Best Practice Guideline

VMware Infrastructure 3.5 Security

Kunde:
<Kunde>

Autor:
Thomas Reichenberger

Version:
1.2

Datum:
Sonntag, 10. August 2008

ACP CompetenceCenter Virtualisierung

Inhaltsverzeichnis

1 Organisatorische Maßnahmen

1.1 Security Policy

Die übergeordneten Sicherheitsanforderungen sind in einem organisationsübergreifendem Sicherheitskonzept zu regeln.

1.2 Namens Konventionen

Eindeutige Namenskonventionen sind für einen reibungslosen IT Betrieb und zur Vermeidung falscher Bedienung durch Verwechslung unbedingt notwendig.

1.3 Aktuelle Dokumentation

Die aktuelle Konfiguration ist vollständig zu dokumentieren. Diese Dokumentation ist stets zu aktualisieren sobald Änderungen in der Systemkonfiguration vorgenommen werden.

1.4 Separation of Duties

Eine Funktionstrennung ist in der Systemadministration so weit wie möglich umzusetzen.

1.5 Physischer Zugriff

Alle physischen Server sind in einem zutrittsbeschränkten und zutrittskontrollierten Bereich aufzustellen. Der Zugang zu den Systemen ist auf die mit der Systemadministration beauftragten Personen zu beschränken.

2 Technische Umsetzung

2.1 Härten der ESX Service Console

Die Service Console des VMware ESX Server basiert auf einer angepassten Redhat Enterprise Linux 3 Distribution, ist jedoch nicht mit dieser identisch.

2.1.1 Firewall Settings auf ESX

In der Service Console des VMware ESX Servers ist eine einfache Firewall integriert. Diese Firewall ist bereits per Default gehärtet, so dass nur benötigt Dienste und Ports per Default freigeschalten sind.

2.1.1.1 Überprüfung der Firewall Konfiguration

Über folgenden Befehl kann die Firewall Konfiguration ausgelesen werden.

```
# esxcfg-firewall -q
```

2.1.1.2 Firewall Default Settings

Per Default ist bereits der gesamte ausgehende und eingehende Netzwerkverkehr blockiert. Diese Einstellung kann auch nachträglich geändert werden.

Folgender Befehl blockiert den gesamten ausgehenden Netzwerkverkehr, ausgenommen der explizit freigeschalten Dienste und Ports.

```
# esxcfg-firewall --blockOutgoing
```

Folgender Befehl blockiert den gesamten eingehenden Netzwerkverkehr, ausgenommen der explizit freigeschalten Dienste und Ports.

```
# esxcfg-firewall --blockIncoming
```

2.1.1.3 Dienste

Alle nicht benötigten Dienste sind zu deaktivieren. Alle für die Funktion benötigten Dienste sind einzeln zu aktivieren.

Aktiviren eines Dienstes

```
# esxcfg-firewall –e [Name_des_Dienstes]
```

Deaktivieren eines Dienstes

```
# esxcfg-firewall –d [Name_des_Dienstes]
```

2.1.1.4 Spezielle Ports aktivieren und deaktivieren

Alle für die Funktion benötigten speziellen Ports sind einzeln zu aktivieren.

Öffnen eines Ports

```
# esxcfg-firewall –o [port],[protocol],[direction],[name]
```

Schließen eines Ports

```
# esxcfg-firewall -c [port],[protocol],[direction
```

2.1.1.5 Beschreibung der Befehle

Kommando	Beschreibung
`esxcfg-firewall -s`	listet alle bekannten Dienste auf
`esxcfg-firewall -q`	zeigt die aktuelle Konfiguration der Firewall
`esxcfg-firewall -e ntpClient`	öffnet den Port für den NTP Dienst für ausgehende Verbindungen
`esxcfg-firewall -e smbClient`	öffnet den Port für den SMB (CIFS) Dienst für ausgehende Verbindungen
`esxcfg-firewall -d smbClient`	schließt den Port für den SMB (CIFS) Dienst für ausgehende Verbindungen
`esxcfg-firewall --allowIncoming --allowOutgoing`	Setzt die Firewall auf „Low“ level security
`esxcfg-firewall --blockIncoming --allowOutgoing`	Setzt die Firewall auf „Medium“ level security
`esxcfg-firewall --blockIncoming --blockOutgoing`	Setzt die Firewall auf „High“ level security
`esxcfg-firewall -o [port],[protocol],[direction],[name]`	öffnet einen bestimmten Port
`esxcfg-firewall -c [port],[protocol],[direction]`	schließt einen bestimmten Port

