf

DSM 7.1 und Synology Directory Server 4.10

Inhaltsverzeichnis

Kapitel 1: Einleitung **01**

Über Synology Directory Server

Synology Directory Grundlagen

Kompatibilität und Einschränkungen

Installieren Sie Synology Directory Server

Knowledge Center

Kapitel 2: Domain-Controller einrichten **05**

Bereitstellungsmethoden

Primären Domain-Controller einrichten

Sekundären Domain-Controller einrichten

Kapitel 3: Die Domain verwalten **09**

Domaininformationen anzeigen

Domain-Rechte anzeigen

FSMO-Rollen abrufen

Richtlinien für Kennwortreplikation hinzufügen

Vorschau von Richtlinien für Kennwortreplikation anzeigen

Kennwörter vorausfüllen

Einen DC zurückstufen

Die IP-Adresse eines DCs ändern

DNS-Ressourceneinträge verwalten

Systemprotokolle anzeigen und verwalten

Firewall-Regeln zur Sicherung des Verzeichnisdienstes hinzufügen

Kapitel 4: Domainobjekte verwalten **20**

Domainobjekte anzeigen

OUs verwalten

Gruppen verwalten

Benutzer verwalten

Computer verwalten

Kapitel 5: Geräte in eine Domain einbinden **37**

Mit Windows-PCs einer Domain beitreten

Mit dem Synology NAS einer Domain beitreten

Kapitel 6: Gruppenrichtlinien konfigurieren **41**

Standard-Domainrichtlinien konfigurieren

RSAT zur Verwaltung von Gruppenrichtlinien verwenden

Kapitel 7: Verzeichnisdienst warten und wiederherstellen 49

Unterbrechungsfreien Verzeichnisdienst mit Synology High Availability sicherstellen

Verzeichnisdienst mit Hyper Backup sichern und wiederherstellen

Kapitel 1: Einleitung

Über Synology Directory Server

Synology Directory Server bietet eine zentrale Plattform für Konten- und Ressourcenverwaltungsdienste mittels Samba-Schema. Das Paket unterstützt gängige Funktionen von Windows Active Directory (AD)®, wie Verwaltung von Benutzern/Gruppen, Organisationseinheiten (OU), Gruppenrichtlinien, Kerberos-basierte Authentifizierung und den Einsatz verschiedener Client-Geräte. Mit dem von Synology Directory Server eingerichteten Domaindienst können Sie auf sichere Weise eine Verzeichnisdatenbank speichern, Nutzerkonten verwalten und Geräte basierend auf Ihrer Organisationsstruktur einsetzen.

Synology Directory Grundlagen

Hier finden Sie einen Überblick über den Synology-Verzeichnisdienst als Grundlage für die Ausführung administrativer Aufgaben mittels Synology Directory Server.

Verzeichnisdienst

Ein Verzeichnis ist ein Repository, das einzelne Benutzer, Gruppen, Orte und verschiedene Arten von Informationen enthält. Es ist ein Werkzeug zum Speichern und Verwalten von Daten und ermöglicht Benutzern oder Geräten, gewünschte Informationen schnell zu finden. In der Informatik dienen Verzeichnisdienste dazu, sämtliche Kontoinformationen an einem zentralen Ort zu speichern. So können verschiedene Ressourcen zusammenspielen und das ist ideal, um Benutzerzugriffe zu autorisieren, Identitäten zu konfigurieren und die Beziehungen zwischen Benutzern und Gruppen zu verwalten.

Active Directory® und Synology Directory-Dienst

Active Directory® (AD) ist ein Typ von Verzeichnisdienst, der eine zentrale Informationsdatenbank bietet. Damit können IT-Administratoren Objekte und Ressourcen wie Konten, Computer und Drucker auf sichere Weise verwalten. Synology Directory Server bietet den auf AD basierten **Synology-Verzeichnisdienst**, mit dem Ressourcen in einer intuitiven Oberfläche gespeichert und bereitgestellt werden können.

Domain Name System (DNS)

Synology Directory nutzt das Domain Name System (DNS), um Rechner, Drucker und andere Ressourcen in einer hierarchischen Struktur zu organisieren.

Eine Domain ist eine zur Erstellung und Verwaltung von Ressourcen eingerichtete logische Grenze. DNS ist ein Standard-Internetdienst, der Ressourcen mittels Domainnamen strukturiert. In einer Domain (z. B. „syno.local“) werde Geräte über DNS bereitgestellt, das Hostnamen (z. B. „pc1.syno.local“) in IP-Adressen übersetzt, mit denen Geräte mit Internetprotokollen gefunden und identifiziert werden können.

Dementsprechend müssen Sie **einen DNS-Server einrichten**, um bei der Installation von Synology Directory Server die Funktionalität der Domain zu gewährleisten.

Domain-Controller

Ein Domain-Controller (DC) ist ein Synology NAS, auf dem die Domain eines Synology Directory Servers gehostet wird. Er ist dafür verantwortlich, die Domainfunktionen aufrechtzuerhalten, Verzeichnisdaten zu speichern und Benutzerinteraktionen innerhalb einer Domain zu verwalten.

In Synology Directory Server wird das Synology NAS, auf dem eine Domain erstellt wird, automatisch zum primären Domain-Controller (PDC) befördert.

Domainobjekt hinzufügen

Die in Synology Directory Server gespeicherte Domaindatenbank besteht aus Informationen über Objekte, die jeweils einen einzelnen und einzigartigen Eintrag in die Datenbank darstellen. Folgende Objekte können in Synology Directory Server verwaltet werden:

- **Benutzer**: Ein Benutzerkonto, das auf in einer Domain bereitgestellte Ressourcen zugreifen kann.
- **Gruppe**: Eine verwaltbare Einheit, in der Domainobjekte zusammengefasst sind. Die Zugriffsberechtigungen einer Gruppe auf Ressourcen in einer Domain (z. B. Dateien und Geräte) gelten für alle ihre Mitglieder.
- **Gerät**: Eine physische Ressource, auf die Domainbenutzer zugreifen können. Das kann ein Computer sein, ein Drucker, ein Synology NAS usw.
- **Organisationseinheit (OU)**: Der kleinste Container in einer Domain, dem Administratorberechtigungen und Gruppenrichtlinien zugewiesen werden können. Organisieren Sie Benutzer, Gruppen oder Computer in OUs, um ihnen dieselben Berechtigungen und Richtlinien zuzuweisen. Sie können OUs auch zu anderen OUs hinzufügen und so eine OU-Hierarchie erstellen, die der tatsächlichen Struktur Ihrer Organisation entspricht. Dies ermöglicht die effizientere Konfiguration von Domainobjekten in Synology Directory Server.

Kompatibilität und Einschränkungen

- DSM-Versionsanforderung: DSM 7.1 und höher.
- Domainfunktionsebene: Wie Windows Server 2008 R2.
- Synology Directory Server muss mit dem Paket **DNS Server** betrieben werden.

- Synology Directory Server ist nicht kompatibel mit Konfigurationen anderer Domain-/LDAP-Dienste.
- Unterstützte Domain-Clients:
  - Windows 7 und höher
  - macOS
  - Linux
- Synology Directory Server kann nur auf **unterstützten Synology NAS-Modellen** installiert werden.
- Einschränkungen:
  - Unterstützt nur eine einzelne Domain.
  - Der Hostname des als DC dienenden Synology NAS **kann nicht mehr geändert werden, nachdem Synology Directory Server darauf aktiviert wurde**.
  - Nach dem Erstellen einer Domain wird SMB-Signatur automatisch aktiviert. Das kann **die Lese-/Schreibleistung bei der SMB-Dateiübertragung beeinträchtigen**.
    - SMB-Signatur ermöglicht die digitale Signatur von SMB-Kommunikation auf Paketebene. Wenn Sie sie deaktivieren möchten, um die Leistung zu verbessern, öffnen Sie **Systemsteuerung** > **Dateidienste** > **SMB** > **Erweiterte Einstellungen** > **Server-Signierung aktivieren**, wählen Sie **Deaktivieren** und klicken Sie auf **Speichern**.
  - DFSR (Distributed File System Replication) wird nicht unterstützt.
  - Das Active Directory-Modul für Windows PowerShell wird nicht unterstützt.
  - Sekundäre Domain-Controller (SDCs) funktioniert nur mit von Synology Directory Server erstellten Domains.

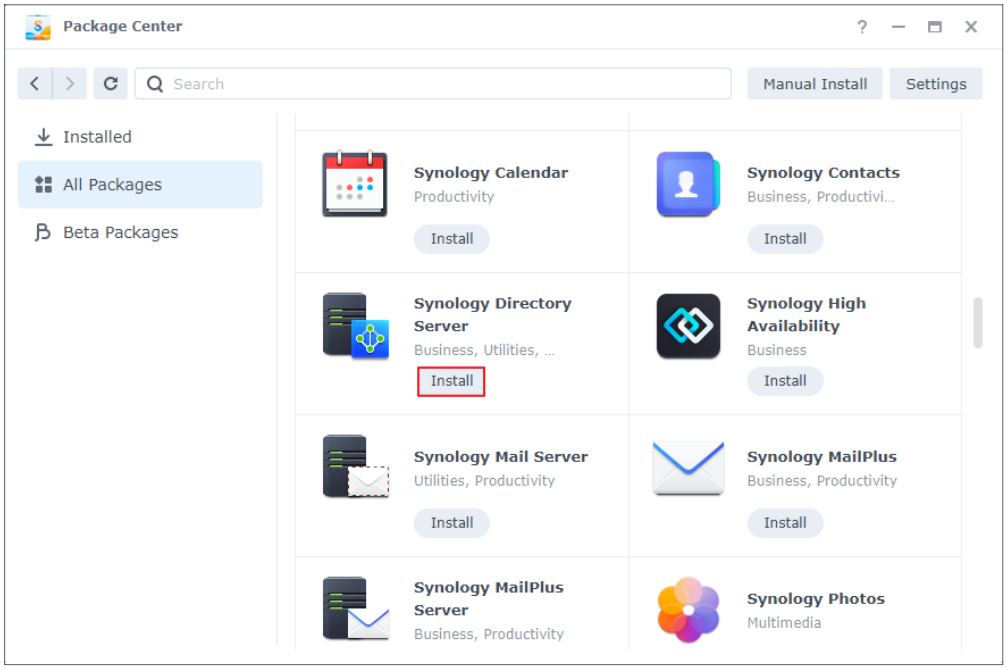
Weitere Informationen finden Sie in den **technischen Spezifikationen** von Synology Directory Server.

Installieren Sie Synology Directory Server

1. Bevor Sie **Synology Directory Server** auf dem Synology NAS installieren, kontrollieren Sie Folgendes:
   - Die Netzwerkverbindung des Synology NAS funktioniert einwandfrei.
   - Der Volume-Status Ihres Synology NAS unter **Speicher-Manager** > **Speicher** lautet **In Ordnung**.
   - Die DSM-Version ist DSM 7.1 oder höher.
   - Sie sind der **DSM**-Administrator (d. h. ein Benutzer aus der Gruppe **administrators**) auf dem Synology NAS.

- Das Synology NAS verwendet eine statische IP-Adresse: Richten Sie in Ihrem lokalen Netzwerk eine statische IP-Adresse für das als DC agierende Synology NAS ein. So verhindern Sie, dass Clients aufgrund einer Änderung der IP-Adresse des Synology NAS getrennt werden.
- Das Synology NAS ist kein Client einer Domain oder eines LDAP-Verzeichnisses: Wenn das Synology NAS bereits einer Domain oder einem LDAP-Verzeichnis beigetreten ist, muss es die Domain bzw. das LDAP-Verzeichnis verlassen.
- Es existieren keine Konflikte mit Domainnamen im lokalen Netzwerk: Synology Directory Server wird von Clients nicht gefunden, wenn es im lokalen Netzwerk mehr als eine Domain mit demselben Namen gibt. Um dies zu vermeiden, wählen Sie einen anderen Namen oder entfernen Sie Domains mit demselben Namen.

2. Melden Sie sich als Administrator (d. h. als Benutzer der Gruppe **administrators**) bei DSM an.
3. Gehen Sie zu **Paketzentrum** > **Alle Pakete**.
4. Suchen Sie **Synology Directory Server** und klicken Sie auf **Installieren**. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation abzuschließen.



Anmerkung:

- Vor der Installation von Synology Directory Server können Sie **einen Synology High Availability-Cluster einrichten für unterbrechungsfreien Verzeichnisdienst**.

Knowledge Center

In unserem **Knowledge Center** finden Sie weitere Hilfe-Artikel, Anleitungen, FAQs, technische Spezifikationen, Versionshinweise und Videoanleitungen zu Synology Directory Server.

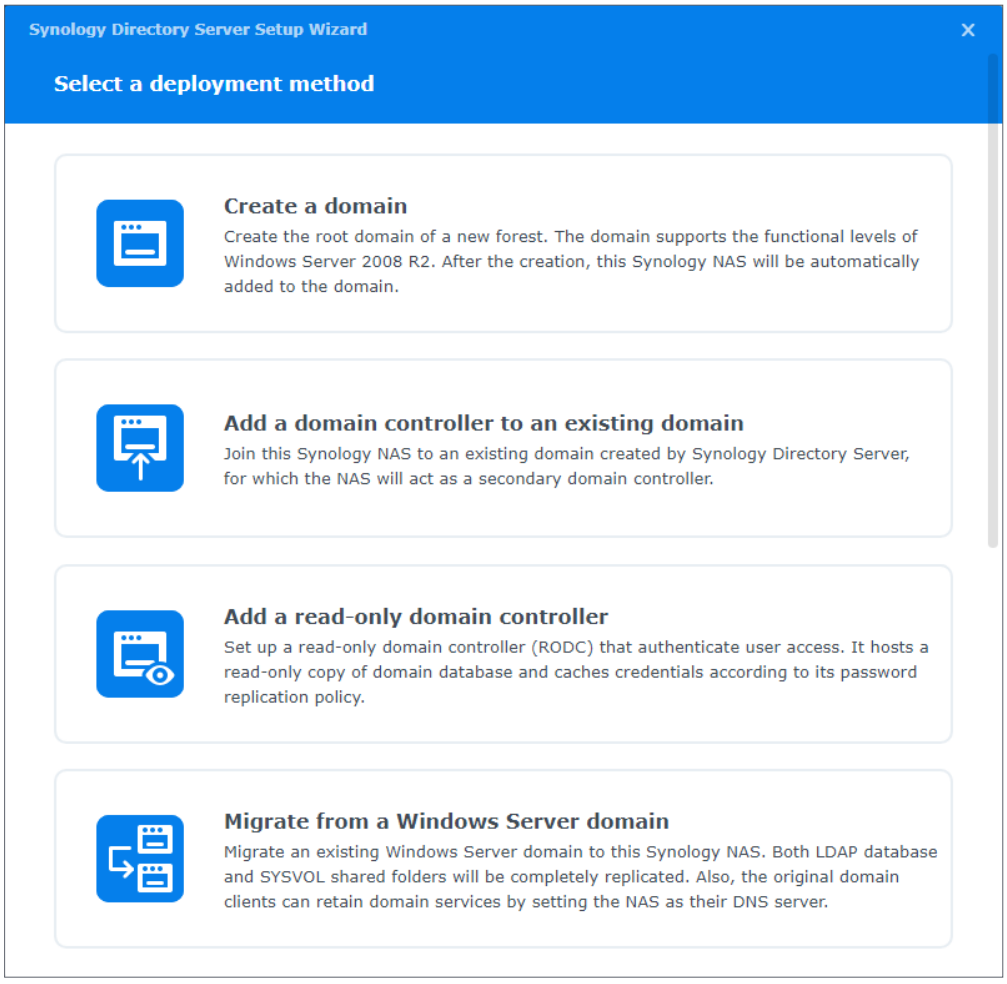
Kapitel 2: Domain-Controller einrichten

Sie können Ihr Synology NAS als primären Domain-Controller (PDC) oder sekundären Domain-Controller (SDC) einrichten, der Konten verwaltet, Dienste bereitstellt, Zugriffsberechtigungen konfiguriert und Autorität in einer Domain delegiert.

- In einer Domain kann es nur einen PDC, aber mehrere SDC geben.
- Der PDC ist ein Lese/Schreib-Domain-Controller (RWDC).
- SDCs können je nach System entweder Lese/Schreib-Domain-Controller (RWDC) oder schreibgeschützte Domain-Controller (RODC) sein.

Bereitstellungsmethoden

Im Bild unten sehen Sie die vier von Synology Directory Server unterstützten Bereitstellungsmethoden. In der nachfolgenden Tabelle finden Sie weitere Informationen dazu.



DC		Bereitstellungsmethode	Beschreibung
PDC	RWDC	Eine Domain erstellen	Erstellen Sie die Stammdomain einer neuer Gesamtstruktur. • Die Domain unterstützt die Funktionsebenen von Windows Server 2008 R2. • Nach dem Erstellen der Domain agiert Ihr Synology NAS als Domain-Client und wird automatisch zur Domain hinzugefügt.
		Von einer Windows Server-Domain migrieren	Migrieren Sie eine bestehende Windows Server-Domain zu Ihrem Synology NAS. • Sowohl LDAP-Datenbank als auch freigegebene SYSVOL-Ordner werden vollständig zu Ihrem Synology NAS repliziert. • Die ursprünglichen Domain-Clients können Domain-Dienste beibehalten, indem das Synology NAS als ihr DNS-Server eingerichtet wird.
SDC	RWDC	Domain-Controller zu vorhandener Domain hinzufügen	Fügen Sie Ihr Synology NAS einer von Synology Directory Server erstellten vorhandenen Domain hinzu.
	RODC	Schreibgeschützten Domain-Controller hinzufügen	Fügen Sie Ihr Synology NAS einer von Synology Directory Server oder Windows AD erstellten vorhandenen Domain hinzu. Richten Sie Ihr Synology NAS als RODC ein, der: • Eine schreibgeschützte Kopie der Domaindatenbank hostet. • Kennwörter von Benutzerkonten vorausfüllt. • Benutzerzugriff authentifiziert.

Primären Domain-Controller einrichten

Wenn Synology Directory Server installiert und keine vorhandene Domain erkannt wurde, können Sie eine Domain erstellen und Ihr Synology NAS zum PDC befördern.

1. Starten Sie **Synology Directory Server**.
2. Wählen Sie die Bereitstellungsmethode:
   - **Eine Domain erstellen**
   - **Von einer Windows Server-Domain migrieren**
3. Geben Sie je nach Domaintyp die folgenden Daten ein.
   - Erstellen einer Domain:
     - **Domainname**: Geben Sie einen FQDN (Fully Qualified Domain Name) für die Domain ein (z. B. „syno.local“).
     - **Arbeitsgruppe**: Der Name der Arbeitsgruppe (oder der NetBIOS-Domainname) wird automatisch eingetragen. Wenn der Domainname „syno.local“ lautet, heißt die Standard-Arbeitsgruppe beispielsweise „syno“.
     - **Kennwort**: Geben Sie ein Kennwort für das Administratorkonto der Domain ein.
     - **Kennwort bestätigen**: Geben Sie das Kennwort erneut ein.

- Migration von einer Windows Server-Domain:
  - **Domainname**: Geben Sie den FQDN der Windows-Domain ein, die Sie zu Synology Directory Server migrieren möchten.
  - **DNS-Server**: Geben Sie die IP-Adresse eines DNS-Servers ein, der den vorhandenen Windows DC auflösen kann.
  - **Konto**: Geben Sie das Administratorkonto der Domain im folgenden Format ein.

    ```
    NetBIOS-Domainname\Administrator-Benutzername
    ```

  - **Kennwort**: Geben Sie das Kennwort des Administrator-Kontos ein.

4. Klicken Sie auf **Weiter**. Der Assistent testet nun, ob die Vorbedingungen erfüllt wurden.
   - ✅: Der Test wurde bestanden.
   - ⚠️: Es ist mindestens ein kleineres Problem aufgetreten, das gelöst werden muss. Solche Probleme können zu Unregelmäßigkeiten bei Domaindiensten führen. Klicken Sie auf **Details** und beheben Sie die Probleme entsprechend den vorgeschlagenen Maßnahmen.
   - ❗: Es ist mindestens ein kritisches Problem aufgetreten, das umgehend gelöst werden muss. Solche Probleme führen dazu, dass die Domainmigration fehlschlägt. Klicken Sie auf **Details** und beheben Sie die Probleme entsprechend den vorgeschlagenen Maßnahmen.
5. Nachdem die Überprüfung der Vorbedingungen ohne kritische Probleme abgeschlossen wurde, klicken Sie je nach Bereitstellungsmethode auf **Domain erstellen** oder **Domain migrieren**. Die Dauer der Migration hängt von der Datenmenge ab.

Bedingungen für Domainnamen:

- Domainnamen dürfen nur Buchstaben, Zahlen, Minuszeichen und Punkte (als Trennzeichen für die Teile der Domain) enthalten.
- Domainnamen müssen aus mindestens zwei Teilen bestehen (z. B. „syno.local“).
- Domainnamen dürfen nicht mit einem Bindestrich (-) beginnen.
- Domainnamen dürfen nicht mit einem Bindestrich (-) oder Punkt (.) enden.
- Domainnamen dürfen nicht gleich lauten wie der Servername Ihres Synology NAS.
- Die Maximallänge beträgt 64 Zeichen.

Anforderungen an die Kennwortstärke:

Kennwörter müssen **mindestens drei** der folgenden Regeln erfüllen:

- Großbuchstaben (einschließlich A-Z mit diakritischen Zeichen) des lateinischen, griechischen und kyrillischen Alphabets.
- Kleinbuchstaben (einschließlich a-z mit diakritischen Zeichen) des lateinischen, griechischen und kyrillischen Alphabets.
- Ziffern (0-9).
- Sonderzeichen wie #, $, !
- Unicode-Alphabete, darunter jene in asiatischen Sprachen.

