EINLEITUNG:

In dieser Anleitung bauen wir einen Domänencontroller (DC) mit einigen grundlegenden Elementen auf und fügen ein Windows-10-Computer der Domäne hinzu.

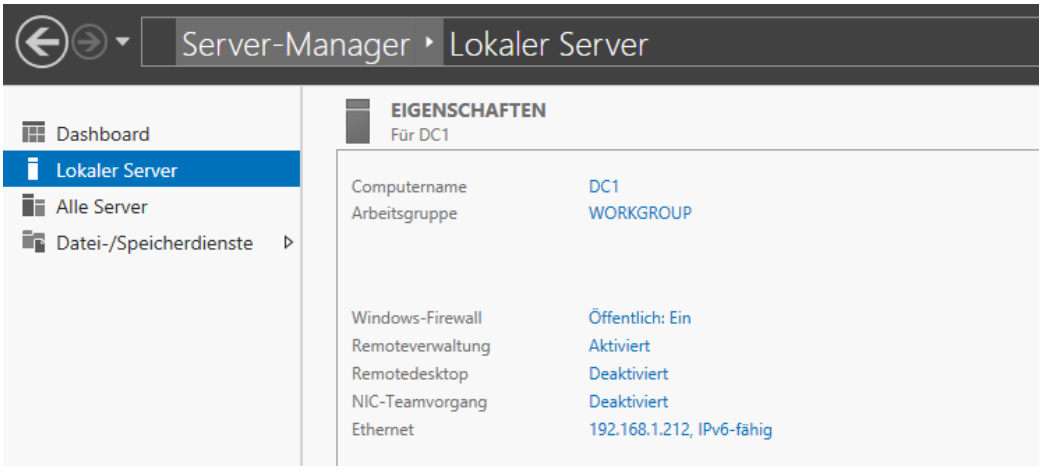
Der Vorgang in der Übersicht:

- Installieren der AD Domänendienste
- Konfigurieren des Windows-Servers als erster DC der neuen Gesamtstruktur victim.local
- Erstellen einer Organisationseinheit (OU) Berlin
- Erstellen von zwei Benutzern Asterix und Obelix
- Verschieben der Benutzer Asterix und Obelix in die OU Berlin
- Hinzufügen des Benutzers Asterix zur Gruppe der Domänen-Admins
- Hinzufügen des Computers Win10 zur Domäne
- Anmelden von Obelix an Win10 und prüfen der Gruppenzugehörigkeiten
- Anmelden von Asterix an Win10 und prüfen der Gruppenzugehörigkeiten
- Anmelden des lokalen Benutzers Bob an Win10 im lokalen Kontext

Dieses Tutorial dient als praktische Anleitung zum Aufbau einer AD-Laborumgebung und als Einführung in die Thematik. Es werden nur ausgewählte Aspekte angesprochen, die erfahrungsgemäß für die ersten Schritte relevant und für das Grundverständnis essentiell sind.

INSTALLIEREN DER AD DOMÄNENDIENSTE

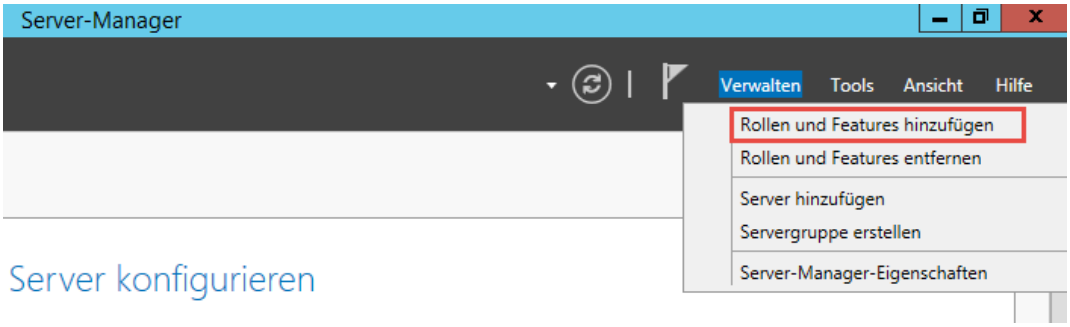
Als erstes ist die Installation der Rolle "AD-Domänendienste" erforderlich. Stelle hierzu zunächst sicher, dass der Server sowohl einen definierten Hostnamen als auch eine feste IP-Adresse zugewiesen bekommen hat. Dies kannst du über den Navigationspunkt **LOKALER SERVER** im **SERVERMANAGER** tun:



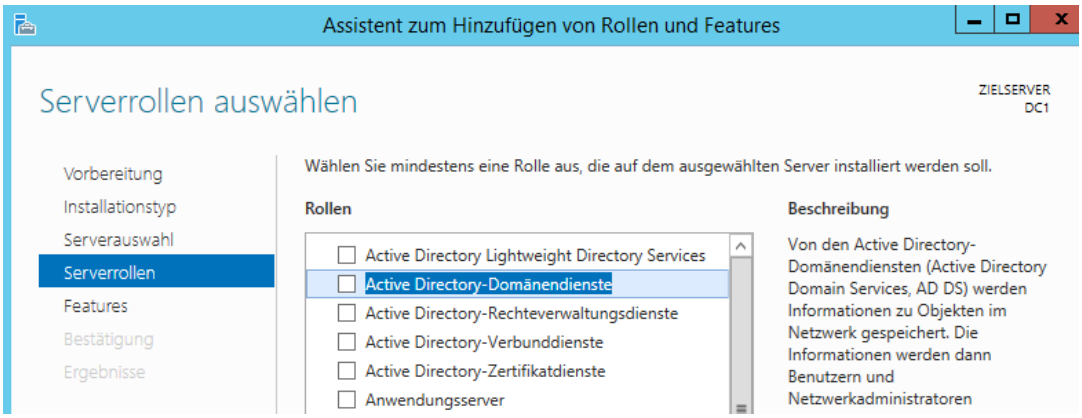
Der Server sollte zu diesem Zeitpunkt in der IP-Konfiguration keine DNS-Server eingetragen haben, da er im Verlauf dieses Prozesses selbst zum DNS-Server wird.

Beachte auch die IPv6-Konfiguration. Solltest du IPv6 nicht nutzen wollen, kannst du es auch deaktivieren. Ansonsten könnte es u. U. an er einen oder anderen Stelle zu zeitlich verzögerten Reaktionen kommen.

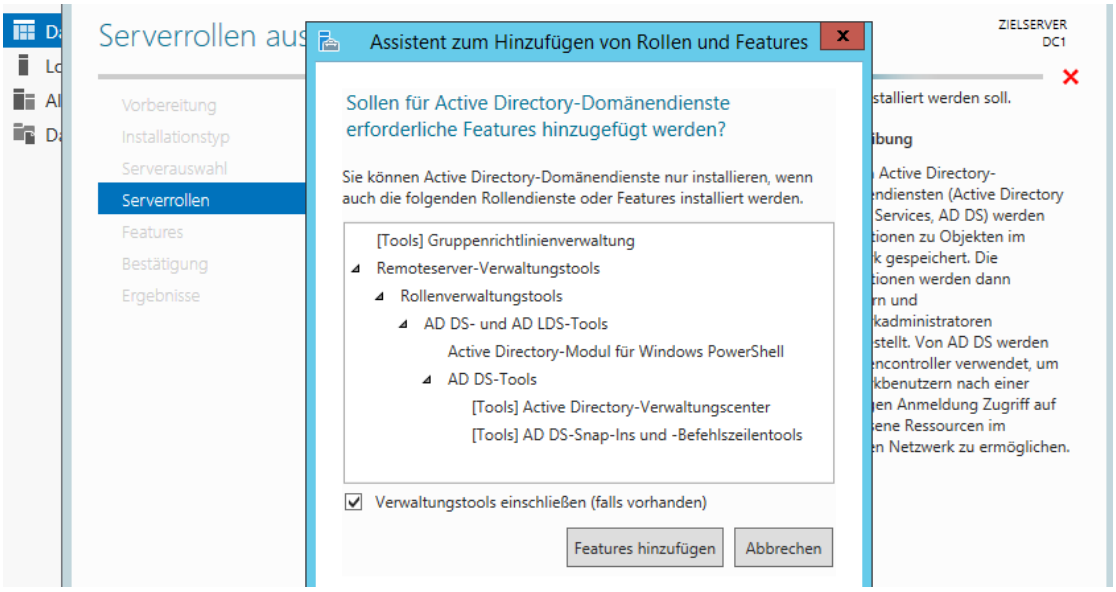
Zur Installation der AD-Domänendienste nutzen wir ebenfalls den Servermanager. Klicke im Menü rechts oben auf **VERWALTEN** und dann auf **ROLLEN UND FEATURES** hinzufügen.



