

Active Directory verwalten mit LDP

von Holger Voges



© 2014 by Holger Voges, Netz-Weise IT Training

Freundallee 13 a
30173 Hannover
www.netz-weise.de

Inhalt

LDP.exe verwenden	4
Verbindung zu einer Domäne herstellen	4
Objekte verändern	7
SID Identifizieren mit LDP.....	8
Über den Autor.....	10

LDP.exe verwenden

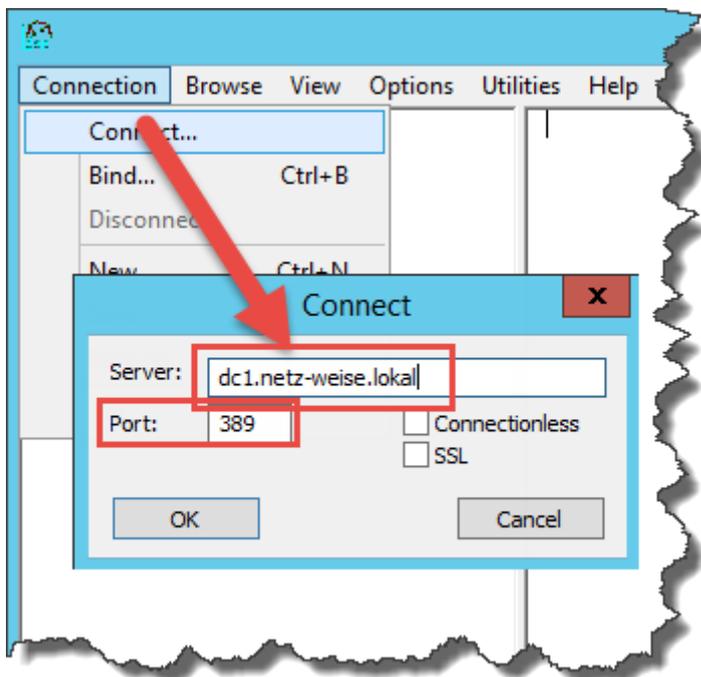
LDP ist ein LDAP-Browser, also ein Tool, um direkt auf LDAP-Verzeichnisdienste wie das Active Directory zugreifen zu können. Anders als Active Directory Benutzer und Computer zeigt LDP die Daten, die das AD liefert, aber ungefiltert an. Es werden also keine grafischen Elemente verwendet, um die Daten aufzubereiten, sondern LDP zeigt die Daten „roh“ an, wie das AD sie ausgibt. In dieser Kurzanleitung möchte ich Ihnen kurz die Basisfunktionalität von LDP zeigen.

LDP.exe war bis Windows Server 2008 Bestandteil der Windows Support Tools. Seit Windows Server 2008 ist LDP Bestandteil der Remote Server Administration Tools (RSAT) und wird mit den AD-Verwaltungstools mitinstalliert. Um LDP zu starten, geben Sie einfach ldp.exe an der Kommandozeile ein.

