|  |  |
| --- | --- |
| **1** | **ESXi** |
|  |  |
| **1.1** | **Installation ESXi V6.5** |
|  | Hier immer die vom Hersteller des Servers (FTS,…) bereitgestellte ESXi-Version verwenden |
|  |  |
| **1.2** | **Datastore** |
|  | Speicher hinzufügen – Festplatte/LUN |
|  | =VMFS6 |
|  |  |
| **1.3** | **Netzwerk** |
|  |  |
| **1.3.1** | **Virtuelle Switches** |
|  | =vSwitch0: VMNetwork Portgruppe entfernen (ACHTUNG: SIEHE auch: 1.3.3) |
|  | =Virtuellen Standard-Switch hinzufügen, Name: paedML\_intern (vSwitch1) |
|  | =Virtuellen Standard-Switch hinzufügen, Name: paedML\_DMZ (vSwitch2) |
|  | =Virtuellen Standard-Switch hinzufügen, Name: paedML\_extern (vSwitch3) |
|  |  |
| **1.3.2** | **Portgruppen** |
|  | =Portgruppe hinzufügen: paedML\_intern, Auswahl Virtueller Switch: vSwitch1 |
|  | =Portgruppe hinzufügen: paedML\_DMZ, Auswahl Virtueller Switch: vSwitch2 |
|  | =Portgruppe hinzufügen: paedML\_extern, Auswahl Virtueller Switch: vSwitch3 |
|  |  |
| **1.3.3** | **Trennung Management-Network und Produktivnetzwerk** |
|  | Das LMZ fügt die Portgruppe paedML\_intern in seiner Anleitung zum Management-Network hinzu (Auswahl also nicht wie oben vSwitch1, sondern VSwitch0), erwähnt aber kurze Zeit später, dass empfohlen wird, Management-Network und Produktivnetz zu trennen…???!!!  Mit der o.g. Konfiguration (vSwitch 0-3) wäre die Trennung aktiviert |
|  |  |
| **1.4** | **Bereitstellung OVA** |
|  | Die bereitgestellten OVAs sind komprimiert und können nicht über die ESXi-GUI importiert werden. Lösung: Import über das VMWare ovftool. Nach Installation des MSI-Paketes zum Import der OVAs zum Speicherort der Vorlage wechseln, hier ein administratives Eingabefenster öffnen und die OVAs wie folgt importieren:  Allgemein:  <Pfad>\ovftool --disableVerification --noSSLVerify --datastore=<Datastore> --network="<Network>" gms1810.ova vi://root@<IP des ESXi> (alles eine Zeile) |
|  |  |
| **1.4.1** | **OVA Filr40** |
|  |  |
|  | ”C:\Program Files\VMware\VMware OVF Tool”\ovftool --acceptAllEulas --disableVerification --noSSLVerify –-datastore=PAEDML\_DATASTORE --diskMode="thin" --network="paedML\_DMZ" –-name=Filr4 filr40.ova vi://root@192.168.10.75 |
|  |  |
| **1.4.2** | **GMSServer** |
|  |  |
|  | ”C:\Program Files\VMware\VMware OVF Tool”\ovftool --acceptAllEulas --disableVerification --noSSLVerify –-datastore=PAEDML\_DATASTORE --diskMode="thin" --network="paedML\_DMZ" –-name=GMSServer gms1811.ova vi://root@192.168.10.75 |
|  |  |
| **1.4.3** | **GServer03** |
|  |  |
|  | ”C:\Program Files\VMware\VMware OVF Tool”\ovftool --acceptAllEulas --disableVerification --noSSLVerify –-datastore=PAEDML\_DATASTORE --diskMode="thin" --net:"bridged"="paedML\_intern" --net:"custom"="paedML\_DMZ" --name=GServer03 gserver03-44.ova vi://root@192.168.10.75 |
|  |  |
| **1.4.4** | **KServer** |
|  |  |
|  | ”C:\Program Files\VMware\VMware OVF Tool”\ovftool --acceptAllEulas --disableVerification --noSSLVerify –-datastore=PAEDML\_DATASTORE --diskMode="thin" --network="paedML\_DMZ" –-name=KServer kserver-vibe-406.ova vi://root@192.168.10.75 |
|  |  |