2.1.2 TCP Wrapper

2.1.2.1 Beschreibung

Im inetd Dienst selbst sind keinerlei Sicherheitsmechanismen implementiert. Deswegen wurde ein Filter geschaffen, der sich zwischen den inetd und den zu startenden Dämonen spannt. Der inetd startet nun nicht mehr den für den Port zuständigen Dienst, sondern den so genannten TCP-Wrapper »tcpd«, der den Programmnamen des Dienstes als Argument erhält.

In den Dateien /etc/hostsallow und /etc/hosts.deny werden explizit erlaubte und nicht erlaubte Hosts festgelegt. Dabei wird geregelt welche Hosts diesen inetd Dienst nutzen dürfen.

2.1.2.2 Hosts.allow

Einträge in die /etc/hosts.allow

Beispiel um nur Zugriffe aus den Subnetzen 192.168.22.0/24 und 192.168.55.0/24 zu erlauben.

```
ALL:192.168.22.
ALL:192.168.55.
```

2.1.2.3 hosts.deny

Einträge in die /etc/hosts.deny

Beispiel um Zugriffe aus allen sonstigen Netzwerken zu verbieten:

```
ALL:ALL
```

2.1.3 ADS Authentifizierung

2.1.3.1 Beschreibung und Konfiguration

Folgender Befehl muss auf dem ESX 3.x Host eingegeben werden um Active Directory Authentifizierung einzuschalten.

```
# esxcfg-auth --enablead --addomain [domainname] --addc [dc name]
```

Folgende Dateien werden dabei angepasst bzw. erzeugt:

```
krg5.conf, kdc.conf, pam.d
```

Konfigurationsdatei anzeigen:

```
# cat /etc/krb5.conf
```

Konfiguration anzeigen:

```
# esxcfg-auth -p
```

AD Zugriff ausschalten:

```
# esxcfg-auth --disablead
```

2.1.3.2 Benutzer

Zusätzlich muss für jeden Benutzer der auf den ESX Server zugreifen soll ein Linux Account auf dem Host eingerichtet werden. Der Benutzername muss dabei dem Account in der Active Directory entsprechen.

Hinzufügen von Benutzern

```
# useradd [username]
```

2.1.3.3 Administratoren Gruppe

Um die Zugriffe einfacher zu steuern ist eine Benutzergruppe für die Administratoren einzurichten.

Hinzufügen einer neuen Gruppe

```
# groupadd [groupname]
```

2.1.3.4 Gruppen Zuordnung

Die Benutzer müssen dann noch der Administratorengruppe zugeordnet werden.

Benutzer zur Gruppe hinzufügen

```
# usermod -G [groupname] [username]
```

2.1.3.5 Umgebung setzen

Damit die neuen Benutzer die administrativen Befehle ausführen können muss noch die Systemumgebung angepasst werden.

In der Datei /home/[username]/.bash_profile jedes Benutzers sind die Pfade durch folgenden Pfad zu ersetzen:

```
PATH=$PATH:$HOME:/bin:/usr/local/sbin:/sbin:/usr/sbin
```

2.1.4 Passwortrichtlinie

Die Passwortrichtlinie für lokale Accounts in der Service Console ist ebenfalls über den esxcfg-auth Befehl zu beschränken.

2.1.4.1 Passwort-Standardverwendungsdauer

- Änderung der Höchstanzahl von Tagen, die ein Anwender sein Passwort behalten kann:

```
# esxcfg-auth --passmaxdays=[Anzahl_von_Tagen]
```

wobei [Anzahl_von_Tagen] die Höchstanzahl von Tagen vor Ablauf des Passworts ist.

