



(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
06.10.2021 Patentblatt 2021/40

(51) Int Cl.:
G06F 8/658 ^(2018.01) **G06F 11/14** ^(2006.01)
G06F 9/455 ^(2018.01)

(21) Anmeldenummer: **20167131.0**

(22) Anmeldetag: **31.03.2020**

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA ME
Benannte Validierungsstaaten:
KH MA MD TN

(71) Anmelder: **Siemens Mobility AG**
8304 Wallisellen (CH)

(72) Erfinder: **LOCHER, Viktor**
8200 Schaffhausen (CH)

(74) Vertreter: **Deffner, Rolf**
Siemens Mobility GmbH
Postfach 22 16 34
80506 München (DE)

(54) **VERFAHREN ZUM QUASI-UNTERBRUCHFREIEN PATCHEN VON EINEM WINDOWS-SYSTEM**

(57) Die vorliegende Erfindung offenbart ein Verfahren zum quasiunterbrechungsfreien Patchen von einem eine insbesondere sicherheitsrelevante Applikation ausführenden Windows-System (WR), umfassend:

a) Aufsetzen des die Applikation (ILTIS) ausführenden Windows-Systems (WR) in einer Produktiv-Instanz (2) mit einer eigenen Produktiv-Speicherinstanz (6) und einer Passiv-Instanz (4) mit einer eigenen Passiv-Speicherinstanz (8);

b) Installieren der Applikation (ILTIS) und ggfs. von für ihre Ausführung erforderlichen Daten auf einer weiteren Applikations-Speicherinstanz (10) und Verbinden dieser Applikations-Speicherinstanz (10) mit der Produktiv-Instanz (4) ;

c) Ausrüsten der Produktiv-Instanz (2) und der Passiv-Instanz (4) mit je einer Netzwerkkarte (12, 16 bzw. 14, 18) für ein Produktiv-Netzwerk (20) und ein Passiv-Netzwerk (22), wobei die Produktiv-Instanz (2) nur mit dem Produktiv-Netzwerk (20) und die Passiv-Instanz (4) nur mit dem Passiv-Netzwerk (22) verbunden ist,

d) Patchen der Passiv-Instanz (4) mit einer neuen Windows-Version über das Passiv-Netzwerk (22), wobei:
e) eine externe Supervisor-Instanz (iHME) bereitgestellt wird, mit der bedienergesteuert über eine der Supervisor-Instanz (iHME) eigenen Benutzeroberfläche:

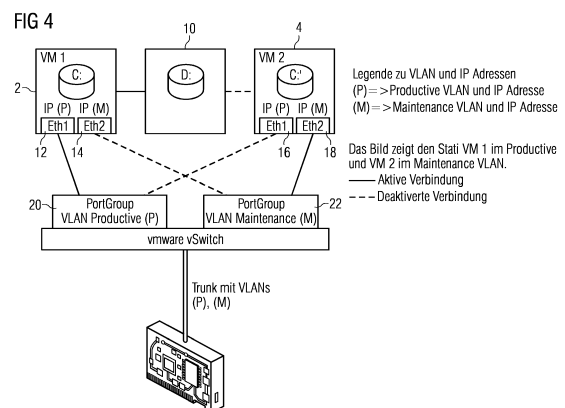
e1) nach erfolgreicher Installation des Patches der neuen Windows-Version die Produktiv-Instanz (2) und die Passiv-Instanz (4) heruntergefahren werden;

e2) die Applikations-Speicherinstanz (10) von der Produktiv-Instanz (2) auf die Passiv-Instanz (4) umgehängt wird;

e3) an der Produktiv-Instanz (2) die Netzwerkkarte (12) für das Produktiv-Netzwerk (20) durch die Netzwerkkarte (14) für das Passiv-Netzwerk (22) und an der Passiv-In-

stanz (4) die Netzwerkkarte (18) für das Passiv-Netzwerk (22) durch die Netzwerkkarte (16) für das Produktiv-Netzwerk (20) ausgetauscht wird; und

e4) nach erfolgreichem Abschluss der Schritte e1) bis e3) die bisherige Passiv-Instanz (4) als Produktiv-Instanz (2) und die bisherige Produktiv-Instanz (2) als Passiv-Instanz (4) neu gestartet werden.



Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zum quasi-unterbruchfreien Patchen von einem eine insbesondere sicherheitsrelevante Applikation ausführenden Windows-System.

[0002] Windows-Systeme werden solche Computersysteme genannt, die mit einem Betriebssystem OS der Microsoft Corp. ausgestattet sind. Ein derartiges Betriebssystem steuert die Abarbeitung von Operationen durch den eigentlichen Mikroprozessor, das Daten- und Speichermanagement, die Verwaltung der laufenden Anwenderprogramme und Applikationen, sämtliche Schnittstellen für Umsystem, wie Maus, Tastatur, Drucker, Scanner, Bildschirm, sowie sämtliche Kommunikationsschnittstellen usw.

[0003] Aufgrund der Komplexität und im Zuge der ständigen Verbesserung derartiger Betriebssysteme sind diese Betriebssysteme stets auf dem neuesten Stand zu halten, besonders dann, wenn auf dem Computersystem eine sicherheitsrelevante Applikation ausgeführt wird, wie dies beispielsweise bei einer Anlagensteuerung für eine industrielle Anlage (pharmazeutisch-technische oder chemische Anlage, Stromerzeugung und dergleichen) oder auch bei einem Zugdispositionssystem zur Steuerung von schienengebundenem Verkehr der Fall ist.

