Collax Active Directory

Howto

Dieses Howto beschreibt die Konfiguration eines Collax Servers um einer Windows Active Directory Service (ADS) Domäne beizutreten. Im Englischen spricht man hierbei von einem Active Directory Join. Des Weiteren geht dieses Howto auf die Einrichtung des Active Directory-Proxy Dienstes ein.

Durch den reinen Domänenbeitritt stehen dem AD-User lediglich die Dienste Files-Shares (FTP, Samba und mit Einschränkungen HTTP(S)) und Web-Proxy zur Verfügung, durch die Nutzung des AD-Proxy können die meisten Dienste des Collax Servers genutzt werden.

Voraussetzungen

- Collax Business Server
- Collax Platform Server
- Collax Security Gateway
- funktionsfähiger AD-Server mit eingerichtetem Domain Name Service (DNS)

Beispielkonfiguration

Collax Server

FQDN:	cbs.intern.collax.com
DNS-Zone:	intern.collax.com
Lokales Netz::	172.17.0.0/24
IP-Adresse:	172.17.0.1

Windows AD-Server

FQDN:	w2k8.intern.collax.com
DNS-Zone:	intern.collax.com
IP-Adresse:	172.17.0.45
ADS-Domäne:	INTERN
Kerberos-Realm:	INTERN.COLLAX.COM

Einleitung

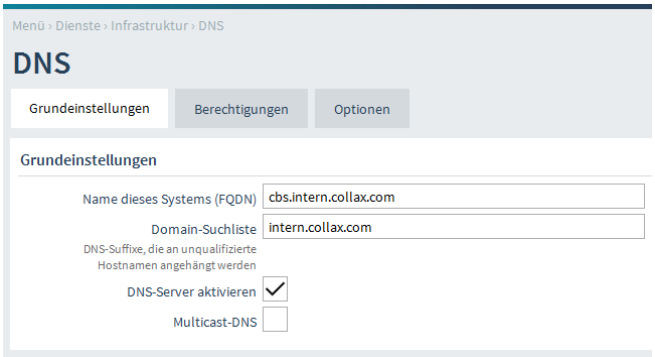
Im ersten Abschnitt wird beschrieben, wie Sie die Einstellungen Schritt für Schritt manuell durchführen. Diese Einstellungen können auch automatisch gesetzt werden, wenn Sie direkt den Dialog „Für ADS vorbereiten“ benutzen. Dies wird im zweiten Abschnitt „Domänenbeitritt“ beschrieben. Des Weiteren wird im zweiten Abschnitt auf die Konfiguration des AD-Proxy eingegangen.

Gehen Sie direkt zu Abschnitt 2 „Domänenbeitritt“ wenn der Collax Server die Grundeinstellungen automatisch durchführen soll und Sie nicht alle Einstellungen von Hand durchführen wollen.

1. Konfiguration des Collax Servers

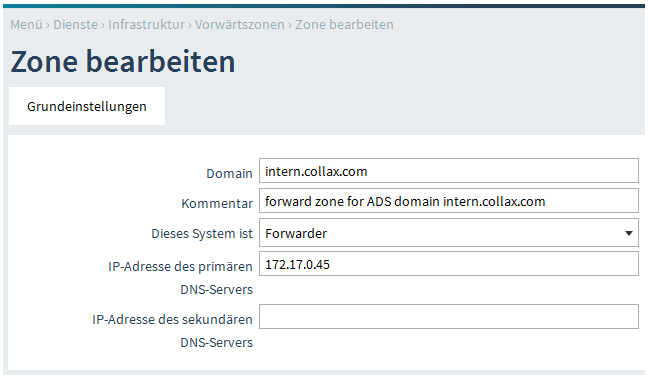
1.1 DNS-Konfiguration

Vergeben Sie unter *„Dienste → Infrastruktur → DNS → Allgemein“* den Fully Qualified Domain Name (FQDN) des Systems und definieren Sie den DNS-Suffix. Der DNS-Server muss zudem aktiviert werden.