- Änderung der Mindestanzahl von Tagen zwischen zwei Passwortänderungen:

```
# esxcfg-auth --passmindays=[Anzahl_von_Tagen]
```

wobei < Anzahl_von_Tagen] die Mindestanzahl von Tagen zwischen zwei Passwortänderungen ist.

- Änderung der Hinweiszeit vor einer Passwortänderung:

```
# esxcfg-auth --passwarnage=[Anzahl_von_Tagen]
```

wobei [Anzahl_von_Tagen] die Anzahl der Tage ist, die ein Anwender vor dem Auslaufen eines Passworts Warnhinweise erhält.

2.1.4.2 Fehlgeschlagene Anmeldeversuche

Änderung der Anzahl von fehlgeschlagenen Anmeldeversuchen bis die aktive Sitzung beendet wird.

```
# esxcfg-auth --maxfailedlogins=[Anzahl]
```

wobei [Anzahl] die Anzahl der fehlgeschlagenen Anmeldeversuche ist.

2.1.4.3 Passwortkomplexität

Änderung der Standardkomplexität von Passwörtern für das Plug-In pam_cracklib.so

```
# esxcfg-auth --usecrack=[Versuche] [Mindestlänge] [KB_Bonus] [GB_Bonus]
[Z_Bonus] [AZ_Bonus]
```

Wobei:
[Versuche] die Anzahl der Wiederholungsversuche ist, die der Anwender hat, bis ESX Server ihn aus dem Passwortänderungsmodus ausschließt.

[Mindestlänge] ist die Mindestanzahl von Zeichen, die ein Anwender eingeben muss, damit das Kennwort angenommen wird. Diese Anzahl ist die Gesamtlänge vor der Anwendung jeglicher Zeichenboni.
Es wird immer mindestens ein Zeichenbonus angewendet, daher ist die Passwortlänge effektiv ein Zeichen kürzer als im Parameter Mindestlänge angegeben. Da pam_cracklib.so nur Passwörter mit mindestens 6 Zeichen annimmt, muss der Mindestlänge-Parameter so berechnet werden, dass die Passwortlänge nach Abzug der Zeichenboni nicht kleiner als 6 sein kann.

[KB_Bonus] ist die Anzahl von Zeichen, um die der Parameter Mindestlänge verringert wird, wenn im Passwort mindestens ein Kleinbuchstabe enthalten ist.

[GB_Bonus] ist die Anzahl von Zeichen, um die der Parameter Mindestlänge verringert wird, wenn im Passwort mindestens ein Großbuchstabe enthalten ist.

[Z_Bonus] ist die Anzahl von Zeichen, um die der Parameter Mindestlänge verringert wird, wenn im Passwort mindestens eine Ziffer enthalten ist.

[AZ_Bonus] ist die Anzahl der Zeichen, um die der Parameter Mindestlänge verringert wird, wenn der Anwender mindestens ein Sonderzeichen wie z. B. einen Unterstrich oder einen Bindestrich verwendet.
Geben Sie die Zeichenbonus-Parameter als positive Zahl oder, wenn der Anwender keinen Bonus für diese Zeichenklasse erhalten soll, als „0" an. Die Zeichenboni werden addiert. Je mehr verschiedene Zeichenarten der Anwender eingibt, desto weniger Zeichen sind notwendig, um ein gültiges Passwort zu erstellen.
Beispiel:

```
# esxcfg-auth --usecrack=3 11 1 1 1 2
```

Mit dieser Einstellung benötigt ein Anwender, der ein Passwort aus Kleinbuchstaben und einem Unterstrich erstellt, acht Zeichen, um ein gültiges Passwort zu erstellen. Wenn der Anwender hingegen alle Zeichenarten (Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen) einfügt, benötigt er nur sechs Zeichen.