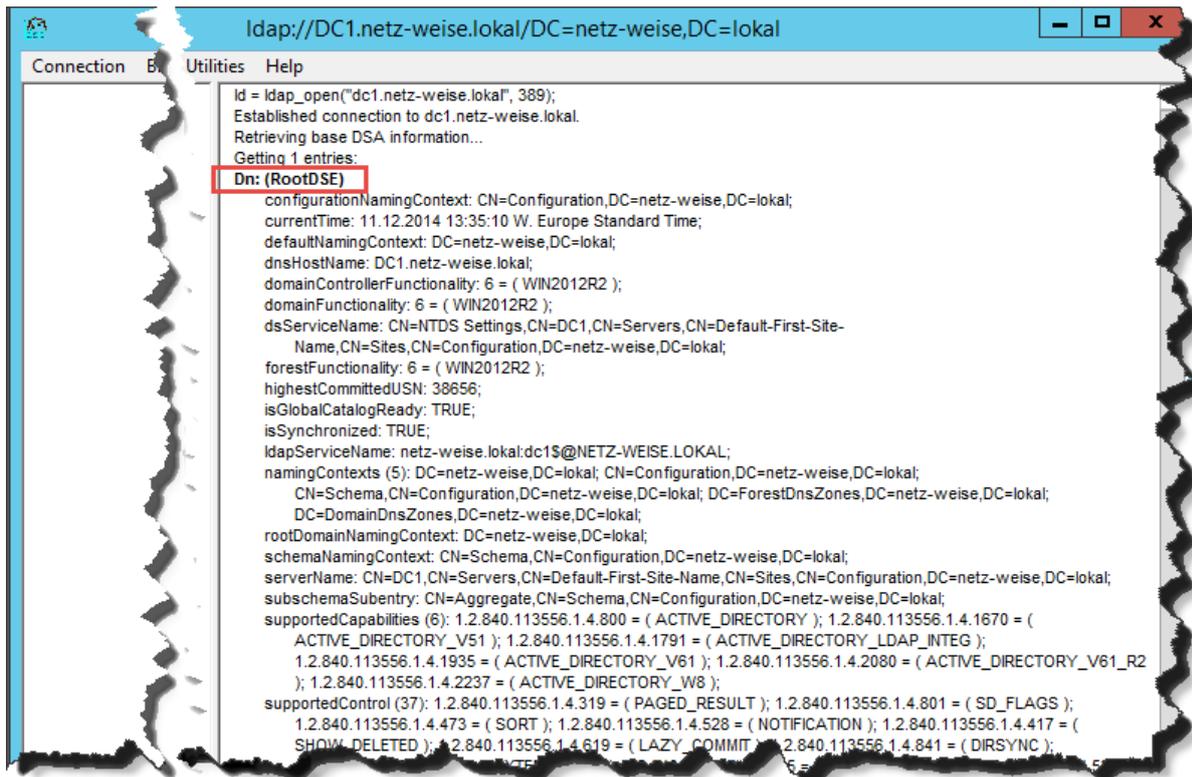
Verbindung zu einer Domäne herstellen

LDP startet sehr spartanisch und ist nicht wirklich selbsterklärend. Wir werden im Folgenden eine Verbindung zur AD-Domänendatenbank herstellen.

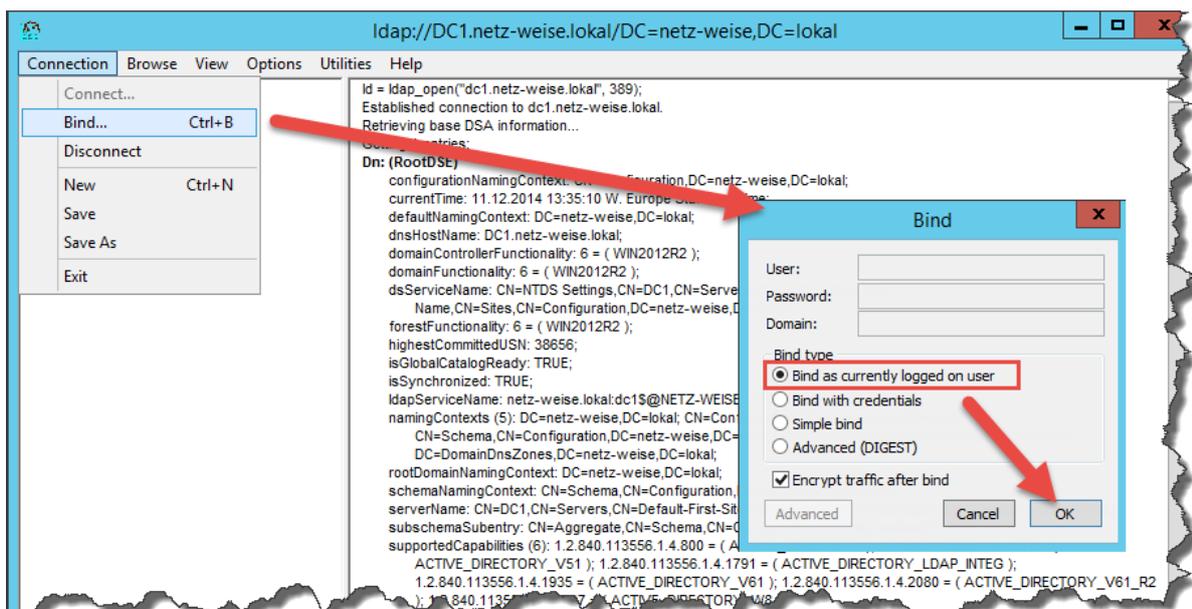
Klicken Sie zuerst auf Connect, um einen Server anzugeben, mit dem Sie sich verbinden möchten. Tragen Sie unter Server den Servernamen eines Domänencontrollers ein. Als Port wird standardmäßig 389 angegeben. Das ist der tcp-Port, auf dem die Domänencontrollerdienste normalerweise Verbindungen annehmen. Wenn sie auf einen AD-Snapshot zugreifen wollen, geben Sie hier den Port ein, den Sie beim Erstellen des Snapshots angegeben haben. Wenn Sie auf einen globalen Katalog-Server zugreifen wollen, geht auch das mit LDP. Der Port, an den der gc normalerweise verbunden ist, ist Port 3268.