Die Namensauflösung der Computer im Netzwerk erfolgt über den bereits konfigurierten Windows DNS-Server. Dem Collax Server muss an dieser Stelle nur mitgeteilt werden, diesen als **Forwarder** zu verwenden. Legen Sie hierzu eine Vorwärts- und Rückwärtszone an.

Unter *„Dienste → Infrastruktur → DNS → Vorwärtszonen“* hinterlegen Sie die IP-Adresse Ihres AD-Servers.



Falls ein BDC zur Verfügung steht und dieser ebenfalls einen DNS Dienst bereitstellt können Sie diesen hier als sekundären DNS-Server hinterlegen.

Unter *„Dienste → Infrastruktur → DNS → Rückwärtszonen“* hinterlegen Sie die IP Adresse Ihres AD-Servers.
Hier kann ebenfalls ein BDC als Sekundärer DNS Server hinterlegt werden falls bei Ihnen vorhanden.

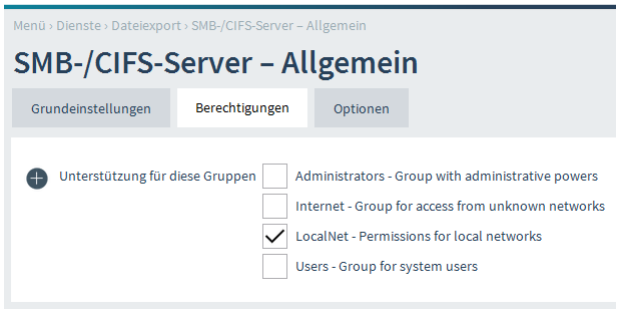
1.3 Windows-spezifische Einstellungen

Die Konfiguration der Windows-spezifischen Einstellungen umfasst die Aktivierung der Netzwerkfunktionalität für Windows-Netze, die Vergabe des Domänennamens und einiger Optionen.

Die Aktivierung erfolgt dabei über den Punkt „*System → Benutzungsrichtlinien → Windows Support → PDC/ADS*“.

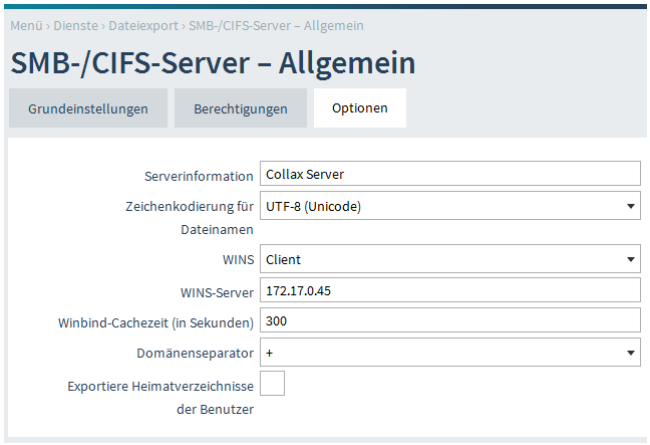
Im Reiter „*Grundeinstellung*“ muss lediglich der Dienst aktiviert und der Name der Domäne hinterlegt werden.

Im Reiter „*Berechtigungen*“ muss zumindest eine Gruppe ausgewählt werden, die das Netzwerk enthält in der der AD-Server und die lokalen Clients stehen.



Im Reiter „*Optionen*“ sind die Punkte WINS und Domänenseparator wichtig. Da der WINS-Server normalerweise der AD-Server ist, arbeitet der Collax Server in diesem Beispiel als Client.

Beim Domänenseparator sollte im Normalfall „+“ ausgewählt werden. Bei einem Unterstrich kann es zu Problemen mit lokalen Gruppen kommen, deren Name einen Unterstrich beinhaltet.



1.4 Kerberos

Die Konfiguration von Kerberos erfolgt über *„System → Benutzungsrichtlinien → Authentifizierung → Kerberos“*. Der Kerberos-Realm muss dem Namen der DNS-Domäne des AD-Servers entsprechen. Als KDC wird der AD-Server hinterlegt. Existiert noch ein BDC so kann dieser hier auch angegeben werden. Die Server werden durch Leerzeichen getrennt hinterlegt.

