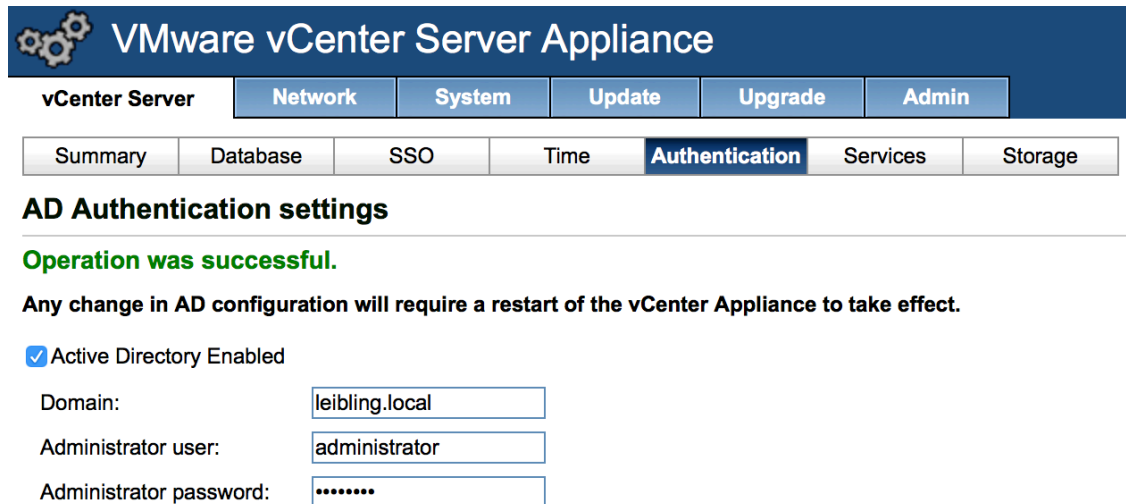


VCSA ans AD anbinden (SSO)

Wenn die VCSA Appliance ans AD angebunden wird, kann man sich am Vsphere Client mit der Windows Integrierten Anmeldung direkt aufrufen.

Dazu wie folgt vorgehen:

An der VCSA anmelden (<https://ip:5480>) mit root und dem Passwort.
Unter Vcenter > Authentication ans AD anbinden:



The screenshot shows the VMware vCenter Server Appliance configuration interface. The top navigation bar includes 'vCenter Server', 'Network', 'System', 'Update', 'Upgrade', and 'Admin'. Below this, a secondary navigation bar shows 'Summary', 'Database', 'SSO', 'Time', 'Authentication', 'Services', and 'Storage'. The 'Authentication' tab is selected, displaying 'AD Authentication settings'. A green message states 'Operation was successful.' Below this, a warning reads: 'Any change in AD configuration will require a restart of the vCenter Appliance to take effect.' The 'Active Directory Enabled' checkbox is checked. The configuration fields are: Domain: leibling.local, Administrator user: administrator, and Administrator password: masked with dots.

vCenter Server	Network	System	Update	Upgrade	Admin	
Summary	Database	SSO	Time	Authentication	Services	Storage

AD Authentication settings

Operation was successful.

Any change in AD configuration will require a restart of the vCenter Appliance to take effect.

Active Directory Enabled

Domain:


Administrator user:

Administrator password:

VCSA Appliance neustarten.

VCSA ans AD anbinden (SSO)


An der Webgui (<https://ip:9443>) als Administrator (administrator@vsphere.local, am besten direkt ändern - in der Webgui auf den Namen oben klicken und Kennwort ändern auswählen) anmelden und unter Verwaltung > Single Sign on die Verbindung zum AD herstellen:

 **Identitätsquelle hinzufügen**


Typ der Identitätsquelle:


- Active Directory (Integrierte Windows-Authentifizierung)
- Active Directory als ein LDAP-Server
- Open LDAP
- Lokales Betriebssystem

Einstellungen der Identitätsquelle

Domänenname: 

Maschinenkonto verwenden
 SPN verwenden

SPN (Dienstprinzipalname): 

UPN (Benutzerprinzipalname): 

Kennwort:

VCSA ans AD anbinden (SSO)

Dann unter Verwaltung > Single Sign on > Benutzer und Gruppen > Tab: Gruppen > Administrator aus wählen und unten dann die Gruppe Domain-admins hinzufügen über die Plus Taste:

Prinzipale hinzufügen ?


Wählen Sie Benutzer aus der Liste aus oder geben Sie Namen in das Textfeld 'Benutzer' ein. Klicken Sie auf 'Namen prüfen', um Ihre Einträge anhand des Verzeichnisses zu validieren.