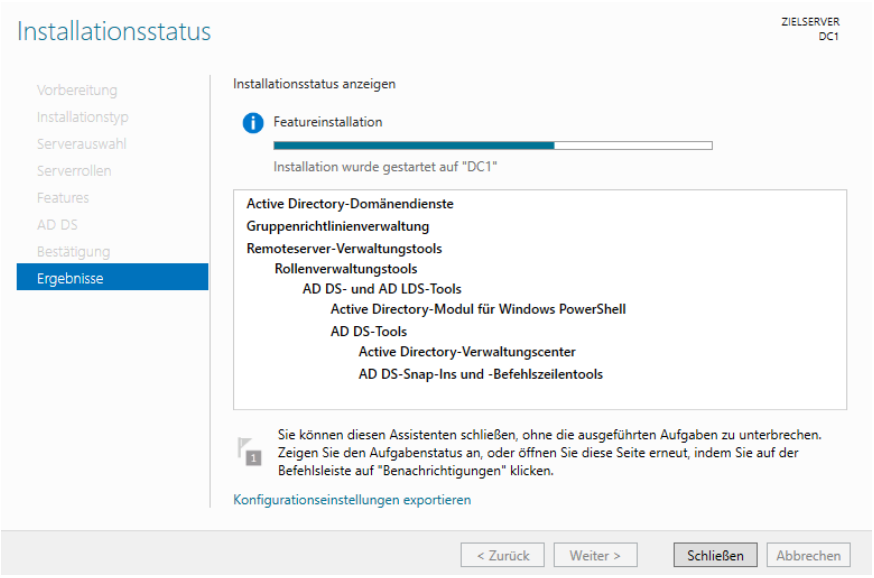
Übernimm die Voreinstellungen in den folgenden Dialogfenstern und wähle die Serverrolle **ACTIVE DIRECTORY-DOMÄNENDIENSTE** aus.



Die erforderlichen Abhängigkeiten werden automatisch aufgelöst. Klicke auf **FEATURES HINZUFÜGEN**.



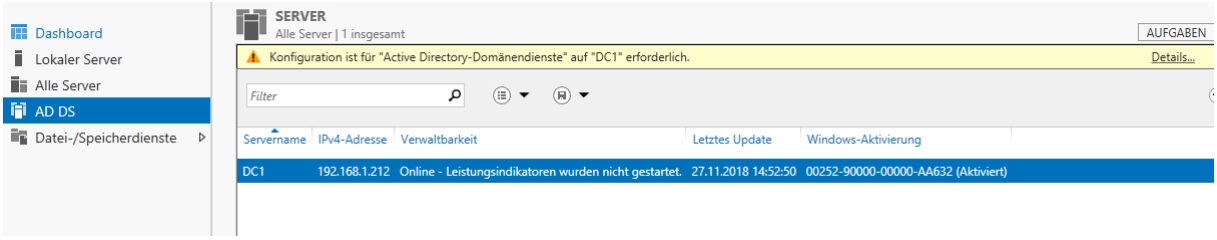
Klicke auf **WEITER** und übernimm alle Voreinstellungen. Schließlich kannst du durch Klick auf **INSTALLIEREN** den Prozess starten.



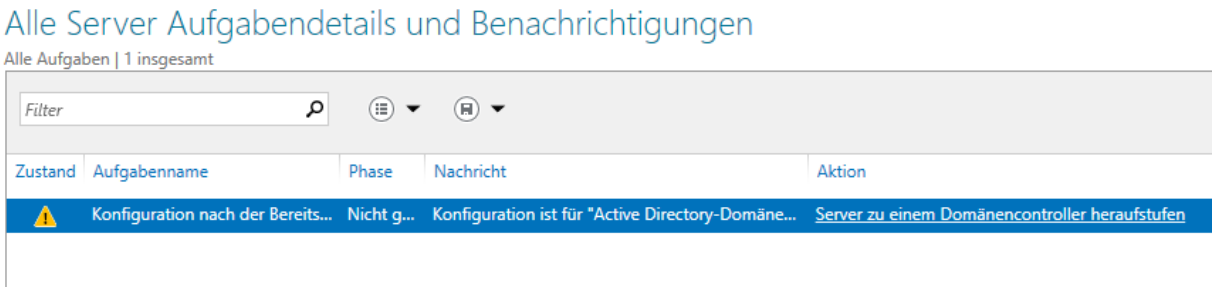
Damit ist die Rolle des Servers vorbereitet, aber dieser noch nicht dafür konfiguriert. Dies folgt nun im Anschluss.

Konfiguration des Windows-Servers als erster DC der neuen Gesamtstruktur victim.local

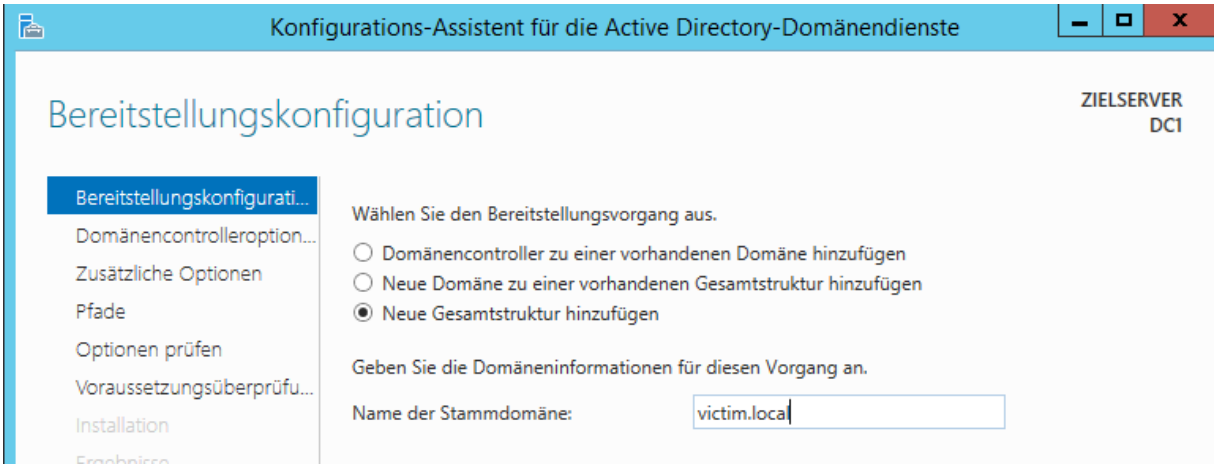
Nach Abschluss der Installation erscheint ein neuer Menüpunkt im Server-Manager namens AD DS. Klickst du darauf, zeigt dir der Server-Manager in einer Hinweis-Meldung oben, dass eine Konfiguration erforderlich ist:



Klicke auf der rechten Seite auf **DETAILS** und wähle als Aktion "**Server zu einem Domänencontroller heraufstufen**".

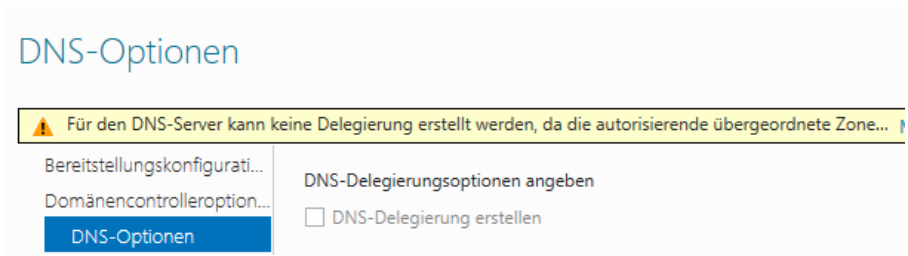


Es startet der Konfigurations-Assistent für die Active Directory-Domänendienste. Wähle "**Neue Gesamtstruktur hinzufügen**" und gib den gewünschten Namen für die AD-Domäne ein. Diese wird als Stammdomäne bezeichnet, da es sich um die erste Domäne in der Gesamtstruktur handelt, die aus diversen Domänen bestehen kann (aber nicht muss):

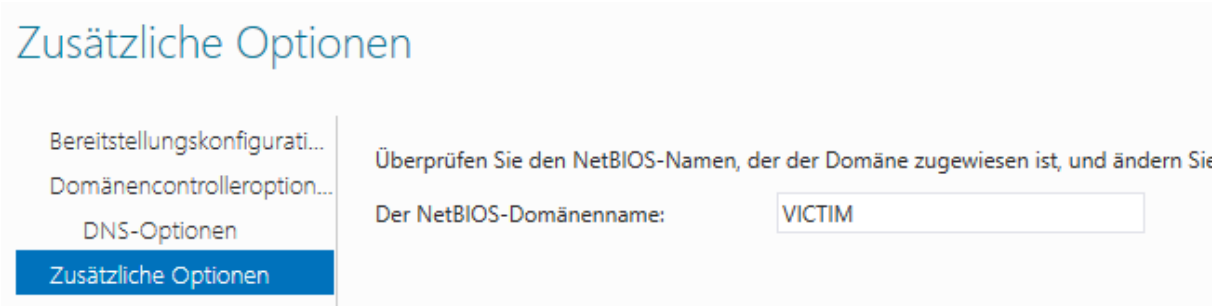


Im nächsten Dialogfenster übernimmst du das voreingestellte Häkchen vor DNS-Server, um den Serverdienst gleich mit zu installieren. Er wird für den Betrieb von AD benötigt. Das festzulegende Kennwort wird nur für Wiederherstellungsvorgänge benötigt und ist nicht für den regulären Betrieb erforderlich. Beachte die Komplexitätsanforderungen an das Passwort bei der Eingabe. Da es sich um eine Laborumgebung handelt, kannst du z.B. für alle Eingaben `Pa$$w0rd` nutzen.