1.5 Umstellung der Benutzerdatenbank

Unter „*System → Benutzungsrichtlinien → Windows Support → PDC/ADS*“ muss abschließend die Benutzerdatenbank von Lokal auf ADS-Mitglied umgestellt werden.

Falls Ihr AD-Server ein Windows 2008 Server ist, muss bei Active Directory Server der FQDN des AD-Server hinterlegt werden.

Über den Punkt „*Benutzer aus anderen Domänen zulassen*“ kann bestimmt werden ob, sich auch Benutzer aus anderen Domänen anmelden dürfen. Damit die Anmeldung dieser Benutzer funktioniert, ist es notwendig dass eine Vertrauensstellung zwischen den beiden Domänen besteht.

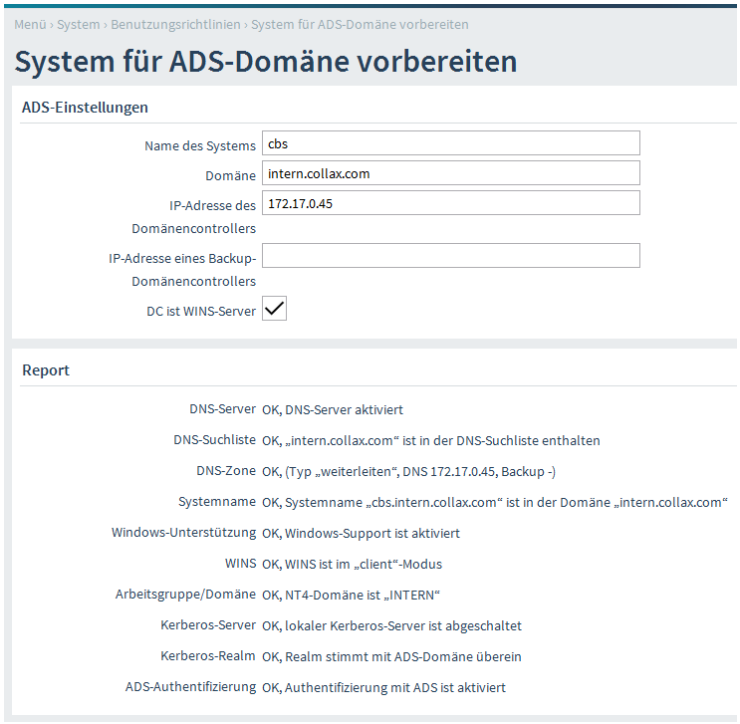
Aus Sicherheitsgründen sollte eine Aktivierung dieser Option gründlich geprüft werden.

Des Weiteren ist zu beachten, dass für die Authentifizierung der zuständige Domänenkontroller kontaktiert wird, bei langsamen Verbindungen kann dies zu Problemen führen.

1.6 Kontrolle der Einstellungen

Die Einstellungen können unter *„System → Benutzungsrichtlinien → Windows Support → Für ADS vorbereiten“* kontrolliert werden.

Der Report im unteren Teil gibt eine Auflistung der notwendigen Einstellungen und meldet OK wenn diese in Ordnung sind.