2.1.4.4 Empfohlene Passwortrichtlinie

Folgende Passwortrichtlinie ist zu verwenden um einen einfachen Grundschutz umzusetzen.

```
# esxcfg-auth --passmaxdays=90
# esxcfg-auth --passmindays=1
# esxcfg-auth --passwarnage=10
# esxcfg-auth --maxfailedlogins=3
# esxcfg-auth --usecrack=3 11 1 1 1 2
```

2.1.5 su & sudo

Wenn Systemadministratoren sich auf dem Host anmelden, um Vorgänge auszuführen, für die Root- Privilegien notwendig sind, sollten Sie sich zuerst als normaler Anwender auf der Servicekonsole anmelden und dann über den Befehl su oder den zu bevorzugenden Befehl sudo als Root anmelden.
Der Befehl sudo erhöht die Sicherheit, da er nur für bestimmte, ausgewählte Vorgänge Root-Privilegien gewährt, während su Root-Privilegien für alle Vorgänge gewährt. Durch sudo sind außerdem alle Vorgänge besser nachvollziehbar, da alle sudo Vorgänge protokolliert werden, wohingegen bei su, der ESX Server nur protokolliert wird, dass der Anwender durch su auf Root umgeschaltet hat.

2.1.5.1 su

Der Befehl su macht durch Anwenderwechsel aus einem allgemeinen Anwender einen Root-Anwender.

```
# su -
```

2.1.5.2 sudo

Systemadministratoren für ESX Server sollten sich nur als normale Anwender anmelden und dann sudo verwenden, um bestimmte Aufgaben, die Root-Privilegien erfordern, auszuführen.

Die Sudo Konfiguration wir in der Datei /etc/sudoers durchgeführt. Über den visudo Befehl können Veränderungen in der /etc/sudoers gemacht werden.

```
# visudo
```

Folgender Test wird dabei in die Datei eingetragen:

```
%[groupname]         ALL=(ALL)        ALL
```

2.1.6 SSH Beschränkung

In der SSHD Konfigurationsdatei /etc/ssh/sshd_config können Anpassungen gemacht werden. Folgende Default Einstellungen sollten dabei nicht geändert werden.

```
Protocol 2
SyslogFacility AUTH
LogLevel VERBOSE
PermitRootLogin no
Subsystem       sftp    /usr/libexec/openssh/sftp-server
Ciphers aes256-cbc,aes128-cbc
```

Der sshd Dienst muss nach einer Änderung der Konfigurationsdatei neu gestartet werden:

```
# service sshd restart
```

2.1.7 Zertifikate

Virtual Center und ESX Server benutzen per Default selbstsignierte Zertifikate. Diese Zertifikate sind durch Zertifikate von einer vertrauenswürdigen Zertifizierungsstelle zu ersetzen.

2.1.7.1 OpenSSL Client

Um ein Certificate-Signing Request zu erzeugen muss zuerst ein OpenSSL Client installiert werden. Für den OpenSSL Client unter Windows ist zudem Visual C++ 2008 erforderlich.

Win32 OpenSSL Download Link:
http://www.slproweb.com/products/Win32OpenSSL.html

Visual C++ 2008 Redistributable Download Link:
http://www.microsoft.com/downloads/details.aspx?familyid=9B2DA534-3E03-4391-8A4D-074B9F2BC1BF

2.1.7.2 Certificate-Signing Request Erzeugen

Für den Virtual Center Server und jeden ESX Server muss ein Certificate-Signing Request durchgeführt werden.

```
C:\> cd \OpenSSL\bin
C:\OpenSSL\bin> openssl req -new -nodes -out [Server_Name].csr -config
openssl.cfg
```

wobei [Server_Name] der FQDN Name des Servers ist. Bei der Frage nach dem „commonName" muss ebenfalls der FQDN Name des Servers eingegeben werden.

Folgende Dateien werden dabei erzeugt:

`[Server_Name].csr`	Certificate-Signing Request Datei
`privkey.pem`	Private Key Datei

2.1.7.3 Zertifikat anfordern

Mit der erzeugten CSR-Datei kann nun von einer vertrauenswürdigen CA ein Zertifikat angefordert werden. Es wird dabei von der CA eine CRT-Datei (Zertifikat) erzeugt. Die neue Datei sollte dabei `[Server_Name].crt` benannt werden.

`[Server_Name].crt`	Serverzertifikat

2.1.7.4 ESX Server Zertifikat

Das Zertifikat und der Privat Key auf dem ESX Server können jetzt ausgetauscht werden.

