VMware ESXi in das Active Directory integrieren

ESXi in das Active Directory integrierenWenn ESXi-Hosts über vCenter verwaltet werden, dann erfolgt die Anmeldung zentral über die Management-Software, wobei der vCenter-Server in der Regel Mitglied in einer AD-Domäne ist. Auf diese Weise authentifizieren sich Benutzer über das AD und die Rechte in vSphere werden an AD-Konten vergeben. Seit ESXi 4.1 ist es aber zusätzlich möglich, auch die lokale Anmeldung am Host über das Active Directory laufen zu lassen.

Üblicherweise besteht nur selten die Notwendigkeit, sich direkt an einem Host anzumelden. Dies ist etwa in sehr kleinen Umgebungen der Fall, wo die virtualisierten Server einzeln administriert werden, oder wenn eine bestimmte Software nur bestimmte Hosts überwachen soll. Ein weiterer Anlass für das lokale Anmelden an ESXi kann das Troubleshooting sein.

Vereinfachtes User-Management

Ein Vorteil der AD-Integration besteht darin, dass man keine Passwörter für die lokalen root-Konten weitergeben oder auf jeder Maschine verschiedene Admin-Accounts pflegen muss. Das vereinfacht die Benutzerverwaltung, wenn beispielsweise ein IT-Mitarbeiter das Unternehmen verlässt. Dann verwehrt man ihm den Zugang zu allen ESXi-Servern, sobald man sein AD-Konto deaktiviert.

Bevor man mit einem ESXi-Rechner einer AD-Domäne beitritt, sind ein paar Voraussetzungen zu erfüllen. Dazu zählt, dass der Host über einen Full Qualified Domain Name (FQDN) verfügen muss. Zu diesem Zweck muss man seine Netzwerkeinstellungen editieren und den Namen der Domäne von jener übernehmen, der er beitreten soll. Bei diesem Vorgang kann man gleich auch noch den Hostname ändern (siehe dazu meine Anleitung).

Zeitsynchronisierung mit dem AD

Der nächste Schritt besteht darin, dass man die Zeit zwischen dem ESXi-Host und dem Domänen-Controller synchronisiert. Beide Seiten unterstützen das NTP-Protokoll, so dass es am einfachsten ist, einen DC als Zeit-Server für ESXi einzutragen.

Man kann einen DC als NTP-Server wählen, um die Systemzeit von ESXi mit dem AD zu synchronisieren.

Dies kann man im vSphere-Client in der Registerkarte Konfiguration unter `Software` ⇒ `Uhrzeitkonfiguration` tun. Dort findet sich rechts oben der Link Eigenschaften, der einen Dialog öffnet, in dem man die NTP-Einstellungen editieren und den NTP-Client starten kann.

NTP-Konfiguration via PowerCLI

Wer für solche Arbeiten PowerShell bevorzugt, kann den Zeit-Server mit Hilfe von PowerCLI eintragen. Wenn man sich über Connect-ViServer mit mehreren Hosts verbunden hat, dann trägt der folgende Aufruf den NTP-Server 192.168.0.100 in die Konfiguration aller ESXi-Server ein:

Get-VMHost -State Connected | Add-VmHostNtpServer -NtpServer „192.168.0.100“

Zu den weiteren Vorbereitungen gehört, dass man in die Netzwerk-Konfiguration des ESXi-Hosts einen DNS-Server einträgt, über dessen SRV-Eintrag er die Domain-Controller finden kann. In der Regel übernimmt der DNS-Dienst des Active Directory diese Aufgabe.

Benutzergruppe ESX Admins

Nicht zuletzt sollte man dann noch im AD eine Sicherheitsgruppe mit dem Namen ESX Admins anlegen. ESXi sucht nach dem Beitritt zu einer Domäne nach dieser Gruppe und räumt ihr automatisch administrative Rechte ein. Dieser Schritt ist nicht zwingend, weil man später auch jeder anderen Gruppe solche Privilegien gewähren kann.

Im vSphere Client 5.x kann man die vorgegebene Gruppe ESX Admins durch eigene AD-Gruppen ersetzen.

Im vSphere-Client 5.x besteht zudem die Möglichkeit, diesen vorgegebenen Gruppennamen zu ändern. Die dafür zuständige Einstellung findet man unter `Konfiguration ⇒ Software ⇒ Erweiterte Einstellungen ⇒ Config ⇒ HostAgent ⇒ plugins ⇒ hostsvc`. Wenn man hier beispielsweise Domänen-Admins eingibt, dann erhalten alle Mitglieder root-Privilegien auf den derart konfigurierten ESXi-Hosts, wenn sie der Domäne beitreten.

AD-Domäne beitreten im vSphere Client

Die eigentliche Integration in das AD erfolgt schließlich ebenfalls über den vSphere Client, und zwar wieder unter der Registerkarte `Konfiguration ⇒ Software ⇒ Authentifizierungsdienste`. Über den Link Eigenschaften kann man die Einstellungen bearbeiten und den vorgegebenen Eintrag Lokale Authentifizierung durch Active Directory ersetzen.

Wenn man alle nötigen Vorarbeiten erledigt hat, geht der eigentliche Beitritt zu einer AD-Domäne schnell über die Bühne.

Wie beim Domain Join eines Windows-Rechners gibt man hier den Domänennamen an und authentifiziert sich danach mit einem Konto, das für den Beitritt autorisiert ist.

Domain Join mittels PowerCLI

Auch hier besteht die Möglichkeit, anstelle des vSphere Clients die Kommandozeile zu wählen und den ESXi-Rechner mittels PowerCLI in die Domäne zu integrieren:

Get-VMHostAuthentication | Set-VMHostAuthentication -JoinDomain -Domain „mydomain.local“

Hier kann man bei Bedarf über den Parameter -VMHost nur bestimmte Server angeben.

Wenn man beim Beitritt zur AD-Domäne mit PowerCLI keine Anmeldedaten eingibt, kann man sich interaktiv authentifizieren.

Vergabe von Rechten an AD-User

Nach erfolgreichem Beitritt eines ESXi-Servers zu einer Domäne wird man anschließend Rechte an AD-User und -Gruppen vergeben. Dies erfolgt im vSphere Client unter der Registerkarte Berechtigungen. Dort bietet der Dialog Berechtigungen zuweisen die Option Hinzufügen, über die sich ein Auswahldialog für Benutzer und Gruppen öffnet. Dort sollte sich im Pulldown-Menü für die Domäne neben dem Eintrag (Server) auch die AD-Domain finden, deren Mitglied der Host nun ist.

Wie man von einer Enterprise-tauglichen Software wie ESXi erwarten kann, erlaubt sie ein differenziertes Rechte-Management. Sie lässt die Zuweisung von Lese- oder Schreibprivilegien zu einer Vielzahl von Funktionen und Einstellungen zu.

Eingabe der Anmeldeinformationen

Zum Schluss stellt sich noch die Frage, wie sich die zur ACL von ESXi hinzugefügten AD-User am System anmelden können. Relativ einfach geht es am vSphere Client, wo man nur die Checkbox Windows-Sitzungsanmeldedaten verwenden aktivieren muss. Möchte man sich mit einem anderen Konto anmelden oder verwendet man für den Host eine IP-Adresse, dann nimmt man wie gewohnt die Notation domain\username.

An der ESXi-Konsole funktioniert die Eingabe der Anmeldedaten so nicht. Vielmehr erwartet sie den Benutzernamen nach dem Muster username@domain. Das Gleiche gilt für den Zugriff über SSH, wo man ebenfalls diese Notation verwendet.