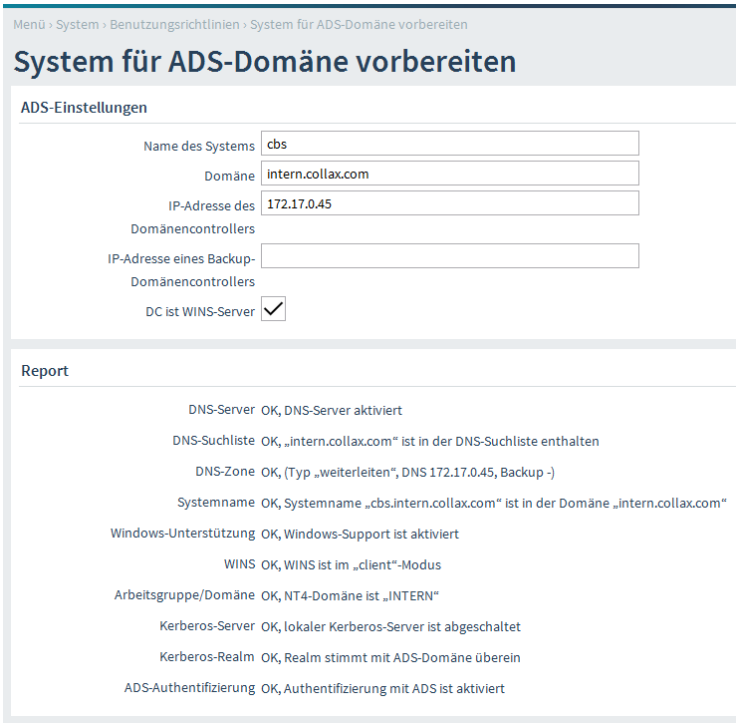


2. Automatische Konfiguration der Einstellungen

Sollen die Grundeinstellungen automatisch durchgeführt werden, geben Sie die Angaben zu Ihrem „AD-Server“ im oberen Abschnitt *„ADS-Einstellungen“* ein. Klicken Sie danach auf Speichern.

Beachten Sie hierbei dass in der Konfiguration automatisch anhand der Angaben Einstellungen überschrieben werden. Davon betroffen sind die Einstellungen für Kerberos, DNS, Authentifizierung und Windows-Unterstützung. Angaben zu Netzwerken, Netzwerklinks oder Gruppen werden nicht geändert.

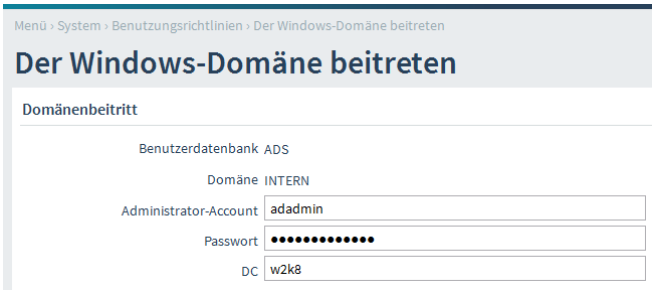
Falls Ihr AD-Server ein Windows 2008 Server ist, müssen Sie nachdem Sie diesen Punkt gespeichert haben unter *„System → Benutzungsrichtlinien → Windows Support → PDC/ADS“* beim Punkt *„Active Direcotry Server“* den FQDN des AD-Servers hinterlegen.



2.1 Domänenbeitritt

Den Domänenbeitritt können Sie unter *„System → Benutzungsrichtlinien → Windows Support → Domänenbeitritt“* durchführen. Achten Sie darauf, die vorher getätigten Einstellungen zu aktivieren.

Verwenden Sie zum Beitritt der Domäne ein Administrator-Konto des AD-Servers, der die erforderlichen Berechtigungen besitzt, um einen so genannten Maschinen-Account auf dem AD-Server zu erstellen. Klicken Sie anschließend auf *„Anmelden“*. Der erfolgreiche Beitritt wird mit der Statusmeldung *„Beitritt erfolgt“* quittiert.



2.2 Sonderfall Windows 2008 Server

Um einer Domäne beitreten zu können, die auf einem Windows 2008 Server konfiguriert ist, muss auf dem Windowsserver eine Veränderung vorgenommen werden.