Sekundären Domain-Controller einrichten

Sie können Ihr Synology NAS als SDC (RWDC oder RODC) einrichten und zu **einer von Synology Directory Server erstellten vorhandenen Domain** hinzufügen.

1. Starten Sie **Synology Directory Server**.
2. Wählen Sie die Bereitstellungsmethode:
   - **Domain-Controller zu vorhandener Domain hinzufügen**: Ihr Synology NAS wird als RWDC eingerichtet.
   - **Schreibgeschützten Domain-Controller hinzufügen**: Ihr Synology NAS wird als RODC eingerichtet.
3. Geben Sie die folgenden Informationen ein:
   - **Domainname**: Geben Sie den FQDN einer bestehenden Synology-Domain ein.
   - **DNS-Server**: Geben Sie die IP-Adresse eines DNS-Servers ein, der den vorhandenen Synology DC auflösen kann.
   - **Konto**: Geben Sie das Administratorkonto der Domain im folgenden Format ein.
     ```
     NetBIOS-Domainname\Administrator-Benutzername
     ```
   - **Kennwort**: Geben Sie das Kennwort des Administrator-Kontos ein.
4. Klicken Sie auf **Weiter**. Der Assistent testet nun, ob die Vorbedingungen erfüllt wurden.
   - ✅: Der Test wurde bestanden.
   - ⚠️: Es ist mindestens ein kleineres Problem aufgetreten, das gelöst werden muss. Solche Probleme können zu Unregelmäßigkeiten bei Domaindiensten führen. Klicken Sie auf **Details** und beheben Sie die Probleme entsprechend den vorgeschlagenen Maßnahmen.
   - ❗: Es ist mindestens ein kritisches Problem aufgetreten, das umgehend gelöst werden muss. Solche Probleme führen dazu, dass die Domainmigration fehlschlägt. Klicken Sie auf **Details** und beheben Sie die Probleme entsprechend den vorgeschlagenen Maßnahmen.
5. Nachdem die Überprüfung der Vorbedingungen ohne kritische Probleme abgeschlossen wurde, klicken Sie auf **Domain beitreten**.

Kapitel 3: Die Domain verwalten

Domaininformationen anzeigen

Auf der Seite **Domain** können Sie Domain und DC anzeigen, bearbeiten oder entfernen.

Domain-Informationen	
Domainname	Der volle Name der Domain.
Domain NetBIOS-Name	Wird verwendet, um das lokale Netzwerk zu identifizieren. Wenn Ihr Domainname beispielsweise „syno.local“ lautet, ist der NetBIOS-Name „syno“.
Domain-Controller	
Typ	**Primärer Domain-Controller** • Der Server, der die Rolle als PDC-Emulator und andere FSMO-Rollen (Flexible Single Master Operation) übernimmt. • Der PDC liefert bei Synchronisierungsproblemen Datenaktualisierungen.
	Sekundärer Domain-Controller • Der Server, der FSMO-Rollen, aber keine Rolle als PDC-Emulator übernehmen kann.
	Schreibgeschützter Domain-Controller • Der Server, der eine schreibgeschützte Kopie der Domaindatenbank hostet, Kennwörter von Benutzerkonten entsprechend der Richtlinie für Kennwortreplikation repliziert, und den Benutzerzugriff authentifiziert. • Der RODC erhält von RWDCs nur Replikationsdaten.
Eindeutiger Name (DN)	Der DN ist der Objektpfad des DCs in der Domain-Datenbank. Beispiel: Wenn der DN eines DCs „CN=SYNOTEST,OU=Domain Controllers,DC=syno,DC=local“ lautet, können Sie seine Elemente wie folgt analysieren: • **CN**=SYNOTEST: Der Hostname dieses DCs lautet „SYNOTEST“. • **OU**=Domain Controllers: Der DC gehört der Organisationseinheit „Domain Controllers“ an. • **DC**=syno,**DC**=local: Der DC wird in der Domain „syno.local“ eingesetzt.
Rollen	**PDC-Emulator** • Der Inhaber der Rolle des PDC-Emulators stellt Zeitsynchronisierungsdienste für die Kerberos-Authentifizierung bereit und zeichnet Kennwort-Aktualisierungen von anderen DCs innerhalb einer Domain auf. • Pro Domain gibt es nur einen Inhaber dieser Rolle und dieser muss ein RWDC sein.

Rollen	**RID-Master** • Der Inhaber der Rolle des RID-Masters (Relative ID) beantwortet RID-Pool-Anfragen von allen DCs in einer Domain, damit DCs Domain-Objekte hinzufügen können. • Pro Domain gibt es nur einen Inhaber dieser Rolle und dieser muss ein RWDC sein.
	Infrastrukturmaster • Der Inhaber dieser Rolle ist für die Aktualisierung domainübergreifender Objektreferenzen verantwortlich. • Pro Domain gibt es nur einen Inhaber dieser Rolle und dieser muss ein RWDC sein.
	Domänennamenmaster • Der Inhaber dieser Rolle kümmert sich um Änderungen im Domainnamensbereich. • Pro Gesamtstruktur gibt es nur einen Inhaber dieser Rolle und dieser muss ein RWDC sein.
	Schemamaster • Der Inhaber dieser Rolle ist für die Aktualisierung des Verzeichnisschemas verantwortlich. • Pro Gesamtstruktur gibt es nur einen Inhaber dieser Rolle und dieser muss ein RWDC sein.

Domain-Rechte anzeigen

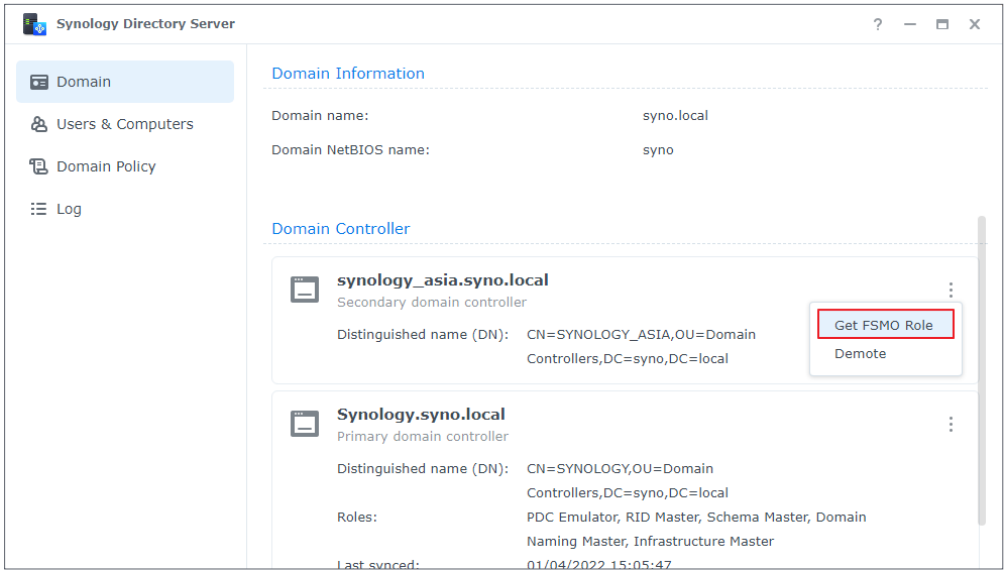
Die folgende Tabelle zeigt die Aktionen, die ein DC ausführen kann.

DC-Typ / Aktion	PDC	SDC	
		RWDC	RODC
FSMO-Rollen abrufen	Ja	Ja	Nein
Richtlinien für Kennwortreplikation hinzufügen	Ja	Ja	Nur anzeigen
Vorschau von Richtlinien für Kennwortreplikation anzeigen	Ja	Ja	Ja
Kennwörter vorausfüllen	Ja	Ja	Nur anzeigen
IP-Adressen ändern	Ja	Ja	Nur anzeigen
DCs zurückstufen	Ja (kann alle DCs zurückstufen)	Ja (kann PDC nicht zurückstufen)	Kann sich nur selbst zurückstufen

FSMO-Rollen abrufen

Der PDC ist standardmäßig Inhaber folgender FSMO-Rollen: PDC-Emulator, RID-Master, Infrastrukturmaster, Domänennamenmaster und Schemamaster. Der als RWDC agierende SDC kann jedoch FSMO-Rollen vom PDC erhalten. Der PDC kann die Rollen auch vom SDC zurückerhalten.

1. Öffnen Sie auf einem RWDC **Domain** > **Domain-Controller**.
2. Klicken Sie auf dem RWDC, der eine FSMO-Rolle erhalten soll, auf ⋮ und wählen Sie **FSMO-Rolle abrufen**.



3. Wählen Sie eine der folgenden Modi im Dropdown-Menü **Modus zum Abrufen von Rollen** aus.
   - **Rolle übertragen**: Eine Rolle vom anderen RWDC zum aktuellen übertragen.
   - **Rolle übernehmen**: Die Übernahme der Rolle des anderen RWDCs erzwingen. Die erzwungene Übernahme einer Rolle kann zu Problemen bei der Synchronisierung zwischen RWDCs führen. Wir empfehlen, diesen Modus nur zu verwenden, wenn der ursprüngliche Inhaber der FSMO-Rolle unerwartet und dauerhaft offline ist.
4. Wählen Sie im Dropdown-Menü **Rolle** die Rolle aus, die übernommen werden soll.
5. Geben Sie das Administratorkonto und Kennwort Ihrer Domain ein.
6. Klicken Sie auf **Senden**, um die Rolle vom anderen RWDC zu erhalten.

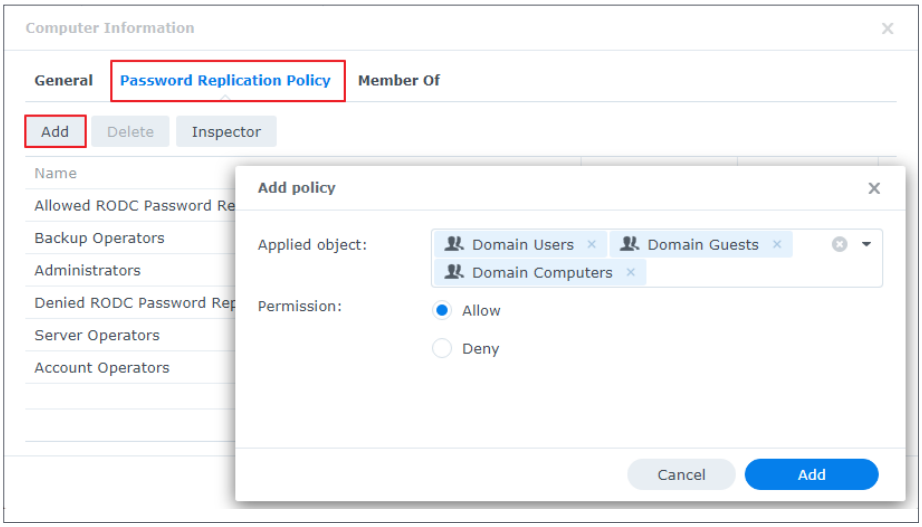
Richtlinien für Kennwortreplikation hinzufügen

Mit der Richtlinie für Kennwortreplikation können Sie festlegen, welche Benutzerkontokennwörter zu einem RODC repliziert werden können. Nachdem eine Richtlinie für Kennwortreplikation hinzugefügt wurde und sich ein Benutzerkonto in der Zulassungsliste der Richtlinie für Kennwortreplikation befindet, wird das Kennwort des Benutzerkontos zum RODC repliziert.

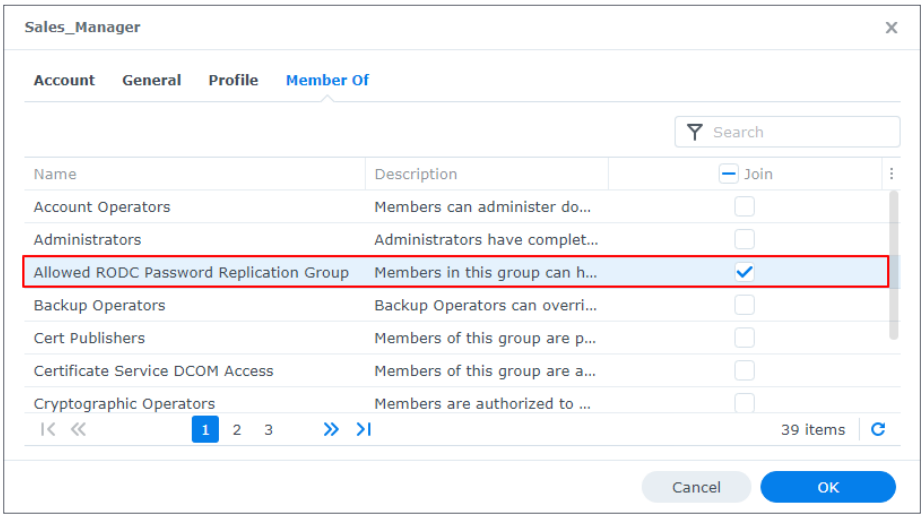
Ein zur Replizierung eines Benutzerkontokennworts berechtigter RODC authentifiziert die Anmeldungen des Benutzers, ohne Authentifizierungsanfragen an einen RWDC (d. h. einen PDC oder SDC) weiterzuleiten. Ein nicht zur Replizierung eines Benutzerkontos berechtigter RODC leitet die Authentifizierungsanfrage jedoch an einen RWDC weiter.

Nur RWDCs können Richtlinien für Kennwortreplikation hinzufügen; RODCs können die hinzugefügten Richtlinien lediglich anzeigen.

1. Öffnen Sie auf dem RWDC die Seite **Benutzer und Computer**.
2. Klicken Sie links von der OU auf ▼, um die Domainobjekte auszuklappen, und wählen Sie eine der folgenden Vorgehensweisen:
   - **Methode 1:**
     a. Klicken Sie auf **Domain Controllers**, doppelklicken Sie auf einen RODC und wählen Sie **Richtlinie für Kennwortreplikation**.
     b. Klicken Sie auf **Hinzufügen** und wählen Sie Objekte im Dropdown-Menü **Angewendetes Objekt** aus.
     c. Wählen Sie eine Option aus und klicken Sie auf **Hinzufügen**:
        - **Erlauben** Sie dem RODC, die gewählten Benutzerkontokennwörter zu replizieren.
        - **Verweigern** Sie dem RODC, die gewählten Benutzerkontokennwörter zu replizieren.
     d. Klicken Sie auf **Hinzufügen**.



   - **Methode 2:**
     a. Klicken Sie auf **Benutzer**, rechtsklicken Sie auf ein Objekt und wählen Sie **Eigenschaften**.
     b. Klicken Sie auf **Mitglieder von** und fügen Sie das Objekt zu **Zulässige RODC-Kennwortreplikationsgruppe** oder einer Gruppe, für die die Kennwortreplikationsrichtlinie übernommen wurde, hinzu.
     c. Klicken Sie auf **OK**.



3. Mit der Funktion **Inspektor** können Sie sicherstellen, dass die Objekte auf der gewünschten Zulassungs- bzw. Verweigerungsliste stehen.

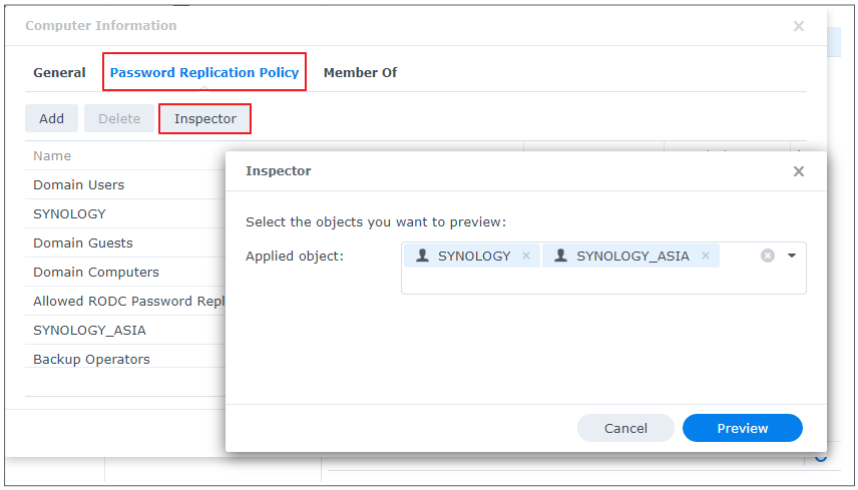
Anmerkung:

- Wenn ein Benutzerkonto sich auf der Zulassungsliste und der Verweigerungsliste befindet, wird das Kennwort des Benutzerkontos nicht repliziert (d. h. die Verweigerungsliste hat Vorrang).

Vorschau von Richtlinien für Kennwortreplikation anzeigen

Mit der Funktion **Inspektor** können Sie eine Vorschau der Benutzerkonten in der Zulassungs- bzw. Verweigerungsliste der Richtlinien für Kennwortreplikation anzeigen.

1. Öffnen Sie auf dem DC die Seite **Benutzer und Computer**.
2. Klicken Sie links von der OU auf ▼, um die Domainobjekte auszuklappen, und wählen Sie **Domain Controllers**.
3. Doppelklicken Sie auf einen RODC und wählen Sie **Richtlinie für Kennwortreplikation**.
4. Klicken Sie auf **Inspektor** und wählen Sie in der Vorschau anzuzeigenden Benutzerkonten aus dem Dropdown-Menü **Angewendetes Objekt** aus.
5. Klicken Sie auf **Vorschau**.

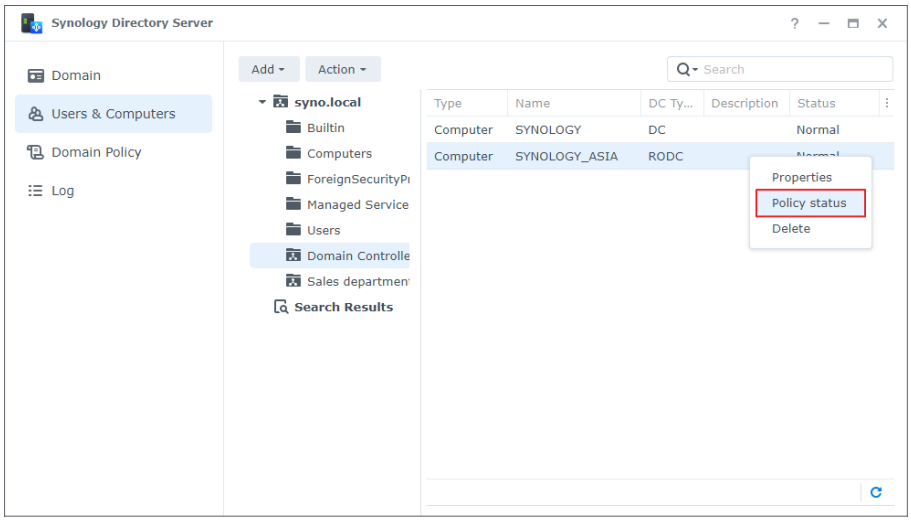


6. Sie können Benutzerkonten je nach Anforderung hinzufügen, entfernen oder exportieren. Für Mehrfachauswahl halten Sie **Strg** und **Umschalttaste** gedrückt.
   - Klicken Sie auf **Hinzufügen**, wählen Sie Benutzerkonten aus dem Dropdown-Menü **Angewendetes Objekt** aus, und klicken Sie auf **Vorschau**.
   - Wählen Sie ein Benutzerkonto aus und klicken Sie auf **Löschen**, um es aus der Vorschau zu entfernen.
   - Klicken Sie auf **Exportieren**, um Benutzerkonten als Excel-Datei zu exportieren.

Kennwörter vorausfüllen

Nachdem Sie Benutzerkonten zur Zulassungsliste einer Kennwortreplikationsrichtlinie hinzugefügt haben, können Sie deren Kennwörter für einen RODC vorausfüllen. So können die Kennwörter zum RODC repliziert werden, bevor Benutzer sich erstmalig anmelden.

1. Öffnen Sie auf dem RWDC die Seite **Benutzer und Computer**.
2. Klicken Sie links von der OU auf ▼, um die Domainobjekte auszuklappen, und wählen Sie **Domain Controllers**.
3. Klicken Sie mit der rechten Maustaste auf einen RODC und wählen Sie **Richtlinienstatus**.

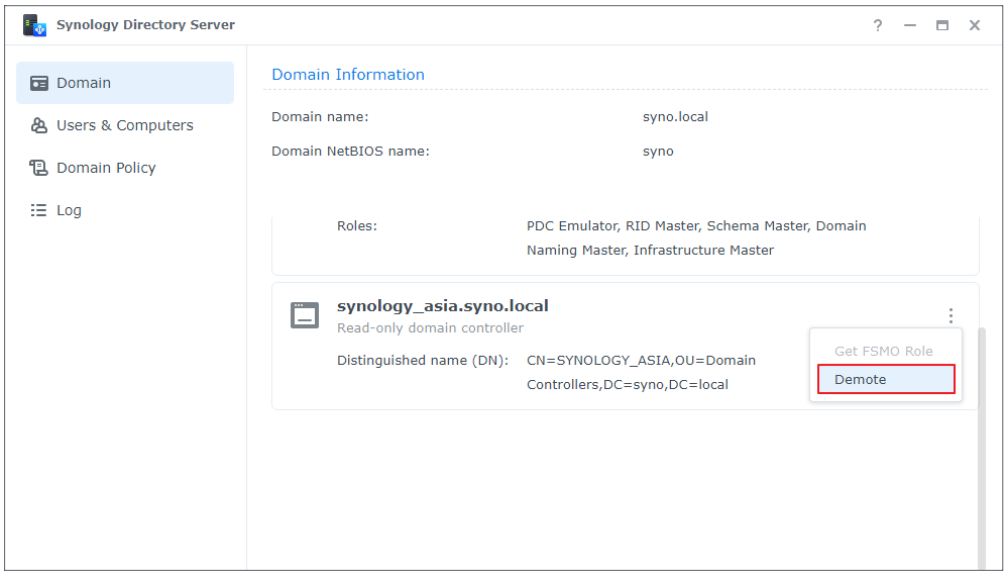


4. Wählen Sie im Dropdown-Menü **Kontotyp anzeigen** eine Option aus:
   - **Konten mit auf diesem RODC gespeicherten Kennwörtern**: Die Liste der Benutzerkonten anzeigen, deren Kennwörter zum RODC repliziert und dort gespeichert werden. Benutzeranmeldungen werden von diesem RODC authentifiziert.
   - **Auf diesem RODC authentifizierte Konten**: Die Liste der Benutzerkonten anzeigen, deren Kennwörter von diesem RODC zum RWDC zur Authentifizierung übertragen werden. Benutzeranmeldungen werden vom RWDC authentifiziert. Diese Liste wird nur angezeigt, wenn der RODC **einem Windows AD beigetreten** ist.
5. Klicken Sie auf **Kennwörter vorausfüllen**.
6. Geben Sie Administratorkonto und Kennwort Ihrer Domain ein, wählen Sie die gewünschten Benutzerkonten und klicken Sie auf **Kennwörter vorausfüllen**.