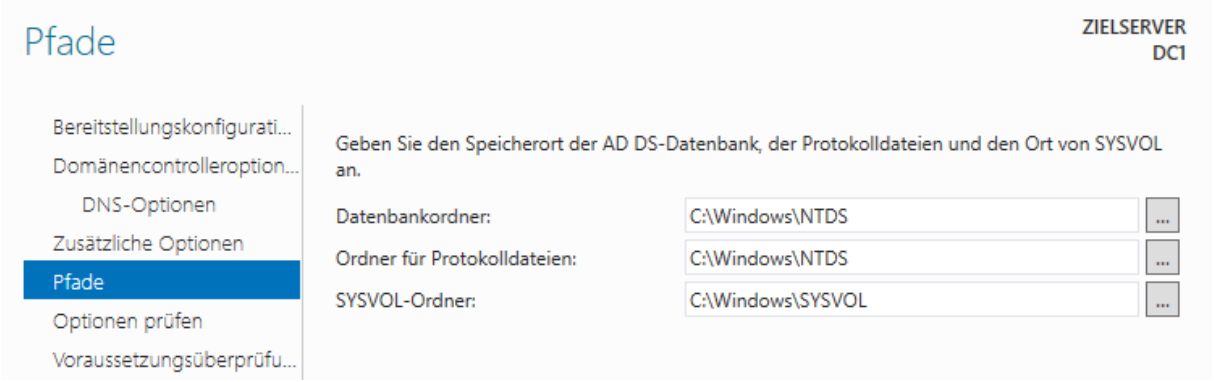
Die nachfolgende Meldung, dass keine DNS-Delegierung erstellt werden kann, können wir mit **WEITER** ignorieren. Sie ist irreführend.



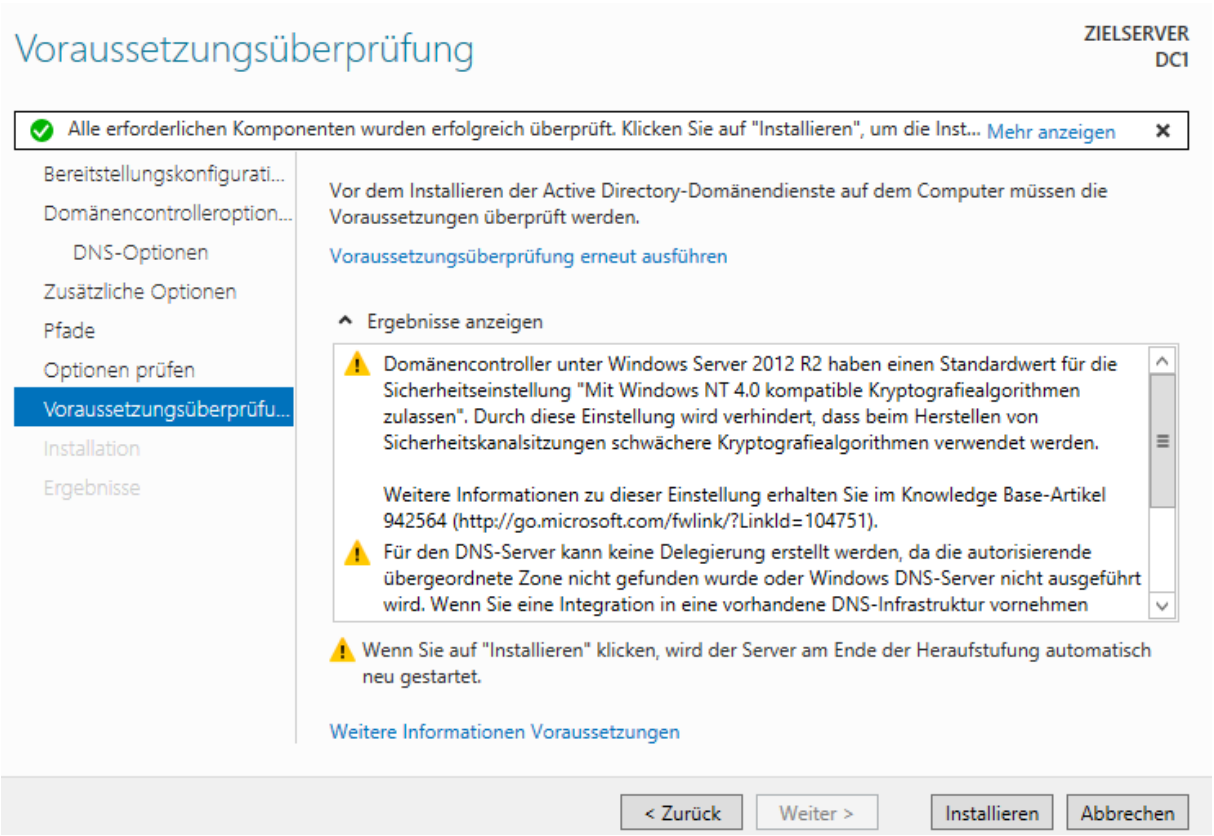
Die anschließende Prüfung des NetBIOS-Domänennamens sollte problemlos verlaufen:



Die Pfade belassen wir auf dem Standardwert:



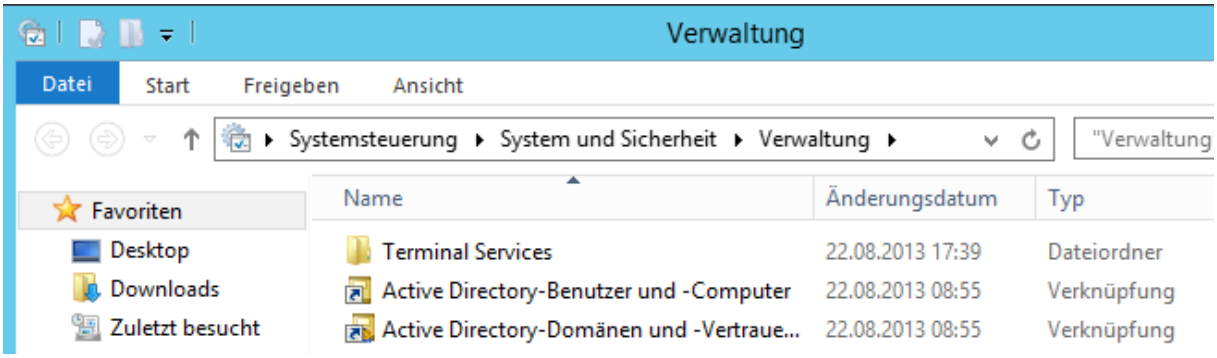
Sind schließlich alle Voraussetzungen überprüft, können wir – trotz einiger Warnhinweise – die Installation beginnen:



Dieser Prozess dauert einige Zeit. Im Anschluss muss der Server neu gestartet werden. Nach dem Neustart melden wir uns als Administrator an, der jetzt jedoch im Domänenkontext (VICTIM) angezeigt wird:

Erstellen einer Organisationseinheit (OU) namens Berlin

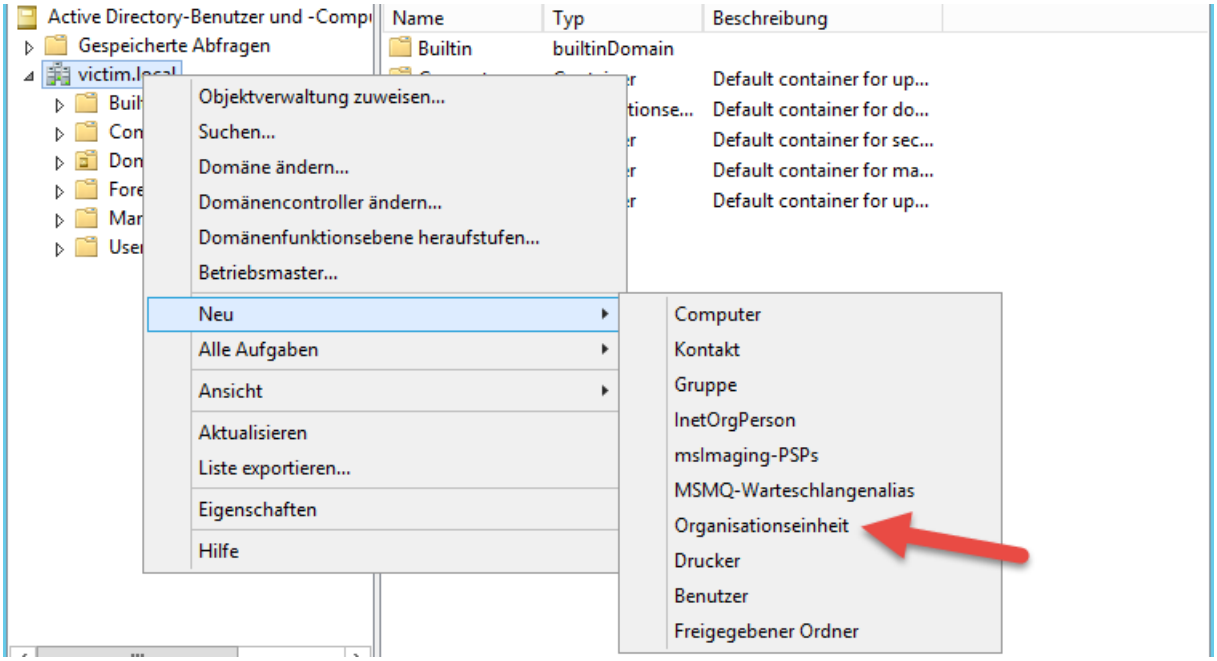
Es gibt zahlreiche AD-Verwaltungstools. Das wichtigste ist **Active Directory-Benutzer und -Computer**. Du kannst es über den **Server-Manager** aus dem Menü **Tools** oder über die **Verwaltung** im Startmenü öffnen:



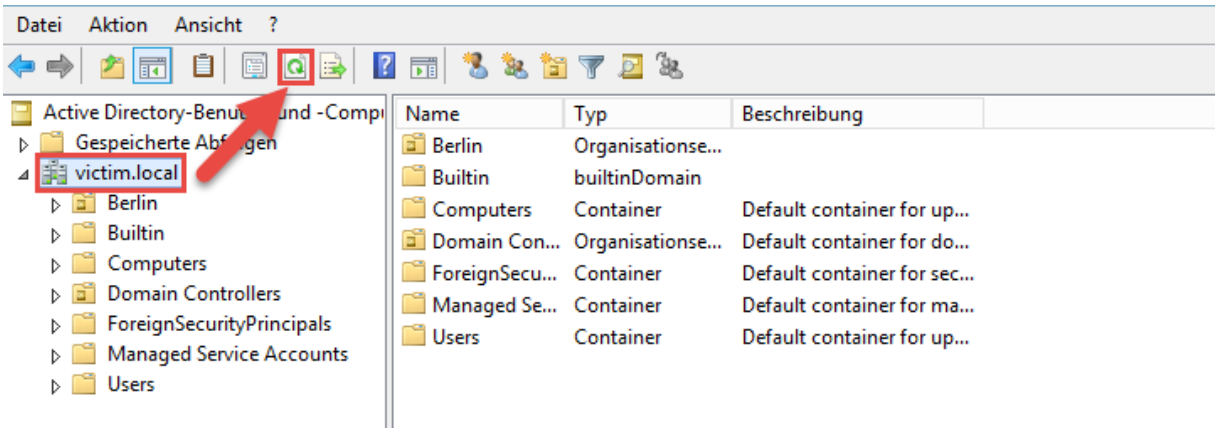
Die Domäne wird als Objekt dargestellt. Hierarchisch darunter kommen weitere Objekte:

- Container: Das sind feste, vorgegebene Strukturen, denen keine Gruppenrichtlinien explizit zugewiesen werden können. Sie sehen aus wie ein normales, leeres Ordnersymbol und enthalten weitere Ressourcen, wie Benutzer- und/oder Computerkonten sowie Gruppen.
- Organisationseinheiten (Organizational Unit, OU): Diesen Strukturen können, im Gegensatz zu Containern, Gruppenrichtlinien (Group Policy Objects, GPOs) zugewiesen werden. Ansonsten dienen Sie ebenfalls der Organisation zusammengehöriger Ressourcen

OUs können weitere OUs enthalten. Die Organisationsstruktur ist nicht vorgegeben und kann z.B. nach Standorten erfolgen. Erstellen wir eine OU namens Berlin. Klicke mit der rechten Maustaste auf das Objekt unter dem du eine neue OU erstellen willst, also z.B. auf das Domänenobjekt **victim.local**. Im Kontextmenü klickst du auf **Neu|Organisationseinheit**:

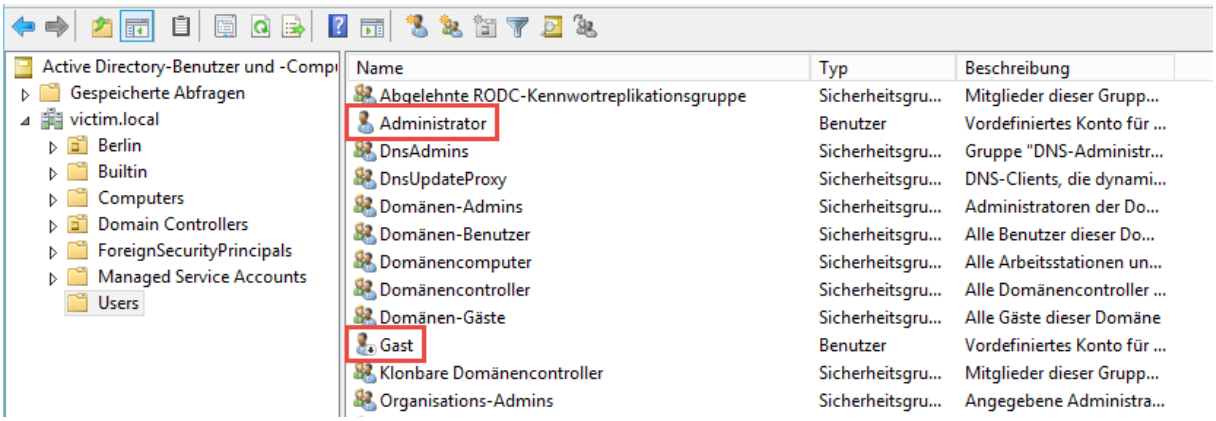


Gib den Namen Berlin ein und erstelle die OU. Sie taucht in der Liste ganz unten auf. Erst, wenn du das Domänenobjekt markierst und dann auf **Aktualisieren** klickst, wird die Liste wieder alphabetisch sortiert.

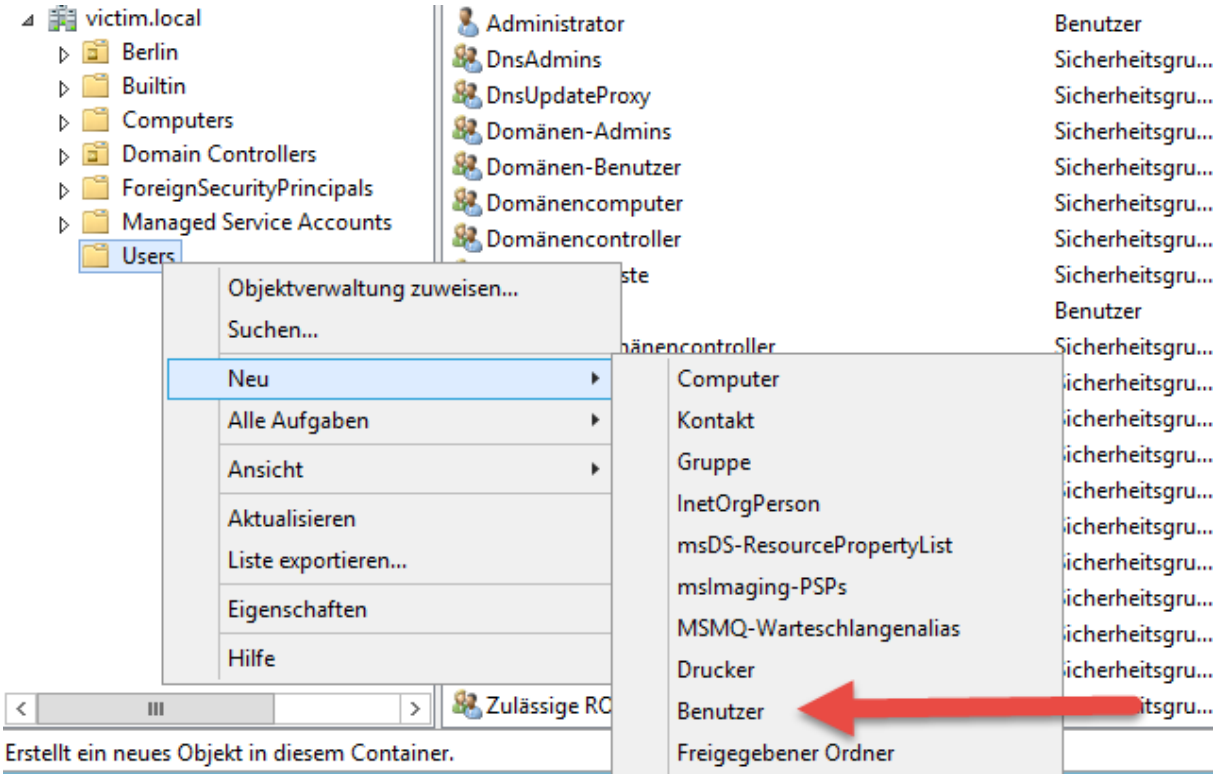


Erstellen zweier Benutzer Asterix und Obelix

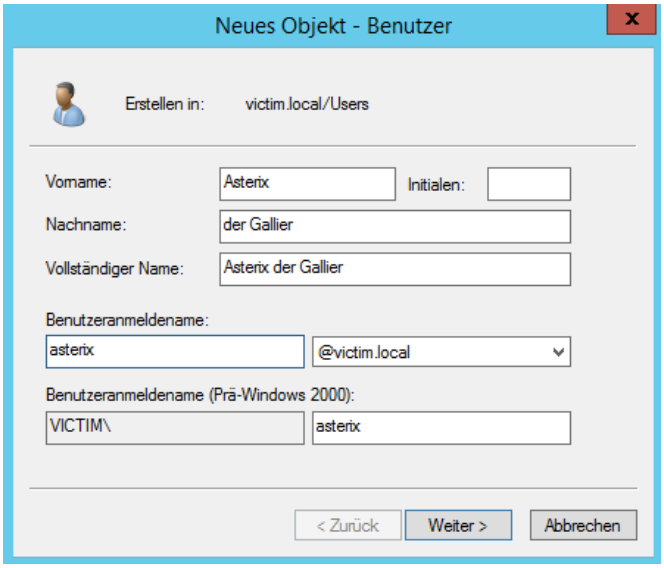
Im Container **Users** befinden sich alle aktuell existierenden Benutzer. Per Default sind das der *Administrator* und der deaktivierte Benutzer *Gast*:



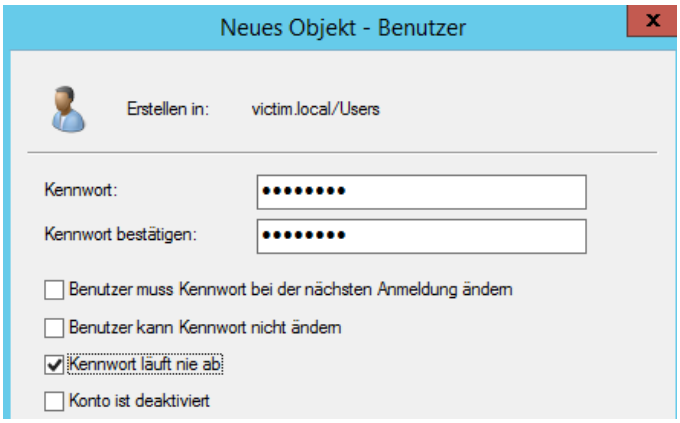
Erstellen wir über denselben Weg wie die OU nun zwei Benutzer namens *Asterix* und *Obelix* im Container **Users**:



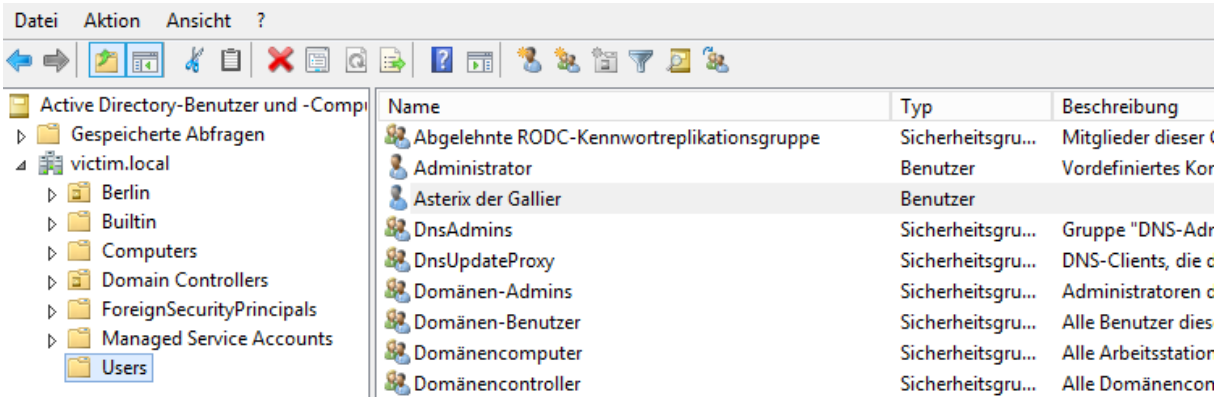
Wichtig ist der Benutzeranmeldename, alle anderen Werte dienen nur der Darstellung und der späteren Suche nach dem Objekt:



Für die Laborumgebung bietet es sich an, das Kennwort nie auslaufen zu lassen. Das Kennwort muss wieder den Komplexitätsrichtlinien entsprechen, daher empfiehlt sich erneut `Pa$$w0rd`.



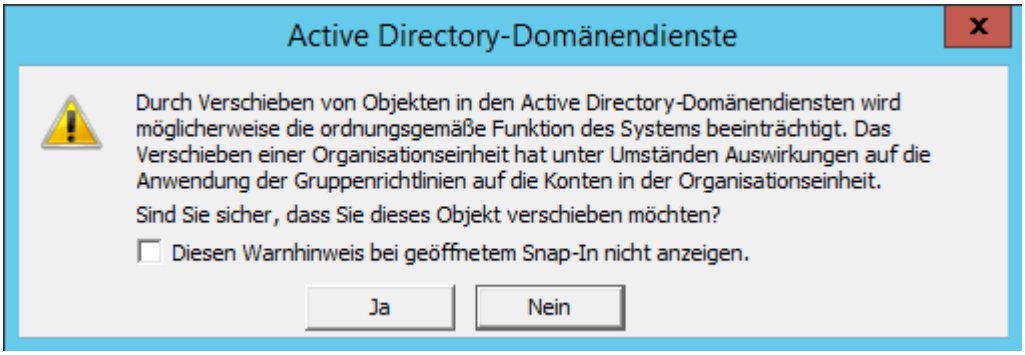
Der neue Benutzer wird im Anschluss erstellt und in der Liste angezeigt:



Erstelle in der gleichen Art nun einen Benutzer *Obelix* (der Hinkelsteinlieferant).

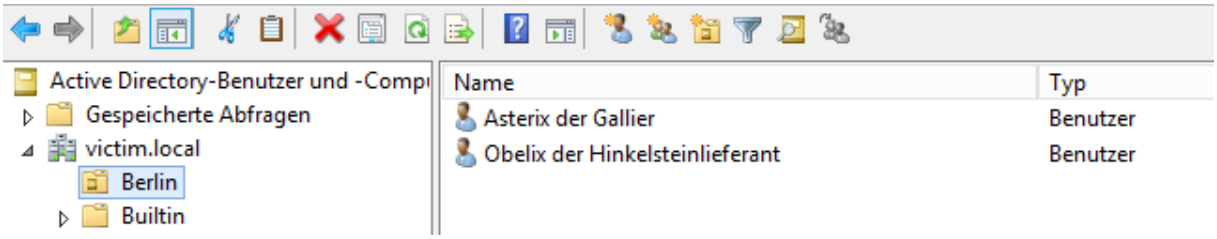
Die neuen Benutzer in die OU Berlin verschieben

Asterix und *Obelix* sind Mitarbeiter der Filiale Berlin und gehören organisatorisch daher in die OU *Berlin*. Benutzer können in jeder OU erstellt werden – wir hätten Asterix und Obelix also auch gleich in der OU Berlin erstellen können. Da wir dies jedoch nicht gemacht haben, müssen wir die beiden Benutzer nun in diese OU verschieben. Dies erledigst du am einfachsten via Drag & Drop. Während des Prozesses wirst du gefragt, ob du dir sicher bist, dass du das betreffende Objekt verschieben möchtest:



Diese Warnmeldung enthält einen wichtigen Hinweis: Gruppenrichtlinien enthalten tausende möglicher Einstellungen, Regeln und Rechte und werden entweder der gesamten Domäne oder einzelnen OUs zugewiesen. Damit wirken sie auf alle untergeordneten Objekte einschließlich der Unter-OUs und deren Objekte. Und zwar hierarchisch ab dem Punkt dem sie zugewiesen wurden. Wandert nun ein Objekt aus einer OU *Stuttgart* in eine OU *Berlin*, die auf derselben Ebene angesiedelt ist, dann werden Richtlinien, die der OU *Stuttgart* zugewiesen sind, keine Bedeutung mehr für die verschobenen Objekte haben, die sich anschließend in der OU *Berlin* befinden. Dieser Auswirkung muss sich ein Administrator klar sein. Für uns spielt es derzeit keine Rolle, zumal dem Container Users keine expliziten GPOs zugewiesen werden können.