| **1.4.5** | **ZServer** |
|  |  |
|  | ”C:\Program Files\VMware\VMware OVF Tool”\ovftool --acceptAllEulas --disableVerification --noSSLVerify –-datastore=PAEDML\_DATASTORE --diskMode="thin" –-net:"bridged"="paedML\_intern" –-net:"custom"="paedML\_DMZ" –-name=ZServer ZServer.ova vi://root@192.168.10.75 |
|  |  |
|  | Achtung: Gem. Anleitung soll für den ZServer für eth0 „paedML\_intern“ und eth1 „pae3dML\_DMZ“ konfiguriert werden. Bei meiner Installation erkennt das ovftools für den ZServer allerdings nur eine Netzwerkkarte,d.h.: Der Import muss wie folgt durchgeführt werden: |
|  |  |
|  | ”C:\Program Files\VMware\VMware OVF Tool”\ovftool --acceptAllEulas --disableVerification --noSSLVerify –-datastore=PAEDML\_DATASTORE --diskMode="thin" --network="paedML\_intern" –-name=ZServer ZServer.ova vi://root@192.168.10.75 |
|  |  |
|  | Dies ist lt. Aussage LMZ ein Fehler des ovftools. Der Importierte Server enthält 2 Netzwerkkarten, über die ESXi-GUI kann nachträglich die zweite Netzwerkkarte auf paedML\_DMZ gesetzt werden |
|  |  |
| **2** | **Anpassung GServer03** |
|  |  |
| **2.1** | **Netzwerkkarten** |
|  |  |
|  | Netzwerkadapter 1: Adaptertyp: E1000 |
|  | Netzwerkadapter 2: Adaptertyp: E1000 |
|  |  |
|  | E1000 oder VMXNET3. Falls Sie eine 10 GB-Verbindung zum Switch betreiben, ist VMXNET3 nötig, um die volle Geschwindigkeit zu erreichen. |
|  |  |
| **2.2** | **Prozessor, RAM, Speicherplatz** |
|  |  |
|  | Kleinere oder kleine Schule:  1 CPU, 4 GB Arbeitsspeicher, 500 GB Festplattenspeicher |
|  |  |
|  | Große Schule, keine GroupWise -Verwendung:  2 CPUs, 8 GB Arbeitsspeicher,  1-2 TB Festplattenspeicher |
|  |  |
|  | Große Schule, GroupWise:  4 CPUs, 12-16 GB Arbeitsspeicher, 2-4 TB Festplattenspeicher |
|  |  |
|  | Mehrschulinstallation, GroupWise:  6-8 CPUs, 16-32 GB Arbeitsspeicher, 2-4 TB Festplattenspeicher |
|  |  |
|  | Die Festplattengröße kann nur verändert werden, wenn keine Snapshots aktiv sind! |
|  |  |
|  |  |
| **2.3** | **Automatisches Starten** |
|  | to be continued |
|  |  |
| **2.4** | **Passwort-Änderung** |
|  |  |
|  | Standard-PW paedML Novell:  =root: 54321  =admin: 12345 |
|  |  |
| **2.4.1** | **Passwort-Änderung User <root>** |
|  |  |
|  | =Login als root in Konsole |
|  | =Befehl: <passwd> |
|  |  |
| **2.4.2** | **Passwort-Änderung User <admin>** |
|  |  |
|  | =Login als root in Konsole |
|  | =Start grafische Oberfläche mit Befehl: init 5 |
|  | =Anmeldung als <root> |
|  | =Aufruf iManager <http://10.1.1.32/nps> und Anmeldung: |
|  |  |
|  | =Roles and Tasks – Users – Modify User |
|  |  |
|  |  |
|  | =Im Feld <Username> eintragen: <admin.server.dienste.ml3> und mit OK bestätigen |
|  | =Registerkarte <Restrictions> - <Password Restrictions>: Set Password |
|  | =Hierzu im erscheinenden FireFox-Fenster Pop-Ups erlauben |
|  |  |
| **2.4.3** | **Weitere Passwortänderungen für User** |
|  |  |
|  | Für folgende User ist nach obiger Vorgehensweise ebenfalls eine Passwortänderung notwendig: |
|  |  |
|  | = |
|  | = ldapuserfilr. server.dienste.ml3 |
|  | = proxyuserfilr. server.dienste.ml3 |