[0004] Besonders aufwändig ist das wiederholte Patchen von Windows-Systemen, bei dem kleinere funktionale und Security-bezogene Verbesserungen und Korrekturen am Betriebssystem in das Betriebssystem eingespielt werden müssen. Das Update (Patching) von einem Windows-Betriebssystem bedeutet aber in der Regel, dass die Ausführung des laufenden Betriebssystems während der Installation des Patches beeinträchtigt ist, da sich das Betriebssystem während der Patch-Installation in einem nicht definierten Zustand befindet. Aus diesem Grunde dürfen/können auch derartige sicherheitsrelevante oder sonst wie kritische Applikationen während der Zeitdauer des Patches nicht ausgeführt werden.

[0005] Somit kann es während der Installation eines neuen Patches zu einem längeren Unterbruch der Funktionalität kommen. Ausserdem ist das Windows-System nach der Installation des Patches noch nicht voll betriebsbereit, sondern muss erst neu gestartet werden, was den Unterbruch der Funktionalität zusätzlich verlängert.

[0006] Es kann zudem vorkommen, dass ein Microsoft-Patch fehlerhaft ist und zu Problemen im Betriebssystem und/oder in der Applikation führt. In dieser Situation wäre es wünschenswert einen Rollback-Mechanismus zu haben, welcher das Computersystem auf den exakten Stand vor der Installation des Patches zurückschaltet. Eine derartige Möglichkeit wird jedoch leider von der Microsoft Corp. nicht angeboten. An dieser Stelle kann möglicherweise nur das gesamte Neu-Aufsetzen des Betriebssystems Abhilfe schaffen, was zu einer noch längeren Unterbrechung der Funktionalität des Windows-Systems führt.

[0007] Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren zum quasi-unterbruchfreien Patchen von einem eine insbesondere sicherheitsrelevante Applikation ausführenden Windows-System anzugeben, bei dem sowohl eine Rollback-Möglichkeit besteht als auch der Unterbruch der Funktionalität durch den Patch-Vorgang auf ein Mindestmass beschränkt wird.

[0008] Diese Aufgabe wird erfindungsgemäss durch ein Verfahren zum quasi-unterbruchfreien Patchen von einem eine insbesondere sicherheitsrelevante Applikation ausführenden Windows-System gelöst, umfassend:

- a) Aufsetzen des die Applikation ausführenden Windows-Systems in einer Produktiv-Instanz mit einer eigenen Produktiv-Speicherinstanz und einer Passiv-Instanz mit einer eigenen Passiv-Speicherinstanz;
- b) Installieren der Applikation und ggfs. von für ihre Ausführung erforderlichen Daten auf einer Applikations-Speicherinstanz und Verbinden dieser Applikations-Speicherinstanz mit der Produktiv-Instanz;
- c) Ausrüsten der Produktiv-Instanz und der Passiv-Instanz mit je einer Netzwerkkarte für ein Produktiv-Netzwerk und ein Passiv-Netzwerk, wobei die Produktiv-Instanz nur mit dem Produktiv-Netzwerk und die Passiv-Instanz nur mit dem Passiv-Netzwerk verbunden ist,
- d) Patchen der Passiv-Instanz mit den benötigten Windows-Patches über das Passiv-Netzwerk, wobei:
- e) eine externe Supervisor-Instanz bereitgestellt wird, mit der bedienergesteuert über eine der Supervisor-Instanz eigenen Benutzeroberfläche:

- e1) nach erfolgreicher Installation der Patches die Produktiv-Instanz und die Passiv-Instanz heruntergefahren werden;
- e2) die Applikations-Speicherinstanz von der Produktiv-Instanz auf die Passiv-Instanz umgehängt wird;
- e3) an der Produktiv-Instanz die Netzwerkkarte für das Produktiv-Netzwerk durch die Netzwerkkarte für das Passiv-Netzwerk und an der Passiv-Instanz die Netzwerkkarte für das Passiv-Netzwerk durch die Netzwerkkarte für das Produktiv-Netzwerk ausgetauscht wird; und
- e4) nach erfolgreichem Abschluss der Schritte e1) bis e3) die bisherige Passiv-Instanz als Produktiv-Instanz und die bisherige Produktiv-Instanz als Passiv-Instanz neu gestartet werden.

[0009] Auf diese Weise wird das Computersystem für die Applikation in zwei virtuellen Instanzen aufgebaut, wobei sich der Windows-Patch vollkommen rückwirkungsfrei für die Produktiv-Instanz auf der Passiv-Instanz installieren und testen lässt. Dieser Patch kann dadurch zu einem beliebigen Zeitpunkt vorgenommen wer-

den und muss beispielsweise bei sicherheitskritischen Anwendungen im Bahnverkehr nicht in nächtlichen Randzeiten ausgeführt werden. Die eigentliche Übergangsdauer zur Umschaltung der gepatchten Passiv-Instanz in die dann aktive Produktiv-Instanz vollzieht sich in einer sehr kurzen Zeitspanne, weil im Besonderen virtuell aufgesetzte Instanzen sehr rasch rebootet werden können. Somit wird der betriebliche Impact des Patchens auf eine sehr kleine Zeitdauer, wie z.B. nur einige Sekunden, minimiert. Besonders hilfreich ist hier auch der Einsatz der Supervisor-Instanz, die im einfachsten Fall von nur einem Memory-Stick aus gestartet und ausgeführt werden kann («Live-System») und die sich über ein vSpere-API an der Virtualisierungs-Schicht ankoppeln kann.