Einen DC zurückstufen

Durch das Zurückstufen können Sie DCs in der aktuellen Domain-Objekthierarchie außer Betrieb setzen, sie jedoch in der Domain belassen.

1. Öffnen Sie auf einem DC **Domain** > **Domain-Controller**.
2. Klicken Sie auf dem gewünschten DC auf ⋮ und wählen Sie **Zurückstufen**.



3. Bestätigen Sie und klicken Sie auf **Zurückstufen**. Das Zurückstufen kann **nicht rückgängig gemacht werden**.
4. Geben Sie das Kennwort Ihres Administratorkontos ein und klicken Sie auf **Senden**.

Anmerkung:

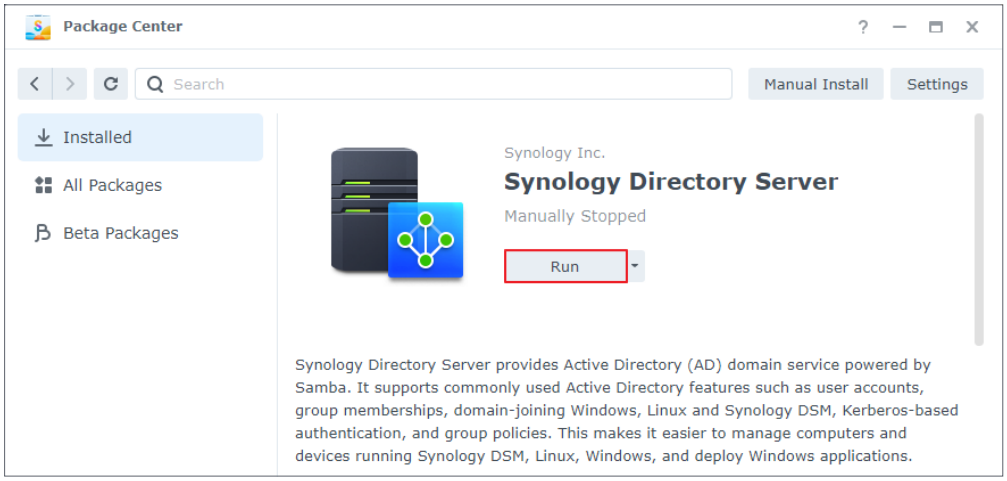
- Der DC mit FSMO-Rollen kann nicht zurückgestuft werden.
- Domaindienste werden entfernt, wenn der letzte DC in der Domain zurückgestuft wurde.
- Wenn Sie sich beim PDC anmelden, um einen SDC zurückzustufen, müssen Sie sich auch beim SDC anmelden, um zu bestätigen, dass Sie die entsprechenden Daten löschen wollen.

Die IP-Adresse eines DCs ändern

Synology Directory Server wird in der Regel mit einer statischen IP-Adresse eingerichtet. Möglicherweise müssen Sie jedoch die IP-Adresse des Synology NAS, auf dem Synology Directory Server ausgeführt wird, ändern.

1. **Synology Directory Server mit Hyper Backup sichern**.
2. Ändern Sie die IP-Adresse des Synology NAS.
3. **Ressourceneinträge in DNS Server bestätigen und aktualisieren**.
4. Starten Sie **Synology Directory Server** neu, um die Netzwerkeinstellungen zu aktualisieren:
    1. Gehen Sie zu **Paketzentrum** > **Installiert** > **Synology Directory Server**.

2. Klicken Sie auf ▼ und wählen Sie **Stopp**.
3. Klicken Sie zum erneuten Start auf **Ausführen**.



DNS-Ressourceneinträge verwalten

Domain Name System (DNS) ist ein Namenssystem, das den Datenaustausch zwischen Computern über das Internet und andere Netzwerke erleichtert. Es wird vor allem verwendet, um einfach zu merkende Domainnamen (z. B. „pc1.syno.local“) in die zugehörigen IP-Adressen (z. B. „192.168.1.5“) zu übersetzen. Diese Funktion ist essenziell für den Betrieb des Domaindienstes von Synology Directory Server.

A/AAAA-Ressourceneinträge

A und **AAAA** sind DNS-Ressourceneinträge für die Auflösung von Domainnamen und IP-Adressen. A-Einträge übersetzen Domainnamen in 32-Bit-IPv4-Adressen. AAAA-Einträge lösen Domainnamen in 128-Bit-IPv6-Adressen auf.

Automatische DNS-Registrierung

Wenn ein Client der von Synology Directory Server erstellten Domain beitritt, wird der Server automatisch einen A-Ressourceneintrag (und AAAA-Ressourceneintrag, wenn IPv6 aktiviert ist) beim DNS-Dienst in DSM registrieren oder aktualisieren, wodurch dem Hostnamen des Clients eine IP-Adresse zugewiesen wird.

Einschränkungen:

- Automatische DNS-Registrierung kann nicht deaktiviert werden.
- Namensregeln für Domain-Clients: Es sind nur Buchstaben (a-z, A-Z), Ziffern (0-9) und Bindestriche (-) zulässig.
- In Windows 7 oder 10: Bei einer Änderung von Hostnamen oder IP-Adresse ist eine erneute Anmeldung bzw. ein Neustart erforderlich.
- In DSM oder SRM: Bei einer Änderung von Hostnamen oder IP-Adresse ist eine erneute Anmeldung bzw. ein Neustart **nicht** erforderlich. Die Ressourceneinträge werden nicht aktualisiert.

A/AAAA-Ressourceneinträge anpassen

Standardmäßig verweisen alle A/AAAA-Ressourceneinträge auf die IP-Adresse des Synology NAS, auf dem die Domain erstellt wurde. So wird sichergestellt, dass Synology Directory Server Dienste erfolgreich bereitstellen kann.

Unter folgenden Umständen kann es jedoch sein, dass die A/AAAA-Ressourceneinträge nicht korrekt auf das Synology NAS verweisen:

- Die IP-Adresse des Synology NAS ändert sich, nachdem die Domain mit Synology Directory Server erstellt wurde.
- Synology Directory Server wird **von einer Hyper Backup-Sicherungsaufgabe wiederhergestellt**.

Passen Sie in den genannten Fällen die A/AAAA-Ressourceneinträge an.

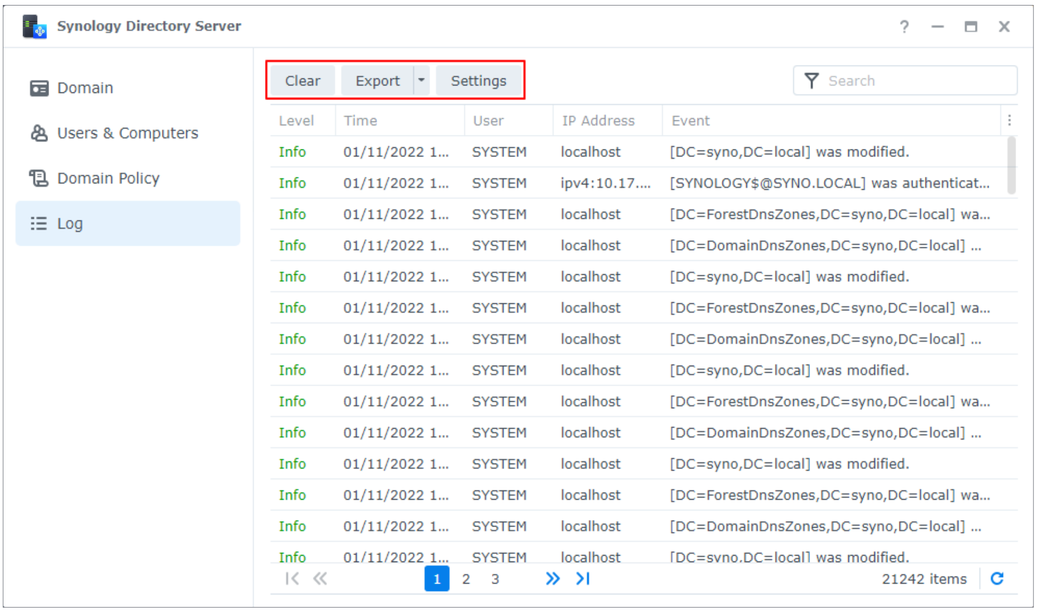
1. Öffnen Sie **DNS Server** > **Zonen**.
2. Wählen Sie die DNS-Zone aus (z. B. ***domainname*@Active Directory** oder **_msdcs.*domainname*@Active Directory**) und klicken Sie auf **Bearbeiten** > **Ressourceneintrag**.
3. Überprüfen Sie die in den A/AAAA-Ressourceneinträgen konfigurierten IP-Adressen. Stellen Sie sicher, dass alle Einträge auf Ihr Synology NAS verweisen.

Anmerkung:

- Für die Stapelbearbeitung halten Sie **Strg** oder die **Umschalttaste** gedrückt, um mehrere Ressourceneinträge desselben Typs mit unterschiedlichen Namen auszuwählen.

Systemprotokolle anzeigen und verwalten

Auf der Seite **Protokoll** werden Anmeldeereignisse und Änderungen an Domainobjekten als Protokolle aufgezeichnet. Domainadministratoren können anhand dieser Aufzeichnungen die Verbindungsinformationen von Synology Directory Server nachverfolgen und mögliche Probleme beheben.



Protokollierung aktivieren

- Klicken Sie auf **Einstellungen** und setzen Sie ein Häkchen bei **Überwachungsprotokollierung aktivieren (kann Datenbankleistung beeinträchtigen)**. Dies kann die Datenbankleistung von Synology Directory Server beeinträchtigen.

Protokolle verwalten

- Suchen Sie in der Suchleiste oben rechts nach zu den angegebenen Kriterien passenden Protokollen.
- Klicken Sie rechts unten auf das Aktualisieren-Symbol, um die Protokollliste zu aktualisieren.
- Klicken Sie auf **Löschen**, um alle Protokolleinträge zu löschen. Das Löschen von Protokollen kann **nicht rückgängig gemacht werden**.
- Klicken Sie auf **Exportieren** und wählen Sie **HTML** oder **CSV** als Exportformat für die Protokolle aus.

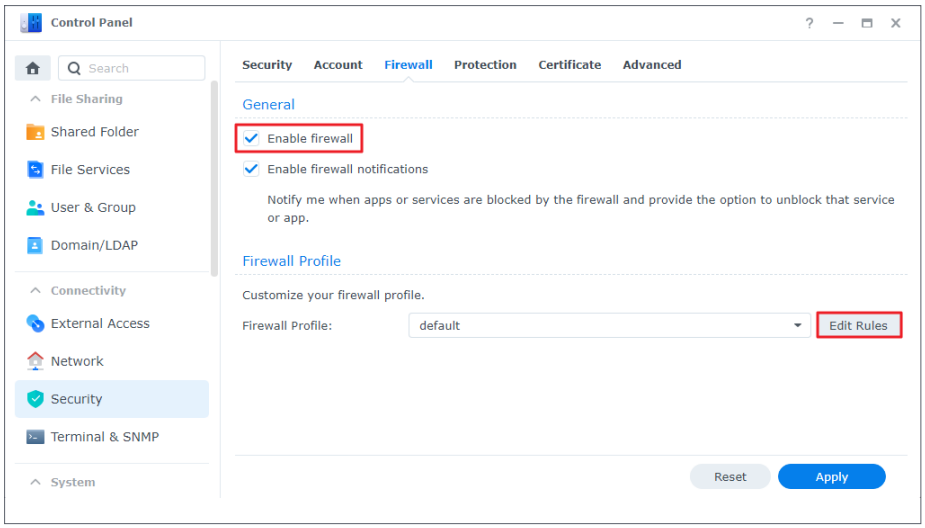
Anmerkung:

- Wenn die Anzahl an Protokollen den Grenzwert (200.000) erreicht, werden die 5.000 ältesten Protokolle gelöscht, um Speicherplatz freizugeben.

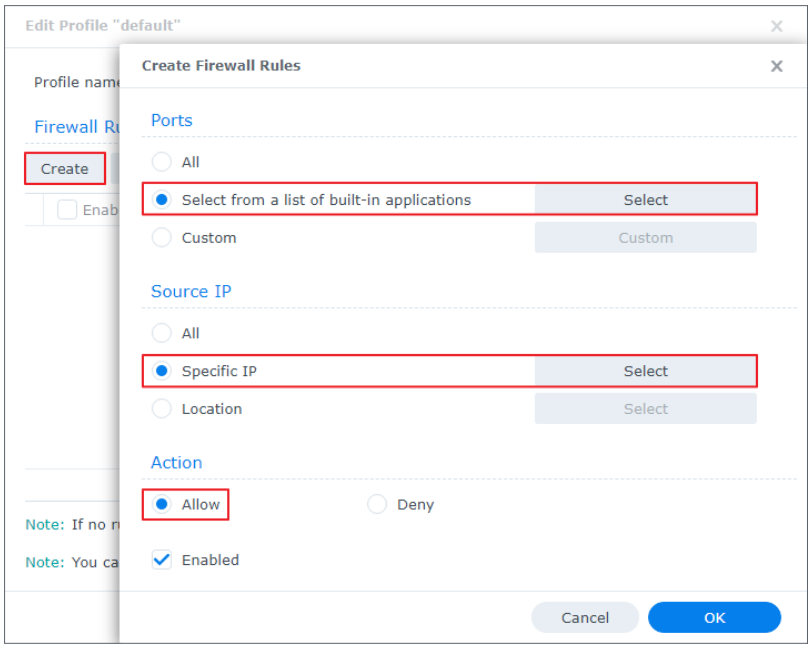
Firewall-Regeln zur Sicherung des Verzeichnisdienstes hinzufügen

Neben der effizienten Verwaltung ist Sicherheit eines der wichtigsten Themen für Synology Directory-Administratoren. Mit Firewall-Regeln können Sie Ihren Verzeichnisdienst vor unbefugten Anmeldungen schützen und den Zugriff kontrollieren.

1. Öffnen Sie auf einem RWDC **Systemsteuerung** > **Sicherheit** > **Firewall**.
2. Setzen Sie ein Häkchen bei **Firewall aktivieren**.
3. Wählen Sie unter **Firewall-Profil** im Dropdown-Menü ein Firewall-Profil aus und klicken Sie auf **Regeln bearbeiten**.



4. Klicken Sie auf **Erstellen**.
5. Wählen Sie unter **Ports** die Option **Aus einer Liste integrierter Anwendungen auswählen** und klicken Sie auf **Auswählen**.
6. Wählen Sie **DNS Server**, **Synology Directory Server** und **Windows-Dateiserver**. Klicken Sie auf **OK**.
7. Wählen Sie unter **Quell-IP** die Option **Spezifische IP** und klicken Sie auf **Auswählen**.
8. Geben Sie eine IP-Adresse oder einen IP-Bereich ein, um das lokale Netzwerk anzugeben, in dem Synology Directory Server ausgeführt wird. Bestätigen Sie die Daten und klicken Sie auf **OK**.
9. Wählen Sie unter **Aktion** die Option **Zulassen**, um den Zugriff über die angegebenen Ports und IP-Adressen zuzulassen.
10. Klicken Sie auf **OK**, um die Einstellungen zu speichern.



Anmerkung:

- Weitere Informationen zu den Firewall-Einstellungen in DSM finden Sie in diesem **Hilfe-Artikel**.

Kapitel 4: Domainobjekte verwalten

In einer von Synology Directory Server gehosteten Domain werden verfügbare Ressourcen in Form von Objekten wie OUs, Gruppen, Benutzern und Geräten (z. B. Computer, Drucker und Synology NAS) erstellt und gespeichert. Nur RWDCs können Domainobjekte verwalten. RODCs können sie nur anzeigen.

Domainobjekte anzeigen

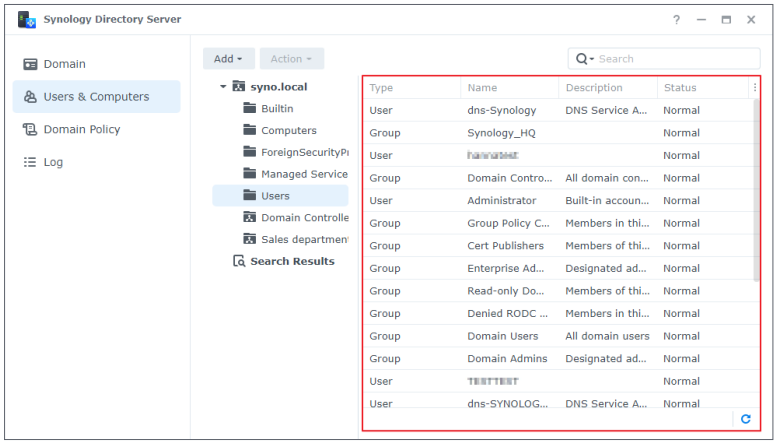
Auf der Seite **Benutzer und Computer** sehen Sie die gesamte Baumstruktur der Domain und rechts Informationen zu Objekten:

- **Typ**: Zeigt den Typ des Objekts an. Objekte können OUs, Gruppen, Benutzer oder Computer sein.
- **Name**: Der Name eines Objekts (ausgenommen OUs) wird im folgenden Format angezeigt.

  ```
  Domain-NetBIOS-Name\Objektname
  ```

- **Beschreibung**: Die Beschreibung des Domainobjekts.
- **DN**: Der definierte Name (DN) ist der Pfad eines Objekts in der Domaindatenbank. Wenn beispielsweise der DN „CN=bach,OU=sales,DC=syno,DC=local“ können Sie dessen Elemente wie folgt analysieren:
  - **CN**=bach: Der Name dieses Benutzers lautet „bach“.
  - **OU**=sales: Dieser Benutzer gehört der Organisationseinheit „sales“ an.
  - **DC**=syno,**DC**=local: Dieser Benutzer befindet sich in der Domain „syno.local“.
- **Status**: Der Status **Normal** oder **Deaktiviert** wird angezeigt, je nachdem, ob ein Domainobjekt aktiviert oder deaktiviert ist.

Klicken Sie auf ⋮, um ein Objekt auszuwählen und weitere Informationen anzuzeigen.

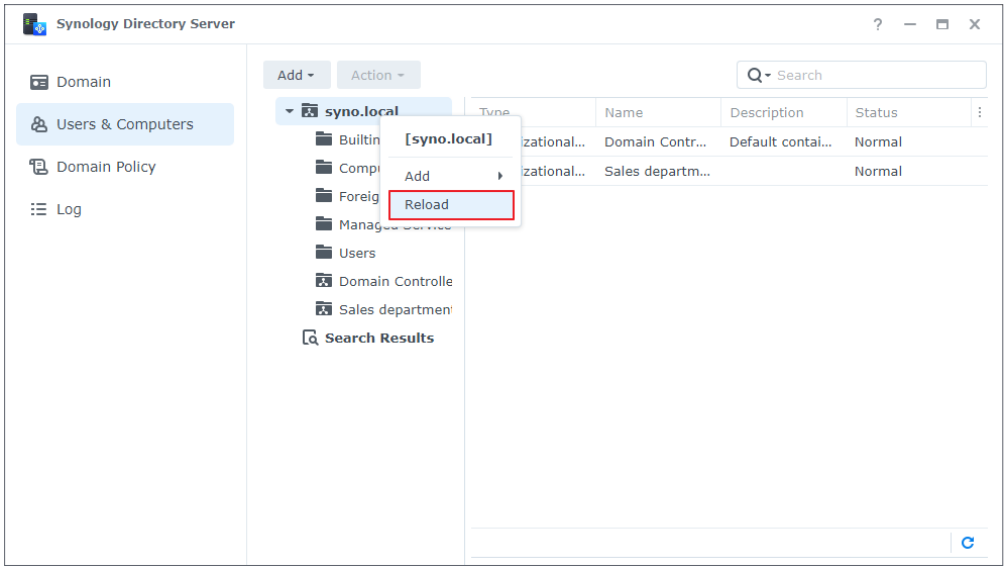


OUs verwalten

Eine OU ist ein Containerobjekt innerhalb einer Domain, dem Sie alle Arten von Domainobjekten, einschließlich Benutzer, Gruppen, Computer und anderer OUs, hinzufügen können. OUs organisieren Domainobjekte hierarchisch, was bei einer großen Anzahl an Benutzern, Computern und Gruppen hilfreich ist. Mit einer gut geplanten OU-Struktur können Sie ganz einfach Gruppenrichtlinien mit bestimmten Domainobjekten verknüpfen und administrative Aufgaben an diese delegieren.