Domäne:

Benutzer und Gruppen

Gruppen zuerst anzeigen

Suchen

Benutzer/Gruppe	Beschreibung/Vollständiger Name
 DHCP-Benutzer	Mitglieder, die nur über Lesezugriff auf ...
 Discovery Management	Die Mitglieder dieser Verwaltungsrollen...
 Distributed COM-Benutzer	Mitglieder dieser Gruppe können Distrib...
 DnsAdmins	Gruppe "DNS-Administratoren"
 DnsUpdateProxy	DNS-Clients, die dynamische Updates f...
 Domänen-Admins	Administratoren der Domäne
 Domänen-Benutzer	Alle Benutzer dieser Domäne

Hinzufügen

Benutzer:

Gruppen:

Mehrere Namen durch Semikola trennen

Namen prüfen

OK

Abbrechen

VCSA ans AD anbinden (SSO)


Danach unter Home > Hosts und Cluster > Host rechte Maustaste auf Einstellungen > im Tab Verwaltung > auf Berechtigungen > die entsprechende Gruppe mit der entsprechenden Berechtigung hinzufügen über die Plus Taste:

ESXI01 - Berechtigung hinzufügen

Wählen Sie links die Benutzer oder Gruppen und rechts die ihnen zuzuweisende Rolle aus.

Benutzer und Gruppen

Den unten aufgelisteten Benutzern oder Gruppen wird die rechts ausgewählte Rolle für 'ESXI01' zugewiesen.

Benutzer/Gruppe	Rolle	Weiter...
 LEIBLING...	Administr...	Ja

Hinzufügen... Entfern

Zugewiesene Rolle

Die Benutzer oder Gruppen erhalten die Berechtigungen für die ausgewählten Objekte, wie dies in der zugewiesenen Rolle definiert ist.

Administrator

- ✓ Alle Rechte
 - ✓ Alarme
 - ✓ Aufgaben
 - ✓ Berechtigungen
 - ✓ Datencenter
 - ✓ Datenspeicher
 - ✓ Datenspeicher-Cluster
 - ✓ Distributed Switch
 - ✓ ESX Agent Manager

Beschreibung: Alle Rechte

An untergeordnete Objekte weitergeben

[Untergeordnete Elemente anzeigen](#)

VCSA ans AD anbinden (SSO)

Die Einstellungen sehen dann wie folgt aus:

vmware vSphere Web Client | peter@LEIBLING.LOCAL | Hilfe

SSO-Konfiguration für 192.168.40.9

Richtlinien Identitätsquellen Zertifikate

Name	Server-URL	Typ	Domäne	Alias
--	--	--	vsphere.local	--
--	--	Lokales Betriebssystem	localos (Standard)	--
leibling.local	--	Active Directory (Integrie...	leibling.local	LEIBLING

vmware vSphere Web Client | peter@LEIBLING.LOCAL | Hilfe

vCenter-Benutzer und -Gruppen

Benutzer Anwendungsbenutzer Gruppen

Gruppenname	Domäne	Beschreibung
Users	vsphere.local	
SolutionUsers	vsphere.local	Well-known solution users' group, which con...
DCAadmins	vsphere.local	
ExternalIDPUsers	vsphere.local	Well-known external IDP users' group, which...
Administrators	vsphere.local	

Gruppenmitglieder

Benutzer/Gruppe	Beschreibung/Vollständiger Name	Domäne	Mitgliedstyp
Domänen-Admins	Domänen-Admins	leibling.local	Gruppe
Administrator	Administrator vsphere.local	vsphere.local	Benutzer

vmware vSphere Web Client | peter@LEIBLING.LOCAL | Hilfe

ESXI01 Aktionen

Erste Schritte Übersicht Überwachen Verwalten Verwandte Objekte

Einstellungen Alarmdefinitionen Tags Berechtigungen Sitzungen Speicheranbieter Geplante Aufgaben

Benutzer/Gruppe	Rolle	Definiert in
VSPHERE.LOCAL\Administrator	Administrator	Dieses Objekt und seine untergeordneten Ele...
root	Administrator	Dieses Objekt und seine untergeordneten Ele...
LEIBLING\Domänen-Admins	Administrator	Dieses Objekt und seine untergeordneten Ele...

VCSA ans AD anbinden (SSO)

Wenn nun noch der Host richtig im DNS angelegt ist und ein Zertifikat angelegt wurde, kann man ganz einfach sich mit seinem AD Account ohne Fehler- oder Hinweismeldungen direkt anmelden mit den Hostnamen.

Mit entsprechenden NAT Forwardern auch direkt übers Internet selber.

Weitere Informationen: <http://wahlnetwork.com/2013/09/09/using-active-directory-integrated-windows-authentication-sso-5-5/>