[0010] In logischer Weiterbildung der vorliegenden Erfindung kann dann nach einer vorgebbaren Zeitdauer auch die ehemalige Produktiv-Instanz auf die neue Windows-Version gepatcht werden. Sie bleibt aber dann weiter die Passiv-Instanz bis der nächste Windows-Patch ansteht.

[0011] Eine besonders vorteilhafte Ausgestaltung der Erfindung kann erzielt werden, wenn nach dem Neustart der bisherigen Passiv-Instanz (4) als Produktiv-Instanz (2) und der bisherigen Produktiv-Instanz (2) als Passiv-Instanz (4) auch ein Rollback ausgeführt werden kann, der vorherige Produktiv-Instanz (2) dann auch wieder als Produktiv-Instanz (2) und die vorherige Passiv-Instanz (4) dann auch wieder als Passiv-Instanz (4) ausführt. Auf diese Weise können eventuell doch nach dem Patchen und dem Umschalten auftretende Probleme isoliert werden. Die eigentliche Applikation kann nach einem kurzen Unterbruch zwecks Rollback zum Zurück-Umschalten auf die Situation vor dem Umschalten wieder störungsfrei ausgeführt werden. Allfällige Fehler können dann auf der Passiv-Instanz analysiert und behoben werden.

[0012] In einer weiteren vorteilhaften Ausgestaltung der vorliegenden Erfindung kann die Supervisor-Instanz so ausgestaltet sein, dass benutzergesteuert über deren Benutzeroberfläche vollständig automatisiert anhand von geschützten Spezifikationen ein virtueller Applikationsrechner aufgesetzt werden kann, der die Produktiv-Instanz mit eigener Produktiv-Speicherinstanz, die Passiv-Instanz mit eigener Passiv-Speicherinstanz und die Applikations-Speicherinstanz umfasst.

[0013] Um hohe Sicherheitsstandards beim Patchen der Passiv-Instanz und bei der späteren Umschaltung der gepatchten Passiv-Instanz in die dann aktive Produktiv-Instanz garantieren zu können, werden die mittels der Supervisor-Instanz (iHME) ausgelösten Schritte e1) bis e4) hard-codiert und können damit über die Benutzeroberfläche der Supervisor-Instanz (10) benutzergesteuert ausgelöst werden. Auf diese Weise ist es ausgeschlossen, dass ein Anwender Konfigurationen des Patches und der Produktiv- und Passiv-Instanz «on the fly» bewusst oder aus Versehen verändern kann.

[0014] Bevorzugte Ausführungsbeispiel der vorliegenden Erfindung werden nachfolgend anhand der Zeich-

nung näher erläutert. Dabei zeigen:

Figur 1 in schematischer Weise eine Benutzeroberfläche der Supervisor-Instanz zur Generierung virtueller Windows-Rechner für die Ausführung einer sicherheitskritischen Applikation, hier eines Zugdispositionssystems;

Figur 2 in schematischer Weise das Set-up der virtuellen Windows-Rechner;

Figur 3 in schematischer Darstellung den Aufbau eines Windows-Rechners für eine Leittechnikzelle des Zugdispositionssystems; und

Figur 4 in schematischer Darstellung den eigentlichen Umschaltvorgang für den Wechsel auf einen neuen Windows-Patch der Produktiv-Instanz einer Leittechnikzelle.

[0015] Die vorliegende Erfindung wird hier nachfolgend nun am Beispiel eines Zugleitsystems (Zugdispositionssystem) erläutert. Ein derartiges Zugleitsystem wird von Siemens Mobility AG, Wallisellen, Schweiz, unter dem Namen ILTIS® Netz vertrieben. Mit diesem Zugleitsystem wird beispielsweise der gesamte Zugverkehr der Schweiz aus einer kleinen Anzahl von Zugleitsständen von Fahrdienstleitern gesteuert. Hierzu ist das Eisenbahnnetzwerk der Schweiz in eine Anzahl von geographisch klar abgegrenzten Leittechnikzellen aufgeteilt worden, wobei jede Zelle mehrere (auch virtuell aufgesetzte) Windows-Rechner zur Ausführung der ILTIS-Applikation umfasst.

[0016] Um nun einen derartigen Windows-Rechner auf einen neuen Patch upzugraden, ist gemäss der vorliegenden Erfindung ein Verfahren zum quasi-unterbruchsfreien Patchen dieses die ILTIS-Applikation ausführenden Windows-Systems vorgesehen. Ein zentraler Bestandteil des Verfahrens ist dabei die Verwendung der System-Virtualisierung und einer Supervisor-Instanz - nachfolgend kurz als iHME (integrated Hypervisor Management Environment) bezeichnet - , deren Benutzeroberfläche schematisch in Figur 1 gezeigt ist. Über diesen iHME lässt sich die Virtualisierung des Windows-Rechners für eine bestimmte ILTIS-Zelle erzielen. Der iHME ist somit eine Management-Software, welche über die offiziellen vSpere-APIs sowohl ESX-Hosts (also der Rechner mit dem Hypervisor) als auch ESX-Guests (die virtuellen Rechner-Instanzen auf dem Host) aufsetzen und verwalten kann.

