

Dokumentation der
Betrieblichen Projektarbeit

Thema:

Einrichten einer virtualisierten Desktopumgebung für Clients

Erarbeitet und vorgelegt von: Marcel Heimke
Jahnstraße 15
28816 Stuhr-Brinkum

Durchführungszeitraum: 25.02.13 – 08.03.13
Durchführungsort: Creative Computer Consulting GmbH
Geisbergstr. 11
28211 Bremen

INHALT

Vorwort.....	1
1.PROJEKTPLANUNG.....	1
1.1 IST-Analyse.....	1
1.2 Zielsetzung.....	2
1.3 Konzept.....	2
1.4 Softwareauswahl.....	3
1.4.1 Virtualisierungssoftware	3
1.4.2 Betriebssystem	3
1.4.3 Auswahl der Antivirenlösung	4
1.5 Hardwareauswahl.....	5
2. TESTSTELLUNG	7
2.1 Erstellen einer Testumgebung.....	7
2.2 Einrichten der Virtualisierungsserver	8
2.3 Erstellen der virtuellen Desktops	9
2.4 Einrichten der Antivirenlösung	10
2.5 Durchführen von Tests	10
3. ROLLOUT BEIM KUNDEN.....	11
3.1 Migration der Server.....	11
3.2 Bereitstellen der virtuellen Desktops.....	12
3.3 Einrichten von Bitdefender	12
3.4 Anpassen der Clients	12
4. PROJEKTABSCHLUSS	13
4.1 Gesamtprojektkosten	13
4.1.1 Softwarekosten	13
4.1.2 Hardwarekosten.....	13
4.2 Zeitplanung	13
4.3 Fazit / Ausblick	15
ANHANG mit seperatem Inhaltsverzeichnis	

VORWORT

Mein Name ist Marcel Heimke und ich bin Soldat auf Zeit bei der deutschen Bundeswehr. Das folgende Projekt fand während der „Zivilberuflichen Aus- und Weiterbildung“ (kurz: ZAW) im Rahmen der Ausbildung zum Feldwebel, allgemeiner Fachdienst statt. Bildungsträger dieser Ausbildung ist das Bildungswerk der niedersächsischen Wirtschaft gGmbH. Der Hauptsitz der BNW gGmbH befindet sich in Hannover, die Ausbildung wurde in einer Außenstelle in Wilhelmshaven durchgeführt. Während eines Praktikums in der Creative Computer Consulting GmbH führte ich das Abschlussprojekt durch. Meine festen Ansprechpartner während der Durchführung des Projekts waren in technischen, sowie kaufmännischen Fragen der Geschäftsführer Herr Rosenkranz, sowie der Consultant Herr Just (beide Creative Computer Consulting GmbH). Der Kunde stimmte der Verwendung dieses Projektes als Abschlussprojekt mit der Bedingung zu, dass er nicht genannt wird. Somit wurden alle Screenshots in der Testumgebung erstellt. **Fette und unterstrichene** Textstellen sind Hyperlinks zu Bildmaterialien im Anhang (Hyperlink zurück zur Textstelle ist vorhanden), *kursive Begriffe* werden im Glossar näher erläutert.

1.PROJEKTPLANUNG

1.1 IST-ANALYSE

Jeder der 20 Mitarbeiter dieser Logistik GmbH nutzt zurzeit jeweils einen vollwertigen Desktop PC. Dieser besteht aus einem Computer, einem Monitor und Eingabegeräten. Auf jedem dieser Desktop PCs ist das Betriebssystem Microsoft Windows XP und das Softwarepaket Microsoft Office XP installiert, sowie eigene Dateien der Benutzer gespeichert. Die Benutzer melden sich an dem Domänencontroller in der vorhandenen Domäne im Netzwerk an, auf dem das Betriebssystem Microsoft Windows Server 2008 R2 installiert ist. Dieser stellt zusätzlich die Rollendienste *DHCP* und *DNS* zur Verfügung. Als Datenspeicher ist ein *iSCSI*-fähiges *NAS* mit einem nutzbaren Volumen von zwei Terabyte im Netzwerk vorhanden. Dieses besteht aus insgesamt vier Festplatten, welche sich in einem RAID5-Verbund befinden. Eine Festplatte wird hierbei für die *Hotspare* Funktion verwendet. Die daraus resultierenden Energiekosten der Desktop PCs werden in **Anhang B: Berechnung der Energieersparnis** aufgeführt.

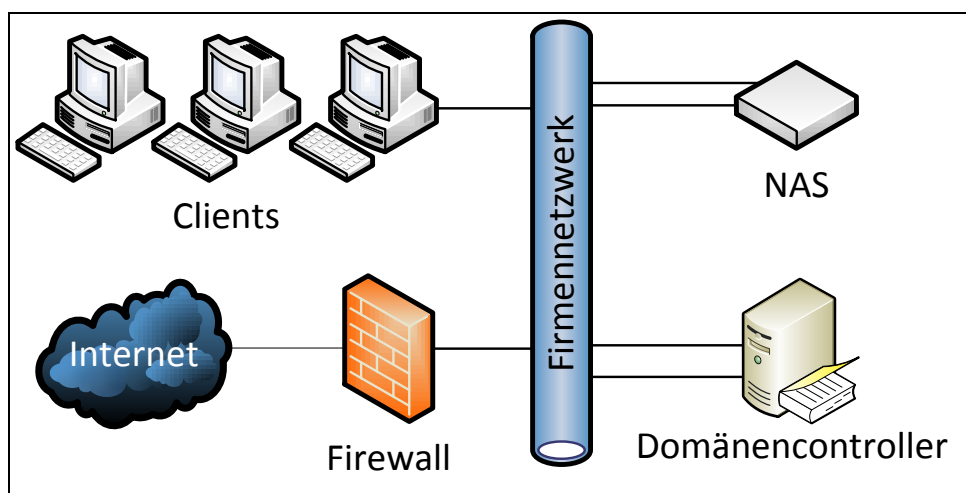


Abb.1 Ausgangssituation

1.2 ZIELSETZUNG

Nach Abschluss des Projekts können die Desktop PCs durch Thin-Clients ersetzt werden, welche eine deutlich geringere Energieaufnahme¹ im Vergleich mit den bisher vorhandenen Computern bieten. Dadurch werden die Energiekosten und damit variable Betriebskosten gesenkt und die Wirtschaftlichkeit des Unternehmens gesteigert. Durch die virtualisierte Desktopumgebung ist es den Mitarbeitern zusätzlich möglich, sich an jedem im Netzwerk befindlichen Gerät mit ihrem persönlichen Desktop, inklusive Dateien und Einstellungen, anzumelden. Dies erhöht die Flexibilität und Mobilität. Durch die Zentralisierung des Systems wird zusätzlich der Administrationsaufwand verringert, wodurch Wartungszeiten und Kosten gesenkt werden. Abschließend wird das verwendete Betriebssystem aktualisiert und somit der fortlaufende Support² sichergestellt.

1.3 KONZEPT

Es werden zwei Virtualisierungshosts in das bestehende Netzwerk implementiert. Die Leistung der Hosts wird so gewählt, dass ein Host die vollständige Last der *virtuellen Maschinen*³ der 20 Mitarbeiter und der für die Virtualisierung benötigten Komponenten tragen kann. Dabei wird auch die Auslastung zu Spitzenzeiten berücksichtigt. Durch redundante Systemkomponenten wird die Ausfallsicherheit gewährleistet.

Beide Server erhalten unabhängigen Zugriff (*shared storage*) auf das NAS, welches weiterhin als zentraler Datenspeicher zur Verfügung steht. Auf diesem werden drei voneinander getrennte Bereiche erstellt: „Profile“ enthält alle Profile und Eigene Dateien der Benutzer, welche zukünftig ausschließlich auf dem NAS gespeichert werden; „vDisks“ enthält die virtuellen Festplatten aller eingesetzten VMs; „Public“ wird als gemeinsamer Speicher für alle Nutzer verwendet.

Jeder Server wird mit zwei Dual-Port Netzwerkkarten ausgestattet. Die insgesamt vier Netzwerkverbindungen dieser Karten führen in das Arbeitsplatznetzwerk, wodurch die Ausfallsicherheit erhöht wird.

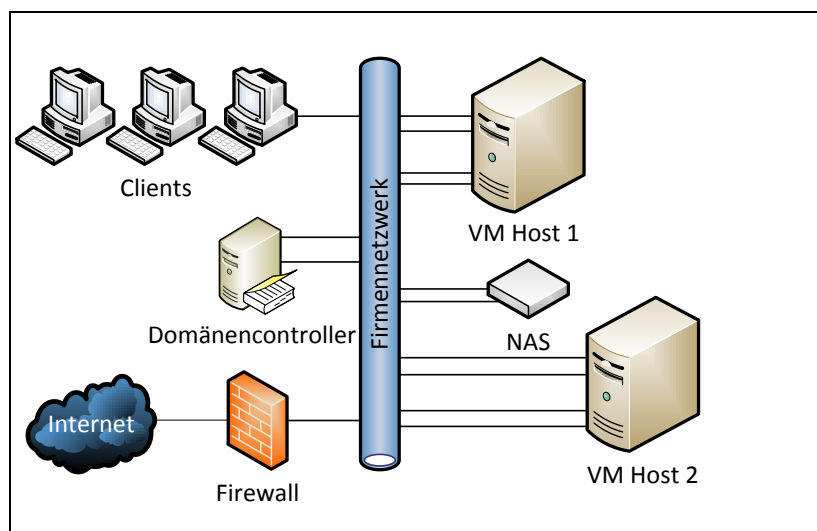


Abb.2 Soll Zustand

¹ Energieverbrauch: ThinClient Ø 7W; Energieverbrauch Desktop PC Ø 80W Quelle: <http://cc-asp.fraunhofer.de/docs/PCvsTC-de.pdf>

² Der Support für Windows XP endet am 08.04.2014 Quelle: <http://www.microsoft.com/de-de/windows/endofsupport.aspx>

³ Im weiteren Verlauf der Dokumentation mit „VMs“ abgekürzt

Außerdem wird eine Sicherheitslösung eingerichtet, die den Schutz von Clients und virtuellen Servern sicherstellt. Auslastungsspitzen des Systems durch Update- und Scanvorgänge müssen dabei beachtet werden.

1.4 SOFTWAREAUSWAHL

1.4.1 Virtualisierungssoftware

Für die Umsetzung des Projektes werden die Produkte der marktführenden Unternehmen VMware und Citrix verglichen. Es wird eine herstellerspezifische Lösung bevorzugt, das heißt der *Hypervisor* und die Bereitstellungssoftware soll vom selben Hersteller sein.

VMware: Der Hersteller VMware nutzt als Basis für virtuelle Systeme den *Hypervisor* ESX bzw. ESXi⁴. Zum Verwalten der VMs auf dem *Hypervisor* wird das vCenter verwendet, das als zusätzlicher Dienst auf einem Windows Server-System installiert wird. Diese Produkte sind unter dem Namen vSphere als Paket verfügbar. Für die Bereitstellung der virtuellen Desktops wird View 5.1 verwendet. Dieses kann aus einer Vorlage, dem so genannten „*Golden Image*“ Kopien von virtuellen Desktops („*Linked Clones*“) erstellen. Durch diese Technologie verwenden alle Benutzer dasselbe Grundgerüst und es muss nur eine vollständige virtuelle Festplatte und die jeweiligen *Deltafiles* der Benutzer gespeichert werden, wodurch sich der Speicherbedarf reduzieren lässt (**Abb. 3 Linked Clones**). Die Verbindung zum virtuellen Desktop wird mit Hilfe des View Clients hergestellt. Daher würde für das Projekt das VMware View 5 Bundle in Betracht kommen. Dieses umfasst alle erforderlichen Lizenzen.

Citrix: Der Hersteller Citrix nutzt als *Hypervisor* den XenServer. Für die Verwaltung der VMs wird das XenCenter verwendet. Dieses kann auf einem Server oder einem Desktopbetriebssystem installiert werden und wird ebenfalls mit dem *Hypervisor* ausgeliefert. Für die Bereitstellung der virtuellen Desktops wird XenDesktop 5.5 verwendet. Der Desktop kann über ein Java Plugin oder den Citrix ICA-Receiver bereitgestellt werden. Ein vom Umfang vergleichbares Produkt von Citrix ist XenDesktop Enterprise Edition.

Nutzenvergleich **Anhang A: Nutzwertanalyse**

Durch den Vergleich beider Lösungen stellt sich heraus, dass der Einsatz der VMware Produkte den Anforderungen des Kunden am besten entspricht, so dass diese dem Kunden empfohlen werden.

1.4.2 BETRIEBSSYSTEM

Der Kunde wünscht eine Aktualisierung des eingesetzten Betriebssystems. Hierbei möchte er, dass auch zukünftig ein Microsoft Windows Betriebssystem eingesetzt wird. Als Auswahlmöglichkeiten stehen somit die zurzeit aktuellen Microsoft Betriebssysteme Windows 7 und Windows 8 zur Verfügung. Diese werden Anhand der Kriterien Performance, Bedienbarkeit, Erfahrungen und Erscheinungsbild verglichen.

Performance: Ein wesentlicher Bonus von Windows 8 bei der Performance wird durch das schnellere Starten des Systems erzielt. Dieses Argument hat in der virtuellen Umgebung jedoch keine Relevanz, da die Systeme bereits gestartet zur Verfügung gestellt werden. Das Verwenden von Office 2010 und dem Internet Explorer 10 (welches die Hauptanwendungen beim Kunden sind) ist bei Windows 8 spürbar schneller als bei Windows 7. Daher Punkt für Windows 8 (1:0).

⁴ ESXi stellt weniger Funktionen als ESX bereit und ist für kleinere virtuelle Umgebungen konzipiert

Bedienbarkeit: Windows 7 ist bei der Bedienung nahezu identisch mit den Vorgängerversionen, weswegen es den Benutzern deutlich einfacher fällt mit dem neuen System zu arbeiten. Das Arbeiten mit der neuen Kacheloberfläche von Windows 8 kann für viele Nutzer sehr umständlich sein, vor allem da das Startmenü nicht mehr vorhanden ist. Benutzer die privat ein Smartphone benutzen könnten dabei schneller mit der neuen Oberfläche vertraut werden, stellen jedoch eher eine Minderheit im Unternehmen dar. Daher Punkt für Windows 7 (1:1).