Im Anschluss befinden sich Asterix und Obelix in der OU Berlin:

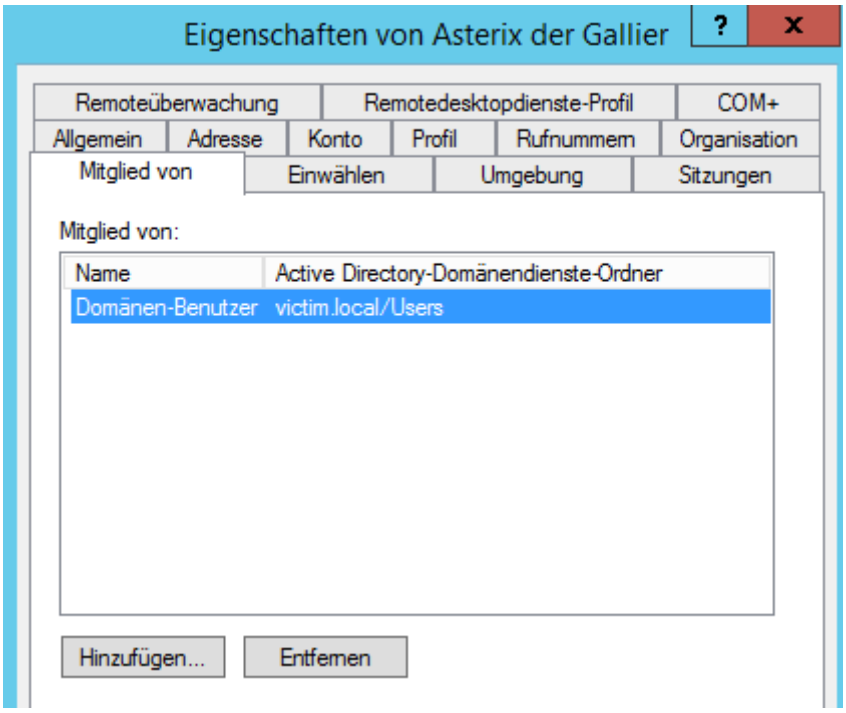


Hinzufügen des Benutzers Asterix zur Gruppe der Domänen-Admins

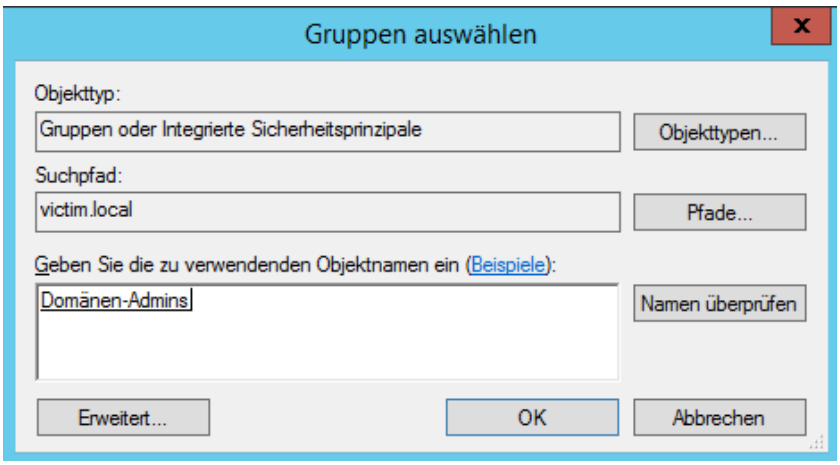
Benutzer werden in Gruppen organisiert. Hier sind Verschachtelungen möglich. Benutzer können auch in mehreren Gruppen sein. Standardmäßig sind Benutzer in der Gruppe der **Domänen-Benutzer**. Dabei handelt es sich um eine globale Gruppe, d.h. sie steht in der gesamten Domäne zur Verfügung. Darauf kommen wir gleich zurück. Wichtig ist, dass dieser Gruppe per Default keine höheren Privilegien zugewiesen sind.

Die Mitglieder der **Domänen-Admins** sind dagegen die Gruppe mit den höchsten Privilegien in der Domäne. Nachfolgend weisen wir Asterix dieser Gruppe zu. Dies geht über das Gruppenobjekt oder das Benutzerobjekt. Nutzen wir letztere Alternative. Klicke rechts auf das Benutzerkonto von Asterix und wähle **Eigenschaften**. Es öffnet sich ein Dialogfenster mit zahlreichen Registern.

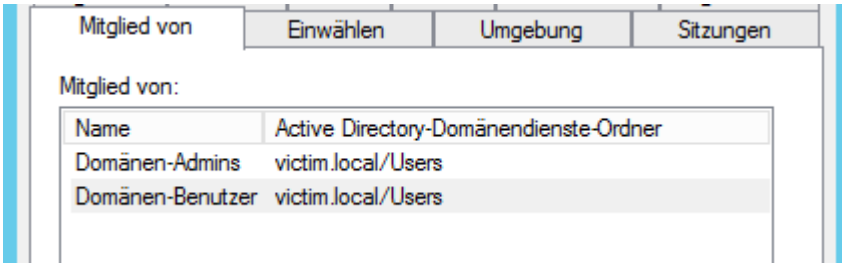
Klicke auf **MITGLIED VON**. Wie zu sehen, ist Asterix derzeit nur Mitglied der **DOMÄNEN-BENUTZER**:



Klicke auf **Hinzufügen** und gib *Domänen-Admins* ein. Über den Button **NAMEN ÜBERPRÜFEN** kannst du sicherstellen, dass diese Gruppe existiert. Sie wird dann unterstrichen:



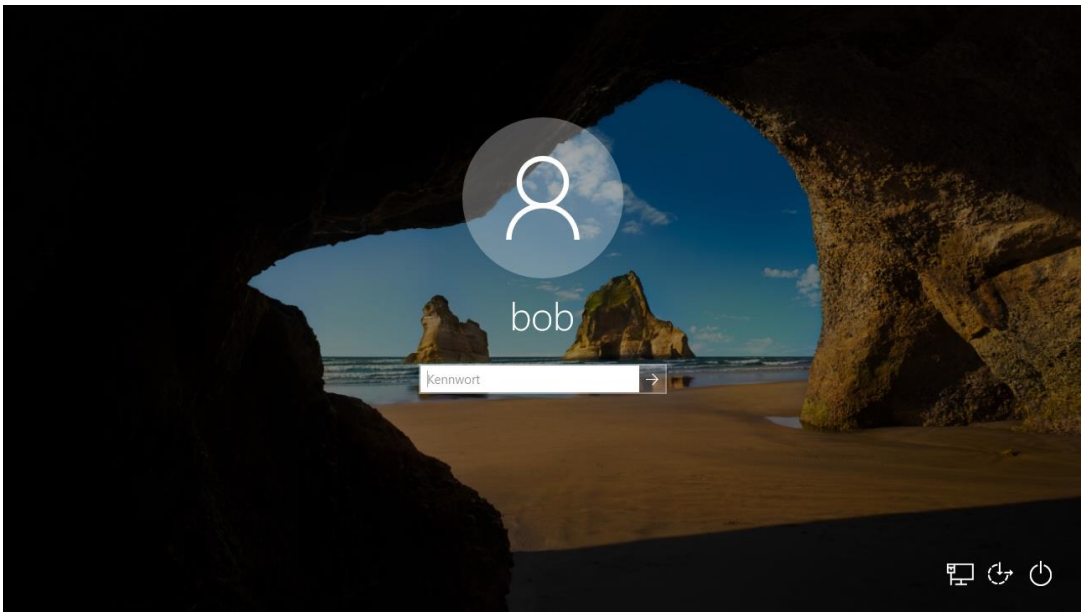
Klicke auf **OK**, um die Gruppenmitgliedschaft zu besiegeln. Damit hast du Asterix zum Domänen-Admin gemacht. Eine Ehre, die dieser hoffentlich zu schätzen weiß …



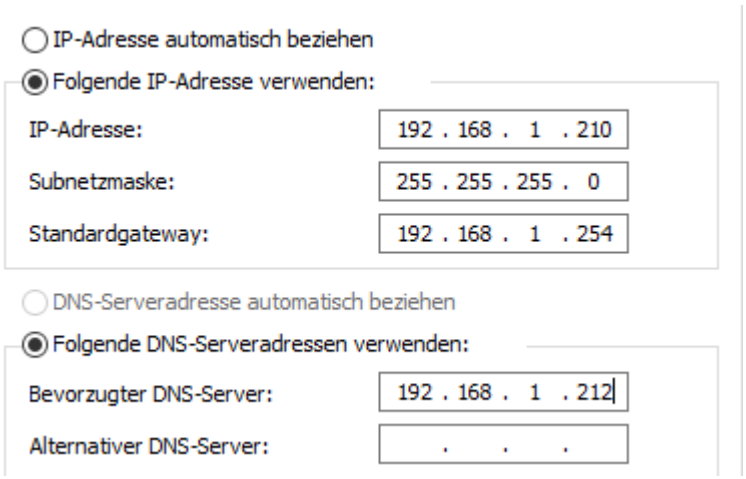
Klicke auf **Übernehmen** und **OK**, um die Eigenschaften zu schließen.