[0017] Die Figuren 2 und 3 zeigen schematisch das Set-Up zum Aufsetzen der virtuellen Windows-Rechner zum Ausführen der ILTIS-Software (ILTIS-Applikation). Im Zuge der Ausführung des Verfahrens wird somit der iHME zum Aufsetzen des die ILTIS-Applikation ausführenden Windows-Rechners WR als Guest-Pair in einer Produktiv-Instanz 2 mit einer eigenen Produktiv-Speicherinstanz 6 und einer Passiv-Instanz 4 mit einer eige-

nen Passiv-Speicherinstanz 8 verwendet. Dieses Aufsetzen erfolgt über versionierte und geschützte Spezifikationen (auch gehashed), sodass ein Anwender an der vorgesehenen Konfiguration nichts ändern und diese auch nicht on-the-fly vornehmen kann. Dieses Aufsetzen schliesst somit das Erstellen der virtuellen Hardware (vDisk, vRAM, vCPUs, vSwitches, vNICs usw.) ein.

[0018] Mit dem iHME können nun auch die sogenannten Guest-Pairs verwaltet werden. Pro virtuellem Windows-Rechner WR gibt es somit die zwei Instanzen, die Produktiv-Instanz 2 und die Passiv-Instanz 4. Ausserdem wird mit dem iHME die ILTIS-Applikation und die für ihre Ausführung erforderlichen Daten auf einer weiteren Applikations-Speicherinstanz 10 (D-Laufwerk) installiert. Diese Applikations-Speicherinstanz 10 wird dann auch mit der Produktiv-Instanz 2 verbunden (wie in Figur 2 gezeigt). Diese vorstehend genannten Komponenten bilden somit den virtuellen Windows-Rechner WR. Im Zuge der Installation der Switches werden die Produktiv-Instanz 2 und die Passiv-Instanz 4 jeweils mit je einer Netzwerkkarte 12, 14, 16, 18 für ein Produktiv-Netzwerk 20 und ein Passiv-Netzwerk 22 ausgerüstet (vgl. Figur 4). Dabei wird die Produktiv-Instanz 2 nur mit dem Produktiv-Netzwerk 20 und die Passiv-Instanz 4 nur mit dem Passiv-Netzwerk 22 verbunden.

[0019] Steht nun ein Windows-Patch an, wird mittels des iHME die Installation des Patches zunächst nur auf der Passiv-Instanz 4 ausgeführt. Dabei kann die neue Windows-Version über das Passiv-Netzwerk 22 auf der Passiv-Instanz 4 (diese kann auch als Maintenance-Instanz bezeichnet werden) installiert werden. Diese Installation ist vollkommen rückwirkungsfrei für die Produktiv-Instanz 2. Auf diese Weise hat auch die zeitliche Dauer der Installation des Patches keinen Einfluss auf die ILTIS-Applikation, was ebenfalls auch für allfällige Reboots der Passiv-Instanz 4 gilt. Somit können nun auch die System-Eventlogs der Passiv-Instanz 4 nach dem Patchen geprüft werden, wodurch sichergestellt werden kann, dass die neue gepatchte Windows-Version auf der Passiv-Instanz 4 wieder stabil läuft. Das Ausrollen und Installieren des Patches kann so zu einem beliebigen Zeitpunkt stattfinden; es muss so auch nicht in Randzeiten des Eisenbahnbetriebs stattfinden.

[0020] Nach dieser erfolgreichen Installation des Patches erfolgt dann die Umschaltung von Produktiv- und Passiv-Instanz. Mit dem iHME werden nun bedienergesteuert über die dem iHME-eigene Benutzeroberfläche (siehe Figur 1) die Produktiv-Instanz 2 und die gepatchte Passiv-Instanz 4 heruntergefahren. Dabei wird die Applikations-Speicherinstanz 10 von der Produktiv-Instanz 2 auf die Passiv-Instanz 4 umgehängt und an der Produktiv-Instanz 2 wird die Netzwerkkarte 12 für das Produktiv-Netzwerk 20 durch die Netzwerkkarte 14 für das Passiv-Netzwerk 22 und an der Passiv-Instanz 4 die Netzwerkkarte 18 für das Passiv-Netzwerk 22 durch die Netzwerkkarte 16 für das Produktiv-Netzwerk 20 am virtuellen Switch umgehängt. Diese Situation ist in Figur 4 vor der Umschaltung gezeigt, was für die aktiven Verbindungen durch die durchgezogenen Linien und für die passiven Verbindungen durch die gestrichelten Linien repräsentiert. Nach der Umschaltung werden die durchgezogenen Linien zu gestrichelten Linien und die gestrichelten Linien zu durchgezogenen Linien. Nach dem erfolgreichen Abschluss dieser Schritte wird die bisherige Passiv-Instanz 4 als Produktiv-Instanz und die bisherige Produktiv-Instanz 2 als Passiv-Instanz neu gestartet werden.

[0021] Diese über die iHME initiierte Umschaltung wird über das vSphere-API realisiert. Die iHME steuert das Herunterfahren der Produktiv-Instanz 2 und der Passiv-Instanz 4, das Umhängen der Applikations-Speicherinstanz (Laufwerk D:/) und der beiden Netzwerkkarten beider Instanzen (Produktiv- und Passiv-Instanz) und den Neustart dieser beiden Instanzen. Diese haben nun ihre "Identitäten" vertauscht. Die ehemalige Produktiv-Instanz 2 verbleibt nun für eine vorbestimmbare Zeitdauer unverändert für Rollback-Szenarien erhalten. Nach Ablauf dieser Zeitdauer kann diese Instanz (nun als Passiv-Instanz) ebenfalls gepatcht werden, wobei durch diesen Vorgang ebenfalls keinerlei Rückwirkung auf die nun laufende Produktiv-Instanz 2 auftritt.