Speicherort der Zertifikate auf dem ESX Server:

```
/etc/vmware/ssl/
```

Name der Zertifikats-Dateien auf dem ESX Server:

`rui.crt`	Server Zertifikat
`rui.key`	Private Key Datei

Backup der alten Zertifikat Dateien

```
# mv rui.crt rui.crt.bk
# mv rui.key rui.key.bk
```

Die Private-Key-Datei privkey.pem und das Serverzertifikat [Server_Name].crt auf den ESX Server in das Verzeichnis /etc/vmware/ssl kopieren.

Zertifikat-Dateien umbenennen

```
# mv [Server_Name].crt rui.crt
# mv privkey.pem rui.key
```

Server Dienst neu starten

```
# service mgmt-vmware restart
```

2.1.7.5 Virtual Center Zertifikat

Für den Virtual Center Server muss zusätzlich eine PFX-Datei erzeugt werden.

```
c:\> type [Server_Name].crt privkey.pem > all.pem
c:\> cd \OpenSSL\bin
c:\OpenSSL\bin> openssl pkcs12 -export -in all.pem -out rui.pfx
```

Speicherort der Zertifikate auf dem Virtual Center Server:

```
C:\Documents and Settings\All Users\Application Data\VMware\VMware
VirtualCenter\SSL\
```

Name der Zertifikats-Dateien:

`rui.crt`	Server Zertifikat
`rui.key`	Private Key Datei
`rui.pfx`	Private Key Datei (pkcs Format)

Backup der alten Zertifikat Dateien

```
c:\> cd Documents and Settings\All Users\Application Data\VMware\VMware
VirtualCenter\SSL\
c:\....\SSL\> move rui.crt rui.crt.bk
c:\....\SSL\> move rui.key rui.key.bk
c:\....\SSL\> move rui.pfx rui.pfx.bk
```

Die Private-Key-Dateien privkey.pem, rui.pfx und das Serverzertifikat [Server_Name].crt auf den Virtual Center Server in das Verzeichnis `c:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL\` kopieren.

Zertifikat-Dateien umbenennen

```
c:\....\SSL\> move [Server_Name].crt rui.crt
c:\....\SSL\> move privkey.pem rui.key
```

Virtual Center Server Dienst neu starten.

2.1.7.6 Clients

Auf allen Clients muss, wenn nicht vorhanden, das RootCA Zertifikat installiert werden. Bei einem erneuten Verbindungsaufbau des VMware Infrastructure Clients zum ESX Server oder Virtual Center Server wird nun keine Zertifikatswarnung mehr angezeigt.

2.1.8 Management Netzwerk Isolierung

Das zur Administration über das Service Consolen Interface verwendete Management Netzwerk ist von Virtuellen Maschinen Netzwerken zu isolieren.

2.1.9 File System

Folgende File System Berechtigungen sind umzusetzen.

Dateien und Verzeichnisse	Berechtigungen
/etc/fstab	640
/etc/group	644
/etc/host.conf	640
/etc/hosts	640
/etc/hosts.allow	640
/etc/hosts.deny	640
/etc/logrotate.conf	640
/etc/logrotate.d/	700
/etc/modules.conf	640
/etc/motd	640
/etc/ntp	755
/etc/ntp.conf	644
/etc/pam.d/system-auth	644
/etc/profile	644
/etc/shadow	400
/etc/securetty	600
/etc/ssh/sshd_config	600
/etc/snmp	755
/etc/sudoers	440
/etc/vmware	755

2.1.10 USB Geräte

Per Default werden USB Geräte und Massenspeicher beim Start des ESX Servers automatisch erkannt und eingebunden.
Diese Funktion kann in der Datei /etc/modules.conf deaktiviert werden.

```
# alias usb-controller usb-uhci
# alias usb-controller1 ehci-hcd
```

2.1.11 Zeitsynchronisierung

Eine Zeitsynchronisierung ist auch wichtig um sicherzustellen, dass Einträge in die Log-Dateien mit dem richtigen Zeitstempel versehen sind.

Beschreibung der Konfiguration einer automatischen Zeitsynchronisierung.