Erfahrungen: Windows 8 stellt das zurzeit aktuellste Microsoft Betriebssystem dar. Daher gibt es nur wenige Erfahrungsberichte im Umgang mit diesem System, jedoch wird aufgrund des durchschnittlichen Lebenszyklus (ca. 12 Jahre) längerer Support sichergestellt. Windows 7 ist bei vielen Unternehmen bereits im Einsatz und auch durch ein Service Pack verbessert worden. Das Ende des Supports wurde jedoch bereits auf den 14.01.2020 festgelegt⁵. Daher hier Punkt für beide (2:2).

Erscheinungsbild: Bei Windows 7 und den Vorgängerversionen werden Anwendungen vor allem über das Startmenü gestartet. Das System bootet hier auf den Desktop, der je nach Benutzer schlicht gehalten ist. Nach dem Start von Windows 8 befindet sich der Benutzer auf der neuen Kacheloberfläche. Diese wirkt auf den ersten Blick eher ungewohnt aber optisch ansprechender und ähnelt vom Aufbau einem Smartphone-Betriebssystem. Informationen von Windows 8 Apps (z.B. Wetter, E-Mail Status) werden dem Nutzer in der Kachel direkt angezeigt. Daher Punkt für Windows 8 (3:2).

Aufgrund des Vergleichs der beiden Betriebssysteme wird dem Kunden der Einsatz von Windows 8 empfohlen. Da dieses virtuell bereitgestellt werden soll, wird zusätzlich eine Software Assurance von Microsoft benötigt. Das Betriebssystem inklusive Software Assurance ist unter der Bezeichnung Windows 8 Enterprise verfügbar und beinhaltet zusätzlich ein Upgrade-Recht für neu erscheinende Betriebssysteme und ein Downgrade-Recht bis einschließlich Windows 98.

1.4.3 AUSWAHL DER ANTIVIRENLÖSUNG

Eine große Herausforderung bei der Planung von Virtualisierungen ist die Verwendung der Antivirenlösung. In jeder VM wird ein vollständiger Antiviren Client installiert, welcher das System mit Update- und Scanvorgängen belastet und damit die Anzahl der möglichen VMs pro Host senkt. Durch massive, gleichzeitige Speicherzugriffe bei diesen Vorgängen wird zusätzlich der gemeinsame Speicher so stark belastet, dass normales Arbeiten währenddessen eingeschränkt wird. Weiterhin entstehen Angriffsflächen während des Hoch- und Herunterfahrens der VM, da der Dienst erst danach gestartet beziehungsweise vorher beendet wird. Um diese Probleme zu vermeiden wird dem Kunden der Einsatz der Bitdefender SVE (Security for Virtualized Environments) empfohlen. Für diese Software wird auf jedem Host die „Security Virtual Appliance“⁶ als eigenständige, auf Linux basierende VM installiert. Die SVA zentralisiert Scanvorgänge, so dass die Arbeitsspeicher- und CPU- Last für Scans auf eine VM reduziert werden. Dazu wird innerhalb der Client VM ein Silent Agent installiert, der eine Tunnel-Verbindung zur SVA herstellt, damit diese den Scanvorgang durchführen kann. Dieser Agent kann als E-Mail, per Weblink oder als Rollout des Administrators über eine zentrale Konsole (Security Console) auf allen VMs installiert werden.

⁵ <http://windows.microsoft.com/de-de/windows/products/lifecycle>

⁶ Im weiteren Verlauf der Dokumentation mit „SVA“ abgekürzt

Die Security Console ist eine weitere VM innerhalb des Clusters, die über den Webbrowser gesteuert wird. Von dort aus kann der gesamte Sicherheitsstatus des Systems mit allen im Cluster vorhandenen VMs überwacht und gesteuert werden, so dass der Administrator jederzeit auf dem aktuellen Stand aller Systeme ist und Scan- und Update- Vorgänge steuern kann. Sicherheitsupdates werden von der Security Console zentral heruntergeladen und bereitgestellt, was den Datenverkehr, die Ressourcenauslastung und die benötigte Zeit für Updates verkürzt. Die dadurch freigewordenen Ressourcen können nun für die Erstellung weiterer VMs verwendet oder mehr Leistung für vorhandene bereitgestellt werden.

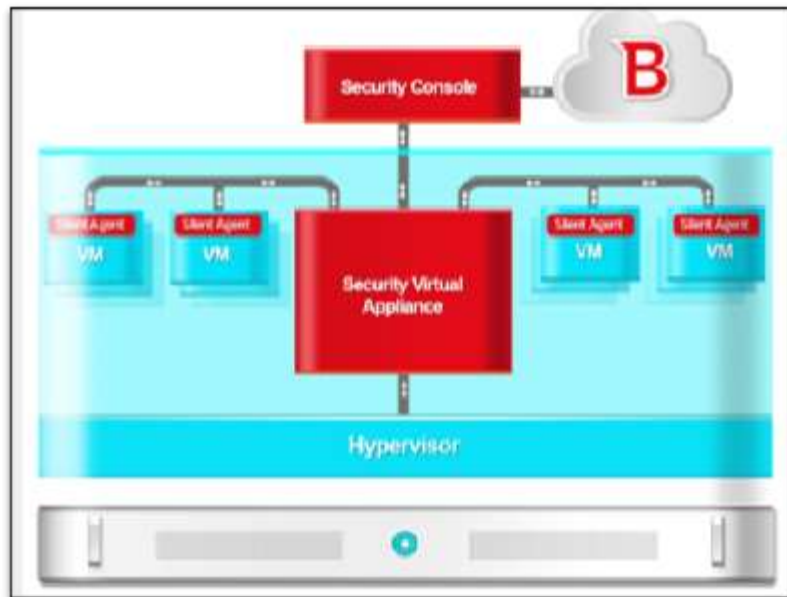


Abb. 5 Struktur Bitdefender

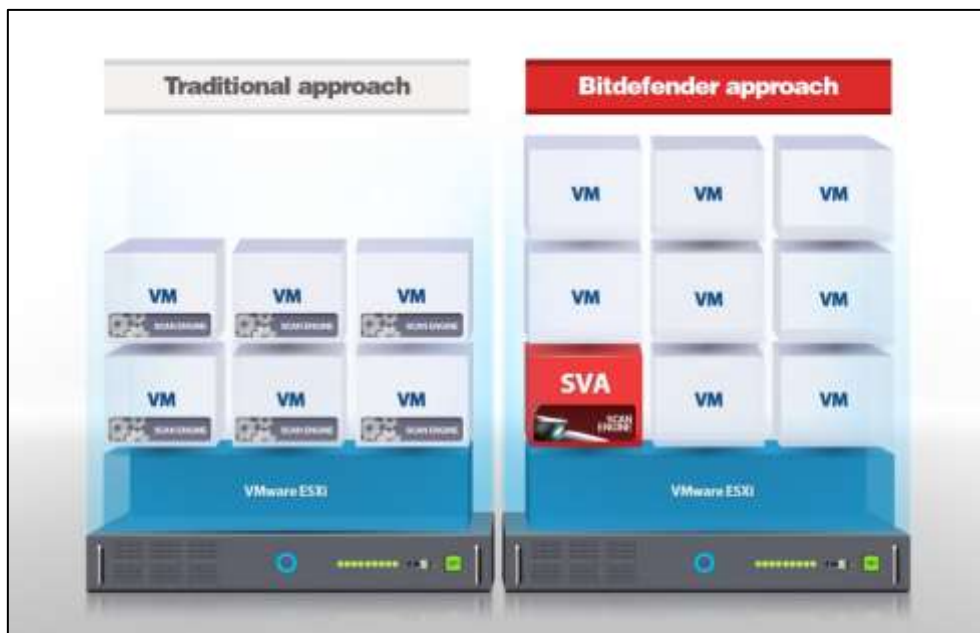


Abb. 4 Vergleich: herkömmliche AV-Lösung – Bitdefender

1.5 HARDWAREAUSWAHL

Aufgrund der bisherigen Infrastruktur ist es notwendig, Hardware für die Virtualisierung zu beschaffen. Diese muss über ausreichend Leistung verfügen, um mindestens 20 virtualisierte Desktops gleichzeitig betreiben zu können. Hinzu kommen die zwei virtuellen Server, die zum Bereitstellen der Desktops benötigt werden (vCenter/Composer, Connection Server). Diese Server und deren Funktion werden in Abschnitt 2.2 „Einrichten der Virtualisierungsserver“ beschrieben. Da das System eine hohe Ausfallsicherheit aufweisen

soll, ist zudem redundant zu planen, das heißt ein zweiter *Host* ist zu beschaffen⁷ und wichtige Komponenten⁸ werden doppelt integriert.

Arbeitsspeicher: Zukünftig soll das Betriebssystem Windows 8 zum Einsatz kommen. Daher wird ein Arbeitsspeicher von 2GB pro *VM* benötigt. Daraus ergibt sich ein Mindestbedarf von 40GB. Zusätzlich werden zwei *VMs* mit Microsoft Windows Server 2008 R2 als Betriebssystem benötigt, für die jeweils 4GB Arbeitsspeicher benötigt werden. Diese werden für die Bereitstellung der virtuellen Desktops mit VMware View benötigt. Für die Bitdefender SVA wird außerdem ein Arbeitsspeicher von 4GB und für die Security Console von 2GB benötigt.

CPU: Um eine ausreichende Performance des Systems sicherstellen zu können, bekommen beide Server *VMs* jeweils vier virtuelle CPUs. Die SVA benötigt für zuverlässige Performance zwei virtuelle CPUs. Für die Security Console und die virtuellen Desktops reicht eine virtuelle CPU je *VM*. Dabei wird davon ausgegangen, dass eine virtuelle CPU ca. ein Achtel eines physikalischen CPU-Kerns auslastet.

Festplattenspeicher: Dem Kunden wurde die Beschaffung eines zweiten Speichersystems (z.B. *SAN*) zur Erhöhung der Ausfallsicherheit und Performance empfohlen. Auf diesem sollten alle virtuellen Festplatten der *VMs* abgelegt werden. Der Kunde entschied sich jedoch aus Kostengründen gegen diese Empfehlung, weshalb das *NAS* als Hauptspeicher eingerichtet wurde.

Die Hauptspeicherlast entsteht auf dem *NAS* als *shared storage*. Wie in Punkt 1.3 „Konzept“ bereits beschrieben wird dieses in drei Speicherbereiche aufgeteilt. Der erste Bereich (400GB Speichergröße) dient als Speicher für die Profile inklusive der eigenen Dateien der Benutzer, wobei jedem Nutzer ein maximales Kontingent von 20GB bereitgestellt wird. Der zweite Bereich (260GB Speichergröße) wird als Speicherort für die virtuellen Festplatten verwendet. Bereits einkalkuliert sind dabei 140GB Speicher für die *Deltafilas* der Benutzer. Da diese jedoch nur temporär sind (Eigene Dateien der Benutzer werden in Bereich eins gespeichert) werden diese nach dem Abmelden der Benutzer automatisch wieder gelöscht. Für das *Golden Image* werden 20GB verwendet. Dem dritten Bereich wird die Restkapazität (1340GB) zugewiesen und kann als gemeinsame Ablage verwendet werden. Auf den *Hosts* werden nur der *Hypervisor* ESXi und die Bitdefender SVA installiert, die gemeinsam ca. 20 GB Speicherplatz auf der *Host*-Festplatte benötigen.

	Virtuelle Maschine	Anzahl	CPU	Arbeitsspeicher [in GB]	HD NAS [in GB]
VMware View Komponenten	vCenter / Composer	1	4	4	50
	Connection Server	1	4	4	50
Bitdefender Komponenten	Security Virtual Appliance	1	2	4	-
	Security Console	1	1	2	20
Benutzer Komponenten	Windows 8	max. 20	20	40	140
	Benutzerprofile	20	-	-	400
	Temporäre Deltafilas	-	-	-	120
Gesamt		max. 24	31 ⁹	54	660

Ermittelter Mindestbedarf (tabellarisch)

⁷ Grundlage der Ermittlung ist ein Leitfaden des Herstellers VMware Quelle: <http://pubs.vmware.com/view-51/topic/com.vmware.ICbase/PDF/view-51-architecture-planning.pdf>, Kapitel 4, Seiten 37 - 46

⁸ Netzteil, Netzwerkkarte, CPU, RAM, Festplatte

⁹ Virtuelle CPU; 1 *vCPU* = 1/8 *pCPU*-Kern; 31 *vCPU* = 3,875 *pCPU*-Kerne

Basierend auf diesen Anforderungen wurde ein Dell PowerEdge™ R420 Server konfiguriert, der diese Anforderungen erfüllt und aufgrund der Skalierbarkeit des Systems Reserveressourcen für spätere Erweiterungen bereithält (detaillierte Konfiguration in **Anhang E: Serverkonfiguration**).

2. TESTSTELLUNG

2.1 ERSTELLEN EINER TESTUMGEBUNG

Es wurde eine Testumgebung erstellt, die der Infrastruktur beim Kunden entspricht. Dies dient der Qualitätssicherung, da mögliche Probleme frühzeitig erkannt und Lösungen gefunden werden können. Zusätzlich verkürzt sich dadurch die Zeit für die Integration in das System beim Kunden.

Es werden zwei Virtualisierungsserver integriert auf denen der *Hypervisor* ESXi 5 installiert ist. Auf diesen werden drei virtuelle Server gehostet, die nachfolgend näher erklärt werden. Alle Systeme (physikalisch und virtuell) befinden sich im selben Netzwerk (Netzwerk ID 192.168.1.0/24).

Der Server „Master“ entspricht dem beim Kunden bereits physikalisch vorhandenen Domänencontroller. Dieser stellt die Dienste *DHCP*, *DNS* und das *Active Directory – Domänendienste* für alle im Netzwerk befindlichen Geräte bereit. Dazu wurde eine *OVF-Vorlage* aus einer vorherigen Testumgebung importiert. Diese enthält bereits mehrere Gruppen und Benutzerkonten sowie einen *DHCP* Testbereich mit den IP-Adressen 192.168.1.1 – 192.168.1.254. Statisch vergebene Adressen innerhalb dieses Bereichs (z.B. 192.168.1.10 für den Sever „Master“) werden als neuer ausgeschlossener Bereich definiert, um Fehler bei der Adressvergabe zu vermeiden.