[0022] Wie in Figur 3 gezeigt, wird zum Beispiel bei der sicherheitskritischen ILTIS-Applikation beispielhaft ein zweiter virtueller und redundant betriebener Windows-Rechner analog dem soeben Beschriebenen betrieben. Darüberhinaus sei an dieser Stelle angemerkt, dass auch mehr als die zwei hier beschriebenen virtuellen ILtis-Rechner auf einem Host ausgeführt werden können.

[0023] Das Verfahren ist damit quasi-rückwirkungsfrei und kann zu einem beliebigen Zeitpunkt vorgenommen werden. Die Umschaltung von der ungepatchten auf die gepatchte Instanz dauert nur wenige Sekunden, da ein Reboot auf virtueller Hardware sehr rasch ausgeführt werden kann. Der Unterbruch der ILTIS-Applikation ist somit auf ein Minimum reduziert. Ein Rollback ist jederzeit möglich. Falls die gepatchte Instanz instabil laufen sollte, kann in wenigen Sekunden wieder auf die alte, stabile Umgebung zurückgeschaltet werden (erneutes Tauschen der Identitäten der beiden Instanzen).

[0024] Der durch das Verfahren bereitgestellte Mechanismus kann auch eingesetzt werden, um mit einer minimalen Down-time der Windows-Systeme und damit der ILTIS-Funktionalität von einer Version der Windows-Betriebssysteme auf eine neue Version migrieren zu können.

[0025] Das vorstehend beschriebene Verfahren stellt zudem eine Lösung dar, die mit einem einzelnen Rechner realisiert werden kann. Es braucht also keine komplexe und daher meist auch teure Infrastruktur, wie z.B. das Clustering von Hosts in einem Rechenzentrum. Es braucht lediglich die Supervisor-Instanz iHME, die auf einem beliebigen Windows-Rechner laufen kann, welcher mit dem Management-Port des iHME temporär oder permanent verbunden ist. Der iHME hat somit einen minimalen Footprint und ist sogar aus einem von einem

USB-Stick bootbaren mobilen Live-System lauffähig. Die Lösung ist zudem gleichermassen für grosse Umgebungen mit vielen virtuellen Windows-Rechnern, die auf einer Anzahl von Rechner (Hosts) verteilt sind, einsetzbar.

[0026] Die Lösung ist auch vergleichsweise einfach umsetzbar, weil sie zu einem grossen Teil auf in Windows-Systemen standardisierte Schnittstellen und Standard-Technologien zurückgreift, wie z.B. Windows-Betriebssystem und ESXi Hypervisor. Bereits mit einer Essential-Lizenz von VMWare ist das Verfahren voll funktionsfähig. Eine VMWare-Lizenz ist notwendig, damit mit dem iHME auf die ESXi-Schnittstellen zugegriffen bzw. eine Automatisierung des Verfahrens über die Schnittstellen vorgenommen werden kann.

[0027] Vorliegend ist das erfindungsgemässe Verfahren nun für eine Leittechnik-Applikation, hier ILTIS® Netz der Siemens Mobility AG, Wallisellen, Schweiz, erläutert worden. Grundsätzlich ist das Verfahren aber überall dort anwendbar, wo zeitkritisch oder sicherheitsrelevante Applikationen auf Windows-Rechnern ausgeführt werden, die nach von der Microsoft Corp. vorgegebenen Intervallen mit neuen Patches oder sogar neuen Betriebssystemversionen ausgeführt werden sollten oder sogar müssen. Derartige Prozesse (Applikationen) können beispielsweise in der Energieerzeugung und -übertragung, in der industriellen Fertigung, in Verkehrsleitsystemen für andere Fahrzeuggattungen usw. auf Windows-Rechnern ausgeführt werden.

Patentansprüche

1. Verfahren zum quasi-unterbruchfreien Patchen von einem eine insbesondere sicherheitsrelevante Applikation ausführenden Windows-System (WR), umfassend:

- a) Aufsetzen des die Applikation (ILTIS) ausführenden Windows-Systems (WR) in einer Produktiv-Instanz (2) mit einer eigenen Produktiv-Speicherinstanz (6) und einer Passiv-Instanz (4) mit einer eigenen Passiv-Speicherinstanz (8);
- b) Installieren der Applikation (ILTIS) und ggfs. von für ihre Ausführung erforderlichen Daten auf einer weiteren Applikations-Speicherinstanz (10) und Verbinden dieser Applikations-Speicherinstanz (10) mit der Produktiv-Instanz (4);
- c) Ausrüsten der Produktiv-Instanz (2) und der Passiv-Instanz (4) mit je einer Netzwerkkarte (12, 16 bzw. 14, 18) für ein Produktiv-Netzwerk (20) und ein Passiv-Netzwerk (22), wobei die Produktiv-Instanz (2) nur mit dem Produktiv-Netzwerk (20) und die Passiv-Instanz (4) nur mit dem Passiv-Netzwerk (22) verbunden ist,
- d) Patchen oder Neu-Aufsetzen der Passiv-Instanz (4) über das Passiv-Netzwerk (22), wobei:
- e) eine externe Supervisor-Instanz (iHME) bereitgestellt wird, mit der bedienergesteuert über

eine der Supervisor-Instanz (iHME) eigenen Benutzeroberfläche:

- e1) nach erfolgreicher Installation des Patches resp. der neuen Windows-Version die Produktiv-Instanz (2) und die Passiv-Instanz (4) heruntergefahren werden;
- e2) die Applikations-Speicherinstanz (10) von der Produktiv-Instanz (2) auf die Passiv-Instanz (4) umgehängt wird;
- e3) an der Produktiv-Instanz (2) die Netzwerkkarte (12) für das Produktiv-Netzwerk (20) durch die Netzwerkkarte (14) für das Passiv-Netzwerk (22) und an der Passiv-Instanz (4) die Netzwerkkarte (18) für das Passiv-Netzwerk (22) durch die Netzwerkkarte (16) für das Produktiv-Netzwerk (20) umgehängt werden; und
- e4) nach erfolgreichem Abschluss der Schritte e1) bis e3) die bisherige Passiv-Instanz (4) als Produktiv-Instanz (2) und die bisherige Produktiv-Instanz (2) als Passiv-Instanz (4) neu gestartet werden.