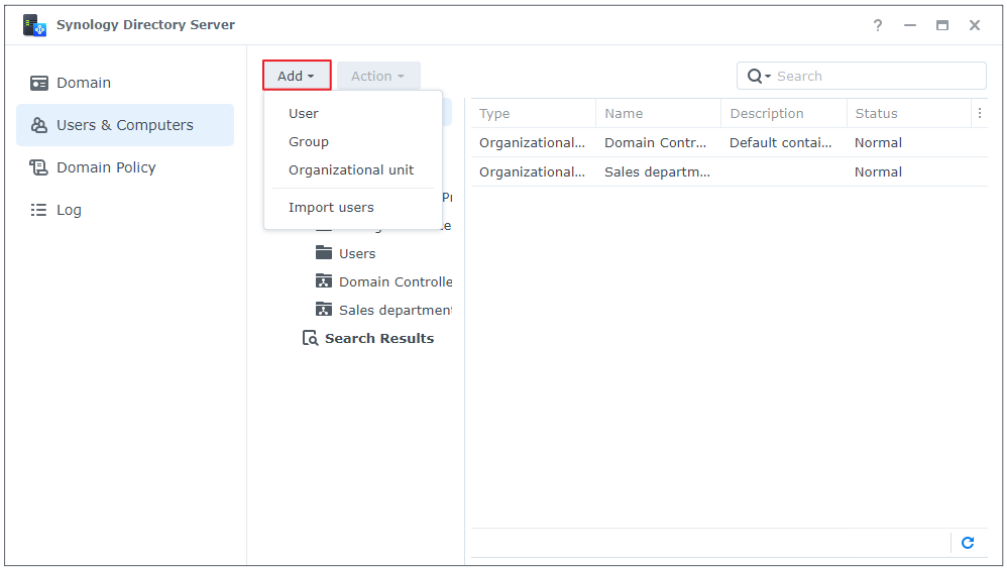
OU hinzufügen

1. Wählen Sie auf einem RWDC auf der Seite **Benutzer und Computer** in der Strukturliste eine Domain oder OU aus und klicken Sie auf **Hinzufügen** > **Organisationseinheit**.
2. Geben Sie der neuen OU im Feld einen Namen und klicken Sie auf **OK**.
3. Klicken Sie mit der rechten Maustaste auf den übergeordneten Container der neu hinzugefügten OU und auf **Neu laden**. Die neu hinzugefügte OU wird in der Strukturliste angezeigt.

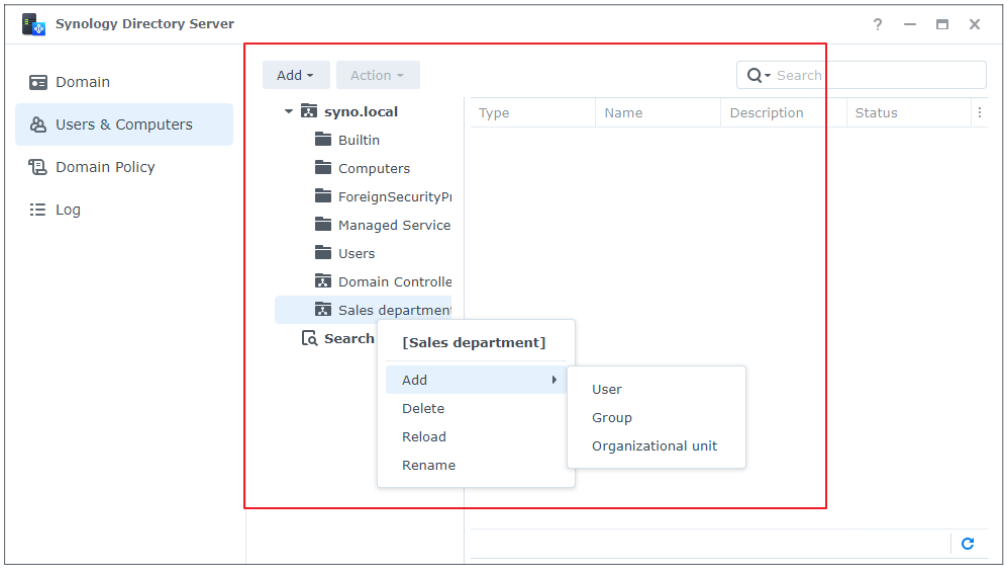


Objekte zu einer OU hinzufügen

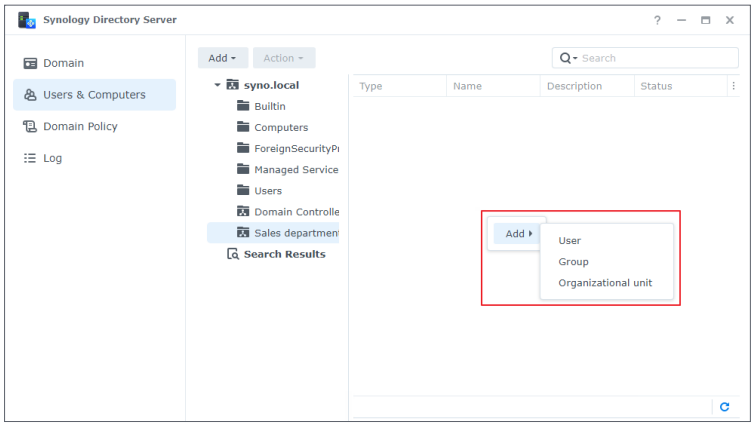
1. Öffnen Sie auf einem RWDC die Seite **Benutzer und Computer**, wählen Sie in der Strukturliste eine OU aus und wählen Sie eine Methode zum Starten des Assistenten:
   - **Methode 1**: Klicken Sie auf **Hinzufügen** und wählen Sie im Dropdown-Menü einen Objekttyp aus.



- **Methode 2**: Rechtsklicken Sie in der Strukturliste auf die gewünschte OU, wählen Sie **Hinzufügen** und wählen Sie dann einen Objekttyp.



- **Methode 3**: Rechtsklicken Sie auf die leere Fläche der gewünschten OU und wählen Sie einen Objekttyp zum Hinzufügen aus.



2. Folgen Sie den Anweisungen des Assistenten, um ein Objekt hinzuzufügen. Weitere Informationen finden Sie unter **OU hinzufügen**, **Gruppe hinzufügen** und **Benutzer hinzufügen**.

Anmerkung:

- Sie können ein oder mehrere Objekte zu einer OU in der Strukturliste ziehen und ablegen.
- Der Standard-Ansichtsmodus des Verzeichnisses zeigt nur Objekte an, die keiner OU angehören. Alle Benutzer, Gruppen, Computer und OUs anzeigen:
  1. Wählen Sie den Stammordner (der nach Ihrer Domain benannt ist) aus der Strukturliste aus und klicken Sie auf das Lupensymbol rechts oben.
  2. Setzen Sie in der Suchleiste ein Häkchen bei **Alle Ableitungen** und klicken Sie auf **OK**.

Eine OU löschen

1. Klicken Sie auf einem RWDC in der Strukturliste mit der rechten Maustaste auf die gewünschte OU und klicken Sie auf **Löschen**.
2. Klicken Sie erneut auf **Löschen**, um das Löschen zu bestätigen. Das Löschen kann **nicht rückgängig gemacht werden**.

Gruppen verwalten

Sie können Domainbenutzer in eine Gruppe geben und für diese eine **Zugriffskontrollliste** (ACL) anwenden, um den Benutzern Zugriffsrechte für Geräte, Anwendungen oder andere Dienste in der Domain zu geben.

Standardgruppen

Wenn Sie eine Domain einrichten, erstellt Synology Directory Server die folgenden Standardgruppen, um Ihnen die Verwaltung der Domain und die Konfiguration von Zugriffsberechtigungen zu erleichtern.

Gruppenname	Beschreibung
Allow RODC Password Replication Group	Mitglieder dieser Gruppe können Ihre Kennwörter für alle RODCs in der Domain replizieren.
Cert Publishers	Mitglieder dieser Gruppe haben Berechtigungen zum Ausstellen von Zertifikaten.
Denied RODC Password Replication Group	Mitglieder dieser Gruppe können ihre Kennwörter zu keinen RODCs in der Domain replizieren.
DnsAdmins	Mitglieder dieser Gruppe können auf DNS in der Domain zugreifen.
DnsUpdateProxy	Mitglieder dieser Gruppe sind DNS-Clients, die im Namen anderer Clients (etwa DHCP-Server) dynamische Aktualisierungen vornehmen dürfen.

Gruppenname	Beschreibung
Domain Admins	Mitglieder dieser Gruppe haben Administratorrechte und können sämtliche Objekte und Einstellungen in der Domain verwalten.
Domain Computers	In dieser Gruppe sind standardmäßig alle Rechner und Server der Domain enthalten.
Domain Controllers	Diese Gruppe enthält standardmäßig alle DCs.
Domain Guests	In dieser Gruppe sind standardmäßig alle Gäste der Domain enthalten.
Domain Users	In dieser Gruppe sind standardmäßig alle Benutzer der Domain enthalten.
Enterprise Admins	Mitglieder dieser Gruppe haben Administratorrechte und können sämtliche Objekte und Einstellungen in der Domainstruktur der gesamten Organisation verwalten.
Enterprise Read-Only Domain Controllers	In dieser Gruppe sind standardmäßig alle RODCs in der Domainstruktur der gesamten Organisation enthalten.
Group Policy Creator Owners	Mitglieder dieser Gruppe können Gruppenrichtlinien für die Domain ändern.
RAS and IAS Servers	Mitglieder dieser Gruppe dürfen Dienste für den Fernzugriff nutzen.
Read-Only Domain Controllers	Diese Gruppe enthält standardmäßig alle RODCs.
Schema Admins	Mitglieder dieser Gruppe können Änderungen am Domainschema vornehmen.

Anmerkung:

- Synology Directory Server entspricht in Sachen Funktionalität Windows Server 2008 R2. Weitere Informationen zu integrierten Domaingruppen finden Sie in **diesem Artikel**.

Gruppe hinzufügen

1. Öffnen Sie auf dem RWDC die Seite **Benutzer und Computer** und klicken Sie auf **Hinzufügen** > **Gruppe**.
2. Geben Sie die Gruppeninformationen ein und klicken Sie auf **Weiter**:
   - **Gruppenumfang**
     - **Domain lokal**: Lokale Domaingruppen werden verwendet, um Berechtigungen für Ressourcen in ihrer Ursprungsdomain zuzuweisen. In diesen Gruppentyp können andere lokale Domaingruppen in derselben Domain verschachtelt werden. Er kann auch Benutzerkonten, globale Gruppen und universelle Gruppen aus allen Domains oder Gesamtstrukturen enthalten.
     - **Global**: Globale Gruppen dienen dem Verwalten von Benutzerkonten. Sie können Benutzerkonten und weiter globale Gruppen in derselben Domain enthalten. In der Praxis empfehlen wir, globale Gruppen in lokalen Domaingruppen mit bestimmten Berechtigungen zu platzieren, anstatt ihnen selbst direkt Berechtigungen zuzuweisen.

    - **Universell**: Universelle Gruppen werden hauptsächlich zur domainübergreifenden Schachtelung globaler Gruppen verwendet. Sie können Benutzerkonten, globale Gruppen und andere universelle Gruppen aus beliebigen Domains in der Gesamtstruktur, in der sie sich befinden, enthalten. In der Praxis empfehlen wir, universelle Gruppen in lokalen Domaingruppen mit bestimmten Berechtigungen zu platzieren, anstatt ihnen selbst direkt Berechtigungen zuzuweisen.
- **Gruppentyp**
    - **Sicherheit**: Sicherheitsgruppen werden eingerichtet, um Zugriffsberechtigungen zur Ausführung bestimmter Systemaufgaben in der Domain festzulegen.
    - **Verteiler**: Verteilergruppen werden eingerichtet, um E-Mail-Nachrichten an eine Reihe von Benutzern zu senden. Sie können als E-Mail-Alias verwendet werden.

3. Bestätigen Sie die Gruppeninformationen und klicken Sie auf **Fertig**.

Gruppeneigenschaften bearbeiten

1. Öffnen Sie auf einem RWDC die Seite **Benutzer und Computer**, wählen Sie die gewünschte Gruppe und eine der folgenden Optionen:
    - Klicken Sie auf **Aktion** > **Eigenschaften**.
    - Rechtsklicken Sie auf die Gruppe und klicken Sie auf **Eigenschaften**.
    - Doppelklicken Sie auf die Gruppe.
2. Bearbeiten Sie die Eigenschaften der Gruppe unter **Allgemein** und **Mitglieder**.
    - **Allgemein**: Gruppenname, Beschreibung, E-Mail, Gruppenumfang und Gruppentyp.
    - **Mitglieder**: Fügen Sie Mitglieder zur Gruppe hinzu oder entfernen Sie sie.
3. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Gruppe löschen

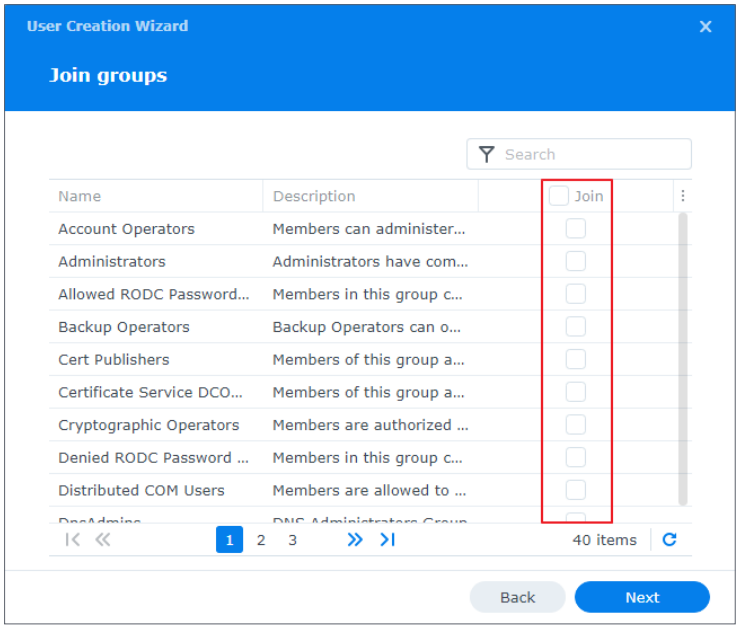
1. Öffnen Sie auf einem RWDC die Seite **Benutzer und Computer** und wählen Sie die gewünschte Gruppe aus. Mit **Strg** bzw. **Umschalttaste** können Sie eine Mehrfachauswahl treffen.
2. Führen Sie einen der folgenden Schritte durch:
    - Klicken Sie auf **Aktion** > **Löschen**.
    - Rechtsklicken Sie auf die Gruppe und klicken Sie auf **Löschen**.
3. Klicken Sie auf **Löschen**, um die Aktion zu bestätigen. Das Löschen kann **nicht rückgängig gemacht werden**.

Mitglieder zu Gruppen hinzufügen

Weisen Sie Benutzer auf eine der folgenden drei Weisen zu Gruppen zu.

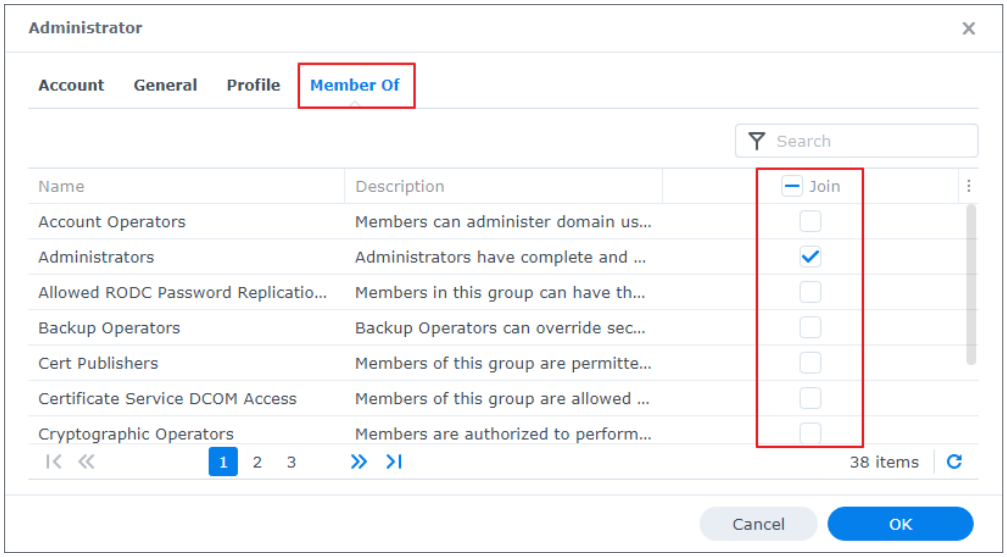
Methode 1: Benutzer beim Erstellen zu Gruppen hinzufügen

1. Folgen Sie den Schritten unter **Benutzer hinzufügen**.
2. Wählen Sie im zweiten Schritt des **Assistenten zur Benutzererstellung** die Gruppen, zu denen Sie den Benutzer hinzufügen möchten, und klicken Sie auf **Weiter**. Folgen Sie dem Assistenten, um den Vorgang abzuschließen.



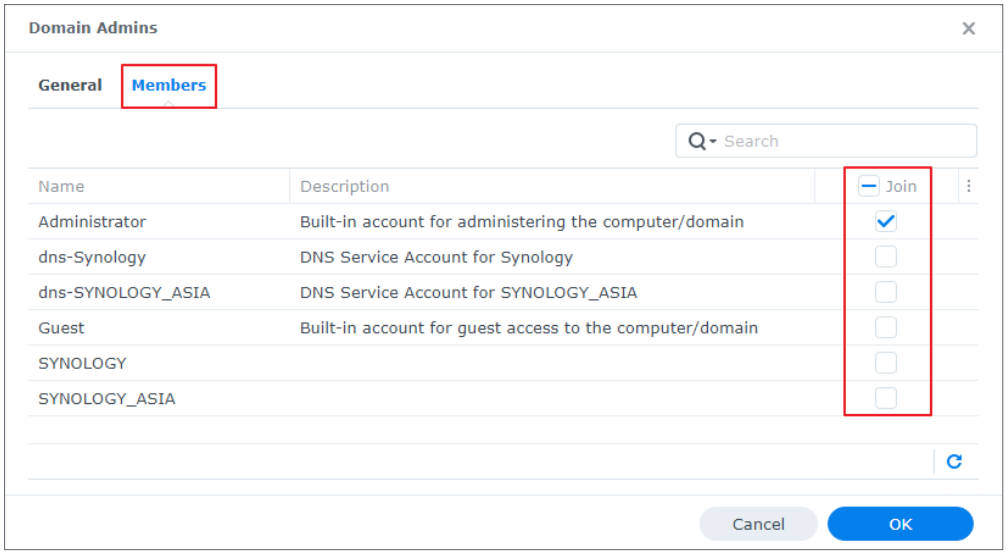
Methode 2: Benutzer durch Bearbeiten von Benutzerprofilen zu Gruppen hinzufügen

1. Öffnen Sie auf einem RWDC die Seite **Benutzer und Computer**, wählen Sie den gewünschten Benutzer und eine der folgenden Optionen:
   - Klicken Sie auf **Aktion** > **Eigenschaften**.
   - Rechtsklicken Sie auf den Benutzer und wählen Sie **Eigenschaften**.
2. Wählen Sie unter **Mitglied von** die Gruppen für den Benutzer aus und klicken Sie auf **OK**.



Methode 3: Benutzer durch Bearbeiten von Gruppeneigenschaften zu Gruppen hinzufügen

1. Öffnen Sie auf einem RWDC die Seite **Benutzer und Computer**, wählen Sie die gewünschte Gruppe und eine der folgenden Optionen:
   - Klicken Sie auf **Aktion** > **Eigenschaften**.
   - Rechtsklicken Sie auf die Gruppe und wählen Sie **Eigenschaften**.
2. Wählen Sie unter **Mitglieder** die Benutzer für diese Gruppe aus und klicken Sie auf **OK**.



Benutzer verwalten

Benutzer in einer Domain sind Benutzerkonten, die entsprechend ihren Rechten auf Ressourcen in der Domain zugreifen können.

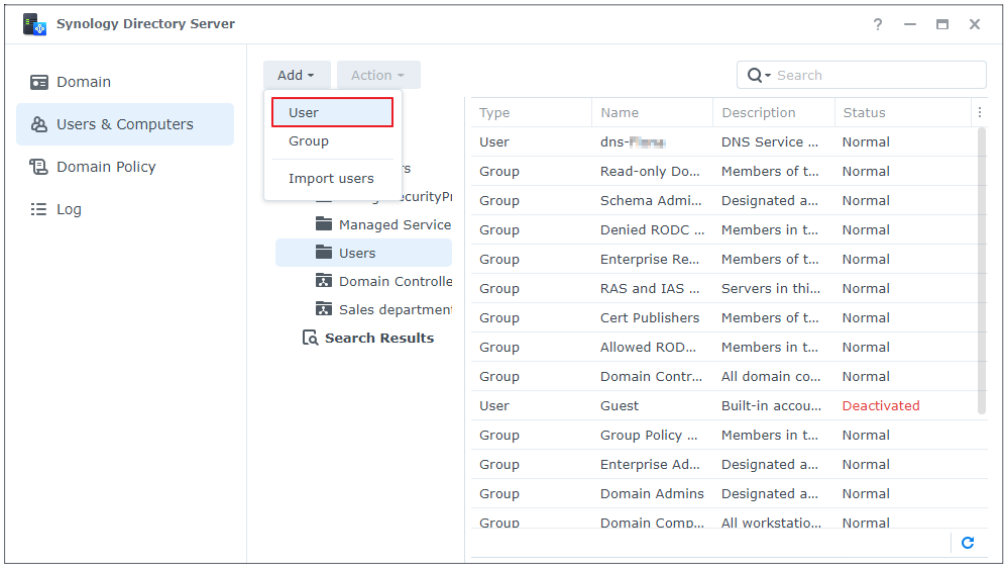
Standardbenutzer

Wenn Sie eine Domain einrichten, erstellt Synology Directory Server die folgenden Standardbenutzerkonten, um die Verwaltung der Domain zu erleichtern.