Die virtuellen Server „vCenter“ und „Connection Server“ beinhalten alle Komponenten, die für das Bereitstellen der virtuellen Desktops erforderlich sind. Zusätzlich wird im Laufe der Installation der Komponenten eine Instanz von MS SQL Server 2008 R2 Express installiert. Diese Server werden während der Durchführung des Projektes beim Kunden ebenfalls virtuell bereitgestellt.

Als Speicher für die *VMs* wird ein *SAN* angebunden, welches per Fibre Channel Kabel über einen Switch mit den *Hosts* verbunden ist. Insgesamt stehen für die Testumgebung 276GB für die virtuellen Systeme zur Verfügung. Die Bitdefender SVA wird auf der lokalen Festplatte des jeweiligen *Hosts* abgelegt.

Die SonicWALL ist eine Firewall, die das Testnetzwerk und das produktive Netz (dieses heißt „3xc“) trennt. Dadurch kann die Testumgebung als eigenständiges Netzwerk betrieben werden. Außerdem ist die SonicWALL das Gateway in das Internet für alle im Testnetzwerk befindlichen Geräte.

Zusätzlich werden drei unterschiedliche Clienttypen in das Netzwerk integriert: Desktop PCs, Laptops und Thin Clients¹⁰, die ihre Netzwerkeinstellungen durch den *DHCP*-Server-Dienst erhalten.

Verbunden sind alle Geräte über eine kabelgebundene Gigabit Netzwerkverbindung und einem Gigabit-Switch.

¹⁰ Samsung SyncMaster TC240

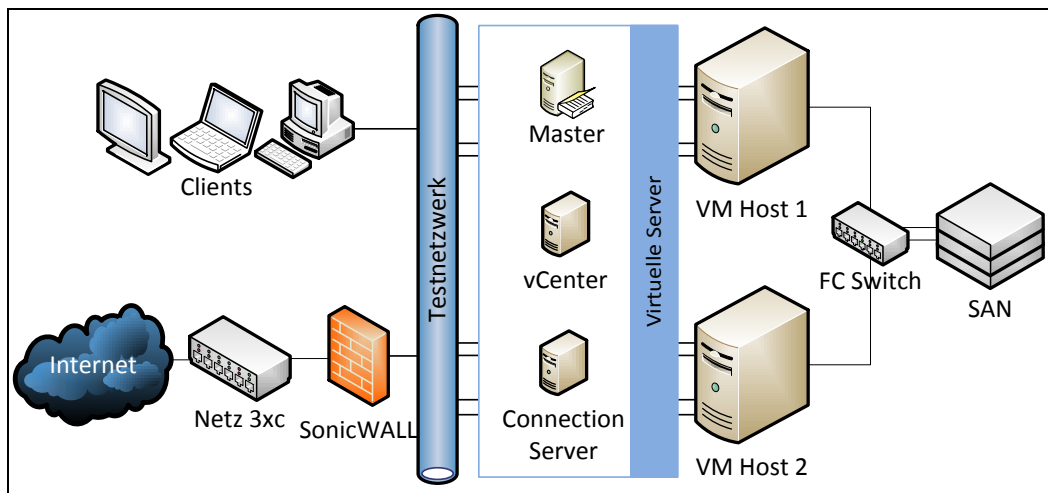


Abb. 6 Struktur der Testumgebung

2.2 EINRICHTEN DER VIRTUALISIERUNGSSERVER

Zum Erreichen des Ziels werden auf dem Server „vCenter“ zwei und auf dem Server „Connection Server“ ein Serverdienst installiert. Deren Funktionen werden im Folgenden erklärt:

vCenter Server: Dieser Dienst wird zum Verwalten der VMware ESXi-Hosts verwendet. Es verwaltet und überwacht alle Ressourcen der Systeme, startet weitere Hosts, verschiebt im Bedarfsfall VMs oder schaltet die Hosts in den Standby, falls diese nicht benötigt werden. Zusätzlich können mit Hilfe des vCenter Servers weitere VMs erstellt, bearbeitet oder gelöscht werden. Der vCenter Server-Dienst ist auf dem Server „vCenter“ installiert.

View Connection Server: Diese Serverfunktion empfängt alle Anfragen zur Bereitstellung der virtuellen Desktops. Er dient zur Authentifizierung der Benutzer und erteilt Ihnen je nach Berechtigung Zugriff auf bestimmte Desktops. Zusätzlich verwaltet er alle Desktop Sitzungen. Durch die Installation dieses Dienstes wird der View Administrator verfügbar. Dieser kann über den Webbrowser aufgerufen werden und stellt die Verwaltungskonsole des Systems dar. Der View Connection Server-Dienst ist auf dem Server „Connection Server“ installiert.

View Composer: Dieser Softwaredienst arbeitet eng mit dem vCenter Server zusammen und ist daher auf dem Server „vCenter“ installiert. Er dient dazu aus dem *Snapshot* einer VM (*Golden Image*) eine festgelegte Anzahl von *Linked Clones* zu erstellen, was den Speicherbedarf laut Hersteller um bis zu 90% reduziert, da alle Benutzer dasselbe Basisimage verwenden. Jeder dieser Klone wird als eigenständiger Desktop mit eindeutiger IP-Adresse und eindeutigen Computernamen verwaltet. Updates und Patches werden zentral von einem Administrator im *Golden Image* installiert. Dadurch erfolgt die Verteilung schneller und zuverlässiger, da die Benutzer hier nicht mehr aktiv werden müssen und Updates übersehen könnten. Zusätzlich verringert sich der Datentransfer bei allen Updatevorgängen.

Zuerst wird auf den Hosts ESXi 5 installiert. Das Image dazu wird als virtuelle CD über die Webkonsolen der Server eingebunden und zum Booten als *primäres Bootdevice* festgelegt. Anschließend wird für beide Hosts eine Management IP-Adresse festgelegt. Nun wird über einen Webbrowser der vSphere Client von einem der beiden Hosts heruntergeladen und installiert. Mit diesem kann eine Verbindung zum Hypervisor hergestellt und eine VM erstellt

werden, auf der Windows Server 2008 R2 als Gastbetriebssystem installiert wird (**Abb. 7 Installation des vCenters 1**). Dieser Server trägt den Namen „vCenter“. Dann wird die Installations –DVD des vCenters als ISO-File in diese VM über das virtuelle Laufwerk eingebunden und installiert. Während dieses Vorgangs wird eine Instanz von MS SQL 2008 R2 Express installiert, die um das MS SQL Management Studio¹¹ erweitert wird. Dieses wird später für die Erstellung von weiteren Datenbanken benötigt. Das vCenter erstellt automatisch alle benötigten Datenbankeinträge. Nachdem die Installation des vCenters abgeschlossen ist, lässt sich eine Verbindung über die IP-Adresse des Servers herstellen (**Abb. 8 Installation des vCenters 2**). Von dort aus werden nun *Hosts* in den *Cluster* hinzugefügt, *Ressourcenpools* und weitere VMs erstellt und installiert (die Server Master und Connection Server, sowie die VMs für Windows 7 und 8).

Die Installation des View Composer Dienstes erfolgt ebenfalls auf dem Server „vCenter“. Dieser benötigt eine Datenbankinstanz (**Abb. 9 Installation des View Composer**), die bereits lokal auf dem Server installiert wurde. Über das nachinstallierte Management Studio kann die erforderliche Datenbank erstellt werden.

Die Installation des View Connection Servers benötigt ebenfalls keine speziellen Konfigurationen. Nach dieser Installation ist der View Administrator über die IP-Adresse oder DNS-Eintrag des Servers „Connection Server“ mit Hilfe des Webbrowsers verfügbar. Zur Protokollierung von Ereignissen wird auch hier eine Datenbank innerhalb der MS SQL 2008 R2 Express Instanz erstellt und im View Administrator hinterlegt. Außerdem wird das vCenter in den Einstellungen hinterlegt und die Option „View Composer wurde zusammen mit vCenter installiert“ ausgewählt, damit später die *Linked Clones* erstellt werden können (**Abb. 10 Konfiguration des View Administrators**).

2.3 ERSTELLEN DER VIRTUELLEN DESKTOPS

Die Installationsabläufe der Betriebssysteme unterscheiden sich kaum, weshalb alle aufgeführten Arbeitsschritte auf dem Windows 7 und 8 System parallel durchgeführt werden.

Zuerst wird das Betriebssystem in der VM installiert. Dazu wird ein Installationsmedium als virtuelle DVD eingebunden und die VM neu gestartet. Danach werden die VMware Tools installiert, welche die Leistung des Gastbetriebssystems verbessern und dieses um eine umfangreiche Treiberdatenbank erweitert. Anschließend werden alle benötigten Softwarepakete wie zum Beispiel MS Office 2010 installiert. Als nächstes wird das Tool Desktop Optimizer von Quest verwendet, welches für virtualisierte Systeme ungeeignete Services und Dienste deaktiviert und somit die Performance verbessert. Da dieses Tool keine Kompatibilität mit Windows 8 besitzt erfolgt dieser Schritt hier manuell¹² (**Abb. 11 Leistungsoptimierung**).

Die Netzwerkeinstellungen werden auf *DHCP* belassen. Dies ist wichtig für das dynamische Erstellen von *Linked Clones*, welches unter Punkt 2.4.4 „Durchführen von Tests“ näher erläutert wird. Außerdem werden die Systeme mit dem Namen „Windows X¹³ Master“ benannt, in die Domäne integriert und in eine neu erstellte *Organisation Unit*¹⁴ „ViewDesktops“ im *Active Directory* auf dem Server „Master“ verschoben.

Als letztes wird der View Agent installiert. Dieser Softwaredienst ermöglicht die Kommunikation zwischen der VM und dem View Connection Server.

¹¹ Frei erhältlich auf <http://www.microsoft.com/en-us/download/details.aspx?id=22985>

¹² Mit Hilfe des Windows Befehls: SystemPropertiesPerformance

¹³ X steht für die Version des Betriebssystems (7 oder 8)

¹⁴ Im weiteren Verlauf mit „OU“ abgekürzt

2.4 EINRICHTEN DER ANTIVIRENLÖSUNG

Auf beiden *Hosts* wird eine *OVF* Vorlage der *SVA* importiert und auf der Festplatte des jeweiligen Servers gespeichert. Durch das Importieren einer Vorlage ist das System bereits vollständig installiert und muss lediglich angepasst werden. Nach dem Starten der dadurch neu erstellten *VM* müssen die Netzwerkeinstellungen und die Adresse der Security Console, welche parallel importiert wird, hinterlegt werden. Die *SVA*s können nun eine Verbindung zur Security Console aufzubauen. Sobald diese vollständig hochgefahren ist und die Verbindung zustande kommt werden die *Hosts* dadurch automatisch im System registriert.

Als Nächstes wird in den Windows *VM*s der Silent Agent installiert. Dieser lässt sich über einen Webinstaller im Betriebssystem installieren und kann je nach Einstellung in der Security Console für den Benutzer unsichtbar arbeiten. Nach der Installation stellt der Silent Agent automatisch eine Verbindung mit der Security Console her, bezieht Updates und führt einen erstmaligen Systemscan durch. Zusätzlich können von der zentralen Konsole Scanvorgänge auf den verwalteten Clients gestartet und der Status abgerufen werden.



Abb. 12 Bitdefender Security Status

2.5 DURCHFÜHREN VON TESTS

Da mit *Linked Clones* gearbeitet werden soll, wird nun von beiden Desktop *VM*s ein *Snapshot* erstellt der die Bezeichnung „Windows_X_GoldenImage“ erhält. Nun sind alle Voraussetzungen erfüllt, um View Desktoppools zu erstellen, was über den View Administrator durchgeführt wird. Nachdem die Konfiguration des Pools abgeschlossen wurde, werden Berechtigungen hinzugefügt, die festlegen, welche Nutzer aus dem *Active Directory* sich mit diesem Pool verbinden dürfen. Nur diese Desktops werden dem Nutzer später in der Auswahl auch gezeigt. Währenddessen werden aus dem *Snapshot* bereits Klone des *Golden Image* erstellt und vorbereitet. Mit Hilfe des im View Composers konfigurierten Administratorkontos werden die neu erstellten *VM*s automatisch in die OU „ViewDesktops“ verschoben (**Abb. 13 Erstellen eines Desktoppools**).

Die Betriebssysteme starten nun wie gewohnt und der View Agent innerhalb der *VM*s stellt eine Verbindung zum View Administrator her. Sobald der Desktop als verfügbar

gekennzeichnet wurde, können die Benutzer sich mit Hilfe des View Clients auf ihrem Gerät mit diesem verbinden.

Es wurde mit verschiedenen Benutzern auf unterschiedlichen Endgeräten eine Desktopverbindung aufgebaut. Dies funktionierte bei Windows 7 ohne Probleme mit den möglichen Protokollen *PCoIP* und *RDP*. Bei der Verwendung von Windows 8 konnte durch Tests ermittelt werden, dass mit View 5.1 nur das Protokoll *PCoIP* zuverlässig verwendet werden kann, da nur dort die Option „Windows 7 3D-Beschleuniger“ gesetzt werden kann. Andernfalls konnte keine Verbindung zum Desktop aufgebaut werden, da durch den View Agent ein schwarzer Bildschirm verursacht wird.

3. ROLLOUT BEIM KUNDEN

In dem anschließenden Kundengespräch konnte dem Auftraggeber das geplante Konzept für die virtuelle Umgebung anhand der Testumgebung präsentiert und dieser überzeugt werden. Auch der Vorschlag für die Sicherheit der virtuellen Clients und Server wurde angenommen. Jedoch möchte der Kunde das vorgeschlagene Betriebssystem Windows 8 selbst testen, bevor er in diesem Punkt eine Entscheidung trifft. Auf Wunsch des Kunden wird daher das zurzeit verwendete Windows XP mit Hilfe des Tools „VMware Konverter“¹⁵ als virtueller Desktop zur Verfügung gestellt. Parallel dazu werden dem Kunden Windows 7 und 8 als Testversionen mit MS Office 2010 vorbereitet. Er kann nun selbst die Systeme ausprobieren und zu einem späteren Zeitpunkt eine Entscheidung treffen. Aufgrund des Downgrade-Rechts der Software Assurance ist dies bereits lizenziert.