2.1.11.1 Datei /etc/ntp.conf bearbeiten

Erstellung einer Sicherheitskopie von ntp.conf

```
# cp /etc/ntp.conf /etc/ntp.conf.bk
```

Den Inhalt von /etc/ntp.conf durch folgenden Text ersetzen:

```
restrict default kod nomodify notrap
restrict 127.0.0.1
server 0.de.pool.ntp.org
server 1.de.pool.ntp.org
server 2.de.pool.ntp.org
server 3.de.pool.ntp.org
driftfile /etc/ntp/drift
```

2.1.11.2 Datei /etc/ntp/step-tickers bearbeiten

Erstellung einer Sicherheitskopie von /etc/ntp/step-tickers

```
# cp /etc/ntp/step-tickers /etc/ntp/step-tickers.bk
```

Den Inhalt von /etc/ntp/step-tickers durch folgenden Text ersetzen:

```
0.de.pool.ntp.org
1.de.pool.ntp.org
2.de.pool.ntp.org
3.de.pool.ntp.org
```

2.1.11.3 Firewall Einstellungen

Den Port des NTP Dienstes auf der lokalen Firewall freischalten.

```
# esxcfg-firewall -e ntpClient
```

2.1.11.4 NTP Dienst starten

Den ntpd Dienst auf der Service Console starten / restarten.

```
# service ntpd restart
```

2.1.11.5 NTP Dienst Autostart

Konfiguration eines Autostarts des ntpd Dienstes bei einem Reboot des Servers.

```
# chkconfig --level 345 ntpd on
```

2.1.11.6 Synchronisierung der Hardware Uhr

Hardware Uhr des Servers regelmäßig synchronisieren.

```
# hwclock --systohc
```

2.1.11.7 NTP Monitoring

Offset (in Sekunden) zwischen der local clock und einem Zeitserver überprüfen:

```
# ntpdate -q 0.de.pool.ntp.org
```

Monitoring des ntpd Dienstes. Nach ca. 5 Minuten setzt die automatische Synchronisierung ein.

```
# watch 'ntpq -p;echo;ntptrace'
```

2.2 Virtual Center Berechtigungskonzept

Dieses VirtualCenter Berechtigungskonzept sieht vor, dass globale Berechtigungsgruppen und Benutzeraccounts in lokale Ressourcengruppen verschachtelt werden. Ressourcengruppen können dann über VirtualCenter Rollen auf Objekte berechtigt werden.

2.2.1 Ressourcengruppen Mitglieder Matrix

In diesem Beispiel für ein Virtual Center Berechtigungskonzept werden Benutzergruppen und User Accounts in Ressourcengruppen verschachtelt.

Name	**Beschreibung**	**Mitglieder**								
		Hans Huber	Dietmar Dober	Thomas Fiedl	Franz Fichtner	Sabine Schröder	Help Desk User Gruppe	Backup Account		
DL_VirtualCenter_FullAdmin	Full Administrator auf VirtualCenter	x	x							
DL_VirtualCenter_WinVMs	Windows VMs in VirtualCenter				x	x	x			
DL_VirtualCenter_LinuxVMs	Linux VMs in VirtualCenter			x	x	x				
DL_VirtualCenter_Backup	VCB Datensicherung von Virtuellen Maschienen							x		

2.2.2 Rollen

Beschreibung der verwendeten VirtualCenter Rollen

Kürzel	Rolle	Beschreibung
A	Administrator	Original Administrator Rolle mit allen Berechtigungen
S	ACP Standard Admin	Original Administrator Rolle ohne Berechtigungen auf Netzwerk und Datastores
R	ACP Read-Only Admin	Original Read-Only Rolle
B	ACP VCB	Original VMware Consolidated Backup Rolle

2.2.3 VirtualCenter Berechtigungen Matrix

Zuordnung von Ressourcengruppen mit VirtualCenter Rollen auf VirtualCenter Objekte. Für die VirtualCenter Rollen werden deren Kürzel in die Matrix eingetragen.

Virtual Center Objekt	**Ressourcengruppen Virtual Center Rollen**							
	DL_VirtualCenter_FullAdmin	DL_VirtualCenter_WinVMs	DL_VirtualCenter_LinuxVMs	DL_VirtualCenter_Backup				
Host & Clusters	**A**							
Virtual Machine Folder Windows Server		**S**						
Virtual Machine Folder Linux Server			**S**					
Host & Clusters				**B**				

2.3 Überwachung

2.3.1 Zentrales Logging

Für eine zentrale Protokollierung der ESX Server kann ein Syslog Server verwendet werden.