Mit dem Connect wird zuerst einmal eine Verbindung zum Domänencontroller hergestellt. Der DC gibt sein RootDSE-Objekt zurück, das bereits eine Reihe von interessanten Informationen zur Verfügung stellt.



Um mehr Daten vom DC zu bekommen, müssen Sie sich erst einmal am DC authentifizieren. Dafür müssen Sie über das Connection-Menü auf Bind klicken. Entweder geben Sie hier Anmeldeinformationen ein, oder Sie melden sich mit dem Benutzerkonto an, mit dem Sie angemeldet sind. Je nachdem, über welche Berechtigungen Ihr Anmeldekonto verfügt, bekommen Sie unterschiedlich viele Informationen zu sehen, da das AD mit Berechtigungen ähnlich NTFS arbeitet.

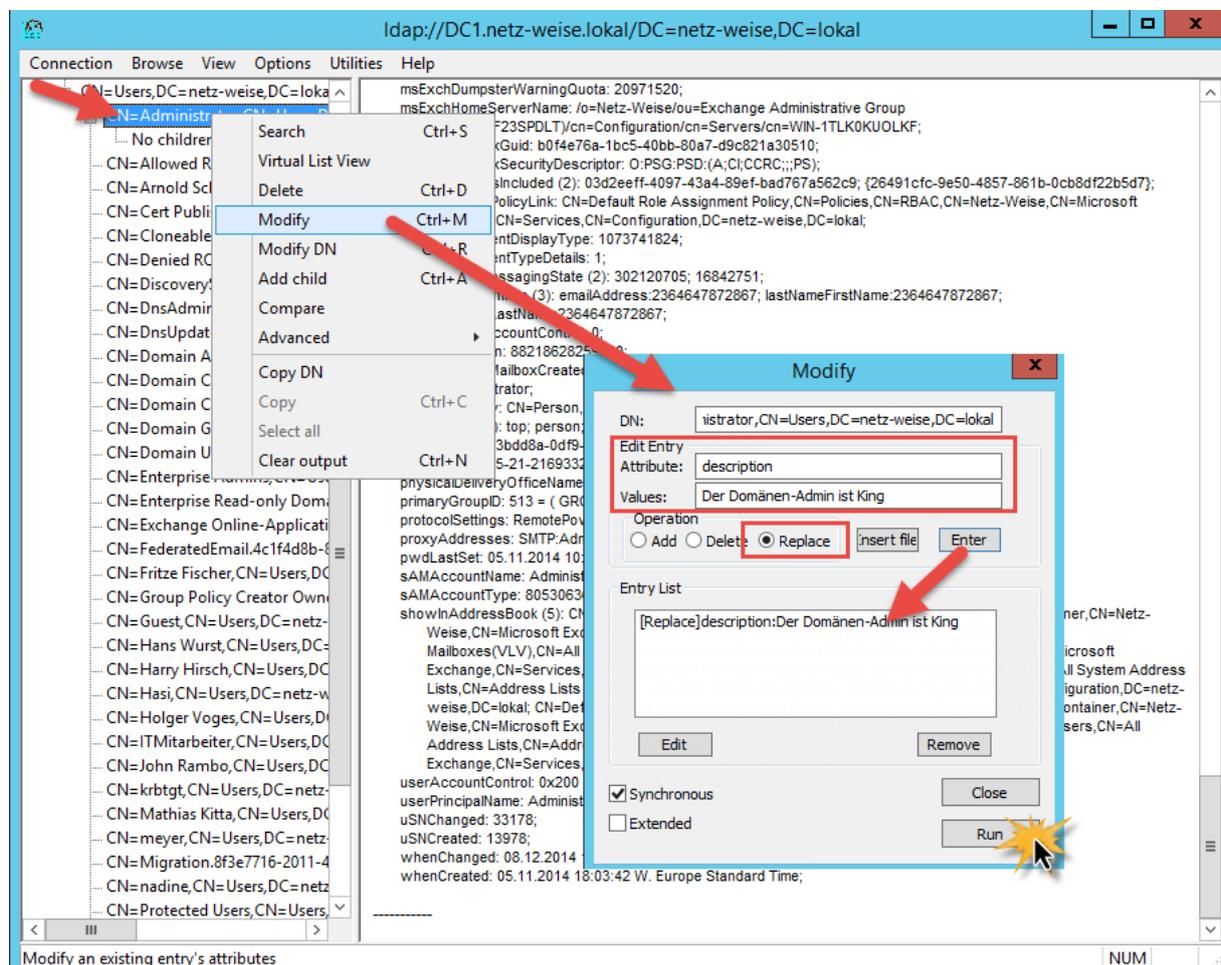


Sie können sich jetzt links durch die Domänenstruktur klicken. Das Detail-Fenster auf der rechten Seite zeigt Ihnen die Eigenschaften der Objekte an.

Objekte verändern