Hinzufügen des Windows 10-Computers zur Domäne

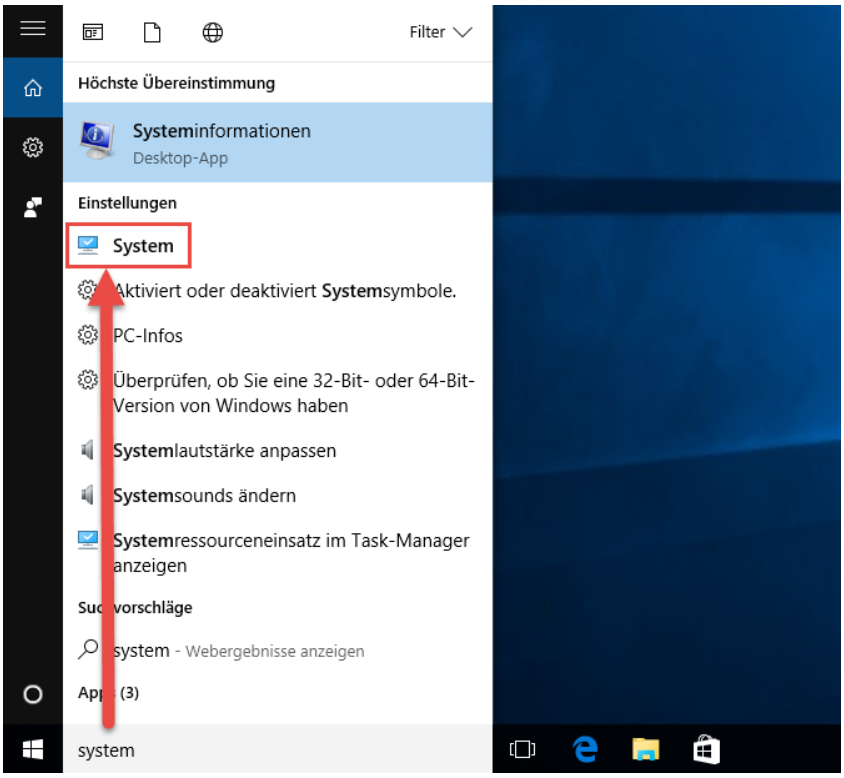
Der Windows 10-Computer namens *Win10* verfügt in unserem Szenario über einen lokalen Benutzer Bob, der auch der Administrator auf diesem System ist:



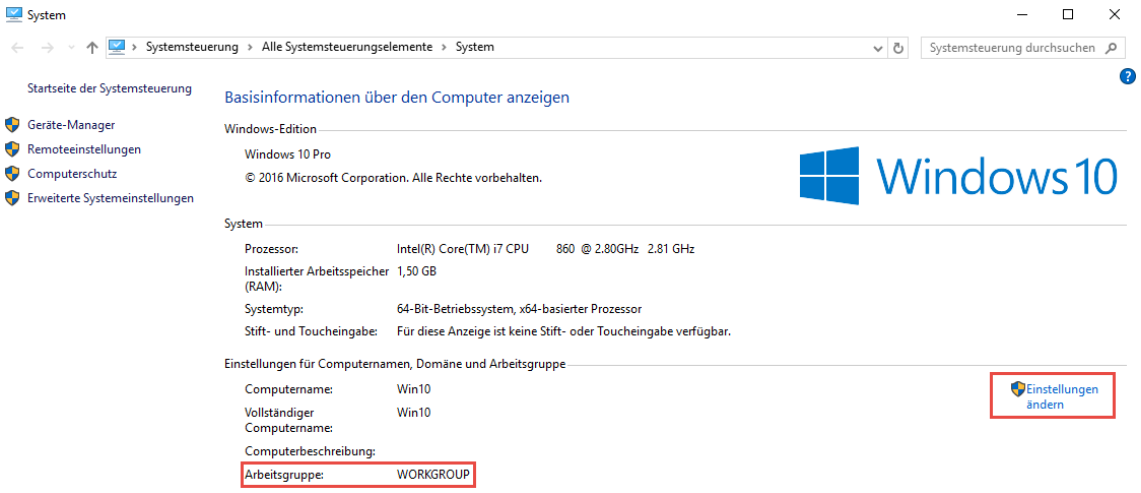
Zunächst stellen wir sicher, dass *Win10* den Domänencontroller als DNS-Server nutzt. Dazu tragen wir die IP-Adresse des DCs in die Netzwerk-Konfiguration ein:



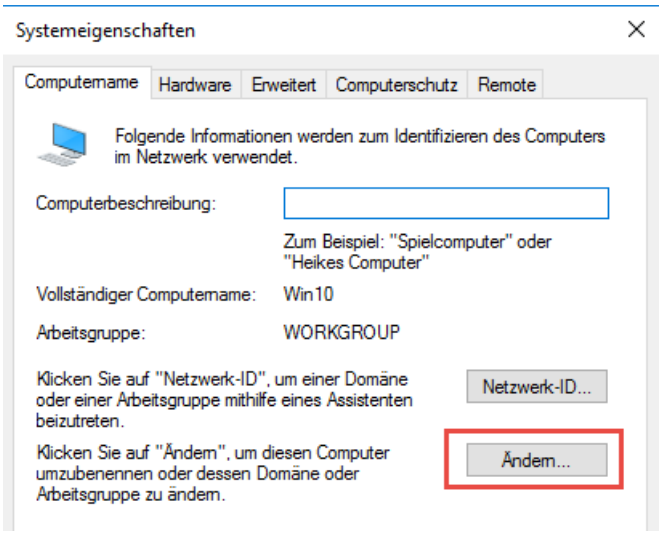
Nun wollen wir die Gruppenzugehörigkeit des Systems ändern. Hierzu gibt es mehrere Wege. Klicke z.B. in das Suchfenster und gib *system* ein. Wähle die System-App:



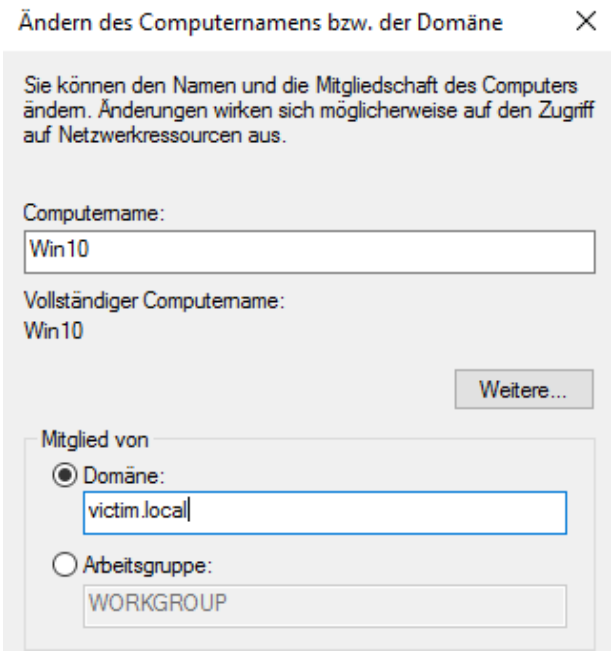
Über diesen Weg öffnet sich die Systemübersicht, in der wir in der Sektion **Einstellungen für Computernamen, Domäne und Arbeitsgruppe** auf der rechten Seite auf **Einstellungen ändern** klicken:



Es öffnet sich darauf ein neues Fenster, Klicke hier auf **Ändern**:

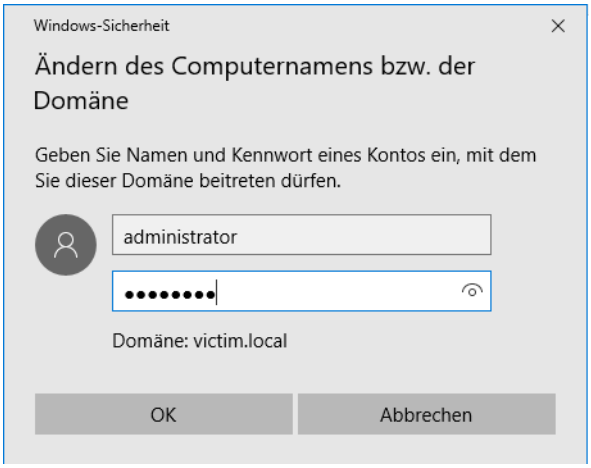


Ändere nun die Mitgliedschaft von *Arbeitsgruppe* auf *Domäne* und trage deine Domäne ein:

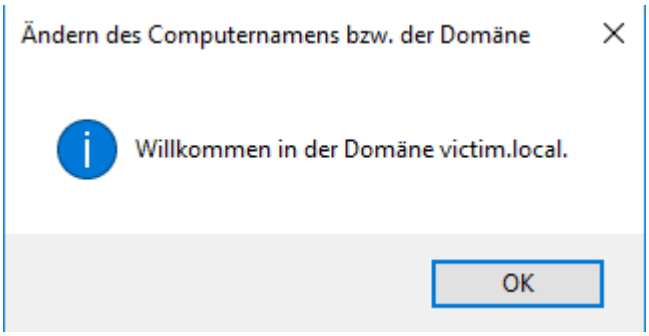


Über **OK** aktivierst du diese Option. Der Computer nimmt nun mit dem eingetragenen DNS-Server Verbindung auf und fragt bestimmte DNS-Einträge ab, um einen Anmeldeserver für die Domäne zu finden. Gelingt dies, erscheint die Aufforderung zur Eingabe eines gültigen Domänen-Benutzers, der diesen Computer der Domäne hinzufügen darf.