Username	Beschreibung
Administrator	Das Administratorkonto hat volle Kontrolle über Synology Directory Server. Es wird zur Verwaltung von Domain und DCs verwendet.
dns-*NAS-Hostname*	Das DNS-Dienstkonto für das Synology NAS. Es ist nach dem Hostnamen des DCs benannt, beispielsweise „dns-MyNAS“.
Gast	Das Konto für den Gastzugriff auf die Domain und bereitgestellte Geräte.
krbtgt	Das Konto für den Dienst Kerberos Key Distribution Center auf dem DC.

Benutzer hinzufügen

1. Klicken Sie auf dem RWDC auf der Seite **Benutzer und Computer** in der Strukturliste auf einen Container, zu dem Sie den Benutzer hinzufügen möchten. Der Container kann der nach Ihrer Domain (z. B. „SYNO.LOCAL“) benannte Container, der Container **Users** oder eine OU sein.
2. Führen Sie einen der folgenden Schritte durch:
   - Klicken Sie auf **Hinzufügen** > **Benutzer**.
   - Rechtsklicken Sie auf den Container und wählen Sie **Hinzufügen** > **Benutzer**.
   - Klicken Sie auf den leeren Bereich des angegebenen Containers und wählen Sie **Hinzufügen** > **Benutzer**.



3. Geben Sie die Benutzerinformationen ein und klicken Sie auf **Weiter**. Um die Sicherheit zu erhöhen, ist **Dieses Konto zwingen, bei der nächsten Anmeldung das Kennwort zu ändern** standardmäßig aktiviert. Die Anforderungen an die Kennwortstärke hängen von der unter **Synology Directory Server** > **Domainrichtlinie** konfigurierten Kennwortrichtlinie ab.
4. Wählen Sie die Gruppen für den Benutzer aus und klicken Sie auf **Weiter**.
5. Bestätigen Sie die Einstellungen und klicken Sie auf **Fertig**, um den Domainbenutzer hinzuzufügen.

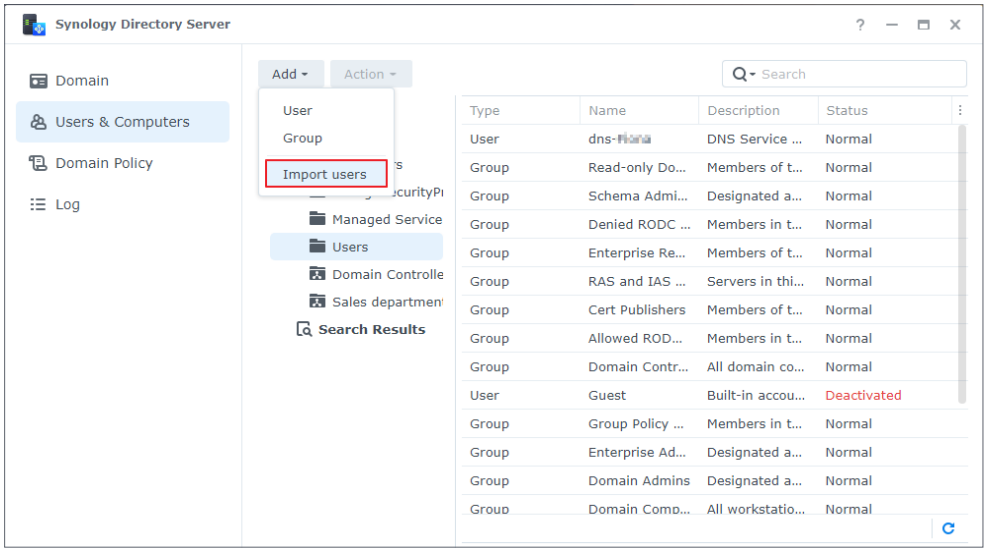
Anforderungen an die Kennwortstärke:

Kennwörter müssen **mindestens drei** der folgenden Regeln erfüllen:

- Großbuchstaben (einschließlich A-Z mit diakritischen Zeichen) des lateinischen, griechischen und kyrillischen Alphabets.
- Kleinbuchstaben (einschließlich a-z mit diakritischen Zeichen) des lateinischen, griechischen und kyrillischen Alphabets.
- Ziffern (0-9).
- Sonderzeichen wie #, $, !
- Unicode-Alphabete, darunter jene in asiatischen Sprachen.

Mehrere Benutzer importieren

1. Klicken Sie auf dem RWDC auf der Seite **Benutzer und Computer** in der Strukturliste auf einen Container, zu dem Sie Benutzer hinzufügen möchten. Der Container kann der nach Ihrer Domain (z. B. „SYNO.LOCAL“) benannte Container, der Container **Users** oder eine OU sein.
2. Klicken Sie auf **Hinzufügen** > **Benutzer importieren**.



3. Setzen Sie nach Bedarf Häkchen bei den folgenden Optionen:
   - **Doppelte Konten überschreiben**: Ersetzt doppelte Konten durch jene in der Benutzerliste.
   - **Eine Benachrichtigung an den neu erstellten Benutzer senden**: Benachrichtigt Benutzer, deren Konto neu erstellt wurde, per E-Mail. Diese Option erfordert die Aktivierung der System-E-Mail-Benachrichtigungen unter **Systemsteuerung** > **Benachrichtigung** > **E-Mail**.
   - **Benutzerkennwort in E-Mail-Benachrichtigung anzeigen**: Zeigt das Kennwort des Benutzerkontos in der Benachrichtigung an. Diese Option ist verfügbar, wenn **Eine Benachrichtigung an den neu erstellten Benutzer senden** aktiviert ist.
   - **Importierte Benutzer müssen bei der ersten Anmeldung ihr Kennwort ändern**: Zwingt importierte Benutzer, bei der ersten Anmeldung ihre Kennwörter zu ändern. Dies bietet zusätzliche Sicherheit für importierte Konten.
4. Klicken Sie auf **Durchsuchen** und laden Sie eine .txt-Datei hoch.
5. Klicken Sie auf **OK**.

Dateiformat:

Wenn Sie eine Datei für den Import vorbereiten, sollte jedes Benutzerkonto in einer eigenen Reihe stehen. Die einzelnen Informationen sollten durch **Tabulator** getrennt in folgender Reihenfolge angegeben sein:

1. Benutzername 2. Kennwort 3. Beschreibung 4. E-Mail
5. Vorname 6. Nachname 7. Voller Name
8. Profil-Pfad 9. Login-Skript 10. Home-Verzeichnis

Das Format sollte folgende Anforderungen erfüllen:

- Die Datei muss das Format UTF-8 haben.
- Die Spalten müssen korrekt angeordnet sein (von links nach rechts).
- Die importierten Kennwörter müssen die **Anforderungen an die Kennwortstärke**erfüllen.
- Jede Zeile mit Informationen muss neun Tabstopps als Trennzeichen enthalten. Wenn Sie eine Information überspringen möchten, müssen Sie dennoch die **Tabulatortaste** drücken, um den leeren Wert vom nächsten Wert abzugrenzen.

Benutzereigenschaften bearbeiten

1. Öffnen Sie auf einem RWDC die Seite **Benutzer und Computer** und wählen Sie den gewünschten Benutzer aus. Mit **Strg** bzw. **Umschalttaste** können Sie eine Mehrfachauswahl treffen.
2. Führen Sie einen der folgenden Schritte durch:
   - Klicken Sie auf **Aktion** > **Eigenschaften**.
   - Rechtsklicken Sie auf den Benutzer und wählen Sie **Eigenschaften**.
3. Bearbeiten Sie unter **Konto** die folgenden Eigenschaften:
   - **Benutzer Anmeldename**: Benennen Sie den Benutzer um.
   - **Anmeldestunden**: Wählen Sie anhand des Rasters aus, wann der Benutzer sich **anmelden kann** und wann **nicht**. Klicken Sie auf Tage oder Stunden, um den ganzen Tag oder die gewünschte Stunde eines Tages auszuwählen.
   - **Verwendbare Geräte**: Wählen Sie, auf welche Computer der Benutzer Zugriff hat.
   - **Kennwort ändern**: Setzen Sie hier ein Häkchen, um das Kennwort des Benutzers zu ändern.
   - **Dieses Konto sperren**: Diese Option ist aktiviert, wenn ein Konto aufgrund der Richtlinien für die Kontosperre unter **Domainrichtlinie** > **Kontosperre-Richtlinie** gesperrt ist. Deaktivieren Sie diese Option, um das Konto zu entsperren.
   - **Dieses Konto zwingen, bei der nächsten Anmeldung das Kennwort zu ändern**: Dieses Konto wird bei der nächsten Anmeldung in Windows oder beim Synology NAS aufgefordert, das Kennwort zu ändern.
   - **Nicht zulassen, dass der Benutzer das Kennwort ändert**: Dieser Benutzer kann das Kennwort nicht selbst ändern.

- **Kennwort läuft nie ab**: Das Kennwort des Benutzers läuft niemals ab. Wir empfehlen, diese Option nur für Administratoren zu aktivieren.
- **Kennwörter mittels reversibler Verschlüsselung speichern**: Das Aktivieren dieser Option gefährdet die Sicherheit der Domain. Diese Option wird nicht empfohlen, außer die Anforderungen von Domain-Client-Diensten haben höhere Priorität als die Kennwortsicherheit.
- **Dieses Konto deaktivieren**: Setzen Sie hier ein Häkchen, um das Benutzerkonto zu deaktivieren.
- **Chipkarte für interaktive Anmeldung erforderlich**: Benutzer müssen für die Anmeldung bei ihren Client-Geräten ihre Chipkarte verwenden.
- **Delegation dieses sensiblen Kontos nicht erlauben**: Dieses Konto ist sensibel und kann nicht delegiert werden. Wenn diese Option aktiviert ist, können auf dem Client-Gerät keine Dienste für einen anderen Benutzer ausgeführt werden.
- **DES-Verschlüsselung für dieses Konto verwenden**: Die Anmeldedaten dieses Kontos werden bei der Kerberos-Authentifizierung mittels DES (Data Encryption Standard) verschlüsselt.
- **Dieses Konto von Kerberos-Vorauthentifizierung ausnehmen**: Setzen Sie hier ein Häkchen, wenn dieses Benutzerkonto keine Kerberos-Vorauthentifizierung benötigt.
- **Einstellungen für Kontoablauf**: Wählen Sie **Konto läuft nie ab** oder geben Sie ein **Ablaufdatum des Kontos** an.

4. Bearbeiten Sie unter **Allgemein** die allgemeinen Daten.
5. Bearbeiten Sie unter **Profil** das Benutzerprofil. So können Benutzer eine einheitliche Desktop-Nutzererfahrung haben, wenn sie auf Geräte in der Domain zugreifen:
   - **Profil-Pfad**: Der Ordnerpfad, der das Profil des Benutzers enthält, wie etwa die Ordner **Desktop**, **Document** und **Picture**.
   - **Login-Script**: Ein Skript wird automatisch ausgeführt, wenn ein Benutzer sich bei Windows anmeldet. Sie können eine Windows .bat-Datei mit maximal 2 MB hochladen, indem Sie auf **Datei hochladen** klicken.
   - **Home-Verzeichnis**:
     - **Lokaler Pfad**: Wählen Sie einen lokalen Ordner als Home-Verzeichnis aus.
     - **Verbinden...mit**: Wählen Sie einen freigegebenen Remote-Ordner auf dem Synology NAS als Home-Verzeichnis aus. Wenn diese Option ausgewählt ist, wird der freigegebene Remote-Ordner automatisch **von Windows als Netzlaufwerk bereitgestellt**.
6. Unter **Mitglied von** können Sie den Benutzer zu einer Gruppe hinzufügen oder aus einer Gruppe entfernen.
7. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Anmerkung:

- Auch die Eigenschaften **deaktivierter** Benutzer können geändert werden.

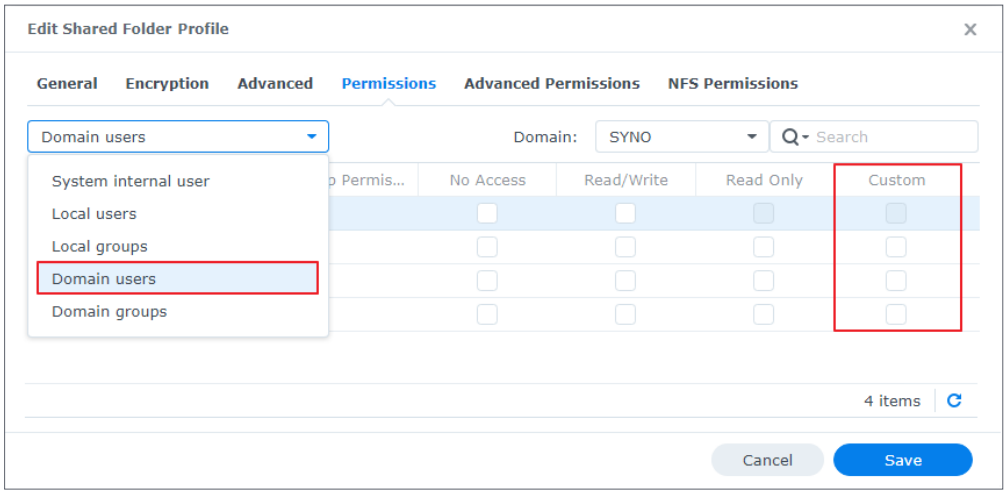
Benutzer löschen

1. Öffnen Sie auf einem RWDC die Seite **Benutzer und Computer** und wählen Sie den gewünschten Benutzer aus. Mit **Strg** bzw. **Umschalttaste** können Sie eine Mehrfachauswahl treffen.
2. Führen Sie einen der folgenden Schritte durch:
   - Klicken Sie auf **Aktion** > **Löschen**.
   - Rechtsklicken Sie auf den Benutzer und wählen Sie **Löschen**.
3. Klicken Sie auf **Löschen**, um die Aktion zu bestätigen. Das Löschen kann **nicht rückgängig gemacht werden**.

Servergespeichertes Profil für einen einzelnen Benutzer zuweisen

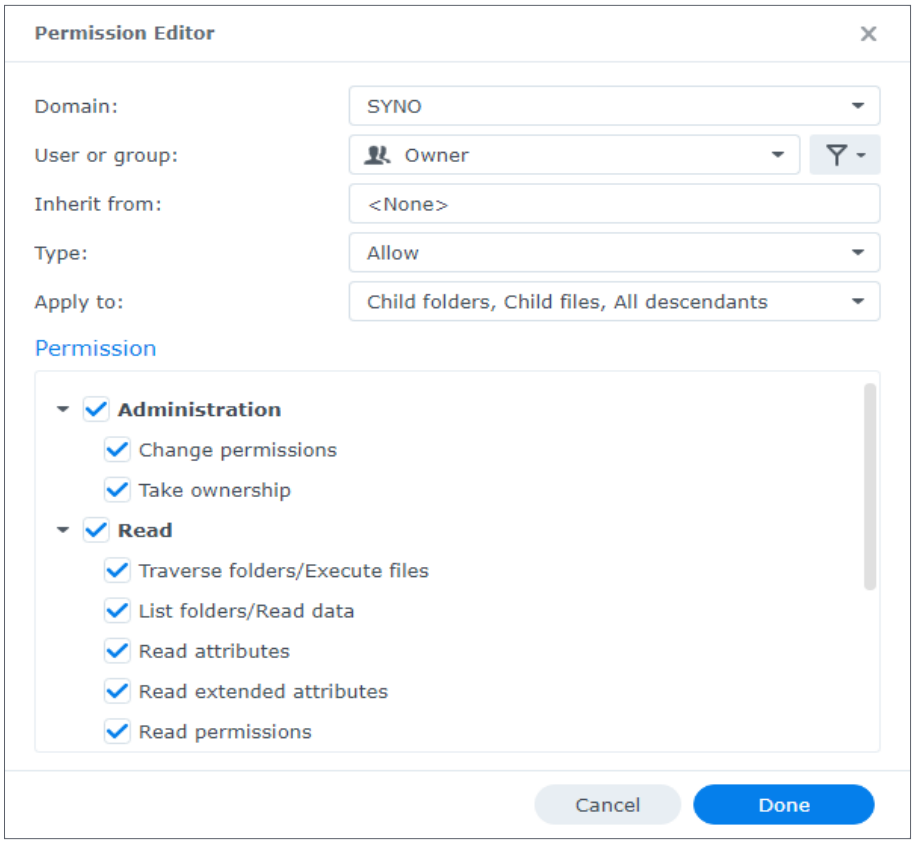
Durch das Zuweisen servergespeicherter Profile können Domainbenutzer stets auf Ihre Dateien zugreifen, auch wenn sie sich bei verschiedenen Computern der Domain anmelden. Bevor Sie einem Benutzer ein servergespeichertes Profil zuweisen, müssen Sie einen freigegebenen Ordner erstellen und mindestens einen Computer zur Domain hinzufügen.

1. **Mit dem Windows-PC eines Benutzers einer Domain beitreten**.
2. Öffnen Sie auf einem RWDC **Systemsteuerung** > **Freigegebener Ordner** > **Erstellen** > **Freigegebenen Ordner erstellen**, um einen freigegebenen Ordner zu erstellen. Die freigegebenen Ordner für einen einzelnen Benutzer und für alle Benutzer sollten verschieden sein.
3. Klicken Sie mit der rechten Maustaste auf den erstellten freigegebenen Ordner und klicken Sie auf **Bearbeiten**.
4. Wählen Sie unter **Berechtigungen** im Dropdown-Menü **Domain Users** aus.
5. Setzen Sie ein Häkchen bei **Benutzerdefiniert**. Der **Berechtigungs-Editor** wird angezeigt.



6. Wählen Sie im Dropdown-Menü **Benutzer oder Gruppe** einen Benutzer oder eine Gruppe aus und richten Sie **Anwenden auf** und **Berechtigung** gemäß den Einstellungen in der Tabelle unten ein. Die Abbildung unten ist ein Beispiel für die Einrichtung der Berechtigungen für die benutzerdefinierte Gruppe „Owner“.

Benutzer oder Gruppe	Anwenden auf	Berechtigung
Benutzerdefinierte Gruppe (z. B. „Owner“)	Setzen Sie Häkchen bei **Untergeordnete Ordner**, **Untergeordnete Dateien** und **Alle Ableitungen**.	Setzen Sie für volle Kontrolle Häkchen bei **Administration**, **Lesen** und **Schreiben**.
Domain Admins	Wählen Sie **Alle**.	Setzen Sie für volle Kontrolle Häkchen bei **Administration**, **Lesen** und **Schreiben**.
Domain Users	Wählen Sie **Alle**.	• Setzen Sie für volle Leserechte ein Häkchen bei **Lesen**. • Setzen Sie unter **Schreiben** nur ein Häkchen bei **Ordner erstellen/Daten anhängen**.



7. Klicken Sie auf **Fertig**, um die Einstellungen zu speichern.

8. Öffnen Sie **Synology Directory Server** > **Benutzer und Computer** > **Benutzer**.

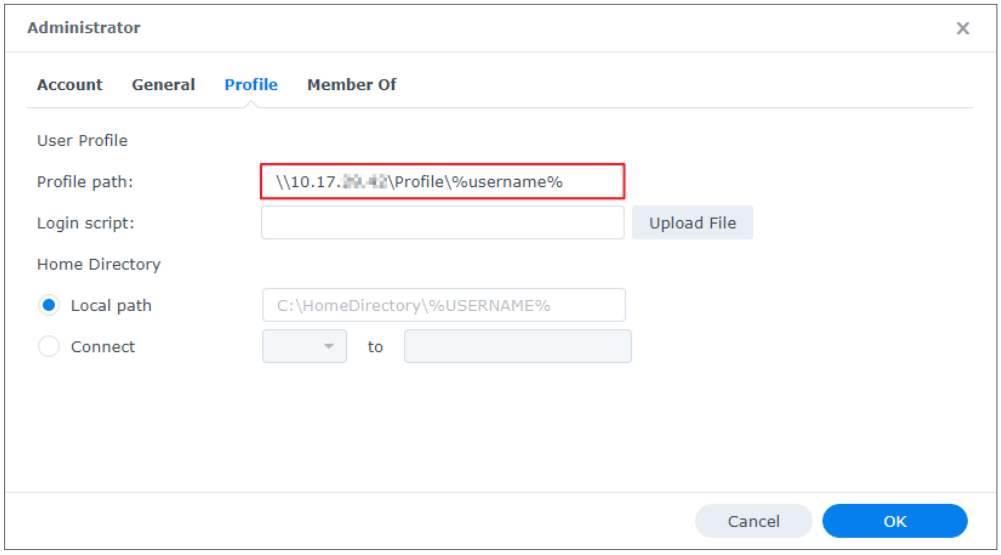
9. Führen Sie einen der folgenden Schritte durch:

   - Wählen Sie einen Benutzer aus und klicken Sie auf **Aktion** > **Eigenschaften**.
   - Rechtsklicken Sie auf einen Benutzer und wählen Sie **Eigenschaften**.