Sie können mit LDP.exe aber nicht nur Daten anzeigen, Sie können mit LDP auch Datensätze verändern. Dafür klicken Sie einfach mit der rechten Maustaste auf das Objekt, das Sie bearbeiten möchten, und klicken Modify.

Geben Sie jetzt im Feld *Edit Entry Attribute* die Eigenschaft ein, die geändert werden soll, sowie unter Value deren Wert. Soll die Eigenschaft überschrieben werden, wählen Sie den Radio-Button „Replace“, wollen Sie eine noch nicht gesetzte Eigenschaft anlegen, wählen Sie Add. Anschließend drücken Sie Enter, um die Eigenschaft einzutragen. Wenn Sie mehrere Werte ändern möchten, können Sie alle Eigenschaften in der Entry-List anlegen. Die Änderungen werden erst durchgeführt, wenn Sie „Run“ drücken. LDP erzeugt dann eine LDAP-Abfrage und schickt Sie gegen das AD.

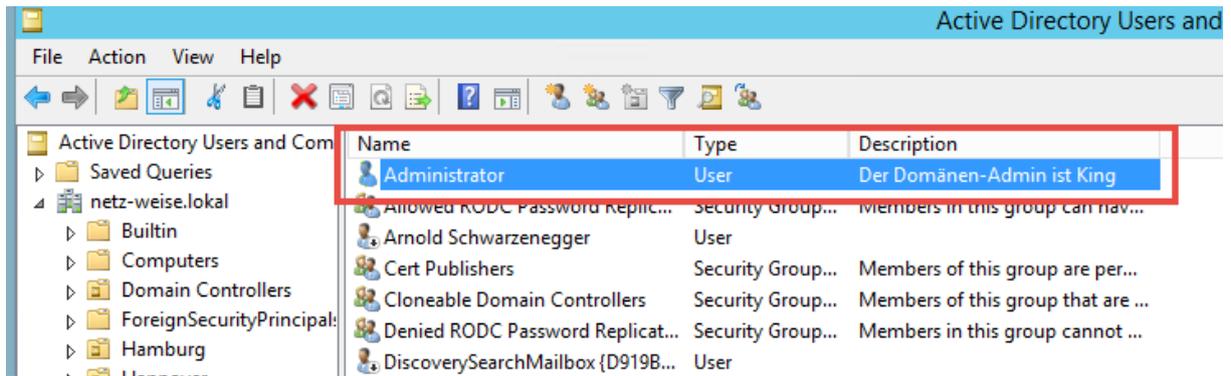


Ob Ihre Modifikation erfolgreich war oder nicht, sehen Sie zum einen an dem Ergebnis, das Ldp.exe Ihnen zurück liefert.