3.1 MIGRATION DER SERVER

Nach dem Einbau der beiden Virtualisierungsserver in das Serverrack wird bei der Installation der benötigten Systeme wie in der Testumgebung verfahren.

Während die Virtualisierungsserver die Installationsroutine für den *Hypervisor* ESXi 5 durchlaufen, werden im *Active Directory* des bereits vorhandenen Domänencontrollers die *OU* „ViewDesktops“ für die dynamisch erstellten View Desktops, die Benutzergruppe „ViewBenutzer“ für alle Benutzer die View verwenden sollen und ein zusätzliches Administratorkonto „ViewAdmin“ erstellt. Das Administratorkonto wird für die Verwendung des View Composer-Dienstes und für das vCenter verwendet. Es dient dazu, die erstellten *Linked Clones* in die Domäne zu integrieren und in die *OU* der View Desktops zu verschieben, sowie Vorgänge innerhalb des vCenters mit Administratorberechtigung automatisch durchzuführen¹⁶.

Nach der Installation des *Hypervisors* ESXi werden die unter Punkt 1.3 „Konzept“ aufgeführten physikalischen Verbindungen hergestellt und konfiguriert. Danach wird der virtuelle Server „vCenter“ erstellt, auf dem das vCenter bereitgestellt und konfiguriert wird. Während anschließend auf diesem der View Composer-Dienst installiert wird, werden in weiteren *VMs* die *OVF*-Vorlagen der Desktopbetriebssysteme importiert und angepasst. Da *Linked Clones* zu Einsatz kommen sollen, wird ein *Snapshot* von jedem Desktopbetriebssystem erstellt. Ebenfalls zur selben Zeit wird auf dem zweiten virtuellen Server „ConnectionServer“ die Installation des View Connection Server Dienstes durchgeführt und abgeschlossen, sobald die Datenbank auf dem Server „vCenter“ verfügbar ist.

¹⁵ Dieses Tool wandelt einen physikalischen Desktop in einen virtuellen Desktop um.

¹⁶ Klonen/löschen, starten/beenden von *VMs*, Hoch-/runterfahren von Host, automatische Lastverteilung

3.2 BEREITSTELLEN DER VIRTUELLEN DESKTOPS

Nachdem alle benötigten Systeme installiert sind, wird der dynamische Desktoppool für Windows XP erstellt. Nach Rücksprache mit dem IT-Verantwortlichen des Kunden wurde die Mindestanzahl der verfügbaren Desktops auf 10, plus 4 weitere Reserve-Desktops¹⁷ festgelegt. Die Anzahl wurde aus Durchschnittswerten ermittelt und kann jederzeit angepasst werden. Mit Hilfe des erstellten Administratorenkontos werden nun insgesamt 14 identische VMs mithilfe des aktuellen *Snapshots* erstellt. Damit die Mitarbeiter die virtuellen Desktops verwenden können, wird die Gruppe „ViewBenutzer“ (in der jeder Mitarbeiter Mitglied ist) berechtigt sich mit dem Windows XP Pool zu verbinden. Außerdem werden auf dieselbe Weise ein dynamischer Pool für Windows 7 und 8 erstellt. Auf Wunsch des Kunden werden die berechtigten Benutzer hier jedoch vorerst auf den IT-Verantwortlichen und eine Auswahl von Nutzern beschränkt die beide Systeme testen sollen.

3.3 EINRICHTEN VON BITDEFENDER

Die Installation des Systems erfolgt identisch zur Testumgebung, da die Infrastruktur bis auf die verwendete Hardware in den *Hosts* und die Anzahl der Clients identisch ist. Zusätzlich zu den in der Testumgebung durchgeführten Arbeitsschritten wird ein Benutzerkonto für den IT-Verantwortlichen des Kunden innerhalb der Unternehmensdomäne erstellt, mit dem das System zukünftig administriert wird. Da der Silent Agent durch den View Composer in allen *Linked Clones* installiert ist, besteht hier kein weiterer Handlungsbedarf. Anders als in der Testumgebung wird der Silent Agent für den Nutzer unsichtbar ausgeführt.

3.4 ANPASSEN DER CLIENTS

Da zurzeit keine Thin Clients im Unternehmen vorhanden sind, werden die bisherigen Desktop PCs weiter verwendet. Zusätzlich werden dem Kunden zwei Thin-Clients¹⁸ zum Testen zur Verfügung gestellt. Um den Geschäftsbetrieb des Kunden nicht zu beeinträchtigen wird ein Zeitraum ermittelt, der außerhalb der Geschäftszeiten des Kunden liegt. Es wird nun der View Client auf den PCs installiert, der Server „Connection Server“ als Verbindungsserver und die Option „als aktueller Benutzer anmelden“ konfiguriert. Dadurch wird der Benutzer nach dem Start des Clients automatisch zur Auswahl des Desktops weitergeleitet. Durch eine Gruppenrichtlinie erhalten die Benutzer an ihrem physikalischen Client lediglich die Optionen den View Client zu starten, sich abzumelden und den Computer herunter zu fahren. Diese Richtlinie stellt sicher, dass die Benutzer nur mit ihren virtuellen Desktops arbeiten.

Eine weitere Richtlinie für die Benutzer leitet die Profile und Benutzerdateien auf die Freigabe auf dem NAS weiter und verbirgt die c:\ Festplatte der VM, so dass die Benutzer keine Dateien innerhalb der VM speichern können. Dadurch wird das Speichermanagement vereinfacht. Außerdem wird die Herunterfahren-Option in den VMs deaktiviert, um die Zeit zum erneuten Bereitstellen eines Desktops zu verkürzen. Nicht benötigte Desktops werden durch das System automatisch heruntergefahren und gelöscht, wenn weniger als die Mindestanzahl an Desktops verwendet werden.

¹⁷ Reserve-Desktops werden erstellt und der View Agent gestartet, ehe die VM bis zu Benutzung ausgeschaltet wird

¹⁸ Samsung SyncMaster TC240, Basisbetriebssystem Windows 7 Embedded

4. PROJEKTABSCHLUSS

4.1 GESAMTPROJEKTKOSTEN

Bezeichnung	Anzahl	Einzelpreis	Gesamtpreis
VMware View 5.1 Kosten	2		
MS Windows 8 Enterprise Upgrade	20		
Bitdefender SVE	24		
Hardwarekosten	2		
Fertigungseinzelkosten (Brutto)	35		
Projektgesamtkosten			

4.1.1 SOFTWAREKOSTEN

VMware View 5 Premier Starter Kit inklusive vSphere Essentials Plus mit je 3 Jahren Support:

Art	+/-	%	Preis je 10 User	Preis für 20 User
Einkaufspreis				
Marge	+			
Mehrwertsteuer	+	19		
Bruttoendpreis				

Microsoft Windows 8 Enterprise (Windows 8 Pro inkl. Software Assurance)

Art	+/-	%	Preis je User	Preis für 20 User
Einkaufspreis				
Marge	+			
Mehrwertsteuer	+	19		
Bruttoendpreis				

Bitdefender Security for Virtualized Environments:

Ein Vergleich der möglichen Lizenzmodelle befindet sich im **Anhang C: Vergleich der Bitdefender Lizenzmodelle**

Art	+/-	%	Preis je VM	Preis für 24 VMs ¹⁹
Einkaufspreis				
Marge	+			
Mehrwertsteuer	+	19		
Bruttoendpreis				

4.1.2 HARDWAREKOSTEN

Dell PowerEdge R420 Server:

Art	+/-	%	Preis je Server	Preis für zwei Server
Einkaufspreis				
Skonto	-			
Marge	+			
Mehrwertsteuer	+	19		
Bruttoendpreis				

4.2 ZEITPLANUNG

¹⁹ 20 virtuelle Desktops + 2 virtuelle Server + 2 Reserve Lizenzen

Aufgabe	Geplante Zeit	Benötigte Zeit	Differenz
Projektbesprechung / Kundengespräch	2	2	+/- 0
Recherche Hardware / Systemlösungen	2	2	+/- 0
Vergleich der Lösungen (Virtualisierung/Betriebssystem)	1	1	+/- 0
Konzeptplanung	2	1	-1
Erstellen einer Testumgebung	2	3	+1
Erstellen von Testimages	2	1	-1
Einrichten von Antivirensoftware	2	1	-1
Funktionsüberprüfung	2	3	+1
Vorstellen der Lösung	2	2	+/- 0
Einrichten der Server	3	3	+/- 0
Erstellen & Einrichten der Images für den Kunden	4	2	-2
Einrichten der Antivirenlösung (für den Kunden)	3	2	-1
Rollout beim Kunden	4	4	+/- 0
Funktionsüberprüfung / Einweisung des Kunden	2	5	+3
Nutzerdokumentation erstellen	2	3	+1
Gesamt	35	35	+/-0

Alle Angaben in Stunden; Grafischer Ablauf im **Anhang G: Zeitlicher Ablauf**

Differenzen zur ursprünglichen Planung:

Konzeptplanung: Durch Auswahl einer einheitlichen Virtualisierungsumgebung sind alle benötigten Komponenten optimal integriert. Dadurch müssen Kompatibilitäten weniger berücksichtigt werden.

Erstellen einer Testumgebung: Es konnten weitere Zusatzfunktionen²⁰ des vCenters für die Präsentation eingerichtet werden, da in der Konzeptplanung Zeit eingespart wurde.

Erstellen von Testimages: Durch das parallele Erstellen der Testimages konnte die benötigte Zeit halbiert werden.

Einrichten der Antivirensoftware: Es waren bereits aktuelle OVF-Vorlagen für Bitdefender im Unternehmen vorhanden, welche importiert und angepasst werden konnten.

Funktionsüberprüfung: Das Anpassen der Konfiguration des Windows 8 Masterimages für die Verwendung mit VMware View 5.1 benötigte mehr Zeit als erwartet, was erst durch das Erstellen eines Windows 8 *Linked Clone Pools* in Erscheinung trat.

Erstellen und Einrichten der Images für den Kunden: Es wurden die erstellten Images der Testumgebung verwendet und für den Kunden angepasst. Eine Neuinstallation war nicht notwendig.

²⁰ vMotion, DRS-Funktion

Einrichten der Antivirenlösung (für den Kunden): Es wurden ebenfalls die vorhandenen OVF-Vorlagen verwendet.

Funktionsprüfung / Einweisung des Kunden: Es konnte intensiver auf das Erstellen und Verwalten von Desktoppools und Systemressourcen in View Administrator sowie vCenter eingegangen werden.

Nutzerdokumentation: Die Nutzerdokumentation konnte aufwändiger gestaltet werden.

4.3 FAZIT / AUSBLICK

Die Infrastruktur des Unternehmens wurde für den Einsatz von Thin-Clients vorbereitet, so dass der IT-Verantwortliche des Kunden nach der Beschaffung der neuen Geräte und Installation des View Clients auf diesen die Desktop PCs austauschen kann. Dadurch wird der Energiebedarf des Unternehmens um 40% verringert und die variablen Betriebskosten gesenkt (siehe **Anhang B: Berechnung der Energieersparnis**)

Die gesamte Administration der neuen IT-Infrastruktur kann mit Hilfe von drei Verwaltungskonsolen²¹ von jedem Arbeitsplatz innerhalb des Firmennetzwerkes erfolgen, sowie Systemupdates zentral gesteuert werden. Dadurch werden Wartungskosten eingespart.

Durch den Einsatz von *Linked Clones* wird der benötigte Speicherplatz des Systems um ca. 90% verringert²². Die für Updates benötigte Zeit kann ebenfalls um bis zu 90% verkürzt²³ werden. Dadurch können weitere Kosten gesenkt werden. Zusätzlich wird die vorhandene Internetbandbreite durch die zentralisierten Updatevorgänge effektiver genutzt.

Die Entscheidung für die Aktualisierung des Betriebssystems wurde auf Wunsch des Kunden auf einen späteren Zeitpunkt verschoben. Durch die bereits erworbene Software Assurance sind die Betriebssysteme Windows 7 und 8 jedoch bereits voll lizenziert. Daher muss das gewählte Betriebssystem lediglich als aktiver Desktoppool konfiguriert werden.

Damit wurden fast alle Ziele des Projektes erreicht. Zusätzlich wurden dem Kunden bei einem projektabschließenden Gespräch weitere Optimierungsvorschläge unterbreitet:

- Durch eine Virtualisierung des Domänencontrollers können zusätzliche variable Betriebskosten gesenkt werden.
- Da der View Client auch für die mobilen Systeme Android und iOS verfügbar ist können die Desktops auch auf mobilen Endgeräten im Netzwerk verwendet werden, sobald ein WLAN im Unternehmen verfügbar ist.
- Die Erweiterung der Infrastruktur durch einen zusätzlichen Speicher (z.B. SAN) zur Erhöhung der Ausfallsicherheit.

²¹ vSphere Client (Programm), Bitdefender Security Console, View Administrator (beide über Webbrowser)

²² Bedarf für 20 physikalische Desktop PCs (je 5GB) ca. 100GB, Bedarf für 20 Linked Clones (5GB Deltadateien) zzgl. 1x Golden Image (5GB) ca.10GB [Speicherbedarf für Benutzerdateien ist für beide Systeme gleich]

²³ Bei Updatedauer 6min; Desktop PC: 20x6min + 15min für Platzwechsel = 135min je Updatevorgang, Linked Clones: 1x6min + 5min für Snapshot erstellen + 5min für Poolanpassung = 16min je Updatevorgang

ANHANG

Anhang A: Nutzwertanalyse.....	1
Anhang B: Berechnung der Energieersparnis	2
Anhang C: Vergleich der Bitdefender Lizenzmodelle	3
Anhang D: Nutzerdokumentation.....	4
Anhang E: Bildmaterialien.....	9
Anhang F: Serverkonfiguration	13
Anhang G: Zeitlicher Ablauf	16
Anhang H: Glossar.....	17
Anhang I: Quellenverzeichnis	18

ANHANG A: NUTZWERTANALYSE

Der Vergleich basiert auf Internetrecherchen und eigenen Erfahrungswerten. Die Punktevergabe erfolgt anhand des Nutzenbeitrages von 0 (=Keinen Nutzenbeitrag) bis 5 (=besonders hoher Nutzenbeitrag).