Dafür muss in der Datei /etc/syslog.conf folgender Eintrag in der ersten Zeile gemacht werden:

```
*.*     @172.17.230.20
```

Zusätzlich muss in der lokalen ESX Firewall ein Port durch folgenden Befehl freigeschalten werden:

```
# esxcfg-firewall -o 514,udp,out,Syslog_Server
```

Der lokale Syslog Dienst muss neu gestartet werden

```
# service syslog restart
```

2.3.2 SNMP Monitoring

In der /etc/snmp/snmpd.conf Datei wird die Konfiguration des snmpd Dienstes festgelegt.

Beispiel:

```
rocommunity       public      [monitoring_host]
trapcommunity     public
trapsink                      [monitoring_host]
syscontact                    [administrator_name]
syslocation                   [room]
```

Starten des SNMP Dienstes

```
# service snmpd start
```

Autostart Konfiguration des Dienstes

```
# chkconfig --level 345 snmpd on
```

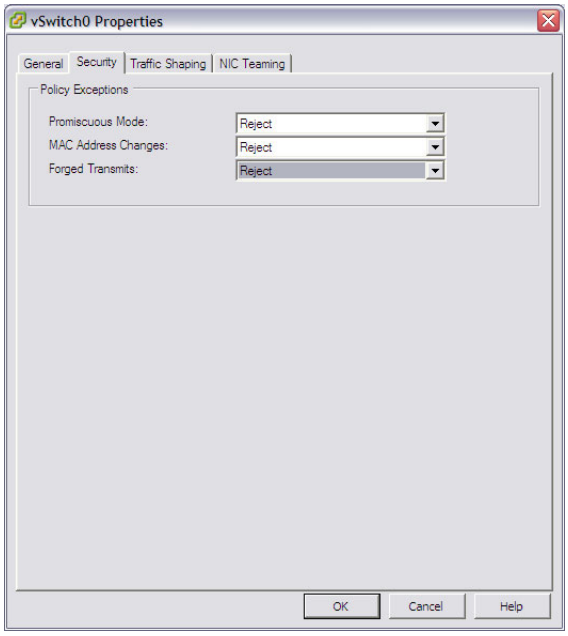
2.4 Layer 2 Security Option auf ESX

Für jeden virtuellen Switch müssen folgende Layer 2 Security Einstellungen durchgeführt werden.

VI Client -> Host auswählen -> Configuration -> Networking

Für jeden einzelnen vSwitch muss die Konfiguration angepasst werden

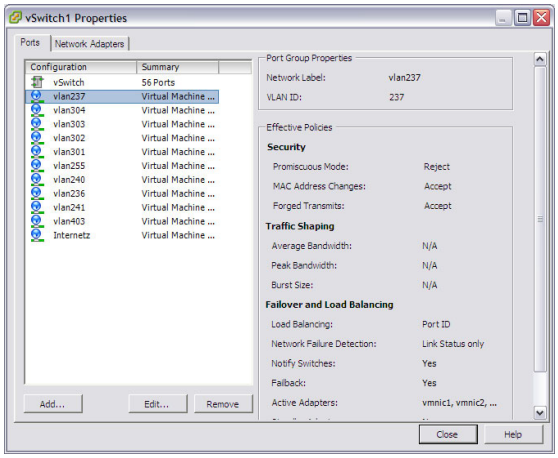
Properties des vSwitch -> „Ports" Tab -> vSwitch auswählen -> „Edit" Button -> „Security" Tab



Es ist darauf zu achten dass bei keiner Port Group die Sicherheitseinstellungen des Switches ausgehebelt werden

