

Netviewer Active Directory-Connector

This White Paper deals with the subject of integrating Netviewer into a company network with an existing Microsoft Active Directory (AD) infrastructure on customer's premise. The document describes in detail the functionality of the Active Directory integration of Netviewer and the benefits of using it.

What is Active Directory?

Generally, Active Directory is used in enterprise environments. Active Directory is an object-based directory service developed by the Microsoft Corporation. It combines the lightweight directory service (LDAP), Kerberos, the common internet file system (CIFS) and the domain name system (DNS) in one package and allows managing user permissions, resources and services in enterprise networks. AD is implemented into the Windows 2000 and 2003 Server operating systems. The purpose of AD is to provide authentication and authorization services in mainly Windows-based networks. AD contains the object classes Resources (e.g. printer, scanner), Services (e.g. e-mail, shared directories) and Users (e.g. user, groups).

Who benefits from the Netviewer AD integration?

The Netviewer AD integration is of interest for companies which either want to distribute the Netviewer clients to a large amount of employees for meeting or support purposes or which want to control a large amount of Netviewer remote hosts without an additional user management. The connection between Netviewer and an existing AD enables the companies to offer Netviewer as 'Software as a service' (SaaS) model to their employees.

This leads to an easier management of the Netviewer system and lower maintenance efforts and to higher acceptance of the users due to an easier use without the need of additional logins and passwords.

The Netviewer AD integration is available for the products Netviewer Support, Netviewer Meet and Netviewer Admin.

Requirements

The Netviewer AD integration requires the use of a Netviewer Server on customer's premise. The Netviewer server system consists of the software Netviewer Server running on a server computer. Neither Netviewer Server itself needs any connection to the AD nor has the server computer to be member of the AD. The entire AD functionality is based on the Netviewer client programs. The Netviewer server can therefore be positioned in the DMZ or even directly in the Internet, if needed.

The Netviewer Server requires a Microsoft SQL Database and should be directly accessible through an IP address or DNS name on port 80 (HTTP), 443 (TCP & SSL) or 2000 (TCP). The hardware requirements depend on the amount of concurrent Netviewer sessions or connected Netviewer Admin hosts.

Advantages of the Netviewer Active Directory integration

No separate login for Netviewer

Normally, the Netviewer user authenticates himself with a user name/password combination when starting the Netviewer client program.

When using the AD authentication the user does not need to separately login at the Netviewer application anymore. Netviewer accepts the user's standard Windows login and acts like a Single Sign-on application (SSO). The user does not need to remind an additional password. This raises the acceptance of using such a system and helps spreading the solution to the desired user groups.

Security

As Netviewer does not need additional logins, the potential risk of unauthorized access due to imprudent handling of passwords is reduced. Furthermore, there is no need to define password rules regarding length, complexity and duration for Netviewer because the existing rules of the AD server are used.

This also ensures the central administration of the Netviewer licenses because it is impossible to copy the client and use the license outside of the company network.

Easier administration

Users only have to be created in the AD. It may be useful to create specific AD user groups which are allowed to use Netviewer, but also existing group structures can be used. Based upon these user groups it is possible to assign rights to users in Netviewer.

Additionally, a user group can be linked with predefined profiles that determine in detail which set of functions the user group may use during the session according to a special use case. For instance a first level support agent can support clients with remote control but is not allowed to use the file transfer function. Second level support agents can support clients with the full set of functions. This gives the possibility of creating a complex rule system defining the permissions and available functions of an AD user group. Profiles can also determine if a user group has the permission to establish sessions with external users who are not part of the customer AD environment.

In a Netviewer Admin scenario it is possible to define which host groups a remote master can see in the computer administration. This gives the opportunity of defining support groups or granting access rights to certain machines for external departments or suppliers.

After the basic setup of the AD connection, users receive their access rights automatically within the normal creation process of an Active Directory account. There is no need of additional administration for the Netviewer programs or server. The administrative effort after the setup of the Netviewer AD integration is very low.

Functionality

For the configuration of the AD connection the domain names of one or more Active Directories have to be stored in the Netviewer server during the setup of Netviewer Server. After the domain has been defined, the administrator can start a Netviewer client in this domain. This first connection will be accepted without valid rights in the domain so that the administrator is able to set up the basic configuration.

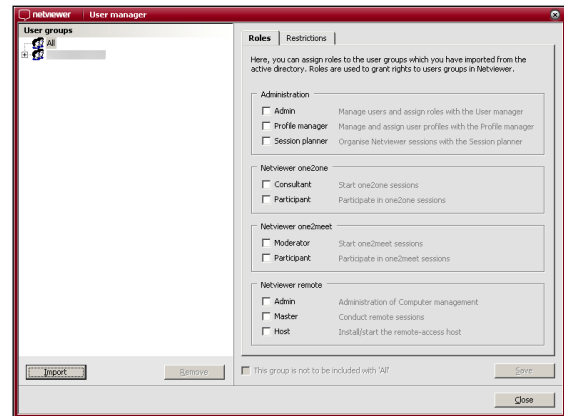


Figure 1

The administrator has to start the Netviewer client program and open the module User Manager. In the User Manager he can assign Netviewer access rights to AD groups.