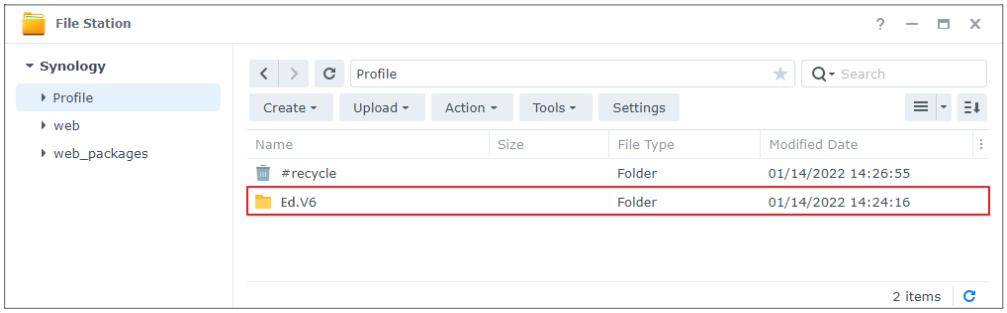
10. Geben Sie unter **Profil** in **Profil-Pfad** den Pfad eines freigegebenen Ordners für das servergespeicherte Profil des Benutzers im folgenden Format ein. Ändern Sie „%username%“ nicht, da diese Umgebungsvariable automatisch auf den Profilordner des angegebenen Benutzers verweist.

```
\\IP-Adresse des NAS\Name des freigegebenen Ordners\%username%
```

11. Klicken Sie auf **OK**, um die Einstellungen zu speichern.



12. Wenn der Benutzer sich mit dem angegebenen Domain-Benutzerkonto beim Windows-PC in der Domain anmeldet, erstellt dieser automatisch ein zugehöriges servergespeichertes Profil im freigegebenen Remote-Ordner auf dem Synology NAS (der Ordnername lautet „*benutzername*.V6“). Wenn der Benutzer sich vom PC abmeldet, werden die Daten zurück zum zugewiesenen Pfad synchronisiert, wenn Daten im Benutzerprofil geändert wurden.



Anmerkung:

- Sie können auch **mit RSAT allen Benutzern ein servergespeichertes Profil zuweisen**.
- Die Option **Lokaler Pfad** in der Registerkarte **Profil** bezeichnet den Pfad zu einem lokalen Windows-Ordner. Stellen Sie sicher, dass dieser Pfad auf dem von Ihnen zugewiesenen Computer bereits erstellt wurde. Andernfalls sind Ihre Einstellungen nicht gültig.

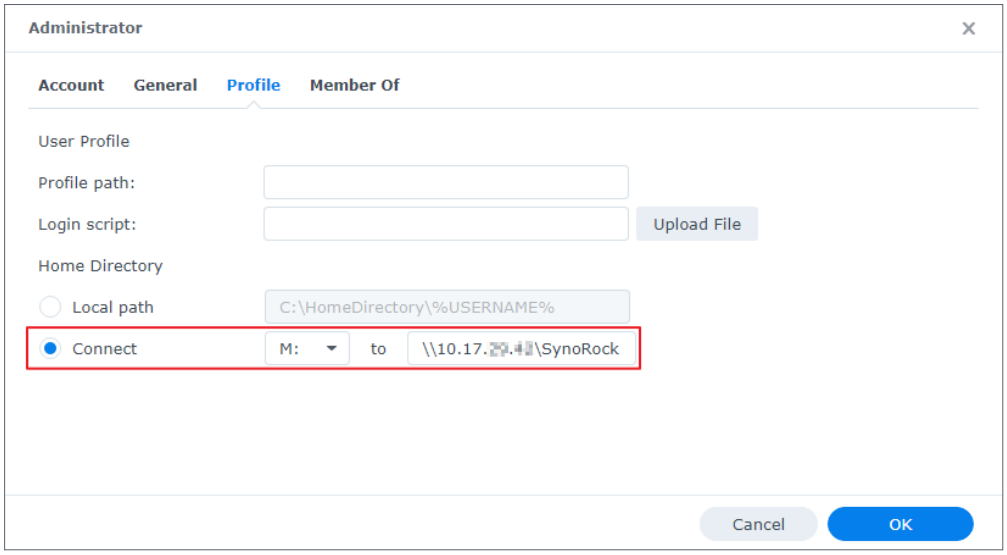
Ein Netzlaufwerk für einzelne Benutzer bereitstellen

1. **Mit dem Windows-PC eines Benutzers einer Domain beitreten**.

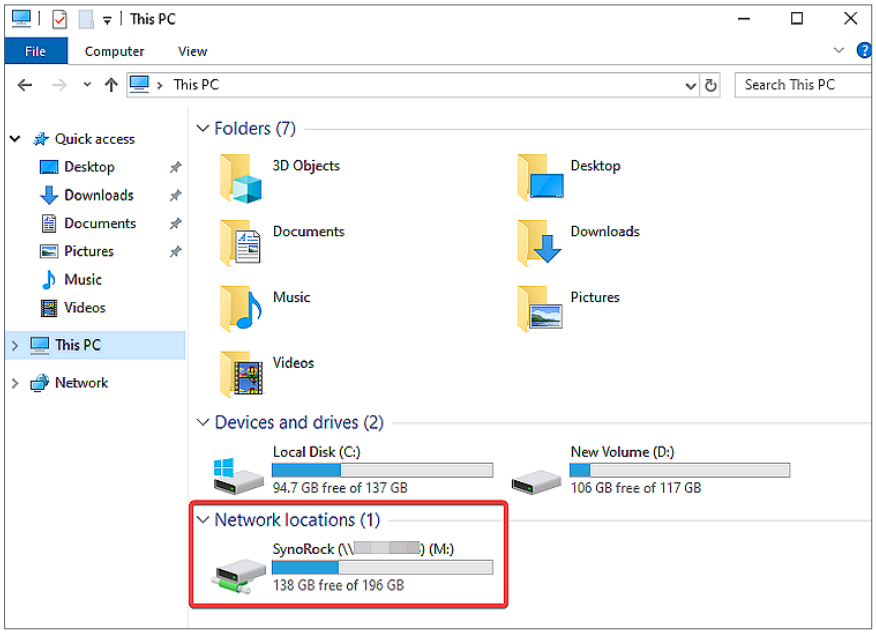
2. Öffnen Sie auf einem RWDC **Systemsteuerung** > **Freigegebener Ordner** > **Erstellen** > **Freigegebenen Ordner erstellen**, um einen freigegebenen Ordner zu erstellen (mindestens Leseberechtigungen erforderlich). Die freigegebenen Ordner für einen einzelnen Benutzer und für alle Benutzer sollten verschieden sein.
3. Befolgen Sie die Schritte 3 bis 9 unter **Servergespeichertes Profil für einen einzelnen Benutzer zuweisen**.
4. Öffnen Sie **Profil** > **Home-Verzeichnis** und wählen Sie **Verbinden mit**.
5. Weisen Sie dem Netzlaufwerk einen Laufwerkbuchstaben zu.
6. Geben Sie den Pfad des freigegebenen Ordners (oder eines Unterordners), den Sie als Netzlaufwerk bereitstellen wollen, im folgenden Format ein.

```
\\IP-Adresse des NAS\Name des (freigegebenen) Ordners
```

7. Klicken Sie auf **OK**, um die Einstellungen zu speichern.



8. Melden Sie sich mit diesem Benutzerkonto beim der Domain beigetretenen Windows-PC an. Der Benutzer sieht das bereitgestellte Laufwerk auf dem Computer.



Anmerkung:

- Wenn Domainbenutzer bereits vor der Bereitstellung eines Laufwerks beim betreffenden Windows-PC angemeldet sind, müssen sie sich erneut anmelden, um auf das bereitgestellte Laufwerk zuzugreifen.

Computer verwalten

Die **einer Domain beigetretenen Geräte** (z. B. Workstations, Server, Drucker und Synology NAS) werden als Computer bezeichnet und können für Benutzergruppen bereitgestellt werden.

Computereigenschaften bearbeiten

1. Öffnen Sie auf einem RWDC die Seite **Benutzer und Computer** und wählen Sie den gewünschten Computer aus.
2. Führen Sie einen der folgenden Schritte durch:
   - Doppelklicken Sie auf den Computer.
   - Klicken Sie auf **Aktion** > **Eigenschaften**.
   - Rechtsklicken Sie auf den Computer und wählen Sie **Eigenschaften**.
3. Unter **Allgemein** können Sie die **Beschreibung** des Computers bearbeiten.
4. Unter **Mitglied von** können Sie den Computer zu einer Gruppe hinzufügen oder aus einer Gruppe entfernen.
5. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Einen Computer löschen

1. Öffnen Sie auf einem RWDC die Seite **Benutzer und Computer** und wählen Sie den gewünschten Computer aus. Mit **Strg** bzw. **Umschalttaste** können Sie eine Mehrfachauswahl treffen.
2. Führen Sie einen der folgenden Schritte durch:
   - Klicken Sie auf **Aktion** > **Löschen**.
   - Rechtsklicken Sie auf den Computer und wählen Sie **Löschen**.
3. Klicken Sie auf **Löschen**, um die Aktion zu bestätigen. Das Löschen kann **nicht rückgängig gemacht werden**.

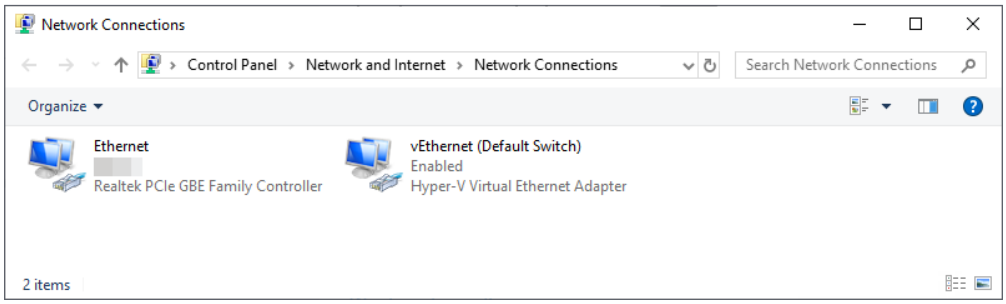
Kapitel 5: Geräte in eine Domain einbinden

Wenn Sie Geräte als Clients in eine Domain einbinden, können Sie die Ressourcen Ihrer Organisation auf effiziente Weise verwalten. Domainbenutzer können sich mit einem Domainkonto und Kennwort bei den Geräten anmelden und auf Ressourcen zugreifen.

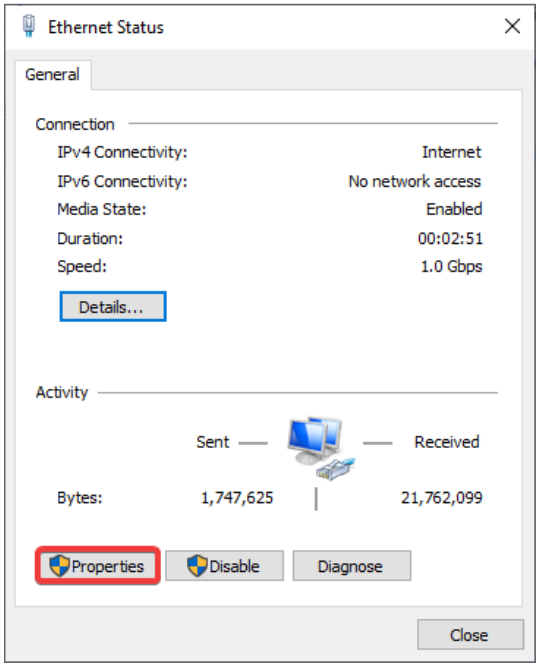
Mit Windows-PCs einer Domain beitreten

PCs mit Windows 7 und höher können einer von Synology Directory Server erstellten Domain beitreten. Hier verwenden wir als Beispiel einen PC mit Windows 10.

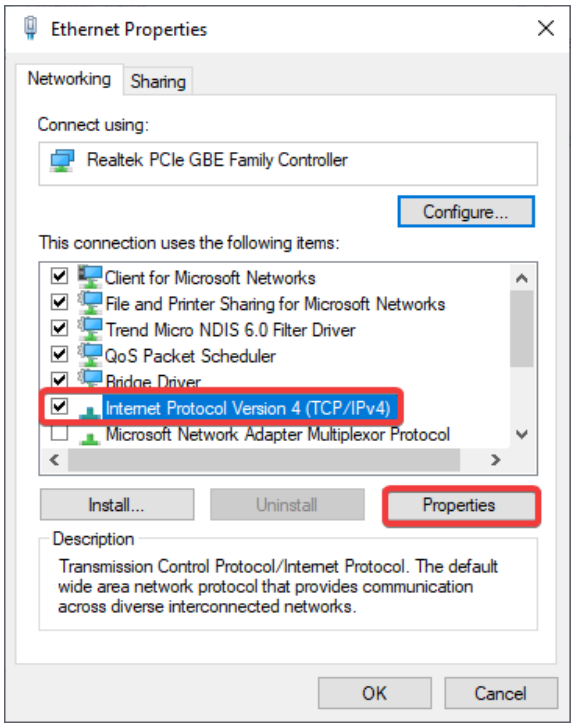
1. Gehen Sie in Windows zu **Start** > **Einstellungen** > **Netzwerk und Internet** > **Status** > **Adapteroptionen ändern** und klicken Sie auf die derzeit verwendete Netzwerkschnittstelle.



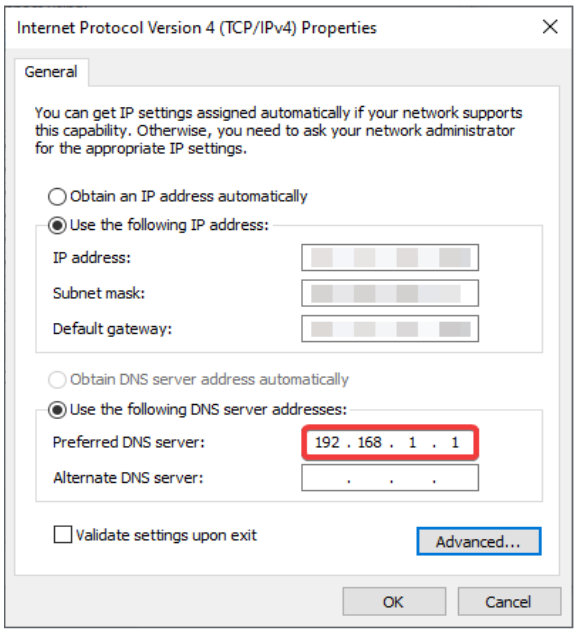
2. Klicken Sie auf der Seite **Status** auf **Eigenschaften**.



3. Wählen Sie in der Registerkarte **Netzwerk** die Option **Internetprotokoll, Version 4 (TCP/IPv4)** und klicken Sie auf **Eigenschaften**.

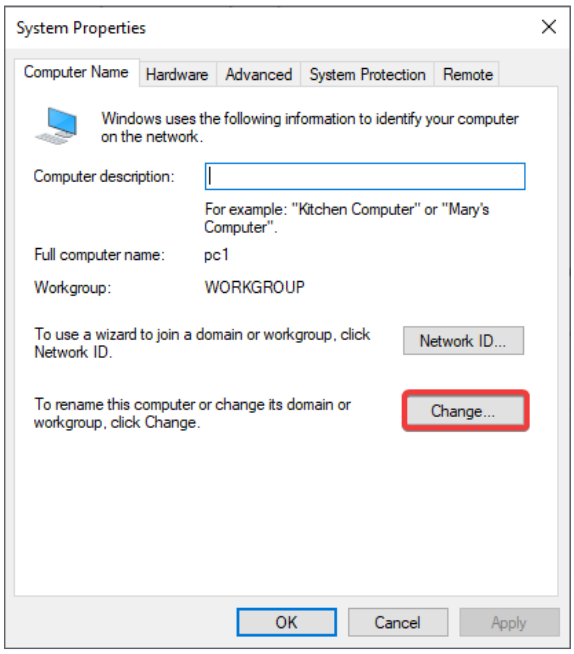


4. Setzen Sie ein Häkchen bei **Folgende DNS-Serveradressen verwenden**, geben Sie die IP-Adresse des DCs in das Feld **Bevorzugter DNS-Server** ein und klicken Sie auf **OK**, um die Einstellungen zu speichern.

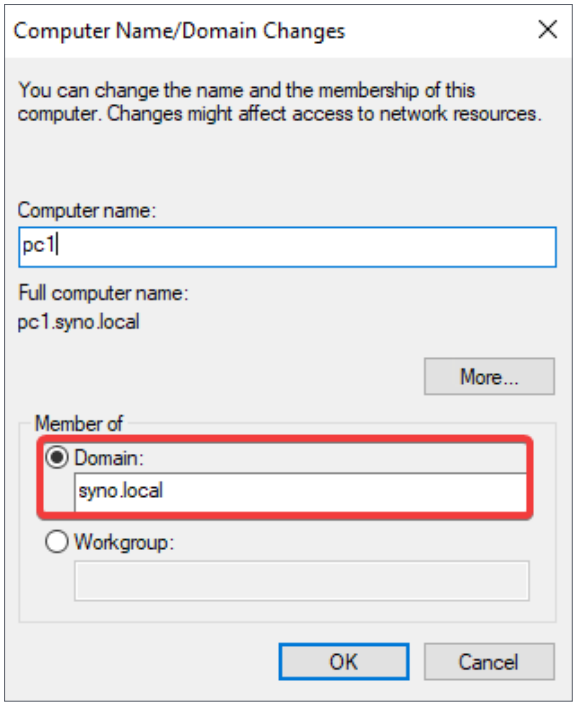


5. Gehen Sie in Windows zu **Start** > **Einstellungen** > **System** > **Info** > **System-Info** und klicken Sie auf **Einstellungen ändern**.

6. Klicken Sie auf der Registerkarte **Computername** auf **Ändern...**



7. Klicken Sie unter **Mitglied von** auf **Domain** und geben Sie den Namen der Domain ein, der Sie mit diesem Computer beitreten möchten. Klicken Sie nach Bestätigung der Einstellungen auf **OK**.



8. Geben Sie die Anmeldedaten des Domainadministrators im folgenden Format ein und klicken Sie auf **OK**.

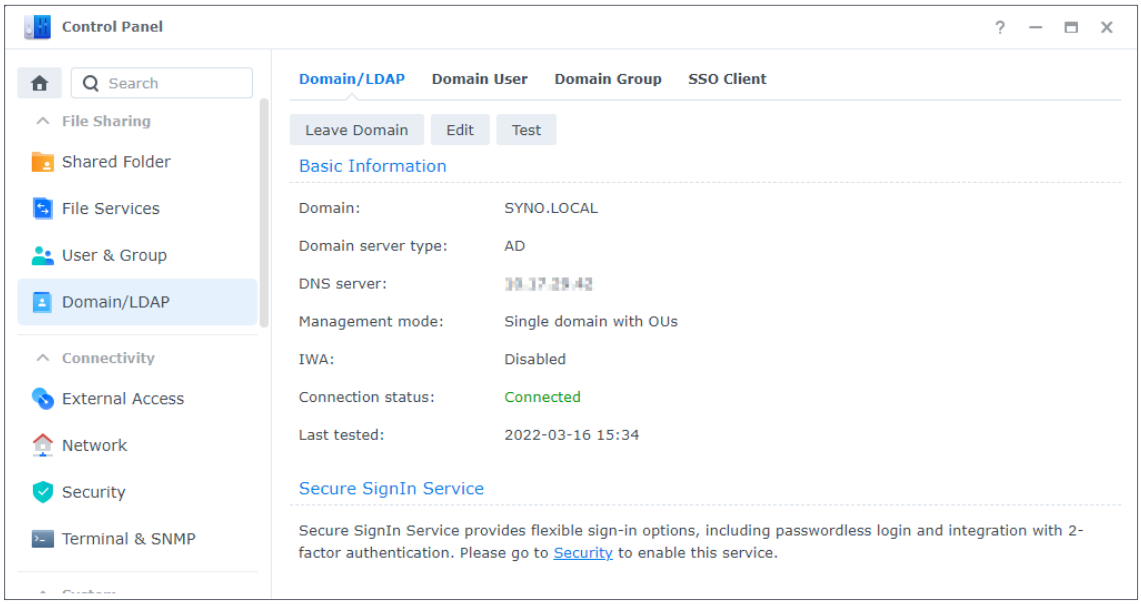
```
NetBIOS-Name der Domain\Benutzername des Administrators
```

9. Starten Sie den Computer neu, um den Beitritt zur Domain abzuschließen.

Mit dem Synology NAS einer Domain beitreten

Wenn ein Synology NAS als Domain-Client einer Domain beigetreten ist, können sich Benutzer mit ihren Domainkonten und Kennwörtern darauf anmelden. So können sie auf Dateien und DSM-Anwendungen zugreifen, ohne sich weitere Anmeldedaten merken zu müssen.

1. Öffnen Sie in DSM **Systemsteuerung** > **Domain/LDAP** > **Domain/LDAP** und klicken Sie auf **Beitreten**.
2. Geben Sie die Serverinformationen ein und klicken Sie auf **Weiter**.
3. Geben Sie die Domaininformationen ein und klicken Sie auf **Weiter**.
4. Der Assistent testet nun, ob die Vorbedingungen erfüllt wurden.
   - : Der Test wurde bestanden.
   - : Es ist mindestens ein kleineres Problem aufgetreten, das gelöst werden muss. Solche Probleme können zu Unregelmäßigkeiten bei Domaindiensten führen. Klicken Sie auf **Details** und beheben Sie die Probleme entsprechend den vorgeschlagenen Maßnahmen.
   - : Es ist mindestens ein kritisches Problem aufgetreten, das umgehend gelöst werden muss. Solche Probleme führen dazu, dass der Domainbeitritt fehlschlägt. Klicken Sie auf **Details** und beheben Sie die Probleme entsprechend den vorgeschlagenen Maßnahmen.
5. Nachdem die Überprüfung der Vorbedingungen ohne kritische Probleme abgeschlossen wurde, klicken Sie auf **OK**, um mit dem Synology NAS der Domain beizutreten.
6. Klicken Sie falls nötig auf **Bearbeiten**, um **allgemeine oder erweiterte Einstellungen zu konfigurieren**.