Kriterium	Hypervisor	Administration	Performance	Preis	Anforderungen	gesamt
Gewichtung	25%	25%	20%	20%	10%	100%
VMware	5	5	4	4	3	21
gewichtet	1,25	1,25	0,8	0,8	0,3	4,4
Citrix	3	4	3	2	5	17
gewichtet	0,75	1	0,6	0,4	0,5	3,25

Hypervisor: VMware stellt mit vSphere 5 den zurzeit besten *Hypervisor* dar. Dabei punktet vor allem die höhere Dichte an VMs pro *Host*, die sehr einfache Administration und Bereitstellung von Updates über das vCenter sowie die Automatisierung vieler Mechanismen (*vMotion*, *DRS*).

Administration: Das vCenter ist sehr übersichtlich und einfach aufgebaut und ermöglicht es den Administrator mit geringem Aufwand den *Host*status und die VMs zu verwalten. Die Administration der Desktops wird über die Webbrowser Oberfläche des View Administrators durchgeführt. Mit Hilfe dieser Tools können VMs und Desktoppools schnell erstellt und bereitgestellt werden. Auch das Update-Management ist einfacher, da nach Auswahl des Clusters die Updatevorgänge (herunterladen und installieren der Updates, verschieben der VMs) automatisch durchgeführt werden.

Performance: Die eigens entwickelten Protokolle (VMware = *PCoIP*, Citrix = *HDX*) unterscheiden sich in ihren Leistungswerten kaum. Jedoch ist die Auslastung der VM-CPU etwas geringer bei der Verwendung des *PCoIP*, womit Ressourcen effektiver genutzt werden können.

Preis: VMware bietet sein Paket mit einem Lizenzmodell je bestehende Verbindung an. Außerdem enthalten sind die Lizenzen für bis zu drei *Hypervisor* mit zwei CPU Sockeln. Citrix kann ebenfalls als Modell „je bestehende Verbindung“ erworben werden. Hierbei ist die Lizenz für einen XenServer enthalten. Daher müsste eine weitere Lizenz für den zweiten *Host* erworben werden. Dadurch wäre der Preis deutlich höher als bei VMware.

VMware View 5 Bundle (10 Pack)			XenDesktop Enterprise Edition ²⁴		
Art	+/-	Preis je 10 User	Preis für 20 User	Preis je 10 User	Preis für 20 User
Einkaufspreis					
Support	+				
Hypervisor	+	-	-		
gesamt					

²⁴ Citrixpreise basieren auf einen Wechselkurs von 1EUR = 1,29 USD

Anforderungen: Zum Verwenden der Desktops ist bei VMware der View Client notwendig. Dieser ist zurzeit für Windows, Linux, Android und iOS verfügbar und muss lokal installiert sein. XenDesktop kann auf nahezu jedem System verwendet werden²⁵. Auch die Serverstruktur für die Verwendung von View ist eingeschränkt (Windows Server 2008 for Core View services, *Active Directory*, VMware vSphere *hypervisor*). XenDesktop bietet auch hier mehr Freiheiten und lässt sich auf mehreren Grundstrukturen betreiben²⁶.

Zurück zur Dokumentation

ANHANG B: BERECHNUNG DER ENERGIEERSPARNIS

Die derzeit im Einsatz befindlichen Desktop PCs verbrauchen jeweils durchschnittlich 155 Watt pro Stunde (inkl. Monitor) an Energie (gemessen). Die folgende Tabelle zeigt die daraus resultierenden Kosten:

Desktop PCs	Energieverbrauch	Energiekosten ²⁷
Durchschnittlicher Energieverbrauch je Gerät	0,155 kWh	0,04 €/kWh
Anzahl Geräte	20	-
Verbrauch/Stunde [20 Geräte]	3,1 kWh	0,84 € /kWh
pro Arbeitstag [8 Stunden]	24,8 kWh / Tag	6,70 € /Tag
pro Arbeitswoche [5 Tage]	124 kWh/Woche	33,48 €/Woche
pro Jahr [252 Arbeitstage in 2013, Bremen]	6249 kWh/Jahr	1687,39 €/Jahr

Würde man die bisherigen Desktop PCs weiter verwenden, würden diese im Jahr 2013 ca. 1687,39 € an Energiekosten verursachen (vorausgesetzt die Mitarbeiter würden täglich 8 Stunden arbeiten und keinen Urlaub bis auf die gesetzlichen Feiertage haben).

zurück zur Dokumentation

Als Vergleich wurde der Energieverbrauch eines Samsung TC240 Thin-Clients gemessen und der Verbrauch für das Jahr 2013 unter denselben Bedingungen ermittelt. Diese haben jeweils einen durchschnittlichen Verbrauch von 40 Watt pro Stunde (inkl. Monitor).

Thin Clients	Energieverbrauch	Energiekosten
Durchschnittlicher Energieverbrauch je Gerät	0,04 kWh	0,01 €/h
Anzahl Geräte	20	-
Verbrauch/Stunde [20 Geräte]	0,8 kWh	0,22 €/kWh
pro Arbeitstag [8 Stunden]	6,4 kWh/Tag	1,73 € /Tag
pro Arbeitswoche [5 Tage]	32 kWh/Woche	8,64 €/Woche
pro Jahr [252 Arbeitstage in 2013, Bremen]	1612,8 kWh/Jahr	435,46 €/Jahr

Da für die Verwendung von Thin-Clients Server benötigt werden, müssen diese für einen Vergleich berücksichtigt werden. Aufgrund der Leistung der Hosts kann ein Host alle VMs bereitstellen, wobei durchschnittlich 410 Watt pro Stunde benötigt werden. Außerhalb der Geschäftszeiten verbraucht dieser Server 190 Watt pro Stunde für die Grundsysteme

²⁵ Windows, Linux, Mac OS, iOS, Android, Windows, Mobile, Solaris, DOS, Symbian, Thin Clients, Webbrowser, Java

²⁶ Windows Server 2008 for core XenDesktop services, Active Directory, Citrix XenServer, VMware vSphere, Microsoft Hyper-V hypervisor

²⁷ Bei einem Energiepreis von 0,27€/kWh

Host (innerhalb der Arbeitszeiten)	Energieverbrauch	Energiekosten
Durchschnittlicher Energieverbrauch	0,41 kWh	0,11 €/kWh
pro Arbeitstag [8 Stunden]	3,28 kWh/ Tag	0,89 € /Tag
pro Arbeitswoche [5 Tage]	16,4 kWh/Woche	4,43 €/Woche
pro Jahr [252 Arbeitstage in 2013, Bremen]	826,56 kWh/Jahr	223,17 €/Jahr
Host (außerhalb der Arbeitszeiten)	Energieverbrauch	Energiekosten
Durchschnittlicher Energieverbrauch	0,19 kWh	0,05 €/kWh
pro Arbeitstag [16 Stunden]	3,04 kWh/ Tag	0,82 € /Tag
pro Woche [5 Arbeitstage]	24,32 kWh/Woche	6,57 €/Woche
pro Jahr [252 Arbeitstage in 2013, Bremen]	766,08 kWh/Jahr	206,84 €/Jahr
Host (an Wochenenden & Feiertagen)	Energieverbrauch	Energiekosten
Durchschnittlicher Energieverbrauch	0,19 kWh	0,05 €/kWh
pro Tag [24 Stunden]	4,56 kWh/ Tag	1,23 € /Tag
im Jahr [113 Tage in 2013, Bremen]	515,28 kWh/Jahr	139,13 €/Jahr
Host-Gesamtkosten		569,14 € Jahr

Um die Energiekostenersparnis zu ermitteln werden die Kosten für die Thin Clients und des Hosts addiert und mit den Kosten der Desktop PCs verglichen:

	Desktop PCs	Thin Clients	Hosts
Energiekosten/Jahr	1687,39 €	435,46 €	569,14 €
gesamt	1687,39 €	1004,80 €	
Ersparnis durch Virtualisierung		682,80 € /Jahr	

Durch den Einsatz der Thin-Clients lassen sich die jährlichen Energiekosten des Kunden um ca. 40 % senken.

[zurück zur Dokumentation](#)

ANHANG C: VERGLEICH DER BITDEFENDER LIZENZMODELLE

Das Produkt Security for Virtualized Environments von Bitdefender kann auf zwei Arten lizenziert werden.

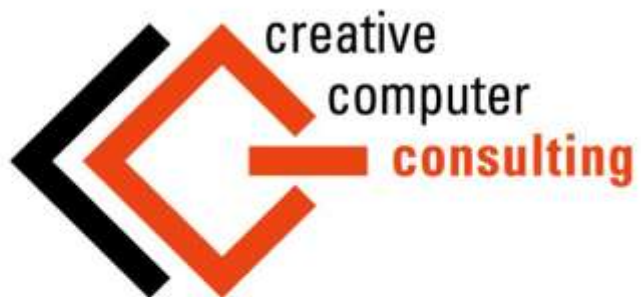
1. Lizenzierung anhand der Anzahl der zu schützenden VMs zu einem Preis von XXXX je VM
2. Lizenzierung anhand der CPU-Sockel der Hosts zu einem Preis von XXXX je Sockel

Beide Möglichkeiten werden verglichen, um das für den Kunden beste Modell zu wählen.

	Anzahl der VMs	Preis	Anzahl der Sockel	Preis
Basispreis	1	XXXX	1	XXXX
Projekt bezogen	24	XXXX	4	XXXX

Durch den Vergleich der Modelle lässt sich feststellen, dass für dieses Projekt die Lizenzierung nach Anzahl der eingesetzten VMs die bessere Wahl ist. Dabei werden die max. 20 virtuellen Desktops + die zwei virtuellen Server geschützt und zusätzlich zwei weitere Lizenzen als Reserve vorgehalten. Eine Lizenzierung anhand der CPU-Sockel würde zwar erlauben mehr als 24 VMs zu schützen, jedoch ist dies zurzeit nicht erforderlich, da durch die Lizenz von VMware View nur 20 virtuelle Desktops gleichzeitig bereitgestellt werden können. Ein Wechsel des Lizenzmodells ist jedoch jederzeit möglich.

[zurück zur Dokumentation](#)



Benutzerdokumentation für den Administrator

VMware vSphere 5, View 5.1

Bitdefender Security for Virtualized Environments

Erstellt durch Marcel Heimke

Erstellt am 08.03.2013

Stand 08.03.2013

²⁸ Die Werte wurden zur Veranschaulichung der Teststellung entnommen

1. SYSTEMINFORMATIONEN

1.1 SYSTEMZUGÄNGE/ADRESSEN

	ESX1.test.local	ESX2.test.local
Service Processor		
Management IP-Adresse	192.168.1.253	192.168.1.252
Login [Username//password]	root//*****	
Hypervisor Management		
Management IP-Adresse	192.168.1.251	192.168.1.250
Login [Username//password]	root//*****	
Bitdefender		
Security Console	192.168.1.248	
Login [Username//Password]	support@3xc.de//*****	
SVA IP-Adresse	192.168.1.247	192.168.1.256
Login [Username//Password]	Admin//*****	
vCenter		
Name	VIEW.test.local	
Login [Username//Password]	Test.local\Administrator//*****	
vMotion Ip-Adresse	10.20.30.1	10.20.30.2
MS SQL 2008 R2 Express		
Servename	vCenter\VIM_SQLEXP	
Login [Username//Password]	Test.local\Administrator//*****	
View Server		
	vCenter	Connection Server
IP-Adresse	192.168.1.30	192.168.1.40
Login [Username//Password]	Test.local\Administrator//*****	

1.2 PORTBELEGUNGEN DER SERVER

Servename: vCenter	
HTTPS-Port	443
HTTP-Port	80
Taktsignal-Port (UDP)	902
HTTP-Port für Webservices	8080
HTTPS-Port für Webservices	8443
Webservices-Port für den Änderungsbenachrichtigungsdienst	60099
LDAP-Port	389
SSL-Port	636
View Composer Port	18443
MS SQL 2008 R2 Express Remote Port	1433
Servename: Connection Server	
HTTPS-Port	443
HTTP-Port	80
PCoIP-Port	4172

Sollten Sie darüber hinaus Fragen oder Probleme haben rufen Sie uns an unter 0421 / 346310 oder schreiben Sie eine E-Mail an support@3xc.de

2. VCENTER

2.1 VERBINDEN MIT DEM VCENTER

1. vSphere Client mit Hilfe einer Hypervisor Management IP-Adresse auf den Computer herunterladen und installieren.
2. vSphere Client starten, IP-Adresse/Name (VIEW.test.local) eingeben und „Windows-Sitzungsanmeldedaten verwenden auswählen“, wenn der angemeldete Benutzer über Administrationsrechte auf dem vCenterServer verfügt. Ansonsten mit Administrator//***** anmelden.

Im linken Bereich werden alle virtuellen Maschinen und Hosts, im mittleren Bereich die jeweiligen Informationen angezeigt. Alle durchgeführten Aufgaben werden im unteren Bereich angezeigt. Alle Vorgänge die automatisch durchgeführt wurden, wurden durch test.local\ViewAdmin initiiert.

2.2 ERSTELLEN EINER NEUEN VIRTUELLEN MASCHINE

1. Wählen Sie im Reiter Datei -> Neu -> virtuelle Maschine, und folgen sie den Anweisungen des Assistenten. Stellen Sie dabei sicher, dass der ausgewählte Speicher über ausreichend freie Speicherkapazität verfügt. Wählen Sie außerdem unter „Festplatte erstellen“ die „Thin-Bereitstellung“-Option aus.
2. Starten Sie die virtuelle Maschine und verbinden Sie das gewünschte Installationsmedium als virtuelles CD/DVD Laufwerk.
3. Installieren Sie das gewünschte Betriebssystem und Entfernen Sie das Medium nach der Installation.

3. VERWENDEN DES VIEW ADMINISTRATORS

3.1 VERBINDEN MIT DEM VIEW ADMINISTRATOR

1. Rufen Sie die IP-Adresse des Servers „Connection Server“ die Oberfläche des View Administrators auf (Adobe Flash Plugin benötigt).

2. Melden Sie sich als Administrator an

Auf der anschließenden Übersicht erhalten sie einen Überblick über den Status des Systems.

Wählen Sie

1. „Pools“, um einen neuen Desktoppool zu erstellen, einen bestehenden Pool zu bearbeiten oder zu löschen.
2. „Desktops“, um eine Übersicht aller erstellten Desktops mit Status zu erhalten, oder diese zurückzusetzen.
3. „Remote-Sitzungen“, um eine Übersicht aller aktuellen Sitzungen zu erhalten, Sitzungen zu trennen oder Benutzer abzumelden.