First, the AD user groups, which are necessary for the Netviewer user management, must be imported from the AD server into the Netviewer server (see figure 1 – Netviewer User Manager Dialogue). This is done through the User Manager in the Netviewer client. The imported user groups are listed in the User Manager and must then be linked to one or more Netviewer roles. A role is for example the right to start the Netviewer Meet moderator program or the right to administrate the computer management of Netviewer Admin.

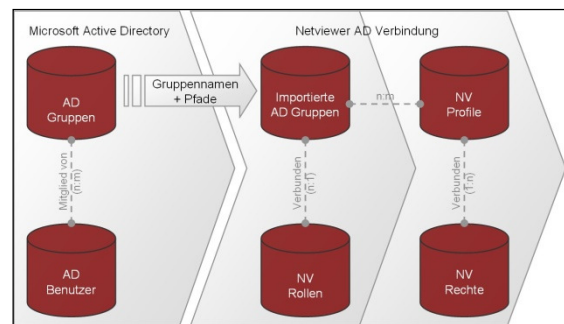


Figure 2

To explicitly prohibit the execution of Netviewer, for example for critical user groups like a research department, it is possible to define negative roles. These negative roles overrule positive roles that a user may have due to the membership in another AD group. This maximizes security and freedom in configuration.

After having imported the user groups and linked them to roles, the administrator can define profiles in the Netviewer Profile Manager and link them to one or more AD user groups (see

figure 2). A profile contains a set of features and settings (rights) which are available within a Netviewer session. A profile can, for instance, define that only selected trays are available in the Netviewer Control Panel or that the participant initially shows his screen to the consultant.

The users that are allowed to use a certain profile can choose this profile during the start up of the Netviewer application. If the user is linked to more than one profile he can choose between the available profiles.

Authentication process with AD

When the user starts Netviewer, the client program gathers the associated user group and its path from the AD server. The user group and the path will be sent to the Netviewer server by using the secure Netviewer protocols. The server verifies the user group against its own directory, checks for associated profiles and sends them back to the client program (see figure 3).

After the user has chosen the desired profile, he is able to invite participants or start a session.

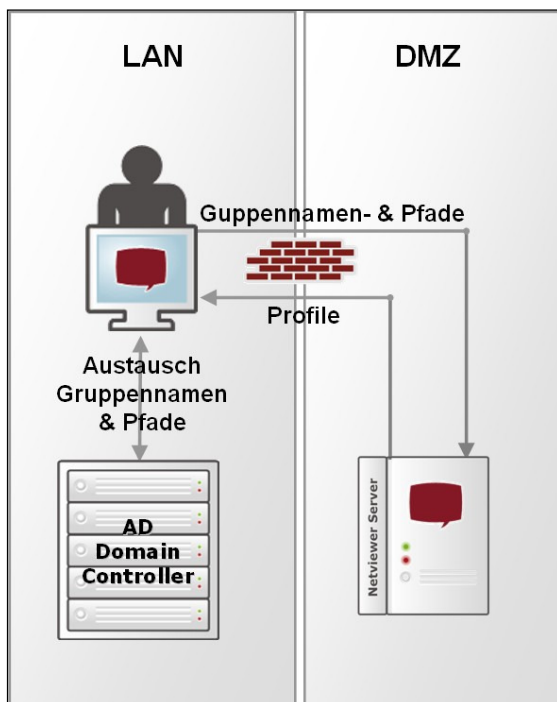


Figure 3

The Netviewer Server does not need to communicate directly with the AD server. Thus it is possible to place the Netviewer Server in the Demilitarized Zone (DMZ). As the clients need to be able to connect to the AD server, they have to be located inside the company's network (see figure 3).

Summary

The Netviewer AD integration offers various advantages for enterprise customers. These advantages are mainly easy administration, security and optimal integration into an existing infrastructure for best possible acceptance of the users.

The administrator is not restricted in terms of configuration or security policies. After the successful setup of the AD connection there is nearly no administrative effort in Netviewer.

The connection to the AD even works if the Netviewer server is not part of the AD domain and is able to handle complex domain structures (trees) and multiple independent domains.

Access rights can be assigned on the basis of the AD group membership of a user. The administrator is able to define roles and profiles for each group or to block certain groups from using Netviewer.

The AD connection requires the use of a Netviewer Server.

Version 1.2 - December 2009

Reference to Server- and Client Version: G3 & G3.1

© 2009 Netviewer AG. Netviewer Support, Meet, Admin, Server, and the Netviewer Logo are registered trademarks of Netviewer. All rights reserved. All other trademarks are the property of their respective owners.