|  | =ldapuservibe. server.dienste.ml3 |
|  | =ldap2edirbinduser. server.dienste.ml3 |
|  | =ZCMDeploy-Zentral. server.dienste.ml3 |
|  | =ldapusergw. server.dienste.ml3 |
|  | =iPrintAdmin.System.Verwalter.DIENSTE.ml3 |
|  | =Installer.Installers.Verwalter.Benutzer.S01.SCHULEN.ml3 |
|  | =ZCMDeploy-S01.System.Verwalter.Benutzer.S01.SCHULEN.ml3. |
|  | = BenAdmin-S01.BenAdmins.Verwalter.Benutzer.S01.SCHULEN.ml3 |
|  | =PgmAdmin-S01.PgmAdmins.Verwalter.Benutzer.S01.SCHULEN.ml3 |
|  | = SchulAdmin-S01.SchulAdmins.Verwalter.Benutzer.S01.SCHULEN.ml3 |
|  | = SpechtB-S01.Lehrer.Benutzer.S01.SCHULEN.ml3 |
|  | = GrossA-S01.Klasse1a.Schueler.Benutzer.S01.SCHULEN.ml3 |
|  |  |
|  | Wird eine eigene Schule generiert:  =Installer.Installers.Verwalter.Benutzer.<Ihre Schule/Schulen>.SCHULEN.ml3 |
|  | =ZCMDeploy-<Schule>.System.Verwalter.Benutzer.<Schule>.SCHULEN.ml3 |
|  | = BenAdmin, PgmAdmin, SchulAdmin sowie für die Benutzer SpechtB- und GrossA-<Schule>. |
|  |  |
| **2.4.4** | **Passwortänderungen in den Dateien <admin.conf> und ggfs. <edirauth.conf>** |
|  |  |
|  | =Konsolenbefehl: vim /etc/apache2/conf.d/admin.conf |
|  | =Anpassung Zeile <AuthLDAPBindPassword> mit dem Passwort für <ldap2edirbinduser> |
|  | =VIM beenden: <:wq!> |
|  |  |
|  | Wird als Intranetseite für das Kollegium eine andere Schule als die S01 eingesetzt, so muss in der Datei edirauth.conf in /etc/apache2/conf.d auch noch in der Zeile  AuthLDAPURL "ldaps://gserver03.oes.ml-bw.de/ou=Lehrer,ou=Benutzer,ou=S01,ou=SCHULEN,o=ml3?cn?sub"  S01 durch das entsprechende Schulkürzel ersetzt werden. Auch hier muss für  <AuthLDAPBindPassword "12345">  <12345> durch das entsprechende Directory-Passwort für <ldap2edirbinduser> ersetzt werden. |
|  |  |
|  | Nach den Änderungen ist ein Apache Neustart mit < systemctl restart apache2.service> notwendig |
|  |  |
| **2.4.5** | **Passwort inetlockuser setzen** |
|  |  |
|  | = http:/10.1.1.32:54080/tasks |
|  | =Anmeldung als <admin> |
|  | =Ordnerinhalt |
|  | =inetlockuser-setpwd.html |
|  | =Passwort für <admin> eingeben |
|  | =Neues Passwort erzeugt und im eDirectory eingetragen |
|  |  |
| **3** | **vhost-ssl.conf** |
|  |  |
|  | Setzen Sie Vibe und/oder Filr mit Zugriff von außen ein? Benötigen Sie vertrauenswürdige Zertifikate? Wollen Sie mit einer einzigen, offiziellen IP-Adresse von außen verschiedene Dienste erreichen? Die dazu nötigen Vorarbeiten sind bereits in der Datei /etc/apache2/vhost.d/vhost-ssl.conf enthalten. Sie müssen allerdings ggf. schulspezifisch angepasst werden. Alle dazu notwendigen Informationen finden Sie im beiliegenden Dokument Zertifikate-Anleitung.pdf. |
|  |  |
| **4** | **NSS-Pool anpassen / Datenverzeichnis** |
|  |  |
|  | =iManager starten und als <admin> an <schulbaum03> anmelden |
|  | =Auswahl: <Storage> - <Pools> |
|  | =Servereintrag: <gserver03.server.dienste.ml3> |
|  | =Mit <Enter> bestätigen |
|  | =Über die Schaltfläche <Increase size> kann die Größe des Datenverzeichnisses bis zur Grenze des unter <2.2 Prozessor,RAM, Speicherplatz> angegebenen Wertes für die zweite Festplatte erhöht werden. |