3.2 ERSTELLEN EINES NEUEN DESKTOPPOOLS

Stellen Sie vor der Erstellung eines neuen Desktoppools sicher, dass Sie folgende Schritte durchgeführt haben:

1. Eine virtuelle Maschine mit einem Gastbetriebssystem wurde installiert und dieser in die Domäne integriert wurde.
2. Zusatzsoftware wurde installiert.

Sollten Sie darüber hinaus Fragen oder Probleme haben rufen Sie uns an unter 0421 / 346310 oder schreiben Sie eine E-Mail an support@3xc.de

3. Bitdefender Silent Agent wurde installiert.
4. View Agent wurde installiert.
5. (Ein aktueller Snapshot für einen dynamischen Linked Clone Pool erstellt wurde)

Anschließend können Sie mit der Erstellung eines Pools fortfahren.

1. Klicken Sie nun unter „Pools“ auf „hinzufügen“ und wählen Sie die Art des Pools (Automatischer Pool/ Manueller Pool).
2. Wählen Sie unter Benutzerzuweisung „Dynamisch“.
3. Wählen Sie nun ob Sie eine vollständige virtuelle Maschine (nicht empfehlenswert) oder View-Composer-Klone verwenden wollen.
4. Vergeben Sie eine ID und Namen für den Pool und legen sie optional eine Beschreibung an.
5. Legen Sie nun die gewünschten Pool-Einstellungen fest.
6. (Geben Sie an, nach welchem Muster erstellte Klone benannt werden und wie viele Klone erstellt werden sollen)
7. Wählen Sie nun das Daten nicht umgeleitet werden sollen (Diese werden durch eine GPO umgeleitet)
8. (Geben Sie Informationen zu Golden Image, Speicherort und Ressourceneinstellungen des Pools an)
9. Schließen Sie die Erstellung ab und erteilen Sie Berechtigungen für den neu erstellten Pool

4. BITDEFENDER SVE

4.1 VERBINDEN MIT DER SECURITY CONSOLE

Mit Hilfe der Security Console können Sie den Sicherheitsstatus aller virtuellen Maschinen überprüfen, Scans durchführen lassen, oder neue virtuelle Maschinen sichern.

1. Geben Sie die IP-Adresse der Security Console in der Adressleiste Ihres Webbrowsers ein.
2. Loggen Sie sich mit ihren Benutzerdaten an.

Sie erhalten nun eine Übersicht über den System Status. Durch klicken auf die Unterpunkte können sie weitere Informationen aufrufen.

4.2 HINZUFÜGEN VON WEITEREN VIRTUELLEN MASCHINEN

Sie haben drei Möglichkeiten, um weitere virtuelle Maschinen in das System hinzuzufügen.

- Installation des Silent Agent über Webinstaller
- Installation des Silent Agent über automatische E-Mail
- Rollout des Silent Agent über die Security Console

Die ersten beiden Varianten erfordern ein direktes Eingreifen auf dem Zielsystem.

4.2.1 INSTALLATION MIT HILFE DES WEBINSTALLERS / AUTOMATISCHER EM-MAIL

1. Wählen Sie „Installation Area“ unter dem Reiter „Computers“
2. (a) Wählen Sie im Bereich rechts „Installation Link“ -> „Webinstaller“, um einen Downloadlink zu erstellen und zu öffnen
- 2.(b) Wählen Sie im Bereich rechts „Installation Link“ -> „Sendby Email“, um die Installationsdatei an eine(n) oder mehrere E-Mail Adresse(n) oder Verteiler zu versenden

Sollten Sie darüber hinaus Fragen oder Probleme haben rufen Sie uns an unter 0421 / 346310 oder schreiben Sie eine E-Mail an support@3xc.de

3. Installieren sie den Silent Agent auf dem System

4.2.2 ROLLOUT ÜBER DIE SECURITY CONSOLE

1. Wählen Sie „View Computers“ unter dem Reiter „Computers“
2. Wählen Sie „Show Managed & Unmanaged Computers“
3. Markieren Sie alle Maschinen auf denen der Bitdefender Silent Client installiert werden soll aus und wählen sie unter Quick Tasks „Deploy“
4. Geben Sie unter „Credentials“ ein Konto an, das berechtigt ist auf dem System Programme zu installieren (z. B. Domänenadministrator) und drücken Sie auf „Deploy“

Auf den Zielsystemen wird nun im Hintergrund der Silent Agent installiert und gestartet.

Sollten Sie darüber hinaus Fragen oder Probleme haben rufen Sie uns an unter 0421 / 346310 oder schreiben Sie eine E-Mail an support@3xc.de

ANHANG E: BILDMATERIALIEN

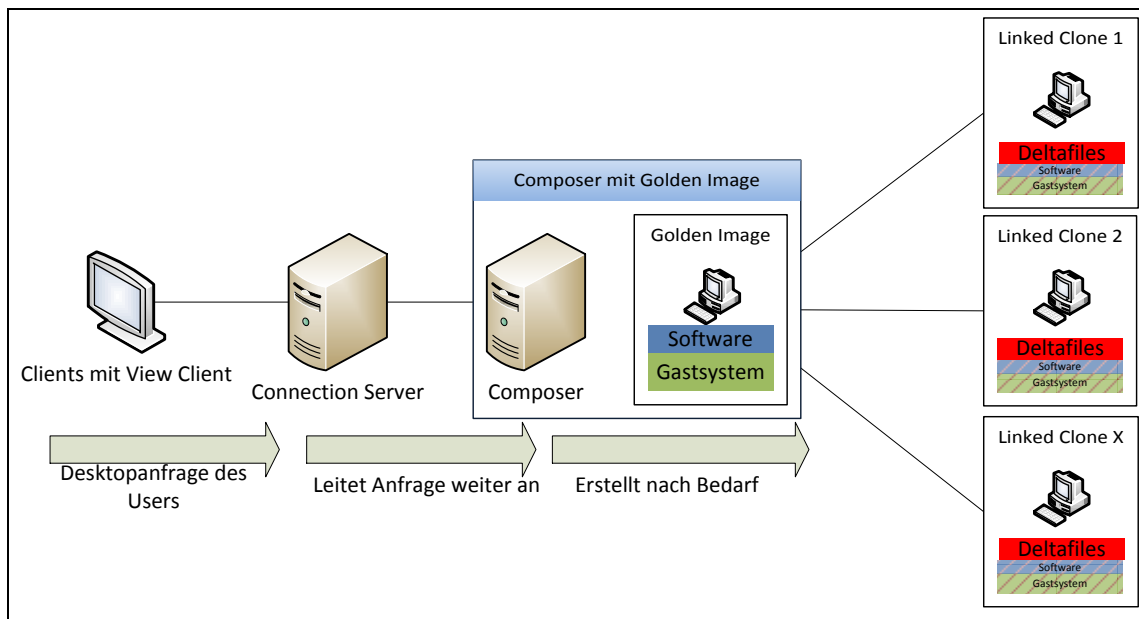


Abb.3 Linked Clones
[zurück zur Dokumentation](#)

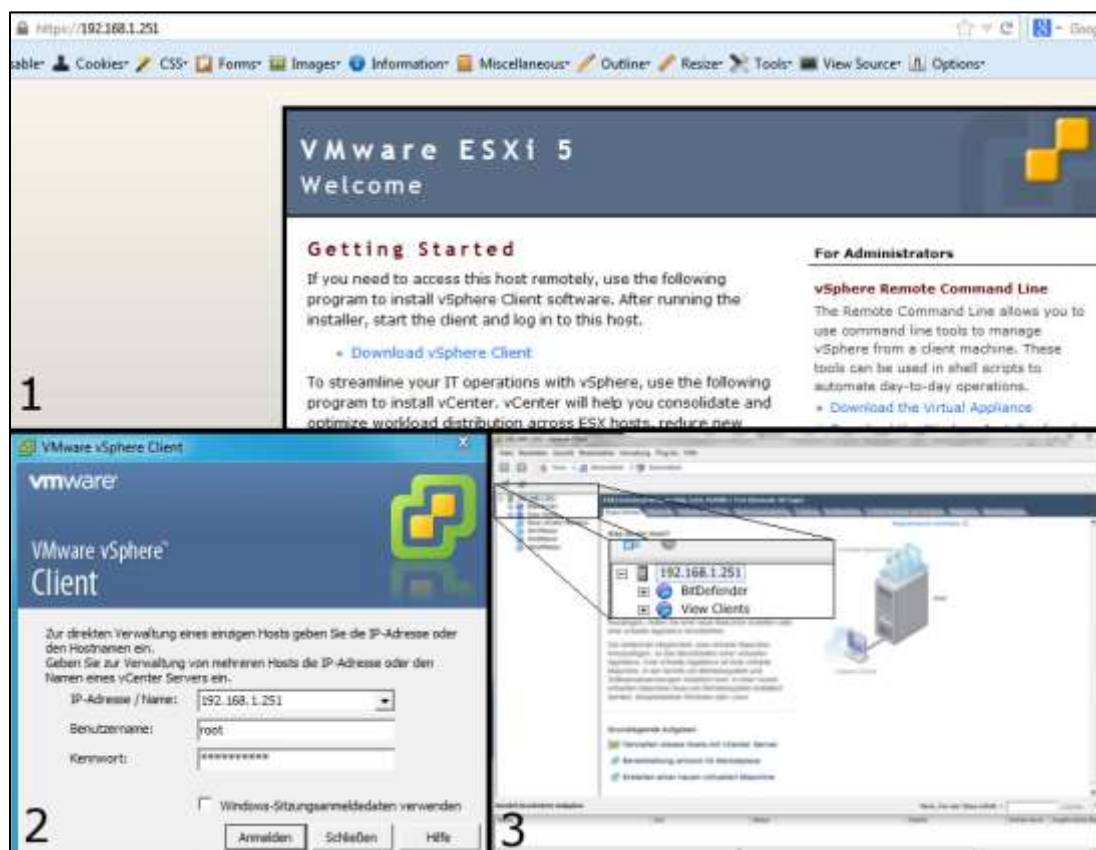


Abb. 7 Installation des vCenters 1
[zurück zur Dokumentation](#)

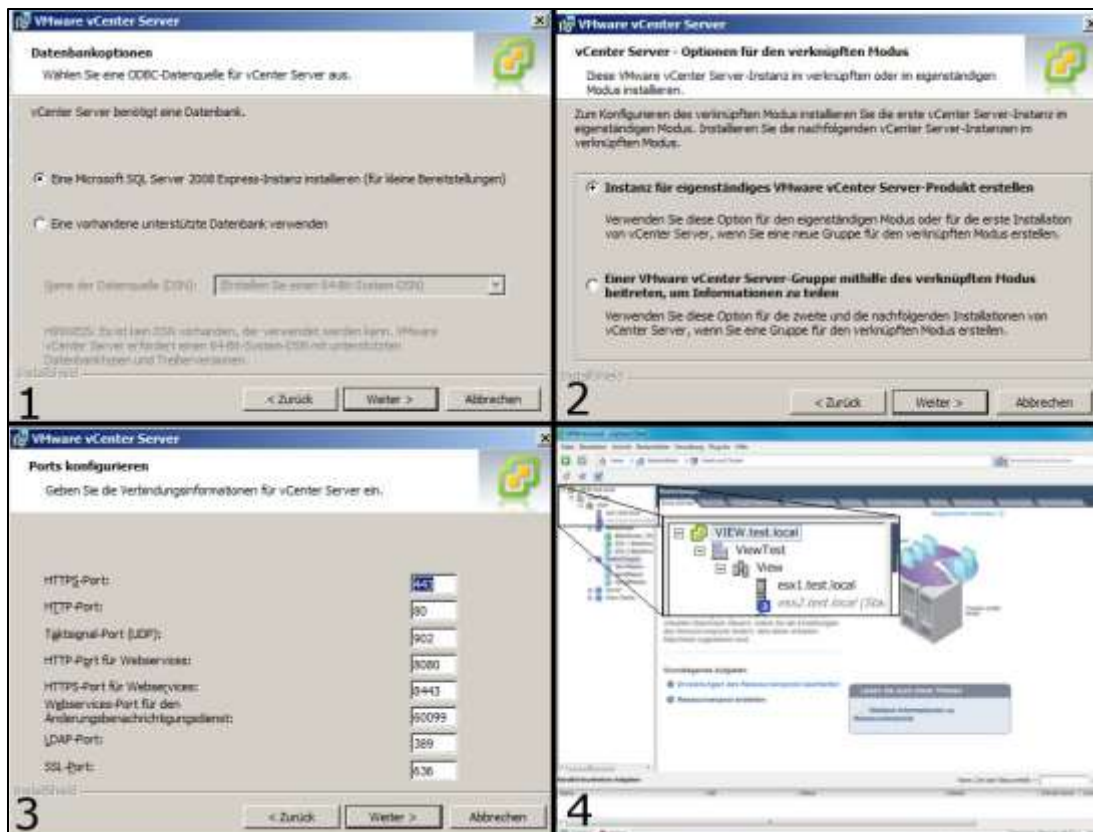


Abb. 8 Installation des vCenters 2
[zurück zur Dokumentation](#)