Anmerkung:

- Weitere Informationen zum Domainbeitritt finden Sie in diesem **Hilfe-Artikel**.

Kapitel 6: Gruppenrichtlinien konfigurieren

Sie können die Benutzer in einer Domain mit Gruppenrichtlinien verwalten. Mit Richtlinien können Einschränkungen bei gängigen Aktionen definiert, Dienste auf Geräten in der Domain bereitgestellt, Aktualisierungen verwaltet und eine einheitliche Arbeitsumgebung für Benutzer sichergestellt werden. Gut gepflegte Gruppenrichtlinien erleichtern die Domainadministration.

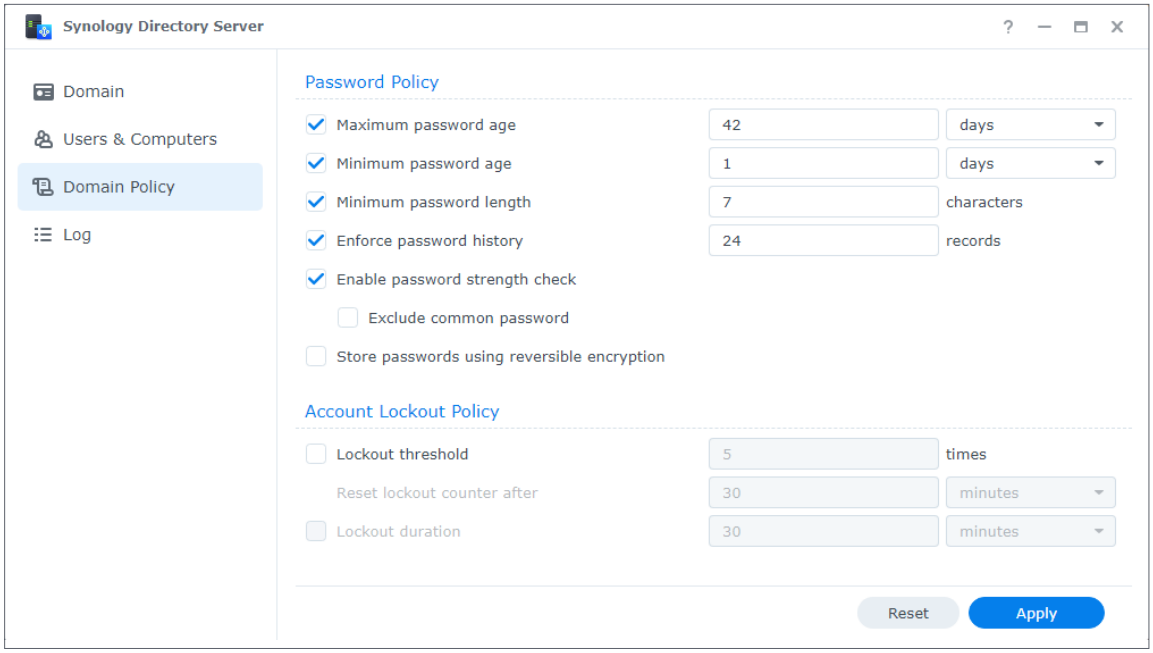
Hier erfahren Sie, wie Sie mit Synology Directory Server und Windows Remote Server Administration Tools (RSAT) Gruppenrichtlinien für Ihre Domain konfigurieren können.

Standard-Domainrichtlinien konfigurieren

Mit der Standard-Domainrichtlinie können Sie Konten auf Ebene der Domain schützen, indem Sie Richtlinien für Kennwort und Kontosperre einrichten. Auf der Seite **Domainrichtlinie** können Sie diese beiden Arten von Standard-Domainrichtlinien verwalten.

Anmerkung:

- Die auf dieser Seite aufgeführten Domainrichtlinien können auch über **Standard-Domainrichtlinie** in Windows RSAT konfiguriert werden.



Kennwortrichtlinie

- **Maximales Alter für Kennwort**: Legen Sie die Zeit fest, nach der Kennwörter ablaufen. Wenn diese Option deaktiviert wird, laufen Kennwörter niemals ab.
- **Mindestalter für Kennwort**: Geben Sie den Zeitraum an, in dem Benutzer nach der letzten Änderung ihr Kennwort nicht erneut ändern dürfen. Wenn diese Option deaktiviert wird, können Kennwörter jederzeit geändert werden.
- **Minimale Kennwortlänge**: Geben Sie die Mindestlänge neuer Kennwörter an.
- **Kennwortverlauf erzwingen**: Alle neuen Kennwörter müssen sich von den zuvor eingerichteten unterscheiden. Geben Sie hier die Anzahl der Einträge an.
- **Prüfung der Kennwortstärke aktivieren**: Kennwörter müssen **mindestens drei** der folgenden Regeln erfüllen:
  - Großbuchstaben (einschließlich A-Z mit diakritischen Zeichen) des lateinischen, griechischen und kyrillischen Alphabets.
  - Kleinbuchstaben (einschließlich a-z mit diakritischen Zeichen) des lateinischen, griechischen und kyrillischen Alphabets.
  - Ziffern (0-9).
  - Sonderzeichen wie #, $, !
  - Unicode-Alphabete, darunter jene in asiatischen Sprachen.
- **Schwache Kennwörter ausschließen**: Hindern Sie Benutzer daran, leicht zu erratende Kennwörter wie „123456“, „password“ und „qwerty“ einzurichten.
- **Kennwörter mittels reversibler Verschlüsselung speichern**: Das Aktivieren dieser Option gefährdet die Sicherheit der Domain. Diese Option wird nicht empfohlen, außer die Anforderungen von Domain-Client-Diensten haben höhere Priorität als die Kennwortsicherheit.

Kontosperre Richtlinie

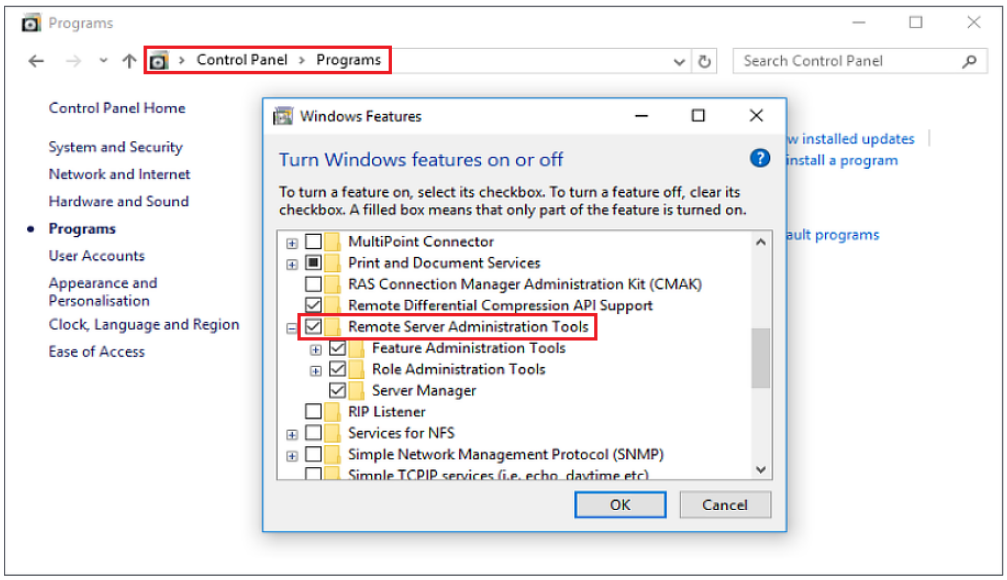
- **Sperre Grenzwert**: Benutzerkonten werden gesperrt, wenn die Anzahl der fehlgeschlagenen Anmeldeversuche über den festgelegten Sperrschwellwert hinausgeht.
- **Sperrzähler zurücksetzen nach**: Nach der angegebenen Zeit wird die Anzahl fehlgeschlagener Anmeldungen wieder zurückgesetzt.
- **Dauer Sperre**: Gesperrte Benutzerkonten werden erst am Ende der festgelegten Sperrdauer wieder freigegeben.

RSAT zur Verwaltung von Gruppenrichtlinien verwenden

Mit den Windows **Remoteserver-Verwaltungstools** (**RSAT**) können Sie auf einem **der Domain beigetretenen Windows-PC** Gruppenrichtlinien abseits von Kennwörtern und Kontosperre konfigurieren.

RSAT auf einem Windows-PC installieren

1. Laden Sie **Windows RSAT** aus dem Microsoft Download Center auf einen Windows-PC herunter. Je nach Windows-Version gibt es unterschiedliche RSAT-Installationsdateien.
2. Führen Sie die heruntergeladene Datei aus und folgenden Sie den Anweisungen des Assistenten, um die RSAT zu installieren.
3. Gehen Sie nach Abschluss der Installation zu Windows **Systemsteuerung** > **Programme** > **Turn Windows-Features aktivieren oder deaktivieren** und setzen Sie ein Häkchen bei **Remote Server Administration Tools**.



4. Stellen Sie sicher, dass Sie mit Ihrem PC der Domain beigetreten sind und sich als Domainadministrator angemeldet haben. Die RSAT finden Sie unter **Systemsteuerung** > **Verwaltung**.

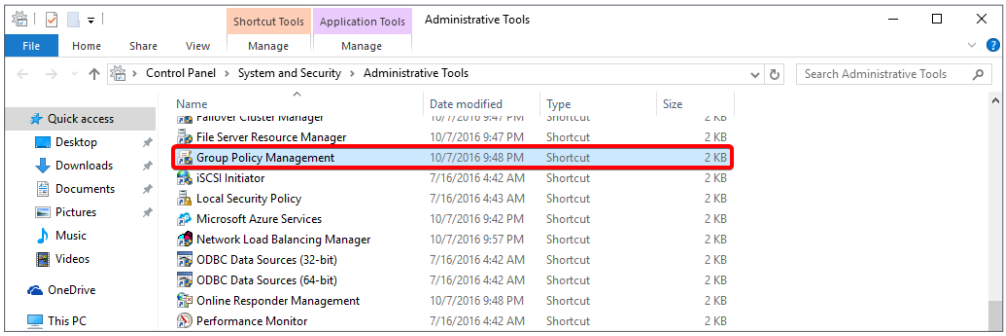
Anmerkung:

- Welche RSAT-Optionen konfigurierbar sind, ist abhängig von der Windows-Version des PCs, auf dem RSAT installiert ist. Beispielsweise können die verfügbaren Einstellungen der Windows 8 RSAT anders aussehen als jene der Windows 10 RSAT.

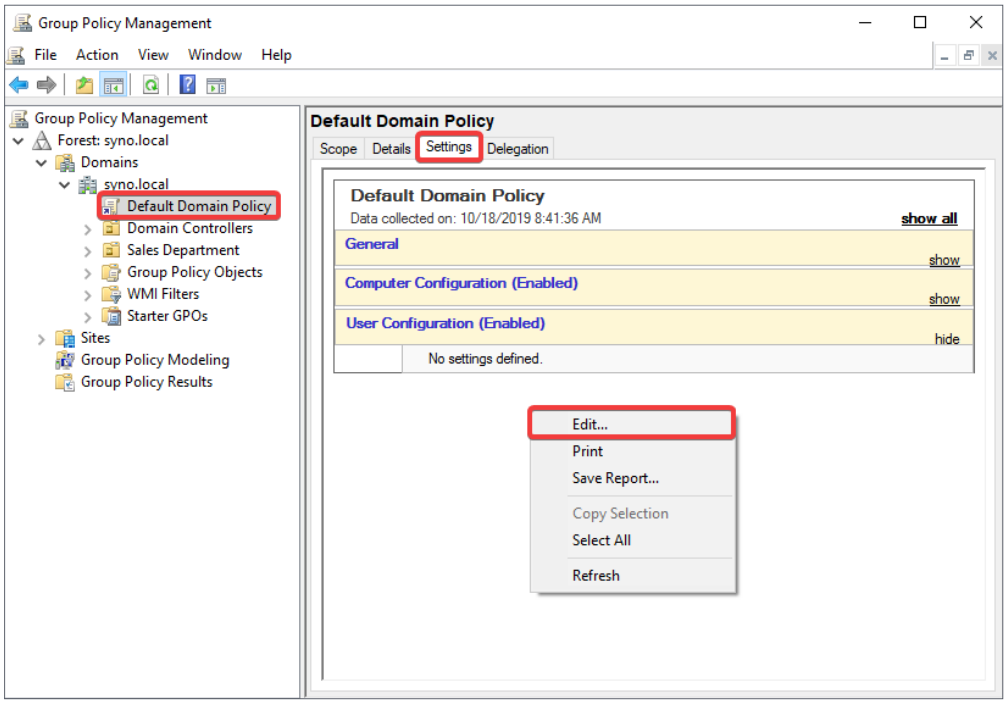
Servergespeichertes Profil für alle Benutzer zuweisen

Mit servergespeicherten Profilen können Domainbenutzer bei der Anmeldung bei verschiedenen Windows-PCs in der Domain auf ihre Dateien zugreifen.

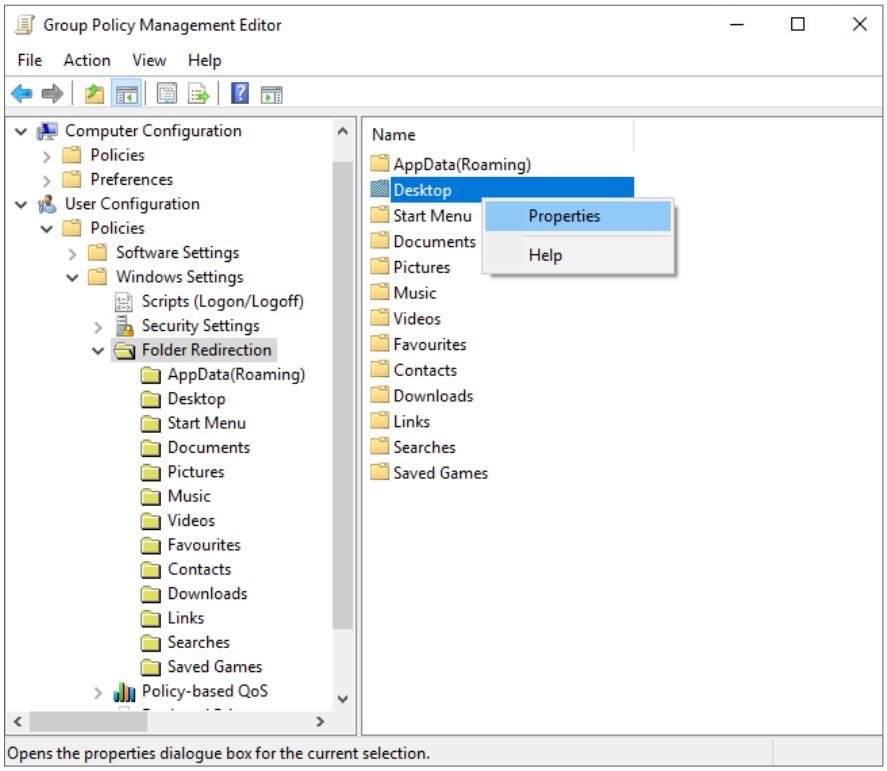
1. Stellen Sie sicher, dass Sie einen freigegebenen Ordner erstellt und allen Domainbenutzern auf dem als RWDC agierenden Synology NAS ausreichende Berechtigungen gegeben haben. Eine detaillierte Anleitung finden Sie in Schritt 1 bis 7 von **Servergespeichertes Profil für einen einzelnen Benutzer zuweisen**.
2. Melden Sie sich als Domainadministrator bei einem Windows-PC in der Domain an.
3. Gehen Sie zu Windows **Systemsteuerung** > **System und Sicherheit** > **Verwaltungstools** > **Gruppenrichtlinienverwaltung**.



4. Gehen Sie zu **Gesamtstruktur: *Domainname*** > **Domänen** > ***Domainname*** > **Standarddomänenrichtlinie**.
5. Öffnen Sie in der Registerkarte **Einstellungen** durch Rechtsklick das Kontextmenü und klicken Sie auf **Bearbeiten**.



6. Gehen Sie zu **Benutzerkonfiguration** > **Richtlinien** > **Windows-Einstellungen** > **Ordnerumleitung**.
7. Klicken Sie mit der rechten Maustaste auf die Ordner, die Sie umleiten möchten, und klicken Sie auf **Eigenschaften**.



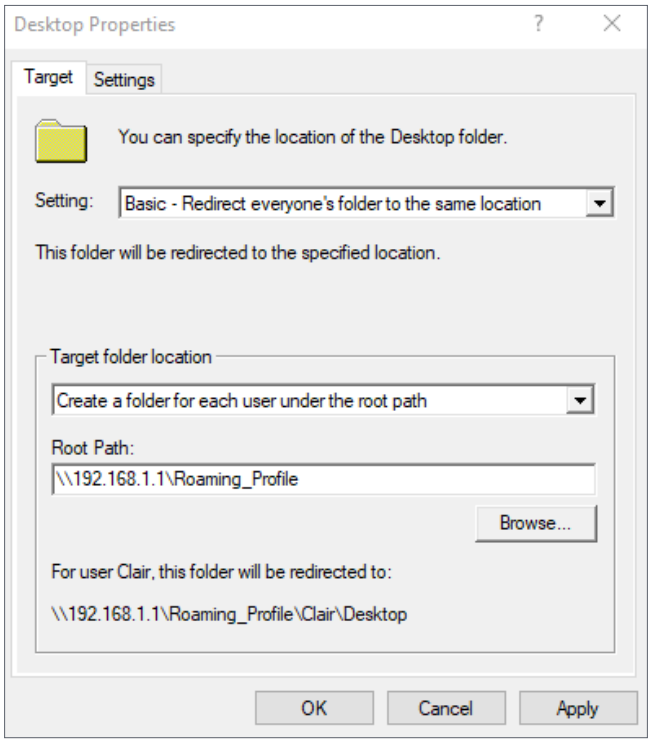
8. Konfigurieren Sie die Einstellungen wie folgt:

   a. Wechseln Sie zur Registerkarte **Ziel**.

   b. Wählen Sie **Standard (Leitet alle Ordner auf den gleichen Pfad um)**.

   c. Geben Sie die benötigten Informationen in **Zielordner** und **Stammpfad** ein.

   d. Klicken Sie auf **OK**.



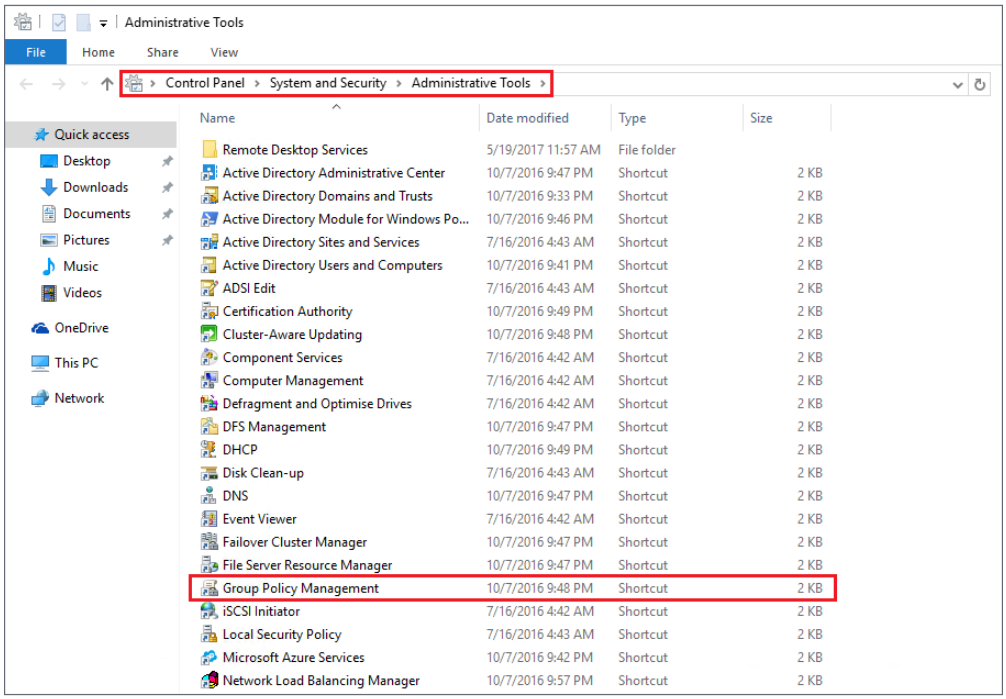
9. Die servergespeicherten Profile von Domainbenutzern werden auf den von Ihnen zugewiesenen Pfad umgeleitet.

Netzlaufwerk für alle Benutzer bereitstellen

1. Stellen Sie sicher, dass Sie einen freigegebenen Ordner erstellt und allen Domainbenutzern auf dem als RWDC agierenden Synology NAS ausreichende Berechtigungen (mindestens Leseberechtigung) gegeben haben. Eine detaillierte Anleitung finden Sie in Schritt 1 bis 7 von **Servergespeichertes Profil für einen einzelnen Benutzer zuweisen**.