2. Verfahren nach Anspruch 1,

dadurch gekennzeichnet, dass

nach einer vorgebbaren Zeitdauer auch die ehemalige Produktiv-Instanz (2) auch auf die neue Windows-Version gepatcht wird.

3. Verfahren nach Anspruch 1 oder 2,

dadurch gekennzeichnet, dass

nach dem Neustart der bisherigen Passiv-Instanz (4) als Produktiv-Instanz (2) und der bisherigen Produktiv-Instanz (2) als Passiv-Instanz (4) auch ein Rollback ausgeführt werden kann, der vorherige Produktiv-Instanz (2) dann auch wieder als Produktiv-Instanz (2) und die vorherige Passiv-Instanz (4) dann auch wieder als Passiv-Instanz (4) ausführt.

4. Verfahren nach einem der vorangehenden Ansprüche,

dadurch gekennzeichnet, dass

die Supervisor-Instanz (iHME) so ausgestaltet ist, dass benutzergesteuert über deren Benutzeroberfläche ein virtueller Applikationsrechner (WR) aufgesetzt wird, der die Produktiv-Instanz (2) mit eigener Produktiv-Speicherinstanz (6), die Passiv-Instanz (4) mit eigener Passiv-Speicherinstanz (8) und die Applikations-Speicherinstanz (10) umfasst.

5. Verfahren nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet, dass

die mittels der Supervisor-Instanz (iHME) ausgelösten Schritte e1) bis e4) hard-codiert sind und damit über die Benutzeroberfläche der Supervisor-Instanz (10) benutzergesteuert ausgelöst werden.

10

15

20

25

30

35

40

45

50

55

FIG 1

iHME (Integrated Hypervisor Management Environment)

Connect Host New Host New Guest

Add Guest Common Settings Tools

Working Host

- test-hostm 1
 - iltis_cell_1
 - Productive Maintenance
- Stored Hosts**
 - test-hostm 1
 - test-m 2

Host Serial Number		YMHV005124														
Host Name		test-hostm1														
Host IP v4 Address		192.168.51.11														
Guest Name Hypervisor		iltis_cell_1@2														
Comment		This is a comment. It can be multiline.														
State		► Started														
Mounted Install Media																
Info		<table border="1"> <thead> <tr> <th>Key</th> <th>Value</th> </tr> </thead> <tbody> <tr><td>RAM Size</td><td>4096 MB</td></tr> <tr><td>CPU Socket count</td><td>1</td></tr> <tr><td>CPU Core per Socket count</td><td>4</td></tr> <tr><td>Disk Count</td><td>0</td></tr> <tr><td>NIC count</td><td>1</td></tr> <tr><td>GuestSpec Version</td><td>1</td></tr> </tbody> </table>	Key	Value	RAM Size	4096 MB	CPU Socket count	1	CPU Core per Socket count	4	Disk Count	0	NIC count	1	GuestSpec Version	1
Key	Value															
RAM Size	4096 MB															
CPU Socket count	1															
CPU Core per Socket count	4															
Disk Count	0															
NIC count	1															
GuestSpec Version	1															
Network Configuration		<table border="1"> <tbody> <tr> <td>vSwitch</td> <td>Physical NICs</td> <td>Port Group</td> </tr> <tr> <td>vSwitch _IltisCell</td> <td>vmnic2, vmnic3</td> <td>Portgroup IltisCell</td> </tr> </tbody> </table>	vSwitch	Physical NICs	Port Group	vSwitch _IltisCell	vmnic2, vmnic3	Portgroup IltisCell								
vSwitch	Physical NICs	Port Group														
vSwitch _IltisCell	vmnic2, vmnic3	Portgroup IltisCell														
Managed Guest																
Shutdown	Restart	Open console Connect USB Device Delete Guest														