|  |  |
|  | **!!!Die Anpassungen sind sofort wirksam und können nicht rückgängig gemacht werden!!!** |
|  | **Wichtiger Hinweis: Erweitern Sie niemals den NSS-Pool auf den eventuell noch frei verfügbaren Speicherplatz des Systemlaufwerks (1. Platte, sda). Systeminstabilitäten, die dadurch verursacht werden, können von der Hotline nicht behoben werden!**  **Eine Empfehlung zur Größe eines NSS-Pools ist stark abhängig von der Anzahl der Benutzer des Systems und des Nutzerverhaltens in der Schule. Bevor Sie den NSS-Pool vergrößern, schätzen Sie den Speicherbedarf Ihrer Schule ab. Die typische Größe eines NSS-Pools einer mittleren Berufsschule beträgt z.B. 2 Terabyte. Bei Bedarf kann dieser erweitert werden. Technisch ist die Größe des NSS-64-Pools auf max. 8 Exabyte begrenzt, abhängig von dem vom ESXi-Host, je nach Version, zur Verfügung gestellten (VMFS-) Dateisystems.** |
|  |  |
|  |  |
| **5** | **VMWare-Tools installieren** |
|  |  |
|  |  |
|  |  |
|  |  |
| **6** | **Internetsperre für Admin-PC aufheben** |
|  |  |
|  | IP-Admin-PC\_ 10.1.254.1 (Wieso/weshalb/warum??? Keine Fundstelle in der Doku) |
|  |  |
|  | Anpassung der Datei: /var/lib/inet/htdocs/isp/intranetausnahmen.acl mit einem Editor (vi) |
|  |  |
|  | *ACHTUNG: Wie ist ein sehr „spezieller“ Editor. Nachfolgend eine Übersicht der wichtigsten vi-Befehle:* |
|  |  |
|  | *i: Startet den „Insert Modus“ ESC: Beendet den „Insert Modus“, jetzt können weitere Befehle eingegeben werden:  Text bearbeiten*  *w – Springt zum Anfang des nächsten Wortes B – Springt zum Anfang des letzten Wortes e – Springt zum Ende des nächsten Wortes G – Springt zum Ende der Datei x – Löscht das aktuelle Zeichen 5x – Löscht die nächsten 5 Zeichen (andere Zahlen möglich!) dd – Löscht die ganze Zeile (und kopiert sie in den Speicher) u – Undo: Macht die letzte Änderung rückgängig . – Redo: Wiederholt die letztee Änderung   Datei bearbeiten*  *:q – vi beenden :q! – vi beenden ohne speichern :w – Datei speichern :wq – Datei speichern und vi beenden*  *Suchen + Zeilennummern*  */Suchwort – Sucht nach “Suchwort” Richtung Dateiende ?Suchwort – Sucht nach “Suchwort” Richtung Dateianfang n – Sucht die nächste Fundstelle in Suchrichtung*  *Zum Einschalten der Zeilennummern gibt man im Command-Modus den Befehl “set number” (ohne Doppelpunkt vorher) ein. Zum Ausschalten der Zeilennummern gibt man, ebenfalls im Command Modus, den Befehl “set nonumber” ein.*  *Um direkt zu einer Zeile springen zu können, gibt man einen Doppelpunkt und die Zeile an: “:429” (ohne Anführungszeichen) – so springt man direkt zur 429. Zeile im Text.* |
|  |  |
|  | =Konsolenbefehl: vi /var/lib/inet/htdocs/isp/intranetausnahmen.acl |
|  | =Eintrag: 10.1.254.1/32 |
|  | =Falls nicht vorhanden: Am Ende der Datei eine Leerzeile einfügen, sonst kann die Liste vom System nicht verarbeitet werden |
|  |  |
|  | Abschließend müssen folgende Dienste neu gestartet werden: |
|  |  |
|  | =systemctl restart inetsperre.service |
|  | =systemctl restart apache2.service |
|  | =systemctl restart squid.service |
|  |  |
|  |  |
|  |  |
|  |  |