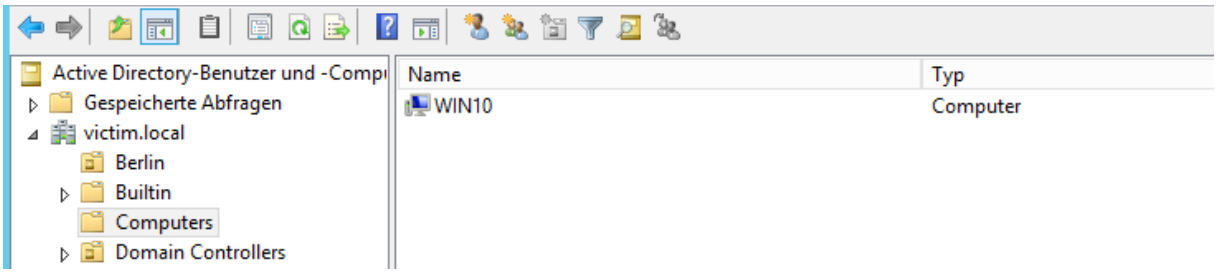
Hier kannst du entweder den Domänen-Admin (also Administrator) eingeben oder aber du nutzt *Asterix* oder *Obelix*. In einer Domäne dürfen standardmäßig auch normale, nicht privilegierte Benutzer einen Computer zur Domäne hinzufügen. Nur auf dem lokalen Computer muss der aktuell angemeldete Benutzer (hier: Bob) Administrator sein.



Anschließend werden wir in der Domäne willkommen geheißen und müssen den Computer neu starten:



Auf dem Domänencontroller (DC1) ist jetzt ein Computerkonto für Win10 erzeugt und im Container COMPUTERS abgelegt worden:

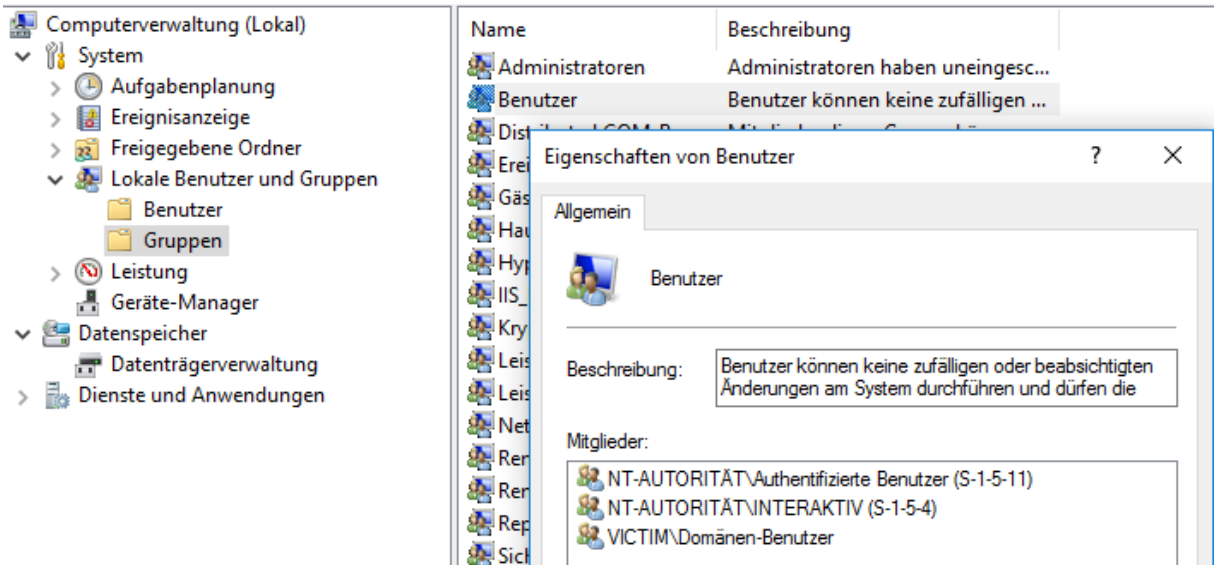


Anmelden von Obelix an Win10 und Prüfen der Gruppenzugehörigkeiten

Auf *Win10* wählen wir nach dem Neustart bei der Anmeldung einen ANDEREN BENUTZER (als Bob) und stellen als erstes fest, dass der Computer sofort davon ausgeht, dass wir uns an der Domäne (VICTIM) anmelden wollen:

Testen wir den Zugang zunächst mit *Obelix*. Dieser Benutzer existiert nicht auf dem lokalen System, aber in der Domäne. Nach der Anmeldung wird zunächst der Desktop für Obelix vorbereitet. Danach erhält Obelix normalen Zugang zum Computer, da dieser Mitglied der Domäne ist.

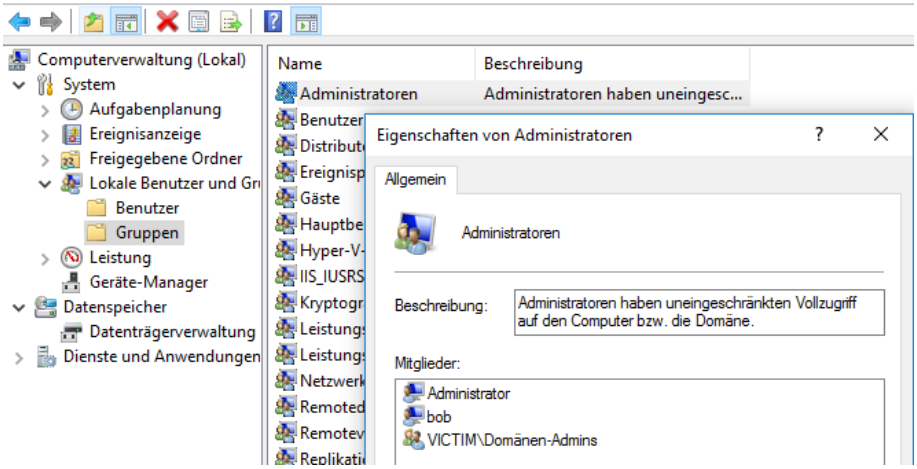
Apropos Mitglied: Schauen wir uns die Gruppenmitgliedschaften von Obelix an. Über Rechtsklick auf den Startbutton finden wir die **COMPUTERVERWALTUNG**. Dort können wir uns unter **LOKALE BENUTZER UND GRUPPEN** die Eigenschaften der (lokalen) Gruppe der **BENUTZER** anzeigen lassen. Deren Mitglieder umfasst nun auch die (globale) Gruppe der DOMÄNEN-BENUTZER:



Damit ist Obelix – als Mitglied der Domänen-Benutzer – auch implizit Mitglied der lokalen Benutzer und hat alle Rechte, die diese Gruppe auf dem lokalen System innehat. Da es sich hierbei um keine privilegierte Benutzergruppe handelt, ist dieser Umstand für dich vermutlich nicht so beeindruckend. Auswirkungen hat dies z.B., wenn Obelix versucht, die IP-Konfiguration zu verändern. Dies ist ihm nicht erlaubt, da er nicht über die dafür erforderlichen Rechte verfügt. Er müsste nämlich ein Administrator auf dem Domänenmitglied sein – ist er aber nicht.

Anmelden von Asterix an Win10 und Prüfen der Gruppenzugehörigkeiten

Melden wir uns als *Asterix* an, passiert vordergründig dasselbe, wie bei Obelix. Doch schauen wir uns die Gruppenzugehörigkeit erneut an. Wie wir über die Computerverwaltung feststellen können, sind auch die DOMÄNEN-ADMINS Mitglieder der lokalen Gruppe der ADMINISTRATOREN.



Das bedeutet nichts anderes, als das der Domänenbenutzer Asterix aufgrund seiner Mitgliedschaft in der globalen Gruppe der DOMÄNEN-ADMINS auch auf jedem Mitgliedssystem der Domäne lokale Administratorrechte hat, da diese Gruppe immer als Mitglied der lokalen Administratorgruppe aufgenommen wird. Ergo kann Asterix z.B. auch die Systemzeit ändern oder die IP-Konfiguration anpassen.

Anmelden des lokalen Benutzers Bob an Win10 im lokalen Kontext

Möchtest du Win10 nun zwischenzeitlich im lokalen Kontext, also ohne Domänenrichtlinien etc. nutzen, so kannst du dich als lokaler Benutzer Bob anmelden. Dazu musst du allerdings den Computernamen mit angeben, da der Anmeldedienst ansonsten davon ausgeht, dass du dich im Kontext der Domäne anmelden möchtest. Dies geschieht folgendermaßen:

Unter der Login-Maske zeigt der der Anmeldedienst an, in welchem Kontext er die Anmeldung versuchen wird. In jedem Fall bleiben die einstmals lokal angelegten Benutzer und Gruppen erhalten und können weiter genutzt werden.

Unter normalen Bedingungen wirst du dich allerdings nur selten im lokalen Kontext anmelden wollen, da ein Mitglied der Domäne auch von den *Single-Sign-On*-Vorteilen profitiert. Durch eine einmalige Anmeldung am DC kannst du domänenweit auf Ressourcen zugreifen, ohne dich an jedem Server der Domäne erneut anmelden zu müssen. Im Unternehmensumfeld ein unschätzbarer Vorteil. Für Angreifer ein interessanter Angriffsvektor, da das Kapern eines privilegierten Domänen-Accounts (z.B. eines Domänen-Admins) den Admin-Zugriff auf zahlreiche Systeme freischaltet …