FIG 2

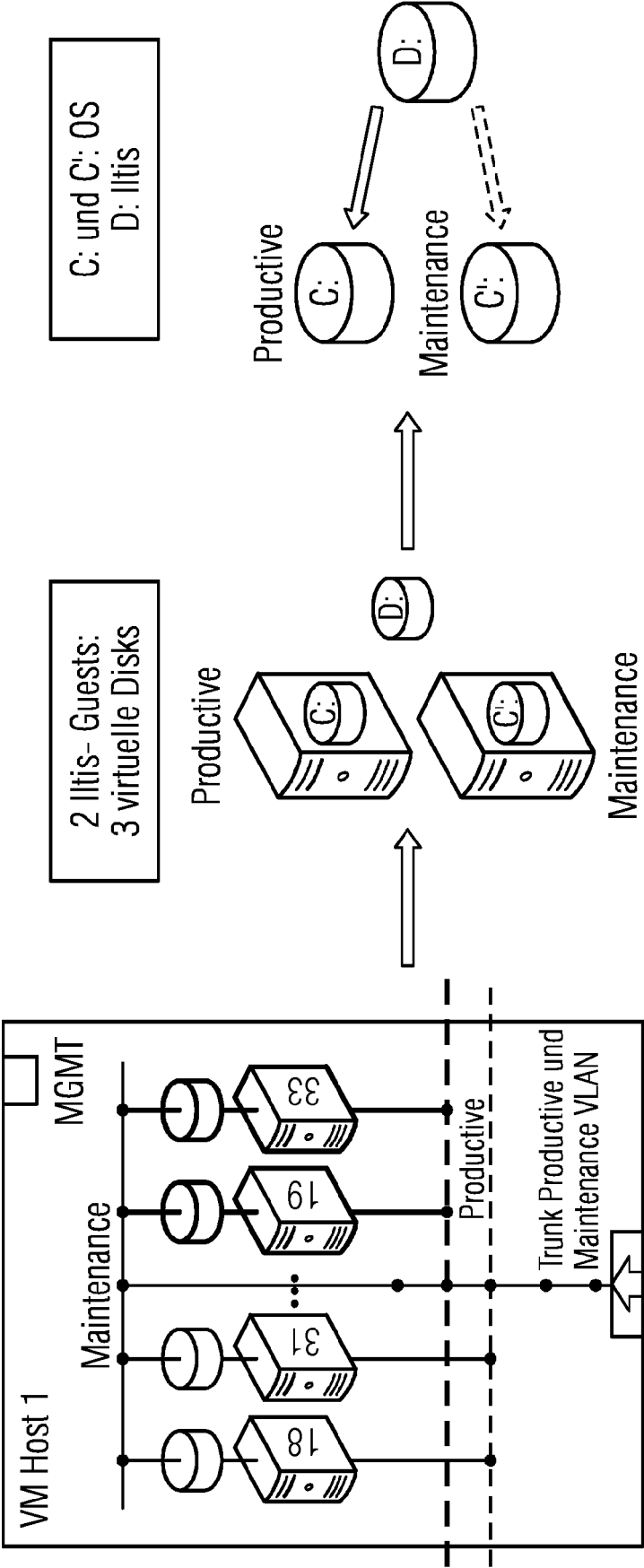


FIG 3

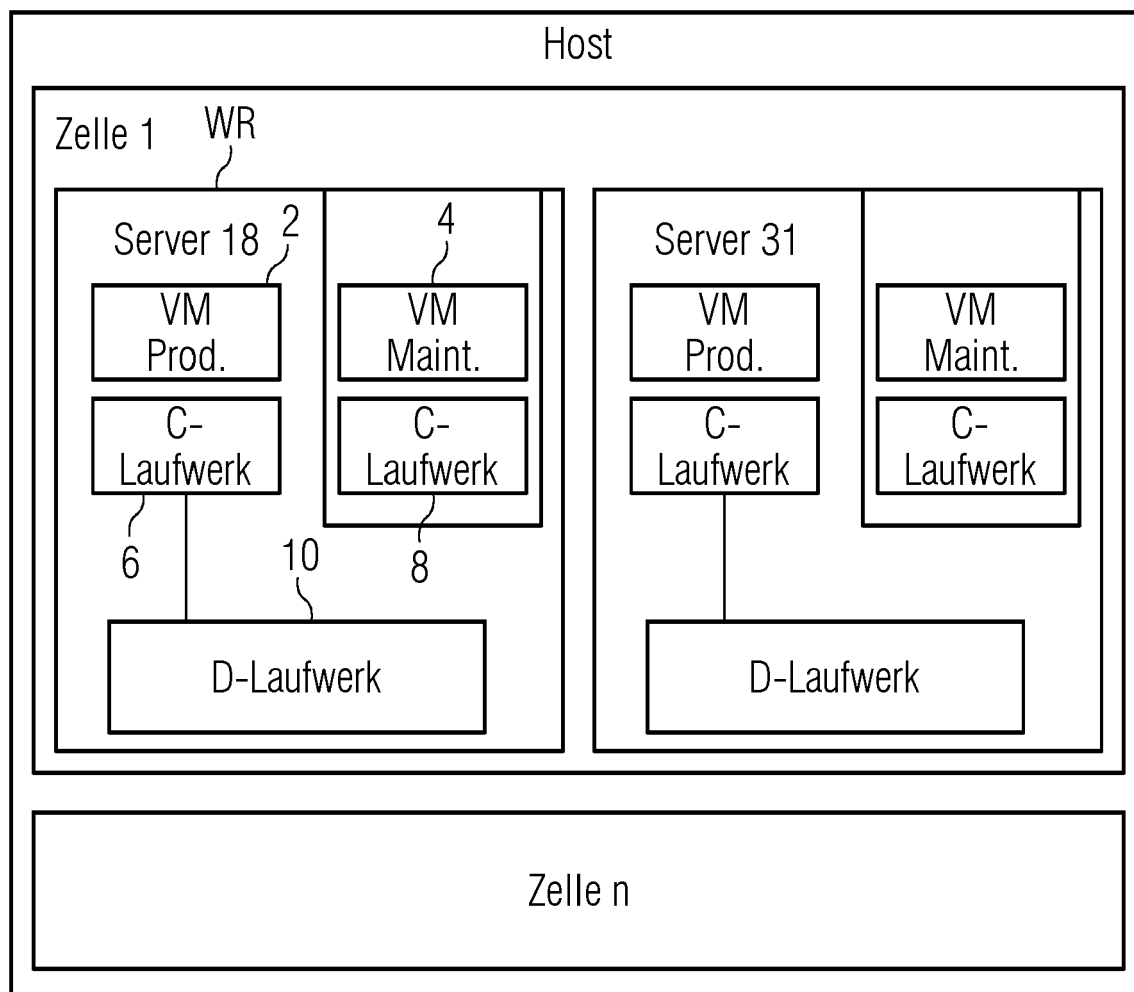
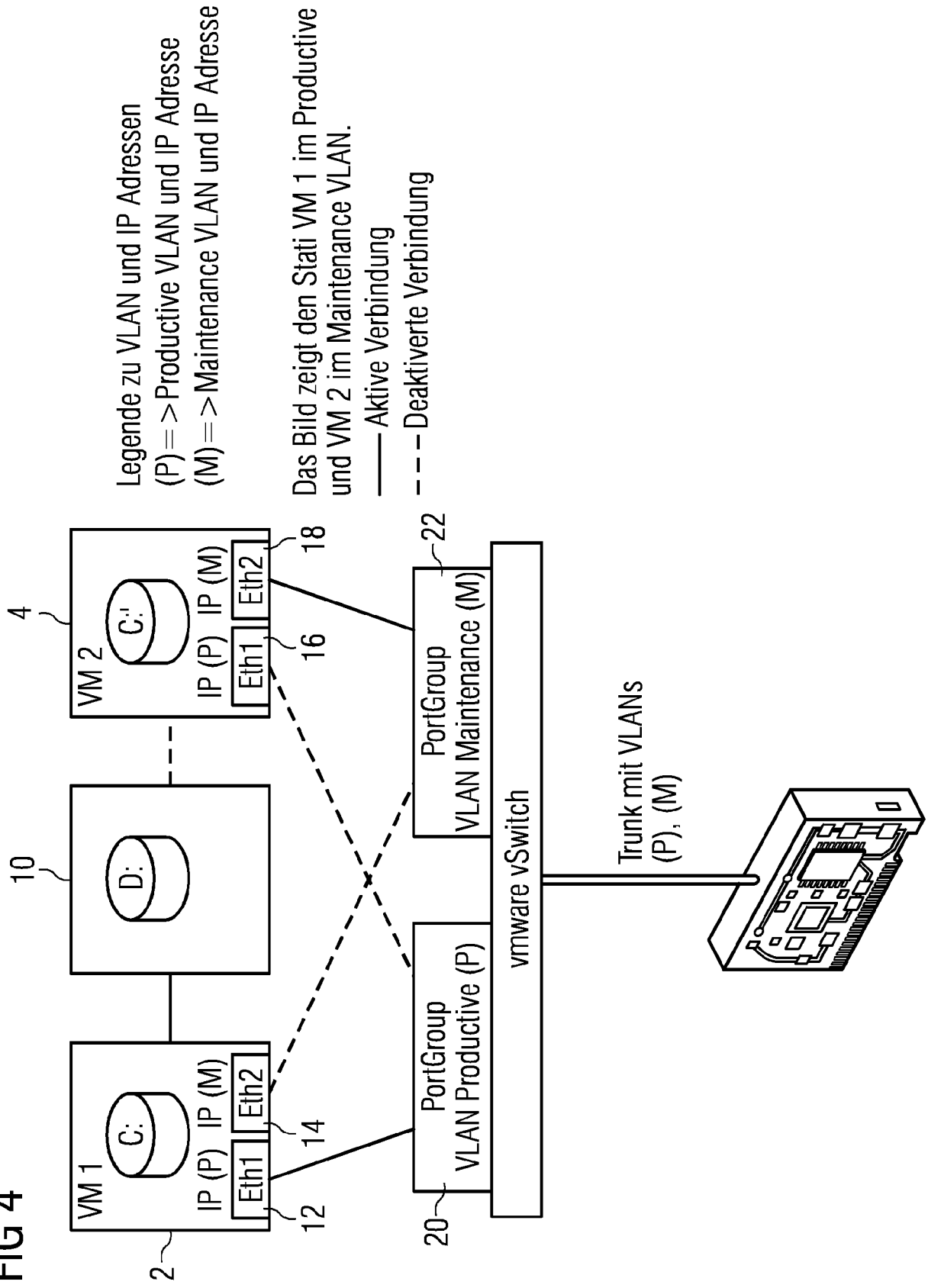


FIG 4





EUROPÄISCHER RECHERCHENBERICHT

 Nummer der Anmeldung
EP 20 16 7131

5

10

15

20

25

30

35

40

45

50

55

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	US 2015/281054 A1 (UTGIKAR ANANT P [IN] ET AL) 1. Oktober 2015 (2015-10-01) * Absätze [0025] - [0026], [0031] - [0064]; Abbildungen 1,2, 3a-3d * -----	1-5	INV. G06F8/658 G06F11/14 G06F9/455
			RECHERCHIERTE SACHGEBIETE (IPC)
			G06F
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort München		Abschlußdatum der Recherche 29. September 2020	Prüfer Gafita, Cristinel
KATEGORIE DER GENANNTEN DOKUMENTE X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : mündliche Offenbarung P : Zwischenliteratur		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	

EPO FORM 1503 03.82 (P04C03)

**ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT
 ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.**

EP 20 16 7131

5 In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
 Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
 Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

29-09-2020

10	Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
	US 2015281054 A1	01-10-2015	US 2015281054 A1	01-10-2015
			WO 2015145291 A1	01-10-2015
15	-----			
20				
25				
30				
35				
40				
45				
50				
55				

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82