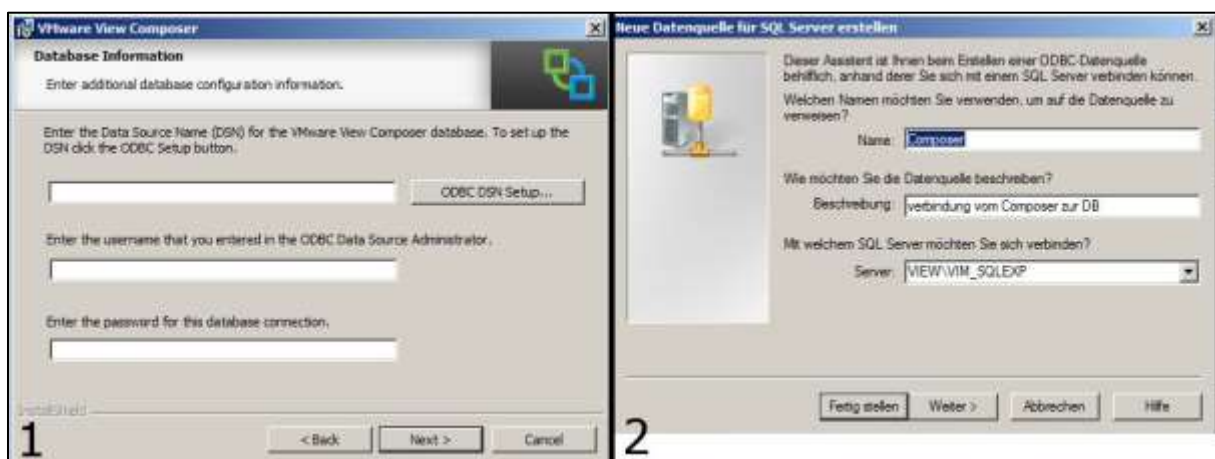


Abb. 9 Installation des View Composer
[zurück zur Dokumentation](#)

vCenter Server hinzufügen VC-Informationen View Composer View Composer-Domänen Hostzwischenspeicher Bereit zum Abschließen	vCenter Server-Informationen vCenter Server-Einstellungen Serveradresse: <input type="text" value="192.168.1.30"/> Benutzername: <input type="text" value="Administrator"/> Kennwort: <input type="password" value="*****"/> Beschreibung: <input type="text"/> Port: <input type="text" value="443"/> Erweiterte Einstellungen	vCenter Server-Einstellungen Installieren Sie, bevor Sie vCenter Server zu View hinzufügen, ein gültiges, von einer vertrauenswürdigen Zertifizierungsstelle signiertes SSL-Zertifikat. In einer Testumgebung können Sie das standardmäßige selbstsignierte Zertifikat verwenden, das mit vCenter Server installiert wird, müssen jedoch den Zertifikats-Fingerabdruck akzeptieren. Geben Sie den vCenter Server-FQDN oder die IP-Adresse, den Benutzernamen und das Kennwort ein.
	View Composer View Composer-Einstellungen <input type="radio"/> View Composer nicht verwenden <input checked="" type="radio"/> View Composer wurde zusammen mit vCenter Server installiert Wählen Sie diese Option, wenn View Composer auf demselben Server wie vCenter installiert ist Port: <input type="text" value="18443"/> <input type="radio"/> Eigenständiger View Composer Server	View Comp View Comp vCenter Ser eigenständig werden. Installieren Composer z gültiges, vor vertrauensw Zertifizierun

Abb. 10 Konfiguration des View Administrators
[zurück zur Dokumentation](#)

Quest vWorkspace Desktop Optimizer File Select Optimization Settings: <input checked="" type="checkbox"/> 18. Disable Large Send Offload <input checked="" type="checkbox"/> 19. Disable TCP/IP Offload <input checked="" type="checkbox"/> 20. Hide Hard Error Messages <input checked="" type="checkbox"/> 21. Disable DFS Change Notifications <input checked="" type="checkbox"/> 22. Disable Logon Screensaver <input checked="" type="checkbox"/> 23. Disable Hibernation <input checked="" type="checkbox"/> 24. Disabling Win 7 boot animation <input checked="" type="checkbox"/> 25. Delete Scheduled tasks <input checked="" type="checkbox"/> 26. Disable Application Experience <input checked="" type="checkbox"/> 27. Disable Base Filtering Engine <input checked="" type="checkbox"/> 28. Disable Background Intelligent Transfer <input checked="" type="checkbox"/> 29. Disable Function Discovery Resource Publication <input checked="" type="checkbox"/> 30. Disable Themes <input checked="" type="checkbox"/> 31. Disable Windows Defender <input checked="" type="checkbox"/> 32. Disable WLAN Autoconfig <input checked="" type="checkbox"/> 33. Disable Windows media player Network Sharing <input checked="" type="checkbox"/> 34. Disable HomeGroup Provider <input checked="" type="checkbox"/> 35. Disable Internet Connection Sharing <input checked="" type="checkbox"/> 36. Disable Routing and remote Access <input checked="" type="checkbox"/> 37. Disable Media Center Extender Service <input checked="" type="checkbox"/> 38. Disable Net.Tcp Port Sharing Service <input checked="" type="checkbox"/> 39. Lower Terminal Server Client send interval <input checked="" type="checkbox"/> 40. Disable auto logon	Description Monitor and reports security health settings on the computer Justification Requires additional CPU and memory, usually not needed in virtual desktops OS Version: All Impact: Low Category: CPU and memory Select All Unselect All Export Run Save Exit	Visuelle Effekte Erweitert Datenausführungsverhinderung Wählen Sie die Einstellungen, die für Darstellung und Systemleistung auf dem Computer verwendet werden sollen. <input type="radio"/> Optimale Einstellung automatisch auswählen <input type="radio"/> Für optimale Darstellung anpassen <input checked="" type="radio"/> Für optimale Leistung anpassen <input type="radio"/> Benutzerdefiniert: <input type="checkbox"/> Animation beim Minimieren und Maximieren von Fenstern <input type="checkbox"/> Animationen auf der Taskleiste <input type="checkbox"/> Durchsichtigen Hintergrund für Symbolunterschriften auf dem <input type="checkbox"/> Durchsichtigen Auswahlrechteck anzeigen <input type="checkbox"/> Fensterinhalt beim Ziehen anzeigen <input type="checkbox"/> Fensterschatten anzeigen <input type="checkbox"/> Kanten der Bildschirmschärten verfeinern <input type="checkbox"/> Mausschatten anzeigen <input type="checkbox"/> Menüelemente nach Aufruf ausblenden <input type="checkbox"/> Menüs in Ansicht ein- oder ausblenden <input type="checkbox"/> Miniaturansichten anstelle von Symbolen anzeigen <input type="checkbox"/> Miniaturansichtsvorschau für Taskleiste speichern <input type="checkbox"/> Offene Kombinationsfelder einblenden <input type="checkbox"/> Optimierten Bildlauf für Listenfelder verwenden <input type="checkbox"/> Peek aktivieren <input type="checkbox"/> QuickInfo in Ansicht ein- oder ausblenden <input type="checkbox"/> Steuerelemente und Elemente innerhalb von Fenstern animieren
---	--	--

Abb. 11 Leistungsoptimierung
[zurück zur Dokumentation](#)

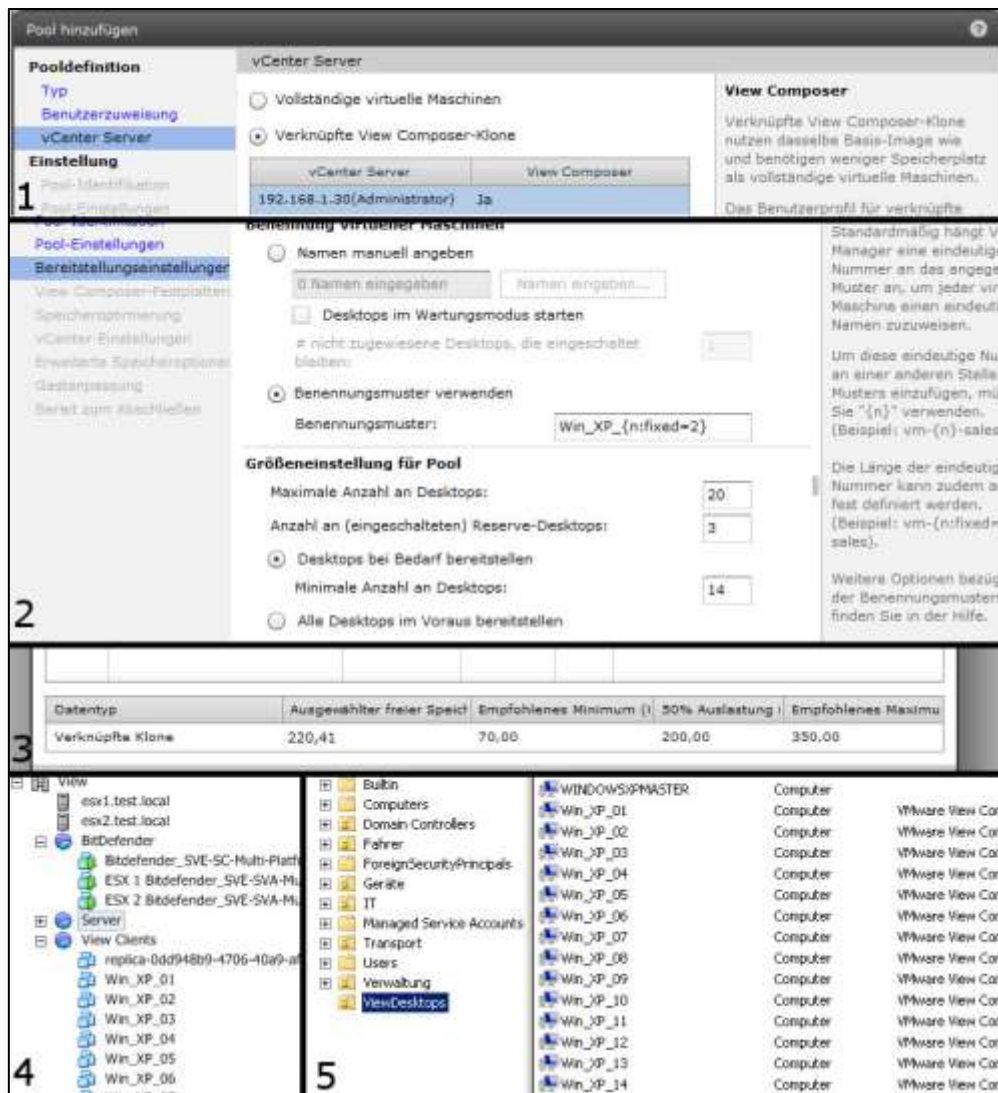



Abb.13 Erstellen eines Desktoppools
[zurück zur Dokumentation](#)

ANHANG F: SERVERKONFIGURATION

The Dell Online Store: Build Your System http://configure.euro.dell.com/dellstore/print_summary_details_popup...

Zusammenfassung drucken



**DELL PowerEdge™
R420**

Listenpreis [redacted]
Rabatt! [redacted]

Zwischensumme [redacted]

[Rückruf anfordern](#)

[Jetzt chatten](#)

Exklusiver Rabattgutschein
Jetzt 150 Rabatt auf alle Dell Server
ab einem Wert von mehr als 950 €!
Einfach Gutschein S0SZ7DQ7P9J99G
in den Warenkorb legen und an der
Kasse einlösen.
Das Angebot endet am 22. März 2013.
Recyceln Sie jetzt Ihren alten Dell
Server und sichern Sie sich 300€
Geld-zurück-Prämie für Einkäufe
über 800€!
zzgl. MwSt. und Versand
[Lieferinformationen](#)
Leasing ab **mtl.**
[Weitere Informationen](#)
[Details Sonderangebot](#)
[Vorläufiges Versanddatum: 27.02.2013](#)

Meine Auswahlen [Alle Optionen](#)

• **DELL PowerEdge™ R420**

Date	25.02.2013 12:40:49 Central Standard Time			
Katalognummer	808 Retail debsdt1			
Katalognummer / Beschreibung	Produktcode	Qty	SKU	ID
Basis:				
PowerEdge R420 TPM	513354	1	[210-39987]	1
Gehäusekonfiguration: 3.5" Chassis with up to 4 Hot Plug Hard Drives	513436	1	[350-11206] [470-13053]	1530
Prozessor: Intel® Xeon® E5-2407 2.20GHz, 10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W	513410	1	[213-15863] [412-10171]	1550
Zusätzlicher Prozessor: Intel® Xeon® E5-2407 2.20GHz, 10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W	513422	1	[374-14622] [412-10171]	1551
Arbeitsspeicherkonfigurations-Typ: Performance Optimized	511811	1	[370-22145]	1562
DIMM-Typ und DIMM-Geschwindigkeit: 1333 MHz RDIMMs	511806	1	[370-22140]	1561
Arbeitsspeicherkapazität: 8GB RDIMM, 1333 MHz, Low Volt, Dual Rank, x4	511802	8	[370-22136]	1560

1 von 3 25.02.2013 12:52

Vorinstalliertes Betriebssystem: Windows Server 2012, Standard Edition, Factory Installed, No Media, 2 Socket, 2 VMs	750360	1	[618-10758]	1650
Kits mit Betriebssystemmedien: No Media Required	511784	1	[805-11443]	1652
Internes SD-Modul: Internal Dual SD Module with 2x 2GB SD Card	546959	1	[385-11128] [385-11128] [385-11225] [385-11232]	1640
RAID-Konfiguration: C8 - RAID 1 for H310/H710, 2 SAS/SATA/SSD HDDs	513382	1	[780-13448]	1540
RAID-Controller: PERC H710 Integrated RAID Controller, 512MB NV Cache, Mini-type	511836	1	[405-12070]	1541
Festplatten: 300GB, SAS 6Gbps, 2.5-in, 10K RPM Hybrid Hard Drive (Hot Plug) in 3.5-in Carrier	546968	2	[400-19714]	1570
BIOS-Einstellungen für die Energieverwaltung: Performance BIOS Setting	393135	1	[223-10221]	1533
Netzteil: Dual Hot Plug Power Supplies 550W	513432	1	[450-18238] [450-18376]	1620
Netzkabel: Rack Power Cord, C13 to C14, PDU Style, 12A, 2M/6.5ft	204752	2	[450-12466]	1621
PCIe Riserkarte: PCIe Riser for Chassis with 2 Proc	513359	1	[330-10266]	1510
Integrierte Systemverwaltung: iDRAC7 Enterprise	513113	1	[528-10005] [528-10019]	1515
Add-in-Netzwerkadapter: Broadcom 5720 DP 1Gb Network Interface Card, Low Profile	683433	1	[540-11057]	1514
Add-in-Netzwerkadapter: On-Board Broadcom 5720 Dual Port 1GBE	702617	1	[540-11217]	1514
Blende: Bezel - 4/8 Drive Chassis	511723	1	[350-11089]	1532
Rackschienen: ReadyRails™ Sliding Rails Without Cable Management Arm	511759	1	[770-11605]	1610
Internes optisches Laufwerk: DVD, SATA, Internal for 4HDD chassis	708377	1	[429-16550]	1600
Clientzugriffslicenzen: No CALs Selected	750373	1	[618-10768]	1658
System Dokumentation: Electronic System Documentation and OpenManage DVD Kit for R420	513430	1	[631-11018]	1590
Versand: SHIP R420, NO, NO, EMEA1	513356	1	[340-29305]	1500
Bestellinformationen: PowerEdge Order - Germany	32382	1	[800-10498]	111
Basis-Service: 3Yr Basic Warranty - Next Business Day - Minimum Warranty	687355	1	[709-11196] [709-11197]	29
Support-Services: 5Yr ProSupport and Next Business Day On-Site Service	687374	1	[710-34783] [710-34785]	30

Dell Service: Installation:				
No Installation Service Selected (Contact Sales rep for more details)	58267	1	[683-11870]	1290
Remote Advisory Service:				
Declined Remote Advisory	691639	1	[715-10836]	735
Proactive Maintenance Services (Proaktive Wartung):				
Declined Proactive Maintenance (info)	135789	1	[713-10026]	140



Kontakte zu Dell

Dell Niederlassung Deutschland

Dell GmbH
Main Airport Center
Unterschweinstiege 2-14
60549 Frankfurt
Deutschland
Telefon: 069/9792-0
Telefax: 069/34824-8000

Bitte adressieren Sie keine Rücksendungen an diese Adresse, sondern kontaktieren Sie uns per mail und wir organisieren die Abholung für Sie.