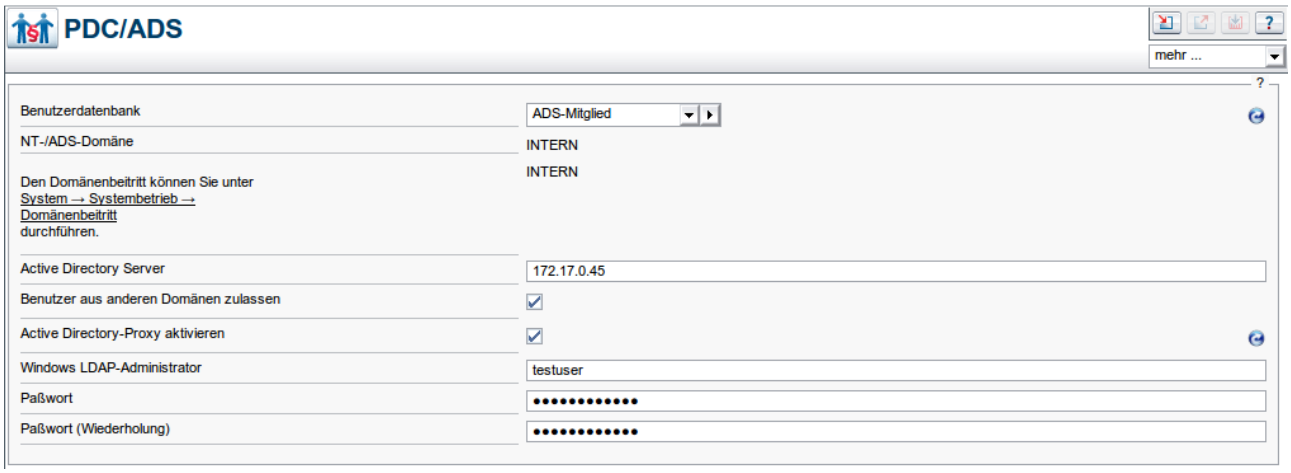
- Gruppenrichtlinienverwaltungseditor auf dem W2K8 aufrufen
- In der Default_DC_Policy unter *„Richtlinien --> Administrative Vorlagen --> Netzwerkanmeldung“* den Punkt *"Mit Windows NT4 kompatible Kryptografiealgorithmen zulassen" auf* "aktiviert" setzen
- Im DNS des W2K8 manuell einen Host für den Collax Server (A) und einen PTR erzeugen

2.3 Konfiguration des AD-Proxy

Erst nach einem erfolgreichen Beitritt in die Domäne kann der AD-Proxy konfiguriert werden.

Die Einstellungen für den AD-Proxy nehmen Sie unter „System → *Benutzungsrichtlinien* → *Windows Support* → *PDC/ADS*“ vor.

Für die Benutzung des AD-Proxy benötigt es lediglich einen AD-Benutzer der Leseberechtigung für das LDAP-Verzeichnis auf dem AD-Server hat.



Aktivieren Sie anschließend die Konfiguration. **Beachten Sie bitte, dass die Synchronisierung mit dem AD-Server, je nach Anzahl der Benutzer, einige Zeit dauern kann.**

Der Collax Server ist nun Mitglied der Active Directory Domäne. Sie können nun AD-Gruppen der lokalen Richtlinienverwaltung zur Verfügung stellen. Diese Gruppen tauchen nachfolgend im Menü Gruppen auf.

Dieser Dialog befindet sich unter *„System → Benutzungsrichtlinien → Windows Support → Importierbare Gruppen“*

In diesem Dialog werden Gruppen angezeigt, die in der Benutzerverwaltung eines Active Directory benutzt werden. Die aufgelisteten Gruppen können dann in die lokalen Benutzungsrichtlinien eingebunden werden, sobald diese über die Aktion *„Zu lokalen Gruppen hinzufügen“* in die Verwaltung aufgenommen wurden. Die Benutzer der AD-Gruppen werden weiterhin über das Active Directory verwaltet und sind nicht Bestandteil des lokalen Systems.

Beachten Sie bitte, dass nur Gruppen aufgelistet werden, die im Active Directory auch Benutzer enthalten.

Ein Abgleich der Benutzer und Gruppen findet in regelmäßigem Abstand jede Minute statt. Mitunter kann eine Änderung im Active Directory allerdings mehrere Minuten dauern, bis auch Windows alle Änderungen veröffentlicht hat.