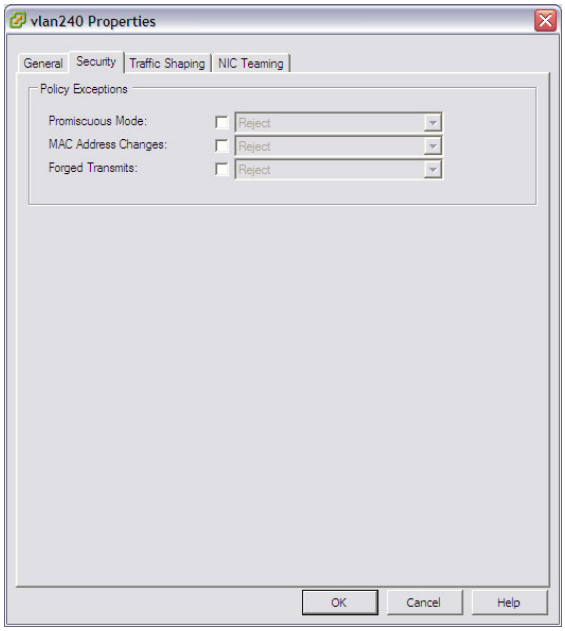
Properties des vSwitch -> „Ports" Tab

Für jede Virtual Machine Port Group z.B.: „vlan217"



die Security Einstellungen überprüfen:

„Edit" Button -> „Security" Tab



2.5 Management Interface

Der Zugriff über Remote Management Interfaces wie z.B.: HP ILO auf die Server ist genauso zu beschränken wie der physische Zugriff auf die Server.

2.6 Storage Network Security

2.6.1 iSCSI SAN

Das iSCSI Netzwerk ist von den Virtuellen Maschinen Netzwerken zu isolieren.
Für den Zugriff auf das iSCSI Storage ist eine CHAP Authentifizierung zu verwenden.

2.6.2 Fibre Channel SAN

Security im Fibre Channel Netzwerk und des SAN Storage Systems sind nicht Bestandteil dieses Dokuments.

2.7 Sichere Aufbewahrung der Datensicherung

Die Datensicherungsmedien sind in einem zugangskotrollierten Bereich aufzubewahren und vor unberechtigten Zugriff zu schützen.

2.8 Virtual Center und Datenbank Server Hardening

Das Härten der Windows Server für Virtual Center und der Datenbank sind nicht Bestandteil dieses Dokuments.

2.9 Scripting und Batch-Dateien

Zur Automatisierung von VirtualCenter Aktionen und zur Datensicherung über VCB können Scripte und Batch-Dateien verwendet werden. Alle verwendeten Accounts deren Passwort im Klartext in diesen Scripten und Batches hinterlegt sind, müssen auf minimale Berechtigungen eingeschränkt werden.

2.10 Virenschutz

2.10.1 Hosts

Wenn das Service Consolen Interface wie empfohlen vom restlichen Netzwerk isoliert ist, kann das Viren Risiko als relativ gering eingestuft werden.
Ansonsten sollte die Service Console durch eine Virenschutzsoftware geschützt werden. Es sollte dabei eine Virenschutzsoftware für Redhat Enterprise Linux 3 Version verwendet werden.

2.10.2 Virtuellen Maschinen

Alle Virtuellen Maschinen sind durch eine aktuelle Virenschutzsoftware zu schützen.

2.11 Verschlüsselung von Virtuellen Disks

Bei Virtuellen Disks handelt es sich nur um Dateien, die einfach durch ein Filecopy kopiert werden könnten. Virtuelle Disks mit sensitiven Daten sollten deshalb mit einer Festplattenverschlüsselungssoftware verschlüsselt werden.

3 Operative Tätigkeiten

3.1 Wartung

In einem mehrstufigen Wartungsplan sollten alle Server- und Speichersysteme der Virtuellen Infrastruktur regelmäßig gewartet werden.

3.2 Patchmanagement

Kritische Patches für die VMware Infrastruktur müssen zeitnah auf den Systemen installiert werden.
Mit dem VMware Update Manager können die ESX Server Patches sehr leicht kontrolliert auf die betroffenen Systeme eingespielt werden.

3.3 Datensicherung der Log Dateien und Systemkonfiguration

Die Logdateien und Dateien der Systemkonfiguration von Systemen der Virtuellen Infrastruktur sind regelmäßig zu sichern.

3.4 Audit

In einem mehrstufigen Auditplan sind sicherheitsrelevante Komponenten regelmäßig zu überprüfen.