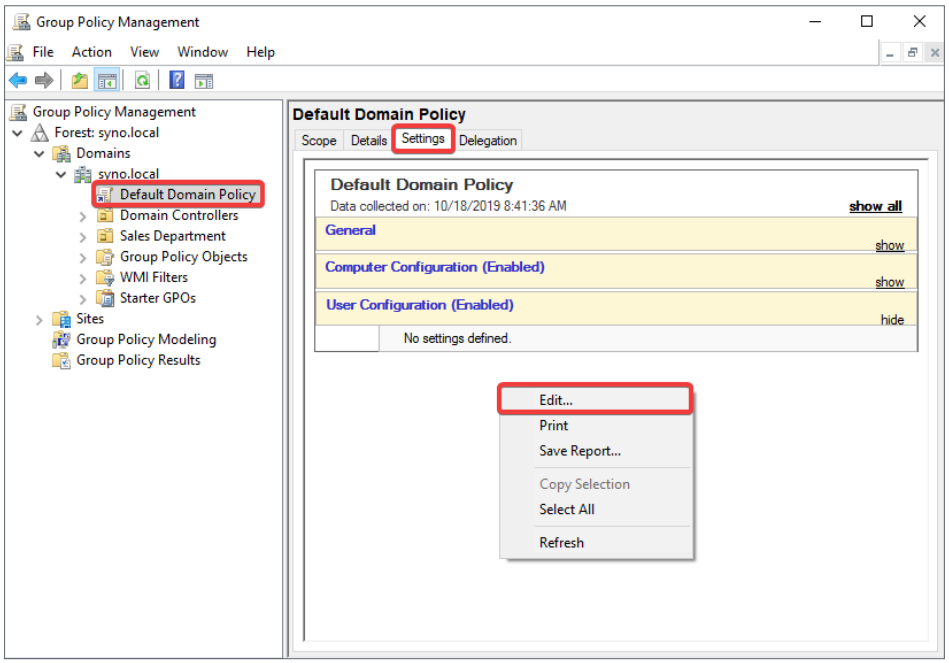
2. Melden Sie sich als Domainadministrator bei einem Windows-PC in der Domain an.

3. Gehen Sie zu Windows **Systemsteuerung** > **System und Sicherheit** > **Verwaltungstools** > **Gruppenrichtlinienverwaltung**.

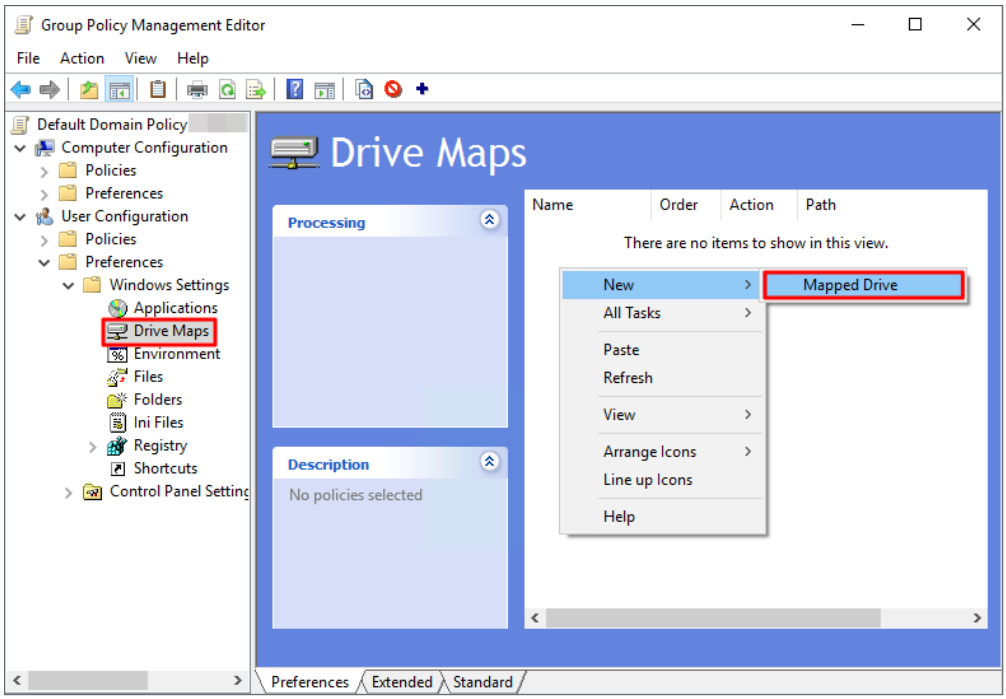


4. Gehen Sie zu **Gesamtstruktur: *Domainname*** > **Domänen** > ***Domainname*** > **Standarddomänenrichtlinie**.

5. Öffnen Sie in der Registerkarte **Einstellungen** durch Rechtsklick das Kontextmenü und klicken Sie auf **Bearbeiten**.

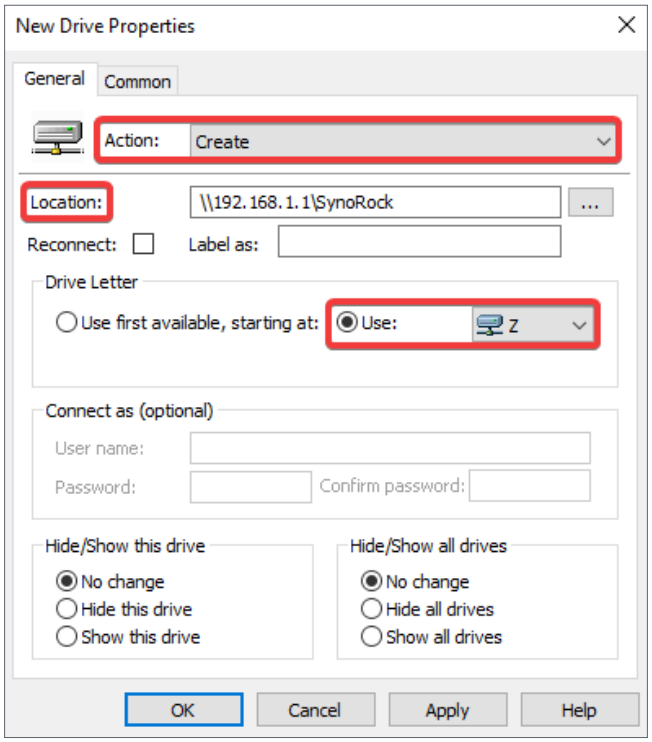


6. Gehen Sie in der Konsolenstruktur zu **Benutzerkonfiguration** > **Voreinstellungen** > **Windows-Einstellungen** > **Laufwerkzuordnungen**. Klicken Sie mit der rechten Maustaste in den rechten Bereich und auf **Neu** > **Zugeordnetes Laufwerk**.



7. Konfigurieren Sie die folgenden Einstellungen und klicken Sie auf **OK**:

   - **Aktion**: Wählen Sie im Dropdown-Menü **Erstellen** aus.
   - **Speicherort**: Geben Sie den Speicherort des Netzlaufwerks ein, etwa „\\192.168.1.1\SynoRock“.
   - **Laufwerkbuchstabe**: Klicken Sie hier auf **Verwenden** und wählen Sie einen Laufwerkbuchstaben.



8. Nach Abschluss der Konfiguration sehen Benutzer das bereitgestellte Netzlaufwerk auf diesem Computer, wenn sie sich mit einem beliebigen Domainbenutzerkonto anmelden.

Anmerkung:

- Es ist nicht nötig, unter **Verbinden als (optional)** einen **Benutzernamen** und ein **Kennwort** einzugeben, da Windows nach Abschluss der Einstellungen das Netzlaufwerk für das Benutzerkonto bereitstellt. Wenn ein Domainbenutzer sich anmeldet, stellt Windows das Netzlaufwerk automatisch für dessen Konto bereit.
- Damit die Netzlaufwerke korrekt funktionieren, stellen Sie sicher, dass deren Speicherort vorhanden ist und Benutzer Zugriffsberechtigungen haben.

Kapitel 7: Verzeichnisdienst warten und wiederherstellen

Bei der Nutzung von Synology Directory Server ist es äußerst wichtig, dafür zu sorgen, dass der Verzeichnisdienst zuverlässig gewartet und gesichert wird. Regelmäßige Wartung und Sicherung schützen Ihre Daten vor Systemausfällen oder versehentlichem Löschen. Hier erfahren Sie, wie Sie mit Synology High Availability einen Hochverfügbarkeitscluster einrichten und mit Hyper Backup Ihren Verzeichnisdienst sichern.

Unterbrechungsfreien Verzeichnisdienst mit Synology High Availability sicherstellen

Mit **Synology High Availability** können Sie Ihre Verzeichnisdatenbank sichern und den unterbrechungsfreien Betrieb von Synology Directory Server sicherstellen.

Synology High Availability verwendet zwei Server, um einen „Hochverfügbarkeitscluster" zu bilden, in dem ein Server die Funktion des „aktiven Servers" übernimmt und der andere als „passiver Ersatz-Server" fungiert. Damit werden Ausfälle aufgrund von Serverdefekten minimiert. Weitere Informationen zu den Elementen und Konzepten von Hochverfügbarkeitsclustern finden Sie in der **Anleitung zu Synology High Availability**.

Systemanforderungen

Synology High Availability benötigt zwei identische Synology NAS mit derselben Systemkonfiguration, um einen Cluster einzurichten. Bevor Sie beginnen, sollten Sie die **Einschränkungen und Systemanforderungen** und die **technischen Spezifikationen** von Synology High Availability kennen und besonders auf folgende Informationen achten.

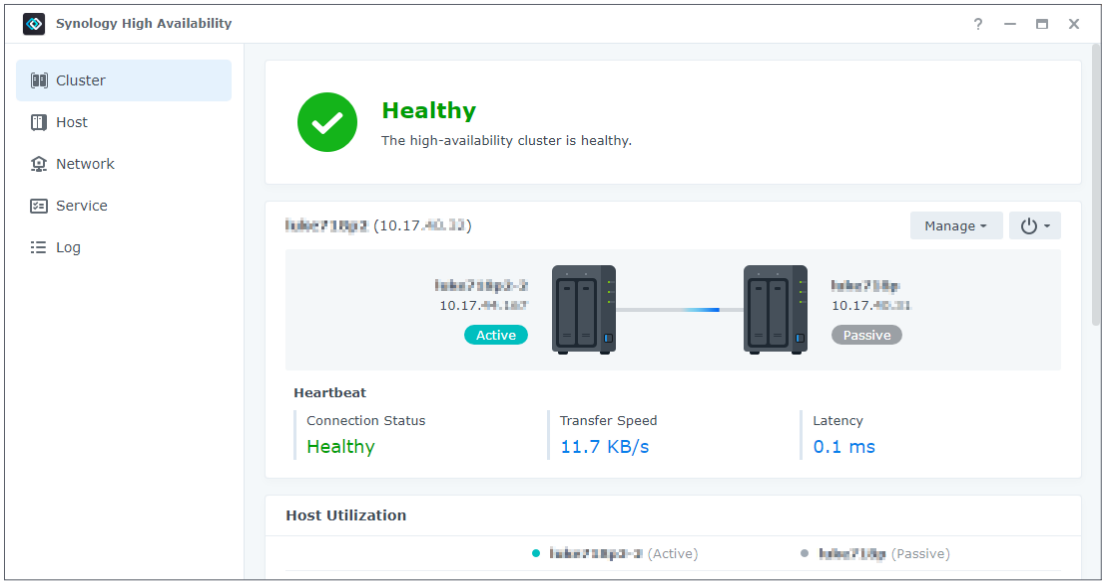
- **Kompatible Modelle**: Aktiver und passiver Server sollten dasselbe Modell sein.
- **DSM- & Paketversion**: Auf dem aktiven und passiven Server muss dieselbe Version von DSM und Synology High Availability installiert sein.
  - **Synology Directory Server** muss mindestens Version 4.10.18-0363 sein.
  - **Synology High Availability** muss mindestens Version 2.1.1-1279 sein.
- **Identische Speicher- und Netzwerkeinstellungen**:
  - Die Anzahl der Laufwerksschächte und Anzahl und Kapazität der installierten Laufwerke müssen bei aktivem und passivem Server identisch sein.
  - Die Gesamtzahl an Netzwerkschnittstellen und die Netzwerkeinstellungen müssen auf aktivem und passivem Server identisch sein.

- Stellen Sie sicher, dass beide Server mindestens eine statische IP-Adresse im selben Subnetz haben.
- Stellen Sie sicher, dass eine Heartbeat-Verbindung für die interne Kommunikation zwischen den beiden Servern eingerichtet ist.

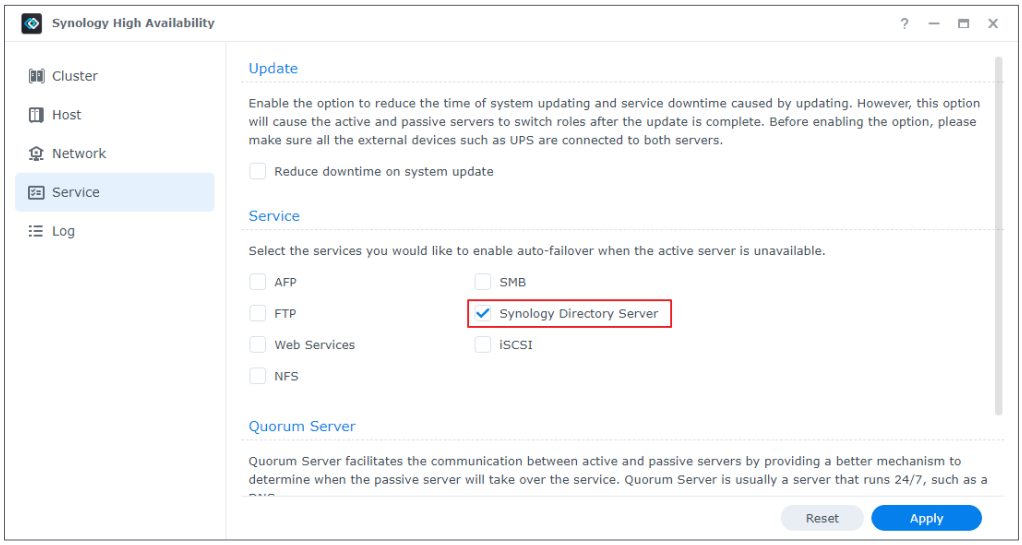
Einen Hochverfügbarkeitscluster einrichten

Um die einwandfreie Funktionalität von Synology Directory Server sicherzustellen, richten Sie den Synology High Availability-Cluster ein, **bevor** Sie den Synology-Verzeichnisdienst aktivieren.

1. Öffnen Sie das **Paketzentrum** und installieren Sie **Synology High Availability**.
2. Starten Sie **Synology High Availability**.
3. Klicken Sie auf **Hochverfügbarkeitscluster erstellen** und folgen Sie den Anweisungen des Assistenten (weitere Informationen finden Sie in den **Hilfe-Artikeln**).



4. **Installieren Sie Synology Directory Server** und richten Sie eine Domain ein.
5. Gehen Sie zu **Synology High Availability** > **Dienste**.
6. Setzen Sie ein Häkchen bei **Synology Directory Server** und klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.



Verzeichnisdienst mit Hyper Backup sichern und wiederherstellen

Hyper Backup bietet folgende Funktionen, mit denen Sie Daten und Einstellungen von Synology Directory Server sichern und wiederherstellen können.

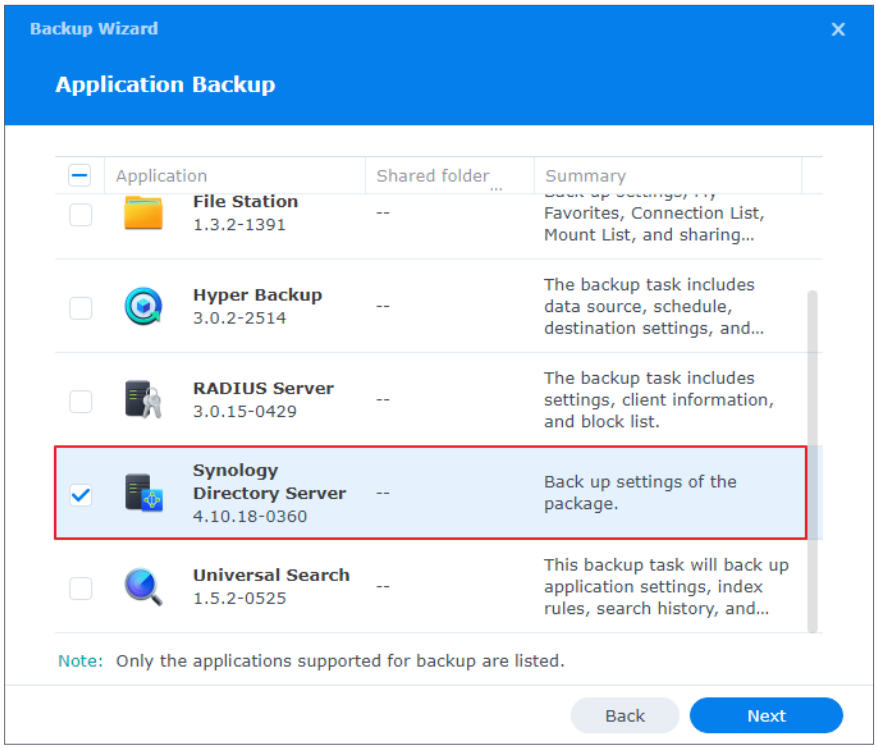
- Bis zu 65.535 Versionen von Daten behalten, wobei der benötigte Speicherplatz durch versionsübergreifende Deduplizierung minimiert wird.
- Gesicherte Daten in einer eigenen Datenbank speichern, die mit einem Versions-Explorer in DSM, Windows und Linux einfach durchsucht, heruntergeladen oder wiederhergestellt werden kann.
- Verschiedene Arten von Daten (z. B. Systemkonfigurationen, freigegebene Ordner, Anwendungen und Pakete) manuell oder automatisch sichern.
- Sicherungsaufgaben in lokalen freigegebenen Ordnern, auf Remote-Servern oder in der Cloud speichern.
- Mehrere Sicherungsversionen für jede Aufgabe behalten. Die automatische Sicherungsrotation ist optional und hat drei Modi: Löschen von der ältesten Sicherungsversion weg, **Smart Recycle** und benutzerdefinierte Richtlinien.

Weitere Informationen finden Sie in den **technischen Spezifikationen** von Hyper Backup.

Erstellen einer Sicherungsaufgabe

Mit Hyper Backup können Sie Datensicherungsaufgaben erstellen, verwalten und überwachen.

1. Öffnen Sie das **Paketzentrum** und installieren Sie **Hyper Backup**.
2. Starten Sie **Hyper Backup**.
3. Klicken Sie oben links auf + und wählen Sie **Datensicherungsaufgabe** aus, um den Sicherungsassistenten zu starten.
4. Wählen Sie den gewünschten Datensicherungszieltyp aus. Wir empfehlen, Ihre Daten auf einem anderen Gerät oder in der Cloud zu sichern.
5. Wählen Sie **Sicherungsaufgabe erstellen**.
6. Wählen Sie die zu sichernden Ordner aus und klicken Sie auf **Weiter**.
7. Setzen Sie ein Häkchen bei **Synology Directory Server** und klicken Sie auf **Weiter**.



8. Folgen Sie dem Assistenten, um die Sicherungsaufgabe fertig zu erstellen.

Eine Datensicherung wiederherstellen

Mit Hyper Backup können Sie Ihr Verzeichnis wiederherstellen, wenn Fehler bei Synology Directory Server aufgetreten sind. Außerdem können Sie den Synology-Verzeichnisdienst über die Dienstwiederherstellung in Hyper Backup zu einem anderen Synology NAS migrieren.

1. Starten Sie **Hyper Backup**.
2. Klicken Sie oben links auf und wählen Sie **Daten**, um den Wiederherstellungsassistenten zu starten.
3. Wählen Sie eine wiederherzustellende Datensicherungsaufgabe aus.
4. Sie werden aufgefordert, Systemkonfigurationen, verschiedene Versionen von gesicherten Daten oder andere Optionen auszuwählen. Dies ist davon abhängig, welche Art von Datensicherungsaufgabe Sie wiederherstellen möchten.
5. Wenn die Sicherungsaufgabe verschlüsselt ist, benötigen Sie für die Wiederherstellung das Kennwort bzw. den Verschlüsselungsschlüssel.
6. Folgen Sie dem Assistenten, um die Wiederherstellung durchzuführen.

Anmerkung:

- Weitere Informationen finden Sie in den **Hilfe-Artikeln zu Hyper Backup**.

SYNOLOGY INC.

9F., No.1, Yuandong Rd., Banqiao Dist.,
New Taipei City 220545, Taiwan
Tel.: +886 2 2955 1814

SYNOLOGY AMERICA CORP.

3535 Factoria Blvd SE, Suite #200,
Bellevue, WA 98006, USA
Tel.: +1 425 818 1587

SYNOLOGY UK LTD.

Unit 5 Danbury Court, Linford Wood,
Milton Keynes, MK14 6PL, United Kingdom
Tel.: +44 (0)1908048029

Synology France

102 Terrasse Boieldieu (TOUR W)
92800 Puteaux France
Tel.: +33 147 176288

SYNOLOGY GMBH

Grafenberger Allee
29540237 Düsseldorf
Deutschland
Tel.: +49 211 9666 9666

SYNOLOGY SHANGHAI

200070, Room 201, No.
511 Tianmu W. Rd.,
Jingan Dist., Shanghai,
China

SYNOLOGY JAPAN CO., LTD.

4F, 3-1-2, Higashikanda, Chiyoda-ku, Tokio, 101-0031, Japan

Synology®

synology.com

Synology kann ohne vorherige Ankündigung jederzeit Änderungen an den technischen Daten und Produktbeschreibungen vornehmen. Copyright © 2022 Synology Inc. Alle Rechte vorbehalten. Synology und Namen anderer Synology-Produkte sind geschützte Marken oder eingetragene Warenzeichen von Synology Inc. Weitere hier genannte Produkte und Firmennamen sind Warenzeichen der entsprechenden Eigentümer.