***Call Modify...

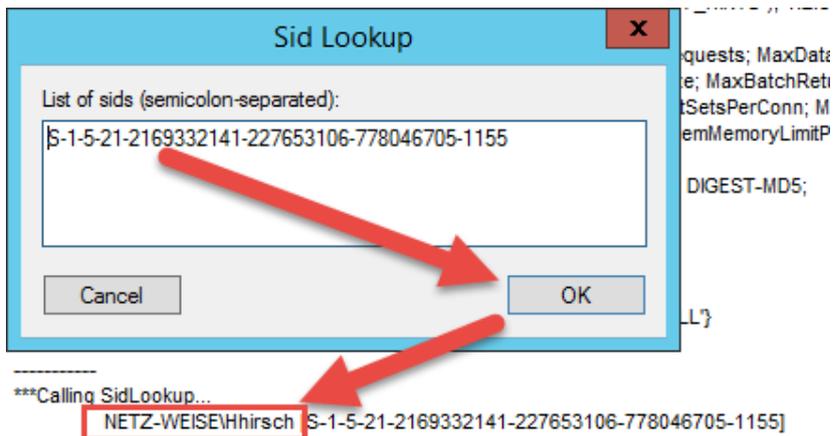
```
ldap_modify_s(ld, 'CN=Administrator,CN=Users,DC=netz-weise,DC=lokal',[1] attrs);  
Modified "CN=Administrator,CN=Users,DC=netz-weise,DC=lokal".
```

In diesem Fall war die Änderung erfolgreich. Das können Sie beispielsweise auch im Active Directory Benutzer und Computer überprüfen:



SID Identifizieren mit LDP

Mit LDP haben Sie auch die Möglichkeit, eine SID in einen Benutzernamen aufzulösen. Wählen Sie hierfür im Menü Utilities auf „SID-Lookup“ und geben Sie im folgenden Fenster eine SID ein:



Sid-Lookup löst Ihnen die eingegeben SID in einen Benutzernamen auf.

Anhang A

Links

[Ldp Overview](http://technet.microsoft.com/en-us/library/cc772839(v=ws.10).aspx)

[http://technet.microsoft.com/en-us/library/cc772839\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc772839(v=ws.10).aspx)

[LDP](http://technet.microsoft.com/en-us/library/cc771022.aspx)

<http://technet.microsoft.com/en-us/library/cc771022.aspx>



Über den Autor

Holger Voges ist IT-Trainer und Consultant. Seine IT-Karriere begann mit einem Atari ST 512 Mitte der 80er Jahre. Seine ersten Erfahrungen mit großen Netzwerken hat er im Systembetrieb der Volkswagen Financial Services 1999 gewonnen. Ab dem Jahr 2000 war er dann als freiberuflicher IT-Trainer für verschiedene Schulungsunternehmen im Bereich Braunschweig und Hannover tätig, bevor er 2002 mit 2 Mitstreitern sein erstes Schulungsunternehmen LayerDrei in Braunschweig gegründet hat. Nach seinem Ausstieg bei LayerDrei war er dann mehrere Jahre als freiberuflicher Consultant vor allem im SQL-Server Umfeld u.a. für T-Home Entertain, e.on und

Hewlett-Packard unterwegs, bevor er 2012 das Schulungsunternehmen Netz-Weise gegründet hat.

Netz-Weise hat sich auf Firmenschulungen im professionellen IT-Umfeld spezialisiert und bietet Schulungen u.a. im Bereich Microsoft, VMWare, Linux und Oracle an.