[E-Mail an den kaufmännischen Kundendienst](#)

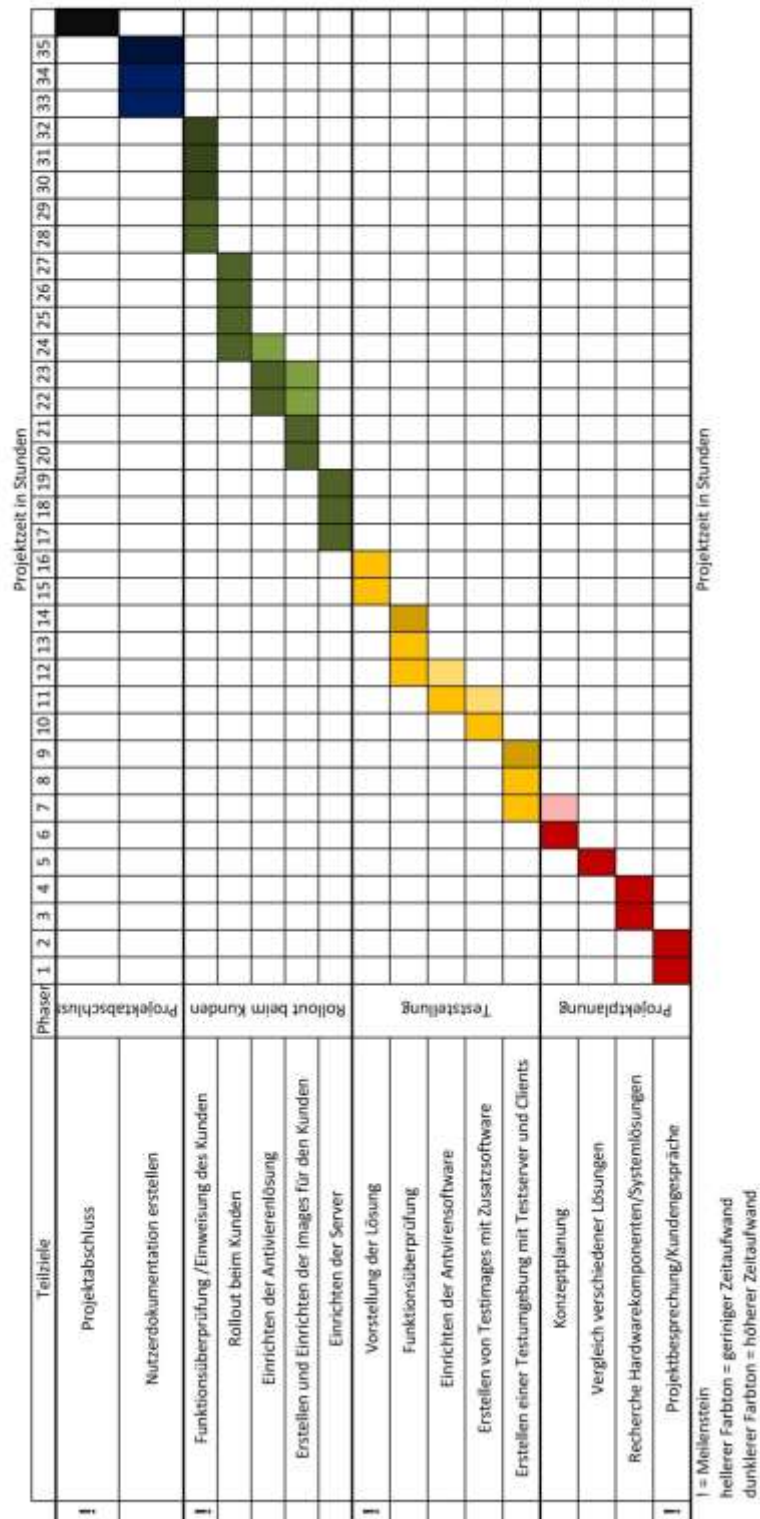
Notebook	Desktop-PCs	Business-Notebooks	Business-Desktops	Workstations	Server	Massenspeicher
Monitore	Drucker	Elektronik	Laptop	VMware	Alienware	Tablets
				Windows 8		Game PC
Copyright 1999-2013 Dell Inc.	Geschäftsbedingungen	Impressum / Anbieterkennzeichnung § 5 TMG	Nicht behobene Probleme	Datenschutz	Über unsere Anzeigen	Kontakte
						Unternehmensprofil
						Wegweiser
						Feedback

¹ * MfL: Leasingrate für Komfort/Lease bei unbestimmter Laufzeit (kalk. Grundlaufzeit 36 Monate) bei quartalsweise vorsch. Zahlung zzgl. gesetzl. MwSt. Mindestbestellwert 5000 EUR netto. Die Leasingraten, Sonder- und Schlusszahlungen berechnen sich nach den Anschaffungskosten des Leasingobjektes, dem gültigen Steuer- und Abgaberecht, der Verwaltungspraxis, der Geld- und Kapitalmarktlage. Ändern sich diese Daten bis zur Abnahme des Leasingobjektes, werden die Leasingzahlungen entsprechend angepasst. Ein Leasingvertrag kommt mit Annahme des Angebots durch Dell Capital Services (positive kreditrechtliche Prüfung vorbehalten) zustande. Dell Capital Services ist ein Programm der Delco Leasing GmbH, die zum Bereich GE Capital gehört. Gültig bis 05.12.2012. Die Aktion gilt ausschließlich für Client Produkte. Reine Softwareangebote und reine Serviceverlängerungen/Garantieverlängerungen sowie Microsoft Lizenzen sind nicht finanzierbar.

Original Windows Vista® Home Premium: Es gelten die allgemeinen Geschäftsbedingungen der Dell GmbH. Druckfehler, Irrtümer und Änderungen vorbehalten. Dell™, das Dell™ Logo, Dimension™, Inspiron™ und Xeon™ sind Marken der Dell™ Inc. Intel™, Intel® Logo, Intel® Inside, Intel® Inside Logo, Celeron®, Intel® XScale™, Intel® Xeon™, Intel® SpeedStep®, Itanium®, und Pentium® sind Marken der Intel® Corporation oder ihrer Tochtergesellschaften in den USA oder anderen Ländern. Microsoft® und Windows® sind eingetragene Marken der Microsoft Corporation. Microsoft® Windows® Mobile™ ist Marke der Microsoft Corporation. AMD, das AMD Arrow-Logo, AMD Opteron, AMD Athlon, AMD Turion, AMD PowerNow!, AMD Cool'n'Quiet (inkl. deren Kombinationen), sind Marken der Advanced Micro Devices, Inc.

snFG05

ANHANG G: ZEITLICHER ABLAUF



[zurück zur Dokumentation](#)

ANHANG H: GLOSSAR

iSCSI – iSCSI ist ein Protokoll zum Anbinden von externen Speichern an ein System. Dieser wird beim Zielsystem wie ein physikalisch eingebauter Speicher verwaltet, wodurch z.B. bessere Zugriffszeiten als bei Netzwerkfreigaben erreicht werden

NAS – Network Attached Storage, Festplattenspeicher der innerhalb eines Netzwerkes verwendet werden kann

Hotspare – Bezeichnung einer Reservefestplatte, die das Wechseln von defekten Festplatten während des laufenden Betriebes ermöglicht

Shared Storage – Bezeichnung für Festplattenspeicher, der von mehreren Servern innerhalb eines Netzwerkes genutzt werden kann

Host – hier: physikalischer Server, auf dem *virtuelle Maschinen* bereitgestellt werden können.

Hypervisor – Basisbetriebssystem, dass mehrere virtuelle Computer und die Ressourcen des Host verwaltet

Cluster – zentral verwalteter Verbund von zwei oder mehr *Hosts*

Ressourcenpool – organisatorische Einheit innerhalb eines *Clusters* zur effektiven Verteilung der vorhandenen Ressourcen (z.B. Arbeitsspeicher, CPU)

VM – Virtuelle Maschine, Computer, der nicht direkt auf dem physikalischen Computer ausgeführt wird, sondern in einer durch den *Hypervisor* bereitgestellten Umgebung. Dadurch können mehrere virtuelle - auf einem physikalischen Computer verwendet werden

Golden Image – dient als Vorlage für das Erstellen weiterer Klone in einer virtuellen Umgebung

Linked Clone – verknüpfter Klon des Golden Image, in dem nur Deltafiles gespeichert werden müssen

Snapshot – hier: Aufzeichnung eines Systemzustandes zu einem bestimmten Zeitpunkt

Deltafiles – hier: Dateien, die sich unterscheiden, zB. Zwischenspeicherungen bei Websitenaufrufen, in diesem Zusammenhang auch durch Benutzer erstellte Dokumente etc.

SVA – Security Virtual Appliance, linuxbasierende *VM* des Herstellers Bitdefender, die auf das Scannen von virtuellen Systemen spezialisiert ist

vCPU – virtual Central Processing Unit, hier: durch den Hypervisor bereitgestellter Prozessor

pCPU – physical Central Processing Unit, hier: auf einem Host tatsächlich vorhandener Prozessor

DHCP – Dynamic Host Controll Protocol, Dienst der IP-Adressen auf Anfrage an *Clients* vergibt

DNS – Domain Name System, wandelt Computernamen in IP-Adresse um und umgekehrt

AD DS – Active Directory Domain Services, hier: auch nur Active Directory, Microsoft Verzeichnisdienst für die zentrale Verwaltung von Benutzerkonten

OU – Organisation Unit, Organisatorische Einheit innerhalb des AD DS

ISO – Bezeichnung für ein Speicherabbild einer CD oder DVD

Primäres Bootdevice: Bezeichnung des Laufwerkes, von dem der Computer als erstes versucht zu starten. Wenn dies nicht möglich ist, wird automatisch das sekundäre Bootdevice gewählt usw.

OVF – Open Virtualization Format, standardisiertes Format für die Exportieren von VMs

PCoIP – Personal Computer over Internet Protocol, Protokoll für die Verwendung von View Desktops

HDX – Protokoll für die Verwendung von XenDesktop

RDP – Remote Desktop Protocol, Microsoft Protokoll für das Herstellen von Remote-Desktop-Verbindungen

vMotion – vCenter-Funktion zum Verschieben von VMs während des laufenden Betriebes

DRS – Distributed Resources Scheduler – vCenter Funktion für die automatische Lastverteilung zwischen Host eines Clusters

ANHANG I: QUELLENVERZEICHNIS

Vergleich Betriebssysteme:

<http://www.itfacts.org/2012/10/windows8-gegen-windows7/>

aufgerufen am 25.02.2013, 10:15 Uhr

Vergleich der Virtualisierungssoftware:

<http://www.infoworld.com/d/virtualization/virtualization-shoot-out-citrix-microsoft-red-hat-and-vmware-666?source=fssr>

aufgerufen am 25.02.2013, 10:30 Uhr

<http://www.infoworld.com/d/virtualization/vdi-shoot-out-citrix-xendesktop-vs-vmware-view-181691?page=0,0>

aufgerufen am 25.02.2013, 10:50 Uhr

<http://www.vmware.com/files/pdf/techpaper/PCoIPvHDXsinglesession03-05-12.pdf>

aufgerufen am 25.02.2013, 11:00 Uhr

<http://virtualization.findthebest.com/compare/1-8-10/VMware-vSphere-Enterprise-Plus-vs-Citrix-XenServer-Advanced-Edition-vs-Citrix-XenServer-Enterprise-Edition>

aufgerufen am 25.02.2013, 11:35 Uhr

Hardware:

<http://pubs.vmware.com/view-51/topic/com.vmware.ICbase/PDF/view-51-architecture-planning.pdf>

aufgerufen am 25.02.2013, 12:00 Uhr

<http://www.dell.com/de/unternehmen/p/poweredge-rack-servers>

aufgerufen am 25.02.2013, 12:30 Uhr

Antivirensoftware:

<http://www.bitdefender.de/sve>

aufgerufen am 25.02.2013, 16:10 Uhr

http://download.bitdefender.com/SMB/SVE/SVE-1.2/VMware-vShield/Bitdefender_SVE_VMwarevShield_AdminsGuide_deDE.pdf

aufgerufen am 25.02.2013, 16:15 Uhr

Einrichten von VMware View:

<http://pubs.vmware.com/view-51/topic/com.vmware.ICbase/PDF/view-51-installation.pdf>

aufgerufen am 28.02.2013, 15:30 Uhr

<http://pubs.vmware.com/view-51/topic/com.vmware.ICbase/PDF/view-51-administration.pdf>

aufgerufen am 28.02.2013, 15:30 Uhr

Sonstige:

<http://cc-asp.fraunhofer.de/docs/PCvsTC-de.pdf>

aufgerufen am: 27.02.2013, 10:10 Uhr

<http://www.microsoft.com/de-de/windows/endofsupport.aspx>

aufgerufen am 27.02.2013, 10:30 Uhr

<http://www.microsoft.com/en-us/download/details.aspx?id=22985>

aufgerufen am 28.02.2013, 16:45 Uhr